Army Science Board
Fiscal Year 2018 Study

The Internet of Things (IOT): Creating "Smart" Installations

Final Report
February 2019

Department of the Army
Office of the Deputy Under Secretary of the Army
Washington, DC 20310-0103

DISCLAIMER:

This report is the product of the Army Science Board (ASB). The ASB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense through the Secretary of the Army and the Chief of Staff, Army. The statements, opinions, conclusions, and recommendations contained in this report are those of the ASB study members and do not necessarily reflect the official position of the United States Army or the Department of Defense.

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

The Assistant Secretary of the Army for Installations, Energy and Environment (ASA (IE&E)) requested that the Army Science Board conduct a study looking at applying Internet of Things (IoT) technologies to enhance readiness at Army installations. Specifically, this study should advance the Army's knowledge of the potential advantages and risks of leveraging the IoT to create smart and resilient installations.

The smart military installation uses multiple types of electronic data collection sensors to provide actionable information that's used to manage assets and resources efficiently, leading to improved readiness, support for modernization, and reduced operating costs. Commercial industry has invested heavily in the development and implementation of the IoT to make processes more efficient while at the same time cutting costs. In recent years, industry has deployed IoT at an exponential rate, fueled in part by reduced costs in sensors and advances in cloud computing and data analytics. The Army can leverage industry advances in this field for use in creating the smart installation.

The study team conducted teleconferences and visits to civilian corporations involved with IoT technologies, to academic institutions with programs related to IoT or city planning, and to Army installations. Additionally, the team talked with DoD and Department of the Army organizations that have a stake in this development, such as Network Enterprise Technology Command (NETCOM), Installation Management Command (IMCOM), and the Army Corps of Engineers Engineer Research and Development Center (ERDC).

Based on the information gathered during those visits and meetings, as well as associated documentation and discussions, the study team made the following findings:

1. **Industry and cities deploy IoT in urban areas when there is significant ROI and sufficient data for relevant analytics.** Utility companies in Central Europe have recently invested in and employed IoT, saving $1.2 billion in the first year. Applying to the Army's present installations around the globe in the fields of IoT and enhanced maintenance techniques, the Army could potentially experience $200 million in savings.

2. **Early industry successes**
   - Energy management
   - Predictive maintenance
   - Improved security
   - Traffic management
   - Corporate campus services

3. **Required technologies are mature and in use today.** Many IoT technologies now exist that can readily be adopted at Army installations.

4. **Army populations (military and civilian) are not constrained to the installations but integrated into the surrounding community.**

5. **Army has not adopted the industry approach for controlled experimentation to deploy IoT on its installations.** There has been a lack of experimenting with pilot programs that exploit a form of IoT to benefit an installation's operations.

6. **ERDC research for data management – Smart and Resilient Installations (SaRI) – first cut at architecture, and Virtual Testbed for Installation Management Effectiveness (V-TIME).**

7. **The study team could not find any Army activity that claims responsibility for an IoT enterprise architecture nor the data.** Installations can be viewed as computing on the edge, but the Army does not resource them to function at the edge.

8. **Technology refresh and contracting are not in sync.**

Based on these findings, the study team made the following recommendations:

1. **ASA (IE&E) establish a Smart Installation Demo Program ($50M annually) facilitated by a flexible contract vehicle (e.g. OTA) with sufficient contract ceiling to allow roll out.**

2. **ASA (IE&E) assign a program manager to identify pilot technology projects, match them with installations, develop a resourcing and acquisition strategy, and manage the efforts.**

3. **Program manager run initial pilot experiments in the following areas:**
   - Energy efficiency
   - Predictive maintenance
   - Others to be determined (e.g., security, community services)

4. **ASA (IE&E) invite other installation organizations (Army and other tenants) to use this platform to conduct pilots in other areas:**
   - Soldier monitoring
   - Training, healthcare services…

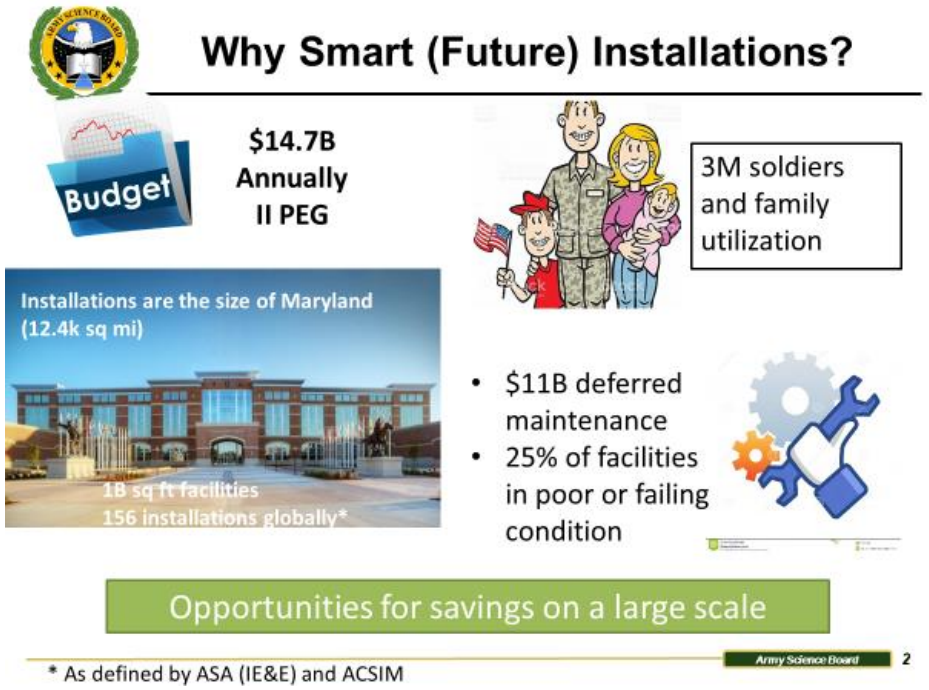
5. **ASA (IE&E) with ACSIM and IMCOM use results of initial pilot experiments to define smart installation rollout.**

Note: ACSIM is now the Deputy Chief of Staff, G9-Installations.

ANNOTATED ARMY SCIENCE BOARD BRIEFING

The following briefing was presented by Dr. Gisele Bennett, Study Chair, to the Army Science Board (ASB) in plenary session on 18 July 2018. By unanimous vote, the Board adopted the findings and recommendations.

WHY SMART (FUTURE) INSTALLATIONS?



Installations make up over 15% of the Army budget. The scale of potential savings from applying program efficiencies and the number of Soldiers and families affected by improved services would be significant. For example, some aspects of the activity in the Army's installations portfolio include:

Infrastructure ($7.9B)

- 1 billion sq ft of building space
- 191.4 million sq. ft. of operational & maintenance facilities
- 13.5 million acres of Army land
- $461B in real property
- $1.7B in military construction
- $331M in family housing construction
- 363 operational range complexes
- 110 Native American sacred sites on 22 installations
- 39 cemeteries

- 226 endangered species on 124 installations

Services ($5.4B)

- 323 utility systems
- 428 MW of renewable energy capacity
- 66,322 (non-tactical) vehicle fleet
- 490,000 barracks spaces
- 267 fire stations

Family and Community ($1.3B)

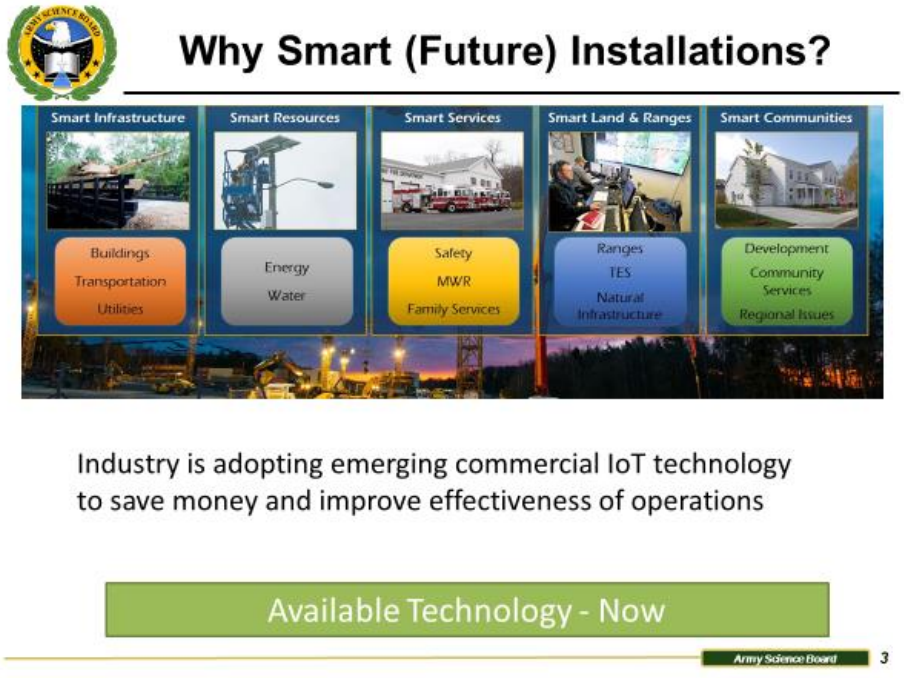
- 1.2 million family members
- 71,500 children in daycare

Security & Force Protection ($1.1B)

- $680M Physical Security
- $248M LE

Thus, investment in IoT to produce energy efficiency across 323 utility systems or to improve sustainment and maintenance costs for over 66,000 vehicles would potentially yield millions of dollars in cost savings for the installation portfolio.

