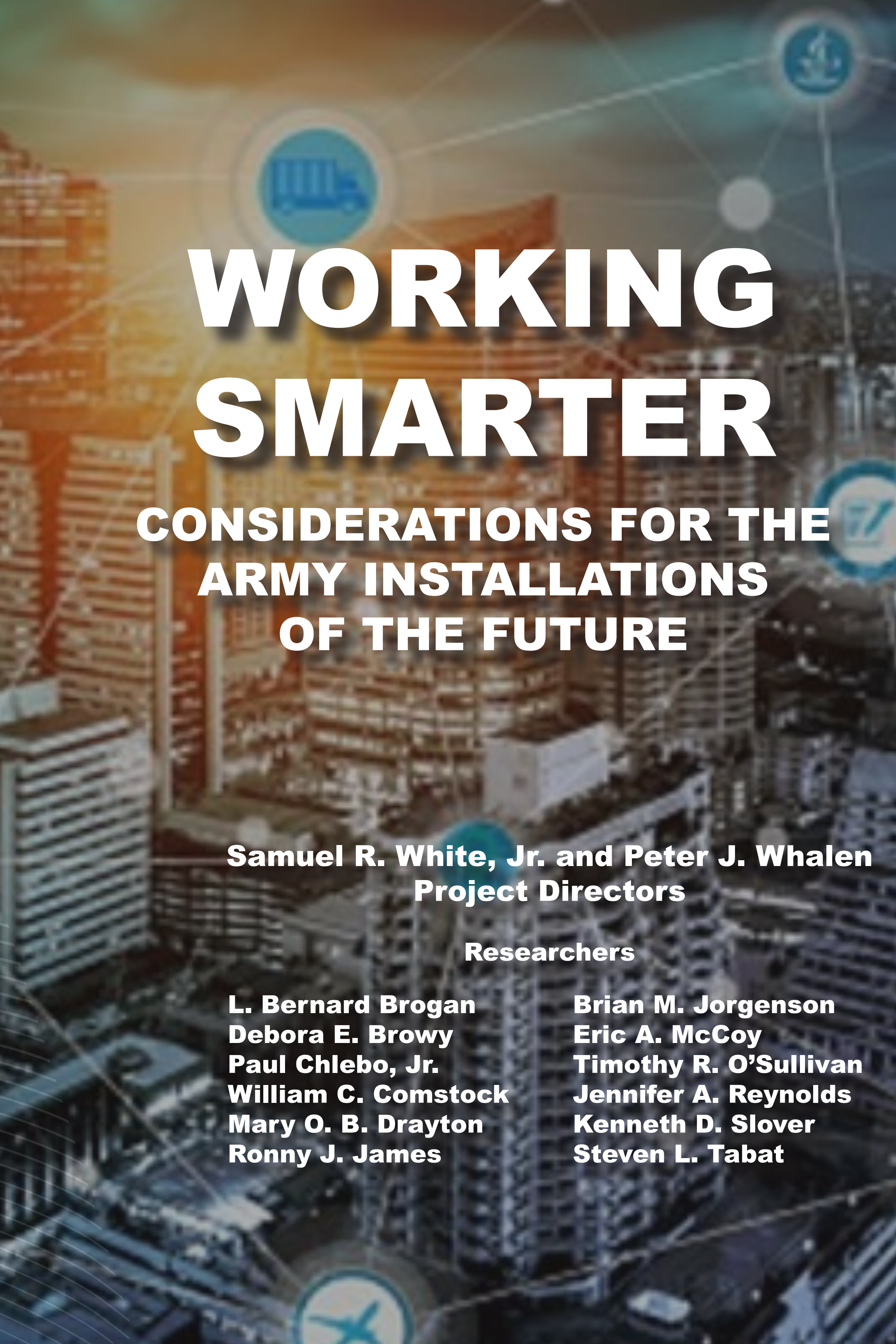

WORKING SMARTER

CONSIDERATIONS FOR THE ARMY INSTALLATIONS OF THE FUTURE

Samuel R. White, Jr. and Peter J. Whalen
Project Directors

Researchers

L. Bernard Brogan
Debora E. Browy
Paul Chlebo, Jr.
William C. Comstock
Mary O. B. Drayton
Ronny J. James

Brian M. Jorgenson
Eric A. McCoy
Timothy R. O'Sullivan
Jennifer A. Reynolds
Kenneth D. Slover
Steven L. Tabat

TABLE OF CONTENTS

FOREWORD

In December 2017 the US Army War College received a request from Mr. Jordan Gillis, then Acting Assistant Secretary of the Army for Installations, Energy, and Environment for research support to assist in examining the development of Installations of the Future (IotF).

The ASA IEE is engaged in a critical and long-term effort to ensure installations have the necessary capability to support soldiers and units now and into the future. The research would help to provide ASA IEE answers to the key question, “What do we want or need installations to do in 20 years or so, in support of our warfighters?”

In support of the ASA IEE effort to understand the capabilities for the Installation of the Future, the U.S. Army War College conducted an eight-month project employing faculty and student researchers to study the possible requirements and capabilities of the IotF and its implications to the Army’s Multi-Domain Operations concept by the year 2035. Given the numerous considerations for the IotF across force design categories (DOTMLPF-P), the students were challenged to focus in certain key areas that they determined. Those key areas are: Infrastructure, Services, Security, and Enabling Capabilities. This determination was based on guidance provided by the ASA IEE leadership. The study team delivered research that addressed

The insights from the team’s research was delivered in an oral presentation to the ASA IEE prior to student graduation. Their presentation, along with this compendium, provides the ASA IEE with ideas and considerations that should assist with their development of this critical Army platform to support future conflicts.

SUMMARY

The vision of the Installation of the Future (IotF) initiative is:

Installations – the Army's initial maneuver platforms – will build readiness, enhance resilience, protect and project forces, through innovation, technology, and partnerships as part of a complex, multi-domain battlespace.[1]

The IotF initiative applies the emerging threats, the expansion of and access to technologies, and the Army's emerging concept of Multi-Domain Operations to set the foundation for the need to prepare installations to meet the need of the future force. This initiative is comprised of three Lines of Effort that addresses the installation's role in preparing the force to conduct combat operations, support the conduct of combat operations, and delivering services and support to the installation, soldiers and their families. This framework provided the students of the Academic Year 2019 Futures Seminar the opportunity to assist the ASA IEE in thinking about ideas, capabilities, and approaches to help achieve the ASA IEE vision. This research focused on four areas: Infrastructure, Services, Security, and Enabling Capabilities.

INFRASTRUCTURE

With the rise of asymmetric adversaries and the acknowledgement in the National Defense Strategy that the homeland is no longer a sanctuary, installations are becoming more vulnerable. There is a need to address the capability gaps and infrastructure of the Army's mobilization and force generation installations and power-projection platforms.

The resiliency of Army installations and its communications networks requires improvement in order to confront adversaries that may pose a risk to them. Identifying and resourcing gaps, investing in resilient technologies, and improving governance are necessary to improve the resilience of installations and networks.

The Army's Multi-Domain Operations concept addresses the shift from counterinsurgency to large scale ground combat operations against a near-peer adversary. Installations need to improve its training capabilities by integrating technology, understanding the threat, and replicating the operational environment to train soldiers to conduct multi-domain operations

SERVICES

With the increase in technology, the role of electricity and the need to sustain its availability becomes critical to installation operations in preparing and engaging in future conflict. Installations will be challenged to protect the sources of electricity from adversary denial and environmental damage to the infrastructure.

The increased speed of combat requires forces to be ready quickly. Installations also need to possess the necessary medical capabilities to help ensure soldiers readiness to support future mission requirements.

The operational environment in 2035 and the needs of future installations will likely impact the role of contracted services. Changes in contracting processes will be required to address the needs of installations in this time horizon.

SECURITY

The current National Defense Strategy acknowledges that the homeland is now a part of the battlespace. In order to meet this reality, U.S. doctrine and policies pertaining to the role of the military in Homeland Defense requires review and modification to address the operational needs of installations within Multi-Domain Operations.

The growth in technologies now provides greater opportunities for future installations to employ these capabilities. A number of recommendations are argued for the use of technologies to improve the installation's force protection capability against the current and future threats.

Along with improving installation security, airfield security also requires improvement to combat emerging threats. Airfields in the homeland are more susceptible to adversary actions. The asymmetric nature of future conflict compels a review of how airfields are defended along with the policies that address airfield operations and responsiveness.

ENABLING CAPABILITIES

Technology can provide the Army with considerations for how the Installations of the Future could operate differently. With the growing amount of data generated and accessible, a digital governance model could be an alternative to use this growing data pool to best conduct the operations within future installations.

This growth of data will also challenge the Army's ability to manage it in order to use it at the point of need and to apply it in support of military operations. Keeping data current, consistent, and available will be key to supporting Installations of the Future.

Technology and data are two factors that contribute to the application of mission command. Installations of the Future could be included in that by the use of an Installation Mission Command Center. This operational design would look to maximize technology and data to enable mission command as well as to increase internal and external collaboration with partners to support Multi-Domain Operations in the future operational environment.

INTRODUCTION

Mr. Peter J. Whalen

The Department of Defense's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation. Should deterrence fail, the Joint Force is prepared to win.

2018 National Defense Strategy[2]

The U.S. Army's mission is "to deploy, fight and win our nation's wars by providing ready, prompt and sustained land dominance by Army forces across the full spectrum of conflict as part of the joint force".[3] Army installations and its functions contribute to preparing the Army to provide a deterrent capability for the Joint Force. Army installations are a key component to soldier and unit readiness. They also provide other important roles for the Army such as capabilities that support force projection. Installations help promote more resilient and efficient use of energy and deliver a number of services to support the soldier, families, and veterans. Installations also serve to foster the Army's relationship with the civilian world through public and private partnerships.[4]

The Assistant Secretary of the Army for Installations, Energy, and Environment (ASA IE&E) is examining ways to modernize and adjust the role of Army installations supporting future conflicts. The changing character of warfare, the future operational environment, and the role of technology are drivers of change to the composition and capabilities of future Army installations.[5]

The current ASA IE&E vision for Army Installations of the Future understands the changing role they will play in this country's wars. It says:

> *Installations – the Army's initial maneuver platforms – will build readiness, enhance resilience, protect and project forces, through innovation, technology, and partnerships as part of a complex, multi-domain battlespace*

Achieving this vision will be pursued through three Lines of Effort: Support the Army as it Prepares for War, Prosecution of War, and Provide Enabling Capabilities.

The Future OE

The conditions that Installations of the Future operate in will contribute to the capabilities resident within them. The U.S. Army Training and Doctrine Command (TRADOC) G2 assesses that the nature of war remains centered on fear, honor, and interest but that the character of war will likely change. Technology and speed are central to this change in the conduct of warfare. In its publication, *The Operational Environment and the Changing Character of Future Warfare*, TRADOC G2 posits:

> The proliferation of high technology coupled with the speed of human interaction and pervasive connectivity means that no one nation will have an absolute strategic advantage in capabilities, and even when breakthroughs occur, the advantages they confer will be fleeting, as rivals quickly adapt. While individual nations may have real advantages in certain technologies or

capabilities, it is unlikely that any will have a decisive edge, meaning that a rough strategic parity will prevail.[6]

Technology will not only create parity but will also extend reach. The publication goes on to say,

> Nations, non-state actors, and even individuals will be able to target military forces and civilian infrastructure at increasing – often over intercontinental – ranges using a host of conventional and unconventional means…. including weapons of mass destruction, hypersonic conventional weapons, and perhaps most critically, cyber weapons and information warfare.[7]

When it comes to specific technological capabilities, the application of Artificial Intelligence (AI) and Robotics and Autonomous systems are often the ones that will factor in military operations in the future. The 2018 Department of Defense Artificial Intelligence Strategy states that it will use AI in a human-centered manner to aid in decision-making in order to reduce risk and create military advantage.[8] The strategy addresses the value of AI in the defense of the homeland. It says, "AI can enhance our ability to predict, identify, and respond to cyber and physical threats from a range of sources, strengthening the defense of the homeland from attack and discouraging attempts to disrupt U.S. infrastructure such as financial networks, electric grids, election processes, and medical systems."[9]

In its Robotic and Autonomous Systems Strategy, the Army pursues the use of these systems to improve its combat effectiveness, learn and adapt in uncertain situations, and to enable leaders to make decisions to achieve gains. These uses will help the Army address the challenges of the increased speed of adversary actions and their increased use of RAS, as well as the challenge of increased congestion of dense urban environments. [10] By the 2035 time frame, the strategy seeks to have autonomous systems fully integrated allowing soldiers to focus on mission execution rather than operating these systems. Achieving this objective will enable commanders to consider and employ multiple options to task organize and fight given the environmental conditions.[11]

An area of interest by the ASA IE&E is the use of Smart Technology at Installation of the Future. According to the website Netlingo, “The term “smart” originally comes from the acronym “Self-Monitoring, Analysis and Reporting Technology” but become widely known as “smart” because of the notion of allowing previously inanimate objects—from cars to basketballs to clothes—to talk back to us and even guide our behavior.”[12] Internet of Things (IoT) devices are a type of smart technology that are software-defined products that are a combination of product, application, analytics and the Internet/networking. They create more value than smart or connected devices. That’s because they are more scalable, upgradable, automated and future ready.[13] This technology is at the heart of the development of smart cities. The ASA IE&E seeks to use these technologies to create smart installations to improve how the Army builds and monitors individual and unit readiness.[14] In its 2017 report titled “Byting the Bullet”, the Deloitte Center for Government Insights asserts that, “a military base that employs smart technologies is better positioned to carry out its mission.”[15]

These technological capabilities will generate larger amounts of data. The usefulness of this data becomes information. The role of information will grow in importance in future conflicts as military parity is achieved. TRADOC G2 sees the use of information to target an enemy’s will. They state that, Sophisticated, nuanced information operations, taking advantage of an ability to directly target an affected audience through cyber operations or other forms of influence operations, and reinforced by a credible capable armed force can bend an adversary's will before battle is joined…. The most effective campaigns are ones that wield all elements of national power to compel an adversary to take or to acquiesce to a specific action, and it will be much easier, cheaper, and effective to use information, backed by credible military force, to achieve these goals.[16]

Strategic Guidance

The National Defense Strategy (NDS) and the U.S. Army Multi-Domain Operations (MDO) concept help set the conditions to drive the development of the Installation of the Future. The NDS states,

"It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated".[17]

With the homeland no longer considered a sanctuary, CONUS-based installations should be viewed as part of the battlespace. This condition merits the consideration for how Installations of the Future should be designed and what capabilities they possess to support operations in future conflicts.

Installations of the Future need to be factored into the Army's emerging MDO concept. The concept of MDO looks to address the problem of layered standoff generated by adversaries. The rapid and continuous integration of the five domains (land, air, sea, cyber, space) to deter during competition. If deterrence is not achieved then the Army formations look to penetrate and dis-integrate enemy standoff systems to exploit the acquired freedom of maneuver to defeat these systems along with enemy formations and objectives to help achieve U.S. strategic objectives and return to competition.[18]

The MDO framework describes seven areas in the battlespace. Figure 1 illustrates these areas. Based on the description, CONUS-based installations would now become part of the Strategic Support Area within the MDO framework. Along with consideration of design and capabilities, policies and authorities may need to be reviewed and updated to address the role of Installations of the Future supporting MDO.

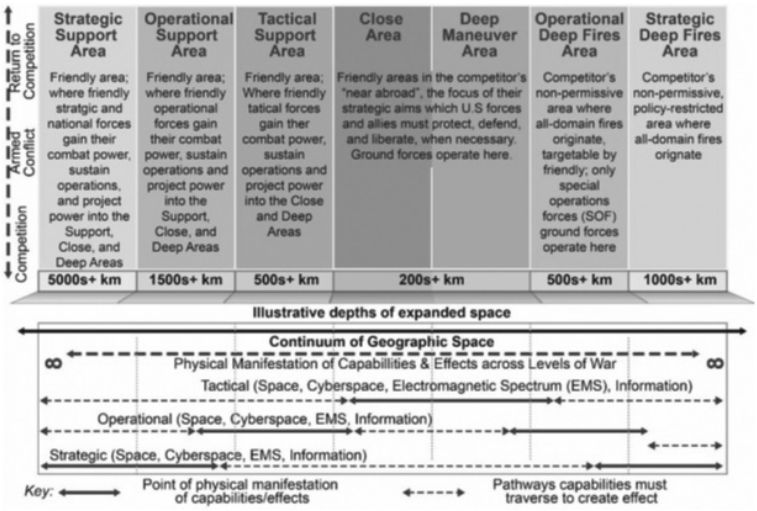
Return to Competition
Armed Conflict
Competition
Strategic Support Area
Friendly area; where friendly stratgic and national forces gain their combat power, sustain operations, and project power into the Support, Close, and Deep Areas
Operational Support Area
Friendly area; where friendly operational forces gain their combat power, sustain operations and project power into the Support, Close, and Deep Areas
Tactical Support Area
Friendly area; Where friendly tatical forces gain ther combat power, sustain operations and project power into the Close and Deep Areas
Close Area
Deep Maneuver Area
Friendly areas in the competitor's "near abroad", the focus of their strategic aims which U.S forces and allies must protect, defend, and liberate, when necessary. Ground forces operate here.
Operational Deep Fires Area
Competitor's non-permissive area where all-domain fires originate, targetable by friendly; only special operations forces (SOF) ground forces operate here
Strategic Deep Fires Area
Competitor's non-permissive, policy-restricted area where all-domain fires orignate
5000s+ km
1500s+ km
500s+ km
200s+ km
500s+ km
1000s+ km
Illustrative depths of expanded space
Continuum of Geographic Space
∞
Physical Manifestation of Capabilities & Effects across Levels of War
∞
Tactical (Space, Cyberspace, Electromagnetic Spectrum (EMS), Information)
Operational (Space, Cyberspace, EMS, Information)
Strategic (Space, Cyberspace, EMS, Information)
Key:
Point of physical manifestation of capabilities/effects
Pathways capabilities must traverse to create effect

Figure 1. MDO Framework[19]

The MDO concept identifies the Strategic Support Area as an area where strategic and national forces gain combat power, sustain operations and project power into the other areas. The enemy will attack the Strategic Support Area to disrupt and degrade deployments by using strategic lethal and nonlethal weapons, as well as special operations reconnaissance and strikes.[20]

Installations of the Future can play important roles for the Army in both the Competition and the Conflict phases of Multi-Domain Operations. The combination of the future operational environment and the homeland as part of the operational framework indicates that installations will need to be more operationally focused to combat adversarial threats.

Threats

U.S. Defense strategy and concepts are written with the return of its focus on great power competition. In a speech soon after the release of the most recent National Defense Strategy, Defense Secretary Mattis said, “We will continue to prosecute the campaign against terrorists that we are engaged in today, but great power competition, not terrorism, is now the primary focus of U.S. national security,”[21] China and Russia are at the heart of this competition. The NDS states. “Long-term strategic competitions with China and Russia are the principal priorities for the Department (of Defense), and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future.[22] The Army’s Multi Domain Operations concept is also centered on these two adversaries. It notes, “They are deploying capabilities to fight the US through multiple layers of stand-off in all domains – space, cyber, air, sea, and land.”[23]

China’s national security strategy is centered on its national rejuvenation and becoming a global power.[24] Its military continues to modernize its capabilities to protect its national security interests while expanding into the cyber and space domains. China’s use of cyber espionage against the U.S. government and corporations is a persistent threat aimed at gaining economic advantage, disrupting critical infrastructure, and shaping information.[25] Its intelligence services continue to exploit the open U.S. society to serve national interests. There is also concern that the intelligence services are using Chinese technology companies as espionage platforms.[26]

Russia's geopolitical aims are to regain its status as a world power in order to counter the United States' role in the international order.[27] It also approaches conflict where war is undeclared to achieve limited political objectives by using all domains.[28] This is reinforced in the 2019 Worldwide Threat Assessment. It states that "Moscow views military force as key to safeguarding its vital interests and supporting its foreign policy; it is becoming more modernized and capable across all military domains and maintains the world's largest operational nuclear stockpile."[29] These capabilities have the ability to reach the homeland. The assessment also states that "Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat."[30] Its intelligence services will continue to target the U.S. to undermine U.S. policies and relationships while increasing its status.[31]

Methodology

In order to frame the student research, the Futures Seminar took an iterative approach. The students received a presentation from then Acting Assistant Secretary of the Army for Installations, Energy, and Environment, Mr. Jordan Gillis and Deputy Assistant Secretary, Mr. Richard Kidd. This session provided the vision, conditions, and outcomes that drive the Installation of the Future initiative.

The students then devoted the next two class periods to brainstorming the information they received to identify categories that could contribute to the development of Installations of the Future. These brainstorming sessions resulted in four main areas to focus student research. They were:

1. Infrastructure

2. Services

3. Security

4. Enabling Capabilities

The students self-selected their area of interest resulting in three students per area. The students then developed the research topics within the assigned area.

Along with developing the research categories, a set of assumptions were identified to help enable the research in a 2035 time frame. The research would focus on Army Installations based in the Continental United States. This was done since the majority reside there, the trend of the Army becoming a more expeditionary force, and the current strategies acknowledging that the homeland is no longer a sanctuary. The United States Army in 2035 would remain an All-Volunteer Force with the current Active and Reserve Components. Finally, the research would be informed by current DoD and Army policies and budgets but not constrained by them in order to consider changes in 2035.

From this methodology and baseline conditions, the students conducted their individual research projects. The results of that research is captured in the following chapters.

Section One:
INFRASTRUCTURE

MOBILIZATION, FORCE GENERATION, AND POWER PROJECTION INSTALLATIONS OF 2035

LTC Eric McCoy, U.S. Army

If the U.S. has a prolonged mobilization timeline, a smart strategy for a nation wishing to secure regional interests contrary to U.S. interests is to do it fast: achieve your objectives…before the U.S.-based forces arrive….

—Major General Joseph Whitlock[32]

Without adequate resourcing, mobilization and deployment infrastructure will remain the Achilles' heel of the U.S. Army's power projection capability. Homeland installations, railways, and ports are lucrative targets for adversaries seeking asymmetrical means to disrupt Army combat power projection. In the *2018 U.S. National Defense Strategy (NDS),* Secretary Jim Mattis warned, "the homeland is no longer a sanctuary."[33] A nightmare scenario for Army senior leaders involves a great power competitor with anti-access/area denial (A2AD) capability that reaches into the homeland to interdict the rapid mobilization and deployment of key active and reserve component units. An A2AD capability could manifest in many ways; blown rail lines, destroyed port facilities, and cyber-attacks against key low-density logistics and other such tactics. If these vulnerabilities are not addressed, the U.S. can expect near-peer interdictions to disrupt or delay the deployment of Army forces and give great power competitors success by fait accompli.

The Army identified this threat in its newly published concept of multi-domain operations (MDO) that defines the strategic support area as the area of cross-combatant command coordination, strategic sea and air lines of communications, and the homeland.[34] Joint sustainment functions required for MDO campaigning throughout competition and armed conflict emanate from this area. In the Future Operational Environment (FOE) of 2035 and beyond, this doctrine anticipates enemy attacks on the strategic support area to disrupt and degrade deployments of military forces attempting to access to the operational support area and move to the close area. Near-peer adversaries will likely take advantage of the unprecedented ranges of emerging strategic lethal and nonlethal weapons, as well as special operations reconnaissance and strikes.[35]

The U.S. has not faced an adversary capable of catastrophically disrupting its theater lines of supply and deployment since the Cold War. Accordingly, the Joint Logistics Enterprise that serves as a backbone for mobilization, force generation, and deployment has suffered neglect and chronic underfunding relative to other Department of Defense (DoD) priorities.[36] Yet, the Army's installations generate, project, and sustain every aspect of combat capability. In the fiscal year (FY) 2019 budget request, the Army made deliberate choices to ensure its formations are prepared to train, fight, and win wars. Senior Army leadership dedicated approximately $10.8 billion to improve maintenance and repair mission facilities (e.g., airfields, training areas, maintenance facilities, roads, ports, dams, bridges, housing, and barracks), which directly enhance and enable readiness.[37] It is essential that the Army also develop enterprise wide strategies to optimize the infrastructure required to raise, train, equip, deploy, and ensure the readiness of all Army forces beyond 2035. Particularly, the infrastructure that is essential to assemble and project combat power forward in support of combatant commander requirements.[38]

Although mobilization and deployment are distinct activities, they intersect at the Army's mobilization and force generation installations (MFGIs) that also function as essential power-projection platforms (PPPs).[39] The current enterprise approach to mobilization and deployment however is ill-suited to the FOE of 2035. Without timely intervention, leaders will not be able to effectively resource the Army's PPPs and active, inactive, and contingency MFGIs to meet the volume and speed required for full mobilization and deployment of the total force in response to MDO threats.

This paper addresses this problem by identifying current shortfalls and making recommendations to address capability gaps. This paper also focuses on infrastructure that enables MFGIs and PPPs to receive, resource, train, and deploy Army forces in support of combatant commander requirements in the FOE. The recommendations presented support initiatives of the U.S. Army Installation Command (IMCOM) aligned to the command's "prepare, prosecute and enable" lines of effort that enable mobilization, force generation, and power projection despite potential enemy disruption activities in the strategic support area.

Framing the Current Operational Environment

Mobilization and sustainability are important elements of military preparedness. Historically, the Army performs best when diversified installations facilitate essential training and furnish essential support. Along with daily installation support and peacetime support capabilities, mobilization and sustainability also addresses the surge capabilities necessary to set the theater and project national power.[40] There are challenges in evaluating logistics preparation of the 2035-2050 FOE. Much of the defense enterprise works within the current program objective memorandum (POM) cycle, primarily two to six years out from the current FY. U.S. Transportation Command (TRANSCOM), in conjunction with the services, assesses and advocates for various military construction (MILCON) projects at the MFGIs and PPPs.[41]

The following assumptions informed the research effort: the Army will be more expeditionary, mission tailored, regionally aligned, and globally responsive; U.S. adversaries will first target and disrupt operations at Army installations during early stages of crisis; the Army will remain as an All-Volunteer Force, leveraged across active, reserve, and national guard components in 2035; research efforts will focus on CONUS-based Army installations primarily serving the active component; the Army in 2035 will be a CONUS-based expeditionary force; the Army will continue to support and integrate with the Joint Logistics Enterprise (JLEnt) which includes the Joint Deployment and Distribution Enterprise; the Army will continue to execute MDO in 2035; U.S. laws governing the role of the Army within the homeland will remain unchanged, and the U.S. will maintain a viable and responsive industrial base with sufficient surge capacity to sustain MDO.[42]

Active MFGIs

MFGIs are Army installations, joint bases, or federally activated state-operated installations designed to provide mobilization support for both current and contingency operations. MFGIs provide pre-and post-mobilization support and deployment preparation in support of combatant command requirements.[43] Further stratified, primary MFGIs are installations that can provide continuous pre- and post-mobilization training, combat preparation, and sustainment. Minimum infrastructure requirements for MFGIs include: reserve component unit mission command facilities; billeting facilities; dining facilities; weapons ranges, training areas, and simulators; motor pools; container yards, reception facilities; retail supply facilities; central issue facilities (CIFs); and ammunition storage facilities.[44] MFGIs designated as primary and active can mobilize designated forces within 14 days of notification of alert or operational commencement (C+14).[45]

Inactive MFGIs

The Army enterprise will resource inactive MFGIs to be fully operationally capable and able to mobilize designated forces within 21 days of operational commencement (C+21). HQDA has designated select US Army Training and Doctrine Command (TRADOC) Army Training Centers (ATCs) to conduct mobilization of select individual ready reserve (IRR) personnel beginning at 30 days of operational commencement (C+30) through 60 days of operational commencement (C+60).[46]

Contingency MFGIs

HQDA designates contingency MFGIs as installations utilized when mobilizing force generating installations exceed primary MFGI operational capacity. MFGIs designated as contingency are currently inactive with minimum MFGI capability, but not resourced. On order, the Army logistics enterprise will resource contingency MFGIs to fully mission capable (FMC) status for mobilizing designated forces after operational demand for mobilized forces exceeds the capacity of primary MFGIs.[47]

Power Projection Platforms (PPPs)

PPPs are Army installations and joint bases that can deploy one or more Army Brigades in accordance with combatant command requirements within 10 days or less.[48] Minimum infrastructure requirements for PPPs include rail load complexes, arrival/departure airfield control group (ADACG) complexes, airfields or airports of embarkation (APOEs) within 50 miles of the installation, commercial truck load complexes, container storage complexes, deployment staging area complexes, privately owned vehicle (POV) storage yards, and Soldier Readiness Processing (SRP) facilities.[49]

Framing the Problem for a Future Operating Environment (FOE)

The Army's MFGIs and PPPs must determine an effective and sustainable means to support MDO in 2035, at sufficient scale, for ample duration, and in coordination with joint, interorganizational, and multinational partners, in order to provide ready forces in support of combatant command requirements. Key social, business, and technology trends will drive changes that affect MFGI and PPP operations in 2035. An increasing number of customers will demand an experience with suppliers that allows them to decide how and when to be involved in decisions from point of sale to manufacturing and delivery. The Army will see use of mobile and wearable devices significantly changing how manufacturing, order fulfillment, delivery, and human resource perspectives influence sustainment.[50]

The proliferation of the Internet of Things (IoT) enables objects to become smart and participate in event driven sustainment processes. Autonomous devices and systems will characterize the future supply chain and unlock the potential for new military applications within mobilization and force generation processes. Civilian consumer demand for cloud-based sustainment services that make secure data and services available remotely will drive innovation within the defense acquisition processes. Finally, the Army enterprise acknowledges the potential for big data to enhance decision support that leads to optimizing sustainment capacity, utilization, and risk reduction.[51]

Army MFGIs and PPPs will sustain MDO in the FOE with a scalable sustainment architecture consisting of numerous routes, modes, nodes, and suppliers that provide multiple options to the supported commander and presents multiple dilemmas to adversaries attempting interdiction within the strategic support area.[52] According to the *2018 NDS*, the DoD intends to prioritize transitioning from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing that includes active and passive defenses.[53] This modification of focus will also inform changes in how bases will support the mobilization, force generation, and deployment of Army forces.

Current sustainment information systems depend on assured communications and access to space capabilities. Moreover, the Army enterprise did not ensure that the design of these systems accounted for disconnected operations. Sustainment information systems support mobilization, force generation, unit readiness, and sustainment operations essential for force projection. Dispersed operations, over extended distances in multiple domains, increase vulnerability to cyber-attack.[54] Successful sustainment operations require protected communications networks and cyber-electromagnetic activities to operate effectively during multi-domain operations in 2035.

Given this problem, the Army must determine the best strategies for infrastructure modernization and development of governance strategies to create resilient MFGIs/PPPs that support the mobilization, generation, and deployment of Army forces to meet future combatant command requirements for multi-domain operations in 2035. The primary challenges associated with this complex and adaptive system for planners, builders, and commanders within the Army enterprise include: incorporating emerging technologies and trends to scale; securing those technologies from, or at least mitigating, external cyber disruption and insider threats; and matching military standards to a wide variety of national and international standards in design, energy output/input, and infrastructure usage.[55]

Necessary short, mid, and long-term operational approaches for change mainly revolve around the triangle formed by innovation, infrastructure, and investment.[56] Innovation for sustainable development requires new formats and partnerships, not least between the Army, academia, and private businesses. The Army must build and refurbish infrastructure in a way that both avoids lock-ins to unsustainable development paths and is resilient to the projected impacts of globalization, urbanization, and environmental change. Additionally, the Army must develop precision logistics that provides reliable, agile, and responsive sustainment capability necessary to support rapid power projection and independent maneuver from the strategic support area to the deep maneuver area.[57]

Developing an Operational Approach for the FOE

To take the fight to the enemy, the U.S. must be able to successfully mobilize the necessary troops, equipment, and supplies at airfields and seaports for deployment overseas. If enemy forces successfully compromise the homeland industrial base, electrical grid, or any other critical MFGI or PPP infrastructure, Army forces will not be able to arrive in theater on time or at all.[58] In addition to strategies focused on installation security and services, infrastructure readiness and modernization will play a critical role in enabling combatant commanders to expand the competitive space.

Recommended near-term and longer solutions target opportunities for investment in technology, reform of business practices within DoD, and public-private partnership (P3) development. The Army's organic industrial base and commercial industry are key strategic partners in this endeavor; enabling military capability by identifying technologies that have military application to maintain overmatch with adversaries. Sustainment challenges at MFGIs and PPPs will require innovative solutions delivered by partnerships not only private industry, but the joint, interorganizational, and multinational community. These partnership efforts must focus on the rapid aggregation and disaggregation of key sustainment nodes in the MFGI/PPP operational apparatus, increased reliance on unmanned systems for routine tasks, and situational understanding through improvements in information systems and network connectivity.[59]

The Army's garrison commanders are key partners with the communities stationed adjacent to installations. Therefore, the installation enterprise must be thoughtful participants in the shaping of policy that influences the design and use of America’s transportation infrastructure. Challenges in achieving bi-partisan consensus will likely affect the development of laws regarding reform, governance, or investment in national infrastructure required to achieve the future vision for the Army’s MFGIs and PPPs.

Finally, total force mobilization plans must identify and incorporate all force enablers—including the reserve component capabilities such as support groups, medical units, and postal units—required to operate the MFGIs. The Army must continue working to establish capacity and capability within the reserve component for surge support augmentation to partial or full mobilization while exploring future technologies that can enable surge capacity at MFGIs and PPPs.[60] The Army also must balance its active-reserve/contractor mix consistent with rapid deployment requirements and operational agility as demanded in the *2018 National Military Strategy (NMS),* to include providing additional full-time reserve manning for early force flow reserve units that the Army will require to source inactive and contingency MFGIs.[61]

Vision of MFGIs/PPPs in the FOE

Rather than conceptualizing installations as concentrations of facilities, the Army defines its MFGIs and PPPs as providers of services to combat future threats within the strategic support area. As concentrated facilities are targets, Installation and Management Command (IMCOM) plans and executes dispersal, arrangement in depth, and redundancy of critical infrastructure that supports mobilization, force generation, and deployment operations.[62] MFGIs and PPPs in 2035 take full advantage of artificial intelligence, automation, sensing, advanced materials, high-powered computing, and secure networks to drive the operation of cost-informed, durable infrastructure.[63] Future MFGIs and PPPs use these emerging technologies to ensure the safety of Soldiers, Families and Army Civilians in a more permissive strategic support area. Smart infrastructure saves money, conserves resources and sustains resilient operations in the face of multi-domain attack.[64]

Warehousing and Supply Facilities of the Future

There is potential to overhaul the DoD supply and distribution chain in support of warehouse facilities for MFGIs and PPPs beyond 2035. Predictive analytics, demand forecasting, production scheduling, anomaly detection, and supply chain/inventory optimization technologies all have the potential to enhance logistics operations that support supply facilities of future installations.[65] Automated Storage and Retrieval Systems (AS/RS) have the potential to redesign the ways in which warehousing and supply facilities store and distribute goods and services. Evolutions in AS/RS technologies have become a means to control and immediately report the movement of material, providing a critical link in the chain of information systems that control work-in-process and distribution of critical materials. Automated Storage and Retrieval Systems enabled warehouses have the potential to reduce the amount of square footage required for storage while minimizing the number of personnel required to run the system.[66]

Future warehousing technology includes an increased usage of drone technology. Current manual inventory procedures are expensive and time consuming. Timelines for a supply support activity warehouse wall-to-wall inventory are typically from 21 to 30 days.

Use of drones equipped with cameras reduce or eliminate the requirement for humans to conduct inventory operations. After flying all over the warehouse, the drone uploads the scanned information to Army logistics information systems. With help of image recognition, warehouse operations personnel can quickly scan and inventory goods.

The proliferation of radio frequency identification (RFID) technologies has the potential for making drone scanning even easier. The use of these light flying devices has the potential to expand exponentially due to technology evolution such as image recognition, indoor geolocalization and drone automatization.[67] Benefit from the use of drone technology in MFGI/PPP warehouses includes higher inventory accuracy, cost reduction, and inventory time reduction. Conversely, potential limits to this technology include a lack of autonomy and acceptability from the human workforce.

Well-designed cobots have the potential to ease human-machine interface and enhance security. A collaborative robot or “cobot” is a robot intended to interact physically with humans in a shared workspace. These machines can work with Soldiers and civilian workers in same areas and manage risks because of their sensitivity and programming.

Installations would be able to emplace multitask machines in supply facilities and warehouses where needed. Cobots will be useful for repetitive activities such as loading pallets and packing. A consideration for design will be work that emphasizes human-machine teaming and integration instead of human replacement across the force.

Maintenance Facilities of the Future

The future Army will fundamentally reduce the demand characteristics of the force and optimizes the sustainment footprint to become expeditionary and to enable semi-independent MDO. The maintenance posture of Army ground and aviation systems is a demand characteristic that influences the size and scope of maintenance infrastructure. In 2035, the Army's ability to use and improve a conditions-based maintenance strategy for both newly fielded and legacy systems will result in enhanced life cycle system readiness and materiel availability while reducing operating and support costs. Future materiel systems monitor condition autonomously, predict and diagnose faults, and integrate with the sustainment common operating picture (COP) to reduce overall demand for maintenance and optimize the sustainment footprint for MFGIs and PPPs.

Self-maintained machines with auto-diagnostic and enhanced learning capability will make maintenance transparent for installation tenants. With the proliferation of predictive maintenance, robotics, and engineers connecting more equipment to installation infrastructure, capability developers will be able to follow real-time indicators of functioning more easily and build notification systems in anticipation of system failure, increasing system availability. This creates the possibility of completely transparent maintenance systems that interface between installation infrastructure, tenants, and combat systems transmitting real-time use data to maintenance technicians at the field, installation, and enterprise level. Improved system analytics will reduce or eliminate requirements for automated logistics specialists, allowing force designers to gain efficiencies with the reallocation or reduction of manpower in Army manning documents.

Mobility Facilities of the Future

Pervasive computing has the potential to improve transportation infrastructure operation and maintenance enabling the rapid deployment of Army units from CONUS-based installations to aerial and sea ports of embarkation. Networked sensors embedded into road, bridges, and other sensitive surface mobility infrastructure will allow installation leaders to detect strain and hazardous conditions and provide damage assessments after natural disaster or enemy interdiction when infrastructure may not be accessible to soldiers or civilians. This instrumentation has the potential to increase safety and efficiency if it can alert system operator to hazardous conditions sooner or better than manual inspections do, and may, in turn, enable installations to use resources more efficiently for infrastructure maintenance.[68]

Environmental changes in temperature, storm activity, and sea level will affect the design, operation, and maintenance of installation rail facilities. Extreme weather conditions and overpopulation will likely lead to disruptions, damages, and failures in older transportation systems. Many U.S. rail systems are either near shore or below sea level.[69] Engineers must design future rail systems that leverage new composites and the IoT to support reliability.

An emphasis on compacting land use requirements as seen in the Army's design concepts for Camp Humphreys would prove useful for installations of the future to manage internal transportation footprints more efficiently. Garrison management should revise traditional neighborhood development practices and promote policies that decrease personal vehicle travel to reallocate transportation infrastructure capability to support strategic mobility. Installations will engage in innovative public-private partnerships to leverage mass transit options that can quickly move tenants between life support, training, and readiness hubs across the installation. Designing facilities and road networks that can promote an increased use of bicycles and other self-propelled transportation devices supports public health and installation resiliency. Finally, moving to electrically powered vehicles for as many services as feasible on the installation will promote improved energy efficiency as well.

Conclusion

Current policies governing MFGIs and PPPs that define strategic readiness by measuring the usage of installation facilities will not meet the Army's MDO needs in the FOE. Instead, future MFGIs and PPPs must define strategic readiness by their ability to support highly effective, expeditionary and campaign-quality forces that can fight and win in MDO.[70] Adoption of commercial technology and development of joint capabilities can evolve today's installations into tomorrow's key deployment platforms. Even if likelihood of a total mobilization beyond 2035 is low, the high risks and severe consequences of disruption of the strategic support area could be catastrophic for the Army and national security.

Many FOE trends forecasted for 2035-2050 have the potential to either help or hinder the Army's MFGIs and PPPs. Continuous examination of these trends followed by incremental and methodical improvement will produce an Army better postured to take advantage of beneficial progress and mitigate the impacts of harmful developments, thereby ensuring improved Soldier, unit, and installation readiness. At end state, the strategic support area infrastructure must support resilient, reliable, and agile power projection to the deep maneuver area. Clear priorities in infrastructure investment, resource allocation, and revision of policy related to the operation of MFGIs and PPPs must guide the Army as it continues to develop its multi-domain forces of the future.

INSTALLATIONS OF THE FUTURE – ACHIEVING COMMUNICATION NETWORK RESILIENCE

Mr. Paul Chlebo, Department of the Army Civilian

It is now undeniable that the homeland is no longer a sanctuary. America is a target...during conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.

Former Secretary of Defense Jim Mattis[71]

Based upon the Former Secretary of Defense's declaration, Army installations must prepare for the attacks predicted to occur in the future threat environment. Army *Multi-Domain Operations* policy echoes the Former Secretary's position by stating installations in the Strategic Support Area are the battlefield of the future and the enemy will attack them with various forms of unconventional warfare.[72] This concerns Army leaders.

As installations will be the first targets in a future crisis, they must be resilient to remain relevant to the fight. "Resilience is the ability to anticipate, prepare for and adapt to changing conditions and withstand, respond to and recover rapidly from disruptions."[73] The Army concept of resiliency for installation services such as water and energy security must apply as well to installation communication networks. Army leaders want installation key dependencies resilient by the year 2035.[74] One key dependency, the communication network, enables essential installation services and it is at risk.[75]

In the future threat environment, Army installation communication networks as currently deployed will fail due to a lack of network resilience caused by gaps in network architecture and design; insufficient investment in resilient technology; and the need for governance improvements.

This paper assesses the future threat environment and its challenges to current installation communications network capability. It provides options that contribute to more resilient network architecture and design, technology, and governance. Holistically, efforts that achieve resiliency also address quantitative and qualitative gaps that improve overall military preparedness of Army installations to support the fight.[76]

Future Threat Environment

The future threat environment has the Department of Defense (DoD) and Army leaders concerned about the risks to Army installations. Therefore, Army leaders must consider how to make installations and their communications networks more resilient in the coming years because "effective communications have always been vital to military forces."[77] This section assesses strategic guidance concerning the impact of the future threat on installations within the Continental United States (CONUS) Strategic Support Area.

The *2018 National Defense Strategy* set a clear mandate for Army leaders to invest in resilient capabilities. To meet Warfighting requirements, they must "address the scope and pace of our competitors' and adversaries' ambitions and… invest in modernization of key capabilities through sustained, predictable budgets."[78]

The Deputy Assistant Secretary of the Army for Strategic Integration, Mr. Richard Kidd, supports the Office of the Assistant Secretary of the Army for Installations, Energy and Environment (ASA (IE&E)). He stated, “Installations of 2035 are the Army’s initial maneuver platforms. They build readiness, enhance resilience, protect and project forces; all through innovation, technology, and partnerships as part of a complex, multi-domain battlespace.”[79] The Deputy Assistant Secretary’s challenge is to integrate resilient capability at our installations to mitigate the future threat.

Former Director for Joint Force Development, Vice Admiral Kevin D. Scott, wrote of a contested and disordered world in which adversaries may attack military bases to degrade U.S. ability to generate, deploy, and maintain the Joint Force. He stated that command, control, and communications (C3)/intelligence systems require enhanced system protection, greater network redundancy, and automated defenses capable of reacting in a highly dynamic environment.[80]

Finally, the Army Training and Doctrine Command (TRADOC) G2 says of the future threat environment, “Adversaries will… force us to operate with degraded capabilities... a force deploying to a combat zone will be vulnerable from the individual soldier’s residence to his or her installation and during his or her entire deployment.”[81] By denying our ability to command and control in the strategic support area, the enemy will drive our power projection, mobilization and deployment centers to operate under disconnected, intermittent, low-bandwidth (DIL) conditions. The Army can mitigate pause in its operations with more resilient communications.

