



Army Science Board
Fiscal Year 2016 Study

The Military Benefits and Risks of the Internet of Things

April 2019

Department of the Army
Office of the Deputy Under Secretary of the Army
Washington, D.C. 20310-0103

DISTRIBUTION A. Approved for public release: distribution unlimited. Other requests for this document shall be referred to Executive Director, Army Science Board, 2530 Crystal Drive, Suite 7098, Arlington, VA 22202-3911

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 the Army (SA) and the Chief of Staff, Army (CSA). Statements, opinions, conclusions, and recommendations contained in this report are those of the Army Science Board and do not necessarily reflect any official position of the United States Army or the Department of Defense.

This document is available from the Defense Technical Information Center (DTIC) at www.dtic.mil.

TABLE OF CONTENTS

Executive Summary.....	1
1. Introduction	7
1.1 Terms of Reference	7
1.2 Review of Past Studies	7
2. Background	10
2.1 Definition of IoT	10
2.2 Industry Use of IoT	11
2.3 Government Use of IoT	12
3. Use Cases	15
3.1 Immediate Opportunities	15
3.1.1 Power by the Hour	15
3.1.2 Smart Cities	17
3.1.3 National Training Center (NTC) Test Bed	18
3.2 Intermediate Opportunities	20
3.2.1 Intelligence, Surveillance, and Reconnaissance (ISR) via IoT.....	21
3.2.2 Disrupting and Controlling Red and Grey IoT Systems	22
3.2.3 Research & Development (R&D) in IoT.....	22
3.3 Long Term Opportunities.....	23
3.3.1 IOT as Input to Big Data Analytic Engines.....	23
3.3.2 Commercial, Intelligence Community, and Army Solutions	25
4. Cross-Cutting.....	26
4.1 Policy	26
4.2 Cyber	26
4.2.1 Risk Analysis – An Example	27
4.2.2 Broad Categories of IoT Cybersecurity Risk Facing the Army.....	29
4.2.3 Software Security	29
4.2.4 Cyber-Related Finding.....	29
4.2.5 Recommended Path Forward	30
5. Findings and recommendations.....	32

APPENDICES

A. Terms of Reference.....	34
B. Study Team Members.....	36
C. Lines of Inquiry and Visitations.....	37
D. ASB Approved Briefing with Findings and Recommendations (28 July 2016)	40
E. Glossary of Terms, Abbreviations, and Acronyms	58

LIST OF FIGURES

2.1 IDC top Industry Based on 5 Year CAGR (2016-2021)	12
3.1 Campaign of Learning for Military IoT	15
3.2 Power by the Hour Methodology for Locomotives	16
3.3 NTC and IoT	19
3.4 IoT Creating Value	20
3.5 IoTINT for Situational Awareness and Understanding	22
3.6 Four V's of Big Data (McKinsey Global Institute)	24
4.1 Cyber Attack on Vehicles: Risk Comparison (Notional Example)	28

EXECUTIVE SUMMARY

The Internet of Things (IoT) is a broad term that encompasses everything, everywhere, to the extent that by 2025, a device's lack of connection with the Internet will be the exception, and no one will be able to avoid some contact with it. Even if that prediction comes partially to pass, IoT is something the Army needs to look at to understand how it will impact operations, people, and strategy.

The study team views the IoT as a melding of the industrial and communications revolutions. Consider, for example, how the machine gun improved fires and re-shaped conflict; how the steam engine improved logistics and mobility; and the jet engine enabled global force projection. On the communication side, radio technology improved warfighter effectiveness, and Internet-based capabilities introduced near real time situational awareness. Each technology on its own produced evolutionary effects in combat operations. Now, the IoT has the potential to build upon these and other previous advances and to produce a combinatory effect that will re-shape the battlespace. Here's what makes IoT different:

- Very large scale (2020 est.: 20 Billion devices, 200 Billion tags)
- Totally pervasive (all over the world)
- All things connected (even threads in clothes)
- Very low cost (pennies per tag)
- Data analytics

The proliferation of sensors throughout society and data generated from those sensors will impact the Army's warfighting capability. And because IoT is spreading rapidly today, the timeframe for the Army to likewise use these technologies is short term, five years or less.