Beyond cost savings, a growing number of the U.S. population lives in smart cities and/or works in smart environments. Converting Army installations to smart installations would provide a recruitment incentive for the next generation of Soldiers who are growing up with technology enabled services and would expect their work environments to be as modernized, if not more so.



The Army has been adopting digital technologies for use in its weaponry, and as a matter of course, units routinely train for combat using digital technologies to enhance their combat effectiveness. The reliance on digital technology will extend to other unit activities, many of which fall under the purview of installation commanders, such as monitoring traffic flow, personnel training, the physical state of equipment, etc. Here again, the application of IoT to optimize these efforts could produce substantial fiscal savings for Army installations, but the real-time access to information on unit activities will also improve commanders' insight into their units' readiness.

INTRODUCTION

The Assistant Secretary of the Army for (Installations, Energy, and Environment) (ASA(IE&E)) requested the ASB conduct a study in FY 18 to further develop the efforts of its FY 16 study, "The Military Benefits and Risks of the Internet of Things." Specifically, this year's study was intended to advance the Army's knowledge of potential risks and advantages gained by leveraging the use of the IoT in creating "smart and resilient" installations.

In its term of reference (TOR), The study team's tasks included:

- Recommending what the Army should consider when designing the core strategy for data collection and analytics, considering cyber security perspectives, and performance efficiencies.

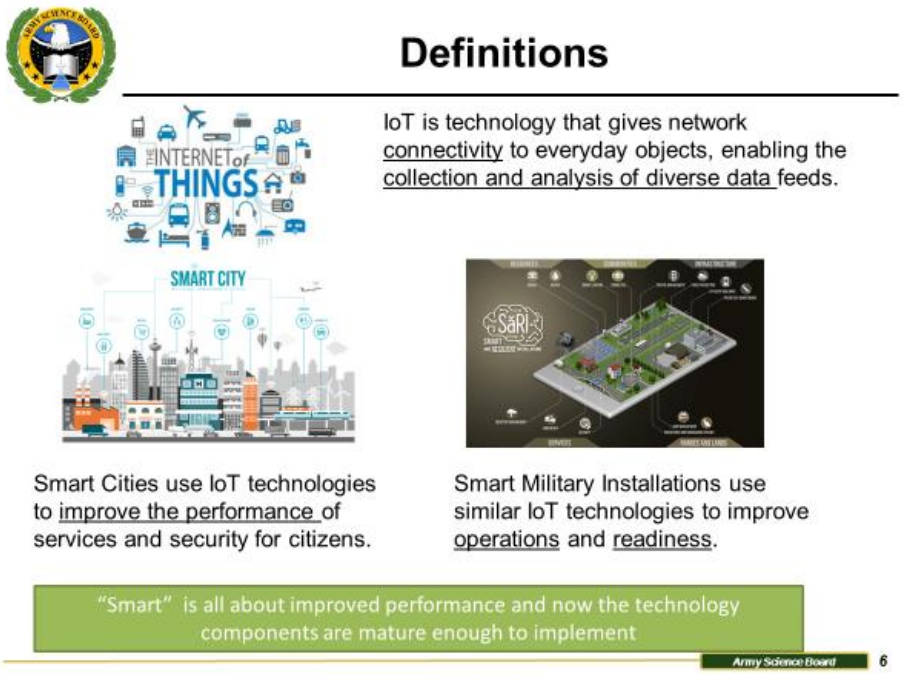
- Exploring how Army installations can effectively partner with industry, academia, and local communities to implement IoT approaches in a cost-effective manner.

- Recommending possible Army specific IoT applications for installations as may be relevant.

- Providing a potential approach or framework the Army could use to prototype and test IoT technology over time.

For this study, the ASB compiled a team that included experts in sensor systems, modeling, logistics, radio frequency identification (RFID), Cyber systems, and medical and human performance, as well as representatives from the ASA(IE&E) office. The government liaisons expertise was invaluable to understanding Army installation operations and opportunities for incorporating data analytics with IoT at the installations level.

The study team convened and held preliminary planning meetings during the ASB's Summer Plenary Session in July 2017. Subsequent data gathering visitations and interviews were conducted from September through December 2017 (Appendix C). Follow-on telephone conferences were held with some organizations as needed.



Early on, the study team adopted the definition of IoT from the FY16 study:[1]

> An infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

For the current study, the definition still aligns with and describes well the opportunities for Army installations to reduce costs and improve operational efficiencies while providing a modernized place to work and live. Furthermore, increasing a commander's visibility into the installation's various operations and activities provides the opportunity to improve readiness for Army installations worldwide. And, since most installations are near or embedded in a city, leveraging IoT infrastructure also allows for integration with city services as appropriate, which allows the Army to tap into and leverage technologies being developed that use digital applications to support communities and businesses.

In the commercial sector, these technologies have been growing almost exponentially over the past decade. Local governments are opting to turn their communities into smart cities, and many businesses are incorporating IoT into their commercial activities at an unprecedented rate. The technological revolution has centered around commercial enterprises that specialize in software development and in academia.

[1] From International Organization for Standardization (IOS) and the International Electrotechnical Commission (IEC) Joint Technical Committee (JTC)-1 definition. See: ISO/IEC 20924:2016 Information technology — Internet of Things (IoT)

The study team met with leaders in IoT technologies to gain information about the state of progress and found variances over a wide spectrum of applications. As one might expect, large, publicly owned corporations like Microsoft, NVIDIA, and C3 IoT are developing very sophisticated software for commerce, industry, and government. For the most part, the earliest software products were applied in the utilities sector to optimize the use of electrical power, water, and heat. The fact that these large corporations are investing substantial resources into this area speaks volumes about the potential for savings and profits. The maturity of artificial intelligence (AI)-based software has contributed to making IoT more lucrative, spurring the growth in the volume of IoT applications. The AI software programs can gather myriad forms of data and intelligently interpret them to guide companies on how to most efficiently operate, resulting in substantial savings in costs.

Companies like C3 IoT have made significant inroads into adopting IoT for many uses, and the study team was introduced to several initiatives being adopted by corporations, agencies, municipalities, and even countries. The team believes industry is at the beginning phase of understanding the possibilities for applying IoT technologies, and the number of applications useful to the Army are significant.

The study team also visited government-related R&D Centers such as the Lawrence Livermore National Laboratory, the Robins Air Force Base 21st Century Partnership Program, and Arlington County's Chief Information Officer. Discussions focused on how government institutions could best leverage IoT technologies. In some cases, such as the U.S. Special Operations Command, military organizations have been making significant inroads to incorporate IoT technologies into their operations.

Discussions with government organizations also revealed the heavier concentration of computer usage required by the IoT comes with a price. The military's increased reliance on computers for installation operations have required and will continue to require additional security procedures and training. Army installations extensively utilizing computers to manage functions can expect serious attempts by adversaries to hack into installation support operations. Thus, a direct but sometimes overlooked cost of employing IoT will involve the requirement to mitigate evolving threats. Other direct costs are related to the acquisition of the digital equipment needed for sensors and relays, software packages needed to employ data input and analyses, and the computers needed for processing. Indirect costs will include heavier use of electrical power (which is not necessarily trivial) and investment in installations systems needed to keep the digital equipment functioning, such as cooling systems. For example, costs for cooling servers at Lawrence Livermore and in several Northeast cities are substantial.