Descriptions of the future have raised a sense of urgency within the Department of the Army to make key installations more resilient. At the direction of ASA (IE&E), the U.S. Army War College formed a team to research and recommend options that provide this resiliency.

Installation Communication Network Challenges

The challenges to implementing installation communication network resiliency (NETRES) include: current network modernization investments fix legacy networks, not resiliency gaps; need to prioritize installations for NETRES investments; and, adapt policy and process to implement network resilience requirements.

The first challenge is that today's network modernization effort does not align with the future threat. The Army's *Installation Information Infrastructure Modernization Program* (I3MP) manages network modernization (NETMOD) guided by Army policy established in *Army Regulation 25-1 Army Information Technology* and *Army Pamphlet 25-1-1 Army Information Technology Implementation Instructions*.[82] The infrastructure components of I3MP support not only the modernization needs of all installations but also provide the foundation for the resiliency needs of key installations of the future.[83]

I3MP modernizes the current communications technical design at all Army installations. Its major components include modernization of inside plant (ISP - the infrastructure that connects people, sensors, and systems to the installation network) and outside plant (OSP - the pathways that connect an installation network to the global communications network). While I3MP supports the general needs of all installations, infrastructure modernization remains a key dependency for resilient capability. I3MP is a key dependency for all installations as well as those selected for NETRES capabilities.

The next challenge is the prioritization of installations that require NETRES investments. The Army manages installation communication networks at over 250 CONUS and OCONUS installations.[84] Given this quantity of world-wide installations, it is critical that leaders assess the global situation and determine which installations must be more resilient than others. Typically, priority should be toward power projection, mobilization, and deployment centers in CONUS to maximize the opportunity to deploy forces and minimize impacts of enemy disruption activities. However, the dynamics of today's global posture and the Joint Strategic Campaign Plan (JSCP) may require OCONUS NETRES investments.

The final challenge is to adapt policy and governance process to the future threat. While many Army policies and processes must adapt to the future threat environment, the Army needs to update four documents in particular. These documents are the *Army Network Campaign Plan* (ANCP), *Army Regulation 25-1 Army Information Technology, Army Pamphlet 25-1-1 Army Information Technology Implementation Instructions*, and *Army Regulation 525-30 Army Strategic Readiness Assessment Procedures*. A review of these documents appears later in the paper.

Overcoming challenges is not new to the Department of Defense. Strategic leaders strive to understand the environment, understand the problem, develop a vision, and lead change. Overcoming these challenges to resiliency requires the same level of strategic leadership that occurred when the military departments pursued *Network Centric Warfare* in 1999. One of the most significant challenges at that time was to implement an investment strategy that balanced tensions between modernization and readiness.[85] Army leaders must again prepare for tough choices and manage the tensions between modernization and resiliency.

Planning Assumptions

The following assumptions support the consideration of broad options that provide communication resiliency at key installations:[86]

- The communication network will remain the key dependency for installations of the future.
- Army Futures Command will evolve force structure and acquisition systems to enable resiliency within the Strategic Support Area.
- The wired and wireless network infrastructure will expand to support the expected deluge of data and the knowledge transfer requirements of users.
- The installation communication network will provide essential services when isolated from the cloud-based network.
- The Army will validate network resiliency requirements and support them with a predictable, adequate, sustained, and timely Army budget.[87]
- The Army will secure critical network installation communications infrastructure that enables connectivity from tactical, operational, and strategic command posts to the DoD Information Network (DoDIN).
- The Army's cybersecurity efforts will mitigate cyber-attacks on Army installations.

- The Army Theater Signal Commands will organize to support future deployment operations with "*Fort to Port"* strategic communications options.

These assumptions focus on enabling two themes to provide resiliency to key installations of the future. The first theme expands network fiber and wireless capability across the installation. This supports mobilization demands as well as the expansion of the internet of things, autonomous systems, artificial intelligence, and robotic systems. The second theme is a network design must support essential Warfighter services when isolated from cloud-based capabilities. These themes build an infrastructure capable of adapting to enemy disruption activities.

Target Objectives for Installations of the Future Communications

The communication network is a key enabler critical to Unified Land Operations described in *Army Doctrine Publication 3-0 Operations.* The Army DA CIO/G-6 enables these operations by focusing on four priorities: a flat network (converged infrastructure); a fast network (ability to enable Army decision making); a mobile network (transition to multi-domain battle); and, a protected network (able to see and defend the network).[88] These priorities guide the design of the networks needed to in a Multi-Domain environment from tactical to strategic.

Army leaders should follow the vision of former Army Chief of Staff, General Reimer, and his leadership methodology to build the *Army After Next* (AAN) in 1995. "Development of distant futures is not an exact science… the idea was to put a mark on the wall as to what the Army needed to do in 2020… you try to not so much get it exactly right, but make sure you don't get it exactly wrong."[89]

Following this vision, the target objectives for technology at installations of the future must align with an architecture that enables the Warfighter to operate within the future threat environment. Resilient installations result from the alignment of architecture and design, technology, and governance. This resilience results from network architecture and design considerations. Leaders must establish a vision, gain support, and maximize the conditions that lead to resilience.

Network Architecture and Design Considerations

There are National and Department of Defense mandates for communications architectures that guide implementation of network resiliency. National level guidance states that architectures "shall develop… a transition plan to get to the target architecture… (and) should align business and technology resources to achieve strategic outcomes."[90] The Department of Defense Architecture Framework "is the overarching, comprehensive framework… supporting development and maintenance of architectures required under the Clinger-Cohen Act."[91] Complying with these mandates ensures the alignment of resources and requirements to integrate resilient options for installations of the future. Communications architecture and design considerations provide networks with "enhanced system protection, greater network redundancy, and automated defenses capable of proactive and reactive means within a highly dynamic environment:"[92]

The considerations of the science and technology community fall within three network concepts. First, the network architecture is the structure of all component parts of a network, to include people, processes, and tools.[93] Second, the network design reflects the infrastructure components based upon accepted models.[94]

Third, system quality attributes describe network characteristics (i.e. 'availability, maintainability, etc.). The following network architecture and design considerations inform a transition plan to achieve resilient capability at key installations of the future:

- Increased Availability and Restorability of Network Capacity. Characterized by guaranteed, uninterrupted or quickly restorable communications bandwidth using redundant terrestrial and non-terrestrial means.

- Autonomous Management. Characterized by trusted, ubiquitous network management to support the exponential growth of the internet of things, autonomous systems, artificial intelligence, and robotic capabilities.

- Smart City and Smart Installation relationships. Characterized by mutual support agreements between smart cities and smart installations to share resources during natural disaster or enemy disruption.

- Scalability. An expanded wired and wireless network across installations providing redundant, ubiquitous capabilities to the Warfighter.

- Access to Data and Services. Characterized by installation *'Fit for purpose'* data center concepts based upon the *2018 DoD Cloud Strategy* to provide access to data for installations isolated from cloud-based services.[95]

- Artificial Intelligence. "Architectures must consider future implications of artificial intelligence influences on warfare. The characteristics may require concepts of infinite, distributed command & control capacity…and instant mission adaptations."[96]

Commercial industry offers lessons learned from their support to smart cities and development of innovative concepts. These lessons learned can facilitate the Army's decision process to implement resilient communications options at installations. Examples of these lessons learned include:

- The digital infrastructure is the common denominator and key to digital cities. "They started with a strong foundation of digital infrastructure. From this base, they can continue to innovate and grow."[97]
- "The network transport, fiber, and wireless are the key to digital transformation. The broadband foundation is citywide connectivity, not just for people, not just for smartphones, but for your sensors and other devices."[98]
- The concept of an adaptive network can use automation to rapidly scale, self-configure, and self-optimize to provide resilient capability that adjusts based upon network pressures and demands.[99]

Technology Considerations

Considerations for resilient technologies include: ubiquitous fiber and wireless connectivity throughout the installation to handle future demands; aerial options to restore lost satellite network connectivity; 'Fit for Purpose' data capabilities that support isolated installations; and, geofencing concepts for installation perimeter defense.

In consideration of fiber and wireless infrastructure, there is a shift in communications infrastructure technology to wireless broadband and wireless area networks. Wireless, with all the risks of jamming and other concerns, is becoming the primary means of network connectivity for all users.[100] Therefore, the Army must significantly increase its secure wireless capacity at installations to support the likely exponential growth of users, mobilization tasks, training exercises, increased quantity of devices, autonomous systems, robotics, and artificial intelligence demands.

Fiber infrastructures have both longevity and capacity to support installation communication requirement growth for installations of the future. From a network resiliency perspective, fiber optic cable is a survivable infrastructure component with no known '*end of life'* expiration that can withstand electro-magnetic pulse and other electromagnetic or radio frequency interference events.[101] "Fiber installed in 1980 is still in use today. The increasing bandwidths experienced over time are leveraging the existing fiber – the limiting factor is the light emitting technology available at any given time."[102] Fiber installed today to support planned growth in requirements will support missions well beyond 2035.

'5G' is the newest wireless capability and industry, academia and the Army have yet to innovate the devices, systems, and services that can use it. 5G will support virtually all autonomous, robotic and AI systems. The Army must coordinate with commercial providers to determine the extent of infrastructure growth as 5G technology requires an increased quantity of cell towers across installations and wireless connectivity in buildings which requires additional fiber infrastructure to connect them to the network.[103]

The second technology consideration is a pseudo-satellite network to restore communications to installations isolated from the satellite network. High altitude pseudo-satellites (HAPS) are systems that float or operate for long periods, sometimes for months, at about 20 km above the Earth's surface. HAPS complement satellite systems, are maneuverable and easier to deploy.[104]

Pseudo satellite technology is not readily available and requires research and development to integrate it within Army and DoD communications networks. Fortunately, the Army's Mission Command network has a requirement to re-establish communications for tactical units isolated from their satellite network. One of the Mission Command requirements is to develop "Network Augmentation and Extension" to overcome space and terrestrial shortfalls. These capabilities include "aerial (aerostats, aircraft retransmission payloads) and near space (high altitude balloons)."[105] This Mission Command Network requirement can fulfill the same requirement and restore network connectivity across the Strategic Support Area.

The third technology consideration is the implementation of '*'Fit-for-Purpose'* on- premises cloud environments to support data requirements of installations isolated from the global network. Enabling access to data at the installation level would "conform to the availability and security standards that mitigate resiliency and redundancy issues as provided within data center standards.[106]

The recent *DoD Cloud Strategy* identifies a general-purpose cloud environment, with computing and storage capacity that spans the homeland to the global tactical edge and addresses warfighting challenges at the speed of relevance.[107] However, commanders at installations need the capability to process data gathered at the local level to continue to provide essential services as well as future autonomous and artificial intelligence capability. According to the *DoD Cloud Strategy*, industry made huge strides in disconnected operations that can provide the warfighter with the latest technology where they need it and when they need it, regardless of the environment.[108] The Army must begin the process to establish Fit-for-Purpose cloud environments at key installations to mitigate the risks of the future.[109]

The final technology consideration is the implementation of geofencing options. “Geofencing is a location-based service in which an application, Wi-Fi or cellular capability triggers a pre-programmed action when a drone, mobile device, or RFID tag enters a virtual boundary set up around a geographical location, known as a geofence.”[110] Installations of the future may integrate geofencing as a perimeter defense against drones to protect critical infrastructure. Installation commanders can employ a geofence as a defensive measure against drones approaching the perimeter to thwart enemy surveillance or attack. “The Federal Aviation Administration (FAA) can set up drone-resistant geofences now – some barriers will stop a drone in mid-air, while others will trigger a warning message to the user.”[111]

Given the probability of isolation from the commercial network, Army leaders may decide to pursue an Army-owned geofence capability that operates within the confines of the installation using the local communications network.[112] Army-owned geofences could one day leverage Carnegie Mellon University Robotics Institute technology to identify and interdict unauthorized drones at the perimeter of the installation. Installation commanders need geofencing options to protect their installations in the future.

Governance Considerations

Periodically, governance must adapt to changes caused by innovation and technology. Based on the guidance contained in the *National Defense Strategy* and other previously mentioned documents, one can argue that enemy capabilities are changing the character of war. This change demands a review of governance to enable more resilient installations by the year 2035.

A number of policy documents that govern investments in the communications infrastructure must be updated to align them to the future threat environment. Four documents govern Army communications networks and installation readiness: 1) the *Army Network Campaign Plan (ANCP);* 2) *Army Regulation 25-1 Army Information Technology;* 3) *Army Pamphlet 25-1-1 Army Information Technology Implementation Instructions;* and, 4) *Army Regulation 525-30 Army Strategic Readiness Assessment Procedures.*

The current *Army Network Campaign Plan* requires an update to align its communications network vision to the future threat environment which predicts CONUS installations isolated from the network. “The ANCP envisions a network that spans all Army operations from garrison to the tactical edge. A network that is highly responsive, providing the information necessary to execute decisive actions anytime, anywhere and on any device. This network is based upon industry best practices to transition to the cloud. The key dependency for a transition to a cloud-based network is assured and sufficient bandwidth connectivity from the installation or the Warfighter to the cloud.”[113] The network of the future must include implementation of resilient capabilities that mitigate enemy disruptive attacks to isolate key installations from the cloud.

Army Regulation 25-1 Army Information Technology also requires an alignment to the future threat environment and its language provides the direction to do so. This regulation describes the" information technology management approach that follows a recurring life cycle of planning, investment, and execution. The life cycle begins with the identification of capability gaps provided by emerging guidance or legislation. Analysis of gaps within the planning phase updates problem statements, IT transformational plans, and hardware and software authorization architectures."[114] Analysis of the future threat provided by DoD, the Joint Staff and the Department of the Army provides the mandate to update requirements that address network resiliency gaps within the I3MP Program as well as installation support services.

DA Pamphlet 25-1-1, Army Information Technology Implementation Instructions, describes the roles, responsibilities, and process to manage information technology at the installation level. The DA PAM requires and update to align to the future threat environment ensuring technology managers have the capabilities to support installations while under enemy attack or disruption. As currently organized today, "installations receive existing services from the U.S Army Network Enterprise Technology Command (NETCOM). NETCOM provides common IT services and applications to Army-wide installations through subordinate theater commands, signal brigades and/or battalions and the network enterprise centers (NEC) or regional network enterprise centers (RNEC)."[115] Gaps in network resiliency prevent senior information management officials on installations from providing their mission commander or key tenant units with the capabilities to operate in an isolated environment.

Army Regulation 525-30 directs the assessment of readiness at installations.[116] Updates to this regulation must create new communication resiliency metrics to assess readiness based on the *Joint Capability Areas.* These new metrics can provide a holistic view of military preparedness in the future. The inclusion of AMC and IMCOM in the readiness assessment process ensures commanders influence the communications readiness and preparedness of their installations.

Conclusion

Strategic leaders anticipate Army installations are vulnerable to enemy attack and will fail to accomplish their missions without resilient capabilities. There is evidence that America's enemies will exploit the seams of our strategic infrastructure and these vulnerabilities ensure the success of an enemy 'first strike" which can delay a deployment. The delay of a strategic deployment puts our soldiers at risk, causes doubt among allies, and removes a U.S. diplomatic and military option from the table.

Army senior leaders directed the U.S. Army War College to strategically think about options to mitigate future threats from the lens of the *Joint Operating Environment 2035*. This manuscript recommends the Army aggressively pursue the requirements and acquisition process to make installations more resilient. If a drone can destroy an ammunition storage area in the Ukraine, then a drone can strike our installations of the future."[117] The way ahead is clear, and the recommendation is that senior leaders take action to make installations more resilient before 2035.

EVOLVING ARMY INSTALLATIONS SUPPORT TO TRAINING IN 2035

LTC Timothy O'Sullivan, U.S. Army

We don't rise to the level of our expectations, we fall to the level of our training

Archilochos[118]

Army installations must improve infrastructure for training to prepare forces to fight and win in the future. Emerging technology, adversaries, and operational concepts will change how Army installations support training forces in 2035 and beyond. Adversaries will employ technological advancements in robotics, cyber/electronic warfare, and hypersonic weapons. Great power competition with Russia and China will threaten the homeland and mitigate U.S. strengths through multiple layers of stand-off. The Army's Multi-Domain Operations (MDO) concept requires that installations improve training ranges and facilities to integrate operational effects in land, air, sea, space, and cyber domains across time and space. While community encroachment, environmental conservation laws, and climate change reduce the availability of land for training. The future environment demands that Army installations build readiness and lethality through versatile ranges, robotic targets, and the synthetic training environment (STE).

This paper begins by defining several key terms, describing the current state of Army installations and the impacts of climate change. It then describes future trends in technology, adversaries, and the MDO concept and their impacts on training requirements. Taking these factors into account, the paper provides three recommendations. First, create versatile ranges that enable units to train multiple individual and collective tasks at one facility. Second, develop a family of robotic targets that will improve marksmanship, enable adaptive training, enhance scenario based collective training, and prepare the force to fight enemy robotic systems. Third, employ the STE to support more echelon above brigade training, assess deployment plans, respond to local incidents, and develop the future force.

The term "installation" used throughout U.S. Department of Defense (DoD) doctrine lacks a formal definition.[119] For the purposes of this work, an installation is an enduring physical location with structures, personnel, organizations, and processes that support building readiness, deploying, or sustaining forces. *Department of Army Pamphlet 525-30 Army Strategic Readiness Assessment Procedures* provides the doctrinal framework to evaluate installations by looking at the services, infrastructure, natural infrastructure, energy and water programs.[120] This paper focuses on installation infrastructure and specifically the land and the facilities that support training.

The Evolution and Current State of Army Installations

Today's Army installations provide units with maneuver areas, ranges, and facilities to build readiness through training. Facilities evolved from investments during the Cold War modified to meet the requirements of the Global War on Terror. Army units train using a combination of Live, Virtual, and Constructive enablers collectively called the Integrated Training Environment (ITE).[121] The ITE consists of systems procured over the last 35 years that are expensive to maintain and unable to meet future needs.[122]

In 2012, the DoD published the *Unified Facilities Criteria (UFC) for Installation Master Planning* to improve future development. For training, it requires "ranges and training areas to meet training and test mission on a consistent and long-term bases."[123] It emphasizes vertical mixed-use facilities.[124] Land preservation is another important factor "to provide and maintain a buffer between the civilian community and key functions of a military installation, including range impact areas, airfields, and maneuver areas."[125] Since investments endure for decades and requirements exceed available resources, it is vital for installation planners to understand the future environment to wisely allocate funds.

As the DoD refocuses on great power competition, strategic guidance is moving installations away from economic efficiency to enemy threats. The *2018 National Defense Strategy* calls for moving "from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing that include active and passive defenses."[126] This is significant for training because it requires developing greater resiliency and operational flexibility. Training infrastructure is important because the resources needed to train active duty forces will also support the mobilization of the reserve components.

Encroachment, Conservation, and Climate Change

Population growth outside urban areas is leading to boundary encroachment on installations. While the physical borders of the installations are remaining steady, development along the edges is creating tension between the land owners and military. Development surrounding installations has created "islands of biodiversity" in training areas leading to new environmental regulations and restrictions.[127]

Endangered and threatened species will "cause more restrictions on testing, training, and installation operations such as building and road construction."[128] The Army owns 4 of the top 10 installations in DoD with the most *Endangered Species Act* (ESA) creatures and 5 of the top 10 for imperiled species.[129] This impacts four installations in Hawaii and those in Washington, New Mexico, and California.[130] The two most famous ESA animals on Army installations, the red-cockaded woodpecker and the desert tortoise, are also the most expensive.[131] Between 1993 and 2012, the DoD spent $161.5 million to protect the red-cockaded woodpecker and $106.8 million on the desert tortoise.[132] Preserving critical habitat requires working with the U.S. Fish and Wildlife Service to ensure the Army completes necessary training while supporting environmental conservations goals.[133]

Global climate change will impact Army installations in the future. In 2016, the DoD published the *Climate Change Adaptation and Resilience* directive that requires installations "to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions."[134] This applies to natural disasters, accidents, terrorist attacks and conventional enemy attacks. Installations need to rapidly recover from an incident and be capable of providing essential support. In January 2019, the *Report on Effects of a Changing Climate to the Department of Defense* detailed the increasing problems on installations due to recurrent flooding, drought, desertification, wildfires, and thawing permafrost.[135] The changing climate will place facilities at certain installations at risk and impact the Army's efforts to achieve necessary training outcomes.

Future Trends

To build for the future, the Army forecasts changes decades in advance to align the internal processes of capabilities development, acquisition, and procurement. The *Joint Operating Environment 2035* provides the consensus DoD view on the future operating environment to assist in planning.[136] For the Army, *The Operational Environment and the Changing Character of Future War* provides the framework through 2050.[137] Both visions predict changes that will impact installations in two big areas: technology and adversaries. The Army's MDO concept incorporates these trends to guide the development of the future force and new training requirements.

Technology

In the next 20 years, science and technology will expand knowledge in "robotics and autonomy, information technology, nanotechnology, and energy."[138] The *2017 National Defense Strategy* points out that private industry develops the majority of advances in technology granting access to competitors and eroding the traditional overmatch of U.S. military forces.[139] Three main areas of technology advancements will have the most impact on installation training: robotics, virtual and augmented reality, and new weapons with longer ranges. In the future, both the U.S. and its adversaries will use these capabilities.

Robots will become effective, cheaper, and more versatile. On the battlefield, robots will work with manned systems to lengthen missions, increase lethality, protect platforms, and improve human performance.[140] The Army is pursing robotic and autonomous systems (RAS) "capabilities with urgency because adversaries are developing and employing a broad range of advanced RAS technologies as well as employing new tactics to disrupt U.S. military strengths and exploit perceived weaknesses."[141] Army installations must prepare and develop training areas and ranges that will support robotic systems.

Advances in virtual reality (VR) and augmented reality (AR) will change training for military forces. VR is defined as "a technology by which computer-aided stimuli create the immersive illusion of being somewhere else."[142] In 2017, the VR worldwide market was $7.17 billion with a projection that it could grow up to $75 billion by 2021.[143] Private industry advancements in VR technology for gaming community will make simulations more realistic. Commercial investments will spiral into military application and dramatically improve the quality and effectiveness of STE training.

The Army is exploring AR through two developmental programs: Tactical Augmented Reality and Head-Up Display (HUD) 3.0 to combine navigation, weapon sights, terrain, and enemy information.[144] In the next 20 years, the Army will gradually incorporate AR into training across the force. Advances with VR will transport soldiers to the virtual battlefields, while AR will enhance live training by bringing virtual capabilities into the training area. As these technologies mature, they will enable the Army to increase the frequency and realism in training at lower costs.

New weapons capabilities will threaten installations in the homeland. Cyber, electromagnetic pulse, and advanced radio-frequency weapons could precisely target electronics-based systems.[145] Hypersonic weapons could travel faster than one mile per second with the range, accuracy, and lethality of offensive global strike capabilities.[146] These capabilities dramatically shorten the time for the decision cycle to react and directly threaten installations in America. The Army must prepare for attacks on installations in the homeland.

Technology developments do not occur on a linear path and the advances may exceed or underperform predictions. Technology pessimists argue that advances in the future will slow down resulting in a gradual evolution of capabilities.[147] That being said, the proliferation of technologies across the globe makes it possible that by 2035 adversaries will have parity in selected capabilities to challenge U.S. interests.[148] The Army needs to continually assess technology and consider innovative ways to apply advancements to solve problems. Installations will train soldiers how to employ new capabilities and also how to defend against enemies using them.

Adversaries

The 2018 National Defense Strategy declared that “the homeland is no longer a sanctuary” and the central challenge to the U.S. is the reemergence of a long-term, strategic competition with Russia and China.[149] Both countries are modernizing their military forces and pursuing advanced technologies in computing, “big data” analytics, artificial intelligence, autonomy, robotics, directed energy, and hypersonics.[150] According to the *Joint Operating Environment 2035*, "the United States will confront a range of competitors seeking to achieve technological parity in a number of key areas. Adversary forces will be augmented by advanced C3/ISR and information technologies, lethal precision strike and area effect weapons, and the capacity to field first-rate technological innovations."[151] Russian and Chinese modernization efforts will require the U.S. Army to train to defeat strategic conventional capabilities within range of the homeland.

Russia and China are aggressively developing their own military robotic capabilities. Russia plans to have robots comprise 30% of its combat power in the next decade and use a variety of systems ranging from small robots to full sized remote armored vehicles.[152]

China is purchasing and developing robotic systems with the goal to become the world leader in this field as a part of "Made in China 2025."[153] In 2019, the International Federation of Robotics projects that China will purchase 160,000 robots to expand their capacity.[154] China's strong industrial base and engineering capabilities will enable the fielding of capable combat robotic systems. By the year 2035, American soldiers will be employing robots and facing them on the battlefield.

Non-state actors and proxy forces will remain a threat to U.S. forces and installations. The *2017 National Security Strategy* states that "during a conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated."[155] Non-state actors, including terrorist groups and transnational criminal organizations, could damage installations or disrupt enabling activities in the surrounding communities. These organizations could act for their own ideological or profit motives or as proxy forces to contest training, deployments, and mobilizations.

They could delay essential activities in the homeland through cyber-attacks on utilities, social media disinformation to distract service members, limited drone strikes, and sabotage of transportation infrastructure to prevent the U.S. Army from making it onto the battlefield.[156] This requires training the force across the continuum of conflict ranging from humanitarian disasters, battling terrorists, competing below the threshold of armed conflict and conducting larger scale combat operations.

Multi-Domain Operations

TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Doman Operations in 2028, guides the development of the Army's future force.[157] It describes how the Army "will militarily compete, penetrate, dis-integrate, and exploit our adversaries."[158] MDO proclaims the need to train "commanders and staff at each echelon to visualize and command a battle in all domains, the electromagnetic spectrum (EMS), and the information environment, converging organic and external capabilities at decisive spaces."[159] Success in MDO requires the Army to harness joint capabilities across all domains to defeat adversaries.

MDO requires higher echelons to train regularly to develop the necessary warfighting skills to integrate the air, sea, cyber, and space capabilities in time and space. Installations will need to support more training above the brigade level for the Army to successfully execute MDO.

Recommendations

Army training and installations must adapt due to new weapon systems and the organization of the force. The Army has six major modernization priorities:

1) Long Range Precision Fires; 2) Next Generation Combat Vehicle; 3) Future Vertical Lift; 4) Network Command, Control, Communication, and Intelligence; 5) Air and Missile Defense; and 6) Soldier Lethality.[160] Army Futures Command is aggressively pursuing these efforts with plans to "innovate, prototype, and begin fielding the next generation of combat vehicles, aerial platforms, and weapons systems by 2028."[161] The Army is developing and experimenting with manned and unmanned teaming. These modernization efforts will require more space to maneuver and greater management of the electromagnetic spectrum on installations.

The training challenge expands beyond just new capabilities. It includes more frequent and effective training to ensure America's soldiers have overmatch against adversaries anywhere in the world. Former Secretary of Defense Mattis stated that "twenty-five virtual battles before actual battle will attune infantry personnel to the shock of first contact within a hyper realistic training environment" through live, virtual, and immersive training.[162] To prepare installations to meet the future training requirements the Army should invest in: 1) versatile ranges, 2) robotic targets, and 3) the STE.

Versatile Ranges

The Army should move from standardized ranges to versatile ranges to free up land for training and to improve the quality of training. Versatile ranges will enable units to train multiple individual and collective tasks using one facility. Many installations lack the range capability for the required collective training events.[163]

Currently, the Army uses specialized ranges built for every major weapon system that consist of hardened firing points and permanent targets. The

Range Design Guide provides templates for designing and constructing 12 standard small arms ranges and 16 maneuver ranges.[164] Nearly all the ranges have the same elements: a control tower, storage building, classroom, covered bleachers, and a mess area.[165] These ranges are built for a specific task such as a firing table, qualification, or battle drill. When the range is not in use, the facilities sit dormant. For live-fire ranges this a concern, because land along the impact area is scarce and could support training other tasks.

Versatile ranges can improve efficiency and cohesion at the company level. Army formations include multiple weapons systems even at the squad level. To complete weapons qualification for an infantry company requires setting up, opening, and closing four separate ranges for pistol, rifle, light machine gun, and medium machine gun. Versatile ranges will enable units to open one range and shoot multiple weapon systems. With a proper setup, a company could qualify on all weapon systems ranging from the pistol to the machine gun for day and night. This will save soldiers' time because they will spend less time opening, closing, and moving to different ranges.

Units can build better cohesion using versatile ranges with everyone training together. Leaders ranging from the team leader to the company commander will be able to actively participate in the training to identify training weaknesses and quickly fix them. This arrangement also supports the cross-training of Soldiers on the multiple weapon systems creating more resilient units.

Versatile ranges also provide the ability to increase the variety of training. Ranges developed to specifically support one task become stale: after multiple iterations of doing the same thing, the training value diminishes because units are not challenged in new ways. A versatile range enables leaders to quickly change targets and scenarios to adapt the training to level of expertise and the mission requirements. Transitioning to ranges that can reconfigured to train multiple weapon systems and collective tasks will support building more effective and lethal units.

Technological advancements will further enable versatile ranges. AR has the potential to reduce the costs for ranges and make them more realistic by superimposing digital terrain, obstacles, and virtual enemies.[166] Building physical training sites for specific scenario events is expensive and incorporating live role-players may not be feasible.[167] AR enhanced training on versatile ranges can combine the harsh realities of the physical world such as fatigue, smoke, noise, weather with enhancements from the virtual world.

Robotic Targets

To advance training the Army should develop a family of robotic targets consisting of human type targets, vehicle targets, small ground and aerial unmanned systems. A 2013 study by National Research Council identified the "need for a quantum leap in training effectiveness" in marksmanship that would provide soldiers better feedback along with adaptive and accelerated training.[168] Improved marksmanship would not only increase lethality, but also make the best use of the weight carried by achieving greater effects with less ammunition.[169] A family of robotic targets will enable units to improve marksmanship, conduct adaptive training, complete scenario based collective training, and prepare to fight enemy robotic systems.

The most basic use of robotic targets would be for marksmanship training. Instead of permanent target locations, mobile robotic targets could position themselves at the various distances required for qualification. Hardened robotic targets could withstand the impacts of training rounds and respond to simulated laser fire. This feature expands the applicability of the targets beyond just live-fire events and into training areas far from the impact area. The robotic targets would provide feedback on the location of hits. On order, they could rapidly reset to support a different firing table or weapon system. Developing a family of targets, ranging from small ground robots, human type, vehicle sized, and low altitude drones, will support the entire training spectrum.

Robotic targets enable soldiers to train with moving targets. A 2017 U.S. Army Research Institute study found that for “many U.S. Army Soldiers, the first opportunity to engage a realistic moving target with small arms live ammunition is in combat.”[170] These targets are not science fiction. The Marines, Army, and Australian Defense Forces have trained and evaluated targets with this capability.[171]

In 2013, the Army’s Asymmetric Warfare Group conducted assessments at Fort A.P. Hill and Fort Bliss using robotic human type targets.[172] The 3-D targets have human mannequins that provide realistic moving engagements. Networked together the robotic targets can perform a variety of collective tasks including patrols, react to fallen comrades, and even maneuver on friendly forces.[173] In 2015, the Joint Sniper Performance Improvement Methodology Quick Reaction Test employed the targets to develop tactics, techniques, and procedures to improve sniper performance. [174] The test report stated that snipers currently lack the necessary training devices to engage moving targets at long distances prior to real-world engagements.[175] The U.S. Army Research Institute study found that training with the robotic targets significantly increased experienced Soldiers and snipers hits on moving targets and that the training was realistic.[176]

Robotic targets will enable units to quickly adapt training. As soldiers, crews, and units demonstrate proficiency, leaders can increase the difficulty level to improve performance. Mobile robotic targets could increase their speed and maneuver more erratically. The robots could attack the friendly forces and then break contact after suffering casualties. The targets could also serve as civilians on the battlefield requiring Soldiers to discriminate during engagements. This capability gives leaders an incredible new tool to enhance training.

Robotic targets also provide the capability to rapidly establish new ranges. Using trailers or shipping containers to store the targets will protect them from the environment and make them easy to move. Mobile systems that are easy to set up can reduce the total number of the targets required by eliminating idle infrastructure. The systems will only require terrain that is suitable for the mobility of the targets and the standard surface danger zones for live-fires. This versatility would be especially useful for the Army National Guard and the Army Reserve. Sharing sets of targets between installations will maximize this resource and support reserve component weekend and annual training. These robotic targets could also support training during deployments enabling soldiers to maintain and develop their skills while away from home station.

Robotic targets will also prepare units to fight enemy robotic systems on the battlefield. As explained in the previous section, America's most capable adversaries: Russia and China are developing these capabilities. This will change tactics in future warfare. Because there is no human life threatened, unmanned systems will be extremely aggressive and take greater risks. The Army must adjust training to respond to this new threat. In addition, robotic targets will assist in the development of U.S. military robotics technology by collecting of large amounts of data in a realistic training environment to support the development of future systems.

Adopting robotic targets on installations for training will be challenging due to costs and setting up the necessary infrastructure. The currently available systems are costly. In 2013, a training package with eight robots sold for $1.8 million.[177] As technology advances and with greater competition in this area, the prices of robotic targets should fall making them more affordable. The Army should establish modest requirements initially and begin to procure systems. This will spur development and competition between venders, increasing the capabilities over time.

Another challenge to implementation is setting up the necessary infrastructure to support the robotic targets. Robotic targets require detailed digital mapping of the training areas, access to a network, and the development of safety measures. Robotic targets will also require specialized technicians that can set up, maintain, repair, and run the systems. Although it requires a substantial investment and a change to the current way of running ranges, robotic targets can provide the Army more realistic training and tremendous flexibility.

Synthetic Training Environment

In 2035, the U.S. Army will use the STE to train individuals and units. In October 2017, the Army established the STE cross functional team to rapidly develop requirements and deliver capabilities.[178] The STE will be an interconnected system to train units from squad through Army Service Component Command in "the most appropriate domain - live, virtual, constructive, and gaming, or in all four simultaneously."[179] The STE will build readiness through training in a safe and cost effective manner. It will also help refine plans, test concepts, conduct rehearsals, and assist in garrison operations. The STE will consist of integrated virtual, constructive, and gaming training environments into a single platform to increase home-station training repetitions in a variety of scenarios.[180] This will move the Army from simulation systems that "operate on closed, restrictive networks, are facilities-based, and require high personnel overhead" to cloud based solutions and integrated training features in new combat systems.[181] The STE will directly impact installations in the next 20 years in four areas: 1) echelon above brigade training, 2) supporting deployment plans, 3) responding to local threats, and 4) developing the future force.

The future Army will incorporate MDO training in all domains: land, sea, air, space, and cyber simultaneously. To enable MDO, Soldiers and leaders "will require state of the art real-time wargame simulation capabilities that include other Service, interagency, and multinational partner capabilities."[182] The Army is also seeking a training environment that facilitates decentralized decision making for leaders.[183] Current system cannot do this, but the STE will evolve to this capability. The complexity of MDO places increased pressure on echelons above brigade generating greater demand for training. The frequency and intensity of warfighting training for the headquarters must increase. Installations with a division, corps, army service component command, or theater army need to assess their current facilities and anticipate expanding to meet future requirements. Installations must also prepare to support joint, interagency, and coalition partners in training and be capable of connecting virtually.

Army installations should use the STE to assist in preparing for contested deployments. Deploying units could practice "virtually" moving from the installation to different aerial and sea ports of debarkation all the way to theater opening, reception, staging, onward movement, and integration processes.[184] The STE needs to incorporate the full spectrum of threats that deploying forces could face in the homeland and enable the installations to coordinate with local, state, federal, and critical private industry partners. This capability will enable the installation to develop resilient deployment plans and building vital partnerships with joint, DoD, and civilian authorities in advance of armed conflict.

The STE can assist installations in responding to local threats. Garrisons could utilize the STE to train and rehearse antiterrorism and force protection requirements in AR 525–13. Scenarios could range from hypersonic weapon attacks, terrorist incidents, accidents, and natural disasters. Instead of merely completing one exercise a year, commanders could economically conduct multiple virtual exercises looking at different scenarios, activities, facilities, and personnel.[185] The STE can facilitate building partnerships with local law enforcement and civil authorities to assess the surrounding community and how to protect local infrastructure prior to a conflict beginning. These training events will not only improve responses to incidents, but also strengthen the relationships between the military and local community.

The STE will play a vital role in building the future force by connecting soldiers at installations across the globe to capabilities development. In the early 2000s, the Army used simulations to develop the Future Combat System concept, but the technology limited the amount of man-in-the loop interaction, required multiple simulation systems, and could not incorporate the interactions between all joint warfighting systems.[186] A fully connected STE can overcome these limitations by connecting warfighters to participate in the development and testing of future capabilities.[187] This will foster real-time user inputs into the development of systems by testing key characteristics in the virtual world. Input on current and future enemy capabilities will help define required capabilities and enable soldiers to develop tactics to defeat future Chinese and Russian systems.[188]

To prepare installations for the STE, the Army must make investments in facilities and the network. In the near term, the Army will have to maintain legacy virtual and constructive systems, while laying the foundation for the next generation.[189] Eventually, the STE should lower costs for installations through cloud computing, reducing the amount of hardware and local sustainment costs while improving availably.[190]

The STE will involve substantial amounts of sensitive or classified data and require sensitive compartmented information facilities (SCIF). The buildings must have high speed network connections to enable cloud computing. While expensive to build secure facilities, these same buildings could also support operations forward by providing a location for soldiers to remotely control unmanned systems. A SCIF STE training center with necessary connectively enables rapid conversion to support to real-world operations. Building new secure facilities from the start and "baking in" SCIF capabilities as a part of construction requirements will save significant funds rather than retro fitting structures.

Conclusion

To meet the demands of the future operating environment, the Army must improve training on installations. The return of great power competition with adversaries that can fight in all domains, places America's military supremacy at risk. The Army must prepare for contested deployments and attacks on installations in the homeland. Inefficient facilities, encroachment along boundaries, environmental conservation efforts, and the impacts of climate change limit training and its effectiveness. Advancements in robotics, virtual and augmented reality, new weapon systems, and the MDO concept will change how the Army trains and fights.

To address these challenges the Army needs to invest in versatile ranges, robotic targets, and the STE. Versatile ranges will enable units to train multiple individual and collective tasks at one facility. By staying abreast of technological developments and making prudent investments, the Army can provide the training facilities required to create ready and lethal forces for decades to come.

Section Two:
SERVICES

INSTALLATIONS NEED ELECTRICAL SUSTAINABILITY FOR 2035 AND BEYOND

Ms. Debora Browy, Department of the Army Civilian

Is it a fact – or have I dreamt it – that, by means of electricity, the world of matter has become a great nerve, vibrating thousands of miles in a breathless point of time?

—Nathaniel Hawthorne[191]

In the future operational environment (OE), Army Installations delivering vital National Security Strategy functions, will depend on increasingly stressed energy supplies threatened by potential catastrophic disruptions from near-peer adversaries. Moreover, these installations will rely on technology such as drone operations, cyber initiatives, and communication that demand ever greater supplies of reliable and sustainable energy. Yet they continue to depend on a US electrical Power Grid susceptible to natural disasters or adversarial attack. Federal deregulation in the 1970's relinquished power generation authority to states and municipalities that are now challenged to secure the grid that is subjected to physical or cyber-attacks every four days.[192] This places the Army at risk. As Assistant Chief of Staff for Installation Management LTG Gwen Bingham has said, "Without energy and water "the Army fails."[193]

This thesis examines how the Army sought to make installations energy resilient against risks. It considers the impact of regulation, policies and laws on installations energy requirements and grid vulnerabilities to attack and disaster. It also examines ongoing installation energy programs against Future Operational Environments (FOE) threats. Finally, it offers recommendations to ensure Army Installations maintain enough supplies of energy during potential attacks or disasters in 2035.

Existing Installation Energy Programs

In 2015, the federal Energy Sustainability & Strategy (ES2), Senior Energy and Sustainability Council (SESC) mandated building infrastructure that secures and maintains installations throughout the Army. The ES2 provides direction to, "integrated sustainability and energy considerations into Army plans, policies, and activities."[194] The Army prepared for the future by building resiliency into existing power generation and planned for upgrades to installations in the 2025 strategic plan to include reliance on the development of business partnerships with local domestic energy suppliers.

However, resiliency for Installations also means the ability to, "avoid, prepare for, minimize, adapt to, and recover from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability sufficient to provide for mission assurance and readiness, including mission essential operations related to readiness, and to execute or rapidly reestablish mission essential requirements."[195]

The Annual Defense Energy Management Report mandated in 10 U.S. Code (USC) 2925, require installations to address their total energy needs, report energy outages and associated costs, to include overall effects outages have on existing missions. The plan requires reporting usage, costs, and risks in addition to, ‘back-up generators’ to act as a supply point for energy in support of continuity of operations. [196]

Furthermore, the Army has been working on alternative energy solution(s) to maintain operations during unplanned outages and to reduce the vulnerability to installations due to interruptions on the local grid. Installations require sustainable electrical power and have built power generation of wind, solar and thermal, partnering with commercial and private industries through ISSA’s and, Public, Private, Partnerships (PPP’s). Installations such as Ft. Benning provide examples of progressive improvements with energy.

Ft. Benning has been leaning forward on understanding power generation and renewable energies. There is now an environmental learning center, focused on training soldiers and civilians to think productively about renewable sustainable energies. The Ft. Benning power generation initiative branched out in 2016 by establishing one solar array site at each of three Georgia Garrisons (Ft. Benning, Ft. Stewart and Ft. Gordon), which have a 30-megawatt power generation capacity.”[197] The solar array, combined with a micro-grid allows Ft Benning to consume power generated on-site.

Another example of installations considering energy requirements of the future is at Ft. Bliss, Texas where the micro-grid technology revealed islandable capabilities. The Commanding General of Ft. Bliss and the 1st Armored Division, Maj. Gen. Dana J.H. Pittard stated, “the system integrates renewable energy, local power, energy storage and load management to guarantee uninterrupted continuous power in adverse conditions."[198] Micro-grid technology with controls will be a key factor to successful energy planning for installations in the future.

Congressional mandates state that installations must develop alternative renewable power of wind, solar, thermal and smart grid technologies as an effort to reduce the installations carbon footprint. Furthermore, obtaining 30% of their consumable power from renewable sources by 2025. The vulnerability to the installation still exists due to agreements that tether them to the local public power supply system.

Applicable Energy Environmental Laws and Policies

Environmental policies beginning in the 1960's have driven the need for alternative power for the DoD installation. Environmental contaminants of the installations became a concern to public and state, causing the federal government to react not only with new technology of alternative power generation but of policies and laws to address existing violations. Included in the policy and decision making are agencies of Agriculture, Commerce, Housing and Urban Development (HUD), Justice, State, Energy, and Defense. While the list of agencies is not all inclusive of stakeholders, it provides a snapshot of the interconnectedness in the power generation, environmental problem and decisions. The electric power grid is massive and requires continuous management through computer programs or add-ons for the increases to outputs and protection against threats, both introduced by nature as well as by man.[199]

The EPAct laws of 2007 implemented a reduction to Greenhouse Gasses (GHG) and included mandates for Department of Defense (DoD). "The goals included in EPAct were intensified by Congress as applied to the DoD in the 2007 National Defense Authorization Act (NDAA), which required DoD to "produce or procure not less than 25 percent of the total quantity of electric energy it consumes within its facilities and in its activities during fiscal year 2025 and each fiscal year thereafter from renewable energy sources."[200]

Vulnerabilities and Threats

The Bulk Electrical System (BES) is a commercially operated and federally regulated system. It consists of "170,000 miles of high-voltage (above 200 kilovolts or kV) electric transmission lines and associated equipment, and almost 6 million miles of lower-voltage distribution lines."[201] The interconnected system of heavy power transmission lines extends throughout the US into Canada and parts of Mexico through Texas.