For the Army, the "things" of the IoT are its Soldiers, equipment, vehicles, and all the assets it needs to win a battle. To the extent that commanders can improve their awareness of the condition of their things, they will have a better understanding of how to optimize the force for a given mission. The level of fidelity the IoT can provide commanders has the potential, if leveraged properly, to enable near real time tailoring of force packages for each unique mission.

To present the potential for Army use of IoT, the study team developed use cases, progressing from what's easy to do today (crawl) to what's going to require more investment and planning (walk to run). The use cases also addressed three questions derived from the Secretary of the Army's (SECARMY) Terms of Reference (TOR):

- How is IoT transforming our world?
- What are the opportunities for the Army?
- What are the consequences of doing nothing?

Early on in the course of its data gathering, the study team adopted the International Organization for Standardization (ISO) definition of IoT:

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.

Focusing on the last element of the definition—“react”—each of the use cases demonstrates how the Army can employ IoT to transform data into actionable information. The Army can use IoT to reduce and find efficiencies in maintenance, readiness, facilities management, and logistics. These are the same types of efficiencies that are driving commercial industry’s adoption of IoT. But the Army can take the IoT even further by focusing more on effectiveness. The IoT may be employed to improve situational awareness in the battlespace, command and control, maneuverability, autonomy, and Soldier performance.

The crawl/walk/run construct of the use cases presents a sequential development of IoT by the Army where initial efforts serve as the foundation for later, more advanced capabilities.

1. Crawl (2-5 years). The Army uses commercial, off-the-shelf (COTS) equipment to realize efficiencies in its infrastructure management and to improve readiness by giving commanders more meaningful situational awareness on the status of their Soldiers and equipment. Developmentally, the Army would work to fully understand IoT employment of its assets. The use cases below represent easy adaptations into what the study team describes as “know thyself”-type IoT applications.
 - a. Power-by-the-Hour – Implemented by many industries, including General Electric (GE) which conducts condition-based maintenance (CBM) using sensors and prognostics to monitor its engines. GE added another layer to CBM by developing a digital twin for each engine, pushing maintenance beyond monitoring and into more predictive models. Similarly, ThyssenKrupp and Microsoft developed a solution to connect thousands of sensors and systems in its elevators to decrease maintenance stoppages and improve “up time.”
 - b. Smart Forts – The development of smart cities in the civilian sector could translate to Smart Forts for the Army. The Army has already begun to implement some elements of Smart City technology in water and energy management, but much more could be done to exploit the applications in security, traffic management, health care, and personnel readiness.

2. Walk (5-10 years). The Army uses a mix of COTS and Army-specific technology to improve situational awareness on the battlefield and in the logistics pipeline supporting Soldiers in battle. It would also develop Army-unique analytics frameworks to more fully exploit IoT beyond traditional industry uses. The Army would also influence the direction of commercial industry research and development (R&D) efforts to move them in directions relevant to the Army, serving as a transition partner, where possible. These use cases represent steps into what the study team describes as “know thy adversary”-type IoT applications.
 - a. Exploit Smart Cities – Once the Army masters its own Smart Fort technology, it could develop proficiency in exploiting adversaries’ smart cities. Information such as traffic control, vehicle types and occupancy, building occupancy, appliance and utility control (e.g., smart homes) inventory status/stock (food, medical, etc.), sewer contents, disease trends, etc., could help Soldiers assess and determine the best avenues for ingress and egress, patterns of life, target locations, and the difference between adversary forces (Red) and civilians (Gray).
 - b. IoT Based Intelligence (IoTINT) – When fused with other intelligence data, IoT data will provide better situational awareness for Soldiers operating in cities, especially megacities. The study team adopted “IoTINT” as a byname to impress its relevance with other intelligence sources (SIGINT, HUMINT, etc.), especially for the planning (the state/attributes of a city) and execution (real-time information) of Army operations. In sum, wherever there’s an IoT, there’s intelligence to gather.
3. Run (<10 years). The Army uses technology it developed to improve combat effectiveness, e.g., to enhance autonomous vehicles, to exploit IoT in contested areas, etc. Research in IoT advancements should be fully funded to maintain the Army’s advantage in the technology.
 - a. Disrupt IoT – A step beyond exploiting IoT for information, the Army’s ability to control and/or disrupt both adversary and civilian IoT to produce effects will enhance its combat effectiveness. Alternately, the Army will also need to defend against such actions by adversaries.
 - b. Augment Autonomy – As urban areas further develop IoT and become dependent on it to manage basic functions (traffic control, utilities, security, etc.), autonomous combat systems can be designed to tap into native IoT to use as a non-organic sensor. The ability to process IoT and local sensor data within the autonomous system implies a future Army requirement to develop capabilities for data fusion at the edge.