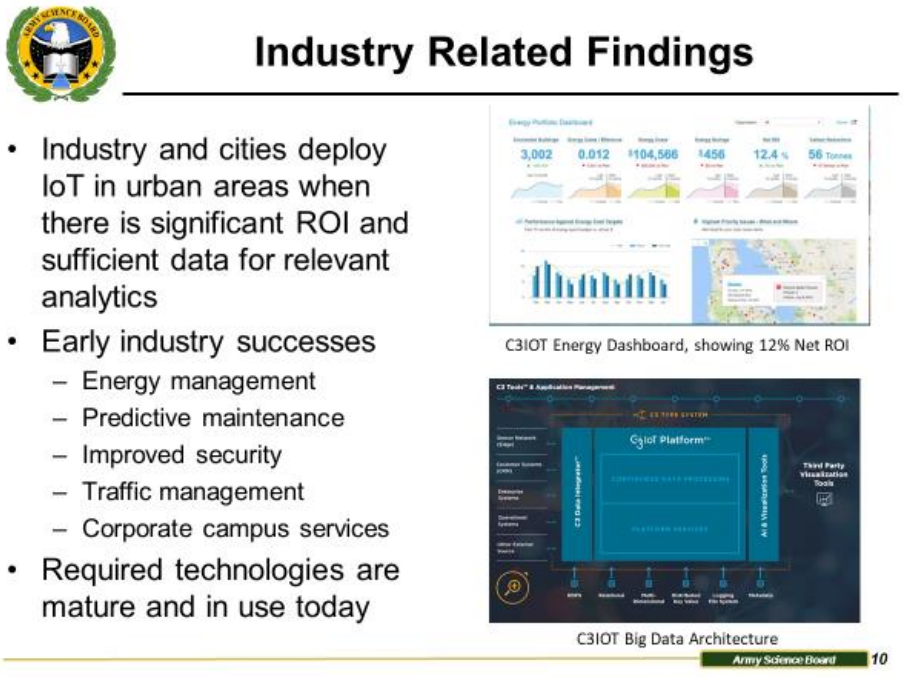
The study team also visited or conducted teleconferences with academic institutions participating in IoT research, such as the Center for Information Technology Research in the Interest of Society (CITRIS), the Center for Long Term Cybersecurity at U.C. Berkeley, the Center for Resilient Infrastructure Systems at Georgia Tech, and the Human Factors Laboratory at the Florida Institute of Technology. While most data gathered from these visits had to do with research on how to expand the use of IoT within communities, much of the research, like that

occurring in industry, ultimately centered around AI. For example, PhD candidates at Georgia Tech were building algorithms for computer applications that sensed and analyzed the flow of human traffic within several city structures in the city of Atlanta. The sensor analyses were being used to coordinate best allocations of electrical and other power sources, with the goal of avoiding waste while ensuring adequate support to highly frequented structures.

Utilization of IoT in smart cities is not just confined to computer science and engineering activities. At U.C. Berkeley, Dr. Costas J. Spanos, the director of CITRIS, showed how students, who comprise a consortium across several universities, are conducting a wide range of studies in expanding the use of AI for community services that include medical and educational institutions.

FINDINGS

Corporate leaders in the IoT industry briefed the study team on the state of their progress employing IoT in communities and installations around the world. The Army could benefit from their lessons learned, and by directing its investment strategy towards those technologies that offer the most promise for success in a military application at scale. In one study conducted by C3 IoT involving 3,002 structures in the San Francisco Bay area, investments of hundreds of millions of dollars in IoT technologies netted a return on investment of 12%.

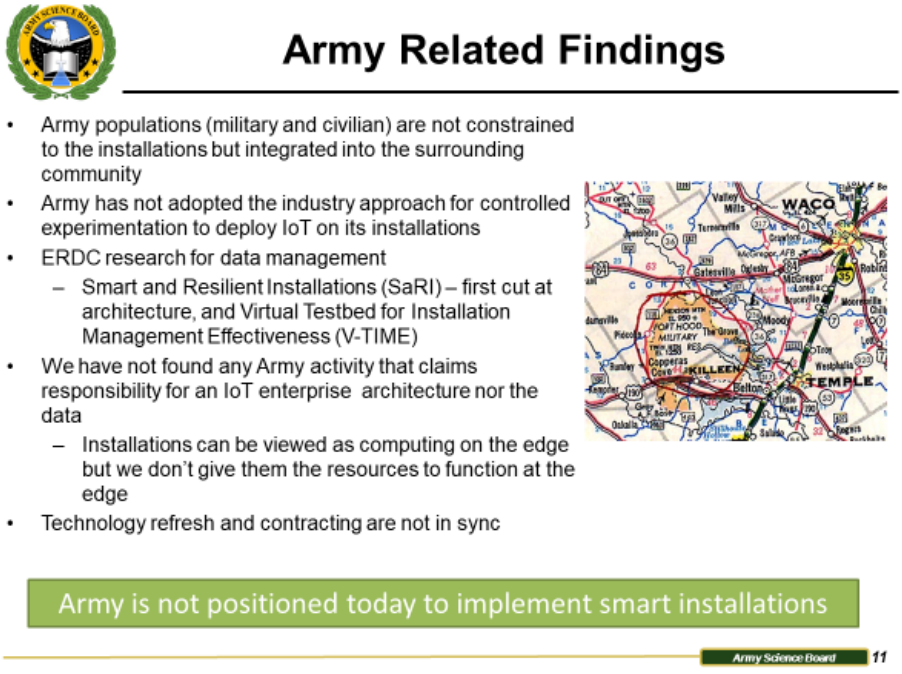


IoT applications that are well founded and mature, such as those in the energy management, could realize similar successes in other areas, including the maintenance of installations and equipment, improvement in facility security, and the management of the flow of employees and general traffic. AI algorithms germane to many of these newer areas were developed a decade ago and are reaching a state of maturity that makes them candidates for use without exposure

to inappropriate risks. In other words, there is significant potential for the Army to leverage and benefit from multiple areas of research in IoT.

When applying IoT to the Army, security becomes a bigger issue than it may be for industry, because the latter alleviates the costs for many of these systems by relying on existing commercial infrastructure. For example, because AI algorithms normally utilize prodigious amounts of data to give adequate guidance for the use of installation systems, the systems use existing commercial infrastructure, like Google Cloud, to cut down the costs of operating the algorithms. Vendors like Google have invested heavily into building secure systems, and the Army could benefit from those same security measures. However, caution must be observed. If, for instance, IoT is used to monitor the physical well-being of Soldiers on installations to give commanders real time feedback on personnel readiness, consideration should be given to whether data bases holding that information should be kept by a commercial vendor, even if they are secure. In other words, the Army must determine whether the degree of security used for commercial purposes is adequate if used for critical combat operations. If it is determined that some IoT technologies being used by Army installations will require added security measures, then obviously, those costs must be considered.

Not all IoT applications may require the same levels of security, and the safeguards established by commercial vendors may satisfy Army needs. Relatively benign uses for IoT may be able to leverage the degree of security adopted by commercial infrastructure. In those cases, savings will be substantial. For example, applications governing the usage of electrical power in housing.



Data collection and interviews with Army organizations revealed that the Army is not positioned today to implement smart installations. A successful transformation from installation to smart

installation, will require an enterprise plan that ties to operational readiness and Soldier support. The enterprise approach must factor in contingencies and engagements and, importantly, the utilization of services from communities adjacent to the installation. Army populations are not constrained to the installation, making it vital to deliberately incorporate the installation with the community. Many well-defined boundaries of Army populations and the installations they traditionally resided upon have blurred over the past several decades. The opportunity to leverage community functions can provide cost savings for the Army and create partnerships for services. Communities and especially cities throughout the country are migrating toward a smart city framework. Leveraging the investments made by these communities through partnerships can facilitate and accelerate deployment of IoT on Army installations.

Challenges associated with deploying IoT technologies on Army installations include upgrading legacy technology and equipment, addressing new types of cyber vulnerabilities, and the bureaucracy associated with each of these tasks. The multi-use potential of data collected by IoT devices also creates dilemma around responsibilities for those data. For example, who should pay for the data collection on occupancy data in buildings, which benefit both energy monitoring and human resource planning? Who owns the data?

Unlike smart cities where the CIO of a city has responsibility for deploying sensors and managing the data and analytics, the Army does not have an enterprise-wide functional responsibility over the architecture needed to deploy IoT across the installations.

Finally, the Amy does not have an acquisition or contracting framework to meet required investments in technology development. The IoT systems will use AI to enable efficiencies, and the Army will need to invest in a continuous development cycle as technology evolves to fully optimize the benefits of IoT as they emerge.

HIGH POTENTIAL APPLICATIONS OF IOT FOR INSTALLATIONS

The Army will realize benefits of IoT applications in the areas of readiness and cost savings. Though not a comprehensive list, examples of high potential applications include:

Readiness:

- Soldier monitoring for physical health and safety
- Enhanced training through digital twins that replicate real environments into virtual ones for modeling and simulation (Soldiers and systems)
- Predictive Maintenance for equipment and real property that produces efficiencies in terms of time and resources

Cost Savings:

- Predictive Maintenance for real property management to include space utilization, utility monitoring, building analytics, etc.

- Building automation[2] including the creation of digital twins for optimizing utilities

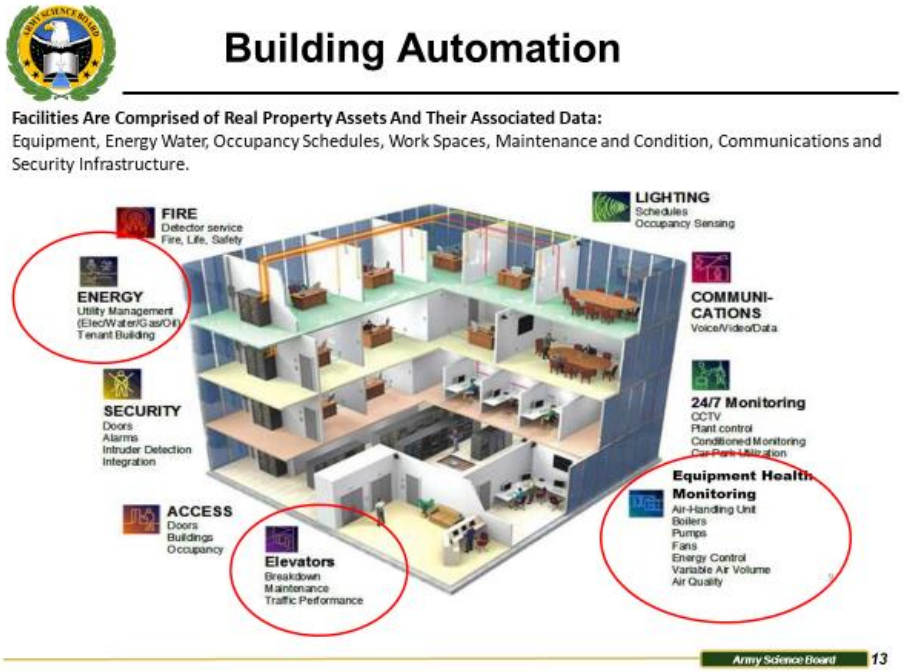
- Security applications including automation at checkpoints, monitoring and compliance at child development centers, frictionless entry control to minimize required security personnel, etc.