There are two primary functions within the grid system that contribute to vulnerability and require security measures. Commonly called the 'grid' with connecting transmission lines carrying electricity across thousands of miles, vulnerable through the aging of material, scheduled maintenance, natural disaster and physical or cyber-attack. Any or all vulnerabilities can cause a loss of transmission for short periods of time, but a well synchronized physical or cyber-attack will be much longer in duration with significant secondary and tertiary ramifications.

Primary threats to the grid come from natural disasters such as weather, earthquakes, mudslides and volcano eruptions with an estimated $25 billion to $70 billion being spent on repairs or for upgrades to continue power service throughout the US.[202]_Reporter Ted Koppel has written extensively on the topic of US power outages and the ramifications for America. Stated costs consider mild weather up to but not including hurricane forces. Some of the worst disruptions for power outages occurred with Hurricane Sandy in 2012 on the Atlantic seaboard, and Hurricane Katrina, a category 5 hurricane that devastated Florida and Louisiana in August of 2005, leaving millions of residents without power.[203]

Nevertheless, these occurrences have the potential to leave the US vulnerable to adversary attack, with Army Installations responsible for US defense and becoming collateral damage. "Without electricity from civilian power plants, the most advanced military in world history could be crippled. The US Department of Energy has begged for new authority to defend against weaknesses in the grid in a nearly 500-page comprehensive study issued in January 2017, warning that it's only a matter of time before the grid fails, due to disaster or attack."[204]

The near-peer threat is the hardest to anticipate, feeding into or out of the BES from insider radical groups. An example of grid vulnerability occurred in 2013 when a sniper attacked a Pacific Gas and Electric (PG&E) substation in California. The attack disabled 17 transformers supplying power to the Silicon Valley, the hub of U.S. cyber development. In what the Federal Energy Regulatory Commission (FERC) called, "the most significant incident of domestic terrorism involving the grid…the attacker fired approximately 100 rounds of .30-caliber rifle ammunition into the radiators of 17 electrical transformers…."[205] The system was able to adjust, transferring power from one substation to another, allowing the Silicon Valley to retain power, but if there were several synchronized attacks at once as intended in 2005 by a group of eco-terrorists, could have been enough to collapse the grid. One group of eco-terrorists attempted to sabotage the grid but were apprehended during the commission of the act and incarcerated under the terrorist acts initiative.[206]

National Interests and Presidential Directive

The expectation for sustainable energy will continue to be true in 2035 but with a greater dependence on electrical reliability supporting the National Security Strategy with increases to Big Data, Artificial Intelligence (AI) and future automation.

National Interests of the United States requires a resilient and defendable sustainable power source for installations. The Presidential Executive Order (EO), signed in March 2017, mandates in Section 1 that, "It is in the national interest to promote clean and safe development of our Nation's vast energy resources, while at the same time avoiding regulatory that unnecessarily encumber energy production, constrain economic growth, and prevent job creation. Moreover, the prudent development of these natural resources is essential to ensuring the Nation's geopolitical security (sic)."[207]

The Presidents Energy Directive allows for multiple resources of power generation covered in section (b), "It is further in the national interest to ensure that the Nation's electricity is affordable, reliable, safe, secure, and clean, and that it can be produced from (clean) coal, natural gas, nuclear material, flowing water, and other domestic sources, including renewable sources."[208] The Presidential policy creates a conflict with the states who maintain the authority to write their laws for local power generators and distribution. More specifically, regulations state, "in accordance with 40 U.S.C. § 591(a), federal agencies cannot purchase electricity in a manner inconsistent with ‘state laws’ governing the provision of electric utility service,” leaving installations vulnerable to local municipalities policies.[209]

Future Programs

The Army is diligently working on solution(s) to harden the power grid and protect Army Installations by seeking redundant and additional power generation on-site. The Army Corps of Engineers is partnering with Construction Engineering and Research Laboratory (CERL) for more reliable and environmentally friendly technologies. Also, the development of alternative power generation as a green incentive to further reduce the carbon footprint of army installations while maintaining continuity during power outages.[210] The redundancy of systems that provide power to the grid complicates the ability to protect the grid from intrusive attacks of cyber or physical means.

The research and development associated with new technologies for power generation is already in place with promising outcomes, utilizing existing technologies of micro-grids, wind power and solar energy and increasing new developments of very Small Modular Reactors (vSMR) will provide the sustainability for energy required to meet AI and Automation development and inclusion, interdependent on existing and emerging technology.

Strategically positioned vSMR technology provides both scalable and clean energy, able to meet the energy demand of installations.

According to former Secretary of Defense James Mattis, “Employment of mobile nuclear power is consistent with the new geopolitical landscape and priorities outlined in the U.S. National Security Strategy

(NSS) and the 2018 National Defense Strategy focusing on China and Russia as the principal priorities for the U.S. Department of Defense (DOD)."[211]

The federal government is already investing in the early support of vSMRs through cost-shared funding projects, loan guarantees and the extension of production tax credits for nuclear projects completed after 2020.[212]

The application of vSMR provides sustainable power generation at the installation with excess power not consumed flowing back to the BES, thereby reducing costs. The primary mission is to support the installations in day to day operations and during significant events. The Department of Energy states vSMR can store power on site for up to two years, allowing recover time for major outages or events such as an attack.[213] Focus on vSMR is critical to maintaining power on-site with the ability to harden this technology. The vSMR housed underground provides necessary protection from physical attack and electromagnetic pulse and increased security for the surrounding community. Reducing access to underground systems provides manageable security measures for vSMR and micro-grid technology. Additional sources of clean energy for installations is that of Fuel Cell Technology, as seen in Hawaii.

The DoD has partnered with CERL to identify reliable independent backup power generation for installations. One design is that of a Fuel Cell (Backup Power Proton Exchange Membrane Fuel Cell Project) combined with a Micro-Grid located onsite, that can produce up to 50% of power needed to run the test installation at U.S. Army Parks Reserve Forces Training Area in Dublin, CA. Providing continuity of power during disruptions on the primary source through the

BES. The backup power runs on natural gas, hydrogen, methanol, and a variety of other fuels. While it is progress it does not provide long term sustainability for installations.[214]

Fuel Cell Technology is scalable to more than 100 megawatt (MW) on site, meets Congressional mandates of clean energy, relying on bio-fuel or natural gas as fuel sources and represents a small foot print on the installation. Installations should also continue to invest in renewable sources of wind and solar to both satisfy mandates and provide redundant energy supplies. Finally, Micro Grid Technology provides the linkage on-site needed to carry power throughout the installation to sustain operations if it includes controls, allowing it to have ‘islandable’ capability.

The Gray Zone of War

The BES is a ‘gray zone’ of opportunity for near-peer competitors such as China with desires to be a superpower and with the reemergence of Russia as an adversary possess potential risk to the U.S. homeland security.

Russia shut down the Ukraine power grid in Kiev to demonstrate their ‘gray zone’ capabilities. According to the Department of Homeland Security, a destructive “Trojan Horse” malware program has penetrated the software that runs much of the nation’s critical infrastructure and is poised to cause an economic catastrophe. This example also targets the power grid to weaken US security. Installations are key to sustaining the NSS globally, currently conducting theater and overseas contingencies of drone operations, cyber initiatives, forward deployments and communication, requiring reliable and sustainable energy.

Adversary Interest in the ‘Gray Zone’

There have been physical attacks as well as natural disasters effecting the stability of the U.S. power system. One expert, Jon Wellinghoff, a former chairman of the FERC, said the susceptibility for the grid is through cascading disruptions or well-planned outages across three primary hubs of BES, or due to the multitude of small substations and other physical equipment[215]

The U.S. has the same vulnerabilities as many Nation-States when thinking about power grids and generation of electrical power. It is a service for a fee, used every day and taken for granted, assuming it will always be available and where over confidence or complacency can make the system susceptible to attack and the inability to uphold national security.

As cyber expert O. Sami Saydjari stated, “If cyber-attacks continue to increase at the current rate, they could destabilize already tense world situations… the components of cyber warfare are the very same components as warfare using guns and explosives… an attacker would seek to damage a critical infrastructure such as power, telecommunications or banking….”[216]

Becoming more predominant is threats from global state actors. To investigate the vulnerability of the grid, a controlled test known as the Aurora test, allowed a circuit breaker controlled by computer software to rapidly turn off and on through a process called pinging, also known as, being out of phase, resulted in the generator tearing itself apart.[217] The Aurora test revealed a considerable risk and actual possibility by exposing the vulnerability of the grid.

In November of 2104, it was reported that there was evidence that malware was inserted by hackers believed to be sponsored by the Russian government… The hacked software is used to control complex industrial operations like oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear plants. Shutting down or damaging any of these vital public utilities could severely impact hundreds of thousands of Americans.[218]

It is not just the unforeseen events that impact the grid but also planned maintenance. The grid is in a constant state of repair and growth, making the US electrical grid hard to defend, due to its enormous size, and dependency on digital communication computerized controlling software. One of the most vulnerable aspects on the BES are the transformers that push the Megavolt current through the wires to its receiving destination, converting to a lower Kilowatt (Kw) for use by the independent company's and sent to the consumer. The transformers, primarily built overseas, are not readily available, are massive to move and are not interchangeable. Often these transformers weigh up to 540 tons and are at least 30 years old with existing infrastructure built close to 100 years ago, still in operation and vulnerable to obsolescence as well as attack.

In March 2019 the power grid collapsed in Caracas, Venezuela due to a malicious attack, rumored by adversaries to have been caused by the U.S., leaving residents without the ability to obtain water, food or medical support resulting in civil unrest, looting and vigilante behavior on the streets. Complete reliance fell on back-up power generators dependent on limited fuel supplies.

The number of potential targets is growing as "internet of things," devices, such as smart meters, solar arrays and household batteries, connected to the smart grid of systems increases."[219]

One well planned attack to our vital power supply system exposes the vulnerability within the BES causing severance of energy to homes, businesses and installations. "In late 2015 and again in 2016, Russian hackers shut down parts of_Ukraine's power grid. In March 2018, federal officials warned that Russians had penetrated the computers of multiple U.S. electric utilities and were able to gain access to critical control systems. Four months after the Ukraine power crises, the Wall Street Journal reported that the hackers' access had included privileges that were sufficient to cause power outages.[220]

Recommended Solutions

What will first have to change is how the government and public understand the vulnerability of the power grid in the US. To include understanding the vulnerabilities of cities and installations responsible for the protection of American interests and her citizens from adversaries attempting to inflect harm, including intrusion below the threshold of armed conflict.

Military Installations must continue to incorporate sustainable clean energy by 2035. Partner with Energy Research Laboratory in building vSMR with micro-grid capability, allowing for scalable requirements. Placement of vSMR will be subterranean, not visible from ground or space providing security from physical attack. Originally designed for field operations, these vSMR are appropriate for CONUS Installations, resulting in continuity of operations, provide capability to harden through underground placement allowing installations the ability to uphold the National Security Strategy, by severing installations from the BES when needed.

The United States Power Grid is susceptible to a multitude of natural disasters or attack from adversaries as an element of war in the gray zone, ‘below the level of armed conflict.’ A well synchronized attack could disable the U.S. grid, thus installations, through a process called, ‘cascading,’ affecting Installations functionality and the ability to support the NSS.

Primary plans for modernization of installation power generation will include using vSMR and microgrid technology by creating a funding plan for all installations responsible for housing and maintaining support of forces and operations. Utilizing the authority provided in the Presidential Energy Directive that includes renewable and sustainable energy from flowing water and nuclear as clean sources of energy. Laws, Regulations and Policies that currently restrict Army Installations from being islandable will require revision to align with the Presidential Energy Directive. The NSS, NDS and NMS will include language that is supportive of sustainable energy on installations, mitigating increased risk by emerging adversaries, near peer competition and insider threat to the Bulk Electrical System. Update power sharing agreements with local municipalities to include severance agreements during compromise of the BES due to disaster or attack, to assure security of the US. Decisions need to provide instantaneous capabilities for DoD to manage energy on installations during significant events of attack or natural disaster that provides capability for Army and services continuity.

What is not known at this time is what the power requirement will be in 2035 but we can assume it will be greater than it is now. In addition to instability of renewable energy is the shortage of well-trained technicians familiar with providing sustainment and servicing of multiple power generation systems. These findings are of concern to Army Installations who partner with and depend on the grid for secure uninterrupted power, ISSA's with local providers, who in turn control and utilize the BES.

The development of vSMR is based in part due to a study by the Department of the Army G-4. This study determined that 52% of all casualties sustained over a nine-year period during Operation Iraqi Freedom and Operation Enduring Freedom were during land transport missions. The study's purpose was "to analyze the potential benefits and challenges of mobile nuclear power plants (MNPPs) with vSMR technology and to address the broader operational and strategic implications of energy delivery and management."[221] While the intention for operation of vSMR power focused on field or contingency operations, the technology is applicable and appropriate to CONUS Installations.

Included in future energy programs will be, 'Pack and Go,' vSMR of clean, sustainable energy providing uninterrupted electrical power for Installations through on-site micro-grid technology with controls, and a hardened underground installation plan to protect vSMR from either physical or cyber-attack. Policies exist to address concerns and provide the necessary support both in funding and development to meet the growing threat to the grid. "It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats… to manage risk and strengthen the security and resilience of the Nation's critical infrastructure…that could have a debilitating impact on national security, economic stability, public health and safety….” [222] By broadening the aperture of what is possible versus what has always been, lends to increased security of army installations as strong holds, with the ability to defend the US.

Conclusion

The increasing importance of electrical energy to Army Installations in the future operating environment requires today's decision makers to identify and address threats to ongoing installations energy resiliency programs. The installations will adopt more Smart City technologies to improve security, data collection, and efficient operations. Although much of this technology will make any disruption in energy supplies catastrophic for Army operations. As recent military conflicts have demonstrated, major powers employ increasing abilities to quickly target and destroy national energy systems. The US demonstrated such power in its operations of the last several decades. Russia shut down the Ukraine power in Kiev to demonstrate their ‘gray zone' capabilities. The National Defense Strategy depends on protection from the effects of near peer competitor disruption of Installation energy supplies.

Current Army “Office of Energy Initiatives” have pursued energy resilience by developing over 530 megawatts of on-site energy production, storage and controls for fully “islandable” capabilities. Schofield Barracks and Wheeler Army Airfield, for example, worked with Hawaiian Electric Company to build the 50-megawatt biofuel Field Station, Kunai to provide secure energy in emergencies. These projects envision installations severing themselves from the grid during disruptions and providing their own power needs over internal micro-grids. Yet in the event of a future near-peer conflict in which an adversary critically disrupts the national power grid, it is likely that states and communities will demand installations energy resources support their most desperate needs. Even 530 mega-watts of supply will not be near enough - Washington D.C. consumes 4,000 mega-watts per hour.

The Army will fail, and the nation with it, if it does not ensure uninterrupted energy supplies for its installations. The Army must continue to incorporate sustainable clean energy fuel cells on installations to meet Federal standards for 2035 and beyond while simultaneously developing installations power resources capable of withstanding near-peer attacks and able to support local communities. To do this, the Army should adopt very Small Modular Reactors (vSMR) that have micro-grid capability on Army Installations. Reliable, clean vSMR with micro-grid technology can be placed underground, safe from near-peer interdiction to ensure Army success in upholding the National Security Strategy.

REVITALIZED MEDICAL SERVICES ARE ESSENTIAL TO SUPPORT FUTURE MOBILIZATION INSTALLATIONS

LTC Chance Comstock, U.S. Army Reserve

The western liberal international order was founded by the United States (U.S.) and the United Kingdom (UK) as a rules-based order that utilizes the United Nations as a negotiator for nations' disputes to prevent future interstate wars.[223] The joint operating environment (JOE) of 2035 to 2050 predicts threats to the western liberal international order from near-peer competitors and persistent disorder among weak nation states.[224] To win the nation's wars, U.S. soldiers must be fit, and ready to execute direct kinetic action to defeat adversaries across a range of military operations. Medical and dental (hereafter referred to as medical) preparedness is vital to providing healthy and ready forces supporting combatant commanders (CCDR) and U.S. vital national interests. To provide capable forces that meet global mobilization requirements future installation leaders must shape the future installation medical operating environment, understand future challenges, and employ potential fixes.

Future Installation Medical Operating Environment

In the future JOE from 2035-2050, the continental U.S. (CONUS) Army base is no longer considered a safe haven. Future U.S. Army CONUS installations will cover a range of facilities including arsenals, depots, bases, ports, and forts. The most complex U.S. Army installations will project power by mobilizing and deploying soldiers to support CCDR missions. Future mobilization and power projection installations are fundamental to the global employment of U.S. forces, and medical processing is an integral component.

Adversaries will try to disrupt U.S. mobilization activities across all domains (space, cyber, land, air, and sea) to deter the U.S. from assembling and deploying armed forces. For the future installation medical screening and processing is an essential component. Medical processing is especially crucial with the U.S. Army reserve component (RC) soldiers. To expedite soldier processing at U.S. Army future installations leaders must understand future installation medical challenges and shape the environment by providing solutions that enhance the soldier mobilization process.

Future Installation Medical Challenges

Challenges affecting future installations that medically prepare soldiers for mobilization include external threats and internal problems. The U.S. external environment is changing due to globalization, near-peer competition, and the proliferation of technology.[225] External threats will come from a range of competitors across the spectrum of competition from conventional operations to operations short of armed conflict.[226] U.S. government stakeholders will add to internal competition between the Department of Defense (DoD) and other governmental agencies for limited resources. From a medical viewpoint, preparedness, medical capabilities at mobilization platforms, U.S. Army organizational culture, and interoperable technology all pose challenges that will affect future installation mobilization procedures. Future installation leaders should understand medical gaps in the mobilization system that adversely affect force projection.

Medical readiness is a crucial component of preparedness. When soldiers are not frequently medically screened, they risk having a medical condition that renders them non-deployable. Missed medical appointments add up and can significantly impede the throughput of soldiers mobilizing and deploying from the installation mobilization site. Missed appointments inhibit the healthcare system by underutilizing healthcare providers and hinder the soldier by losing valuable training time. There is also a monetary cost to the government and federal taxpayer for missed medical appointments. Once a medical condition renders a soldier non-deployable, they are removed from the mobilization roster and assigned to the installation headquarters for further medical treatment until they are returned to duty or discharged from the U.S. Army. This process leads to significant requirements for additional medical personnel at installations to care for non-deployable soldiers. Non-deployable soldiers hinder the unit and personnel system by dead lining valued team members and requesting new personnel replacements. It is essential for future installation leaders to ensure soldiers (including the RC) attend their yearly medical appointments ensuring they are medically ready to deploy. Another impediment to CONUS based mobilization installations are the different levels of medical capabilities across the U.S.

To complicate the situation, not all installation medical activities offer the same on-site medical capabilities. Fort Bliss, Texas (FBTX) and Fort McCoy, Wisconsin (FMWI) are mobilization installations and provide medical soldier readiness processing sites yet do not have the same medical capabilities. This arrangement leads to medical inefficiencies across the CONUS where soldiers deploy faster based on the installation they mobilized through. Some installation medical activities lack effective medical infrastructure and send soldiers off base to the civilian community for medical care.

To further strain the situation, the U.S. Army organizational culture affects medical capacity and capability. Medical doctors (MD) are a low-density specialty and hard to recruit and assess into the service, yet they are discharged from the U.S. Army when they are considered twice for promotion and not selected.[227] This practice needlessly expels MDs from the inventory. MD shortages in the U.S. increase stress in the U.S. Army healthcare system adversely impacting soldier care.[228] The lack of doctors and other medical providers in the U.S. Army terminates preventive services at local military treatment facilities. The shortage of MDs increases referrals to the civilian market and increases requests for additional medical providers. Pay and incentives are reasons why MDs leave the military.[229]

Another course of action downgrades the medical provider from an MD to a nurse practitioner or physician assistant. Downgrading medical providers decrease the quality of soldier care, delays treatment, and compromises military readiness.[230] Supported military units and the local population suffer second and third order effects including longer wait times, fewer appointments, and diminished medical care. Current MD compensation packages do not compete with lucrative private employment offers. MDs commissioned as U.S. Army Captains earn around 60K-70K annually and receive a yearly bonus around 20K.[231] The average salary for an emergency room physician in the U.S. is around 288K.[232] While recruiting and retaining medical providers is a problem another issue is the lack of adaptive technology.

The situation becomes further compounded by *interoperable technology* challenges across the board in the Army Medical Department (AMEDD). While the current AMEDD IT system the Armed Forces Health Longitudinal Technology Application (AHLTA) maintains the current soldier electronic health record (EHR) and makes continuous system upgrades it is not interoperable with other U.S. government information technology (IT) systems. The EHR for the Department of Veterans Affairs and the U.S. Army EHR do not communicate well.[233] Deficient IT communication leads to further delays in soldier care and compromises the quality of EHR information. Many AMEDD IT systems are developed and implemented in silos and stovepipe systems. Virtual health technology is expensive and not defined well in future programming, planning, budgeting, and execution (PPBE) models. Future installation leaders must execute bold, innovative, flexible options to support healthcare solutions at future installations.

Solutions

U.S. Army future installation leaders should influence their internal environment by adopting smart solutions to contest and counter the external threat by providing greater efficiencies and business processes across the enterprise.[234] Future installations should be organized effectively to assemble, mobilize and project forces quickly. This threat includes attacks on future installations across multi-domain operations from air, sea, land, space to cyber denial of service attacks on IT and the electrical grid. On base medical services are subject to the same threat and should be executed more effectively to safeguard soldiers at future U.S. Army mobilization installations. Future U.S. Army mobilization medical platforms will need to incorporate redundancy and speed effectively into complex healthcare systems.

Future installation leaders should develop medical administration procedures that support rapid processing and mobilization of individuals and equipment. Medical solutions should include first *changing the U.S. Army culture*, second *leveraging technology*, and third *aligning medical capabilities*. The first critical requirement for future installation leaders is *changing the U.S. Army culture*.

To *change the culture* installation future leaders must first change the U.S. Army's organizational culture to value medical preparedness instead of medical readiness, and then shift force structure and personnel policies. The preparedness method will take a more strategic look by asking readiness for what, for where, and when and will provide a better view of overall medical preparedness across the force.[235] Medical preparedness is a more holistic way of managing soldier medical readiness than just taking a snapshot in time.

A high level of medical preparedness requires future installation leaders to change the "just in time" medical appointments culture to a "proactive" culture across the U.S. Army's three components. Future installation leaders should use embedding mechanisms (policies) and reinforcing mechanisms (data metrics and trends analysis) to change the culture.[236] These measures will allow future installation leaders to maintain preparedness which will positively affect overall medical readiness. Next, they should modify force structure and policy.

Future installation leaders ought to drive installation personnel requirements by shaping U.S. Army personnel policies and force structure to support the next installation mobilization key task- mobilizing and deploying soldiers. Future installation leaders should modify personnel policies to retain the best medical talent. An option for addressing the MD shortage is keeping those that are already in the service. The "up or out" promotion system adversely affects medical officers and revising it will retain vital MDs in the service to provide the best health service support to soldiers and family members.[237] The U.S. Army should cease the "up or out" promotion system retaining technically skilled MDs in non-leadership positions. While keeping current personnel in the U.S. Army is vital another issue for future installation leaders to focus on is medical force structure

Future installation leaders should fix force structure vacancies. There are not enough MDs on the books to fill current tables of organization and tables of distribution and allowances documents in field units or installation medical activities.[238] To negate the effect of the U.S. MD shortage, future installation leaders should work with accession commands to recruit MDs and human resources specialists to offer extra pay and incentives to attract and retain MDs in the military service. Increasing the incentives will attract a better qualified and skilled medical professional to stay in the U.S. Army. While the lack of force structure, pay, and incentives are some reasons MDs leave the service another is the lack of adequate IT systems.[239]

The future installation medical site will be affected positively by implementing *technological solutions*. This process starts with procuring interoperable and adaptive medical capabilities. Integrating MDs and future installation leaders with health information exchanges (HIE) will allow leaders to get the best real-time information and provide more effective soldier readiness processing. Developing virtual health, mobile applications (APP), and health IT systems are starting points for future installation leaders to shape and craft the best practices. Future technologies from mobile applications to virtual health and body scanners will provide a more comprehensive look at overall soldier health instead of only treating a disease or injury.[240] Virtual health refers to providing advanced medical care to patients that are not physically in the presence of an MD but connected virtually by IT, networks, and video.[241]

Virtual health and wearable sensors will be necessary for the future environment to decrease the strain on MDs and will track a soldier's health metrics providing a real-time picture of individual soldier preparedness to future installation leaders.[242] Medical drones are another option to increase the speed and efficiency of medical processing on future installations. Medical drones will increase productivity by transporting materials, blood, tissue, etc. between buildings and will be an effective method for relaying information on the installation while reducing the workforce.[243]

A mobile application (APP) is a solution that better enables soldiers to monitor their medical readiness from their mobile phone. The U.S. Army is already going mobile with an APP that links mobile electronic devices to news, morale, welfare, recreation, and housing; however it does not yet relate to soldier medical status.[244] Private corporations currently utilize APPs that display employees' EHRs to include medical results, histories, patient education, and prescriptions.[245] Future installation leaders should encourage the U.S. Army Chief of Staff for Information Management (G-6) to create and develop a medical readiness APP and short message service. Future installation leaders should also work with the U.S. Army Chief of Staff for Readiness (G3/5/7) to introduce the needed fiscal requirements into the PPBE cycle.

Future installation leaders should leverage interoperable IT systems. The key to incorporating this technology is through a Health Information Exchange (HIE). The HIE allows patients and MDs to share confidential medical information via secure electronic means.[246] An essential component of the HIE is interoperability between IT systems. Interoperability in a medical sense refers to the "ability of different information systems, devices or applications to connect, across organizational boundaries, cooperatively use data among stakeholders, with the goal of optimizing the health of individuals."[247] Interoperability is at the core of the HIE, with constant upgrades to technologies IT systems require communication with all devices on a seamless platform.

Without the interoperability built into the IT system, it further complicates the process and delays implementations of technologies which then require additional workarounds. The current solution to achieving interoperability is an application programming interface (API) and is an essential component to achieve interoperability at its current state. Currently to have two software systems communicate it requires an API. APIs are translators between two types of software.[248] APIs are beneficial because they provide an additional layer of security. HIE, by way of API, will grant greater interoperability to AMEDD IT systems but will require continuous upkeep and maintenance. The AMEDD is working with the VA to integrate medical information from the start to end of a soldier's military service into a comprehensive overarching IT system.

The future solution should model the Military Health System (MHS) Genesis IT system. When this system is activated "it will tie together inpatient, outpatient, and dental information for soldiers, family members, and veterans."[249] Additionally, it will improve efficiencies for health care providers and beneficiaries by sharing information from the Department of Veterans, military operations, and civilian health care providers maintaining access to both dental and health care records.[250] MHS Genesis is an upgrade and step in the right direction for the integration of AMEDD IT systems.

Upgrading medical IT systems to adaptable (ability to improve) and portable (hand-carried) systems will provide U.S. Army medical providers with state-of-the-art technology. This method will drive down medical provider complaints about the current state of IT.[251] Flexible, portable, and mobile health IT systems will deliver comprehensive information to soldiers and the U.S. Army medical providers assisting them in making the best medical decisions for the patient. A comprehensive soldier electronic medical history that is secure and portable will help soldiers and future installation leaders by lessening processing times at future installation mobilization platforms.

Soldiers will not need to restate all of their medical history with each new medical provider they encounter. Interoperability along with the HIE will improve the lives of soldiers, increasing medical efficiency, decreasing the stress on medical personnel, and streamlining patient care. Though technology is critical, future installation leaders must also align installations with suitable medical capabilities to support mobilizing soldiers.

Future installation leaders should align medical capabilities with CONUS mobilization installations, so they all have the same baseline medical capability. This planning effort should level the playing field for medical capabilities between Fort Bliss, Texas (FBTX), and Fort McCoy, Wisconsin (FMWI). While FBTX has the entire spectrum of medical care on post, FMWI does not and has to refer soldiers to the local economy. Future installation leaders should have a plan to field medical capabilities on FMWI to support mobilization and deployment. Future installation leaders should plan medical options that include expansion abilities with RC support and referral functions to prevent mobilization installations from becoming overwhelmed.

Medical services at future installations should provide a range of care that supports soldiers assigned to the local area, and soldiers deploying to overseas locations. Medical services should cover a variety of options including assessment, psychological services, hospitalization, medical holding, emergency medical care, diagnostic procedures, lab facilities, and others as requested. By providing a range of healthcare services, future installation commanders will maintain flexibility and scalable health care options. Future installation leaders must be aware of all of their internal assets and capabilities including their relationships to RC medical forces. RC medical forces must be part of the solution to assist future installation commanders during peak times.

The ability to expand medical services relies on support from the RC. The majority of medical resources are located in the U.S. Army Reserve and programmed to support CCDR requirements.[252] To ensure the RC soldiers are ready to perform their missions when called to active duty integrating them in the planning and execution phases of operations is essential. This option requires future installation leaders to coordinate and build relationships with their supporting RC units to provide backfill support before it is needed. Future installation leaders must plan and rehearse the backfill plan with RC medical forces before waiting until the eleventh hour. When military health care providers and RC medical forces are unavailable, future installation leaders must use their last medical expansion option, the civilian healthcare network.

Future installation leaders must provide for an overflow medical system when expanding medical services does not relieve the installation of hospital congestion. Leveraging the civilian healthcare network is an alternative option. They should have the ability to refer soldiers to the civilian healthcare system without going through a bureaucratic process. By building local coalitions with medical partners in civilian practice, future installation leaders can extend their reach and unclog the military health care system and train soldiers for the trauma they will see on the next battlefield.[253] Prior coordination and rehearsals with private medical facilities must occur before internal medical capabilities are overwhelmed. This process includes having signed agreements between the U.S. Army and civilian community ready to execute. All of these recommendations support a complex adaptive healthcare system that future installation leaders must manage carefully to mitigate second and third order effects.

Summary

Future installation leaders must provide a vision for the installation of 2035-2050 that understands the challenges of the future installation medical environment. The AMEDD and the U.S. Army mobilization system must be aligned to combat the coming threat and change the technological environment to provide efficient medical processing at future installations. The requirement for speed when medically processing soldiers to get to the fight is essential to support future operations. Future installation leaders should also incorporate updated medical technology IT systems that support virtual health combat the MD shortage.

Changing the culture, leveraging technology, and aligning capabilities are essential for future installations. Future installation leaders will need to provide a vision and manage change through strategic leadership and fiscal lenses to revitalize essential medical services. While the monetary cost to enhance future installations with the best medical IT, aligned medical capabilities, and installation force structure is high, not paying the price will be more significant to the U.S. if soldiers are inadequately prepared to mobilize to support U.S. vital national interests.

Future installation leaders will need to introduce technology requests into the programming phase of the PPBE to receive the capability in the next five years. Technology is essential to change and align the culture that operates the medical portion of the future mobilization installation. Alignment also includes an organizational culture the arrays medical services appropriately to support the future installation requirements of readiness, mobilization, and force projection.

A critical component of an aligned culture is ensuring future installations have the proper medical capabilities on the installation to care for mobilizing soldiers, utilize the RC support, and acquire assistance from the civilian medical network. To embed change in the U.S. Army culture future installation leaders will need to craft policy that directs soldiers to change their behavior from a medical readiness model to a medical preparedness model.

Leveraging interoperable technology and adaptive IT systems will improve medical business processes supporting mobilization. Developing situational awareness and data sharing among the U.S. Army's three components is critical to combat the threat in contested environments. An updated information picture is essential for future installation leaders to process soldiers for mobilization expeditiously. U.S. Army future installation leaders must implement solutions that positively impact culture, and technology to affect the future installation positively. These procedures will help to counter the MD shortage, provide appropriate human capital, and technological solutions for medical activities on future installations that enhance combat preparedness and force projection.

INSTALLATIONS CONTRACTED SERVICES-2035 AND BEYOND

COL Mary Drayton, U.S. Army

"Deliver performance at the speed of relevance. Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting…. Our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades. We must not accept cumbersome approval chains, wasteful applications of resources in uncompetitive space, or overly risk-averse thinking that impedes change."[254]

2018 National Defense Strategy

To meet the challenges of the Future Operational Environment (FOE) in 2035 and beyond, CONUS-based Army Installations will require changes in how they acquire contracted services and supplies in support of Warfighters, family members, retirees and Department of Defense civilians. This paper will examine Department of Defense service contracts, Intergovernmental Service Agreements (IGSA), and FOE threats, and offers recommendations for increasing future Installation requisition efficiency and effectiveness.

Current Contracted Services

Installation Management Command (IMCOM) maximizes the use of IGSAs over conventional Department of Defense contracting solutions through the Army Contracting Command, United States Air Force or United States Army Corps of Engineers for services on their installations. By the year 2035 IGSAs may comprise the majority contracted services on installations (i.e. waste management, snow and ice removal, grounds maintenance, etc.) IGSAs allow for flexibility, less oversight, and burden-sharing with surrounding local governments. IGSAs strengthen public-military relationships.

However, the use of IGSAs pose three challenges. The DoD authorizes use of IGSAs with terms less than 10 years, lack of need for oversight for the services provided, and, if the IGSAs fail to provide the service due to a lack of capacity, the current fallback mechanism is conventional contracting. Many local governments have contracted services over ten years and the military must consider extending allowable service terms. In addition, the current approval process for IGSAs within the Army is lengthy and hampers the partnering opportunities because local governments adhere to strict schedules to have services in place for their communities.

The Department of Defense (DOD) obligated $273.5 billion in fiscal year 2015 on contracted goods and services including major weapon systems, support for military bases, information technology, consulting services, and commercial items. Contracts also included supporting contingency operations, such as those in Afghanistan and Iraq. DOD is, by far, the single largest contracting agency in the federal government, typically accounting for about two-thirds of all federal contracting activity.

Future Operational Environment and Threats

Military installation is a, “base, camp, post, station, yard, center, homeport facility for any ship, or other activity under the jurisdiction of the Secretary of a military department.”[255] This definition remains the same for the FOE and is used throughout this paper when addressing Army contracted services.

The Army must prioritize the requirements for the contracting organizations to deliver on-time, in the right place and at the best value. All three of these have the potential for accomplishment with the right organizational structure, a trained and talented workforce and the right resources. A future attack on our installations is highly probable, the method of attack can occur in any of the five domains (cyber, land, sea, air and space) and the attack can have far reaching impacts not only for our military members but for their families, DoD employees and the civilians that live and work in surrounding communities.

Threats to the contracting system will only increase in 2035 with greater potential to degrade the readiness of our Warfighters. According to the Homeland Security Secretary, “cyberweapons and sophisticated hacking poses a greater threat to the United States than the risk of physical attacks.”[256] The threats on contracting functions, contracts and contracted services and goods will impact financial systems and contracting systems. Delivery of goods and equipment may be re-routed or intercepted by drones. Competitors can compromise the payment systems by shifting payments to various accounts to fund violent extremist groups or other non-state actors. Chloe Demrovsky states, “Cyber threats to supply chains have become increasingly prevalent due to extensive sharing of digital information between organizations and their suppliers.”[257] This share of the information will greatly impact the supply chain for major systems and may be an area for investment in 3D printing to shorten the chain between production and user.

The future will see accelerated use of unmanned vehicle technology or unmanned aircraft systems (UAS). Ever since 2015, the Obama administration promoted the use of unmanned aircraft systems for greater “operational flexibility” and “lower cost”.[258] The current Trump administration has created a new drone Integration Pilot Program that acknowledges “drones are a critical, fast-growing part of American aviation, increasing efficiency, productivity, and jobs”.[259] This program is designed to provide the “delivery of life-saving medicines, commercial packages, inspections of critical infrastructure” which will enable efficiencies on the installations.[260] Installations will have to embrace the use of the new technology to remain competitive in all aspects. Vendor delivery of supplies not only affects family members but impacts each tenant unit on the Installation.

In 2016, Amazon introduced a new delivery system designed to get packages to customers in about 30 minutes from the time of purchase using unmanned aerial vehicles. Vendors in the United Kingdom utilized this new delivery system to deliver packages weighing five pounds or less. Amazon is working with industry to ensure they are in strict compliance with the airspace regulations.[261] Amazon uses “sense and avoid technology” to scan for potential hazards. Amazon is not the only company looking into the use of remotely piloted vehicles to deliver goods, Walmart and Ford are researching options as well to remain competitive. Ford has also invested in a new business unit through 2023, Ford Autonomous Vehicles, focused on self-driving vehicles.[262] The United States military needs to partner with industries to incorporate the technology that will help identify and scan “friendly” or “safe” drones or autonomous vehicles to ensure delivery of goods to individuals that work, live and operate on the installations. If entry access points can scan possible threats, then it should be easy to quickly counter and disable the system.

The rise of near-peer competitors and the increase of non-state actors with access to technology pose a threat to contracting and delivery of goods and services. Competitors can compromise drone delivery because of the widespread availability of commercial drones. As of 2018 there were over a million operators in the United States licensed by the Federal Aviation Administration (FAA) to use drones.[263] However, these numbers do not include the potential for the increase of weaponized drones with “explosive payloads, deliver harmful substances and conduct reconnaissance”. Moreover, the FAA estimates drones will triple to 3.5 million by the year 2021.[264] This includes actors and non-state actors who will leverage the use drones for illicit purposes threatening U.S. national interests and citizens.

Previously the United States operated in multiple domains freely without fear of threat to national interests and U.S. citizens. However, competitors now challenge the U.S. in every domain and the U.S. Army must ensure it maintains its competitive advantage. Additionally, the security and defense strategies of the U.S. no longer regard the homeland as a sanctuary but the Army will likely require future military installations provide services to individuals who work and/or live within the established boundaries. The domain of the most importance for contracting services and goods in the FOE is the cyber domain which allows for ease of access to banking systems, proprietary information, intellectual property, sensitive information pertaining to weapons systems or programs, and personnel data by our adversaries. To counter the threat of access to the military must either reduce the footprint on the installations to decrease the amount of contracted services or explore alternate means of providing the same level of support with redundant systems capable of safeguarding critical information.

An excellent opportunity to leverage is public sector physical fitness businesses in place of installation fitness centers. Investing in gyms that have all the required equipment, accessible 24 hours a day to account for various shifts and provide a range of classes will benefit the Warfighter. Currently, some of the larger installations like Fort Hood, Fort Bragg, and Fort Carson have more than five fitness centers or gyms each with aging equipment, limited hours and sporadic fitness classes. The FOE of a reduced footprint on installations should allow for a consolidation of fitness facilities, leveraging resources which the Army can shift to overall training of the force.

Amazon and Walmart businesses provide a wider selection of goods, more competitive prices and faster delivery than the PX. By 2035, the U.S. military should partner with Walmart or like-businesses to provide benefits that are commensurate to the savings earned now for Active duty, family members and retirees. Many businesses provide discounts varying from 5-20%, some on only specific days of the week or holidays. However, the military should conduct market analysis and either compensate service members or negotiate benefits with the local businesses.

Another area that impacts the readiness of the force in respect to family members is the Exceptional Family Member Program (EFMP). The EFMP requires better automation to streamline the process of information sharing from the EFMP coordinator to required agencies that deliver services to family members with special needs, i.e. the Child and Youth Services (CYS) or the schools. The lack of interoperability within the systems create inefficiencies. Interoperable automated services could easily transcribe this information. Implement the utilization of biometrics to authorize sharing the information between systems would provide security for the patients. This would give time back to the soldier who may have a special needs family member who utilizes services on post. The movement to interoperable systems with access to health information, financial data, etc. increases the vulnerability of personally identifiable information to attack of compromise from malign actors.

As with the increase of human-machine interfaces, there will be an increase of the use of drones and autonomous vehicles to deliver goods and provide services. Autonomous dump trucks, autonomous snow removal systems and autonomous vehicles that can conduct mundane, repetitious actions without worker fatigue or environmental conditions impacting their operation. These systems will be critical to maintaining roads and training areas on the installations. However, the increased use will allow for more opportunities for cyber-attacks on critical systems. The threat on these systems requires redundancy in the military systems and increased investment in the U.S. cyber capabilities.

Army Contracting Reorganization

The consolidation of service contracting agencies and integration of Artificial Intelligence (AI) in procurement systems can provide greater efficiency to contracting offices and benefits the customers. This efficiency and effectiveness in the DoD procurement process will enable the readiness and lethality of the Warfighter and ensure the United States competitive edge in a strategic competitive environment. In addition to a reorganization of the contracting organizations within the services, implementation of AI in the procurement systems will decrease the burden on the approximately 8000 contracting professionals within the Department of the Army (DA).

The reorganized Army Contracting organization would work directly with DoD customers/requiring activities to ensure they receive the supplies and services-at the right time and right place, while achieving the best return on investment for taxpayers. The consolidation of Air Force, Army and Navy contracting organizations into one contracting agency-level organization would provide consistency, reduce redundancy and potentially save millions of dollars.

Currently separate services perform pre-award contracting. However, the Defense Contract Management Agency (DCMA) conducts post-award functions. DCMA is the Department of Defense (DoD) component that works directly with Defense suppliers to help ensure that DoD, Federal, and allied government supplies and services are on-time, at projected cost, and meet all performance requirements. DCMA directly contributes to the military readiness of the United States and its allies and helps preserve the nation’s freedom.[265]

In addition, the Army carries the burden for the majority of the deployments in support of Joint, Interagency, Intergovernmental and Multi-national operations. Combining the services under one umbrella will sustain a contract ready Active Duty (AD)/Reserve Component (RC) through high quality integrated health care. Maintain a trained and ready deployable contracting force to include both military and DoD civilians. The Defense Contract Management Agency staffs a combat support center to manage the worldwide deployment requirements. The Combat Support Center (CSC) will receive validated CCAS deployment requirements from DCMA International (DCMAI) via a CCAS Manpower Authorization Document and fills the requisitions.[266] Combining the services under the DCA would achieve significant cost savings through reduction in redundancy and variation. The different services all have a different contract writing system. The Army uses the Procurement Defense Desktop (PD2) and will replace it with the Army Contract Writing System (ACWS).[267] The Air Force uses the Standard Procurement System. The Navy was also pursuing a separate contract writing system in 2017 valued at approximately $250M.[268] With multiple offices there is often an opportunity for requiring activities or customers to "shop" around for an office that will provide a particular service or interpret a regulation a certain way. Each contracting organization uses the same regulations, the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement. Agencies have typically added separate levels of additional policy adding levels of review and overall timeline of awarding a contract. With one agency, the desire is that there would be less self-imposed policy. Each organization utilizes the same regulatory guidance and customers will receive the same business advice regardless of office. There would be clear lines for decision authority and accountability.

A common operating picture for all contracts around the world utilizing existing contract vehicles to fulfill the requirements of a requiring activity would greatly decrease the amount of time required on cradle-to-grave contracts. It is imperative that the Army ensure outstanding contracting support for both current and future military operations and exercise cost-saving and containment measures required that the DoD maintains its competitive edge with the rapid technological and innovation. The DoD needs to operate the most efficient procurement system possible, elevating cost containment as a priority objective and increasing unity of effort as an implementation capability. A new contracting command organization will provide unity of command, accountability, and readiness at the speed and scale required to prevail in future conflicts.

A general or flag officer at the 3-star level would lead the DCA, directly reporting to the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD (AT&L)]. Additionally, all contracting activities would be transfer to the DCA and would operate under its authority, direction, and control. The Military Departments would continue to own all military personnel and be responsible for organizing, training, and equipping their deployable military contracting forces. It is important that our Acquisition contracting workforce is agile, along with its systems, to procure services and supplies that will enable readiness in a multi-domain environment. Personnel requirements of the Services' operational forces needed for deployment and/or training require approval from the Director, DCA. Each Service claims there are "service specific" acquisitions that prevent consolidation of the services under one umbrella.