There are several areas where the use cases overlap in terms of capabilities, policy, technology requirements, etc. The study team prioritized four cross-cutting issues the Army needs to consider moving forward with IoT:

1. The National training Center (NTC). The Army has an opportunity to harvest data during training at NTC. Currently, the Army conducts at least 10 Brigade Combat Team (BCT) training evolutions each year at NTC. During these evolutions, the BCT's maneuver data is recorded over an ATT 4G/5G cell network. NTC's exercise opposing force (OPFOR) uses the same network to conduct its exercise operations against the BCT in training. A significant amount of logistical platform data is recorded on each vehicle and downloaded after the training exercise. The Army could enhance the existing data with additional recorders and sensors, pull all the data into an analytic framework—yet to be designed—that would fuse the data and enable deep learning in areas such as situational understanding, combat requirements, and evolutionary tactics.
2. Policy and Requirements. The Army's requirements community has no experience with IoT systems and isn't writing requirements. Without requirements, the acquisition community has no program plan to integrate IoT technology into any platform or product. Further, there's a fear of "connected" devices and the study team heard anecdotal evidence of conscious decisions made to remove or disable IoT-like capabilities from systems such as commercial vehicles. Likewise, Army Centers of Excellence (CoEs) haven't internalized the impact of IoT or its potential benefits for the Army leaving little to no advocacy for pursuing the technology. Thus, the Soldiers don't have access to IoT enabled combat capabilities. In short, the Army has not yet developed a vision and strategy to use IoT.
3. Cyber Security and Risk. The Army needs to understand risks associated with the deployment of IoT. The study team developed a notional formula for understanding risk as a function of a system's or unit's vulnerability, the method of exploitation, the impact in scale of the attack, and the perpetrator's intent. The study team applied this formula to two situations: an attack against an automobile and an attack against a deployed Army vehicle. Obviously, the risk to the Army vehicle in most phases of conflict is much higher than risks faced in commercial IoT cyber-attacks. The resulting damage to expensive equipment, probable injury and/or loss of life, possible mission degradation, etc., carry greater consequences than a stalled SUV on the highway, so the Army needs to fully understand the risk and vulnerabilities of IoT to get ahead of the threat.
4. Doing Nothing. If the Army were to ignore IoT and fail to understand, develop, and employ the technology, it would simply cede that battlespace to adversaries. This would pave the way for adversaries to successfully exploit U.S. and allied IoT systems, causing secondary effects for the Army such as overpayment for maintenance systems (e.g. vehicles), the creation of waste in buildings and infrastructure management, and unacceptably low readiness due to wrong data, inefficient management, etc. On the battlefield, the Army could also suffer limited situational awareness leading to ineffective operations, especially in urban areas.

From its data gathering and analyses, the study team made findings in five categories:

1. Army is not taking full advantage of industrial advances in IoT for warfighter effectiveness and cost savings:
 - a. Industry is investing and implementing IoT at an exponential rate
 - b. Success in industrial deployment of IoT is due to the reduced cost of deployment, advancements in cloud computing, and data analytics
 - c. Industry is using standards bodies to develop interoperability of IoT and there is no evidence of Army participation in these bodies
2. Army does not have IoT system level requirements that are needed for adoption on the battlefield and in the Army industrial base
3. There are cyber and network connectivity challenges that the Army has not yet solved
 - a. Current commercial IoT does not provide sufficient cyber security for critical Army missions
 - b. Some battlefield environments offer limited network connectivity
4. IoT issues cross policy and legal boundaries that must be resolved for Army applications
5. Army can harvest data and develop analytics that identify improvements of warfighter effectiveness:
 - a. NTC and other sources to inform on uses and defenses for IoT enabled things to include an EW environment
 - b. IMCOM as it permeates posts, camps, and stations (government and non-government sources)
 - c. AMC installations for the Army industrial base (depots, arsenals, ammunition storage facilities, and ocean ports)
 - d. MEDCOM as it pertains to Soldier performance

Based upon these findings, the study team made the following recommendations to Army senior leadership:

