The U.S. Army must change how it thinks about its military installations. Installations are not sanctuaries; they are vulnerable soft-targets for a growing host of sophisticated threats seeking to degrade U.S. Army combat capabilities long before they deploy. Now is the time to act and update U.S. Army installations or risk stifling current modernization efforts with an Industrial Age past.

With all the recent emphasis placed on modernization, how is it that U.S. Army installations are not included? If the primary reason installations exist is to ensure combat readiness, then what good is innovating new capabilities if they are increasingly vulnerable to future attacks? How effectively can the U.S. Army project combat power from Industrial Age installations that are designed more for their functional geography than as the first skirmish lines of asymmetric defense?

Industrial Age Installations

The advent of the Industrial Age provided the U.S. Army new means to more efficiently marshal, mobilize and deploy men and materiel across a sprawling country. The rapid pace of industrialization gave birth to numerous pivotal technologies like the telegraph, locomotives and the internal combustion engine, which all served to unlock the U.S. Army’s ability to move further away from water-based garrisons to more remote areas capable of being supplied by rails and roads.

This new functional geography permitted U.S. Army forts to spread across expanding frontiers. The forts served as self-contained small cities that provided Soldiers and their families some of the goods and services they could not find in austere local markets. Situated on key terrain, frontier


forts had high stockade fences, serpentine defenses and were manned by sentries with guns.\(^3\) They had clear fields of fire, few entry points and perimeter earthworks which channeled movement along over-watched terrain.\(^4\) The U.S. Army developed a fortress mindset about its installations, viewing them both as sanctuaries for Soldiers and families and as secure assembly areas that could be used before deploying troops outside their walls.\(^5\) The security of frontier forts was oriented on outside threats and remains the model emulated by U.S. Army installations today.

### Modernization

The U.S. Army is in the midst of profound technology change and faces increasingly complex challenges. Over the past 16 years, advances in adversary capabilities have eroded the U.S. Army’s technological superiority and pose sophisticated new challenges. This requires the re-examination of all readiness assumptions. Past ways of thinking, organizing and executing limit the U.S. Army’s ability to keep pace with technology and increasingly bold adversaries.\(^6\)

In October 2017, the U.S. Army launched a bold new strategy to modernize its capabilities development process that has been described as an Industrial Age model by the Chief of Staff of the Army.\(^7\) The goal of modernization strategy is to accelerate and fuse disparate research and development (R&D), experimentation and acquisition efforts into a more streamlined process that closes future combat readiness gaps and makes Soldiers and units more lethal.\(^8\) The strategy has six critical capability priorities: long-range precision fires, next generation combat vehicles, future vertical lift platforms, communication networks, air and missile defense and Soldier lethality systems.\(^9\) While modernizing these six critical capabilities is necessary and long overdue, excluding the sprawling information systems, infrastructure and networks upon which they depend may undermine their ultimate effectiveness.

While the U.S. Army is focusing most of its modernization efforts on traditional combat systems, it is interesting to note that Marine Corps

---


\(^4\) Ibid.

\(^5\) Ibid.


\(^8\) Ibid.

\(^9\) Ibid.
Installation Command (MCICOM) has launched a modernization Base of the Future campaign and is establishing a new technology accelerator called Installation-werX (I-werX). At I-werX, MCICOM will explore, experiment and rapidly adapt emerging technologies and processes to rethink the way their installations are built, maintained and operated. With the singular focus of enhancing force readiness, I-werX will test future base concepts and technologies using the Internet of Things (IoT) and smart-city data analytics. I-werX recognizes the importance of installation modernization to enhance force readiness and increase infrastructure resilience against future asymmetric attacks.10

Asymmetric Future

In November 2017, a dystopian short film entitled Slaughterbots went viral on the internet, fanning fears about the use of lethal autonomous weapon systems gone wrong.11 The film depicted swarms of drones powered by artificial intelligence (AI) scouring social media posts for prospective targets and then using facial biometrics to attack college students, assassinate government officials and terrorize entire cities. The film is shocking and profound, but, more importantly, it is instructive.