Artificial Intelligence

There are numerous systems within the Department of the Army utilized to procure services and supplies on behalf of the warfighter. Department of the Army contracting professionals typically use: a system to appoint contracting officer representatives; verify contractor eligibility for a Department of Defense Contract Award in the System for Award Management; award the contract in the Procurement Defense Desktop (PD2); file and manage the contract in the Paperless Contracting File (PCF); ensure payment in the Wide Area Workflow (WAWF); verify previous performance in the Contractor Performance Appraisal Reporting System (CPARS) prior to award; and, review prior contracts and payments through the Electronic Data Access system. Many of these systems are redundant, slow to respond, and require multiple passwords or data to access. When an employee misplaces or forgets their password it can take up to 48 hours to reset the password. This negatively impacts and extends the timeline of the availability of the supply or service needed by the requiring activity. In addition, security requires that passwords must change frequently. Creating a system that allows for a biometric scan to gain access to the many systems can decrease the amount of time required to operate in the systems.

There are several innovative products that can positively influence the contracting process. In many households, families use technology like Amazon’s Alexa to search the web for products and services. Alexa provides several options that could be applied to obtaining market research for the commodities and services the organizations on installations require. Through a voice recognition platform, requiring activities and contracting offices could simply request “Alexa” to provide options for the companies that can provide a capability or fulfill a requirement.

In addition, there are several issues with bridge contracts "when a contract is set to expire and there is a continuing need for services, but the follow-on contract is not ready to be awarded, the government can extend the existing contract or award a short-term sole-source contract to an incumbent contractor."[269] Awarding contracts without competition potentially costs more money to the taxpayer. Bridge contracts are mostly a result of a lack of planning, lack of oversight for expiring contracts, personnel turnover, and unexpected requirements. However, humans paired with machine learning contracting activities or agencies could automatically reach out to requiring activities based of the period of performance to verify continued use of the service, should the agency exercise an option year, end a contract or solicit for a new contract.

Service Contract Oversight

Contracting officers designate a Contracting Officer's Representative (COR) for all service contracts prior to awarding a contract. "A *Contracting officer's representative* is an individual designated in accordance with DFARS subsection 201.602-2 and authorized in writing by the contracting officer to perform specific technical or administrative functions."[270] Based on the complexity and value of the service contract there are several training courses, exams, monthly reports to include surveillance and Contractor Performance Appraisal Reporting System. The performance of these additional duties requires time in addition to the primary duty or responsibility of the employee. Failure to perform these duties can have a negative impact especially if the execution of the contract is not according to its terms and conditions, ultimately costing time and money.

Recommendations

Recently, IMCOM established a Senior Contracting Executive position as a senior advisor to the IMCOM Commander on contracted solutions in support of the installations. The current approval process for the use of IGSAs involves significantly low thresholds and numerous approval levels. The following is a proposal for an approval process based on the addition of the Senior Contracting Executive and embedded contracting cell which will create flexibility for IMCOM thereby decreasing the amount of reviews and time required to approve IGSAs:

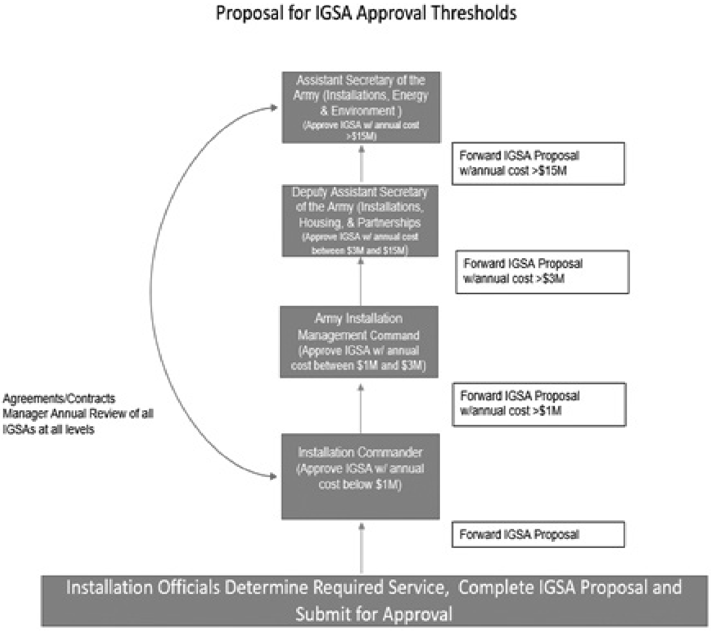
Proposal for IGSA Approval Thresholds
Assistant Secretary of the Army (Installations, Energy & Environment) (Approve IGSA w/ annual cost >$15M)
Forward IGSA Proposal w/annual cost >$15M
Deputy Assistant Secretary of the Army (Installations, Housing, & Partnerships (Approve IGSA w/ annual cost between $3M and $15M)
Forward IGSA Proposal w/annual cost >$3M
Army Installation Management Command (Approve IGSA w/ annual cost between $1M and $3M)
Forward IGSA Proposal w/annual cost >$1M
Agreements/Contracts Manager Annual Review of all IGSAs at all levels
Installation Commander (Approve IGSA w/ annual cost below $1M)
Forward IGSA Proposal
Installation Officials Determine Required Service, Complete IGSA Proposal and Submit for Approval

Figure 1: Proposed Intergovernmental Support Agreement Approval Flow

It is important for the military to partner with agencies like the Federal Bureau of Investigation and Federal Aviation Administration as they research ways to detect “rogue” drones, as similar applications are useful for detection around military installations.[271] The military effort in interagency collaboration to ensure the safety and security of the homeland is critical to the CSA’s top priority of readiness.

The Army must consider moving soldiers, families and civilians off the installations as the delivery of items by unmanned aerial vehicles (UAVs) increases, otherwise thousands of drones could potentially fly over Installations. As an alternative, Installations could create designated delivery drop-off zone(s) on the installations for tenant units and individuals to pick up goods or an approved autonomous vehicle can pick up the items from the drop site.

If the businesses do not want to provide discounted goods and services then perhaps a military version Walmart on the Installations, accessible to DoD civilians, and private citizens, would be of interest. The same with the commissary, partner with the nearby grocery stores to open a neighborhood version on the installation. Moving on the installation will provide job opportunities for the service member spouses, however the FOE should promote working and training only on the installations. Stores would provide discounts based off eligibility; easily applied by reading eligibility benefits off the common access card chip, phone number or special military benefits card provided by the store. The partnerships with the surrounding communities to either build on-post or provide the benefits off-post could strengthen public-military relationships.

For the services provided by the Installations, implementation of human-machine interfaces providing feedback to service members, families, DoD civilians and retires will increase efficiencies. Making user-friendly platforms or "reputation management software" offering real-time reporting on contracted services is crucial to prioritizing services and resourcing appropriately.[272] These feedback mechanisms, based on the data collected, allow for flexibility and adjustment of services in a more efficient manner especially as the DoD expects to operate in a more resource constrained environment. The amount of data that these systems can collect would outpace that currently provided by physically filling out forms, answering telephonic surveys or using the Interactive Customer Evaluation (ICE) link.

To assist with the functions of the COR, there are ways to monitor performance of contracts through surveillance cameras with "digital brains." The implementation of artificial intelligence will assist with surveillance schedules, data compilation and submission of reports on the performance of contractors. For example, there is the product by IC Realtime named Ella, which partners CCTV with AI and analyzes what is happening in video feeds and make the content searchable.[273] This searchable feature would allow the COR to review when contractors are performing functions and analyze the level of performance.

Organizational Change

There will need to be a change in military culture, to include the retiree communities, to move from government-provided services to private partnerships and organizations. Many veterans return to commissaries and post exchanges to maintain their connection to an institution they were a part for a significant part of their lives. Veterans travel hours to these facilities because they feel a sense of belonging. Senior leaders would need to message early and often prior to the transition of these services while providing the benefits of privatization. In addition, it is known that DoD "recognizes that a large influx of new patrons is necessary to continue efficiently providing commissary and exchange benefits into the future."[274] In order to create the revenue required opening on-post access to our surrounding communities will be critical or cost-sharing with off-post businesses. This will provide the opportunity to reinvest revenue generated by the Warfighters, family members and veterans into readiness and modernization of the force.

Conclusion

Given current Army requisition processes, Installations will fail to meet FOE demands. Installations require changes in how they acquire contracted services and supplies in support of Warfighters, family members, retirees and Department of Defense civilians. The challenges of the future multi-domain environment include multiple threats to services currently provided by CONUS installations. To compensate, the Department of the Army must: decrease the footprint on the Installations and strengthen partnerships with surrounding communities; increase utilization of Intergovernmental Service Agreements (IGSAs) for Installation services; and explore the utilization of artificial intelligence and machine learning to increase efficiency and effectiveness of contracting oversight functions. By implementing these recommendations, the Installations will be able to ensure the readiness of our Warfighters and maintain the nation's competitive edge in the volatile, uncertain, complex and ambiguous environment.

Section Three:
SECURITY

FUTURE ARMY INSTALLATIONS: A COMPREHENSIVE APPROACH TO CONVERGENCE

COL Kenneth Slover, U.S. Army

A conceptual revolution is underway for United States (U.S.) Army operations. The concept that will drive future force structure, modernization and readiness efforts in the Army of 2035 is Multi-Domain Operations (MDO). Current U.S. defense strategy acknowledges that Army installations will not be sanctuaries[275] and therefore homeland defense doctrine will require evolution to enable the Department of Defense (DOD) to become the supported institution in this endeavor. Informed by threat assessments in the Joint Operating Environment (JOE) 2035, the MDO foundational documents rely upon the notion of convergence to enable overseas operational reach; the ability to rapidly optimize combat power projection and inflict will upon a peer state competitor through all domains.[276] Convergence of Anti-Access Area Denial (A2AD) systems, cyber, space, information, and intelligence technologies reinforces Max Boot's opinion in *The New American Way of War* that the offensive-minded Army remains reliant on speed, maneuver, flexibility, and surprise.[277] Evolving the Army's traditional role of Defense Support to Civil Authorities (DSCA), the conduct of offensive, defensive, and stability operations within CONUS will require a change in Army doctrine to enable the DOD as the lead for Homeland Defense within sovereign U.S territory.

As a strategic competitor, The People's Republic of China (PRC) advances their organizational design and doctrine to a similarly emerging concept of system destruction warfare.[278] The PRC structures their military force, modernization efforts and readiness to achieve a decisive victory at or below the threshold of armed conflict for the remainder of the 21st century.[279] Instead of MDO methods of penetrating, dis-integrate and exploit; the unified People's Liberation Army (PLA) systems destruction method of warfare centers on disruption, paralysis, and destruction of the enemy's operational system capability through lethal and non-lethal means. The PRC also aspires to target systems distant from its sovereign territory. The PRC and U.S. concepts are similarly concentrating on offensive Freedom of Maneuver (FOM) projecting from the homeland in 2035. The PRC are gaining the capacity to organize and resource toward driving wedges in the Army installation enterprise by indirectly targeting vulnerabilities and seams in authorities. Whether through disruptive technologies that appear in the traditional domains or new technologies impacting all domains, the Army installation enterprise will likely require new countermeasures and cooperative authorities between the Department of Homeland Security (DHS) and DOD's Army to conduct Decisive Action (DA) within the continental U.S. (CONUS). The PRC takes an indirect approach with systems warfare by targeting vulnerabilities in force generation, sustainment, and power projection capabilities; essential activities of Army installations.

This research will provide analysis and recommendations of doctrinal changes vital for Army MDO concepts to provide security and further define the warfighting role of Army in 2035. A literature review of U.S. strategic guidance and direction affirms the necessity of doctrinal change to incorporate MDO concepts as a protagonist to the 2035 threat environment. A methodology of comparison between current homeland security policy and defense doctrine with emerging MDO and the JOE 2035 concepts will reveal unacceptable gaps in ways the U.S. approaches warfighting within the CONUS. A logical output of the analysis are recommendations to adjust doctrine, enabling the Army warfighter in protecting the homeland through defensive integration of installation strongpoints, enabling offensive power projection through FOM and MDO competition through stability operations.

Before analysis, some assumptions are necessary to provide the context of future MDO requirements of Army installations. The first assumption considers the current political landscape and direction; that national security and nested defense and homeland security guidance remain relevant from current strategic documents and congressional testimony. While formally recognized in the JOE 2035 and the Army Training and Doctrine Command's (TRADOC) *Operational Environment and the Changing Character of War,* a second assumption is the assessed future threat environment.[280] Through the year 2035, the Operational Environment (OE) is characterized by what TRADOC labels the "Era of Accelerated Human Progress." It is in this era where there is an anticipated convergence of thought and technologies that create multiple dilemmas for the U.S., both abroad and in the homeland, which is no longer considered a sanctuary.[281]

MDO is the U.S. Army's approach to counter multiple threats across the OE with similar, near-peer, operational approaches in 2035. It predicates a CONUS-based Army and Joint Force executing outside CONUS, or OCONUS, offensive action through operational and strategic maneuver in great power competition over all domains. When necessary, an offensive systems approach penetrates and dis-integrates A2AD defenses, exploits FOM and returns to a state of competition. The U.S. conceptualizes MDO offensive FOM projecting from the homeland to enable Geographic Combatant Commands (GCC) with Multi-Domain Formations; calibrated to compete, penetrate, dis-integrate, exploit then re-compete against a peer state adversary, such as the PRC. The MDO concept of future warfare does not address defensive, offensive and stability tasks across all domains within the homeland where operational and strategic maneuver generate. In the event of competition at or below the level of armed conflict, the CONUS-based Army installation's inability to defend against a multi-tiered threat force while conducting force generation and protection activities is a significant vulnerability that flaws many foundational assumptions of MDO, the operational concept for 2025-2045.[282]

Policy Review

An analysis of current strategic guidance and direction indicates there is an acknowledgment of a complex future threat environment, but without current urgency to necessitate an organizational and cultural change for how the Army operates in the CONUS of 2035. The National Security Strategy (NSS) describes a homeland enhanced missile defense A2AD, ensuring the defense of sovereign territory against an arsenal of advanced missiles.[283] Defense is in the domains of air, sea, and cyberspace. The land domains' focus is on border security, countering terrorism and weapons of mass destruction through efforts by DHS, law enforcement and the intelligence community. The Army's offensive mass promotes peace through strength, deterring adversaries through competition using all instruments of national power.[284] Acknowledging the rapid advance of technology, the NSS calls for new concepts and capabilities to protect the homeland.[285]

The 2018 National Defense Strategy (NDS) states that the homeland is no longer a sanctuary, an assumption that emphasizes a critical vulnerability. Army installations within the CONUS Strategic Support Area (SSA) from the MDO framework are prone to attack from state competitors. Most Army forces will remain based in CONUS installations preparing for and prosecuting warfighting tasks enabled by an installation force generation and power projection enterprise necessary for future operations.**[286]** U.S. adversaries will be capable of resourcing competition in all domains at the right time and place by 2035. Additionally, since urgency drives change,[287] a fundamental assumption of MDO and future installations is the appetite to commit national, joint and Army resources by adjusting national authorities for the conduct of warfighting tasks within CONUS to deter and defeat adversaries.**[288]**

The principal objective in the NDS is to defend the homeland from attack.[289] Nested within the NSS, the Defense Strategy asserts that the U.S. “must anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us while developing operational concepts to sharpen our competitive advantages and enhance our lethality.”[290] The National Military Strategy (NMS) identifies globally integrated force design, management, and development as the joint method to compete with our adversaries and protect the homeland through deterrence, assurance, and response;[291] all through the perspective of offensive, defensive and stability operations conducted OCONUS. The Chairman of the

Joint Chiefs of Staff (CJCS), General Dunford, speaks to a “boxer stance” to emphasize the constant level of readiness necessary to counter any adversary in any locale.[292]

Following the terrorist attacks of September 11, 2001, the U.S. became acutely aware of a homeland vulnerability; creating domestic urgency to hold adversaries accountable overseas and prevent future attacks within the territorial boundaries from reoccurring. There is not a similar sense of urgency to enable FOM by Army forces within CONUS. Restrictions on the employment of military forces in domestic spaces are most significant in the land domain because of traditional concerns over internal abuse.[293] The Posse Comitatus Act prohibits the use of Title 10 forces for domestic law enforcement.[294] The President of the United States (POTUS) can make exceptions through the Insurrection Act, under which Title 10 forces conduct law enforcement only under emergency circumstances. However, these are about law enforcement activities and if utilized, only have DOD in the lead for a short amount of time.

DHS policy prescribes conduct in response to or preparation for threats to the homeland. DHS in concert with state and local law enforcement and emergency response agencies, develop procedures, policy, and protocols to safeguard against primarily a Violent Extremist Organization (VEO) threat, secure and manage the borders, enforce immigration laws and strengthen national preparedness and resilience.[295] The National Strategy of Homeland Security (NSHS) focuses on the safety and security of the nation through the development and implementation of a National Planning Framework (NPF). According to the framework, it is everyone’s responsibility, from an individual through the community to state and federal government to adapt and act in the event of a homeland threat – terrorist or otherwise regardless of scale.[296]

In 2018's Association of the United States Army (AUSA) annual conference, the DHS Secretary, Kirstjen M. Nielsen, described a "Relentless Resilience Agenda." This resilience described cybersecurity, border security, and disaster response depend heavily on DHS and DOD collaboration. Also, she told the Army audience to "think creatively about how we can partner …how we can combine our authorities to overcome the threats. Look outside of traditional boundaries and lines of effort." [297] This statement echoes the NSS and NDS guidance of creativity in new concept development. Current policy, however, does not permit the flexibility to converge an interagency effort to conduct offensive, defensive and stability tasks in all domains from CONUS installations that support the force development, generation, and integration enterprise for the Army.

The U.S. Northern Command (USNORTHCOM) GCC is responsible for homeland defense and coordinating DSCA.[298] In her 2018 USNORTHCOM and NORAD posture statement before the Senate Armed Service Committee (SASC), General Lori Robinson described the missile threat to the homeland from the global peer and regional adversaries, unmanned aerial systems and transnational crime.[299] These threats of today do not compel Decisive Action changes in the future without the before mentioned POTUS direction. The routine USNORTHCOM mission requires assisting civil authorities to establish cooperative agreements at the DHS, state, and local levels to enable a ground component "homeland in depth."[300] The Army components of USNORTHCOM work with DHS, interagency partners, and civil authorities to support homeland security, complementing some aspects of composite security.[301] The USNORTHCOM GCC does not have a relationship with Army installations for a DOD and Army integrated defense in depth. Instead, it is reliant on the DHS, the Justice Department, state and local law enforcement agencies.

Strategic guidance and policy acknowledge homeland vulnerability and a need to act cooperatively between DOD and DHS to achieve resilience. The Army and its enterprise partners have vulnerabilities with the information technology network, airspace management, logistic readiness center, and politically-sensitive local cooperative agreements.[302] According to DOD Instruction 3020.45, Mission Assurance (MA) is strategic-level risk management across all protection and resilience programs of DOD to include cyber information security. In the future threat environment, peer adversaries such as the PRC present multiple, simultaneous dilemmas in all domains. The MA strategy may not suffice to sustain a CONUS force generation base because it does not subscribe to the characteristics of synchronization, simultaneity, depth, and flexibility. MA centers on identification of hazard, assessment, management of risk, and continued monitoring. MA is valuable to the CJCS to provide strategic direction, but it is an inadequate warfighting method to support an MDO concept of offensive, defensive and stability DA tasks within CONUS Army installations.

In terms of urgency, current Army leaders do not describe an immediate need for change toward the future, CONUS-based OE in their congressional testimony. In Army Secretary, Mark Esper, and Chief of Staff, General Mark Miley’s 2018 posture statement testimony to the Senate Armed Services Committee

(SASC), they cite the homeland efforts include the Global Response Force (GRF) able to project anywhere in ninety-six hours and the Army commitment to DSCA in disaster relief efforts.[303] However, neither leader describes installation and enterprise support to enable future soldier readiness, nor did they make budget priorities of the kind. General Miley and Secretary Esper go on to attest that the competitive advantage held by the U.S. Army is the trained and ready soldier's ability to deploy rapidly and gain a decisive advantage. Readiness is significant to acknowledge as it is out of alignment with an infrastructure modernization effort to resource the future MDO capable Army. These missions, tasks, and operational funding are effective in meeting the current threat environment; however, the character of war is changing.[304] Likewise, Army installations must change.

Doctrine Review

For clarity, it is useful to consolidate discussion of Army doctrine into a series categorization. The Army Doctrine Publication (ADP) defines fundamental principles, the Army Doctrine Reference Publication (ADRP) provides details on the fundamentals, and the Field Manual (FM) describes tactics and procedures.[305] Each series has a similar title and index publication number. For this Army doctrinal review, the fundamentals are resident throughout each series with a shared index number. A specific reference to one implies application across the series; for example, a reference to ADP 3-07, *Stability* also fundamentally resonates with ADRP 3-07 and FM 3-07 with the same title of *Stability*.

All Army doctrine is logically nested to describe its contribution to joint operations through Unified Land Operations (ULO). ULO is executed through DA, the continuous, simultaneous combinations of offensive, defensive, and stability or DSCA tasks.[306] Outside the U.S., the Army executes the tasks of offense, stability, and defense in varying degrees and primarily conducts DSCA within CONUS.[307] Similar to Max Boot's characteristics of American warfighting, the Army develops operations characterized by simultaneity across many domains, depth as an extension of time and space, synchronization to maximize effective combat power, and flexibility of options and formations. In the homeland, "Army forces apply the tenets of operations when supporting civil authorities to save lives, alleviate suffering, and protect property."[308] Upon review of ADRP 3-0, *Operations,* ULO isolates DA tasks of offense, defense, and stability to OCONUS primary warfighting roles with mission dependent degrees of intensity. Within CONUS, the Army does not possess the liberty to pursue warfighting roles given the supporting nature of the DSCA task and reactive nature of a defense to an attack on the homeland.

According to ADP 3-28, *Defense Support of Civil Authorities*, providing support for domestic disasters, incidents, civilian law enforcement agencies and whatever designated by the DOD are subtasks for DCSA within CONUS. The DSCA reactive purpose is to save lives, restore essential services, maintain or restore law and order, protect infrastructure and property, and support maintenance or restoration of local government. The term, "A2AD bubble," describes the DOD defense of the homeland through a primarily missile-heavy defensive posture.[309] For the land domain, law and guidance are more restrictive, permitting the support of and assistance to civil authorities in a variety of missions from disaster relief to suppressing insurrections.[310] Certain military functions such as intelligence operations, rules of engagement, and rules for the use of force have restrictive legal implications. According to Joint Publication (JP) 3-27, *Homeland Defense*, the "DOD must be postured to take immediate, decisive action to defend against and defeat the threat in the homeland."[311] There currently is no legal prohibition that limits the POTUS from directing and the Secretary of Defense (SECDEF) from implementing a more robust force structure, posturing to conduct offensive, defensive and stability operations against a peer-state competitor within the American population at the Army installation level.

The tenets of ULO pertain to the DA tasks of offense, defense, and stability. Each task has characteristics that further describe fundamentals for application. Those that are relevant within a homeland defense discussion are concentration, operations in depth and a comprehensive approach. Concentration describes massing of effects on a decisive point across all domains with all elements of combat power. Operations in-depth expand on concentration and extend the scope to the entirety of the OE. A comprehensive approach integrates the cooperative effort and unity of purpose of all Joint, Interagency, Intergovernmental, and Multinational (JIIM) partners in leveraging instruments of national power toward ULO.[312]

No Army doctrine provides principles, fundamentals or tactics and procedures specifically for homeland defense. The defensive task of DA has related subtasks of area defense, mobile defense and retrograde. The Army contribution to an area defense in the air domain is homeland missile defense. The extended purpose of the area defense is to deter or defeat enemy offense, gain time, achieve economy of force, retain key terrain, and protect the population, critical assets, and infrastructure.[313] This purpose would be advantageous to Army installations of the future because it enables warfighting against the anticipated PRC systems destruction warfare concept within all contested domains to safeguard the force and population. DHS is the primary government agency for the security of land, and the Coast Guard for the sea. Currently, to achieve a unity of command in all domains, the POTUS is the first common authority as he can direct both secretaries. The relevance of a comprehensive approach to DA tasks is already resident in Army doctrine; only without the authorities to execute homeland defense within CONUS territory. The DA task of stability focuses explicitly on the maintenance of a safe and secure environment by meeting the survival needs of an OCONUS population. The stability task is a constant in any Army operation and leverages all instruments of national power to be successful; diplomatic, information, economic and military (DIME). It is prevalent across the Range of Military Options (ROMO), with the highest intensity before and following large scale combat operations.

The necessity of a comprehensive approach to concentrate, or converge, DIME throughout the depth of all domains is the MDO concept of competition. Like stability, competition is prevalent across ROMO and below the level of armed conflict. An MDO tenant of Army Multi-Domain Formations will conduct simultaneous offensive, defensive and stability tasks. Under MDO, the tasks are conducted with relative intensity both CONUS in the SSA, and OCONUS throughout the depth of the expanded operational framework. A cyber offensive operation will originate from CONUS Army installations. Likewise, many future technologies will provide standoff but still receive guidance and direction from the SSA. This ability is also a vulnerability in the cyber domain that necessitates an active defense. The MDO concept calls for a present forward force as an initial contact force with an adversary. Contact does not mean physical contact in OCONUS locations. Instead, it could be from fixed CONUS positions. Positional reference is an important distinction when discussing MDO as it provides a framework for understanding where actions occur. Points and pathways illustrate the depth of reach Army forces will achieve under MDO in 2035. The SSA consists of CONUS Army installations as a source of force generation and convergence within space, cyberspace, information, and electromagnetic spectral domains.

A merger of current doctrine and future concepts provide an option of how the Army needs to fight in the future threat environment. Recently aligned under the Army Materiel Command (AMC), the Assistant Chief of Staff for Installation Management (ACSIM) support GCC and provide critical infrastructure to organize, train, equip, deploy, and conduct combat operations by land forces.[314] Within ACSIM is Installation Management Command (IMCOM) whose mission is to deliver and integrate base support to enable readiness for a self-reliant and globally-responsive Army.[315] While the Commanding General (CG), IMCOM does not manage all Army installations, there is a dual-hatted relationship between a warfighting unit CG (usually a division commander) and the non-warfighting enabler in the U.S. Army Garrison (USAG) Commander. This command relationship is worth noting regarding the authorities for mission assurance, force protection, and Decisive Action requirements. The separation sets a tone of enterprise management focus instead of warfighting capability. The *IMCOM 2025 and Beyond* strategy neither references the future threat environment[316] nor describes a necessity for DA tasks from an installation enterprise.

Analysis

As MDO is a concept, there is ample opportunity to shape doctrinal design. There is a gap in consideration of where to conduct DA tasks as they apply to MDO concepts. No Army doctrine describes homeland defense. Execution of offensive tasks from the homeland will enable convergence in MDO. Future installation commands will leverage CONUS-based defensive tasks to deter or defeat an enemy systems offense, gain time, achieve economy of force, retain key terrain, and protect the population, critical assets, and infrastructure. Support to civil authorities will need to remain for law enforcement and disaster response activities, but the Army will need to adjust doctrine to defeat the adversary through the depth of competitive space, to include CONUS. The warfighters that train for and execute DA tasks reside on Army installations. They will be expected to be fluent in MDO, able to navigate every area in competition and armed conflict.

From a policy perspective, DHS is currently responsible for security, but they are not considering a peer adversary with the intent to destroy our warfighting system through a canvased application of their national power. The current design of homeland defense is reactive according to JP 3-27. The Army does not have any doctrine that describes homeland defense, only DSCA as a supporting effort in ADP 3-28. Current Homeland Defense and DHS strategies are to retain and protect sovereign space. Deterrence and defeat are missions and language that needs to be in CONUS-based operational Army doctrine. Equally crucial under the MDO concept is convergence in physical, virtual and cognitive spaces. Optimizing these authorities enable employment of cross-domain capabilities; cross-CONUS through OCONUS.

There is a seam between DHS and DOD regarding authorities within CONUS, only deconflicted by POTUS direction and SECDEF and DHS execution. DOD needs a more significant role in homeland defense in addition to missile defense, a reaction to an offensive threat. Cyber operations are a current, single-domain precedent for the DOD and the U.S. Army to conduct offensive and defensive tasks to protect national interests within CONUS. In the 2018 U.S. Army Cyber Command statement to the SASC Cyber-Security Subcommittee, Lieutenant General Paul Nakasone testified the conduct of Army Offensive and Defensive Cyber Operations as originating from CONUS. Currently, the Army can conduct offensive and defensive operations within CONUS in the cyber domain and without specific POTUS direction.

Army installations remain administrative instead of warfighting capable. A business-like efficiency is an output of the policy that DOD applies toward protection and resilience. The DOD applies an MA framework toward reporting protection, continued function, and resilience of capabilities and assets within DOD. Installation commanders, tenant unit commanders, and asset managers are responsible for protecting and ensuring the continued availability of personnel, equipment, facilities, networks, information, infrastructure, and supply chains.[317] The DOD MA Strategy consolidates service and GCC assessments of vulnerability to inform the CJCS Risk Assessment but requires local solutions when assessing the risk to essential warfighting tasks. Therefore, Army installations are reliant on their commanders to coordinate for partnership agreements with local governance, fire-EMS, and physical security,[318] instead of aligned command relationships with collocated operational units or allocated to the GCC.

There are striking similarities with the current Army's operating concept of ULO and the future MDO concept. ULO balances application of offense and defense, with stability OCONUS and DSCA CONUS. The ULO tenants of simultaneity, synchronization, depth, and flexibility are very similar in meaning and context to MDO's tenants of Calibrated Force Posture, Cross Domain Formations, and Convergence. The characteristics of DA are all relevant to the execution of ULO and MDO alike. DA characteristics such as concentration and a comprehensive approach enable the convergence of all DIME through JIIM partners. The homeland is no longer a sanctuary and GCC's need flexible options to defeat the PRC's systems destruction concept of future warfare throughout the depth of the MDO framework, both OCONUS and CONUS.

Recommendations

Installations will be vulnerable in the future due to a gap in doctrine. According to the 2018 NDS and earlier referenced comments by DHS Secretary Neilson, both the Department of Defense and Department of Homeland Security acknowledged the need to develop creative methods of winning a great power competition with our noted adversaries. As the land component to the national defense, the Army has a strong start with the MDO construct and framework that relies on a JIIM partner comprehensive approach and convergence. The Army will need to implement DA throughout the MDO framework to include the SSA where combat power generates from Army installations.[319] Diverging from the current structure, the future DHS, along with local and state law enforcement and emergency management agencies will need to be in a support role to DOD's MDO-enabled formations at Army installations. Homeland defense doctrine is needed for the future Army of 2035 to defend key terrain and project offensive attacks against near-peer threats from the SSA. This doctrine needs to nest with an updated 3-0 series of operational doctrine to expand offensive, defensive and stability task ratios in CONUS and establish the MDO framework. Additionally, ADP 3-90 and 3-07 series manuals will need homeland applications of offensive, defensive and stability tenants, such as comprehensive, the whole of government concentration of resources enabling full use of DA tasks, such as strongpoint Army installations as part of an integrated and MDO.

Acknowledging a need for conceptual refinement to MDO and future doctrinal change enable the conduct of CONUS Army installation-based offensive, defensive and stability operations. The MDO concept relies on convergence. The CONUS installation is a source of capabilities, whether force generation and power projection or strategic support. These capabilities need a deliberate defensive effort, as does the installations that prepare, prosecute and enable them. DOD's role in convergence to be the supported department for homeland defense will change the apex doctrine of JP 3-27, *Homeland Defense*. This joint doctrine will inform a future Army *Homeland Defense* with the logical title of ADP 3-27 series of manuals. In 2035, the ADP 3-0, *Operations*, series will continue to execute DA, but now in support of MDO, through offensive, defensive and stability tasks either CONUS or Outside CONUS (OCONUS), further described in an amended

ADP 3-90, *Offense, and Defense* manual series. ADP 3-07, *Stability*, series of manuals changes remove the locality restriction and incorporates a commander constraint of the supported agency to enable stability operations within a contested CONUS requiring constant competition. DSCA remains an option for the Army as a supporting agency if not in conjunction with any MDO tenants.

In 2035, an integrated installation area defense in the Army's DA framework deters adversary offensive action in this competitive space while protecting the population, critical assets, and infrastructure. Installations currently deter threats through force protection measures and MA risk monitoring protocols. They are also geographically separate, providing depth of capabilities. The establishment of an area defense provides depth and hardening Army installation into strongpoints provide anchors to the U.S. to the homeland defensive effort. The area defense will necessitate a change in U.S. policy regarding authorities for DOD to respond to threats, specifically conducting warfighting tasks among the civilian population. DOD would maintain control of the operations and DHS; state and local law enforcement would support.

The current CONUS installation MA protocols will not be enough to compete, enable penetration, disintegration, and exploitation in 2035 and beyond because MDO is an operational concept; MDO is a precursor to warfighting doctrine for design and development purposes. In 2035 installations, as part of the SSA, will likely be attacked through multiple domains. The physical security and force protection regulations of today can transition to a deliberate, integrated defense already addressed in doctrine. IMCOM is not a fighting headquarters as it is designed and resourced to be an administrative caretaker, the maintenance of service capabilities and facility enterprise. IMCOM should be considered an operational unit headquarters (either merged the senior command or stand-alone) in 2035. It will replace the administrative role directed in Army regulations with integration and convergence necessary of decisive action MDO in future doctrine. In his article about installations in future wars, COL Pat Duggan concludes, “we must update our concepts of installations from being sanctuaries to being the first skirmish lines of future defense.”[320]

In conclusion, the Army doctrinal evolution will necessitate training, leadership, personnel, and facilities prioritization necessary to accomplish the homeland area defense. The tenets of offense, defense and stability will remain, but operational application and reach of these DA tasks will require expansion to include the CONUS vulnerabilities. Due to the contested nature of future Army installations, an area defense is necessary within the DA framework to deter and defeat adversary offensive action and protect the population, critical assets, and infrastructure in the SSA. An area defense and installation strongpoints to rapidly regain offensive initiative or stability task resiliency are potential methods of incorporating current doctrinal practice to a future threat environment from a land component force. The building blocks to this homeland defense in depth through all domains exist. Requirements are the senior level urgency, attention, and resources to enact change.

USING TECHNOLOGY TO IMPROVE SECURITY AND INSTALLATION FORCE PROTECTION

COL Steven Tabat, U.S. Army

In 2035, the United States will confront an increasing number of state and non-state actors with the will and capabilities to threaten targets within the homeland and U.S. citizens with the ultimate intention to coerce. Joint Operating Environment 2035[321]

This statement from the Joint Operating Environment 2035 explains that enemies of the United States will seek to target locations within the confines of the homeland. Adversaries will select targets that are emblematic and will induce high losses, particularly in terms of personnel, with the intent of preventing the US military from being able to respond and to influence the American public or political leaders from supporting military action.[322] This makes military installations enticing targets for terrorists and other groups. It is for these reasons that it is necessary for the Army to develop and integrate technology to improve access control, perimeter security, and force protection of critical facilities on military installations.

What this paper seeks to highlight is the current US strategic guidance on future threats and what technology and capabilities can be developed now to counter the actions of individuals or groups seeking to attack the United States homeland. In fact, the analysis indicates that there are many current capabilities that can be improved or developed now, to better prepare for the future. The paper concludes with recommendations for actions to begin laying the groundwork to incorporate new technology and capabilities into the force protection efforts at military installations worldwide.

Future Conditions

The 2018 National Security Strategy (NSS) states that the fundamental responsibility of the US Government is to protect the American people, the homeland and the American way of Life. The NSS adds that protection of critical infrastructure is a key element of protecting the homeland.[323] The NSS explains that the United States faces threats from a host of adversaries who seek to exploit vulnerabilities in the homeland that could potentially disrupt US military command and control capability.[324]

Supporting the NSS, the 2018 National Defense Strategy (NDS) declares that the United States homeland is no longer a sanctuary, and that US military forces will not enjoy the luxury of preparing for future conflicts in an environment that is safe, secure, and uncontested. Adversaries will seek to damage or destroy critical infrastructure, sow disinformation, create disruption, and slow or prevent U.S. military forces from responding to events around the world. Furthermore, the NDS asserts that the future will be characterized by accelerated technological advances that allows for increased access to new capabilities such as autonomous vehicles, robots, Artificial Intelligence (AI), advanced computing, and even biological weapons. Many of these emerging technologies are being developed in the commercial sector and are being used by both state and non-state actors to disrupt and degrade orderly and peaceful societies.[325]

The Joint Operating Environment (JOE) 2035 discusses warfare in the future and how adversaries will seek to do harm against the United States. Conflict in the future will be characterized by several new contexts. Most notable is the specific targeting of US territory and sovereignty by adversaries. Although the United States has been subject to spectacular attacks in the past (Pearl Harbor and the terrorist attacks on September 11, 2001), the future OE brings with it an increasing number of adversaries who have the ability and desire to conduct attacks in the homeland.[326] The theme across all three of these strategic documents is that there are adversaries who seek to attack targets in the homeland. The next step is identifying the adversaries, the actions they might take, and how the US military can counter or defend against such attacks.

The NSS, NDS, and the JOE all support the notion that the threats faced by the United States consist of a mix of state and non-state actors. Foreign countries such as China, Russia, Iran, and North Korea make up the group of nations that seek to counter U.S. actions and interests in the world. All three documents are consistent in saying that a direct, traditional military confrontation in the U.S. homeland is not likely to occur but that these traditional, state actors may seek to use smaller, specialized irregular forces or partner with non-traditional elements such as Violent Extremist Organizations or criminal elements to carry out spectacular attacks against the homeland.[327] The attackers will use everything from Weapons of Mass Destruction (WMD) that may include Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) or other easily procured, commercially produced weapons.[328] The challenge for the United States military is how to detect and prevent a terrorist from carrying out a devastating attack against critical infrastructure, specifically an attack against a military installation.

Technology

Advances in technology are occurring at a more rapid rate than ever before. Increasingly fast paced changes in the fields of Artificial Intelligence (AI), computing, robotics, and autonomous systems, are altering the security environment as the new technologies are more readily available to not only the U.S. and its allies, but to adversaries as well.[329] As technology continues to develop, access to new technology is emboldening enemies at all levels and will force the US to change how it approaches security for installations and critical facilities.

The importance of continuing to develop new capabilities cannot be understated. Secretary of Defense Mattis explained the importance of investing and developing new capabilities in the 2018 NDS. He said, "Without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people."[330] It is critical that research, development, and testing of AI enabled technology, and the infrastructure to support these new technologies, is conducted now so that the Army is better prepared for future threats.

This is further supported by the 2018 DOD Artificial Intelligence Strategy. The document specifies that the DOD seeks to improve security by developing AI technologies to execute tasks that usually requires a human to perform. The DOD AI strategy states:

AI is poised to transform every industry and is expected to impact every corner of the Department, spanning operations, training, sustainment, force protection, recruiting, healthcare, and many others. With the application of AI to defense, we have an opportunity to improve support for and protection of U.S. service members, safeguard our citizens, defend our allies and partners, and improve the affordability and speed of our operations.[331]

The strategy goes on to say that the DOD seeks to improve AI technology to not only protect the country and create efficiencies, but to lead in the development of AI on a global and widely applicable use.[332]

The field of robotics has seen significant growth in the past few years. It is not unheard of to see robotic devices in grocery stores that can answer questions for shoppers or even detect and clean up spills.[333] Entirely new sectors of industry that specialize in robotic devices have emerged to augment humans conducting a host of different on tasks. Unmanned autonomous or semi-autonomous vehicles can be integrated into a security plan to provide ground or air surveillance capability or conduct patrols covering large areas. Robots that are integrated into security plans that are outfitted with sensors or other devices that can collect and transmit data for analysis and allow humans to make better decisions and cover larger areas. Robots can also be used to scan large amounts of data or video feeds and look for changes or irregularities. This combination of man and machine offers opportunities to conduct more persistent, varied patrolling techniques, provide coverage in remote areas, conduct more thorough analysis and improve response times when an incident does occur.[334]

The robot is only part of the equation. The continued improvement and employment of sensors to collect and transmit data is another critical aspect that will improve security in the future. Sensors can provide images, video, motion detection, thermal imaging, navigation assistance, audio, and chemical detection or a host of other capabilities. Information is collected and transmitted to a location for observation or analysis with software or other AI enabled technology.

Sensors can be utilized in several different manners. A technique is to mount sensors on mobile platforms such as manned, autonomous, or semi-autonomous vehicles to cover large open spaces as a part of an area patrolling plan. Fixed or static position sensors are employed to provide constant surveillance of buildings, secure areas, high traffic areas, or remote areas that are isolated or difficult to get to. Fixed position sensors are also used to monitor air and water quality and can determine if toxins or pollutants are present.

The benefits of integrating technology into security efforts are evident. Robots can be used to more efficiently employ humans by allowing human security personnel to monitor multiple facilities or larger areas from a centralized location rather than putting people in multiple locations. Technology can also more effectively support and augment humans as robots and sensors are not limited by senses or environmental changes such as weather or daytime versus nighttime. Technology, sensors, and robots are limited only by the types of sensors that are in use. Use of technology essentially extends a human's ability to monitor and observe larger areas.[335]

Successful employment of new technology such as AI, robots and sensors are dependent on the ability to quickly process and analyze large amounts of data from a multitude of sources.[336] These sources are a wide range of various electronic devices that can connect to a network and transmit data to some type of AI enabled device, or devices, for analysis and use. This is the so called “Internet of Things” (IoT) that is quickly developing.[337]

In terms of being useful for installation security, data provided by the various systems and sensors must be processed quickly, requiring a network that is fast and capable enough of handling large volumes of data. This network must also be secure so that security personnel can control and communicate with robots and other devices that are in use without the threat of hacking or loss of control. This leads to the role of Fifth Generation or 5G technology.

In a 2018 Center for Strategic and International Studies (CSIS) report on 5G technology and its importance, author John Lewis writes that 5G technology is critical because it is designed to reliably transmit and receive massive quantities of data over a network that is faster than existing networks. Additionally, 5G networks will support more devices connecting to each other creating an entirely new and larger digital domain.[338]

Development of 5G technology and equipment is important as it provides improved speed and access for the number of sensors and devices required to provide information in the future security environment. A specific challenge regarding 5G is, as the DOD AI strategy points out, there are four major companies that are leading the development of 5G technology equipment and they are from China (Huawei, ZTE) and Europe (Nokia, Ericsson). This presents a security challenge for the United States and allied countries because two of the four major 5G companies are closely tied to a chief competitor (China).[339]

Access Control Points

Installation access control is the first physical line of defense to deterring and preventing terrorists, criminals, and possible insider threats from carrying out attacks directed against military installations. By denying access to individuals seeking to inflict damage or disruption on an installation, the Army can create a safer environment where units can focus on readiness and preparations necessary to deploy in support of national interests.

Installation access control is governed by Department of Defense Manual 5200.08, Volume 3, Physical Security Program: Access to DOD Installations. The manual establishes standards for access control, methods for verifying identity, and protocols for determining the fitness of individuals entering DoD installations and it establishes types of access to DoD installations (unescorted, trusted traveler, and escorted). Additionally, the manual directs that services field an electronic physical access control system to determine suitability for access to DoD installations.[340] This is the first step in attempting to field an automated system that can verify identification and suitability for access by referencing data in DoD personnel database systems. DoD installations that have not fielded automated systems depend on visual verification if identification by a human guard.

The Army's Automated Installation Entry (AIE) system satisfies the DoDM 5200.08 and is a good first step to using technology to assist installation force protection personnel in determining who should be granted access to Army installations. Installations without an

AIE system rely on humans at a gate to verify identification based on what is presented to them. The guard is limited to what they can remember when it comes to being able to know who should not be allowed access to an installation.

