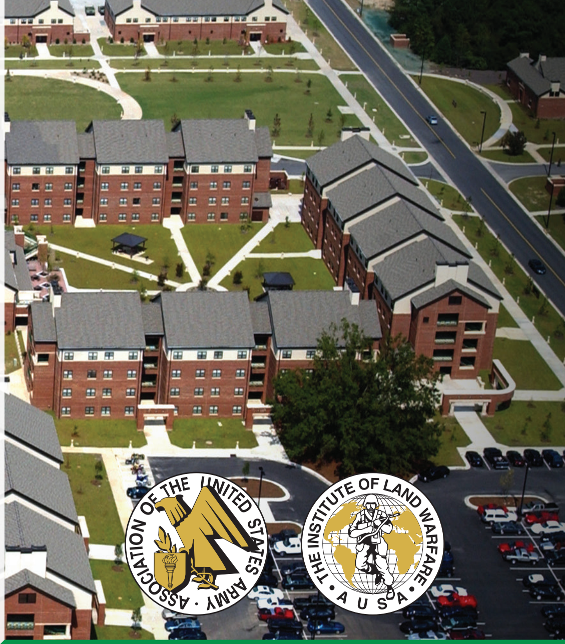
ILW SPOTLIGHT 18-1

Modernization for Industrial Age U.S. Army Installations

by Colonel Patrick M. Duggan, U.S. Army

PUBLISHED BY THE INSTITUTE OF LAND WARFARE
AT THE ASSOCIATION OF THE UNITED STATES ARMY



FEBRUARY 2018

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[1] installations that are designed more for their functional geography[2] 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

ISSUE

As the U.S. Army pursues a comprehensive modernization strategy to update and innovate its combat capabilities, it should also undertake a complementary effort to modernize its Industrial Age installations in order to ensure that future combat capabilities can even get to the fight.

***SPOTLIGHT* SCOPE**

- Assesses implications of not modernizing U.S. Army installations to address emerging threats.
- Identifies imperatives for installation modernization.

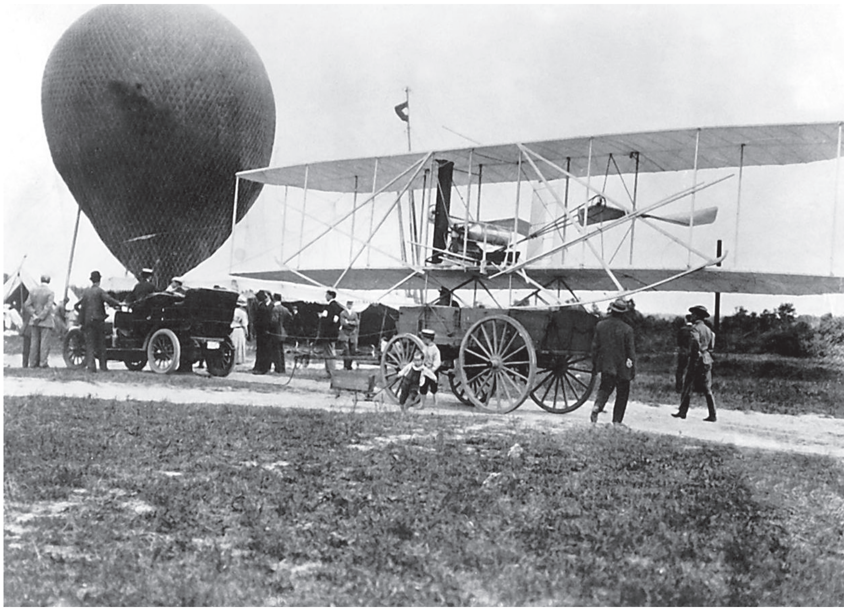
INSIGHTS

- Installations are no longer sanctuaries for U.S. Army forces deploying to battle; they are the first skirmish lines of defense against growing asymmetric threats.
- Today's installations host the sprawling information systems, infrastructure and networks upon which U.S. Army combat capabilities increasingly depend.
- Tomorrow's character of conflict will be increasingly asymmetric and are likely to take place on American soil.
- Failure to modernize Industrial Age installations will limit the U.S. Army's ability to project multi-domain combat power.