Building automation is common throughout industry because it improves the delivery of services to tenants and the cost effectiveness for building managers/owners:

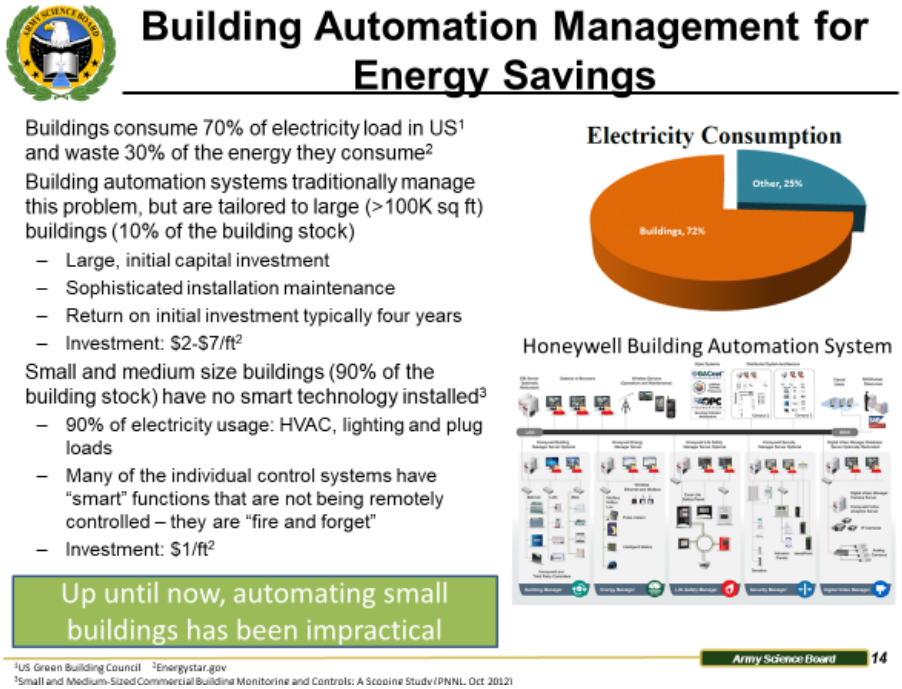
> New building construction as well as retrofit projects provide opportunities for companies in the building automation space…. For one, they view a more integrated approach to modernization as way to save energy costs. Integration also saves administrative dollars, since it is more efficient to manage systems with one console as opposed to several. Concerns over obsolescence also play a role in encouraging building owners to take a fresh look at automation. Aging, proprietary controllers…will eventually outlive vendor support.[3]

[2] The centralized, computerized control of heating, ventilation and air conditioning, lighting, security, fire, and other systems by a building management system or building automation system.

[3] https://internetofthingsagenda.techtarget.com/feature/Building-automation-systems-Internet-of-Things-meets-facilities-management



Building automation systems have operated as independent entities on different delivery platforms but are instrumented and generate data, offering the potential for using the IoT to synchronize dashboards. The comprehensive catalogue of objects and people in the building allows managers to optimize its role to suit the best purposes of its state at the time. [4]



[4] Ibid.

The U.S. Green Building Council estimates that buildings consume 70% of the electricity load in the U.S.[5] and DoE estimates 30% of that electricity is wasted.[6] Given that the Army will budget $955M for installation energy expenses in FY 19,[7] the study team proposes building automation should be one of the IoT applications investigated by the Army.

Building automation systems are traditionally employed in larger facilities, i.e., over 100,000 square feet. Honeywell, Johnson Controls, and other companies manufacture systems that permit building owners to control energy, life safety, security, and other services. The initial capital investment, recurring installation, and maintenance ($2-$7 per square foot) can be recouped in energy efficiency and other savings in as little as four years.[8]

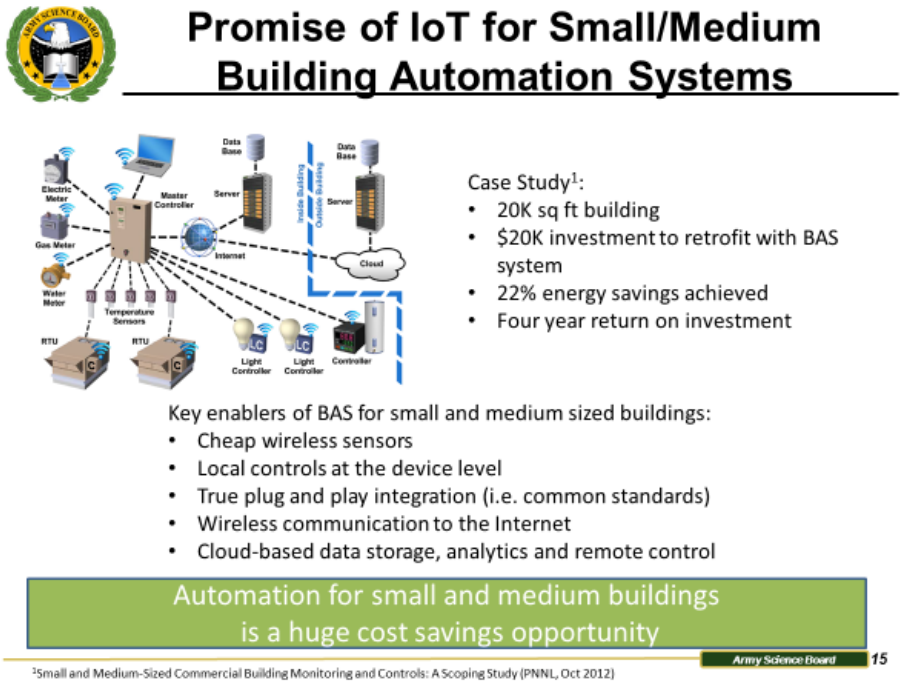
Small and medium sized buildings, i.e., 50,000 square feet and under, make up 90% of the U.S. building stock, and these often have no centralized, automated control over their systems. A team from Pacific Northwest National Laboratory (PNNL) studied the problem of implementing automated monitoring and control in small and medium size buildings[9] and found that 90% of electricity usage powers heating, ventilation, and air conditioning (HVAC), lighting, and plug loads. Though these buildings may have individual control systems with smart function capability, they are usually not remotely controlled, often pre-programmed at installation, and rarely reprogrammed.

The key enablers for providing building automation services in small and medium size buildings are already available:

- Cheap wireless sensors
- Local control at the device level
- True plug-and-play integration (i.e., open, common, standards)
- Connectivity to the Internet
- Cloud-based configuration control, remote monitoring, and data analytics
- Wireless communication for the sensors and controllers

[5] Buildings and Climate Change. US Green Building Council. http://www.eesi.org/files/climate.pdf
[6] About the Commercial Buildings Integration Program. Office of Energy Efficiency and Renewable Energy, US Department of Energy. https://www.energy.gov/eere/buildings/about-commercial-buildings-integration-program
[7] Assistant Secretary of the Army (Installations, Energy and Environment), President's Budget FY2019, 7 April 2018.
[8] Gunjan Rawal, Cost, Savings and ROI for Smart Building Implementation. IoT @ Intel Blog, June 20, 2016. https://blogs.intel.com/iot/2016/06/20/costs-savings-roi-smart-building-implementation/
[9] S. Katipamula et. al., Small- and Medium-Sized Commercial Building Monitoring and Control Needs: A Scoping Study. Pacific Northwest National Laboratory, PNNL-22169, October 2012, https://www.pnnl.gov/main/publications/external/technical_reports/pnnl-22169.pdf.

All these technologies are inexpensive and commercially available today. Individual components support wireless communication, avoiding costly wired infrastructure installation. Pushing the data collection, storage, and processing into the cloud eliminates the need for expensive, special-purpose, on-site computing.