AIE is a Department of the Army, Office of the Provost Marshal General initiative to enhance screening of personnel who present a valid form of identification for personnel from all services, all components, retirees, family members, DOD employees, and contractors who have been issued DOD ID cards. AIE utilizes Joint Service information architecture and verifies identity through a variety of DOD systems and law enforcement databases at the federal, state, and local levels. It also allows for non-DoD ID card holders to register and AIE checks the names against various law enforcement data base systems. The intent of AIE is to determine suitability for access of an individual and possibly prevent criminals or terrorists from gaining access to military installations.[341]

AIE works when a person seeking entry to a military installation presents their identification for scanning. The identification card is scanned at a fixed kiosk at the Access Control Point or with a handheld scanner. The individual's information is checked in various personnel databases and law enforcement systems, most notably, the National Crime Information Center Interstate Identification Index (NCIC-III). This has proven to be effective. During calendar year 2018 (01 January to 31 December), the NCIC-III database was used to grant more than three million personnel access to Army installations. During that same period, NCIC-III was used to deny access to 34,756 individuals. Individuals were denied access because of some type of felony in their record. [342] Use of the AIE system potentially prevented more than 34,000 harmful or destructive acts from occurring.

There are weaknesses with the AIE system. The vulnerability with AIE is that if the person is not specifically listed in the various databases that are checked, then they would be granted entry. This is a vulnerability of the AIE system as insider threats can gain access to an installation with weapons or explosives in their vehicle unbeknownst to force protection personnel. This is where additional sensors and AI enabled technology can assist.

For installations of the future, the Army should research and develop additional systems to collect and analyze information on various aspects of the vehicle, the driver, and passengers. These systems would augment the AIE system as additional identity proofing of the individuals in the vehicle. The ACP of the future should employ sensors and cameras with automated license plate recognition technology. These would scan vehicle license plates and immediately compare that license plate to a motor vehicle registry database that contains law enforcement and motor vehicle registration information from all states and territories of the United States. This will assist force protection efforts in providing additional proof of identity by matching the driver of the vehicle to the vehicle registration. It also helps to rule out if the vehicle is listed as stolen or wanted.[343] Simultaneously, a system of cameras is capturing images of the vehicle as it enters the ACP lane and begins to search for images of the vehicle in a vehicle identification and information database. This database contains information on vehicles manufactured over the last 50 years and the AI enabled technology would scan the database to determine the make and model of the vehicle.[344] AI enabled technology allows for the rapid identification of the vehicle by make and model and by license plate registration.

As well as identifying the make, model, and registration of the vehicle, a series of sensors in the roadbed weigh the vehicle to determine if it is within an acceptable weight range. These weight scales can be placed in the roadbed prior to entering the ACP so that the vehicle can continue to move forward while the scales determine the weight even while the vehicle remains in motion. This dynamic weighing or Weight In-Motion (WIM) technology, can help to determine if the vehicle is carrying contraband, explosives, or other illicit cargo.[345] If a vehicle is determined to be outside of an acceptable weight range, ACPs of the future are equipped with improved vehicle scanning technology to scan all vehicles as they enter the ACP, effectively taking an x-ray of the vehicle to see where contraband, explosives, narcotics, or other illegal cargo may be hidden.[346]

Mounted throughout the ACP are a series of AI enabled cameras capable of adjusting to the type of vehicle that enters the ACP and taking images of the personnel in the vehicle for purposes of facial recognition identification. These images are used to verify the identity of all personnel in the vehicle by comparing the images against all federal, state, local, and international criminal databases. Although the driver may have presented a DOD issued Common Access Card (CAC), the facial recognition technology ensures that the driver is presenting an authentic, unaltered DOD CAC ID as a supplemental proof of identity to support the AIE system. Any passengers in the vehicle would also be verified and cleared for entry through facial recognition since, under DOD Trusted Traveler Access guidelines, personnel may be allowed access to installations if they are with an authorized DOD CAC ID holder.[347]

There is also an opportunity for the Army to employ sensors that can quickly and accurately detect Chemical, Biological, Radiological, Nuclear, and Explosive materials and place those at every ACP to assist in the force protection efforts of the installation. This is important to prevent these types of materials from being brought on to a military installation for use as a part of some type of attack. Many of these technologies already exist but they are independent in terms of not being part of a larger system of sensors that can provide information to a much larger network. The U.S. Army should explore ways to connect multiple sensors that complement the AIE system to provide additional assurances that the personnel being granted entry are not terrorists, criminals, or even an insider threat.

All of the sensors and data collection devices discussed in the aforementioned scenario are dependent on the development of AI. It is AI that will allow all of the various systems to share information and establish the identity of the individuals seeking entry. AI will help to determine the good (or bad) standing of the individuals, rule out the possibility of the individual's vehicle as a carrier of weapons, explosives, or other dangerous materials. These AI enabled systems provide information to the force protection personnel as to whether the person or persons seeking entry are safe to allow access. It is through a secure and reliable network that the information can be checked quickly in a multitude of information databases.

These improved technologies and capabilities will assist in deterring or preventing attacks by improving the screening of personnel seeking installation access, enhancing screening of vehicles for access, and providing enhanced security technology through the incorporation of robotics and autonomous systems.

Perimeter Security

Army installation cantonment areas are surrounded by a perimeter fence that is, in many cases, extremely long and remote as compared to the rest of the installation area. The sheer length of the fencing makes it a difficult prospect to secure, monitor, and maintain. Army Regulation 190-13, The Army Physical Security Program, identifies considerations for perimeter fencing and discusses lighting and the use of Intrusion Detection Systems (IDS) but specifies that IDS and other electronic security systems are not routine requirements for Army facilities or areas, but rather for assets when specifically prescribed in policy.[348]

Typical installation perimeter security consists of fencing, lighting, video cameras, monitors observed by human personnel, and random or planned patrols by force protection personnel.[349] Although there may be more advanced capabilities employed at certain locations, that information was not available.

Incorporation of technology into installation security efforts would enhance and increase the effectiveness of security force personnel. The addition of sensors that, when activated, can send a signal to the nearest light set to turn on. When the light set is activated, a camera is also activated to relay images of the area in question to security force personnel or to a robotic device that could search for changes or abnormalities. These sensors can also include thermal imaging and night vision capability that can be activated by an individual in a force protection operations center for random video surveillance on certain areas of the perimeter fence at various times throughout the day or night. The sensors could also be connected to autonomous systems.

The perimeter or area security plan includes the addition of Unmanned Aerial Vehicles (UAV) and autonomous wheeled vehicles that are located throughout the installation at docking or charging stations. When a sensor is activated to a potential intrusion, a signal is sent to the nearest UAV at rest in a docking station. The UAV is alerted and provided information as to what sensor was activated. The UAV then departs the docking station and proceeds to fly to the portion of the perimeter that may have a possible intruder. On board the UAV is a set of cameras that can relay images back to the force protection command center. Once the observation services of the UAV are no longer required, it can simply return to a docking station, recharge, and await its next mission.

In conjunction with the UAV, there are autonomous wheeled vehicles that can be alerted to respond to the area in question. These autonomous vehicles could be no larger than a current model all-terrain vehicle (ATV) and outfitted with cameras, communications equipment, Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) detection sensors, lights, and even a broadcast speaker that can transmit voice information from the force protection operations center personnel.[350]

When used in conjunction with the perimeter fence sensors, the autonomous ATV could respond to the same location as the UAV but would offer personnel in the force protection operations canter a ground perspective as to what may have activated the sensors. If the actual fence was breached, the autonomous ATVs could remain on site in an observation mode until a human element could respond and conduct any necessary repairs to the perimeter. As technology improves, there may be an opportunity to have repair equipment on board the autonomous ATV that could repair a breach in the fence. When the autonomous ATVs are not responding to potential perimeter security issues, the force protection operations personnel can assign a patrol route and have the autonomous ATV move about the installation while relaying footage of the patrol to the Force Protection Operations Center or the Directorate of Emergency Services. These patrols would also utilize their sensors to test the air and water around various parts of the installation to possibly detect the presence of any CBRNE materials.

Incorporation of autonomous vehicles provides better use of human resources by using the autonomous systems to patrol largely uninhabited or remote areas of an installation. This allows the human force protection personnel to spend the bulk of their time in the areas of an installation that are more populated and require more human interaction.

Facility Protection

Military installations have numerous facilities that are listed as critical assets or require higher levels of security or controlled access. As was previously mentioned, Army Regulation 190-13, The Army Physical Security Program, identifies considerations for facility protection. Just like the perimeter security section, typical facility security consists of fencing, lighting, video cameras, monitors observed by human personnel and patrols by force protection personnel.[351] If the facility meets certain requirements based on the mission that the facility supports, an Intrusion Detection System or electronic security system may be applicable.[352] Legacy IDS will require upgrades or be replaced completely to as improved systems are developed and fielded.

As discussed earlier, devices and sensors used for facility security are connected to through a reliable network and monitored with AI enabled technology (motion sensors, facial recognition). Facility security is enhanced by verifying if an individual is authorized to be in the area or facility. In this case, the technology would be used to more quickly determine if an individual is authorized to be in the facility by comparing the images with those of an authorized personnel database. If an individual is determined to be unauthorized, an alert can be sent to one of the previously discussed UAVs for additional surveillance. The alert would also transmit to a response center and force protection personnel can be alerted to further investigate. This saves time by only having personnel respond when necessary rather than conducting long, random security and inspection patrols.

Incorporation of sensors to identify unauthorized personnel can help to improve and control access to maintenance facilities, unit operations buildings, headquarters areas, and barracks. This type of technology can also assist connected force protection elements from seeing where attempts to gain access by unauthorized individuals occurred and respond to the location as a means of thwarting any additional attempts or potential attacks.

Recommended Actions

The Department of the Army should seek partnerships with private, commercial firms, and academia to research, develop, and employ new technologies to improve security and force protection. Partnerships can better enable innovation, research, adaptation, and development of new technologies by creating understanding and coordinating the efforts of the civilian and government sectors. This explains why the DOD AI Strategy directs and encourages the establishment of partnerships that are broad and varied and includes traditional industrial partners along with venture capital firms and smaller, start-up firms.[353] Additional opportunities include working with University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs) and Department of Defense Laboratories.

Another potential partnership area for the Army to explore is in the research and development of Fifth Generation (5G) technology. To encourage development and address security risks posed by the limited number of private firms involved in 5G equipment development, the Army and the DOD, should seek to enter into cooperative partnerships with American based telecommunications firms to create the needed equipment and network architecture to support 5G and beyond.

These partnerships can offer funding, laboratory space, testing facilities, or proving ground space to the companies so that they can design, install, experiment, and evaluate the technology. As a tradeoff for providing space and sharing costs, the Army would benefit from updated technology that is installed and prepared to receive the numerous hardware devices required to support the force protection schemes of the future. Partnerships such as these could benefit all parties by establishing creative space for design, testing, and reduced expenses. Partnerships could also lead to new facility designs with an ability to adjust and receive new and emerging technologies beyond 5G. There is an opportunity for the Army to explore the benefits of new and emerging computing techniques on improved data networks that can support the future technology and devices required for the various future force protection initiatives.

The improvement of installation networks and network capacity would be a major benefit for the Army in a partnership or service contract with private technology and communications companies. It is estimated that 70% to 90% of all information technology and voice network infrastructure at all Army installations, is at or near the end of its designed life cycle. This presents a significant vulnerability for security and the inability of the network to handle any new future technologies. Before any new capabilities can be added or tested, the network must be improved. It is estimated that it would take the Army until 2030 to replace all the network infrastructure at every installation if the traditional methods for network improvements were employed.[354] Partnerships with commercial firms could speed the pace of network upgrades as the Army could work with multiple partners to upgrade several installations simultaneously rather than simply doing the work internally and sequentially.

The Army should work with organizations like the Defense Innovation Unit (DIU) for assistance in establishing partnerships for research and development specific to 5G and other technologies associated with AI enabled force protection technologies. During the short time that the DIU has existed, it has awarded upwards of 100 contracts for the incorporation of prototype commercial technology into the military.[355] All partnerships or contracts would be subject to any existing network security requirements so there would be uniformity if multiple private firms were involved.

Specific to the integration of autonomous systems, the Army can work closely with the Defense Advanced Research Projects Agency (DARPA) to capitalize on their decades of experience in the development and testing of AI enabled technology and the research that has emerged through the AI Next initiative.[356] The AI Next initiative seeks to develop machines and computers that are robust and more like a partner to humans in the decision-making process. This would be helpful for the integration of robotics and autonomous vehicles as a part of installation force protection programs. Also, the Army can capitalize on the dedicated funding for research and development and the existing partnerships that DARPA has built over the years with industry and academia to rapidly develop prototypes for testing and faster production and fielding.[357]

Another recommendation is to create a formalized, consolidated, plan that establishes a coordinated effort to focus on the improvement of installation force protection across the DoD.[358] The DoD should provide formal guidance and directives that establishes a uniformed approach to installation force protection improvements. Doing so has the potential to reduce redundancy, lower costs, and create a unity of effort through a joint approach that would benefit the entire DoD. This formal plan could also extend to other governmental departments. It is likely that many of the enhancements that have been discussed previously can be applied to border security efforts and critical infrastructure protection. By creating close working relationships with other governmental departments, the potential exists to elevate the importance of National Security and National Defense initiatives across the Whole of Government and not limit the effort to the DoD.

In addition to departmental changes, technology improvements will likely require a review of existing access control and force protection policies. It is recommended that, as new technology is developed and tested, reviews of existing policies occur so that the policy can support the fielding of the newly developed technologies and capabilities.

Conclusions

The future operating environment is likely to be extremely volatile and fast paced, resembling very little of what the Army has faced in the past. Proliferation of new and emerging technologies, increased number of threats, higher reliance on terrorist tactics, cooperation between state and non-state actors, transnational criminal organizations, and insider threats are all things that may be used to strike a blow directed against the U.S. Army and the DoD. The Army can reduce vulnerabilities at installations by developing and employing technology that can quickly and reliably sort through the vast amounts of data available to deter and prevent attacks. These new technologies can be used not only to identify known terrorists and criminals, but to look inside of vehicles, identify the presence of CBRNE material, use AI enabled machines to reduce response times and to increase security coverage areas on military installations.

The future looks bleak, but there are numerous opportunities for the Army to improve and develop technologies to provide better security for military installations and other critical infrastructure. The U.S. Army should take all necessary steps to increase the security and provide a secure environment for military personnel to train, maintain, and prepare for operations in support of U.S. national interests. Installations of the future must have the networks, technologies, resourcing, partnerships, and any other needed requirements to prevent and deter potential attacks.

There is no guarantee that new technology will stop all attacks or deter all terrorists but the Army has a major responsibility to create as safe and secure an environment as possible so that units can focus on training, preparation, and readiness to support the promotion of U.S. national interests.

MULTI-DOMAIN OPERATIONS AND AIRFIELD SECURITY ON ARMY INSTALLATIONS IN THE FUTURE

LTC Jennifer Reynolds, U.S. Army

> An America that is safe, prosperous, and free at home is an America with the strength, confidence, and will to lead abroad. It is an America that can pre- serve peace, uphold liberty, and create enduring advantages for the American people.
>
> 2017 National Security Strategy[359]

As one of the tools of National Power, the Military must ensure readiness to answer the call whenever and wherever it may come. Until recently, the United States has been secure in the ability to train and operate within the Continental United States (CONUS). Deployments from CONUS have been without challenge from an adversary intent on disrupting or defeating the military while in and around installations. The 2018 National Defense Strategy states that "Challenges to the U.S. military advantage represent another shift in the global security environment. For decades the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Every domain is contested today—air, land, sea, space, and cyberspace."[360]

The concept of Multi-Domain Operations (MDO) and the assertion that the homeland is a contested environment in 2035 has exposed a need to shift how the Army addresses security in CONUS.[361] The environment is one of constant competition and the installation should be considered battlespace in need of an offensive and defensive plan. The Department of Defense can expect to face emerging and evolving challenges on Army Installations and specifically to airfields and airspace. These challenges require a shift in the way that the Army addresses the security of airfields, changes in infrastructure and modernization and procurement efforts, and a plan to communicate the need to adjust policy and or law to provide maneuver space.

This paper will explore airfields and airspace security as part of the security line of effort, the broader objective of improving installations in CONUS by 2035. Challenges and gaps exposed by the MDO concept rest in the ability to properly secure airspace, airfields, and assets. Addressing these challenges can be accomplished by increased security of airfields and airspace; Installation and infrastructure development and airfield modernization; and improved and targeted communication strategies with both the Executive and Legislative branches to address funding, law and policies.

Increasing Security of Airfields and Airspace

Multi-Domain Operations specifies that adversaries will threaten the United States in all domains and that the homeland can no longer be considered a safe haven. This operating concept produces a need to view airfields and the airspace above them as contested, which requires a potentially controversial and adversarial shift to how assets are employed in the future.

A critical aspect of security is the airspace above and around installations. At present, airspace is observed by Air Traffic Controllers (ATC), who monitor and provide direction to aircraft in transit through and around controlled airspace. Controlled airspace, as defined by the Federal Aviation Administration (FAA) is airspace that provides "sufficient airspace for the safe control and separation of aircraft."[362] Other than verbal commands, the FAA and ATC have no way to counteract a threat from the air. Airspace is another avenue from which to be attacked. As a result, the airspace above and around installations ought to be considered in the same way as physical security on the ground when establishing a security plan.

The rules and regulations that govern national airspace are determined by the FAA for commercial, private and military aircraft which include fixed wing, rotary wing, and Unmanned Aerial Vehicles. There are already regulations in place to ensure that pilots, to include commercial, private, and military understand where aircraft and UAVs may fly. There are varying types with a wide range of restrictions. However, the primary type that relates to military airspace is Special Use. Special Use Airspace is defined by the FAA as "Special use airspace or special area of operation (SAO) is the designation for airspace in which certain activities must be confined, or where limitations may be imposed on aircraft operations that are not part of those activities."[363] Special Use airspace includes Military Operation Areas (MOAs), Prohibited areas, Warning areas, Alert areas, and Controlled Firing Areas (CFAs).[364] Airspace rules and regulations will not prevent an adversary, who has no vested interest in following them, from attempting to disrupt or cause harm in and around Installations.

UAVs, in particular, have drastically increased in numbers and are easy to procure. The FAA estimates that “the commercial drone fleet would grow from 42,000 at the end of 2016 to about 442,000 aircraft by 2021”[365] The proliferation of unmanned aerial vehicles (UAV) in hostile and disruptive operations means that taking advantage of emerging innovation is critical. The recent examples of commercially procured UAVs causing the London Gatwick airport to close for over eight hours, as well as the attempt to assassinate the President of Venezuela (Maduro) with UAVs demonstrate the real and immediate threat and the ease with which UAVs are employed by individuals.[366] The ability to counter the UAV or other airborne threats can be addressed through the use of emerging technologies and can enhance the ability to protect airspace and as a result, installations.

Capitalizing on relationships and proven technology is a way to increase speed as well as potentially save money spent on development and testing. Hostile and disruptive operations mean that taking advantage of emerging innovation is critical. Equipment to counter airborne threats, should be considered. A properly planned and resourced airspace protection plan could provide valuable standoff and time to react, as well as generate information to those responsible for making decisions.

The Pentagon is actively pursuing software to counter UAVs from an airspace security company called Dedrone.[367] The software is declared to be able to detect antagonistic UAVs and, according to claims made by the company, can be incorporated with frequency sensors, cameras, and microphones. Proven systems in use by allies will enhance and supplement technology which emerges from the U.S. The Israeli

Army possesses an advanced counter drone system known as the “Rafael Advanced Defense Systems Drone Dome counter-drone solution (RADA).” These systems, also supplied to the United Kingdom (UK) Army, enable surveillance over 360-degrees “and detects drones at distances of 3-5 kilometers. The signals intelligence system along with electro-optical sensors, provide additional layers of threat classification and identification, while RF (Radio Frequency) jamming provides additional protection.”[368] Incorporating technology already used by allies, with U.S. technology can only assist in the attempt to stay ahead of the rapid proliferation of UAVs and provide additional layers of security.

The U.S. is already capitalizing on relationships and the use of proven technology. A bill titled, “United States-Israel Joint Drone Detection Cooperation Act,” [369] passed in both the Senate and the House of Representatives in July of 2018. Expansion of the Act is addressed in the John S. McCain National Defense Authorization Act for Fiscal Year (FY) 2019.[370] The NDAA was signed into law on 13 August 2018 and included a section that addresses cooperation between the U.S. and Israel in countering UAVs. Hostile and disruptive operations predicted by the Joint operating Environment (JOE) 2035 means that taking advantage of emerging innovation and partnerships is critical. A properly planned and resourced airfield and airspace protection plan provides valuable standoff and time to react.

A proactive rather than reactive stance is key to deterrence and protection. Preparations made on the installation, before an attack, are critical to providing rapid response time and the ability to shift from defense to offense. This includes the focused analysis of the use of airspace and airfields and how to increase security for the installation and by extension, the surrounding communities. To better safeguard the homeland, one method to defend installations would be to conduct defense in depth as well as the ability to transition to immediate offensive operations. The ability to shift focus based on an established plan will increase the chance of preserving the ability for installations to protect personnel and assets as well as remain a viable Power Projection Platform for Outside Continental United States (OCONUS) operations.

A different way of thinking about airfields and the airspace needs to evolve to mirror that of operations along a full spectrum from competition to conflict. MDO and JOE 2035 both assert that the future will be a range of operations from competition to conflict. The ability to react in a timely manner rests on a cohesive, well established, and rehearsed plan to transition from one end to the other along that spectrum.

Installation and Infrastructure Development and Airfield Modernization

Infrastructure investment and development is another aspect of enhancing the security of Army Installations. The Department of Defense's (DoD) priorities have been focused on a counterinsurgency fight rather than against a peer or near-peer adversary intent on challenging the United States in every domain. An assertion made by Gen. Mark Milley, the Army's Chief of Staff (CSA), was that "adversaries including Russia, China, Iran, and North Korea have spent nearly two decades studying the U.S. military's strengths and vulnerabilities as it has fought terrorist groups. Those nations have invested in modernizing their forces and preparing them to exploit vulnerabilities developed while the United States focused on fighting insurgents."[371] As a result, the CSA established six priorities to target for modernization.[372] However, installations, which have been lagging in development, are the foundation that is key to the successful protection and employment of those priorities, are the.

Military personnel and the surrounding communities have been reasonably assured a safe haven on installations in CONUS. For almost two centuries, the tyranny of distance, geography, and separation by two large oceans has provided a standoff distance which has kept U.S. installations relatively free from attack.[373] One exception was the attack on deploying Soldiers at Fort Hood, Texas by MAJ Nadal Hasan, a radicalized soldier.[374] The rule, rather than the few exceptions, has resulted in underfunding and limited focus on the security of installations and safeguarding of assets in the Continental United States (CONUS).

In conjunction with a well-planned modernization strategy, the Army must develop, procure, and implement methods to ensure the survivability of assets, infrastructure, and personnel in CONUS and specifically airfields and aircraft. Ensuring that airfields and hangars become hardened against severe weather, cyber-attacks, electromagnetic and hypersonic weapons, or the more conventional missiles and rockets needs to be a priority. The U.S. Army War College's Defense Management Primer highlights that "defense management is less about the details of personnel, equipment, and facilities and more about what the overall force can do now (capabilities), how much it can do (capacity), and what it needs to do that it cannot (requirements).[375] In order to protect assets from known current threats, both kinetic as well as severe weather impacts, the defense acquisition process cannot lose sight of the need to address challenges faced on installations. At the moment, the force cannot provide adequate protection against known kinetic (missiles, rockets, and the like) or severe weather let alone the threat faced by emerging technologies. Technology requires constant evaluation and addressed as they evolve to maintain a competitive edge.

The current effects of severe weather, such as tornadoes, hurricanes, and high winds, cause units to lose critical training time as well as the ability to react to threats should they emerge. Severe weather causes aviation units to push as many assets as possible into hangars, while the remaining aircraft are flown to distant locations until it is deemed safe to return. Hurricane Michael, which made landfall on 10 October 2018 caused severe devastation to Tyndall Air Force Base. "With billions of dollars of assets in harm's way and more weather extremes on the horizon, making and enacting disaster plans are becoming all the more critical for the military."[376] The modernization of hangars could contain features that allow assets to shift from above to below ground, similar to the method an aircraft carrier uses to clear the deck.[377] This is one way to provide protection from damage from the environment or antagonists and would enhance the survivability of personnel and equipment against a wide range of threats. Innovation and modernization of airfields and hangars also needs to take the effects of climate change into account.

The effects of severe weather cannot be understated. Studies published by the National Aerospace and Space Administration (NASA) point to scientific evidence that climate change will continue, and that effects will be felt with changes to weather patterns as time progresses. The Intergovernmental Panel on

Climate Change has asserted that "Taken as a whole, the range of published evidence indicates that the net damage costs of climate change are likely to be significant and to increase over time."[378] Underscoring this assertion is testimony recorded by the current Army Assistant Secretary, Alex Beehler during his hearing for confirmation by the Senate. Secretary Beehler commented that "I will do everything to encourage installations and help direct installations to properly prepare on a case by case basis for both adverse weather and effects long-term from climate."[379]

The acquisition of modern and more advanced infrastructure, which enhances the protection of high-value assets against severe weather, conventional and unconventional threats, will ensure that critical assets can be maintained for training and readiness as well as immediate employment when needed. The ability to mobilize rapidly should the need for offensive operations arise provides flexibility for the commander in a time of crisis. Ignoring the modernization of installations could cause a significant loss to assets that cost the taxpayers billions of dollars as well as the amount of time and money it would take to get those assets back into operation.

Policy Changes

Policy and law should be re-evaluated using the lens of MDO. A concept based on future threats can pose complications to long-standing law and policy. A challenge in addressing the possibility that installations in CONUS may have to conduct both offensive and defensive operations, is a law that has stood since 1878. The Posse Comitatus Act, Section 1385 of Title 18, United States Code (USC) prohibits active duty forces (Title 10) from direct military involvement in law enforcement.[380] Homeland Security is charged with safeguarding the American people, the homeland, and our values.[381] With only 240,000 employees, they are undermanned and underequipped to face a conventional threat without assistance from the military. Partnerships between local, state and federal law enforcement are critical as well as the continued improvement of training between all Army components. Further coordination of and refinement of title 10 and title 32 troop use in the case of a transition from defensive to offensive operations must be carefully considered and re-worked to ensure the ability to rapidly respond to threats.

Interoperability challenges between the Army and civilian and law enforcement partners must be addressed as communication and coordination play a critical role in response to both environmental as well as antagonistic threats. The ability to provide defense in depth as well as the capacity to rapidly shift from defense to offense will require law and or policy changes as well as partnerships with Title 32 or law enforcement to be re-looked. Without express authorization by an Act of Congress or a change in the Constitution, the military faces several hurdles in the protection of Installations.

To stay proactive and maintain a competitive edge, the Army must take a serious look at a shift in policies that could currently hinder installation's abilities to defend itself. Once such policy is DoD Directive 3000.09, Autonomy in Weapon Systems." There are stringent guidelines that could prove too restrictive in the event of a threat. The directive states, "Human-supervised autonomous weapon systems may be used to select and engage targets, with the exception of selecting humans as targets, for local defense to intercept attempted time-critical or saturation attacks for: (a) Static defense of manned installations."[382] This policy provides the ability to meet a threat but requires a human in the decision cycle which could cause costly delays. Artificial Intelligence is capable of making decisions more rapidly than a human and can have the added benefit of allowing a commander to conduct overwatch over a broader range of threats and unfolding events.

Another policy that could cause a costly delay is one that dictates where and how ammunition is stored and maintained on Army Installations. Department of the Army Pamphlet (DA PAM) 700-16 restricts how close ammunition can be placed to aircraft or airfields. The current policy places such severe restrictions on separation distances that a rapid response to immediate threats to the installation is impossible. The current ammunition storage rules are peace-time focused and do not consider that CONUS installations are now part of the battlefield. Adjustments could be made ranging from establishing Ammunition Holding Areas (AHA) adjacent to helicopters or Unmanned Aerial Vehicles (UAVs) on the flight line, to establishing a rapid ammunition deployment force in order to comply with ammunition handling and transport requirements. Without a shift in policy or a method to rapidly distribute ammunition, installations could lose critical time to respond to threats. The loss of essential reaction time in responding could mean a loss of life, assets and the ability to act as a Power Projection Platform (PPP).

Communication with Lawmakers

It is of vital interest to the United States' status as a world power to ensure that installations remain as uncontested and secure as possible in the volatile, uncertain, ambiguous and complex (VUCA) environment in which we operate. Appreciation for the tensions between desired modernization requirements for the Army, and requirements both made, and faced by the Congress, is critical in developing an approach to gain support from the legislative branch.[383] Senior leaders must employ a comprehensive, well planned and focused communications strategy in order to move forward and ensure that the United States can maintain dominance in any operation conducted OCONUS due to assured resiliency and protection of assets in CONUS.

Strategic guidance in the form of the National Security Strategy (NSS), National Defense Strategy (NDS), and MDO assert that it is a necessity to modernize. Senior Leaders must convince Congress, and specifically appropriators, to spend money on infrastructure modernization. It is imperative that the development of a communication strategy is resourced and conducted in the same manner as a campaign plan for major offensive operations. Challenges in achieving bi-partisan consensus will likely impact the development of laws regarding reform, governance, or investment in infrastructure and procedures that that are required. The Army can actively shape policy discussion through active and pre-emptive communication, with focused, objective and plausible recommendations.

As stated in the 2018 NDS, “This increasingly complex security environment is defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest continuous stretch of armed conflict in our Nation’s history. In this environment, there can be no complacency—we must make difficult choices and prioritize what is most important to field a lethal, resilient, and rapidly adapting Joint Force."[384] The time for increased cooperation between the Military and its Civilian leaders is now, reaction to an attack, as outlined in the MDO and by the Secretary of Defense, will be too late and will have grievous consequences to the Nation's survival. Without an aggressive shift in policy, law, and the conduct of operations and modernization, the homeland will be ill-prepared to answer the threats that will be faced in the future.

Conclusion

It is critical that the Department of the Army and DoD challenge the status quo and develop ways to capitalize emerging technology and leverage partnerships at a joint and interagency level to ensure a wide range of coverage and ability to react to threats that have been forecasted in strategic guidance and the MDO concept. The assertion presented by the MDO, that CONUS is no longer a sanctuary, increases the need to protect assets that enable training, equipping and deployment. All of which allow the Nation to project power across the globe. As The U.S. Army Futures Command (AFC) moves to full operational capability, continued partnership between AFC, The U.S. Army Installation Command (IMCOM), U.S. Army Material Command (AMC) and the private sector should be actively pursued regarding the development and acquisition of technology investments that can rapidly address closing capability gaps.

The Chief of Staff of the Army established readiness as the Army's first priority.[385] The ability to provide assets, both people and equipment, prepare for the transition from peace to conflict and protect the Nation is vital. "You can only deter your opponent if your opponent believes that you have the will and the capability," stated GEN Milley. "So, readiness has a deterrent value as well as a war-fighting value."[386] Through investment in emerging technologies such as Artificial Intelligence (AI), advanced robotics, unmanned vehicles, sensors which feed information to a hub and enable decisions, advances in computing and other promising equipment, the Department of the Army and Department of Defense can better ensure the protection of the homeland as well as the ability to project power. Should the Army fail to invest, then the ability to defend installations against a multitude of threats, project power to secure and defend the homeland and our allies, provide less of a deterrent and be unable to provide the other instruments of National Power the strength of the military to enhance and bolster positions. The system at large must evolve to secure the necessary funding and resources to produce solutions, and that will provide greater protection for the Army's assets. "The Department of Defense's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation. Should deterrence fail, the Joint Force is prepared to win. Reinforcing America's traditional tools of diplomacy, the Department provides military options to ensure the President and our diplomats negotiate from a position of strength."[387]

Section Four:
ENABLING CAPABILITIES

INSTALLATIONS OF THE FUTURE AND DIGITAL GOVERNANCE

LTC Brian Jorgenson, U.S. Army

"To maintain our competitive advantage, the United States will prioritize emerging technologies critical to economic growth and security, such as data science, encryption, autonomous technologies…advance computing technologies, and artificial intelligence."

- National Security Strategy[388]

Advances in technology have enabled an explosion of information and data that may quickly overwhelm human cognitive abilities in the future environment. Technology enables innovation, but these advances also introduce threats from our adversaries. As the National Security Strategy states, "Risks to U.S. national security will grow as competitors integrate information derived from personal and commercial sources with intelligence collection and data analytic capabilities based on artificial intelligence and machine learning."[389] The increased reliance on technology coupled with the associated threat that emanates from its use, requires a change in how one thinks about the balance of delivering services while simultaneously providing security. This is especially important for the U.S. Army as it modernizes installations with a focus on how installations of the future support the Army across the three lines of effort of: "Support the Army as it Prepare for War, Prosecution of War, and Provide Enabling Capabilities."[390] The U.S. Army needs to consider a digital government model for public administration as a concept to employ the emerging technologies directed in the National Security Strategy and the National Defense Strategy to improve efficiency and decision making at installations. One must understand the historical use of technology in public administration to gain insight into the creation of a digital government model.

The use of technology in public administration did not start with the development of the digital government model. Technology has always played a part of how society governs itself. Previous public administration models, such as the 'New Public' management model of the 1980s relied on technology, but only in a secondary role focused on productivity and spreading information.[391] In 2010, Techno enthusiast, Tim O'Reilly first described a digital model for government administration as "Government 2.0" where the use of digital technology was to improve and innovate the functions of government.[392] The shift to a digital government model originated through several causes: the rise of the Internet, the interconnectivity of society via digital means, the electronic transfer of services, the development and sharing of open source code, and the idea of open data.[393] The ability for someone to use, update, or improve upon another application's source code combined with open shareable data created what Tim O'Reilly describes as an environment, "…of creativity and collaboration to address challenges facing our country and the world."[394] Tim O'Reilly's idea of improvement is found at the core of the model.

The digital government model is a cognitive method for incorporating technology into the day-to-day operation of public administration. Tim O'Reilly states that the model, "…is not a new kind of government;

it is government…rediscovered and reimagined…”[395] This renaissance leverages digital technology to innovate. The digital government model follows three main principles: the pursuit of a seamless cooperative digital world; the preservation of open data and citizen’s rights; and the improvement of public administration decision making.[396] Based on these principles, the digital government model concentrates on four main activities: design new administrative functions that reduce cost, eliminate duplicative processes, and build efficiency; implement a service delivery activity that focuses on the customer point of view, employs integrated tools, leverages big data, and increases the operational flexibility to respond to and solve issues in real-time; the digitalization of government by increasing the access to administration resources; and maintaining an ethical approach to accumulating, warehousing, and using big data.[397] Improving government through technology is the overall aim of the model. Tim O’Reilly described the model as, “…the use of technology, especially the collaborative technologies…to better solve collective problems at a city, state, national, and international level.”[398] The use of digital government model is not just about accepting and implementing technological advances, but increasing ‘digital openness’ in the day-to-day operation with the goal of becoming a collaborative partner with the society that receives services from the government.[399] In this model, society is not only a consumer, but also a producer of information that is capable of providing near instantaneous feedback to the government. Cities around the U.S. and the world have applied aspects of the digital government model toward daily operations including the cities of Cleveland, Los Angeles, San Antonio, Pittsburgh, and Singapore. The following examples below offer insight into the possibilities of applying features of the digital government model to improve public administration.

Digital Government Model Examples

The digital government model may improve the public administration and the day-to-day operation of cities through the application of artificial intelligence. Artificial intelligence projects that leverage big data have the potential to generate innovation in a diverse range of fields.[400] This includes improvements in the areas of healthcare, customer service, traffic control, and fire inspections. The following examples highlight advances in efficiency and decision making that cities achieved using a digital government model.

Healthcare

The Cleveland Clinic, a non-profit academic medical and research center, is looking at artificial intelligence to create efficiencies and improve patient care. In their recent *Medical Innovation for 2019* report, the clinic stated, "…artificial intelligence is helping physicians make smarter decisions at the point of care, taking the hassle and uncertainty out of view patient scans…" and that "…machine learning algorithms have the ability to highlight problem areas on images, aiding in the screening process."[401] These advances improved the effectiveness of care and the competence in the decisions doctors made.

Customer Service

The Singaporean Information Communications Development Authority implemented a customer service chatbot for use across the city-state's different agencies' websites. *Ask Jamie*, the virtual assistant, would generate a pop-up window whenever a user visited an agency website, ask if the user had any questions, reply to any user request with the requested information or even ask clarifying questions if the request was too general, and transfer the conversation to a human customer service representative if the artificial intelligence algorithm could not find an answer.[402] This innovation improved the efficiency and timeliness of the customer service request system for Singaporean government agencies.

Automated Traffic Control

The safe and efficient movement of people and commerce along municipal roads is a complex endeavor. Kevin McCaney argues, in *GovernmentCIO Media*, that driving in city traffic is not about the distance, but about the time required and that, "adaptive signal control, applied in Los Angeles, San Antonio, Pittsburgh, and some other cities, used real-time data to change the timing on traffic lights to adjust to the flow of traffic."[403] Applying artificial intelligence to improve the efficiency of city traffic is a potential way to reduce the complexity of moving people and goods on the same infrastructure.

Fire Inspections

The city of Pittsburgh, Pennsylvania in partnership with Carnegie Mellon University's Metro21 Smart Cities Institute developed an artificial intelligence project in 2018. The completed project, "…use[d] fire incident and property data to develop predictive model of structure fire risk…[to] prioritize [Fire Marshall] property inspections with data-driven insights from the fire risk analyses from machine learning models…in order to target their inspections at the properties at [the] greatest risk of fire."[404] Implementing sensors and an artificial intelligence machine learning system provided huge benefits for the city of Pittsburgh through the prioritization of limited manpower to complete the inspections.

These projects may not have received the support required to achieve success if it were not for adoption of the principles and the features of the digital government model in each of the respective cities. U.S. Army installations are population centers that deliver public services like those found in small cities.[405] The U.S. Army can learn from the experiences of these cities. As the recent Department of Defense *Artificial Intelligence Strategy* stated, "We must learn from others to help us achieve the fullest understanding of the potential of artificial intelligence…"[406] Other than the Department of Defense direction to study and adapt innovative technology into everyday use, why should the U.S. Army consider a digital government model for the use at installations?

George Box's famous quote, "…All models are wrong, but some are useful," aptly explains why one relies on a model; to extract information of interest from data.[407] Adopting the digital government model for public administration at U.S. Army installations has the potential to generate improvements in the efficiency of operations and in decision making. First, installations have the potential for improvements by applying the digital government model's first key task; reducing cost, eliminating duplicative processes, and building efficiency. The day-to-day mission of U.S. Army installations, as described by the Installation Management Command (IMCOM) Annual Command Guidance, is to, "…integrate and deliver base support to enable readiness for a globally-responsive Army."[408] Installations are service providers, supporting the Army to build readiness. The Annual Command Guidance further describes that installations operate within established priorities based on "accessibility, affordability, quality, and sustainability."[409] Running an installation in a limited budget or a resource inhibited scenario requires an established priority system for delivering services.[410] One of the key features of the digital government model is the concept of generating efficiencies. The previous examples highlighted the successes of other cities that implemented aspects of the digital government model and improved their operational efficiency. U.S. Army installations could achieve similar efficiencies through the application of a digital government model. The conditions are similar in that installations of the future will continue to provide healthcare for soldiers, manage traffic on installation roads, and inspect facilities for potential fire risk.

The second potential improvement of implementing the digital government model at U.S. Army installations is enriched decision making. As described in the examples above, the increase in efficiency through sensor data has the potential to generate massive amounts of data and could quickly overcome human comprehension capabilities. This is where a digital government model utilizing machine learning processing make it possible to statistically analyze the data at a faster rate.[411] If decisions are based on the availability of relevant data, then the ability to access and process more data could ideally lead to better informed decisions. The recent Department of Defense Cyber Strategy directs leveraging automation and data analysis to improve effectiveness by, "…us[ing] cyber enterprise solutions to operate at machine speed…"[412] The rapid data analysis necessary for installation leaders to make decisions may not be fast enough for future threats; this may require advanced computing and artificial intelligence systems to assist. In 2018, the Congressional Research Service described the advantages of assistance from artificial intelligence systems as, “Artificial Intelligence systems may provide decision makers with the ability to quickly assimilate large volumes of data and suggest actions faster than current command and control tools…[this] would facilitate rapid reactions to an adversary, possibly outpacing the opponent’s ability to understand the environment and respond in kind if the opponent is relying solely on human judgment.”[413] The capability to assist installation leaders make decision through analysis of large data sets can be achieved through a data driven culture that operates using the digital government model.

In addition to efficiency and decision making, applying the digital government model to U.S. Army installations may provide a method for interacting with a new generation of techno-focused soldiers. Integrating technology into all aspects of an installation could be a recruiting and retention tool. Availability, access, and familiarity with technology could be a consideration for future soldiers as evidenced by the purpose of the U.S. Army Recruiting Command’s recent creation of an Army E-Sports team, “…we need to be where young people are and they are operating in the digital world.”[414] Additionally, in a 2018 Department of the Army survey, first-term Soldiers expressed their desire, “…to use apps to bypass bureaucracy, and directly access a service to support their readiness.”[415] These examples are just a few of the potential improvements of considering the digital government model for use on U.S. Army installations. However, achieving these improvements might come at a cost or at least an acceptance of a trade-off as the Defense Cyber Strategy highlighted, “The arrival of the cyber era has created new opportunities and challenges…”[416]

Application of the digital government model has the potential for improvements, but also it also introduces challenges for the U.S. Army. As described earlier, the digital government model focuses on increasing digital openness and collaboration. Tension exists between the model's idea of openness and the U.S. Army's need for security. Army Regulation 380-5 directs the protection of national security information both classified and sensitive but unclassified from unauthorized disclosure.[417] Data security is a national priority as stated in the National Security Strategy, "The United States will expand our focus beyond protecting networks to protecting the data on those networks so that it remains secure both at rest and in transit."[418] Academic literature for the digital government model does not establish a relationship between digital openness and collaboration with building efficiency and improved decision making. They are both aspects of the model, but one does not rely on the other.[419] This tension highlights an area that requires further analysis to study the implications of digital openness and data security when applying a digital government model to U.S. Army installations.

The epigraph of this paper highlights the National Security Strategy's emphasis on emerging technologies. Artificial intelligence, machine learning, and other advances have the potential to improve both efficiency and decision making. Information and data from interconnected devices are likely to increase in the future. As innovation advocate Tom Ark stated in early 2018, "There will be 50 billion devices connected [to the Internet] by 2020 including a billion cameras, all feeding data to artificial intelligence platforms."[420] The recent U.S. Army publication, *The U.S. Army in Multi-Domain Operations 2028*, illustrates a way to leverage technology to counter this increase in data as, "Man-machine interfaces enabled by artificial intelligence and high-speed data processing, improve human decision making in both speed and accuracy."[421] U.S. adversaries are likely to leverage these technological advances too. In the 2019 *Worldwide Threat Assessment of the U.S. Intelligence Community*, the Director of National Intelligence, Daniel Coats, described the threat environment as, "The global race to develop artificial intelligence, systems that imitate aspects of human cognition, is likely to accelerate the development of highly capable, application-specific artificial intelligence systems with national security implications… presenting the world with a host of economic, military, ethical, and privacy challenges."[422] Advanced technologies have the potential to improve operational efficiency and decision making which can improve one's competitive advantage. The U.S. Army can leverage this competitive advantage across the Installations of the Future Campaign Plan to ensure installations are ready for the future fight.