[1] Patrick Tucker, "US Army Chief Announces Major Reorganization For How Army Develops, Buys Weapons," *DefenseOne*, 6 October 2017, accessed 26 December 2017, http://www.defenseone.com/technology/2017/10/feeling-rivals-heat-us-army-streamlining-and-centralizing-way-it-buys-weapons/141603.

[2] Parag Khanna, *Connectography: Mapping the Future of Global Civilization* (New York, NY: Random House, 2016), p. 14.

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.



U.S. Army photo.

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

ARMY MODERNIZATION PRIORITIES

- Long-Range Precision Fires
- Next Generation Combat Vehicle
- Future Vertical Lift
- Network
- Air and Missile Defense
- Soldier Lethality

[3] Patrick Duggan, "How the Enemy can Hit the US Army at Home," *War on the Rocks*, 3 August 2017, accessed 26 December 2017, https://warontherocks.com/2017/08/how-the-enemy-could-hit-the-u-s-army-at-home.

[4] *Ibid*.

[5] *Ibid*.

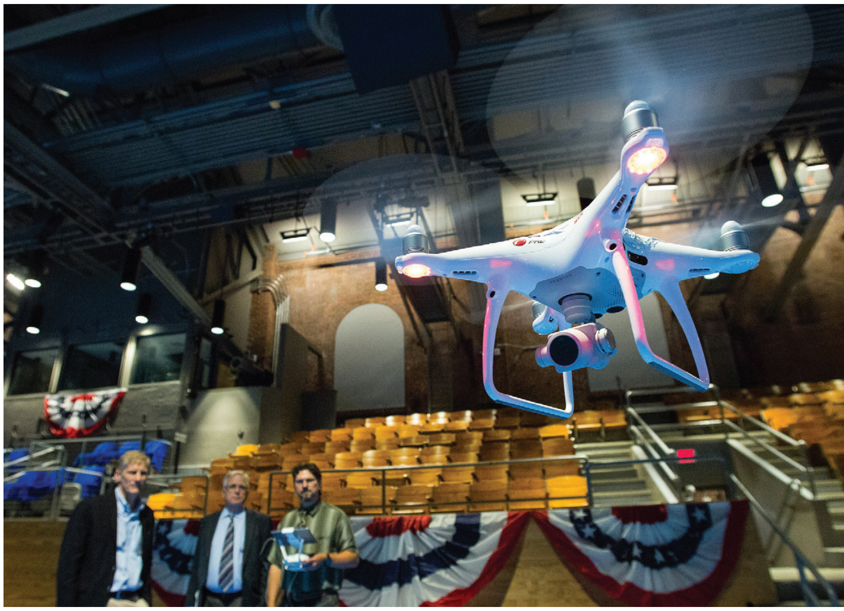
[6] U.S. Congress, Senate, Committee on Armed Services, "Nomination Hearing for Secretary of the Army Dr. Mark Esper Opening Statement Before the Senate Armed Services Committee," 2 November 2017, accessed 26 December 2017, p. 4, https://www.armed-services.senate.gov/imo/media/doc/Esper_11-02-17.pdf.

[7] "Modernization Priorities for the United States Army," 3 October 2017, accessed 26 December 2017, p. 2, https://admin.govexec.com/media/untitled.pdf.

[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]



Andrew St. Laurent (right), senior Unmanned Aircraft System pilot for PrecisionHawk, conducts a drone demonstration while Matt Hardison (left), principal at Hardison Consulting Group, and Dr. Richard Mudge, president of Compass Transportation and Technology, look on at Conmy Hall during Joint Base Myer-Henderson Hall's inaugural Industry Day on 14 September 2017. (Photo by Francis Chung/JBM-HH PAO.)