1. AMC: identify the appropriate platform to implement power by the hour using Army railroad as an initial pilot to demonstrate cost savings and readiness improvements

2. AMC and IMCOM: expand existing efforts in depots and smart forts by utilizing smart cities technologies for cost savings, and efficiencies
3. MEDCOM: identify Soldier performance data that are important for battlefield awareness
4. G3/5/7 and OGC: update policies for both legal and implementation issues required to utilize IoT
5. DUSA: task AAG to create an analytics framework for experimentation for knowledge, acceptance, and development of DOTML-PF that will:
 - a. Support Blue on Blue and Blue on Red analysis for a tactical analysis (SME: FORSCOM, MEDCOM)
 - b. Support Blue on Blue and Red on Blue, OPSEC assessments (SME: FORSCOM, MEDCOM, and AMC)
 - c. Inform requirements process across all Army (SME: TRADOC and ASA(ALT))
6. TRADOC: define requirements for IoT systems and have representation on R&D programs related to IoT
7. G6: actively participate in IoT commercial standards bodies to represent the Army's interest
8. ARL: advocate and co-fund (e.g. with DARPA or IARPA) research programs around
 - a) offensive use of adversary's IoT (blue on red/grey)
 - b) adapting the analytics from IoT to disadvantaged (intermittent connectivity, low data rate) networks
9. ASA (ALT), CIO-G6, G3/5/7, AMC, & ARCYBER: include IoT considerations in Army cyber resiliency efforts
10. ARCYBER: develop a risk mitigation strategy for inclusion of IoT in military operations and platforms
11. ARCYBER: conduct adversarial cyber red teaming using IMCOM smart forts as test beds

1 INTRODUCTION

Throughout the commercial industry sector, the internet of things (IoT) acts as a game changing technology, providing increased situational awareness, efficiencies, and cost savings. There's great potential for the Army to realize similar benefits by connecting devices throughout its enterprise systems.

1.1 TERMS OF REFERENCE

To assist the Army in assessing the potential benefits of IoT, the Acting Secretary of the Army requested the ASB conduct this study to "determine the advisability of the Army applying the commercial practice of networking civilian physical systems into a military analog of the internet of things" (see Appendix A). The study team's specific tasks included:

- a. Establishing which military functions and systems should be networked into an integrated tactical network, to include systems necessary to provide a comprehensive situational awareness to the military formation and other military systems that could exploit that situational awareness.
- b. Addressing the vulnerability of such a concept, including risk as a function of the level of integration, and recommending architectures that minimize this vulnerability.
- c. Assessing the performance implications of such an integration and the tradeoffs between performance and vulnerability.
- d. Assessing the process for determining, on a continuing basis, via Red Teaming and other techniques, the balance of performance improvement and vulnerability.

The study team was also asked to review relevant studies performed by DoD science boards and the National Research Council.

1.2 REVIEW OF PAST STUDIES

Though the Obama Administration shows interest in promoting technology, there's not much evidence of government leadership and sponsorship for intergovernmental IoT policy or interagency information sharing. It's yet to be determined how leadership will address IoT and fix responsibility beyond the definitions of IoT drafted by the National Institute for Standards and Technology (NIST).¹ Because IoT now permeates information technology and systems of systems, most of the Army has vested interests and responsibilities in identifying platforms that will benefit from IoT.

¹ NIST Publication 800-183 "Network of Things" Jeffrey Voas July 2016.

According to an Amazon.com report, IoT spending is growing at a rate of 17 percent and is expected to reach over \$1 trillion by 2019. By then, it will affect most aspects of organizations and systems involved with manufacturing, transport, insurance and healthcare. Commercial development of IoT will continue to drive efficiencies and cost reductions that will eventually force adoption by the government into its operations. The Army will benefit by leveraging IoT efficiencies that can be tailored to weapons platforms, logistics, and C4ISR systems. However, strategic guidance and a more deliberate planning process is essential to educate, recruit, and retain IoT expertise.

The Center for Strategic and International Studies (CSIS) made the following suggestions in leveraging IoT innovation:

- Enhance Logistics Management such as real time fleet management, inventory management and base energy efficiency management
- Build out IoT enhancing capabilities such as commercial satellites, high altitude communications relay platforms, cube sat technology, and security overlays for commercial devices and applications.