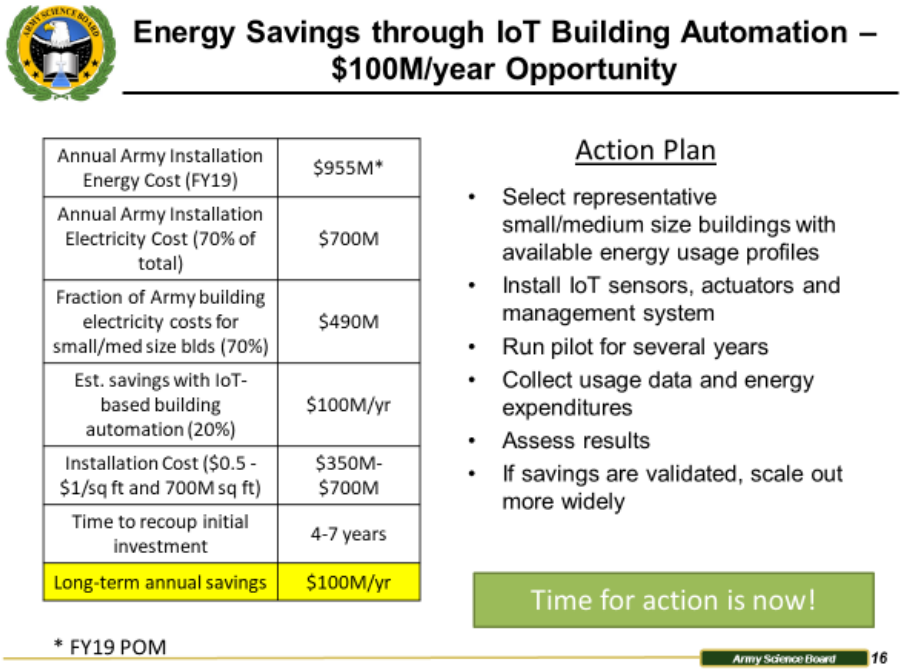


Highlighting the positive ROI of these systems in smaller buildings, PNNL reported a case study in which a 20,500 square foot building was retrofitted with an IoT-enabled, inexpensive, control system. The upfront investment of $20,000 (i.e., approximately $1 per square foot vs $2-$7 per square foot for a conventional building automation system) was recouped in four years, which included an annual 22% energy savings ($5,000 per year).

The ASB study team performed a high-level analysis to estimate how much of its small and medium size building energy cost the Army could expect to save from the installation of IoT-based building automation. Of the $955M that the Army is likely to spend on installation energy in FY19, the team estimates that perhaps $700M (i.e., approx. 70%) of the total amount will be spent on electricity. Assuming 70% of the Army's electricity costs are spent for small and medium size buildings,[10] the total Army cost for electricity in such buildings will be about $490M. Based on the PNNL case study, the study team estimates that if all these small and medium size buildings were outfitted with IoT-based building automation systems, the savings would reach about $100M/year (i.e., 20% of the total current annual cost). If the installation cost were $0.50 to $1 per square foot (based on the PNNL case study, but also assuming additional savings due to scale and technology advances in the next six years), the Army's total cost to install these

[10] The actual fraction of electricity used in buildings <100,000 square feet was 73% at Fort Benning in FY17.

systems would be approximately $350M-$700M, leading to a 4-7-year period to recoup the initial outlays, followed by an annual savings of $100M/year.



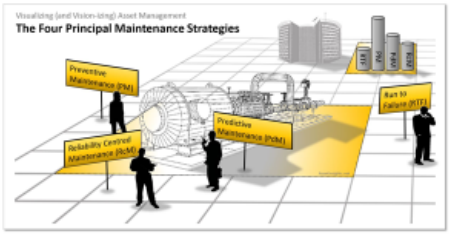
The study team believes the best way for the Army to move forward in developing smart buildings would be to run a multi-year, energy savings pilot project. The Army would select a representative set of small and medium size buildings at one or more representative Army installations. The set should be large enough and selected in such a way as to ensure that lessons learned from the pilot can be scaled and extrapolated to Army installations generally. These buildings should also be selected such that energy usage data from past years (pre-pilot) are available as a baseline against which to measure the impact of the pilot project. Inexpensive IoT sensors and actuators should be installed for the lighting, HVAC, and plug-based systems, and a cloud-based building management system should be acquired that permits collection, storage, and analysis of the data together with centralized control. If the actual savings afforded by the pilot system justify it, a wider roll-out should be undertaken across the rest of the Army's small and medium size buildings.

IoT offers the ability to optimize real property asset reliability, availability, and performance by analyzing specific technology, critical functions, age, and use performance history. It may be employed using existing sensors and data, new construction, and/or retrofitting facilities. Together, these techniques enable predictive maintenance for real property systems.

Predictive Maintenance for Real Property

IoT offers the ability to optimize asset reliability, availability, and performance taking into account specific technology, critical functions, age, and use and performance history

Independent maintenance studies have indicated the following average savings can be achieved by carefully balancing maintenance strategies:



Return on investment	Maintenance cost reduction*	Reduction in breakdowns*	Reduction in downtime*	Increase in production*
≤3X	≤30%	≤75%	≤45%	≤25%

* Annual returns

http://www.assetinsights.net/Glossary/G_Maintenance_Mix.html

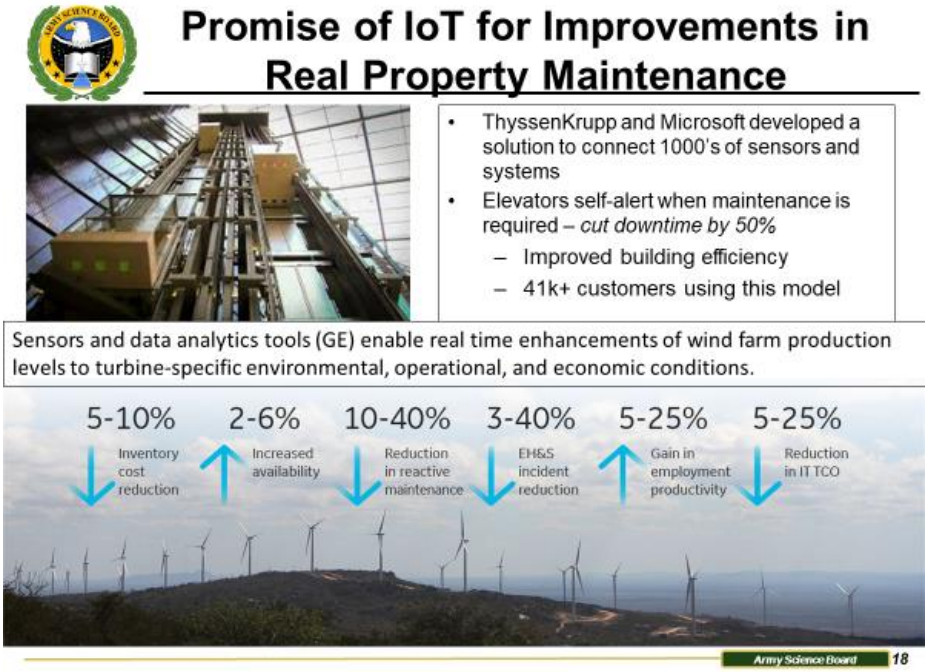
Army Science Board 17

The building automation systems (including servers and networks) are handled as facility assets, the same as elevators, HVAC, etc. Many of these systems operate independently, with routine maintenance programs based on set frequencies, "fix when fail" using corrective maintenance only, or "run to fail" for assets that are not critical or are at end of life.

The purpose of the maintenance program is to manage risk and reduce operating costs as well as to optimize the service life of the capital assets. Industrial maintenance programs are typically a mix of preventive, corrective, and predictive maintenance. Industry studies have shown that by carefully balancing maintenance approaches, significant improvements can be made cost reduction (up to 30% annually), reduction in breakdowns (up to 75% annually), reduced downtime (up to 45% annually), and an increase in production (up to 25% annually). Additionally, industry studies report up to 3x ROI,[11] which translates to cost savings and improved service delivery. For the Army, the benefits could go beyond cost savings to also improving readiness.

Predictive maintenance programs are not new. The IoT presents an opportunity already demonstrated in industry with advanced connected sensors, actuators, networks, data analytics, and machine learning. The improvements in optimization have not been available through traditional technologies.