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,

ASYMMETRIC THREATS TO ARMY INSTALLATIONS

- Drones
- Artificial Intelligence
- Meme Warfare
- Social Media Micro-Targeting
- Cyberattacks
- Ransomware

[10] Colonel A.C. Bolden, USMC, Marine Corp Installation Command G-7 Staff Briefing, 4 December 2017.

[11] "Slaughterbots," *YouTube*, 12 November 2017, accessed 26 December 2017, https://www.youtube.com/watch?v=9CO6M2HsoIA.

[12] Joseph Marks, "FBI, DHS Warn of Hacker Mercenaries Funded by Nation-States," *DefenseOne*, 1 December 2017, accessed 26 December 2017, http://www.defenseone.com/threats/2017/12/fbi-dhs-warn-hacker-mercenaries-funded-nation-states/144231.

[13] Jonathan Drew, "Ransomware hack slows North Carolina county's government to a crawl," *Fifth Domain*, 6 December 2017, accessed 26 December 2017, https://www.fifthdomain.com/civilian/2017/12/06/deadline-looms-for-north-carolina-county-hit-with-ransomware.

[14] Francis Chung, "Detection Program finds drones over joint base," *Pentagram*, 25 October 2017, accessed 26 December 2017, https://www.army.mil/article/195901/detection_program_finds_drones_over_joint_base.

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 IoT[19] hobbles collective efforts and is a growing problem for which U.S. Army installations are ill-prepared.**

U.S. Army Sergeant Robert Matz, assigned to 10th Combat Aviation Brigade, 10th Mountain Division, observes Specialist Christanjon Burr, assigned to the Enterprise Service Gateway Landstuhl, 102nd Strategic Signal Battalion, 2nd Theater Signal Brigade, while he checks signal connection strengths 11 July 2017 in Landstuhl, Germany. The largest Army-operated satellite communications facility outside the continental United States, the ESG-L is providing strategic signal support to participants of Saber Guardian 17, a U.S. Army Europe-led, multinational exercise, taking place in Bulgaria, Hungary and Romania 11–20 July 2017. (U.S. Army Photo by Staff Sergeant Brian Cline.)

INTERNET OF THINGS OPERATIONAL RISKS

- Informational and Operational Technologies
- Industrial Controls
- Cyber-Physical Systems

[15] Patrick Duggan, "How the Enemy can Hit the US Army at Home."

[16] Vala Afshar, "Cisco: Enterprises Are Leading The Internet of Things Innovation," *Huffpost*, 28 August 2017, accessed 26 December 2017, https://www.huffingtonpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_us_59a41fcee4b0a62d0987b0c6.

[17] Jeff Evans, "The Internet of Things: A Promising Market," Georgia Tech Center for the Development and Application of Internet of Things Technologies, slide 21, 2 November 2016, accessed 26 December 2017, https://cdait.gatech.edu/sites/default/files/iot_promising_market_mobility_live_jeff_evans_georgia_tech_cdait_november_2_2016.pdf.

[18] United States Government Accountability Office, "Internet of Things: Enhanced Assessments and Guidance are Needed to Address Security Risks in DOD," Report to Congressional Committees (Washington, DC: Government Printing Office, July 2017), p. 2, https://www.gao.gov/assets/690/686203.pdf.

[19] *Ibid*., p. 4.

Information Age Installations

29 ID Soldiers trained with DroneDefender, a point-and-shoot, electromagnetic, rifle-shaped weapon that disrupts communications between a remote-controlled drone and its operator. While the U.S. military works on a range of options to counter drone technology, the system provides a safer and more accurate alternative than other methods, such as shooting drones with a rifle. (Photo by Captain Nicole Vajda.)

U.S. Army installations no are longer Industrial Age forts, but are real-time hubs of *functional connectivity*[20] 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 decisionmaking 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.[21]

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.[22] 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.[23] Installations without sufficient countermeasures and layered defenses will quickly

U.S. Army installations host the sprawling information systems, infrastructure and networks on which combat capabilities increasingly depend.