The CSIS study also recommends that IoT, like all technologies, needs common standards and protocols to enable quick and efficient adoption. The government can also pursue innovative ways to incorporate IoT, such as frequent acquisition requirement updates, adoption of agile software development, and platform as a service contracting methodology.

In the Department of Commerce, NIST has taken the first steps to define five building blocks of IoT in the draft regulation entitled “Primitives and Elements in the Internet of Things Trustworthiness.” The five network and IoT attributes that help define and compare common standards and protocols are: sensor, aggregator, communication channel, e-utility, and decision trigger. According to this report, primitives allow for analytics, arguments in IoT use cases, and support IoT trustworthiness by using encryption as an example to protect systems. This initial effort to define standards and methodologies may allow government and industry to have a common language, standards and protocols in discussing IoT.

Several IoT systems could prove to be important to improving Soldier situational awareness when connected data provides a common operating picture and a way for military members to understand their real time environment. Big data and analytics provide leaders with improved decision-making tools in evaluating data and scenarios. These industry developments need to be evaluated for efficiencies and cost savings to better communicate the value of IoT to the Army, DoD, and government. To that end, a recent IBM report on the topic identifies the following benefits from adopting IoT:

- Scale driven data dominance to expand capacity and build on data driven initiatives

- Scale collaborative innovation creates cross agency, cross sector user centered information platforms that improve service delivery by matching user needs and capabilities that expands economic development
- Promote innovation by acquiring the best possible talent and safeguard information; Prioritize Evidence Based Innovation through testing, evaluation and analytics.

Other studies show opportunities for remote monitoring and accident prevention, maintenance support, common operating picture (COP), facility utilities management, and reality training.²

The Army will greatly benefit by leveraging IoT and the capabilities from other services, agencies, industry, academia and nationalities. Resource constraints within DoD make IoT efficiencies and cost savings attractive, but leadership must fix responsibility to study and evaluate IoT for effective implementation. In the Army, IoT falls into information technology, communications, and cyber security, thus Army Chief Information Officer/G-6 (CIO/G-6) will play a crucial role in developing IoT policy and guidance.

The need for leadership will become more acute because the Army purchases commercial products and IoT is slowly becoming part of systems of systems combat platforms and operational concepts. The requirements for these need to be formalized, but the Army doesn't have IoT systems level requirements. Leadership will be instrumental in educating the work force, establishing guidance, policy, and strategic planning. Effective communications and recognition of the contributions of IoT is key to retaining and further educating the work force for the Army to take full advantage of industrial advances.

² Kimball, Vossell, Ertell, Onignanjo, "Department of Defense and the impact of the Internet of things", Aim White Paper, 14 Dec 2012.

2 BACKGROUND

A society's technological advances affect how it conducts warfare. Two events have allowed the U.S. to reach its superior military capabilities: the Industrial Revolution and the Communications Revolution.

With the invention of the steam engine in the 18th century, mankind no longer had to rely on wind, water, or horse power to drive either industrial production or transportation. The evolution of motorized trains, boats, cars and airplanes have led to supersonic jets and nuclear submarines as part of the development of cutting edge warfighting tools. A major result of this is a dramatic reduction in the time required to initiate or respond to changing security needs.

Likewise, the invention of the telegraph in the mid-19th century collapsed the time required to communicate over long distances from days or weeks to minutes or seconds. The progression from telephone to radio to television to internet has vastly increased the amount of information that can be communicated instantaneously. Now, society is faced with the problem of how to pull trusted, actionable knowledge out of all the raw information.

The ubiquitous use of miniaturized sensors in a rapidly increasing number of automated systems combined with ever more sophisticated methods of handling data has led to the merging of the two types of expanding technologies into the IOT. It's not surprising to think that timers on lights and programmable thermostats would be incorporated into computer-controlled security systems, but the number of applications exploding into all facets of society, from tracking towels at a gym to self-regulating power grids, is remarkable.

The introduction of multiple sensors to monitor values such as temperature, current, air flow, moisture content, presence and movement of humans/vehicles, mechanical stress, etc., allows the optimization of large, complex systems that couldn't be achieved without an enormous amount of time related data. This vast array of data provides unprecedented situational awareness and the opportunity to apply automated controls that can "learn" from experience with the system. Smart homes, cities, industries, and utilities are springing up all around the globe. Predictions are that these kinds of smart operating systems will save industries and municipalities billions of dollars in the next 5 years.