Tomorrow’s character of conflict will be increasingly asymmetric and take place on American soil. Whether AI, meme warfare, social media micro-targeting or ransomware, the lines between government-backed hackers, non-state actors, cyber-mercenaries, criminals and “patriotic hackers” are getting fuzzier.12 Malicious actors and adversaries are likely to target U.S. Government industry sectors as well as private and public infrastructure. Even non-national security-related infrastructure systems are targets. (In December 2017, Mecklenburg County in North Carolina was paralyzed by attacks that disrupted 911 calls, counselor hotlines, medical information, tax data and the digital records for over 1 million residents.13)

The miniaturization of threats is another aspect of asymmetric conflict. Drones continue to get smaller, faster, cheaper and potentially more lethal. In August 2017, there were 52 reports of drone activity near Fort McNair in only 26 days.14 (Fort McNair, only four miles from the White House,

---

10 Colonel A.C. Bolden, USMC, Marine Corp Installation Command G-7 Staff Briefing, 4 December 2017.
is located in one of the most heavily restricted air spaces in the United States.) While the intentions of these drone pilots are unknown, what is clear is that drones are being increasingly used for asymmetric attacks. In 2017, a Russian drone carrying a single thermite grenade destroyed the largest ammunition depot in the world—located on Balakleya military base in Eastern Ukraine—causing over a billion dollars in damage.15

The Internet of Things

Tomorrow’s asymmetric threats will ride the growing backbone of IoT. By 2020, there will be over 50 billion connected devices;16 wearables, ingestibles, sensors, devices and undreamed of tech, being perpetually fueled by declining costs, more powerful processing capabilities and ever-growing availability. Everything that can be connected will be, creating unforeseen opportunities and potential vulnerabilities for Soldiers, families and a workforce fueled by an intractable fixation on the latest devices. The IoT will drive connection of big things to countless little things on an unprecedented scale. As the co-founder of the internet Vint Cerf said, “By 2025, you will not be able to avoid being connected.”17 This phenomenon exposes a critical and widening vulnerability gap.

According to a July 2017 unclassified Government Accountability Office report, Internet of Things: Enhanced Assessments and Guidance are needed to Address Security Risks in DoD, there is no single lead office or organization in the Department of Defense (DoD) responsible for IoT security.18 The report highlights several shortcomings and operational risks, some of which are especially acute for U.S. Army Installations. IoT operational risks reside in informational and operational technologies, industrial controls and cyber-physical systems. If not addressed, they may permit asymmetric actors to sabotage military missions and equipment, conduct espionage and surveillance and endanger key leaders with cyber-physical effects. The lack of guidance, organization, policies or even a standardized definition for IoT19 hobbles collective efforts and is a growing problem for which U.S. Army installations are ill-prepared.

15 Patrick Duggan, “How the Enemy can Hit the US Army at Home.”
19 Ibid., p. 4.
Information Age Installations

U.S. Army installations no are longer Industrial Age forts, but are real-time hubs of functional connectivity that enable the synchronization and deployment of multidomain capabilities around the globe. This functional connectivity impacts readiness more than functional geography because U.S. Army installations host the sprawling information systems, infrastructure and networks upon which combat capabilities increasingly depend. This dependence requires the secure flow of data, information and shared understanding to help accelerate decision-making and rapidly align resources with emergent and fleeting needs. Functional connectivity means maximizing system flows and ensuring that all parts of the system connect to all other parts.

Greater installation connectivity provides combat capabilities with greater integrated power, and greater integrated power increases the prospects of multidomain success. Multi-Domain Battle (MDB) requires that the U.S. Army enhance its ability to project an array of cross-domain combinations and preserve connectivity for integrating air, cyber, land, sea, space and information capabilities. Better integrated multidomain capabilities allow U.S. Army leaders to achieve decision-dominance over adversaries, as long as installation infrastructure and system flows remain secure and resilient. This network effect means future Army readiness will be decided more by connectivity flows than geographic position.

However, greater connectivity brings greater risk. Once the arena of nation-states, today, non-state actors, super-empowered individuals and hybrid actors can all access increasingly affordable and sophisticated technologies to challenge the U.S. Army at home. Modern-day technology not only continues to compress geography and decisionmaking time, but also increases the variety, velocity and volume of future asymmetric threats. Unlike the days when adversaries physically attacked Army frontier forts from the outside, today they increasingly attack multidomain vulnerabilities inside.