[20] Parag Khanna, *Connectography: Mapping the Future of Global Civilization*, p. 17.

[21] *Ibid*., p. 31.

[22] U.S. Army Training and Doctrine Command G-2, "The Operational Environment and the Changing Character of Future Warfare," 30 July 2017, accessed 26 December 2017, p. 22, https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/215990/download.

[23] *Ibid*., p. 40.

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

Major Christine Pierce, the Pennsylvania National Guard Defensive Cyber Operations Elements team chief, and Scott Poley, security operations center supervisor at FirstEnergy, complete a practical exercise as part of a cybersecurity course during exercise Cyber Shield 17 at Camp Williams, Utah, 28 April 2017. (Photo Credit: Sergeant Michael Giles.)

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]

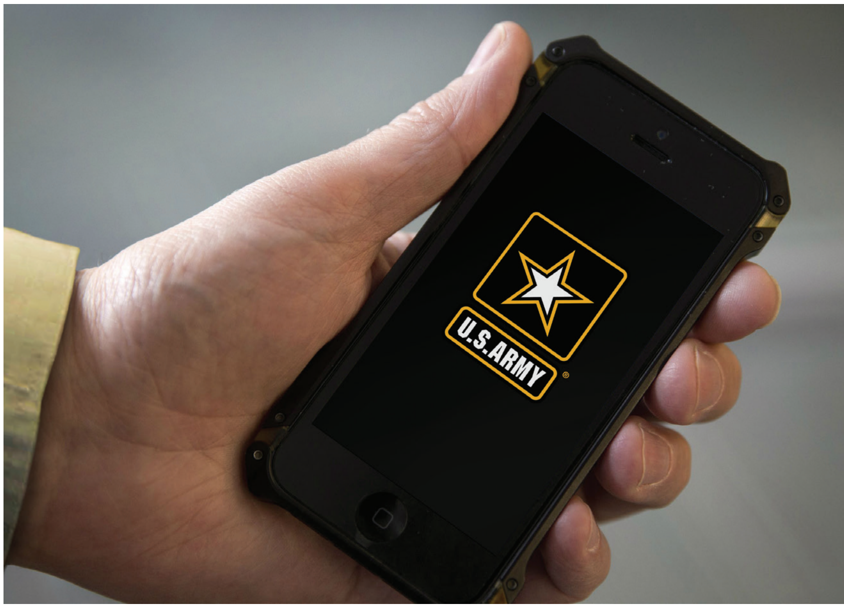
IMPERATIVES FOR INSTALLATION MODERNIZATION

- Change in mindset
- Accelerate R&D transitions onto installations
- Explore, experiment and rapidly adapt emerging technologies to update how installations are built, maintained and operated
- Build infrastructure protection teams
- Establish mission assurance benchmarks
- Utilize cybersecurity scorecards
- Automate and operationalize data

[24] U.S. Government Accountability Office, "Internet of Things: Enhanced Assessments and Guidance are Needed to Address Security Risks in DOD Report to Congressional Committees," p. 16.

[25] Dwight Howell, "Army installations of the future: urban + shrinkage + landscape," Master's Thesis, (Cambridge, MA: Massachusetts Institute of Technology, February 2015), p. 4, https://www.researchgate.net/publication/279809996_Army_installations_of_the_future_urban_shrinkage_landscape.

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[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.

The Association of the United States Army is a private, non-profit educational organization that supports America's Army—Regular Army, Army National Guard, Army Reserve, retired Soldiers, government civilians, wounded warriors, veterans, concerned citizens and family members.

Interested in becoming a member of AUSA? See the benefits of membership and join online at:

www.ausa.org/membership

[26] U.S. Army Training and Doctrine Command, *Multi-Domain Battle: Combined Arms for the 21st Century*, 24 February 2017, accessed 26 December 2017, p. 1, http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_WhitePaper.pdf.

Association of the United States Army | 2425 Wilson Boulevard, Arlington, VA 22201 | 703-841-4300 | www.ausa.org