[11] http://www.assetinsights.net/Glossary/G_Maintenance_Mix.html



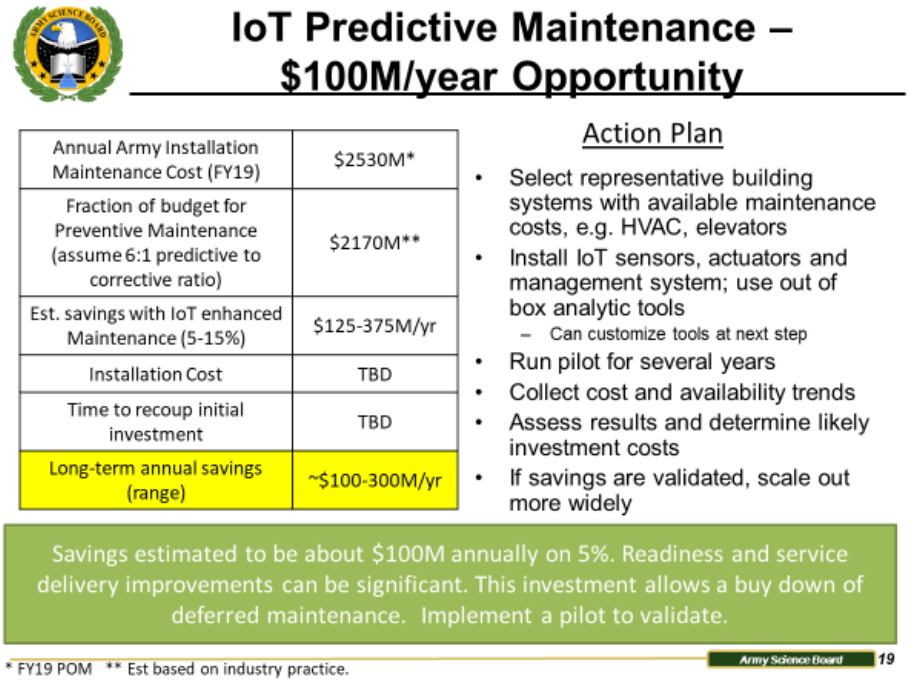
Examples of industry using IoT to significantly improve the maintenance of real property include:

1. ThyssenKrupp Elevator gained a competitive edge by focusing on reliability or "up time." The company's business model now sells the availability of the elevator service rather than the elevator itself. It significantly improved operations by drawing on the IoT and Microsoft technologies connecting its elevators to the cloud, gathering data from sensors and systems, and transforming that data into valuable business intelligence. They now offer something the company's competitors do not: predictive and preemptive maintenance.[12] Individual elevators self-monitor their usage and condition, alerting when maintenance is required. This approach tailors the maintenance program to the actual asset condition at the individual elevator, significantly increasing overall reliability and reducing downtime. ThyssenKrupp now has more than 10% of its asset base worldwide signed up for this service, representing over 41,000 customers and 120,000 elevators.[13, 14]

2. GE Renewable Energy assists wind farms drive safer and more reliable operations while facilitating optimal performance using sensors and data analytic tools. The tools monitor changes over time, including operational conditions and demands, equipment ageing and replacement, and upgrades/improvements. GE's approach enables dynamic performance management on an enterprise level using turbine-specific environmental, operational, and even economic conditions. Systems are continuously monitored, maintenance is

[12] https://azure.microsoft.com/en-us/resources/videos/thyssenkrupp-giving-cities-a-lift-with-the-internet-of-things/
[13] https://www.computerweekly.com/feature/AI-elevates-predictive-maintenance-for-Kone-and-ThyssenKrupp
[14] https://max.thyssenkrupp-elevator.com/en/

predictive based on specific asset conditions, and potential faults are detected early, avoiding costly emergency maintenance. Additional benefits have been seen in reduced inventory costs, reduction in safety incidents, and reduction in total cost of ownership.[15]

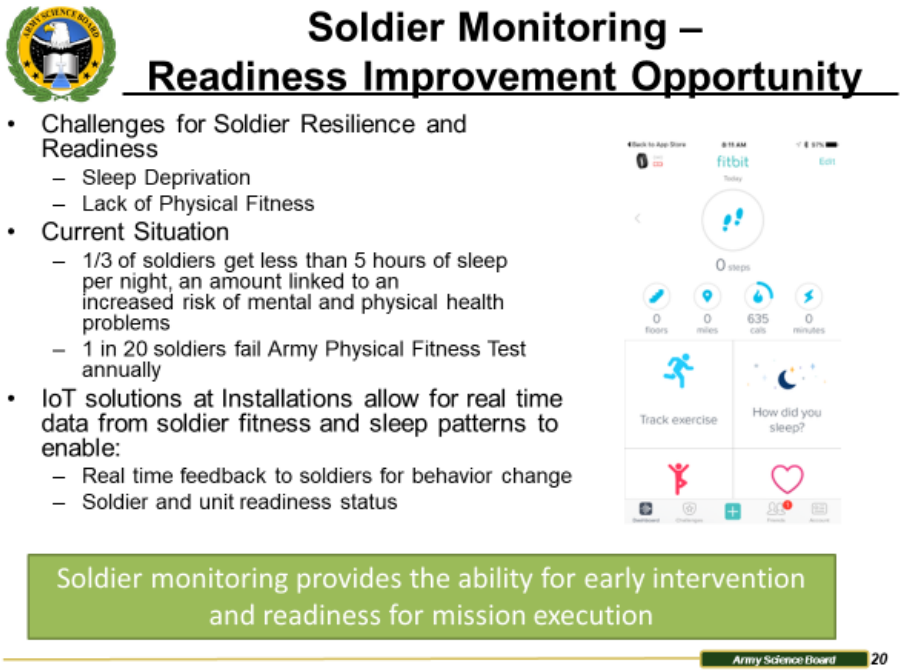


Based on the FY19 Program Objective Memorandum (POM) for Army Installations, the study team developed an evaluation of potential cost savings for IoT-enabled predictive maintenance. Against the installation maintenance program is $2530M in FY19, an industry standard ratio of 6:1 for preventive and corrective maintenance was applied, producing an estimated annual budget of $2170M. Based on industry reports of up to 30% savings from an optimized maintenance program, the study team evaluated a conservative range of 5-15% potential savings, allowing for the possibility that some optimization may already be done, resulting in a potential savings of $125M-$375M per year. Installation costs and time to recoup the initial investment will depend on the specifics of the pilot project, equipment, and installations selected. After recouping the initial investment, an annual savings of at least $100M and up to $300M was projected. In addition to cost savings, readiness and service delivery improvements should also be expected, and the investment should allow a buy down of deferred maintenance.

The study team believes the Army should run a pilot for several years to accumulate enough data on costs and availability trends. The pilot will use representative building systems with available maintenance costs, e.g., HVAC and elevators. Some systems may already be instrumented but not managed in a coordinated system. As needed, the pilot should employ IoT sensors, actuators,

[15] https://www.ge.com/content/dam/gepower-renewables/global/en_US/downloads/brochures/ge-digital-wind-asset-performance-management.pdf

and a management system using customizable analytic tools (making modifications as the pilot continues or later during the roll out). The pilot should be executed at sufficient scale to provide a realistic deployment strategy and costs.



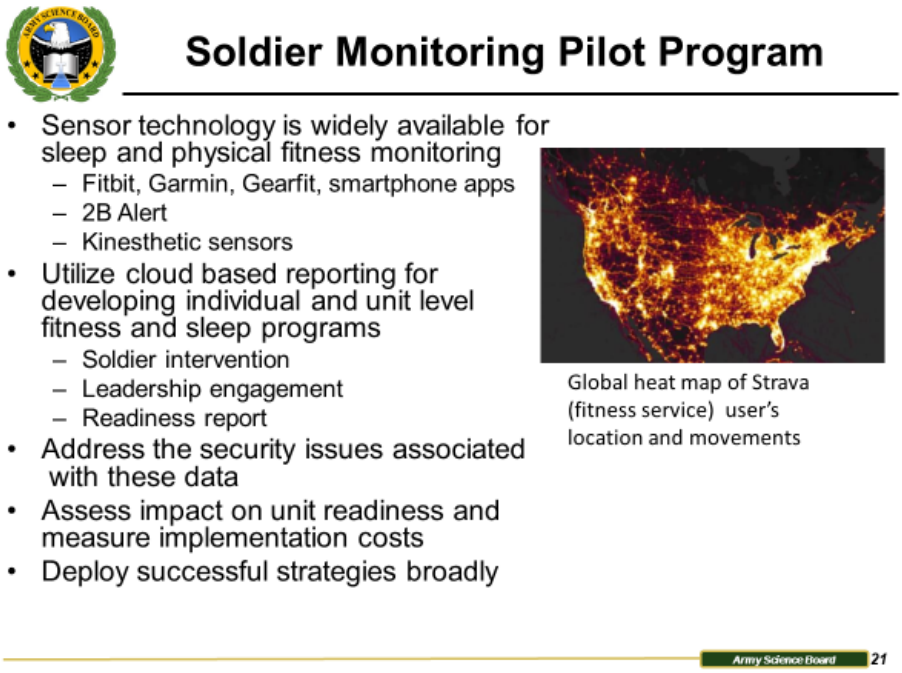
The IoT may also be employed to support Army readiness beyond real property operations to monitor Soldiers' fitness. One in twenty Soldiers fail their annual Army Physical Fitness Test and over 78,000 soldiers are clinically obese (Body Mass Index >30). In addition, one third of the Soldiers get less than five hours of sleep per night and 10% are diagnosed with a sleep disorder.[16,17] The effects of poor physical fitness and sleep deprivation are detrimental to both the individual Soldier's health and wellbeing and the Army's overall readiness, but as with predictive maintenance, the IoT may provide solutions to improving both.

The Army could leverage IoT technology to optimize individual Soldiers' physical fitness and sleep. Existing commercial technology allows for real time assessment and immediate feedback to foster behavioral change. Results could inform commanders' assessments of each Soldier's and their unit's readiness.