2.1 DEFINITION OF IOT

There are numerous definitions for IoT, but the International Organization for Standardization and International Electrotechnical Commission's Joint Technical Committee 1 definition provides:

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.

The study team focused on this definition because it encompasses what's important to the Army—connecting sensors, collecting data, getting actionable information—to perform its various missions.

The Government Accountability Office produced a technology assessment³ that provided the following definition: “IoT refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.”

From these definitions, the basic idea is that IoT consists of devices that can connect via some form of communication (e.g. machine-machine or machine-cloud-machine), and process information using some form of analytics (e.g. computing in the cloud or computing at the edge, i.e., devices in the field).

2.2 INDUSTRY USE OF IOT

The use of connected, communicating and controlling devices is exploding across all sectors of the economy. Based on current estimates, there will be 25 billion IoT devices in use by 2020.⁴ This number is expected to more than double in the next five years. A reduction in the cost per sensor or control module as well as the development of low power networks have allowed systems that control such diverse entities as building environments, traffic flow, consumer supply chains, patient wellbeing, and machine maintenance to obtain greatly expanded real time situational understanding and control. This allows the operators of these systems to achieve unprecedented efficiencies and cost savings.

A major global initiative regarding IoT is the implementation of the “Smart City,” which will allow municipalities to save a great deal of money through efficiencies and provide a safer environment through timely situational awareness and response. A first step could be an expansion on existing traffic control systems, making them interactive with monitored flow patterns and smart parking systems. The next generation would see cars communicate with each other and the city system. In addition, city-wide video and audio monitoring could enable identifying safety or security incidents, allowing for quicker, more appropriate responses. Likewise, air quality and weather monitoring could be added to trigger health and safety warnings.

Industries are now implementing condition-based maintenance (CBM) programs. “Power by the hour” is the new paradigm for industrial equipment whereby the manufacturer of the equipment owns the hardware and the customer pays for its utility. All aspects of the equipment are monitored continuously so maintenance needs can be predicted and scheduled in a timely manner.

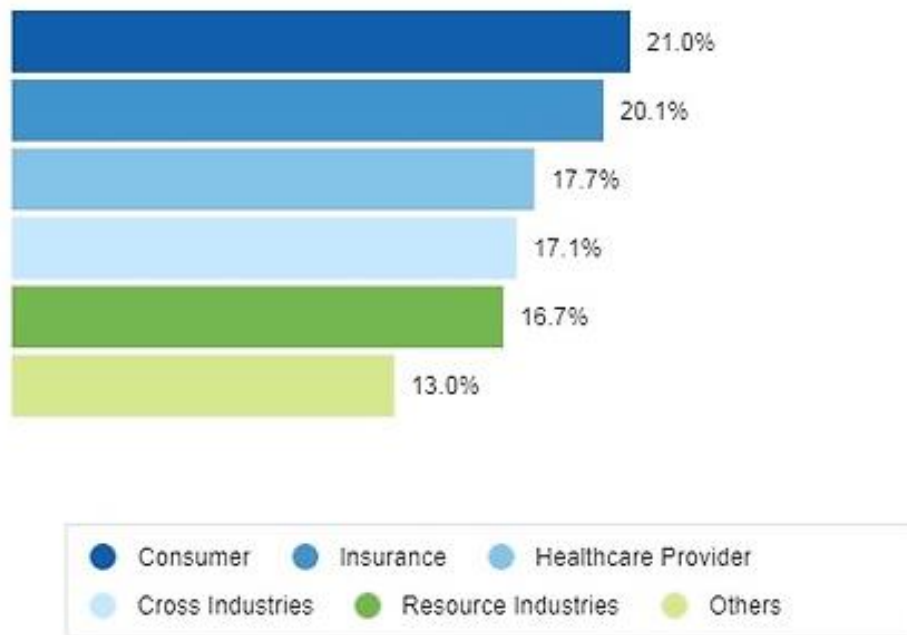
³ GAO, “Internet of Things: Status and implications of an increasingly connected world,” 2017

⁴ Association for Automatic Identification and Mobility; www.aim-na.org

“Just in time” inventory control has been in practice for many years, but the addition of warehouse sensors communicating with suppliers can make it much more efficient. A current practice sees machines ordering their own supplies.