Installation boundaries no longer demarcate safe-zones. Adversaries seek to take advantage of growing vulnerabilities across sprawling informational and operational technologies, industrial controls and cyber-physical systems to disrupt the U.S. Army’s ability to deploy and degrade its ability to operate effectively. Adversaries will leverage advances in technology to more deliberately time their attacks, seeking to maximize their asymmetric benefit while minimizing the ability of the U.S. Army to react. Installations without sufficient countermeasures and layered defenses will quickly

---

become compromised and degraded. **To counter these efforts, the U.S. Army must harden its installations and improve infrastructure resilience against more sophisticated threats.**

- **Installation Modernization Imperatives**

Installation modernization requires many things. It requires defining future requirements by accelerating R&D transitions onto installations to determine what does and does not work. It means: exploring, experimenting and rapidly adapting emerging technologies to update how installations are built, maintained and operated; establishing infrastructure protection teams (IPT) to help installations manage and secure their growing patchwork of IoT; and creating installation-specific mission assurance benchmarks\(^{24}\) to holistically assess multi-domain operational security. Operational security is much more than simply securing physical perimeters—it requires layering networks, devices and data into virtual defenses. IPTs should use installation cybersecurity scorecards to survey multi-domain defenses and mitigate potential vulnerabilities. **Most important, modernization means changing the mindset of installations from sanctuaries to growing battle spaces inside the U.S. Army’s own backyard.**

Finally, the U.S. Army must automate and operationalize its installation data. Current installation reports attempt to project future readiness by measuring elapsed results. Instead, real-time automation and robust analytics could better ensure the most timely and effective use of resources for programs and services. Countless efficiencies can be captured by automated algorithms and AI to synthesize disparate installation common levels of support reports, periodic assessment reports, infrastructure status reports, service status reports, defense readiness reports and many others. Automation is key to modernizing base of the future concepts; data must be converted into a real-time feedback loop that more precisely connects resources to emerging requirements.

Meaningful installation modernization requires challenging all assumptions, including whether the scope, scale and size of Industrial Age social programs remains valid. In today’s fiscally austere environment, the U.S. Army must objectively balance legacy programs with current and emerging mission and security requirements. It would be wise for the Army to leverage the available services in local economies rather than creating redundant efforts. The Army no longer needs to measure its force readiness by Industrial Age standards, diverting precious funds, resources, manpower and space in trying to do so.\(^{25}\)

---


**Recommendations**

1. The U.S. Army should rethink the roles and purpose of its installations.

2. The U.S. Army should prioritize installations as being integral to its overall modernization strategy.

3. Leverage the concepts and framework articulated in Multi-Domain Battle\(^\text{26}\) to take a joint approach to developing concepts for the base of the future within strategic support areas. Expand partnerships with MCICOM and I-werX to define new battle-space requirements.

4. Recognizing that there is no such thing as a non-IoT installation, DoD and the U.S. Army must update IoT policies and regulations to establish minimum baselines for installation information systems, infrastructure and networks.

5. Installation commanders, Senior Commanders and Installation Management Command need the flexibility to modify, scale and tailor the delivery of goods and services according to the realities of the mission, threats, budget constraints and viable economic alternatives on the ground. The U.S. Army must rebalance Industrial Age programs with Information Age security requirements so that installation service standards do not emulate frontier forts when surrounding markets are able to provide comparable goods and services.

**Conclusion**

The Army is in the midst of profound technology change and must update the way it thinks about its installations. Installations are not sanctuaries; they are the first skirmish lines of defense against growing asymmetric threats. As the U.S. Army embraces a comprehensive modernization strategy to innovate new combat capabilities, now is the time to rethink the role its installations provide, as they host the information systems, infrastructure and networks on which those capabilities increasingly depend. Ultimately, if the U.S. Army wants a more agile, lethal and modern force, it must include updating its Industrial Age installation design.

*Colonel Patrick M. Duggan is the Commander of Joint Base Myer-Henderson Hall in Washington, DC, and is a career Special Forces officer with cyber expertise. He has published numerous articles and is the recipient of the 2015 Chairman of the Joint Chiefs of Staff National Defense and Military Strategy Writing Award.*

---