The U.S. Army Installations of the Future Campaign Plan includes three lines of effort: "Support the Army as it Prepare for War, Prosecution of War, and Provide Enabling Capabilities."[423] Assessing how the digital government model will function within each line of effort provides insight into the usefulness of the model. The identified outcome of the first line of effort, Prepare for War, is, "[To] provide world class training, maintenance and industrial base facilities."[424] The digital government model has the potential to support this outcome in two ways: Improving the efficiency of U.S. Army operated facilities and establishing a robust network of people and sensors. The prioritization of services is the key to building efficiency. In a fiscally constrained environment, an installation cannot fund all the facility requirements. Knowing where or how to prioritize services requires a succinct method to ensure that the higher precedence actions occur first.[425] The digital government model and its focus on technology can provide a guide for this prioritization. The analysis and correlation of vast amounts of this data can build predictive trends that feed efficiency. Capturing accurate data requires an immense network of sensors and people trained to operate and interpret the sensor data. The digital government model relies on individuals trained on all aspects of data. These 'Data Scientists' understand where to capture data, how to secure it, how to interpret it, and most importantly how to use it to gain efficiency and improvements. As Lieutenant General Kenneth Dahl, the previous commander of IMCOM stated, "[An installation's] ability to prioritize resources towards key installation readiness drivers is critical to the Army's success in mobilization, training, deployment, and combat operations."[426]

The Prosecution of War, the second line of effort for the Installations of the Future Campaign Plan has the outcome of, "Protecting, projecting, and sustaining combat power formations, enabling cyber warfare assets, and delivering state-of-the-art strategic command and control infrastructure."[427] The digital government model will operate in a similar fashion as the first line of effort, Prepare for War. The model improves efficiency through an enhanced decision-making capability, which the U.S. Army's multi-domain operations publication states is necessary to counter the strategic ambiguity created by competition with near-peer advisories.[428] As described above big data and artificial intelligence systems offer the potential to increase the amount of information analyzed and considered before deciding on a plan of action. This may also reduce the time required to decide; a critical skill as functions become more automated. Identifying, mitigating, and resolving cyber threats with artificial intelligence systems may reduce the impact on installations of the future vice relying on human processes. The National Defense Strategy identifies some of the technological advances required to compete and win future conflicts as, "advanced computing, big data analytics, artificial intelligence, autonomy, and robotics."[429] These advances will provide the U.S. Army with the advantage and overmatch required to win future battles. This will become especially important as installations of the future become part of the battle space. Initial contact with the enemy may begin at the installation and force combat units to fight their way from the installation to projecting power to a forward location. Improving situational awareness and decision making could be a combat multiplier as the Department of Defense *Artificial Intelligence Strategy* highlights, "Artificial Intelligence can generate and help commanders explore new options so that they can select courses of action that best achieve mission outcomes, minimizing risks to both deployed forces and civilians."[430] The digital government model provides a means for incorporating technology into the operation of the installation not only for day-to-day operations, but also for combat related tasks. Project Maven is a recent example of the Department of Defense's inclusion of emerging technology to assist deployed forces. Project Maven is a machine learning algorithm that receives, processes, and interprets drone footage looking for weapons and other threats at a faster rate than a human operator.[431] The prosecution of war is a critical task for installations of the future, however the fundamental purpose of installations remains providing services.

Provide Enabling Capabilities is the third line of effort in the U.S. Army's installations of the future campaign plan. The outcome of this line of effort is, "[To] provide Soldier protection; sustain resilient installation management and service delivery; and care for Soldiers, civilians, and families."[432] The digital government model operates within this line of effort in three ways: through an increased efficiency of service delivery, an improved process of feedback, and enhanced predictive analysis. First, focusing information technology into existing and new operating procedures takes advantage of the advances in automated processes which lead to efficiencies. The collection of data alone does not achieve efficiencies, the improvements come through the combination of data, analysis, and the capability to put context to the resulting information.[433] Then applying the resulting knowledge to improve an existing function. Second, feedback is a process to determine whether a decision or action achieved the desired result. In the digital government model, feedback is part of the continuous evaluation or assessment. Using technology, one can assess actions for efficiency and then adjust if required to meet the objective; all accomplished in a matter of seconds. Lastly, the digital government model can leverage advanced technologies to implement predictive analysis into existing processes. The Department of Defense *Artificial Intelligence Strategy* describes this analysis as, "We will use Artificial Intelligence to predict the failure of critical parts, automate diagnostics, and plan maintenance based on data and equipment condition."[434]

The earlier examples of the digital government model operating at the city-level relate to installations of the future and providing enduring capabilities. In these examples, technology improved efficiency or decision making in the areas of healthcare, customer service, traffic control, and fire inspections. Using technology to enhance efficiency or decision making in these fields is analogous to improving efficiency or decision making at U.S. Army installations. The outcome is the same; efficiency is efficiency and decision making is decision making. The digital government model is a means for achieving efficiency in the service delivery function of U.S. Army installations.

Technology is affecting change throughout the world. One only must look in the U.S. strategic documents to see the threats and opportunities advanced technology brings. The Department of Defense *Artificial Intelligence Strategy* provides the most succinct warning of dismissing advances in technology, “Failure to adopt Artificial Intelligence will result in legacy systems irrelevant to the defense of our people…”[435] The U.S. Army should consider the principles and key features of the digital government model through the installation modernization effort as a concept to employ the emerging technologies directed in the National Security Strategy and the National Defense Strategy to improve efficiency and decision making. However, this consideration necessitates an area of additional study to analyze the tension between the digital government models’ key features of digital openness and building efficiency especially as it relates to data security. Adopting the fundamental concepts of the digital government model for use at U.S. Army installations is not just about converting pen and paper processes into the digital functions or creating a cool webpage, the model is a cultural shift in the way installations operate to take advantage of technological advances.[436] Advances in artificial intelligence and machine learning can assist commanders by reducing the required time to process data while at the same time increasing the amount of data considered in the decision-making process.[437] The efficiencies created through the use of advanced technologies can improve installation service delivery and create cost savings.

FUTURE CHALLENGES OF BIG DATA

Mr. Ron James, Department of the Army Civilian

"To maintain our competitive advantage, the United States will prioritize emerging technologies critical to economic growth and security, such as data science, encryption, autonomous technology, gene editing, new materials, nanotechnology, advanced computing technologies, and artificial intelligence."

2017 National Security Strategy[438]

Future installations will require big data that is trusted to fulfill its role as part of a complex multi-domain battlespace. For the Army to trust data it must be current, consistent and collaborative. By looking at what big data is, how it is processed, stored and secured this paper will address how big data is kept current, consistent, and available for collaboration and why it is necessary for these three conditions to exist. The President's National Security Strategy of December 2017 describes the importance of data this way, "Data, like energy, will shape U.S. economic prosperity and our future strategic position in the world. The ability to harness the power of data is fundamental to the continuing growth of America's economy, prevailing against hostile ideologies, and building and deploying the most effective military in the world."[439] Likewise, former Secretary of Defense, James Mattis, in the National Defense Strategy (NDS) emphasized the challenges of defending against expanding technologies at accelerating rates of speed, the NDS states, "New technologies include advanced computing, 'big data' analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology – the very technologies that ensure we will be able to fight and win the wars of the future."[440]

Defining big data remains fairly consistent across multiple sources. Two consistent factors are that it is a large amount of data, structured and unstructured, that can provide value after some amount of analysis. According to the Dell company, "Because of advances in technology, the definition of big data has changed over the years. Yet, one thing that remains the same is that the amount of data is continuously growing at an extremely rapid rate. All data, in any form, that is used for gaining insight and generating value is considered big data."[441] Abhinav Rai, an author and data analyst at the education platform UpGrad, takes the definition a step further and assigns some basic tenets of Big Data:

A massive amount of data that keeps growing over time; So voluminous that it cannot be conventionally processed or analyzed; Includes data mining, data storage, data analysis, and data visualization; An all-inclusive term that includes data, their frameworks, and tools and techniques used to process and analyze the data.[442]

As people continue to add connected devices to their normal routines, the amount of data will continue to grow. The number of connected devices (Internet of Things) worldwide by 2025 will be 75.44 billion.[443] The United Nations forecasts the world population to be 8.1 billion that same year. Forecasting that out 10 more years results in 122.35 billion and 8.89 billion respectively.[444] To put that in perspective, that is nearly 14 connected devices per person in the world. With this number of devices creating data, it is estimated that 1.7MB of new information will be created for every human on the planet – every second of every day – by 2020.[445] This will challenge bandwidth, forcing future installations to weigh the benefits and risks associated with being on an open system with a large number of devices or attempting to limit that to a more closed, less crowded, system. This would also restrict access to data that may be necessary to assist with decision making.

The amount of data is only part of the picture. Data is expanding on three fronts, in 2001 Doug Laney introduced the 3Vs concept. The 3Vs are; Volume (the amount of data), Velocity (the speed at which the data is generated), and Variety (the kind of data available).[446] The 3Vs present challenges to future installations in the amount of data they will be able to store and in the area of power requirements, both computing and electrical. Varied data that is being generated at a high rate of speed requires a great deal of computing power, which in turn, requires a great deal of electrical power.

The challenge this growth presents is the ability for computers to increase in processing power at a rate comparable to the growth of data. A concept of computing power is Moore's Law. The simplified version of this law states that processor speeds, or overall processing power for computers will double every two years."[447] Moore's Law held true for many years. However, in 2005 it was observed that Moore's Law was coming to a halt. With transistors being measured in nanometers and producing more heat as a result, they are reaching their physical limits.[448] With computing power struggling to keep up with the amount of data to be processed, more efficient, methods of computing will be necessary. Super computers and algorithms help make sense of increasingly larger amounts of information in real time. This high-performance computing will be essential in making data useful. High-performance computing entails the use of "supercomputers" and massively parallel processing techniques to solve complex computational problems through computer modeling, simulation, and data analysis.[449]

One of the benefits of high-performance computing is the necessary computing power to produce real-time, or near real-time, outcomes and recommendations. "Real-time Big-Data Analytics or Real-time business intelligence (RTBI) is the process of delivering information about business operations as they occur. Real time means near to zero latency and access to information whenever it is required."[450] One of the challenges outlined in the 2018 Department of Defense (DoD) Cloud Strategy is to "Enable AI and Data Transparency". The strategy states, "DoD must enable decision makers to use modern data analytics such as AI or machine learning, at the speed of relevance to make time critical decisions rapidly in the field to support lethality and enhance operational efficiency."[451] In order to provide outcomes in real time while contending with the challenges of more computing power, high-performance computing brings together multiple technologies, including computer architecture, algorithms, and application software under a single system to solve advanced problems quickly and effectively.[452] This is akin to tens of thousands of workstations synchronized to perform together to process billions of bits of data every second, for numerous users simultaneously. This ability makes high performance computers ideal for handling tasks that require large amounts of data to be computed quickly. The next level of high-performance computing is exascale computing. According to the Exascale Computing Project, “Exascale computing will have a profound impact on everyday life in the coming decades. At 1,000,000,000,000,000,000 oper ations per second, exascale supercomputers will be able to quickly analyze massive volumes of data and more realistically simulate the complex processes and relationships behind many of the fundamental forces of the universe.”[453] The Department of Energy (DOE) is currently conducting the Exascale Computing Project with participation from six DOE core national laboratories across the United States.[454] Exascale computing overcomes the limitations of Moore’s Law while enabling computing power to keep pace with the 3Vs described above. By overcoming these restrictions, installations of the future will have the computing power to assist in such matters such as real time decision making. Exascale computing helps reduce the risk associated with computing power but does not address all of the challenges.

One of the challenges of managing big data and retaining its usefulness is to keep it current. The Army’s top leaders recognize both the value of big data and the challenges associated with managing it. In a 2018 article discussing U.S. Army Futures Command, LTG Piggee stated, “The Army is working hard to improve our information management processes by maximizing the usefulness of the massive amounts of data we get through our enterprise resource planning systems like the Global Combat Support System–Army. This will result in improved data-driven decision-making for all Army leaders and managers.”[455] Erroneous data is one of the challenges with keeping data current, big data sources can generate erroneous data. When data is being collected from a wide variety of inputs at ever increasing speeds it is difficult to differentiate between correct and incorrect input. A 2017 *Deloitte Insights* article explored how these errors occur and came up with five broad observations:

1. Outdated or incomplete information may persist due to the cost and/or effort of obtaining up-to-date information
2. An organization that uses multiple data sources may incorrectly interweave data sets and/or be unaware of causal relationships between data points and lack proper data governance mechanisms to identify these inconsistencies
3. An organization may fall prey to data collection errors like biased sampling data, or self-reported data rather than observed behaviors
4. Data analysis errors may lead to inaccuracies due to such things as incorrect inferences that lead to flawed conclusions or incorrect data collection models
5. Malicious parties may corrupt data (for example, cybercrime activity that alters data and documents)[456]

This demonstrates how bad data can get into a system resulting in inaccurate predictive capability, which is one of big data's primary benefits to installations of the future. This bad data then degrades its trustworthiness.

Being able to trust data, especially when it is being utilized to assist in decision making, is important to any organization. Timo Elliot, a self-described Innovation Evangelist for SAP (a leading enterprise application software company), describes the trust of big data this way, "it's a key part of digital transformation and the business models of the future – and organizations that have robust systems in place to ensure that it can be trusted will be better positioned to take advantage of these powerful new technologies."[457] Some ways that organizations can increase their trust in data and to ensure it is used appropriately is to; define the return on investment for data quality, by measuring the effort necessary to collect the data compared to its value/ quality. Robust governance is another method for increasing trust, each enterprise should establish a set of standards that governs data collection, processing, storage and utilization in a manner that reduces bad data through a set of enforceable standards. Training can also assist in ensuring data remains trustworthy. This could include all the techniques utilized by data handlers as well as understanding the opportunities and limitations of big data. Finally, transparency and ethics can help in this area. Sources of data should be revealed and auditable by governing bodies to ensure standards. This could also verify that data is being utilized in an ethically appropriate manner.[458]

The notion of training is also emphasized in the National Defense Strategy which states, "We will emphasize new skills and complement our current workforce with information experts, data scientists, computer programmers, and basic science researchers and engineers – to use information, not simply manage it."[459] Given the emphasis on big data from the national leadership and across the DoD, organizations are considering the benefits of big data in accomplishing their mission. A 2018 article written by Major Jason Woods, discussed the value of big data in streamlining the auditing process. He argues that the streamlined process will allow auditors to focus more on actual auditing rather than data collection, "Bots, big data, and data science will give financial managers the ability to focus more on the analytics of the data, rather than gathering data."[460] This demonstrates how big data, that is current, can be utilized to conduct the more mundane tasks to enable humans to focus on higher priorities. On a future installation this could translate to monitoring security systems and notifying humans as necessary. In addition to being current, data is most effective and functional when it is consistent.

Consistency on data allows for more predictable and reliable outcomes. “Data that belongs together with regard to content and describes a process state at a specific time is called consistent data. For data to be consistent, it must not be changed or updated during processing or transfer.”[461] Because data is utilized for multiple purposes it is challenging to maintain this consistency. As Henning Lund, CEO of the IT company Rapidi, puts it, “Data is not static, stored once and for all in your systems. Many things will happen with your data from the day it is created in your system and throughout its lifecycle. It can be transferred to other systems, altered and updated multiple times.”[462] Given that data are not static they must be handled and stored in a consistent manner in the event that data recovery is necessary. This consistency is necessary for keeping information uniform as it moves across a network and between various computing applications. There are typically three types of data consistency: point in time consistency, transaction consistency and application consistency.

1. Point in time consistency deals with ensuring that all elements of a system are uniform at a specific moment in time. This prevents loss of data during system crashes, improper shutdowns, and other problems on the network.

2. Transaction consistency is consistency of a piece of data across a working transaction within

the computer, a starting point in a transaction that can be referred back to for accuracy. Without transaction consistency, nothing entered into a program remains reliable.

3. Application consistency is transaction consistency between programs. Without application consistency, the same problems arise as with flawed transaction consistency: there will be no way to tell whether a value entered into the system remains correct over time.[463]

Ensuring that a network has all three elements of data consistency covered helps ensure that data is not lost or corrupted as it travels throughout the system. In the absence of data consistency, there are no guarantees that any piece of information on the system is uniform across the breadth of the computer network. It is across the breadth of the network where collaboration is instrumental.

To be collaborative data should be securely stored in a manner that allows access to those authorized to utilize the data. According to Dr. Martin Strobach et al., the storage of big data is concerned with not only storing the data but also gaining flexibility by managing it in a manner that is scalable, while satisfying the needs of applications that require access the data.[464] More specifically, the key requirements of big data storage are that it can handle very large amounts of data and keep scaling to keep up with growth, and that it can provide the input output operations per second necessary to deliver data to analytical tools."[465] The DoD selected a cloud solution to handle their big data storage requirements. Among the challenges outlined in the DoD Cloud Strategy, three relate to storage:

1. Keep pace with accelerating data growth.

2. The ability to scale, taking advantage of the elasticity of the commercial cloud architecture.
3. The cloud will allow DoD to consolidate data center assets and enable more centralized cloud management.[466]

Likewise, installations of the future will be challenged with data growth and the capability to maintain it in a manner that allows for the necessary level of collaboration.

As noted earlier, the increase in devices globally will greatly increase the amount of data which, in turn, drives up the requirements for data centers. This greater requirement for data centers will increase the need for electricity. According to a power consumption forecast written by Anders Andrae, "On the global scale, data centres are poised to be the largest global energy users by 2025 at 4.5%, an increase from just 0.9% in 2015."[467] Currently 7 of the top 10 data centers in the world are located in China, and all 7 require in excess of 100 MW of power.[468] To put that is perspective, according to California Independent System Operator, a nonprofit that oversees the operation of California's bulk electrical power system, "One megawatt equals one million watts, or 1,000 kilowatts, roughly enough electricity for the instantaneous demand of 750 homes at once. That number fluctuates (some say one megawatt is enough for 1,000 homes) because electrical demand changes based on the season, the time of day, and other factors.[469] Given the data requirements of future installation, Army installations will have to consider electricity production capabilities when planning installation infrastructure requirements. A key component to keeping data collaborative is to ensure its security.

Whether data is in the cloud or on-site, it needs to be protected. The value of protection is emphasized in the National Cyber Strategy, "Malicious cyber actors from other nations have stolen troves of trade secrets, technical data, and sensitive proprietary internal communications. The United States Government will work against illicit appropriation of public and private sector technology and technical knowledge by foreign competitors,"[470] demonstrating America's commitment to protecting data. There are multiple threats to big data, and it is a valuable target for intruders. In a January 2018 interview Army LTG Alan Lynn, director of the Defense Information Systems Agency (DISA) and commander of the Joint Force Headquarters, DoD Information Networks, stated, "A few years ago, getting a 1-gigabyte or 2-gigabyte attack at the internet access point was a big deal. Now, we get 600-gig attacks on the internet access points and unique, different ways of attacking that we hadn't thought of before."[471] An attack could be in the form of a ransomware attack in which the intruders take data hostage and agree to release it for a price. Another threat is unauthorized access, in this case someone who does not have the necessary authorization for access, somehow gains access in an effort to take, and possibly sell valuable data. The mission of those who are tasked with securing data is fairly straight forward; monitor hardware and software for any suspicious behavior or traffic.[472] However, in the case of big data, things are more complicated. In a 2017 article Christine Taylor, of Datamation, described it this way, "However, big data environments add another level of security because security tools must operate during three data stages that are not all present in the network. These are data ingress (what's coming in), Stored data (what's stored), and data output (what's going out to applications and reports)"[473] By 2035 advancements in artificial intelligence and machine learning will likely have advanced enough that they will assist with cyber security. According to Jeffery Cooper, this is currently being explored and shows potential. He says,

> "One of the most important potential use cases for artificial intelligence in government is cyber security. Most cyber security solutions use rules-based or signature-based methodology that requires too much human intervention and institutional knowledge. These systems require constant updates to those rules – taking up employee time – and typically forcing analysts to only look at a single part of the enterprise, failing to get a holistic picture of the environment."[474]

With the exponential growth in data described earlier, current security measures will have a difficult time keeping pace. In order to keep up, cyber protection will need to be able to respond to threats at a cyber pace rather than a human pace. Mr. Dana Deasy, DoD's Chief Information Officer, sees a partnership with artificial intelligence as a way to accomplish the tasks, like cyber security that must happen at a speed beyond human capability.[475] When attacks are happening in cyber space they are happening at cyber speed, which means the counter to the attack must also be operating in the same timeframe.

The value of keeping big data current, consistent and collaborative is that the organization's data is available in a standardized format to the analysts who require it to assist in overall decision making. It is supported by adequate computing power and is stored in a manner that facilitates collaboration while maintaining data security. As was outlined in this paper, data will continue to grow. The strategic challenge is to have the computing, infrastructure, storage, and security systems in place to optimize the usefulness of the data.

An Assessment of the U.S. Army Installations of the Future Campaign Plan Lines of Effort:

In order to support the Army as it prepares for war, installations of the future should provide world class training facilities. Former Secretary of Defense Mattis, in testimony to the senate armed services committee discusses integrating human factors and technology, "We will expose troops to as many simulated tactical and ethical challenges possible before they see combat, ensuring that their first time in combat doesn't feel like their first time in combat."[476] The "U.S. Army Fort Bragg, N.C. is developing a Virtual reality (VR) program that will provide a realistic training program with minimum risk to life and health of soldiers. The program allows squads to maintain their battle experience or prepare for new missions."[477] This type of training could be made more realistic, and therefore more beneficial, through the utilization of big data. According to DataFloq.com, "While Augmented Reality (AR) as a standalone technology offers its own set of solutions, it is now increasingly being used to work in tandem with other technologies to leverage and complement the technological capability of the other. Big Data and AR now work seamlessly together to deliver greater value."[478] Facility maintenance is another area were installation can assist in preparation for war. The Integrated Infrastructure Investment Project Prioritization, Sequencing, and Optimization Process was presented at a Facilities Management Workshop at IMCOM Headquarters in San Antonio, TX February 6-8, 2019. The objective of the workshop was to develop and implement a system that performs prioritization, balancing, sequencing and optimizing of infrastructure investment projects for stakeholder decision-making and strategic planning. The process builds on existing data and the key functionalities and required functions are:

- Utilizes existing data and provides input into an interactive, integrated site-wide Integrated System Planning (ISP) system
- Comprises all infrastructure assets and proposed projects
- Governs and optimizes lifecycle achieving a sustainable site objective
- Demonstrate sequencing in future years
- Show risk reduction over time
- Provide data for PPBE annual planning cycle.[479]

The National Defense Strategy indicates that the homeland is no longer a sanctuary; therefore, installations of the future must also be prepared for the prosecution of war.

Two aspects that will be important to the prosecution of war from an installation are force protection and initial maneuver platforms. Drones and other early warning sensing equipment provide threat assessment data to an Installation Operations Center (IOC) where it is compiled with other data to provide immediate AI driven threat assessments. Likewise, initial maneuver platform security and operational data is provided to the IOC. Cyber warfare is also a likely domain for conflict on installations of the future. Artificial intelligence is seen as a viable defense mechanism to cyber-attacks, “Cyber threats regularly overwhelm traditional security solutions. It’s growing clear that artificial intelligence and machine learning is the safest path to lock down data and protect the enterprise."[480] An additional consideration for the prosecution of war from an installation is command and control. An AI and machine learning reliant command center that operates constantly to augment security and to defend against attack, will rely heavily on big data. Additionally, big data will assist in enabling key installation functions.

Providing enabling capabilities is also a key objective of installations of the future. Soldier protection and resiliency are key components to enabling soldier lethality. The Army partnered with academia in a 2013 study that leveraged big data for studies of psychological strengths in soldiers. They, "examine the confluence of psychological health, soldier performance, economics, and more. The results of this research may inform Army-wide policy decisions regarding recruitment, prevention and treatment programs, job assignments, manpower training, and budgeting."[481] Big data enabled virtual reality (VR) can also serve as a tool to enhance soldier resiliency. An example of in this area is the utilization of big data driven augmented reality to help soldiers who suffer from PTSD, "With such VR applications, soldiers experience different battle scenes that had once influenced their psyche. However, this is absolutely safe and is aimed at overcoming fears and healing."[482] In addition to soldier resiliency, installation infrastructure should be resilient as well. A path to resilient infrastructure is contained in the interactive, integrated site-wide Integrated System Planning (ISP) system described above.

As Army installations become more reliant on technology in the future their dependency on big data will increase. In order to ensure data will be beneficial it should be current, consistent and collaborative. The challenges future Army installations will have with big data are the ability to store a large amount of useful data, the availability of computing power, electrical power, and supporting infrastructure to utilize the data to its full extent, and keeping this amount of data secure so that it is not able to be corrupted or used by adversaries.

INSTALLATION MISSION COMMAND CENTER (IMCC) FOR 2035 AND BEYOND

LTC Bernard Brogan, U.S. Army

“It is now undeniable that the homeland is no longer a sanctuary.”

2018 National Defense Strategy[483]

The *National Defense Strategy (NDS)* states, “Long-term strategic competitions with China and Russia are the principal priorities for the Department, and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future.”[484] An Installation Mission Command Center (IMCC) may help prevent aggressive competitors such as China and Russia from affecting the movement and maneuver of Joint Forces at their home station. In an October 2017 Army Times article, the Assistant Chief of Staff for Installation Management (ACSIM), LTG Gwen Bingham stated, “Army installations are already a front on the modern battlefield, and they need new protections and technology to keep enemies from sabotaging soldiers before they even reach the fight.”[485] The IMCC may support all phases of the *Army’s Multi-Domain Operations (MDO)* concept with the use of a modernized operations center to synchronize installation activities in the air, land, sea, space, and cyberspace domains. In 2035 and beyond, an IMCC may help Army Garrison Commands increase their resilience using modernized information technologies (IT) for their operations centers.

Aggressive competitors such as China and Russia currently affect Joint Force maneuver due to potential threats against critical infrastructure on installations. Army Garrisons in the future environments of 2035 and beyond will need to increase resiliency against competitor threats by using modernized IT for their operations centers. Army senior leaders and strategists should champion and consider integrating the IMCC within the future environment because it can support all phases of the *MDO* concept. Implementing an IMCC can help installations improve their Command and Control (C2) and increase interoperability with internal and external partners, but also manage increased volumes of data generated by the different installations. Leveraging collaborative software and innovative technologies can help build efficiencies that enable the installations to operate in all domains. Moreover, the IMCC can assist Garrison Commanders to mitigate hybrid threats, enhance utility monitoring, and primarily manage all their building control systems to enable the Joint Force to fight near-peer competitors from their home station, Mobilization Force Generation Installation (MFGI) or Power Projection Platform (PPP) and deter future national threats.

Background

An IMCC is an operational name for a digitized operations facility or an existing Command Center. The IMCC is similar to Headquarters, Department of the Army (HQDA) and U.S. Army Forces Command's (FORSCOM) on-going Home Station Mission Command Center (HSMCC) initiatives. The HSMCC initiatives involve the modernization of Army Corps and Division operations centers due to its IT being non-compatible, out of life-cycle, and requiring costly annual upgrades without sustainable warranty plans.

The IMCC is a recommendation for Army installations in 2035 and beyond. The IMCC can leverage best business practices, engineering milestones, and overall investment strategies using the HSMCC implementation plan for Army senior leaders to consider in the modernization of Garrison Commands.

Improve Command and Control

In 2035 and beyond, an IMCC enable Garrison Commanders with improved Command and Control (C2) primarily using commercial visual automation tools and dashboards to monitor their building systems in real-time and installation services. In Fort Benning's Installation of the Future (IotF) report, there is no IMCC assessed or listed because it is currently an idea. However, as a proposal, the IMCC idea may serve as an ideal C2 initiative and platform for the Army Senior Leaders to consider since the same Application Programming Interfaces (APIs) and automation systems are used to support the Joint Force. Additionally, it may also serve as an Army proof of concept or pilot if integrated within Garrison modernization initiatives or an on-going IotF assessment. For example, in 2018, the Army contracted a strategy firm name, Intelligent Buildings Limited Liability Company (LLC), to conduct an assessment on current and future capabilities at Fort Benning, Georgia. The IMCC idea is not captured or required in Fort Benning's IotF assessment. In the future, the aspects of an IMCC should help improve C2 in future assessments if it is considered and integrated as part of on-going operational assessments and reports. The IotF initiatives serve as an ideal baseline on ways Fort Benning incorporates various commercial API software and network technologies for building and management control systems. The IMCC is not part of Fort Benning's IotF assessment; the report provides a description on the roles, functions, and technical capabilities an installation may potentially adapt to improve their C2 for infrastructure and services. It also provides an approach for the Army to consider if IotF is adopted because Fort Benning's C2 processes use a Smart+-Connected approach for the integration of current and future IT monitoring and service capabilities. Fort Benning's IotF defines the Smart+Connected as, "SMART: the ability to collect, visualize, share, and analyze data that informs decisions resulting in increased operational efficiency or enhanced occupant experiences. The assessment defines CONNECTED as implementing and operating an integrated infrastructure and technical ecosystem that facilitates the deployment of Smart solutions."[486] The ability for a Garrison to conduct C2 using the IMCC may increase situational awareness (SA) for the Garrison Commander since they need to make timely decisions on the status of utilities, installations services, and critical infrastructure that enables the Joint Force.

As an example, integrated lighting systems offer automatic centralized command and control of a building's interior and exterior lighting. The system includes software, hardware, and a data network. Local occupancy sensors and switches are networked back to the control software for scheduling and monitoring.[487] In the future, an IMCC idea incorporates innovative visualization, monitoring, and service capabilities to improve C2 using geographic information system (GIS) and system modeling technologies that the Garrison staff may operate remotely with their municipal partners which creates a shared understanding of installation services. If Army leaders employ IMCCs, the use of commercial GIS and dashboards capabilities can increase support to the Garrison's ability to integrate interoperable technologies. The modernized IT in the IMCC can help perform data aggregation that enables the Garrison to integrate and increase their partner's ability to support capacity using digital C2 tools. During daily operations and any potential execution of the Army's MDO concept, an IMCC may assist the Garrison Commanders in achieving the ability to collaborate, monitor utility services, allocate resources to tenant units, and defend building the infrastructure the Joint Force uses at their home station, SSAs, or daily operation.

For example, the IMCC leverages APIs to implement innovative C2 capabilities that include interoperable wearable technologies to help digitally synchronize user activities and share information. Wearable technologies such as Global Position System (GPS) enabled devices, and Fitbit devices may help the installation monitor, track, inform, and notify the Joint Force during operations. According to a U.S. Army Environment Command article, Engineer Research and Development Center (ERDC) liaison, Dr. Jason R. Dorvee stated, "Installations of the future will need to take full advantage of artificial intelligence, automation, sensing, advanced materials, high-powered computing, and secure networks to drive the operation of cost-informed, durable platforms."[488] According to the Army Installations 2025, digital interconnectivity and shared common operational pictures resources help provide Garrisons with Mission Command.

In 2016, former Army Assistant Secretary for Installation Energy and Environment (IE&E) Mrs. Katherine Hammack stated, "To meet the needs of Force 2025 and beyond, Army installations and other enduring locations outside the United States may serve as home station command posts for higher echelon (theater, corps, division) operational forces executing expeditionary missions."[489] In 2035, installations integrating an IMCC with autonomous systems may aid the Garrison Commanders in their abilities to visualize requirements, hurdle challenges, and make informed decisions while maintaining complete situational awareness (SA) across their installation or within the global security environment. As IE&E portrays, "Installations may be required to support basic command post functions related to the mission command network, physical infrastructure, uninterrupted energy supply, as well as the scalability and flexibility to meet the needs of operational Commanders."[490]

Increase Interoperability with Partners

In 2035 and beyond, an IMCC with modernized IT capabilities may increase interoperability with internal and external partners who receive support from their installation. There are two basic types of organizations who may benefit from modernized IT with smart capabilities. In the future, Joint or conventional Army installations an IMCC combined with smart capabilities may help increase interoperability with the partners of a Garrison Command. An example of a joint installation is Joint Base Myer-Henderson Hall in Washington, D.C. In this case, the installation may need an IMCC because it may help increase interoperability with primarily utility management systems that integrate a collection of installation-level service providers, all tenant units, and mission partners.

The external partners would be local, state, federal government entities, private industry, and other stakeholders. An example of a standard Army installation that may benefit from an IMCC with increased interoperability is Carlisle Barracks located in Carlisle, Pennsylvania. In both instances, an IMCC should help these type Garrison Command's increase their interoperability using innovative APIs that digitally integrate utility monitoring software; the installations can seamlessly exchange information or a common operational picture with their mission partners. Additionally, smart capabilities that include innovative SmartHub technologies can help build interoperability with partners, provide automated efficiencies, and help installations in the SSAs to support the tenets of the Army's MDO concept. As an industry leader in modernized IT, Verizon defines as SmartHub technologies, "SmartHub is a wireless, smart home solution that manages your connected home devices, provides reliable, high-speed internet powered by America's Largest and Most Reliable 4G LTE network, and home phone service with HD Voice*, all in one elegant device."[491] The IMCC is essential because it will bridge new technologies with standard operating procedures and capabilities required to manage interoperable solutions with legacy devices. Therefore, an IMCC helps the installation generate options for managing various forms of data installation Commanders will need to manage infrastructure and make informed decisions.

As the requirements for the Joint Force evolve, an IMCC and SmartHub capabilities may enable the Garrison to have interoperable communications and connectivity with tenant units as a globally integrated Army. According to the CENTCOM J4, MG Christopher J. Sharpsten, "The SmartHub will integrate planning to ensure that critical munitions, Prepositioned War Reserve Materiel (PWRM), force enablers needed for Joint Reception, Staging and Onward Movement (JRSO) of combat forces, Operational Contract Support, Energy Production, Operational Project Stocks and interagency supply sources are optimally postured and managed to support assigned missions in multi-domain operations."[492] The MDO concept is ideal because convergence is a crucial factor of mission command. Implementing new technologies that include an IMCC can help the Army lead DoD with interoperability supporting internal and external Joint partners.

In the future, interoperability with partners may increase if an IMCC and SmartHub technologies are employed together because the Garrison Commander needs to maintain C2 of digitally connected devices that support the utilities and select logistics functions on a Joint or an Army installation. In this instance, SmartHub technologies improve interoperability for internal and external partners since they utilize the Internet of Things (IoT) solutions. As the CENTCOM – J4 advises, "From a joint logistics and engineering perspective, designing a concept for a 'smart capability' to support 21st Century Warfare by deploying and leveraging proven IoT solutions, like Smart Cities technologies, is one way to enable the joint force, allies and partners to better build and manage our enduring locations and support distributed operations in a contested environment."[493] The 2016 Department of Defense's Policy Recommendation for IoT states, "IoT is extending the reach of the Internet to inexpensive, miniature, pervasive computing and control devices."[494] As the Army considers new technologies, an IMCC leveraging the IoT and SmartHub capabilities may help increase interoperability since the installation uses information from utility systems, sensors, and multiple data sources. If considered, the IMCC may resolve an installations ability to exchange information using interoperable virtual software, visual touch screen monitors, and network access with internal and external partners.

For context, the IMCC leverages modernized IT and infrastructures to help resolve interoperability with internal and external partners. The employment of innovative software solutions are used to automate and integrate the different service applications. If the Army modernizes installations, the Joint Force becomes more interoperable with ways to deploy, fight, and win against near-peer competitors using IT as a tool. An interoperable IMCC is how the Army may use this tool to become more resilient. As highlighted by FEMA, "Despite the crucial role of technology, FEMA's IT systems historically have not fully met mission needs. Major disasters in the past number of years exposed numerous limitations in FEMA's IT infrastructure and system capabilities."[495] Based on the installation location in CONUS, various essential services require municipal partners to support utility services on an installation. Garrison Commands require more than just email, phone calls, and video teleconference capabilities to be interoperable with partners. According to a disaster expert, Mr. Robert M. Scholander, "The consequences of a failure to achieve communication interoperability or of a breakdown in communication interoperability during disasters can be catastrophic."[496] The IMCC may align digitized capabilities with integrating calibrated force posture because the installation needs to be interoperable with municipal partners who provide essential resources and services. As part of MDO, the IMCC combined with SmartHub solutions may increase interoperability so the installations can support the MDO concept. Based on the echelon, "Calibrated force posture is the combination of capacity, capability, position, and the ability to maneuver across strategic distances. It includes, but is not limited, to basing and facilities, formation and equipment readiness, the distribution of capabilities across components, strategic transport availability, *interoperability*, access, and authorities."[497] Commercial API software reflects an important capability, integrated since "The C2 software helps operators save time and resources in critical situations by enabling fast and informed decision-making."[498] Going forward, the IMCC may use "Smart City" technologies to integrate domain solutions using management control systems differentiate service capabilities that include potential solutions.

Manage Increased Volumes of Data

The DoD cloud strategy may help Garrison Commands manage the increased volume of data on installation if an IMCC is employed to automate operations processes. As highlighted in DoD's cloud strategy, "To adapt to the continuously growing data environment, DoD requires an extensible and secure cloud environment that spans the homeland to the global tactical edge, as well as the ability to rapidly access computing and storage capacity to address warfighting challenges at the speed of relevance."[499] Although the IMCC is a modernized operations facility, Garrisons also have a robust computing and data requirement required to operate efficiently across the installation. According to Dr. Harold Arata, a lead system engineer for AT&T stated, "On the other hand, automated and data-powered actions can process 55 trillion measurements per day and make 1.3 million automated optimizations per day."[500]

The IMCC idea may help manage the increased volume of data on installation using future technologies such as dashboards, commercial industry providers such as AT&T, and sister service on joint concepts supporting Army installations. Modernizing the Garrison

Command's operation centers using the IMCC should help the Army manage innovation and challenges of the increased volume of data because the leadership and partners need to track system trends, monitor surveillance systems, sustain logistics, capture system anomalies, and forecast maintenance requirements across the installation. Moreover, in 2035, the IMCC is ideal because it may enable the Garrison Command and staff to possess C2 of autonomous systems such as driverless cars, robots, alternative 5G secure communications, and drone technologies.

The Army's CIO G6, the Network Cross Function Team (CFT) from Futures Command, U.S. Army's Corps of Engineers, and ACSIM are researching potential ways to leverage data the Internet of Things (IoT) technologies may require so installations can manage public services, traffic, city utilities, and providing first responders with real-time data interconnected to a secure commercial network. In a *Cyber Defense Review* article labeled "Smart Cities, Smart Bases", AT&T's approach consists of the use of IoT devices in eight areas. The data for Smart City initiatives use the IoT devices to support "Public Safety, Infrastructure Monitoring, Multi-Network Solutions, Logistics Management, Waste Management, Water Management, Smart City Operations Center, and Traffic Analytics."[501] The IMCC may operate similarly to a Smart City Operation Center because it uses the same data capabilities residing on a modernized network infrastructure and HCI software tools in the Garrison Headquarters to manage similar information and services for the entire installation. The *Cyber Defense Review* defines a Smart City Operations Center as "a data visualization tool that integrates and aggregates various data points and outputs the data in an easy to digest format. The aggregated IoT data is then used by local utilities, chief information officers, and mayors, to track and improve issues and efficiencies in real-time."[502] In the future, the IMCC is interconnected to various data devices using IoT that provide Garrison Commanders with situational awareness of their installation. Overall, the critical factor in managing data is the Army considering DoD's cloud computing strategy as an option the IMCCs can utilize to enable the Garrison's effort to manage the installation's data.

Conclusion

The Army in Multi-Domain Operations provides senior leaders and Commanders with the flexibility to integrate new technologies such as an IMCC. The installation is a critical component since it supports calibrated force posture, Multi-Domain formations, and convergence as part of the tenets of Multi-Domain Operations. In the future, the IMCC helps the installation with the ability to C2 installation services, synchronize large amounts of data and enable the Joint Force to operate in the strategic support areas during all phases of Competition and Armed Conflict.

ABOUT THE CONTRIBUTORS

BERNARD BROGAN, Lieutenant Colonel (LTC), is a 1998 graduate of Tuskegee University with a Bachelor of Science in Electrical Engineering. He also holds a master's degrees from Webster University. He is a Signal officer and has held a variety of command and staff positions in Army, Special Operations and Joint organizations.

DEBORA E. BROWY, Department of the Army Civilian, is a graduate of Northern Arizona University where she earned a bachelor's degree in Science and Public Service. She served in the U.S. Army with Corp of Engineers, Combat Heavy Brigade, Army Material Command, Army Tank and Automotive Command, and Army Test and Evaluation Command. Ms. Browy has been an Army Logistician and Manager since 2008. Following graduation from the Army War College, she will serve the Army G-3/5/7 at the Pentagon.

PAUL CHLEBO, JR, is a 1984 graduate of Norwich University, earning a Bachelor of Science in mechanical engineering. In 1988 he earned a Master of Science in telecommunications management from Golden Gate University. Mr. Chlebo served as an active Army Officer and currently serves as a Department of the Army civil servant. Mr. Chlebo reports to Headquarters, Communications Electronics Command at Aberdeen Proving Grounds following graduation from the U.S. Army War College.

WILLIAM (CHANCE) COMSTOCK, Lieutenant Colonel (LTC), is a Medical Service Corps officer in the U.S. Army Reserve. LTC Comstock is 1995 graduate of Virginia Commonwealth University (Bachelor of Science), and a 2001 graduate of the California University of Pennsylvania (Master of Arts). He has held *various leadership, staff, and technical positions in the U.S. Army Medical Department in field units and fixed facilities.*

MARY O. B. DRAYTON, Colonel (COL), is a 1996 graduate of the United States Military Academy and was commissioned as a second lieutenant in the Chemical Corps. Additionally, she earned a master's degree in business administration from Regis University. COL Drayton became a member of the Army Acquisition Corps in 2005. She has held a variety of Acquisition positions to include Deputy Assistant Secretary of the Army (Procurement) Executive Officer and recently as Battalion Commander and Director of Contracting at the Mission and Installation Contracting Command-Fort Riley, Kansas.

RONNY J. JAMES is a Department of the Army Civilian, since 2005 he has been involved in installation management at the installation and regional levels. He has specific installation experience as a Region Installation Support Team member, Deputy to a Garrison Commander, and Lead Strategic Planner. Additionally, he has worked base closure and realignment efforts in Europe, Korea and CONUS.

BRIAN JORGENSON, Lieutenant Colonel (LTC), is a 1998 graduate of Gonzaga University. He holds master's degrees from the U.S. Naval War College and USAWC. He commissioned as a Signal Corps Officer and has held a variety of command and staff positions in Army, Joint, and Special Operations organizations.

ERIC MCCOY, Lieutenant Colonel (LTC), is a 1998 graduate of Morgan State University and received master's degrees from Central Michigan University, Georgetown University, and the U.S. Army War

College. He entered the Army as an Ordnance Officer and has served as a multifunctional logistics officer in tactical, operational, and strategic formations. Prior to attending the War College, he served as the Chief of Sustainment for the 25th Infantry Division. Following graduation, he will serve as the Chief, Subsistence Supply Chain, Defense Logistics Agency - Troop Support.

TIMOTHY R. O'SULLIVAN, Lieutenant Colonel (LTC), is a 1997 graduate of the U.S. Military Academy with a bachelor's degree in mechanical engineering. Additionally, he earned a master's degree in policy management from Georgetown University. LTC O'Sullivan is a force management officer with 22 years of service and deployments to Kosovo, Iraq, and Afghanistan. His last assignment was on the Army Staff and will next serve at the Mission Command Center of Excellence at Fort Leavenworth.

JENNIFER REYNOLDS, Lieutenant Colonel (LTC), is a 1998 graduate of Colorado State University and was commissioned as an Aviation officer. She also holds an MS from Kansas State University. LTC Reynolds has served in a variety of staff and command positions from the tactical to strategic levels. Her previous two assignments were as the senior aviation trainer at the Joint Readiness Training Center in Fort Polk, LA, and as the battalion commander for 3-1 Assault Helicopter battalion in Fort Riley, Kansas.

KENNETH D. SLOVER Colonel (COL), is a 1995 graduate of Clarkson University where he earned a Bachelor of Science degree in biology and was commissioned as a Field Artillery officer. Additionally, he received a master's degree in Emergency and Disaster Management from Trident University. In 24 years of service, he *has served in various tactical and operational assignments. He is currently serving as the 8th Army Fire Support Coordinator at Camp Humphreys, ROK.*

STEVEN TABAT, Colonel (COL), is a 1996 graduate of Texas Christian University with a degree in history and was commissioned as an Infantry Officer. He holds an MS from Central Michigan University. COL Tabat has commanded at the company and battalion level and served in a variety of staff positions in the Army and Joint Community. COL Tabat most recently served as the Chair of the Military Science Department and Professor of Military Science for Texas Christian University Army ROTC, preceding that as the Division Chief of Staff for Division West, First Army, Fort Hood, TX.