Beyond the technology, and perhaps more fundamental to optimizing Soldiers' fitness and readiness, the Army will need to understand and define individual performance tasks. The Army made advancements to that end when it established gender neutral standards for combat arms military occupational specialties (MOS).

[16] The Army Surgeon General, Performance Triad: Strengthening the Health Readiness of the Total Force.
[17] Keller, Jared, Task & Purpose, May 17, 2017

Once the tasks are defined, techniques such as those used at the U.S. Olympic Team Training Center, the Auburn University School of Kinesiology, or the University of Pittsburg Neuromuscular Research Laboratory may be used to monitor Soldiers. For example, cameras and/or motion and torque sensors are increasingly affordable and could become regular features at installation Fitness Centers.

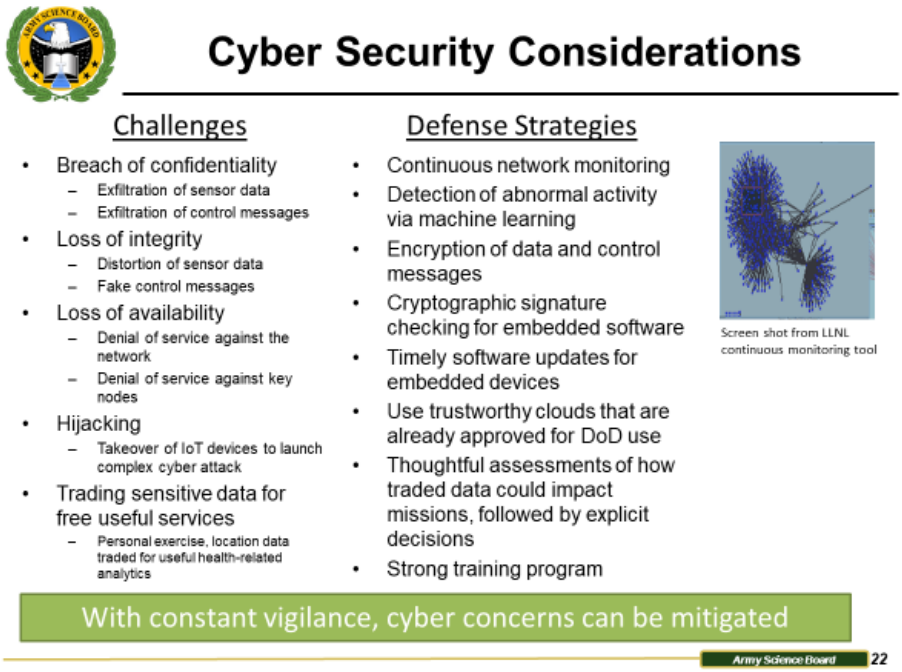


The data generated by IoT monitors will become readily available to Soldiers and may be accessible, in varied forms, to supervisors and commanders. Recent breeches in the security of commercial fitness trackers provide insight on maintaining operational security while using these devices.[18] To optimize operational security (OPSEC) and prevent similar occurrences, the data generated by these devices or similar devices must be secured.

Multiple, readily available sleep assessment tools may help Soldiers and commanders with measurable indicators of the Soldier's sleep and related cognitive functioning. The Army Medical Research and Materiel Command developed a mobile tool, "2B Alert," which provides data regarding fatigue, sleep, and cognitive functioning. [19] The Air Force developed a similar technology, the "Fatigue Avoidance Scheduling Tool (FAST),"[20] that improved pilots' readiness by optimizing their sleep and cognitive performance.

[18] The data generated by these privately-owned devices was not secured and revealed the location of U.S military operational facilities in Syria, risking Soldiers' lives. See Gallager, Sean, Ars Technica, August 7, 2018.
[19] http://techlinkcenter.org/summaries/2b-alert-personalized-alertness-and cognitive-performance-app
[20] Eddy, Moise, Miller, & Welch, 2009

The Army has pioneered Telemedicine and eHealth for over 25 years. Applications to improve the health and readiness of the force are already in use, and many more will be available in the smart installation as the IoT leverages data analysis in new areas.



The Army's move towards the use of IoT devices, techniques, and technologies must include a careful analysis of the potential risk of cyber-attack. The Army should seek to use IoT in a way that maximizes value while minimizing the cost to provide mission resilience against attacks, while making it harder on the adversary, i.e., maximizing the adversary's workload to execute a successful attack. The National Institute of Standards and Technology (NIST) has developed a risk management framework that should help the Army model how cyber risks can be mitigated in a systematic way.[21]

The study team identified classes of cyber exploitation relevant to the use of IoT for Army installations:

- Breach of confidentiality – building monitoring sensor data indicating which parts of which buildings are occupied as a function of time could be exfiltrated by an adversary, as could the messages from the central control systems to individual lighting and HVAC actuators. These sensor data and control messages could compromise OPSEC by aiding an adversary's understanding of how buildings are being used.

- Loss of integrity – data coming from building sensors could be distorted. For example, counterfeit control messages could be sent, giving the adversary the ability to destroy

[21] https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

parts of a building by, e.g., causing a fire, or making a building uninhabitable at a crucial time by e.g., raising or lowering the temperature to extremes.

- Loss of availability – an adversary could disable both the sensors and the control systems, making it impossible for the automated system to control building services, at which point the building would be uncontrollable and uninhabitable.

- Hijacking – the Army's IoT devices could be attacked in such a way as to be repurposed for other adversary missions. For example, the 2016 "Dyn" distributed denial of service attack on the Internet Domain name System caused major Internet platforms and services to be unavailable to large swaths of users in Europe and North America.[22] The activities were executed through a botnet affecting various IoT devices including printers, IP cameras, residential gateways, and baby monitors.

- Trading sensitive data for free, useful services – while millions of people, including military personnel, use personal health and fitness monitors (e.g., Fitbits, etc.) to analyze their health and exercise programs, they are revealing personal information, including location.[23]

While there is no single solution for mitigating all types of cyber exploitation, the use of best practices and timely adaptation to evolving threats can mitigate much of the risk associated with employing IoT on Army installations. Some defensive strategies the Army would likely apply include:

- Continuous host and network monitoring, with automatic detection of malicious and abnormal activity. Advances in machine learning will make this more manageable.

- Use of encryption and digital signatures for all sensor data and control messages, making it harder for adversaries to gain the situational awareness to counterfeit data.

- Cryptographic signatures for all software with hardware roots of trust (e.g., trusted platform modules), making it difficult to install malicious software on IoT devices.

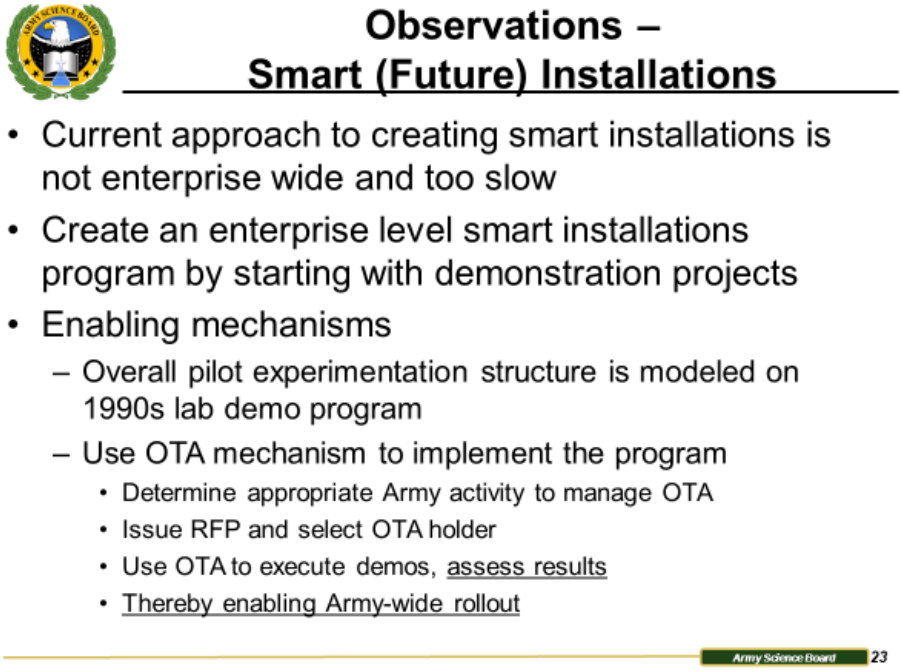
- Timely software updates to patch vulnerabilities on devices. For wireless devices, the Army will need to select vendors with security architectures that support these updates.

- Use of DoD-approved, trustworthy, cloud computing infrastructure. The Army should avail itself of low-cost, trusted, cloud services provided by the DoD.