Endnotes

1. Richard Kidd, “Installations of the Future: Providing the backbone for Army to prepare and engage in war,” (Presentation slides from AY19 Futures Seminar class, October 26, 2018), 1.

2. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), 1. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed March 10, 2019).

3. Mark A. Milley, Mark T. Esper, *The Army Strategy* (Washington, DC: U.S. Department of the Army, 2019), 1.

4. AUSA, Installations : the bedrock of America’s Army, 1.

5. ASA IE&E Brief, OCT 26, 2019

6. U.S. Army Training and Doctrine Command G-2, *The Operational Environment and the Changing Character of Future Warfare* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, October 2019), 21.

7. TRADOC, The Operational Environment, 23.

8. Summary of the 2018 Department of Defense Artificial Intelligence Strategy, (Washington, DC: U.S. Department of Defense, February 2019), https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (accessed March 1, 2019). 6.

9. DoD AI Strategy, 6.

10. U.S. Army Training and Doctrine Command, *The U.S. Army Robotic and Autonomous Systems Strategy* (Fort Eustis, VA: Maneuver, Aviation, and Soldier Division Army Capabilities Integration Center, March 2017), 1.

11. TRADOC, Robotic and Autonomous System Strategy, 9.

12. “Smart Tech definition,” Netlingo, https://www.netlingo.com/word/smart-tech.php.

13. “Smart, Connected and IoT Based Devices. What’s the Difference?”, Medium, https://medium.com/@YogeshMalik/smart-connected-and-iot-based-devices-whats-the-difference-36fc1bdc36b2

14. ASA IE&E brief, 6.

15. Erv Lessel, Bill Beyer, Ted Johnson, *Byting the Bullet – Now is the Time for Smart Military Bases*, Deloitte Center for Government Insights, 2017, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-fed-byting-the-bullet.pdf , 2.

16. TRADOC, The Operational Environment, 22.

17. Mattis, National Defense Strategy

18. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (December 6, 2018), iii.

19. TRADOC, MDO, 8.

20. TRADOC, MDO Advance Summary, 12.

21. Idrees Ali, “U.S. military puts ‘great power competition’ at heart of strategy: Mattis”, Reuters, January 19, 2018, https://www.reuters.com/article/us-usa-military-china-russia/u-s-military-puts-great-power-competition-at-heart-of-strategy-mattis-idUSKBN1F81TR

22. Mattis, National Defense Strategy

23. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (December 6, 2018), Foreword.

24. Defense Intelligence Agency, *China Military Power*, 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf , 13.

25. Daniel R. Coats, “Statement for the Record Worldwide Threat Assessment of the US Intelligence Community,”

(Washington, DC: Director of National Intelligence, January 29, 2019), 5.

26. Coats, Worldwide Threat Assessment,5.

27. Defense Intelligence Agency, *Russia Military Power*, 2017, https://www.dia.mil/portals/27/documents/news/military%20power%20publications/russia%20military%20power%20report%202017.pdf , 14.

28. DIA, Russia Military Power, 22.

29. Coats, Worldwide Threat Assessment, 37.

30. Coats, Worldwide Threat Assessment, 5.

31. Coats, Worldwide Threat Assessment, 14.

32. MG Joseph Whitlock, *The Army's Mobilization Problem,* The War Room, October 13, 2017, https://warroom.armywarcollege.edu/articles/armys-mobilization-problem/ (accessed January 26, 2019)

33. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed January 26, 2019), 3.

34. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (December 6, 2018), GL-9.

35. TRADOC Pamphlet 525-3-1, C-4.

36. Defense Science Board, U.S. Department of Defense, *Task Force on Survivable Logistics Executive Summary* (November 2018), https://apps.dtic.mil/dtic/tr/fulltext/u2/1064537.pdf 1.

37. Department of Defense, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request* (Washington, DC: Department of Defense, February 2018), https://comptroller.defense.gov/Portals/45/Documents/

defbudget/fy2019/FY2019_Budget_Request_Overview_Book.pdf, 3-16 (accessed February 17, 2019).

38. U.S. Army War College, *Key Strategic Issues List (KSIL) 2018-2020,* (Carlisle Barracks, PA: U.S. Army War College, 2018), 9.

39. Olen Bridges and Andree Navarro, Mobilizing for Major War, *Parameters* (Volume 47, Issue 2) (Carlisle Barracks, PA: U.S. Army War College, Summer 2017), 90.

40. Thomas P. Galvin, "Military Preparedness," *Faculty Paper* (Carlisle, PA: U.S. Army War College, 2019).

41. Alexander King, *MFGIs of 2035 Project* (Email to author, February 4, 2019).

42. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-4-1, *The U.S. Army Functional Concept for Sustainment 2020-2040* (February 2017), 6.

43. Headquarters, Department of the Army (G3/5/7 and G4), *MFGI and PPP Definitions per Draft SecArmy Policy Directive* (Revised Per DA G3/5/7, (Presentation, July 12, 2018 World Wide Secure Video Teleconference). Final SecArmy Policy pending completion of Army Wide-Staffing and publication by Army Publication Directive.

44. Headquarters, Department of the Army (G3/5/7 and G4), *Minimum Installation Mobilization Capabilties*, (Presentation, July 17, 2018).

45. Headquarters, Department of the Army (G3/5/7 and G4), *Army Mobilization and Deployment Sequencing*, (Presentation, July 17, 2018).

46. *Army Mobilization and Deployment Sequencing*, (Presentation, July 17, 2018).

47. *Army Mobilization and Deployment Sequencing*

48. *MFGI and PPP Definitions per Draft SecArmy Policy Directive* (Revised Per DA G3/5/7, (Presentation, July 12, 2018 World Wide Secure Video Teleconference)

49. Headquarters, Department of the Army (G3/5/7 and G4), *Minimum Installation Power Projection Capabilties*, (Presentation, July 17, 2018).

50. TRADOC Pamphlet 525-4-1, 10.

51. TRADOC Pamphlet 525-4-1, 10.

52. TRADOC Pamphlet 525-4-1, 10.

53. Mattis, National Defense Strategy, 6.

54. TRADOC Pamphlet 525-4-1, 9.

55. Mad Scientist Laboratory, *Smart Cities and Installations of the Future: Challenges and Opportunities*, https://madsci-blog.tradoc.army.mil/21-smart-cities-and-installations-of-the-future-challenges-and-opportunities/, January 18, 2018, (accessed January 26, 2019).

56. Asian Development Bank, *Region at Risk: Human Dimensions of Climate Change in Asia and the Pacific* (ADB, Manila: July 2017), 4.

57. TRADOC Pamphlet 525-3-1, xi.

58. Defense Science Board, 3.

59. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-4-1, *The U.S. Army Functional Concept for Sustainment 2020-2040*, February 2017, 10.

60. Headquarters Department of the Army (HQDA) Draft Execution Order (EXORD) 065-19, *Total Army Unit Movement Readiness*, O-6 Review Version dated December 21, 2018.

61. Duggan, 2.

62. James Morningstar, *Reinventing Installations for the Next War*, (Working Manuscript) 3.

63. Dorvee, *A Modern Army Needs Modern Installations*.

64. Assistant Chief of Staff for Installation Management (ACSIM), *U.S. Army Modern Installations*, Stand-To: The Official Focus of the U.S. Army (September 26, 2018), https://www.army.mil/standto/archive_2018-09-26, (accessed January 27, 2019).

65. Defense Science Board, 6.

66. Acker, https://www.wbdg.org/building-types/warehouse/ (accessed January 28, 2019).

67. *Drone Stock Counting,* The Future Warehouse by Argon, http://www.thefuturewarehouse.com/drones/ (accessed on February 18,2019)

68. Beth E. Lachman, Agnes Gereben Schaefer, Nidhi Kalra, Scott Hassell, Kimberly Curry Hall, Aimee E. Curtright, and David E. Mosher, Key Trends That Will Shape Army Installations of Tomorrow. Santa Monica, CA: RAND Corporation, 2013. https://www.rand.org/pubs/monographs/MG1255.html , 186.

69. Carlos Gonzalez, *All Aboard! The Future of Railroads, Subways, and Smart Cities* (July 27, 2016), https://www.machinedesign.com/iot/all-aboard-future-railroads-subways-and-smart-cities/ (accessed February 1, 2019).

70. Headquarters Department of the Army (HQDA), Department of Army Pamphlet (DA PAM) 525-30, *Army Strategic Readiness Assessment Procedures*, June 9, 2015, 30.

71. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), 3, 6. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed March 10, 2019).

72. U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028 Advance Summary* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), 13.

73. J.E. “Jack” Surash, “Off The Grid,” *ARMY Magazine* (Arlington, VA, February 2019), 28; *The United States Army Homepage*, https://www.army.mil/

article/195245/a_message_from_the_sergeant_major_of_the_army_energy_action_month (accessed March 7, 2019).

74. U.S. Army Training and Doctrine Command G-2, *The Operational Environment and the Changing Character of Future Warfare* (Fort Eustis, VA: U.S. Army Training and Doctrine Command), 4, 19.

75. Dr. Jason R. Dorvee, Mr. Richard G. Kidd IV, and Mr. John R. Thompson, "Army Installations: A Whole Flock of Pink Flamingos," *Mad Scientist Laboratory* (October 18, 2018), blog entry, https://madsciblog.tradoc.army.mil/91-army-installations-a-whole-flock-of-pink-flamingos/ (accessed December 24, 2018).

76. Thomas P. Galvin, "Military Preparedness," *Faculty Paper* (Carlisle Barracks, PA: U.S. Army War College, 2019), 12.

77. Rebecca Robbins Raines, *Getting the Message Through – A Branch History of the U.S. Army Signal Corps* (Washington, DC: U.S. Army Center of Military History, 1996), 3.

78. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America,* 3, 6.

79. Mr. Richard Kidd, Deputy Assistant Secretary of the Army for Strategic Integration, *Installations of the Future: Providing the Backbone for Army to Prepare and engage in War* (Washington, DC: February 2, 2018). https://armywarcollege.blackboard.com/webapps/blackboard/execute/content/file?cmd=view&content_id=_200124_1&course_id=_3993_1&framesetWrapped=true (accessed December 1, 2018)

80. U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035 (JOE 2035), Version 1.0* (Washington, DC: U.S. Joint Chiefs of Staff, July 14, 2016), 18, 26. https://www.airuniversity.af.mil/Portals/10/CMSA/documents/Required_Reading/Joint%20Operating%20Environment%202035%20The%20Joint%20Force%20in%20a%20Contested%20and%20Disordered%20World.pdf (accessed December 31, 2018).

81. U.S. Army Training and Doctrine Command G-2, *The Operational Environment and the Changing Character of Future Warfare*, 4, 19.

82. U.S. Department of the Army, “Army Information Technology,” *Army Regulation 25-1* (Washington, DC: U.S. Department of the Army, June 25, 2013); U.S. Department of the Army, “Army Information Technology Implementation Instructions”, *Department of the Army Pamphlet 25–1–1* (Washington, DC: U.S. Department of the Army, September 26, 2014).

83. U.S. Department of the Army, “Army Information Technology Implementation Instructions”, *Department of the Army Pamphlet 25–1–1*, 8-9.

84. U.S. Army Network Enterprise Technology Command, NETMOD Installation Tracking Portal (Fort Huachuca, AZ: U.S. Department of the Army) https://army.deps.mil/netcom/sites/G357/NETMOD/Pages/Home.aspx (CAC Only) (accessed 2 November 2018).

85. David S. Alberts, John J. Gartska, Frederick P. Stein, *Network Centric Warfare Developing and Leveraging Information Superiority* (Washington, DC: DoD Command and Control Research Program CCRP, 1999), 223, 228.

86. U.S. Joint Chiefs of Staff, “Joint Planning,” *Joint Publication 5-0* (Washington, DC: U.S. Joint Chiefs of Staff, June 16, 2017) IV-6, IV-15. (Consideration of planning assumptions addresses strategic gaps that may hinder the development of an approach to options for resiliency).

87. Mark A. Milley, Mark T. Esper, *The Army Strategy* (Washington, DC: U.S. Department of the Army, 2019), 3.

88. Bruce T. Crawford, “CIO G-6 Signal Conference,” *Office of the Army Chief Information Officer* (Washington, DC: U.S. Department of the Army, March 6, 2018), linked from the AFCEA Home Page, https://www.afcea.org/event/sites/default/files/files/1300%20-%201345%20-%20Crawford%20Keynote.pptx (accessed March 7, 2019).

89. Dr. Conrad C. Crane, Dr. Michael E. Lynch, Mr. Shane P. Reilly, *A History of the Army’s Future: 1990-2018 v.2.0* (Carlisle Barracks, PA: U.S. Army War College, September 2018), 10-11.

90. Executive Office of the President of the United States, Office of Management and Budget, Circular A-130 revised, (Washington, DC: 28 July 2016). 6. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf (accessed January 15, 2019).

91. U.S. Department of Defense, Chief Information Officer, Department of Defense Architecture Framework (DoDAF), Version 2.02, (Washington, DC). Introduction. Common Access Card (CAC) Required. https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_background/ (accessed December 20, 2018).

92. U.S. Joint Chiefs of Staff, *Joint Operating Environment (JOE) 2035*, 18.

93. Efraim Turban, Ephraim Mclean, James Wetherbe, *Information Technology Management* (New York: John Wiley & Sons, 1996), 309.

94. Turban, et al, Information Technology Management, 320-321.

95. U.S. Department of Defense, *DoD Cloud Strategy* (Washington, DC: U.S. Department of Defense, December 2018), 6. https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF (accessed February 1, 2019).

96. Brad D. Williams, *Emerging 'hyperwar' signals 'AI-fueled, machine-waged' future of conflict* (Fifth Domain Home Page: August 7, 2017) https://www.fifthdomain.com/search/68968334/?q=emerging+hyperwar (accessed 1 Feb 2019).

97. Joel Barbier, Kevin Delaney, and Nicole France, "Digital Cities: Building the New Public Infrastructure Cities show proven results through digital transformation," *CISCO White Paper* (San Jose, CA: 2017), 16. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/scc/digital-cities-value-at-stake.pdf (accessed December 26, 2018).

98. Barbier, et al, Digital Cities, 14.

99. “Introducing the Adaptive Network Vision,” *Ciena White Paper* (Hanover, MD: 2018) (https://media.ciena.com/documents/Introducing-the-Adaptive-Network-Vision-WP.pdf (accessed 20 March 2019).

100. Rohit Mehra and Nolal Greene, *Software Defined Network Architectures; A Key Building Block for Digital Transformation* (Framingham, MA: IDC Analyst Connection, January 2017), 2.

101. “Getting the Facts on Optical Fiber,” *Corning Media Release* (Corning, NY: 2012) http://media.corning.com/flash/opticalfiber/2012/corning_optical_fiber/Documentation/FIBER_MATTERS/flipbook/585324499/files/inc/585324499.pdf (accessed February 20, Feb 2019)

102. “Frequency Asked Questions on Fiber Reliability,” *Corning White Paper* (Corning, NY: April 2016) http://www.corning.com/media/worldwide/coc/documents/Fiber/RC-%20White%20Papers/WP5082%203-31-2016.pdf (Accessed 20 Feb 2019).

103. Klint Finley, “The Hyper-Speed Promise of 5G,” *Wired Magazine (*February 2019), 26.

104. Mark Altaweel, *High Altitude Pseudo-Satellites* (February 22, 2018), blog entry, https://www.gislounge.com/high-altitude-pseudo-satellites/ (accessed 5 March 2019).

105. U.S. Department of the Army, *Mission Command Network Requirements & Architecture Summary* (Washington, DC: U.S. Department of the Army, 7 September 2018), 5.

106. “Telecommunications Infrastructure Standard for Data Centers,” *Telecommunications Industry Association, Approved American National Standard ANSI/TIA-942-A* (Arlington, VA: March 2014), 10-11.

107. U.S. Department of Defense CIO, “DoD Cloud Strategy,” (Washington, DC: U.S. Department of Defense, December 2018), 3.

108. DoD Cloud Strategy, 6.

109. DoD Cloud Strategy, A-2.

110. Sarah K. White, "What is geofencing? Putting location to work," CIO (November 1, 2017), blog entry, https://www.cio.com/article/2383123/geofencing-explained.html (accessed 18 March 2019).

111. White, Geofencing.

112. "Programmable Automotive Headlights," *Illumination and Imaging* (Pittsburgh, PA: Carnegie Mellon University, 2014) http://www.cs.cmu.edu/smartheadlight/ (accessed January 20, 2018).

113. Office of the Army Chief Information Officer/G-6, *Army Network Campaign Plan* (Washington, DC: U.S. Department of the Army, July 2015), 6-10.

114. U.S. Department of the Army, "Army Information Technology," *Army Regulation 25-1* (Washington, DC: U.S. Department of the Army, June 25, 2013), 19-20, 43.

115. U.S. Department of the Army, "Army Information Technology Implementation Instructions", *Department of the Army Pamphlet 25–1–1* (Washington, DC: U.S. Department of the Army, September 26, 2014), 58.

116. U.S. Department of the Army, "Army Strategic Readiness Assessment Procedures," *Army Regulation 525-30.* (Washington, DC: U.S. Department of the Army, June 9, 2015), 30.

117. *Dr. James K. Morningstar, "Reinventing Installations for the Next War," Faculty Paper* (Carlisle, PA: U.S. Army War College, 2019), *4.*

118. This quote is attributed in multiple sources to the ancient Greek poet Archilochus from 650 BCE.

119. In U.S. Army doctrine ADRP 1-02 provides definitions for military terms. This manual's chapter 6 is titled "Installations" and provides 9 pages of military symbols related to installations, but neglects to precisely define the term. U.S. Department of the Army, *ADRP 1-02 Military Terms and Symbols* (Washington, DC: U.S. Department of the Army, 16 November 2016), 6-1.

120. Department of the Army, *DA PAM 525-30 Army Strategic Readiness Assessment Procedures* (Washington, DC: Headquarters Department of the Army, June 9, 2015), 30.

121. Department of the Army, *Training Units and Developing Leaders Army Doctrine Publication 7-0* (Washington, DC: United States Combined Arms Center, August 23, 2012), 4.

122. Combined Arms Center Training, *Synthetic Training Environment (STE) White Paper* (Fort Leavenworth, KS: U.S. Army Combined Arms Training Center, 2017), 1, https://usacac.army.mil/sites/default/files/documents/cact/STE_White_Paper.pdf (accessed March 9, 2019).

123. U.S. Army Corps of Engineers, *Unified Facilities Criteria (UFC) Installation Master Planning UFC 2-1001-01 Change 1* (Washington, DC: U.S. Army Corps of Engineers, November 28, 2018), 2.

124. Army Corps of Engineers*, Unified Facilities Criteria,* 7.

125. Army Corps of Engineers*, Unified Facilities Criteria,* 12.

126. Jim Mattis, Summary of the 2018 National Defense Strategy of the United States of America (Washington, DC: U.S. Department of Defense, 2018), 6. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

127. Mattis, *Summary of the 2018 National Defense Strategy*, i-ii.

128. Lachman, *Key Trends That Will Shape Army Installations of Tomorrow*, 17.

129. Bruce Stein, Cameron Scott, and Nancy Benton, "Federal Lands and Endangered Species: The Role of Military and Other Federal Lands in Sustaining Biodiversity," *BioScience* (58, no. 4, April 2008), 345.

130. Stein, et al, Federal Lands 345.

131. L. Peter Boice, "Threatened and Endangered Species on DoD Lands" (Washington, DC: Natural Resources Department

of Defense, May 2013), 2, http://www.dodnaturalresources.net/files/TE__s_fact_sheet_5-24-13.pdf (accessed March 13, 2019).

132. Boice, Threatened and Endangered Species.

133. Elsie Davis, "Base recognized for conservation work: Home for woodpeckers, tortoises, awarded" (Atlanta, GA: U.S. Fish and Wildlife Service, May 30, 2018), 1, https://www.fws.gov/southeast/news/2018/05/base-recognized-for-conservation-work/#contacts-section (accessed March 5, 2019).

134. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *DoDD 4715.21 Climate Change Adaptation and Resilience* (Washington DC: Department of Defense, January 14, 2016), 11.

135. Office of the Under Secretary of Defense for Acquisition and Sustainment, *Report on Effects of a Changing Climate to the Department of Defense* (Washington, DC: Department of Defense, January 2019*)*, 4.

136. Kevin Scott, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, Joint Force Development, July 14, 2016), I.

137. U.S. Army Training and Doctrine Command, *The Operational Environment and the Changing Character of Future War* (Fort Eustis, VA: U.S. Army Training and Doctrine Command G-2 OE Enterprise, 2017), 1.

138. Scott, *Joint Operating Environment 2035*, 15.

139. Mattis, *Summary of the 2018 National Defense Strategy of the United States of the America*, 3.

140. Scott, *Joint Operating Environment 2035*, 18.

141. U.S. Army Training and Doctrine Command, *The U.S. Army Robotic and Autonomous Systems Strategy* (Fort Eustis, VA: Maneuver, Aviation, and Soldier Division Army Capabilities Integration Center, March 2017), 1.

142. Peter Rubin, “The Wired Guide to Virtual Reality,” *Wired* (September 11, 2018) https://www.wired.com/story/wired-guide-to-virtual-reality/ (accessed March 5, 2019).

143. Janko Roettgers, “Virtual Reality Projected to Become a $7 Billion Business This Year,” *Variety* (April 11, 2017), 1, https://variety.com/2017/digital/news/virtual-reality-industry-revenue-2017-1202027920/ (accessed March 5, 2019).

144. Roettgers, Virtual Reality.

145. Scott, *Joint Operating Environment 2035*, 17.

146. Scott, *Joint Operating Environment 2035*, 19.

147. Patrick J. Mahaney Jr. and Cohort IV of the Chief of Staff of the Army’s Strategic Studies Group, *The Character of Warfare 2030 to 2050: Technological Change, the International System, and the State* (Washington, DC: Chief of Staff of the Army’s Strategic Studies Group, November 22, 2017) 62.

148. Scott, *Joint Operating Environment 2035*, 15.

149. Mattis, *Summary of the 2018 National Defense Strategy*, 3.

150. Mattis, *Summary of the 2018 National Defense Strategy*, 3.

151. Scott, *Joint Operating Environment 2035*, 15.

152. Tamir Eshel, “Russian Military to Test Combat Robots in 2016,” *Defense Update* (December 31, 2015), blog entry, https://defense-update.com/20151231_russian-combat-robots.html (accessed online March 8, 2019).

153. Tate Nurkin, *China’s Advanced Weapons Systems* (London, UK: Jane’s by IHS Markit, May 12, 2018), 111.

154. Nurkin, China’s Advanced Weapons.

155. Mattis, *Summary of the 2018 National Defense Strategy*, 3.

156. This is a summary of the article: Dr. Jason R. Dorvee, Mr. Richard G. Kidd IV, and Mr. John R. Thompson, “Army Installations: A Whole Flock of Pink Flamingos,” *Mad Scientist Laboratory* (October 18, 2018), blog entry, https://madsciblog.tradoc.army.mil/91-army-installations-a-whole-flock-of-pink-flamingos/ (accessed January 23, 2019).

157. Mark Milley, *The U.S. Army in Multi-Doman Operations in 2028*, i.

158. Milley, *The U.S. Army in Multi-Doman Operations in 2028*, i.

159. Milley, *The U.S. Army in Multi-Doman Operations in 2028*, xi.

160. Ryan D. McCarthy, *Army Directive 2017-24 (Cross-Functional Team Pilot In Support of Materiel Development),* 2, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6101_AD2017-24_Web_Final.pdf (accessed January 13, 2019).

161. Mark T. Esper and Mark A Milley, *The Army Strategy* (Washington DC: U.S. Department of the Army, November 1, 2018) 7.

162. James Mattis, “*Directive-type Memorandum (DTM)-18-001 – “Establishment of the Close Combat Lethality Task Force (CCLTF)”* (Washington, DC: Secretary of Defense, March 16, 2018), 10.

163. James C. Crowley, Bryan W. Hallmark, Michael G. Shanley, and Jerry M. Sollinger, *Changing the Army’s Weapon Training Strategies to Meet Operational Requirements* (Santa Monica, CA: RAND Corporation, 2014), xv.

164. The Range Design Guide (RDG) is a web-based tool that provides guidance for design and construction of Army ranges from the training requirements in TC 25-8. U.S. Army Corps of Engineers Range Design Guide homepage, https://www.hnc.usace.army.mil/Missions/Installation-Support-and-Programs-Management/Range-and-Training-Land-Program/Range-Design-Guide/ (accessed March 5, 2019).

165. U.S. Army Corps of Engineers Range Design Guide homepage, *Standard Range Support Building Matrix*, May 2018. https://www.hnc.usace.army.mil/Portals/65/docs/Directorates/ISPM/RTLP/PDFs/Range%20Operations%20and%20Control%20Area/Standard%20Range%20Support%20Building%20Matrix%20MAY%2017%202018.pdf?ver=2018-05-17-122426-033 (accessed March 5, 2019).

166. Sydney J Freedberg Jr. "HUD 3.0: Army To Test Augmented Reality For Infantry In 18 Months" *Breaking Defense* (March 29, 2018), 1, https://breakingdefense.com/2018/03/hud-3-0-army-to-test-augmented-reality-for-infantry-in-18-months/ (accessed March 7, 2019).

167. National Research Council. *Making the Soldier Decisive on Future Battlefields* (Washington, DC: The National Academies Press, 2013), 53.

168. National Research Council. *Making the Soldier Decisive on Future Battlefields*, 51.

169. National Research Council. *Making the Soldier Decisive on Future Battlefields*, 47.

170. Elizabeth R. Uhl, Martin L. Bink, David R. James, and Marc Jackson, *Realism and Effectiveness of Robotic Moving Targets Research, Report 2009*, (Fort Belvoir, VA: U. S. Army Research Institute for the Behavioral & Social Sciences, April 2017), 1.

171. A current leader in the field is Marathon Targets from Australia https://marathon-targets.com. The author of this paper conducted training with these targets while assigned to the U.S. Army Asymmetric Group in 2012-2013. The United States Marine Corps and U.S. Army Asymmetric Warfare Group both conducted assessments of the Marathon targets and they are being used by the Australian Defense Forces.

172. Seth Robinson, "A GI's next target? That autonomous moving robot at 50 yards," *Stars and Stripes*, (Defense Media Activity, September 4, 2013), 1, https://www.stripes.com/news/a-gi-s-next-target-that-autonomous-moving-robot-at-50-yards-1.239194 (accessed January 13, 2019).

173. Robinson, A GI's next target?, 2-3.

174. Nicholas Milano, "QRT Aims To Improve Sniper Performance When Engaging Moving Targets," *Infantry Magazine* (January/March 2017), 1, http://www.benning.army.mil/infantry/magazine/issues/2017/JAN-MAr/pdf/10)Milano_JointSniper_txt.pdf (accessed February 18, 2019).

175. Milano, QRT Aims To Improve Sniper Performance.

176. Uhl et al., *Realism and Effectiveness of Robotic Moving Targets Research,* 10-11.

177. Robinson, "A GI's next target? That autonomous moving robot at 50 yards," 3.

178. McCarthy, *Army Directive 2017-24 (Cross-Functional Team Pilot In Support of Materiel Development),* 1.

179. Combined Arms Center Training, *Synthetic Training Environment (STE) White Paper* (Fort Leavenworth, KS: U.S. Army Combined Arms Training Center, 2017), 1, https://usacac.army.mil/sites/default/files/documents/cact/STE_White_Paper.pdf (accessed March 9, 2019).

180. Esper *The Army Strategy*, 5.

181. Maria R. Gervais, "The Synthetic Training Environment Revolutionizes Sustainment Training," *Army Sustainment* (September-October 2018), 26.

182. Milley, *The U.S. Army in Multi-Doman Operations in 2028*, F-2.

183. Milley, *The U.S. Army in Multi-Doman Operations in 2028*, F-3.

184. Gervais, "The Synthetic Training Environment Revolutionizes Sustainment Training," 29.

185. Headquarters Department of the Army, *Antiterrorism Army Regulation 525–13* (Washington, DC: Department of the Army, February 17, 2018), 9.

186. Randall Steeb, John Matsumura, Paul S. Steinberg, Thomas J. Herbert, Phyllis Kantar, and Patrick Bogue, *Examining the Army's Future Warrior: Force-on-Force Simulation of Candidate Technologies* (Santa Monica, CA: RAND Corporation, MG-140-A, 2004), XV.

187. Combined Arms Center Training, *Synthetic Training Environment (STE) White Paper*, 3.

188. Milley, *The U.S. Army in Multi-Doman Operations in 2028*, 5.

189. Combined Arms Center Training, *Synthetic Training Environment (STE) White Paper*, 2.

190. Combined Arms Center Training, *Synthetic Training Environment (STE) White Paper*, 3.

191. Nathaniel Hawthorne, "Electricity Quotes," *Good Reads*, https://www.goodreads.com /quotes/tag/ electricity (accessed September 19, 2018).

192. Sabrina Toppa, "The National Power Grid is Under Almost Continual Attack, Report Says," *Time*, March 25, 2015, https://time.com/3757513/electricity-power-grid-attack-energy-security, (accessed March 6, 2019).

193. Statement by LTG Gwen Bingham, Assistant Chief of Staff for Installation Management, United States Army, Address to the Committee on Appropriations United States Senate Subcommittee on Military Construction and Veterans Affairs and Related Agencies, First Session, 115th Congress, Fiscal Year 2018 Department of Defense Budget Request for Military Construction and Family Housing, Washington, D.C., June 6, 2017, 8. https://www.appropriations.senate.gov /imo/media/doc/06017-Bingham-Testimony.pdf (accessed September 15, 2018).

194. Daniel B. Allyn and Brad R. Carson, Energy Security and Sustainability (ES2) Strategy, (Washington D.C., U.S. Department of the Army, May 1, 2015) 3-24.

195. Allyn and Carson, Energy Security.

196. Legal Information Institute, “10 U.S. Code § 2925: Annual Department of Defense Energy Management Reports,” Cornell Law School, https://www.law.cornell.edu/uscode /text/10/2925 (accessed September 19, 2018).

197. Combined Arms Center Training, *Synthetic Training Environment (STE) White Paper*,

198. Lisa Ferdinando, “Fort Bliss Unveils Army’s First Microgrid,” *ARNEWS*, May 17, 2013, https://www.army.mil/article/103577/fort_bliss_unveils_armys_first_microgrid (accessed November 20, 2018).

199. Robert Bryce, “Why Wind Power Isn’t the Answer,” *City Journal*, October 30, 2018, https://www.city-journal.org/wind-power-is-not-the-answer (accessed December 24, 2018).

200. Skully Capital, *Examination of Federal Financial Assistance in the Renewable Market: Implications and Opportunities for Commercial Deployment of Small Modular Reactors*, October 2018, https://www.energy.gov/ne/downloads/report-examination-federal-financial-assistance-renewable-energy-market, (accessed December 10, 2018).

201. Joskow, “The Future of the Electric Grid,” 4.

202. Executive Office of the President 2013, “Economic Benefits of Increasing Electric Grid Resilience to Weather Outages,” Energy.gov, August 2013, https://www.energy.gov/ sites/prod/files /2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf (accessed December 11, 2018)

203. Koppel, *Lights Out*, 100.

204. U.S. Department of Energy, “Transforming the Nation’s Electricity System,” *Quadrennial Energy Review, Second Installment*, January 2017, https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf (accessed February 5, 2019).

205. Frank R. Spellman and Revonna M. Bieber, *Energy Infrastructure Protection & Homeland Security*, (Washington, D.C.: Government Institutes, 2010), 15-21.

206. Spellman and Bieber, Energy Infrastructure Protection.

207. Donald J. Trump, "Presidential Executive Order: Promoting Energy Independence and Economic Growth."

208. Trump, Promoting Energy Independence.

209. Office of Nuclear Energy, "Advanced Small Modular Reactors (SMR)," Energy.gov, https://www.energy.gov/ne/nuclear-reactor-technologies/small-modular-nuclear-reactors (accessed November 11, 2018).

210. U.S. Army Corps of Engineers, "Fuel Cells for Energy Security," Engineer Research and Development Center webpage, December 3, 2012,

https://www.erdc.usace.army.mil/Media/Fact-Sheets/Fact-Sheet-Article-View/Article/476732/fuel-cells-for-energy-security/ (accessed November 23, 2018).

211. Juan A. Vitali, Joseph G. Lathome, et al., *Mobile Nuclear Power Plants for Ground Operations*, (Washington, D.C.: U.S. Department of the Army, October 26, 2018).

212. Office of Nuclear Energy, "New DOE Report Examines How Incentives Used for Renewables Could Benefit Small Modular Reactors," *EE Online*, November 26, 2018, https://www.energy.gov/ne/articles/new-doe-report-examines-how-incentives-used-renewables-could-benefit-small-modular (accessed December 24, 2018).

213. Department of Energy, "Report Explores U.S. Advanced Small Modular Reactors to Boost Grid Resiliency," Energy.gov, January 25, 2018, https://www.energy.gov/ne/ articles /department-energy-report-explores-us-advanced-small-modular-reactors-boost-grid (accessed February 1, 2019).

214. U.S. Army Corp of Engineers, "Fuel Cells for Energy Security."

215. Jon Wellinghoff, “When the Lights Go Out,” *USA Today,* March 24, 2015, https://www.usatoday.com/story/news/2015/03/24/powergridblackout/24963123/ (accessed October 10, 2018).

216. Larry Greenemeier, “Here’s What a Cyber Warfare Arsenal Might Look Like, Stuxnet Was Just The Beginning, as Malware Becomes the New Nuclear Option,” *Scientific American* website, May 6, 2015, https://www.scientificamerican.com/article/here-s-what-a-cyber-warfare-arsenal-might-look-like/ (accessed Oct 10, 2018).

217. Greenemeier, Here’s What a Cyber Warfare Arsenal Might Look Like.

218. Cloherty and Thomas, “Trojan Horse’ Bug Lurking in Vital U.S. Computers Since 2011”

219. Manimaran Govindarasu and Adam Hahn, “As Russians Hack the U.S. Grid, a Look at What’s Needed to Protect It,” *The Conversation*, August 7, 2018, https://theconversation.com/as-russians-hack-the-us-grid-a-look-at-whats-needed-to-protect-it-100489, (accessed January 3, 2019).

220. Govindarasu and Hahn, “As Russians Hack the U.S. Grid, a Look at What’s Needed to Protect It.”

221. Vitali, et al., “Mobile Nuclear Power Plants for Ground Operations.”

222. Barrack Obama, “Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience,” The White House: President Obama Archives, https://www.dhs.gov/cisa/national-infrastructure-protection-plan (accessed January 23, 2019).

223. “What Is the Liberal International Order?” The German Marshall Fund of the United States, January 2, 2019, http://www.gmfus.org/publications/what-liberal-international-order (accessed January 30, 2019).

224. “Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World,” Office of the Chairman of the Joint Chiefs of Staff, July 14, 2016, https://www.jcs.mil/

Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917 (accessed January 30, 2019).

225. Robert E. Litan, "The "Globalization" Challenge: The U.S. Role in Shaping World Trade and Investment," The Brookings Institution, July 28, 2016, https://www.brookings.edu/articles/the-globalization-challenge-the-u-s-role-in-shaping-world-trade-and-investment/ (accessed March 25, 2019).

226. "Joint Concept for Integrated Campaigning," Office of the Chairman of the Joint Chiefs of Staff, March 16, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257 (accessed March 27, 2019).

227. "10 U.S. Code § 14501 - Failure of Selection for Promotion," Legal Information Institute, https://www.law.cornell.edu/uscode/text/10/14501 (accessed March 18, 2019).

228. "New Research Shows Increasing Physician Shortages in Both Primary and Specialty Care," Association of American Medical Colleges News, April 11, 2018, https://news.aamc.org/press-releases/article/workforce_report_shortage_04112018/ (accessed December 16, 2018).

229. Benjamin F. Mundell, "Retention of Military Physicians: The Differential Effects of Practice Opportunities Across the Three Services," RAND Corporation, 2010, https://www.rand.org/content/dam/rand/pubs/rgs_dissertations/2010/RAND_RGSD275.pdf (accessed March 27, 2019).

230. Will Morris, "Shortage of Civilian Doctors in Military Hospitals Causing Treatment Problems," *Stars and Stripes*, November 29, 2018, https://www.stripes.com/news/shortage-of-civilian-doctors-in-military-hospitals-causing-treatment-problems-1.558417 (accessed March 27, 2019).

231. "Physician Benefits & Salary," *Army Medicine*, U.S. Army Homepage, https://www.goarmy.com/amedd/physician/benefits.html (accessed January 05, 2019).

232. “Salary for Physician - Emergency Room in the United States,” Salary.com, https://www1.salary.com/ER-Doctor-Salary.html (accessed January 05, 2019).

233. Leo Shane III, “VA to Use DOD’s Electronic Medical Records System,” Reboot Camp, *Military Times*, October 16, 2017, https://rebootcamp.militarytimes.com/news/pentagon-congress/2017/06/05/va-to-use-dod-s-electronic-medical-records-system/ (accessed January 26, 2019).

234. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed March 26, 2019).

235. Thomas P. Galvin, “Military Preparedness,” Faculty Paper (Carlisle, PA: US Army War College, 2019).

236. “Embedding Culture,” High Growth, March 19, 2011, https://highgrowth.com/embedding-culture/ (accessed January 29, 2019).

237. Carl Forsling, “The ‘Up-Or-Out’ Promotion System Hurts the Military,” Task and Purpose, October 19, 2016, https://taskandpurpose.com/military-needs-abandon-promotion-boards (accessed March 26, 2019).

238. United States Government Accountability Office, “Military Personnel Additional Actions Needed to Address Gaps in Military Physician Specialties,” (Washington, DC, February 2018), https://www.gao.gov/assets/700/690409.pdf (accessed March 27, 2019).

239. Maggie Mahar, “AHLTA Continues to Disappoint,” *Health Beat*, Healthbeatblog.com, http://healthbeatblog.com/2008/08/ahlta-continues/ (accessed March 26, 2019).

240. “Full Body Health Scanners to Aid Early Diagnosis,” *Reach MD*, April 2, 2018, https://reachmd.com/news/full-body-health-scanners-to-aid-early-diagnosis/1615130/ (accessed March 14, 2019).

241. Ronald W. Wolf, “Army Virtual Health: Meeting the Needs of the Soldier Today and Tomorrow,” U.S. Army Homepage, October 5, 2017, https://www.army.mil/article/194468/army_virtual_heatlh_meeting_the_needs_of_the_soldier_today_and_tomorrow (accessed March 26, 2019).

242. Kyle Jahner, “Surgeon General Outlines Future of Army Medicine,” *Army Times*, August 7, 2017, https://www.armytimes.com/your-army/2015/10/12/surgeon-general-outlines-future-of-army-medicine/ (accessed March 14, 2019).

243. Mesko Bertalan, “Medical Drones Will Thrive in Healthcare: A Safe Road to Health,” *The Medial Futurist*, August 13, 2018, https://medicalfuturist.com/medical-drones (accessed March 27, 2019).

244. “Army Values,” *U.S. Army Mobile*, U.S. Army Homepage, https://www.army.mil/mobile/ (accessed January 06, 2019).

245. “Mobile Health Apps,” *Mobile Health Technology Knowledge Hub*, Athenahealth, Inc. https://www.athenahealth.com/knowledge-hub/mobile-health-technology/apps (accessed January 06, 2019).

246. “Health Information Exchange,” The Office of the National Coordinator for Health Information Technology The Office of the National Coordinator for Health Information Technology The Office of the National Coordinator for Health Information TechnologyOffice of the National Coordinator for Health Information Technology , https://www.healthit.gov/topic/health-it-basics/health-information-exchange (accessed January 17, 2019).

247. “HIMSS Health Information and Technology Resource Library,” Healthcare Information and Management Systems Society (HIMSS), https://www.himss.org/library/interoperablity-standard/what-is (accessed January 26, 2019).

248. Dave Roos, “How to Leverage an API for Conferencing,” HowStuffWorks, November 23, 2007, https://money.howstuffworks.com/business-communications/how-to-leverage-an-api-for-conferencing2.htm (accessed January 26, 2019).

249. “MHS Genesis,” Military Health System Homepage, https://www.health.mil/Military-Health-Topics/Technology/Military-Electronic-Health-Record/MHS-GENESIS (accessed January 26, 2019).

250. MHS Genesis.

251. U.S. Medicine, “Electronic Records System Unreliable, Difficult to Use, Service Officials Tell Congress,” May 29, 2009, http://www.usmedicine.com/2009-issues/may-2009/electronic-records-system-unreliable-difficult-to-use-service-officials-tell-congress/ (accessed January 26, 2019).

252. MG Steven W. Ainsworth and COL John A. Stokes, Jr., “The Multiple Dimensions of Talent in the Army Reserve Soldier,” U.S. Army Homepage, June 26, 2018, https://www.army.mil/article/206867/the_multiple_dimensions_of_talent_in_the_army_reserve_soldier (accessed January 05, 2019).

253. Gigail Cureton, “New Program Teams Army Medicine with Civilian Hospitals,” U.S. Army Homepage, January 29, 2019, https://www.army.mil/article/216704/new_program_teams_army_medicine_with_civilian_hospitals (accessed March 27, 2019).

254. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed 10 February 2019).

255. Danielle Mary Catherine Wheeler, *Back in BRAC: A Predictive Model of Military Base Realignments, A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree Doctor of Public Administration*, College of Business and Public Management Department of Public and Health Administration, January 2016, https://search.proquest.com/docview/1758001299/fulltextPDF/450FA6F728E34EB2PQ/1?accountid=4444 (accessed 18 February 2019).

256. Nick Miroff, “Hacking, Cyberattacks Now the Biggest Threat to U.S., Trump’s Homeland Security Chief Warns,” *The Washington Post*, September 5, 2018, https://www.washingtonpost.com/world/national-security/

hacking-cyberattacks-now-the-biggest-threat-to-us-trumps-homeland-security-chief-warns/2018/09/05/d0045800-b119-11e8-a20b-5f4f84429666_story.html?utm_term=.06d3ff1c66b8 (accessed 20 February 2019).

257. Chloe Demrovsky, "Cyber Threats to Supply Chain on the Rise," *Global Trade Magazine*, June 5, 2016, http://www.globaltrademag.com/global-trade-daily/commentary/cyber-threats-to-supply-chain-on-the-rise/ (accessed 18 February 2019).

258. *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, The White House*, February 15, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua (accessed 20 February 2019).

259. "UAS Integration Pilot Program White House Fact Sheet," U.S. Department of Transportation, https://www.transportation.gov/sites/dot.gov/files/docs/briefing-room/288091/uas-integration-pilot-program-fact-sheet.pdf (accessed 20 February 2019).

260. UAS Integration Pilot Program White House Fact Sheet.

261. "Amazon Prime Air," Amazon.com, https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011 (accessed 20 February 2019).

262. "Ford and Walmart Collaborate to Design Automated-Vehicle Delivery," CNBC, November 14, 2018, https://www.cnbc.com/2018/11/14/ford-and-walmart-collaborate-to-design-automated-vehicle-delivery.html (accessed 20 February 2019).

263. W.J. Hennigan, "Experts Say Drones Pose a National Security Threat-and We Aren't Ready," *Time*, May 31, 2018, http://time.com/5295586/drones-threat/ (accessed 20 February 2019).

264. Hennigan, "Experts Say Drones Pose a National Security Threat-and We Aren't Ready,".

265. “About the Agency,” Defense Contract Management Agency website, https://www.dcma.mil/About-Us/, (accessed 26 January 2019).

266. “Intent/Outcome/Purpose,” Defense Contract Management Agency website, https://www.dcma.mil/Portals/31/Documents/Policy/DCMA-INST-1001.pdf (accessed 23 March 2019).

267. Lieutenant Colonel Rob Wolfe, *2016 Major Automated Information System Annual Report*: *Army Contract Writing System* (Alexandria, Virginia: Department of the U.S. Army, March 2016) https://apps.dtic.mil/dtic/tr/fulltext/u2/1019571.pdf (accessed 23 March 2019).

268. “Intent/Outcome/Purpose,” Defense Contract Management Agency.

269. U.S. Government Accountability Office, Report to Congressional Requesters, “Sole Source Contracting: Defining and Tracking Bridge Contracts Would Help Agencies Manage Their Use,” October 2015, https://www.gao.gov/assets/680/673110.pdf accessed 23 February 2019).

270. “Contracting Officer’s Representative (COR),” Defense Pricing and Contracting, https://www.acq.osd.mil/dpap/ccap/cc/jcchb/html/Topical/cor.html (accessed 18 February 2019).

271. “FAA Tests FBI Drone Detection System at JFK,” Federal Aviation Administration, July 1, 2016, https://www.faa.gov/news/updates/?newsId=85546 (accessed 20 February 2019).

272. “Simple Messaging, Reviews, and Insights for Local Business,” Podium website, https://go.podium.com/reputation-online-management/?_bt=257758420999&_bk=reputation%20management&_bm=p&_bn=g&_bg=67415304936&gclid=EAIaIQobChMI69-vtOPQ4AIVFovICh1yBwi5EAAYASAAEgLk0PD_BwE (accessed 22 February 2019).

273. James Vincent, “Artificial Intelligence is Going to Supercharge Surveillance: What Happens When Digital Eyes Get the Brains To Match?” *The Verge*, January 23, 2018, https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security (accessed 20 January 2019).

274. Tom Philpott, “Congress, DoD Step Toward Expanding Access to Commissaries, Exchanges,” Military.com, July 5, 2018. https://www.military.com/militaryadvantage/2018/07/05/congress-and-dod-step-toward-expanding-access-commissaries-and-exchanges.html (accessed 22 February 2019).

275. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, (accessed February 6, 2019).

276. Headquarters, U.S. Army Training and Doctrine Command, “The U.S. Army in Multi-Domain Operations 2028,” *TRADOC 525-3-1*, (Fort Eustis, VA: Headquarters U.S. Army Training and Doctrine Command, December 6, 2018), 20.

277. Max Boot, *A New American Way of War*, Foreign Affairs https://www.foreignaffairs.com/articles/united-states/2003-07-01/new-american-way-war. (accessed December 12, 2018).

278. Jeffrey Engstrom, “Systems Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare,” RAND (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf (accessed January 31, 2018).

279. Engstrom, Systems Confrontation.

280. U.S. Joint Chiefs of Staff, “Joint Operating Environment 2035,” (Washington, DC: U.S. Joint Chiefs of Staff, July 14, 2016), https://www.airuniversity.af.mil/Portals/10/CMSA/documents/Required_Reading/Joint%20Operating%20Environment%202035%20The%20Joint%20Force%20in%20a%20Contested%20and%20Disordered%20World.pdf (accessed September 21, 2018).

281. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, (accessed February 6, 2019).

282. Headquarters, U.S. Army Training and Doctrine Command, "The U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade: 2025-2045," *TRADOC 525-3-8*, (Fort Eustis, VA: Headquarters U.S. Army Training and Doctrine Command, December 6, 2018), 7-8.

283. Donald J. Trump, National Security Strategy, (Washington D.C.: The White House, December 2017), 3, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed November 28, 2018).

284. Trump, National Security Strategy, 4.

285. Trump, National Security Strategy, 7, 11, 26.

286. Headquarters, U.S. Army Training and Doctrine Command, "The U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade: 2025-2045," *TRADOC 525-3-8*, (Fort Eustis, VA: Headquarters U.S. Army Training and Doctrine Command, December 6, 2018), 7.

287. John P. Kotter, *Leading Change*, (Boston, MA: Harvard Business Review Press, 1996), 42-43.

288. Headquarters, U.S. Army Training and Doctrine Command, "The U.S. Army in Multi-Domain Operations 2028," *TRADOC 525-3-1*, (Fort Eustis, VA: Headquarters U.S. Army Training and Doctrine Command, December 6, 2018), A-1.

289. Mattis, *Summary of the 2018 National Defense Strategy*, 3.

290. Mattis, *Summary of the 2018 National Defense Strategy*, 7.

291. Francis J.H. Park, "Global Integration 2018 National Military Strategy Joint Strategic Planning System," *Directorate for Strategy, Plans, and Policy (J-5) Briefing Slides,* (Washington D.C.: U.S. Joint Chief of Staff), https://armywarcollege.blackboard.com/bbcswebdav/courses/19WF2200012R1/Faculty%20Addendums/SLIDES/TSC-02/COL%20Park%20GI_NMS_JSPS%20Brief.pptx (accessed November 28, 2018).

292. Joseph Dunford, Jr., "From the Chairman: Maintaining a Boxer's Stance," *Joint Force Quarterly*, (86, 3rd Quarter 2017), https://ndupress.ndu.edu/Publications/Article/1218381/from-the-chairman-maintaining-a-boxers-stance/ (accessed November 28, 2018), 2-3.

293. U.S. Army War College, "The Military's Domestic Imperative: Homeland Defense & Defense Support of Civil Authorities," *Theater Strategy and Campaigning Briefing Slides*, (Carlisle Barracks, PA: U.S. Army War College, January 3, 2019), https://armywarcollege.blackboard.com/bbcswebdav/courses/19WF2200012R1/Faculty%20Addendums/SLIDES/TSC-16/TSC16%20HD%20%26%20DSCA%20%28Pesile%29.pptx (accessed January 4, 2019).

294. Jennifer K. Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, (Washington D.C.: Congressional Research Service, R42659, Version 7, November, 6 2018), https://fas.org/sgp/crs/natsec/R42659.pdf (accessed January 9, 2019), 21-22.

295. Jeh Charles Johnson, *U.S. Department of Homeland Security (DHS) Strategic Plan for Fiscal Years (FY) 2014-2018*, (Washington D.C.: U.S Department of Homeland Security), 6.

296. U.S. Department of Homeland Security, *National Prevention Framework*, (Washington D.C.: U.S. Department of Homeland Security, June 2016), 3-4.

297. Kirstjen Nielsen, "Secretary Nielsen Remarks at AUSA Annual Meeting and Exhibition: As Prepared For Delivery," *U.S. Department of Homeland Security News*, https://www.dhs.gov/news/2018/10/09/secretary-nielsen-remarks-ausa-annual-meeting-and-exhibition-prepared-delivery (accessed January 15, 2019).

298. U.S. Northern Command, *About USNORTHCOM*, http://www.northcom.mil/About-USNORTHCOM/ (accessed January 8, 2018).

299. Lori J. Robinson, Statement of Commander, United States Northern Command and North American Aerospace Defense Command Before the Senate Armed

Services Committee, (February 15, 2018), http://www.northcom.mil/Portals/28/Robinson_02-15-18%20SASC%20Testimony.pdf?ver=2018-02-15-105546-867 (accessed January 27, 2019).

300. U.S. Joint Chiefs of Staff, "Homeland Defense," *Joint Publication 3-27*, (Washington D.C.: U.S. Joint Chief of Staff, April 10, 2018), 51.

301. U.S. Department of Defense, *Strategy for Homeland Defense and Defense Support of Civil Authorities,* (Washington D.C.: Department of Defense, February 2013), https://apps.dtic.mil/docs/citations/ADA582464 (accessed January 22, 2019).

302. Zack Coleman, "Pentagon: Climate Change Threatens Military Installations," *Politico*, (January 18, 2019), https://www.politico.com/story/2019/01/18/pentagon-military-installations-climate-1098095 (accessed March 24, 2019).

303. Mark T. Esper and Mark A. Milley, "Statement by the Secretary of the Army and Chief of Staff United States Army before the Senate Armed Services Committee," *Posture of the United States Army* (April 12, 2018), https://www.armed-services.senate.gov/imo/media/doc/Esper-Milley_04-12-18.pdf (accessed November 25, 2018).

304. U.S. Army Training and Doctrine Command, *The Operational Environment and the Changing Character of Future Warfare,* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, May 31, 2017), 3.

305. U.S. Army Combined Arms Center, "Doctrine 2015 Information Briefing," (Fort Leavenworth, KS: U.S. Army Combined Arms Center), https://usacac.army.mil/cac2/adp/Repository/Doctrine%202015%20Briefing%2029%20FEB%202012.pdf (accessed March 25, 2019).

306. U.S. Department of the Army, "Operations," *Army Doctrine Reference Publication 3-0*, (Washington D.C.: U.S. Department of the Army, October 2017), 33.

307. U.S. Department of the Army, "Operations, 35.

308. U.S. Department of the Army, "Operations, 45.

309. Luis Simon, “Demystifying the A2/AD Buzz,” *War on the Rocks*, (January 04, 2017), https://warontherocks.com/2017/01/demystifying-the-a2ad-buzz/ (accessed February 23, 2019).

310. U.S. Army Judge Advocate General’s Legal Center and School, *Operational Law Handbook*, (Charlottesville, VA: U.S. Army Judge Advocate General’s Legal Center and School, 2017), http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2017.pdf (accessed February 21, 2019), 200.

311. U.S. Joint Chiefs of Staff, “Homeland Defense,” *Joint Publication 3-27*, (Washington D.C.: U.S. Joint Chief of Staff, April 10, 2018), 26-27.

312. U.S. Department of the Army, “Stability,” *Army Doctrinal Reference Publication 3-07* (Washington D.C.: U.S. Department of the Army, August 2012), 14-15.

313. U.S. Joint Chiefs of Staff, “Homeland Defense,” *Joint Publication 3-27*, (Washington D.C.: U.S. Joint Chief of Staff, April 10, 2018), 34.

314. *The Office of the Assistant Chief of Staff for Installation Management Home Page*, www.acsim.army.mil (accessed November 23, 2018).

315. U.S. Department of the Army Installation Management Command, “Organization, Mission and Functions U.S. Army Installation Management Command,” *IMCOM Regulation 10-1*, (San Antonio, TX: U.S. Department of the Army, March 2, 2015), 3.

316. David D. Halverson, *IMCOM 2025 and Beyond*, (U.S. Army Installation Management Command, November 2014), http://www.benning.army.mil/Garrison/Sustainability/content/pdf/2025%20and%20Beyond.pdf (accessed January 22, 2019).

317. Ash Carter, *Department of Defense Mission Assurance Strategy*, (Washington D.C: Department of Defense, April 2012), 1.

318. Carter, *Department of Defense Mission Assurance Strategy*, 16-17.

319. Headquarters, U.S. Army Training and Doctrine Command, "The U.S. Army in Multi-Domain Operations 2028," *TRADOC 525-3-1*, (Fort Eustis, VA: Headquarters U.S. Army Training and Doctrine Command, December 6, 2018), C-2.

320. Patrick Duggan, "How the Enemy Could Hit the U.S. Army at Home," *War On The Rocks*, https://warontherocks.com/2017/08/how-the-enemy-could-hit-the-u-s-army-at-home/ (accessed October 22, 2018).

321. U.S. Joint Chiefs of Staff, Joint Operating Environment 2035 (JOE 2035), Version 1.0 (Washington, DC: U.S. Joint Chiefs of Staff, July 14, 2016), https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917 (accessed March 27, 2019). 24.

322. U.S. Joint Chiefs of Staff, Joint Operating Environment 2035, 26-27.

323. Donald J. Trump, National Security Strategy of the United States of America, (Washington, DC: The White House, December 2017) https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed February 7, 2019).4.

324. Trump, National Security Strategy, 12.

325. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed February 7, 2019). 3.

326. U.S. Joint Chiefs of Staff, Joint Operating Environment 2035, 24-25.

327. U.S. Joint Chiefs of Staff, Joint Operating Environment 2035, 26.

328. U.S. Joint Chiefs of Staff, Joint Operating Environment 2035, 9.

329. Mattis, Summary of the 2018 National Defense Strategy, 3.

330. Mattis, Summary of the 2018 National Defense Strategy, 1.

331. Summary of the 2018 Department of Defense Artificial Intelligence Strategy, 5.

332. Summary of the 2018 Department of Defense Artificial Intelligence Strategy, 5-6.

333. David Grossman, "Googly-Eyed Robots Are Coming to Hundreds of Grocery Stores", *Popular Mechanics,* (January 14, 2019), https://www.popularmechanics.com/technology/robots/a25896081/marty-giant-robot-grocery-stores/ (accessed March 26, 2019).

334. Steve Reinharz, "Combining Man and Machine", Security Industry Association (September 1, 2017), https://www.securityindustry.org/2017/09/01/robots-guards/ (accessed on March 28, 2019).

335. Kara Klein, "Key Factors Driving Robotic Technology Adoption in the Security Industry: Top Statistics From SIA's Report", Security Industry Association, (February 18, 2019), https://www.securityindustry.org/2019/02/18/key-factors-driving-robotic-technology-adoption-in-the-security-industry/ (accessed March 29, 2019)

336. Sonitrol Security, "How Artificial Intelligence Will Help The Physical Security Industry", (Fresno, CA: Kimberlite Corporation, March 2019), https://sonitrolsecurity.com/how-artificial-intelligence-will-help-the-physical-security-industry/ (accessed March 12, 2019).

337. Jacob Morgan, "A Simple Explanation Of 'The Internet Of Things'", *Forbes Magazine,* (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#e3bf26f1d091 (accessed March 20, 2019).

338. James A. Lewis, "How Will 5G Shape Innovation and Security: A Primer", A Report of the CSIS Technology Policy Program, Center for Strategic and International Studies (Washington, D.C., December, 2018) https://www.csis.org/analysis/

how-5g-will-shape-innovation-and-security (accessed March 2, 2019). 6.

339. Lewis, “How Will 5G Shape Innovation and Security, 5.

340. DOD Manual 5200.08 Volume 3, Physical Security Program: Access To DOD Installations, (Washington, DC: US Department of Defense January 2, 2019) https://fas.org/irp/doddir/dod/m5200_08_v3.pdf (accessed March 10, 2019), 1-2.

341. Automated Installation Entry fact sheet, Joint Program Executive Office Chemical and Biological Defense (Aberdeen Proving Ground, MD: U.S. Department of Defense, December 2015), https://jacks.jpeocbd.osd.mil/Public/FactSheetProvider.ashx?productId=358 (accessed March 2, 2019).

342. Kevin Palgutt (February 5, 2019), Office of the Army Provost Marshal General (OPMG) Physical Security Branch, email message to author.

343. Automated License Plate Recognition Technology, International Association of Chiefs of Police (Alexandria, VA: International Association of Chiefs of Police), https://www.theiacp.org/projects/automated-license-plate-recognition (accessed March 12, 2019).

344. AI Based Vehicle Recognition, Deep Vision (Atlanta, GA: Deep Vision AI), https://www.deepvisionai.com/landings/computer-vision-vehicle-recognition (accessed March 12, 2019).

345. Weighing In Motion (WIM) Scales, (Arlington, TX: General Electrodynamics Corporation) http://www.gecscales.com/truck-scales/wim-weighing-motion-scales/ (accessed March 12, 2019).

346. Cargo and Vehicle Inspection Systems, (Torrance, CA: Rapiscan Systems, An OSI Systems Company) https://www.rapiscansystems.com/en/products/category/cargo-and-vehicle-inspection (accessed March 12, 2019).

347. DOD Manual 5200.08 Volume 3, Physical Security Program: Access To DOD Installations, (Washington, DC: US

Department of Defense January 2, 2019) https://fas.org/irp/doddir/dod/m5200_08_v3.pdf (accessed March 10, 2019), 9.

348. U.S. Department of the Army, "Intrusion Detection Systems", *Army Regulation 190-13* (Washington, DC: U.S. Department of the Army, February 25, 2011), 31.

349. Kevin Palgutt, (March 29, 2019), Department of the Army Office of the Provost Marshal General Physical Security Branch, telephone conversation with author cited with permission.

350. Mobile Robotics for Physical Security of Critical Infrastructure, (Burlingame, CA: SMP Robotics Systems Corporation) https://smprobotics.com/application_autonomus_mobile_robots/robotics_physical_security/ (accessed March 12, 2019)

351. Kevin Palgutt (March 29, 2019), Department of the Army Office of the Provost Marshal General Physical Security Branch, telephone conversation with author cited with permission.

352. U.S. Department of the Army, "Intrusion Detection Systems", Army Regulation 190-13 (Washington, DC: U.S. Department of the Army, February 25, 2011), 31.

353. Department of the Army, "Intrusion Detection Systems, 12.

354. Sydney J. Freedberg, Jr, "Army Bets Big On Service Contracts To Fix Aging IT," *Breaking Defense*, (March 5, 2019), https://breakingdefense.com/2019/03/army-bets-big-on-service-contracts-to-fix-aging-it/?utm_campaign=Raytheon%202019%20AUSA%20Global%20Force&utm_source=hs_email&utm_medium=email&utm_content=71203052&_hsenc=p2ANqtz-9eAT-G1We5BOqXCLqMP3HURvK3rbSub0jNbm_0mxzSX0g-Zm3gkKK-9hIC7EE38eC7JOnGMie9gjav6O3ukzmZzF8L-J71A&_hsmi=71203052 (accessed on March 26, 2019).

355. Summary of the 2018 Department of Defense Artificial Intelligence Strategy, 13.

356. Summary of the 2018 Department of Defense Artificial Intelligence Strategy, 16.

357. Defense Advanced Research Projects Agency, "AI Next Campaign", https://www.darpa.mil/work-with-us/ai-next-campaign (accessed March 18, 2019).

358. COL Anthony (Che) Bolden (March 25, 2019), G-7 Marine Corps Installation Command, briefing and discussion to US Army War College Futures Seminar.

359. Donald J. Trump, President of the United States, "*National Security Strategy 2017*," December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, p1, (accessed 16 March, 2019).

360. James Mattis, Secretary of Defense, "*National Defense Strategy 2018,*" Sharpening the Military's Competitive Edge, Strategic Environment p3, USAWC Blackboard.

361. Headquarters, U.S. Army Training and Doctrine Command, "The U.S. Army in Multi-Domain Operations 2028," *TRADOC 525-3-1*, (Fort Eustis, VA: Headquarters U.S. Army Training and Doctrine Command, December 6, 2018) https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf, (accessed 1 March, 2019).

362. Federal Aviation Administration (FAA), Regulations and Policies Handbook, Chapter 15, p 15-3, https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/phak/media/17_phak_ch15.pdf, (accessed 27 March 2019).

363. Federal Aviation Administration (FAA), Regulations and Policies Handbook.

364. Federal Aviation Administration (FAA), Restricted or Special Use Airspace, https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_restrictions/tfr/, (accessed 27 March, 2019).

365. David Sherpardson, "*FAA Bans Drones Over U.S. Military Bases Due To Security Risks*," Military Times, 8, April 2017, https://www.militarytimes.com/news/pentagon-congress/2017/04/08/faa-bars-drones-over-u-s-military-bases-due-to-security-risks/, (accessed 26 March, 2019).

366. Eric Limer, “Gatwick Airport Shut Down Due to ‘Deliberate’ Drone Interference,” *Popular Mechanics*, 20 December 2018, https://www.popularmechanics.com/flight/drones/a25641077/gatwick-airport-drones/, (accessed 1 March, 2019) and Katy Watson, “Venezuela President Maduro Survives ‘drone Assassination Attempt,’” *BBC News*, 5 August 2018, https://www.bbc.com/news/world-latin-america-45073385, (accessed 1 March, 2019).

367. Connie Lee, “Pentagon Exploring Counter-UAS Software,” *National Defense*, 6 January 2018, http://www.nationaldefensemagazine.org/articles/2018/6/1/pentagon-exploring-counter-uas-software, (accessed 3 March 2019).

368. iHLS startups, *Advanced Israeli Counter-Drone System to Be Supplied To The UK Army*,” RSS Air And Missile Defense, 26 August, 2018, https://i-hls.com/archives/85081, (accessed 23 February, 2019).

369. Seth J. Frantzman, “New Defense Budget Bill Foresees US-Israel counter-drone Cooperation, *Defense News*, 13 August, 2018, https://www.defensenews.com/unmanned/2018/08/13/new-defense-budget-bill-foresees-us-israel-counter-drone-cooperation/, (accessed 28 February, 2019).

370. 115th Congress, “*H.R.5515-John S. McCain National Defense Authorization Act for Fiscal Year 2019”,* 13 April, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5515/text, (accessed 2 March, 2019).

371. Corey Dickstein, Army Rolls Out New Field Manual Focused On Fighting Neer-Peer Adversaries, Stars And Stripes, 10 October, 2017, (accessed 21 March 2019).

372. Stand-To, The Official Focus of The U.S. Army, U.S. Army Training and Doctrine Command’s Army Capability Integration Center, 6 June, 2018, https://www.army.mil/standto/2018-06-06, (accessed 23 March, 2019).

373. Richard G. Kidd IV, “Threat To Posts: Army Must Rethink Base Security,” Association of the United States Army (AUSA), 21 December, 2017, https://www.ausa.org/articles/threats-posts-army-must-rethink-base-security, (accessed 22 March, 2019).

374. Elias Groll, “The Five Worst Attacks on U.S. Bases,” *Foreign Policy*, 17 September, 2013, https://foreignpolicy.com/2013/09/17/the-5-worst-attacks-on-u-s-bases/, (accessed 2 March, 2019).

375. United States Army War College, *Defense Management Primer For Senior Leaders*, 1st Edition, Department of Command, Leadership, And Management, School of Strategic Landpower, IX, USAWC Blackboard.

376. Umar Irfan, “*Hurricane Michael showed how woefully unprepared the military is for extreme weather*,” Vox, 16 October 2018, https://www.vox.com/2018/10/15/17978902/hurricane-michael-panama-city-tyndall-air-force-f22-climate-change, (accessed 25 March, 2019).

377. Thomas C. Hone, Norman Friedman, and Mark D. Mandeles, “*The Development Of The Angled-Deck Aircraft Carrier*,” Naval War College Review, (Vol 64, Number 2 Spring, Article 5, 2011), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1532&context=nwc-review, (accessed 26 March 2019).

378. National Aeronautics and Space Administration, Global Climate Change, “*Vital Signs of the Planet,”* https://climate.nasa.gov/effects/, (accessed 23 February, 2019).

379. Caitlin Werrell and Francesco Femia, “*Army Assistant Secretary Nominee on Whether or Not Climate Change Affects the Military: “Absolutely.”* The Center for Climate and Security, 22 Aug, 2018, https://climateandsecurity.org/2018/08/23/army-assistant-secretary-nominee-on-whether-or-not-climate-change-affects-the-military-absolutely/amp/, (accessed 19 March, 2019).

380. U.S. Legal, “*Posse Comitatus Act Law and Legal Definition*,” Legal Definitions, https://definitions.uslegal.com/p/posse-comitatus-act/, (accessed 2 February, 2019).

381. Department of Homeland Security (DHS), Mission, https://www.dhs.gov/about-dhs, (accessed 23 March, 2019).

382. DoD Directive 3000.09, “Autonomy in Weapon Systems,” November 21, 2012 incorporating change 1 May 8, 2017,

https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf, (accessed 23 March, 2019).

383. United States Army War College, *Defense Management Primer For Senior Leaders*, 4.

384. Secretary of Defense, James Mattis, "*National Defense Strategy 2018,*" Sharpening the Military's Competitive Edge, Strategic Environment, 2, USAWC Blackboard.

385. CSA Mark Milley, 39th Chief of Staff of the Army Initial Message to the Army, Memorandum, https://www.army.mil/e2/rv5_downloads/leaders/csa/Initial_Message_39th_CSA.pdf, (accessed 19 March, 2019).

386. Timothy Hale, "*CSA Milley: 'Readiness is my No 1 Priority*'" 27 April 2017, https://www.army.mil/article/166838/csa_milley_readiness_is_my_no_1_priority, (accessed 19 March, 2019).

387. Mattis, "*National Defense Strategy 2018,*" 1.

388. Donald J. Trump, National Security Strategy of the United States of America (Washington, DC: The White House, December 18, 2017), https://whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed October 13, 2018), 20.

389. Trump, National Security Strategy, 24.

390. Richard Kidd, "Installations of the Future: Providing the backbone for Army to prepare and engage in war," (Presentation slides from AY19 Futures Seminar class, October 26, 2018), 3.

391. Artem A. Kosorukov, "Digital Government Model: Theory and Practice of Modern Public Administration," Journal of Legal, Ethical and Regulatory Issues (20, no. 3 2017), 3.

392. Tim O'Reilly, "Government as a Platform," Innovations, Vol. 6, no. 1 (2010), 17.

393. Kosorukov, "Digital Government Model," 4.

394. O'Reilly, "Government as a Platform," 13.

395. O'Reilly, "Government as a Platform," 14.

396. Kosorukov, "Digital Government Model," 1-2.

397. Kosorukov, "Digital Government Model," 3-4, 6.

398. O'Reilly, "Government as a Platform," 14.

399. Kosorukov, "Digital Government Model," 9.

400. Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Haner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari, Andrej Zwitter, "Will Democracy Survive Big Data and Artificial Intelligence," *Scientific American* (February 25, 2017) https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ (accessed February 2, 2019), 15.

401. Cleveland Clinic, "No. 2 Medical Innovation for 2019: The Advent of AI in Healthcare," *ConsultQD* (October 31, 2018) https://consultqd.clevelandclinic.org/no-2-medical-innovation-for-2019-the-advent-of-ai-in-healthcare/ (accessed February 2, 2019), 1.

402. Raghav Bharadwaj, "AI in Government – Current AI Projects in the Public Sector," *Emerj* (December 13, 2018) https://emerj.com/ai-sector-overviews/ai-government-current-ai-projects-public-sector/ (accessed February 2, 2019), 4.

403. Kevin McCaney, "4 Example of How AI Can Make Cities Smarter," *GovernmentCIO Media & Research* (March 22, 2018) https://www.governmentciomedia.com/4-examples-how-ai-can-make-cities-smarter (accessed February 2, 2019), 2.

404. Metro21: Smart Cities Institute, "Fire Risk Analysis: Predicting Fire Risk to Prioritize Commercial Property Fire Inspections," (Pittsburgh, PA: Carnegie Mellon University, August 14, 2018), https://www.cmu.edu/metro21/projects/fire-risk-analysis.html (accessed January 26, 2019), 1.

405. *The United States Army Installation Management Command Home Page*, https://home.army.mil/imcom/index.php/about/mission-and-vision (accessed March 25, 2019).

406. U.S. Department of Defense, *Summary, 2018 DoD Artificial Intelligence Strategy* (Washington, DC: U.S. Department of

Defense, February 12, 2019), https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (accessed February 13, 2019), 4.

407. George E. P. Box, Norman R. Draper, "Empirical Model-Building and Response Surfaces," (Hoboken, NJ: Wiley, January 16, 1987), 424.

408. Kenneth R. Dahl, "FY19 Installation Management Command Annual Command Guidance," *Memorandum for Distribution* (Joint Base San Antonio Fort Sam Houston, TX: IMCOM, August 20, 2018), 2.

409. Dahl, "FY19 Installation Management Command Annual Command Guidance, 4.

410. Dahl, "FY19 Installation Management Command Annual Command Guidance, 2.

411. Kosorukov, "Digital Government Model," 6.

412. U.S. Department of Defense, *Summary, Department of Defense Cyber Strategy, 2018* (Washington, DC: U.S. Department of Defense 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed September 21, 2018), 4.

413. Daniel S. Hoadley and Nathan J. Lucas, *Artificial Intelligence and National Security* (Washington, DC: U.S. Library of Congress, Congressional Research Service, April 26, 2018), 27.

414. Michelle de Guzman-Watson, "ESPORTS warrior wanted: Army seeks Soldiers for competitive online gaming team," (December 7, 2018) https://www.army.mil/article/214760/esports_warriors_wanted_army_seeks_soldiers_for_competitive_online_gaming_team (accessed March 5, 2019), 1, quoting MG Frank Muth, U.S. Army Recruiting Command commander.

415. U.S. Department of the Army, "Installations of the Future: What Today's Soldiers Want for Tomorrow's Installations," *A Report of Site Visits with Young Solders* (Washington, DC: U.S. Army Office of the Assistant Chief of Staff for Installation Management, August 30, 2018), 14.

416. Department of Defense, *Summary, Department of Defense Cyber Strategy*, 7.

417. “Department of the Army Information Security Program,” *Army Regulation 380-5* (September 29, 2000) https://armypubs.army.mil (accessed March 5, 2019), 1.

418. Trump, *National Security Strategy*, 22.

419. Kosorukov, “Digital Government Model,” 1-4.

420. Tom Vander Ark, “How Cities Are Getting Smart Using Artificial Intelligence,” *Forbes* (June 26, 2018) https://www.forbes.com/sites/tomvanderark/2018/06/26/how-cities-are-getting-smart-using-artificial-intelligence/#7f7401a53803 (accessed February 2, 2019), 4.

421. Headquarters, U.S. Army Training and Doctrine Command, *The Army in Multi-Domain Operations 2028,* TRADOC Pamphlet 525-3-1 (Fort Eustis, VA: Headquarters, U.S. Army Training and Doctrine Command, December 6, 2018), https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf (accessed December 12, 2018), 20.

422. Daniel R. Coats, “Statement for the Record Worldwide Threat Assessment of the US Intelligence Community,” (Washington, DC: Director of National Intelligence, January 29, 2019), 15-16.

423. Kidd, “Installations of the Future,” 3.

424. Kidd, “Installations of the Future,” 2.

425. Dahl, “FY19 Installation Management Command Annual Command Guidance,” 2.

426. Dahl, “FY19 Installation Management Command Annual Command Guidance,” 1.

427. Kidd, “Installations of the Future,” 2.

428. Training and Doctrine Command, *The Army in Multi-Domain Operations 2028,* 7.

429. James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: The Department of Defense, January 19, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed October 12, 2018), 3.

430. Department of Defense, *Summary, 2018 DoD Artificial Intelligence Strategy*, 11.

431. Kelsey Atherton, "Targeting the future of DoD's controversial Project Maven initiative," *C4ISRNET* (July 27, 2018) https://www.c4isrnet.com/it-networks/2018/07/27/targeting-th-future-of-the-dods-controversial-project-maven-initiative/ (accessed October 12, 2018), 2.

432. Kidd, "Installations of the Future," 2.

433. Jason Axelrod, "The Big Deal about Big Data," *The American City & County* (March 05, 2018), 2.

434. Department of Defense, *Summary, 2018 DoD Artificial Intelligence Strategy*, 11.

435. Department of Defense, *Summary, 2018 DoD Artificial Intelligence Strategy*, 5.

436. G. David Garson, "The Promise of Digital Government," *Digital Government: Principles and Best Practices* (Hershey, PA: Idea Group Publishing, 2003), 2.

437. Johann Höchtl, Peter Parycek, and Ralph Schöllhammer, "Big Data in the Policy Cycle: Policy Decision Making in the Digital Era," Journal of Organizational Computing and Electronic Commerce, 26 (2016), 3.

438. Donald J. Trump, National Security Strategy of the United States of America (Washington, DC: The White House, December 2017), https://www.whitehouse.gov/wp-content/uploads/ 2017/12/NSS-Final-12-18-2017-0905.pdf (accessed January 15, 2019).

439. Trump, National Security Strategy

440. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S.

Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed January 15, 2019).

441. “What is Big Data” *Dell*, https://www.dellemc.com/en-us/big-data/definitions.htm, (access, November 16, 2018).

442. Abhinav Rai, “What is Big Data: Types, Characteristics, Benefits, and Examples,” *upGrad*, (August 16, 2018), blog entry, https://www.upgrad.com/blog/what-is-big-data-types-characteristics-benefits-and-examples/ (accessed December 20, 2018)

443. “Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in billions),” *Statista: The Statistics Portal*, (November 2016), https://www.statista.com/statistics/ 471264/iot-number-of-connected-devices-worldwide/ (accessed January 10, 2019).

444. “World Population Prospects 2017,” *United Nations DESA/Population Division* https://population.un.org/wpp/DataQuery/ (accessed March 13, 2019).

445. “IDC Digital Universe Study: Big Data, Bigger Digital Shadows and Biggest Growth in the Far East,” *EMC Corporation sponsored study*, (2011), https://www.whizpr.be/upload/medialab/21/company/Media_Presentation_2012_DigiUniverseFINAL1.pdf (accessed January 10, 2019).

446. Doug Laney, “3D Data management: Controlling Data Volume, Variety and Velocity,” *Application Delivery Strategies*, META Group file 949, February 6, 2001.

447. “Moore’s Law,” *Moore’s Law*, http://www.mooreslaw.org/ (accessed January 12, 2019).

448. Hans A. Gunnoo, “Moore’s Law is Dying. Here’s How AI is Bringing it Back to Life!,” Towards Data Science, August 15, 2018 https://towardsdatascience.com/moores-law-is-dying-here-s-how-ai-is-bringing-it-back-to-life-c9a469bc7a5a (accessed January 12, 2019).

449. “High-Performance Computing (HPC),” *Techopedia*, https://www.techopedia.com/ definition/4595/high-performance-computing-hpc. (accessed January 11, 2019).

450. “Real Time Big-Data Analytics,” *Gigaspaces*, https://docs.gigaspaces.com/product _overview/real-time-analytics.html (accessed, March 13, 2019)

451. Patrick Shanahan, Department of Defense Cloud Strategy (Washington DC: U.S. Department of Defense, 2018), https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF (accessed March 15, 2019).

452. “High-Performance Computing (HPC),” *Techopedia*, https://www.techopedia.com/ definition/4595/high-performance-computing-hpc. (accessed January 11, 2019).

453. “Life at Exascale,” *Exascale Computing Project*, https://www.exascaleproject.org/what-is-exascale/ (accessed January 15, 2019)

454. “ECP Receives HPCwire Editors’ Choice Award for Best HPC Collaboration of Government, Academia, and Industry,” (November 13, 2018), *Exascale Computing Project*, *https://www.exascaleproject.org/ecp-receives-hpcwire-editors-choice-award-for-best-hpc-collaboration-of-government-academia-and-industry/* (accessed January 15,2019).

455. Aundre F. Piggee, “The Army’s New Start-Up,” Army Sustainment (50, no. 5 September, 2018): 3-4. https://search-proquest-com.usawc.idm.oclc.org/docview/ 2114589620?accountid=4444. (accessed 24 February 2019)

456. John Lucker, Susan K. Hogan, Trevor Bischoff, “Predictably inaccurate: The Prevalence and Perils of Bad Big Data,” *Deloitte Review*, issue 21, July 31, 2017, https://www2.deloitte.com/insights/us/en/deloitte-review/issue-21/analytics-bad-data-quality.html (accessed January 15, 2019).

457. Timo Elliott, “Can You Trust Your Big Data?”, *Digital Business & Business Analytics,* (February 7, 2018), blog entry, https://timoelliott.com/blog/2018/02/can-you-trust-your-big-data.html (accessed 14 March, 2019)

458. Timo Elliott, “How Trustworthy Is Big Data?,” *Brink News*, February 2, 2018 https://www.brinknews.com/how-trustworthy-is-big-data/ (accessed January 15, 2019).

459. Mattis, National Defense Strategy

460. Jason M. Woods, C.D.F.M. “Bots, Big Data, and Auditing the Military.” *The Armed Forces Comptroller* 63, no. 3 (Summer, 2018): 17-18. https://search-proquest-com.usawc.idm.oclc.org/docview/2181692410?accountid=4444. (accessed 24 February 2019)

461. “What is Consistent Data?” *Siemens Company,* https://support.industry.siemens.com /cs/document/5116353/what-is-consistent-data-?dti=0&lc=en-WW (accessed March 12, 2019)

462. Henning Lund, “Data Integrity: What is it and Why is it Important?,” Rapid Online, (February 15, 2017), blog entry, https://www.rapidonline.com/blog/data-integrity-what-and-why (accessed January 15, 2019).

463. “Data Consistency Explained,” *Recovery Specialists*, http://recoveryspecialties.com/dc01.html (accessed January 15, 2019).

464. M. Strohbach, J. Daubert, H. Ravkin, M. Lischka (2016) Big Data Storage. In: Cavanillas J., Curry E., Wahlster W. (eds) New Horizons for a Data-Driven Economy. Springer, Cham

465. Antony Adshead, “Big data storage: Defining Big Data and the Type of Storage it Needs,” *ComputerWeekly.com*, https://www.computerweekly.com/podcast/Big-data-storage-Defining-big-data-and-the-type-of-storage-it-needs (accessed March 14, 2019)

466. Shanahan, Department of Defense Cloud Strategy

467. Anders S. G. Andrae, “Total Consumer Power Consumption Forecast,” *Research Gate*, (October 2017), https://www.researchgate.net/publication/320225452_Total_Consumer_Power_Consumption_Forecast (accessed January 15, 2019).

468. "Most Power Consumed (MW)," *World's Top Data Centers*, (2014), http://worldstopdatacenters.com/power/ (accessed January 15, 2019).

469. "California ISO Glossary," *California Energy Commission*, https://www.energy.ca.gov/glossary/ISO_GLOSSARY.PDF (accessed January 15, 2019).

470. Donald J. Trump, National Cyber Security Strategy of the United States of America (Washington, DC: The White House, December 2017), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed January 15, 2019)

471. Lisa Ferdinando, "'Terabyte of Death' Cyberattack Against DoD Looms, DISA Director Warns, *US Department of Defense News, Defense Media Activity*," (Jan. 11, 2018), https://dod.defense.gov/News/Article/Article/1414146/terabyte-of-death-cyberattack-against-dod-looms-disa-director-warns/ (accessed March 12, 2019)

472. "Information Assurance Management," *Information Security Institute*, https://resources.infosecinstitute.com/job-titles/information-assurance-manager/#gref (accessed March 15, 2019)

473. Christine Taylor, "Big Data Security," *Datamation*, (June 27, 2017), https://www.datamation.com/big-data/big-data-security.html (accessed January 19, 2019)

474. Jeffery Cooper, "Three Ways Artificial Intelligence Can Improve Cyber Security," *Fifth Domain*, (November 27, 2018), https://www.fifthdomain.com/thought-leadership/2018/11/28/how-artificial-intelligence-can-improve-cyber-systems/ (accessed January 20, 2019).

475. Billy Mitchell, "Artificial Intelligence is the Heart of CIO Dana Deasy's Plan to Modernize the DOD," August 23, 2018, *FEDSCOOP*, https://www.fedscoop.com/artificial-intelligence-dod-strategy-cio-dana-deasy/ (accessed February 24, 2019)

476. James Mattis, “Secretary of Defense Jim Mattis Senate Armed Services Committee Written Statement for the Record (APRIL 26, 2018),” page 11 https://www.armed-services.senate.gov/imo/media/doc/Mattis_04-26-18.pdf (accessed March 4, 2019)

477. “Virtual Reality in Military,” *ThinkMobiles*, blog entry, https://thinkmobiles.com /blog/virtual-reality-military/ (accessed March 14, 2019)

478. Tuhin Bhatt, “Big Data is Helping Augmented Reality Deliver Massive Visual Entertainment,” *DataFloq,* https://datafloq.com/read/big-data-augmented-reality-deliver-entertainment/5556 (accessed March 5, 2019)

479. Jerel G. Nelson, “Integrated Infrastructure Investment Project Prioritization, Sequencing, and Optimization Process”, Facilities Management Workshop, 6-8 February, 2019, Slide 3

480. “AI is Giving Companies a Fighting Chance Against Cyber-Attacks”, *Venture Beat*, https://venturebeat.com/2019/02/08/ai-is-giving-companies-a-fighting-chance-against-cyberattacks-vb-live/ (accessed March 12, 2019)

481. Loryana L. Vie; Kevin N. Griffith; Lawrence M. Scheier; Paul B. Lester; and Martin E.P Seligman, “The Person-Event Data Environment: leveraging big data for studies of psychological strengths in soldiers” (2013).US Army Research. 316. http://digitalcommons.unl.edu/usarmyresearch/316 page 6-7

482. “Virtual Reality in Military,” *ThinkMobiles*, blog entry, https://thinkmobiles.com /blog/virtual-reality-military/ (accessed March 14, 2019)

483. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), 3 https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed October 13, 2018).

484. Mattis, *Summary of the 2018 National Defense Strategy,* 4.

485. Todd South, “The Army Must Better Protect Installations From Enemy Sabotage, Leaders Say,” *The Army Times Outline* (October 10, 2017), 1, https://www.armytimes.com/news/your-army/2017/10/10/the-army-must-better-protect-installations-from-enemy-sabotage-leaders-say/, (accessed October 17, 2018)

486. Intelligent Building LLC, “Fort Benning Installation of the Future,” 614 Fort Benning ~203 Installation of the Future v1.0-09122018, 1, (accessed March 26, 2019).

487. Intelligent Building LLC, “Fort Benning Installation of the Future,” 4-1.

488. Dr. Jason R. Dorvee, A Modern Army Needs Modern Installations, September 17, 2018, https://www.army.mil/article/211231/a_modern_army_needs_modern_installations, 1, (accessed November 7, 2018).

489. Katherine Hammack, Army Installations 2025, Assistant Secretary of the Army for Installations, Energy, and Environment (IE&E), (July 5, 2016), 21, https://www.army.mil/e2/c/downloads/454188.pdf (accessed March 2, 2019).

490. Hammack, Army Installations 2025, 21.

491. Verizon, SmartHub and Verizon FAQs, “What is SmartHub and what can it do for me?”, 1, https://www.verizonwireless.com/support/smarthub-faqs/, (accessed 27 March 2019).

492. MG Christopher J. Sharpsten, “Leveraging Internet of Things (IoT) Technology to Improve Theater Posture and Sustainment: SmartHub, February 14, 2019, 3, United States Central Command, Directorate of Logistics and Engineering (J4), Whitepaper.

493. MG Sharpsten, “Leveraging Internet of Things (IoT) Technology, 5.

494. Department of Defense (DoD) - Chief Information Officer, The DoD Recommendation for the Internet of Things (IoT), (Office of the Secretary of Defense, Washington D.C.), 1.

https://www.hsdl.org/?view&did=799676, (accessed March 28, 2019).

495. House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications Hearing. Washington: Federal Information & News Dispatch, Inc, 2018, 1. https://search-proquest-com.usawc.idm.oclc.org/docview/2076166721?accountid=4444. (accessed March 5, 2019).

496. Robert M. Scholander, “The Role of Trust in Communication Breakdowns in Disaster Situations.” Order No. MR58546, Simon Fraser University (Canada), 2008, 1, https://search-proquest-com.usawc.idm.oclc.org/docview/304323443?accountid=4444. (accessed March 6, 2019).

497. Headquarters, U.S. Army, *The Army in Multi-Domain Operations*: 2028 – Initial Coordination Draft v0.6h dtd, (August 7, 2018), 12, (accessed March 4, 2019).

498. Ultra-Electronics, Fence Systems, https://www.ultra-3eti.com/products/virtualfence-systems/ , 1, (accessed 7 March 2019).

499. Mattis, *2018 DoD Artificial Intelligence Strategy*, 3, https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF (accessed February 13, 2019).

500. Dr. Harold J. Arata III and Mr. Brian L. Hale, “Smart Bases, Smart Decisions”, *Cyber Defense Review*, July 31, 2018, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Smart%20Bases%20Smart%20Decisions_Arata_Hale.pdf?ver=2018-07-31-093711-343, (accessed March 2, 2019), 75.

501. Arata and Hale, Smart Bases, Smart Decisions, 72-73.

502. Arata and Hale, Smart Bases, Smart Decisions, 74.

THE
UNITED STATES
ARMY WAR COLLEGE

STRENGTH and WISDOM

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
http://www.carlisle.army.mil/

CSL Website

USAWC Website