[22] https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
[23] https://decorrespondent.nl/8480/this-fitness-app-lets-anyone-find-names-and-addresses-for-thousands-of-soldiers-and-secret-agents/260810880-cc840165

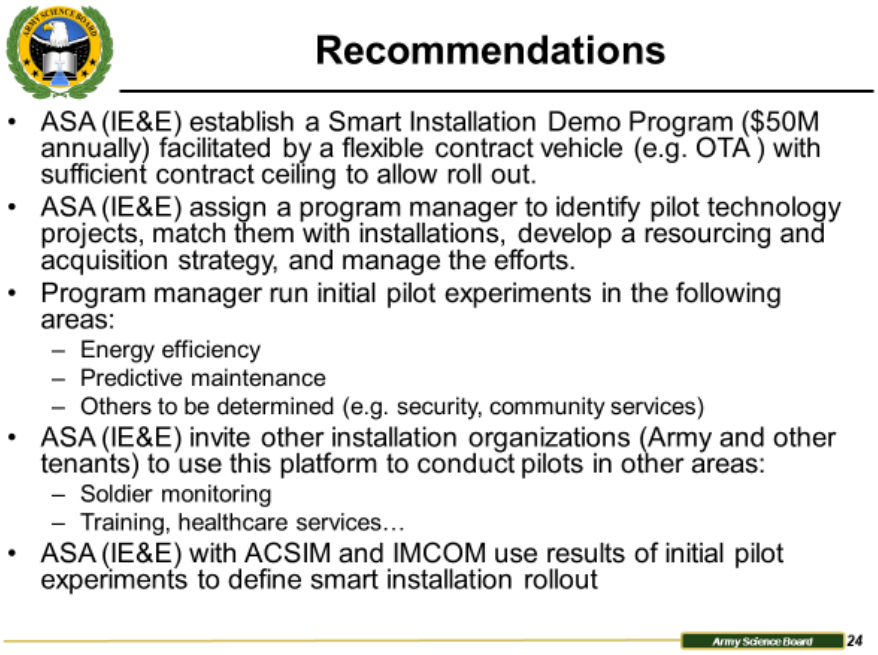
- Assessments of the trades between desired functionality and control of data privacy that will be translated into policy.

- A strong training program to ensure all Soldiers, civilians, and Army installation tenants practice good cyber hygiene.



The study team made additional observations associated with transforming installations into force projection platforms. Interviews with various garrison commanders revealed each installation had small IoT-enabled pilot projects but none developed an enterprise approach to the problem/solution. Furthermore, resources for these pilot projects were limited and lessons learned were not captured. The Army should have an enterprise approach for converting installations (as traditionally conceived) into force projection platforms, thereby enhancing its strategic support capabilities. To successfully deploy IoT technologies, the Army should identify enterprise objectives and start with demonstration projects at CONUS installations. Novel contracting approaches will be essential for the timely employment of rapidly developing technologies. Some options include the use of Other Transaction Authority (OTA) to engage industry and academia for a broad range of research and prototyping activities. The OTA may be used for executing demonstrations, assessing results, and enabling an Army-wide rollout of technology and systems. To successfully execute the demonstration projects, an Army activity will need to be identified to manage the OTA.

RECOMMENDATIONS



A general lack of funding for experimentation with technologies to improve housing and installation activities and services makes funding for experiments with IoT even more scarce. Though introducing IoT does raise concerns of vulnerabilities and risk, it is also an opportunity to create test beds and pilot projects at Army installations. Cyber security can be maintained with proper training and risk mitigation in proportion to the amount of reliance placed on IoT.

The study team's findings identified opportunities for utilizing IoT on installations to provide cost savings, improved readiness, and potential recruitment incentives for the future Army Soldier. The study team's recommendations focus on developing pilot programs to demonstrate the benefits of IoT and data analytics. By adopting the recommendations, the Army can transform installations to serve as more strategic elements to support operational capabilities.

APPENDICES

APPENDIX A. TERMS OF REFERENCE

DEPARTMENT OF THE ARMY
OFFICE OF ASSISTANT SECRETARY OF THE ARMY
INSTALLATIONS, ENERGY AND ENVIRONMENT
110 ARMY PENTAGON
WASHINGTON, DC 20310-0110

SAIE

AUG 1 3 2018

MEMORANDUM FOR Dr. Leonard W. Braverman, Chairman, Army Science Board, 2530 Crystal Drive, Suite 7098, Arlington, VA 22202

SUBJECT: Army Science Study entitled "The Internet of Things (IoT): Creating "Smart Installations"

1. I request the Army Science Board (ASB) conduct a study entitled, "The Internet of Things (IoT): Creating 'Smart Installations'." The objective of the study is to further develop the efforts of ASB's FY16 study, "The Military Benefits and Risks of the Internet of Things." Specifically, this study should advance the Army's knowledge of potential risks and advantages gained by leveraging the use of the IoT in creating "smart and resilient" installations that enhance Army readiness.

2. Commercial industry has invested heavily in the development and implementation of IoT to make processes more efficient while at the same time cutting costs. In recent years, industry has deployed IoT at an exponential rate, fueled in part by advances in cloud computing and data analytics. While the Army has begun to use some IoT applications, it's not taking full advantage of industrial-level advances thus, it isn't experiencing the full benefits of IoT-related efficiencies.

3. To assist the Army in further exploring the potential of IoT applications, the ASB study team's tasks will include, but not be limited to, the following:

a. Recommending what the Army should consider when designing the core strategy for data collection and analytics, incorporating cyber security perspectives, and performance efficiencies.

b. Exploring how Army installations can partner effectively with industry, academia, and local communities to implement IoT approaches in a cost-effective manner.

c. Recommending possible Army specific IoT applications for installations.

d. Providing a potential approach or framework the Army could use to prototype, test and infuse IoT technology over time.

SAIE
SUBJECT: Army Science Study entitled "The Internet of Things (IoT): Creating "Smart Installations"

4. A briefing with findings and recommendations will be provided by October 31, 2018 to the Assistant Secretary of the Army (IE&E) and the Assistant Chief of Staff of the Army for Installation Management. The study will operate in accordance with the Federal Advisory Committee Act and DoD Directive 5105.4, DoD Federal Advisory Committee Management Program. It is not anticipated that this study will need to go into any particular matters regarding the meaning of United States Code, nor will it cause any member of the study team to be placed in the position of acting as a procurement official that may constitute a conflict of interest.

JORDAN GILLIS
Acting Assistant Secretary of the Army
Installations, Energy and Environment

APPENDIX B. STUDY TEAM MEMBERS

Gisele Bennett, PhD., Chair
(Florida Institute of Technology)

COL William Crowder (USA, Ret.), Vice Chair
(LMI)

Study Team Members

Vivian Baylor
(Independent Consultant)

Mary Crannell
(Idea Sciences)

MG Lester Martinez-Lopez, M.D.
(USA, Ret.)

Evelyn Mullen. P.E.
(Los Alamos National Laboratory)

Tom Ramos
(Lawrence Livermore National Laboratory)

Allan Willner, PhD.
(University of Southern California)

Mary Anne Yates, PhD.
(Ames National Laboratory)

Marc Zissman, PhD.
(MIT-Lincoln Laboratory)

Senior Advisor – Jim Shields

Study Manager – Vince Bullard

Pentagon Liaison – John Thompson

Tech Writer/Editor – Mark Swiatek

Areas of Expertise

Physics, Engineering, Computer Science, ISR, Optics, Cyber, Network Architecture, Human Dimension, Program Management, Sensors, Logistics, Acquisition, Sustainment, RFID, Machine Learning, Physics, Medical and Human Performance

APPENDIX C. LINES OF INQUIRY AND VISITATIONS

Private Industry:

- Microsoft Headquarters
- Synexxus, Inc
- Cougaar Software
- NVIDIA Headquarters
- Booz-Allen
- C3 IoT Headquarters
- Honeywell

Government and National Labs:

- Lawrence Livermore National Lab
- Mr. Daniel Rhoades, Robins AFB 21st Century Partnership Program
- Col. Massey, Warner Robins AFB
- CIO, Arlington County VA

Academia:

- UC Berkeley: The Center for Long Term Cybersecurity; The Center for Information Technology Research in the Interest of Society (CITRIS); The Banatao Institute Headquarters
- Georgia Tech: Center for Resilient Systems
- Florida Institute of Technology: Human Factors Lab

Army Leaders/Installations:

- COL Joe Holland former Garrison Commander, Camp Humphries Korea
- Joint Base Lewis McChord
- Mr. Gary Wang, former CIO/Deputy G6
- Mr. Lloyd Caldwell, Director of Military Programs, USACE
- Dr. David Pittman, Director, ERDC
- Mr. Jordan Gillis, Acting ASA, Installations, Energy and Environment (IE&E)
- Mr. Richard Kidd, Acting Deputy ASA, IE&E and DASA, IE&E Strategic Integration
- LTG Gwen Bingham, Assistant Chief of Staff for Installation Management (ACSIM)
- Mr. J. Randall Robinson, former Acting Deputy ASA, IE&E
- Mr. Paul Cramer, DASA, IE&E, Installations, Housing and Partnerships
- COL Kim Peeples, Garrison Commander, Ft. Myer, VA
- Mr. George Steubner, Deputy Garrison Commander, Fort Benning, GA
- Installation Management Command (IMCOM), Fort Sam Houston, TX
- NETCOM
- TRADOC Mad Scientist: Multi-Domain Battle in MegaCities; Smart Installations