In the medical fields, smarter monitoring of patients, whether in hospitals or at home, is being developed to allow quicker and more accurate response to changing health conditions as well as more complete documentation of recovery. More accurate patient monitoring in hospital allows the institution to be more efficient in scheduling tests and procedures as well as restocking supplies and equipment.

Commercial industry is moving toward faster networks, increased machine intelligence, and connected consumers for a collaborative economy. The International Data Corporation (IDC) predicts that market opportunity for IoT technologies and IoT enabled products will reach \$1.7T by 2020 with 5-year compound annual growth rate~16% (Fig. 2.1).⁵



Source: IDC Worldwide Semiannual Internet of Things Spending Guide, 2017H1

Figure 2.1: IDC top Industry Based on 5 Year CAGR (2016-2021)

2.3 GOVERNMENT USE OF IOT

The recent initiative by Secretary of Defense Ashton Carter to establish Defense Innovation Unit X (DIUX) in Silicon Valley, along with other technology centers, is increasing the visibility of IoT, however, it's unclear if IoT is a term de jour or whether related concepts will result in the establishment of government policy and programs. The Army purchases commercial products

⁵ IDC IOT Forecast; May 2015

that are adapted to combat conditions, and IoT is increasingly becoming part of those commercial solutions to defense requirements. Unfortunately, neither DoD nor the Army have acted to shape or formalize IoT standards or parameters for military specifications. The U.S. military has, in effect, ceded the IoT battlespace to potential adversaries, allowing them to develop the capability to exploit friendly IoT systems. In addition, the military's failure to keep up with the advances in IoT used by commercial industry has led, or will lead to overpayment for maintenance of systems, waste in the management of buildings and infrastructure, low readiness because of inefficient maintenance and accounting systems, and sub-optimal situational awareness for Army operations.

Strategic leader engagement and support is key. A national IOT strategy with policies and an assessment of technical skills is needed to plan for the long term. Coordinating IOT leadership and efforts would establish federal standards to guide research and development, budgeting, and funding pilot projects. A relationship between cybersecurity research, the growing field of privacy engineering, and research with IOT may develop out of necessity. The Army should monitor these synergies, as they affect its enterprise in the same manner as civilian society.

Early IoT adopters in the government demonstrating the potential benefits of IOT include the National Security Agency's (NSA) Advanced Encryption Standards, Defense Information Systems Agency cloud computing and analytics, and the Army Common Operating Picture Environment in communications and intelligence. Despite these, federal government adoption of IOT technologies is slow due to:

- A lack of funding to modernize IT infrastructures
- Risks and uncertainty about privacy, security, and interoperability
- Problems with measuring return on investment

Other agencies deploying IOT are realizing cost reductions by implementing technologies such as the General Service Administration's (GSA) smart building that uses sensors to secure and power down when buildings are unoccupied. GSA and DoD fleet telematics and asset management systems are also monitoring hundreds of thousands of vehicles and equipment to report on maintenance and operating requirements. DoD and the Army specifically are implementing Enterprise Resource Planning using SAP technologies for financial and logistics data management, forecasting and analytics.

Due to the necessity of having to integrate computing, informational, and communications systems, the Army has taken some initiative in testing and evaluating IoT systems in Army Warfighting Exercises (AWE) and Network Integration Exercises (NIE). The lessons learned from these events need to continue to be widely disseminated for government, academia, and supporting industry to get the maximum return on the IoT investments.

DoD is also developing government-industry relationships and leading efforts through professional organizations to leverage IoT development. Some of these organizations include:

- International and Interservice Training, Simulation and Education Conference (IITSEC)
- National Defense Industrial Association (NDIA)
- The Association of the United States Army (AUSA)

These groups bring together DoD, the Department of Homeland Security, commercial industry, and academia to share technologies and systems that enhance military training and operations. Some efforts are underway to modernize government IT infrastructure, such as developing cloud computing and data analytics, but departments and agencies should do more to incentivize collaboration and information exchange to improve IOT requirements. The study team believes establishing a federal Chief Information Office is instrumental to coordinating these efforts. A joint service and interagency approach to IOT systems collaboration will result in even greater efficiencies and cost savings since there are many common communications, intelligence, and information sharing platforms in the government.

3. USE CASES

Several use cases were developed to explore Army opportunities to leverage commercial best practices in IoT. These use cases can be characterized as “crawl, walk, run” or immediate intermediate, and long-term opportunities. The study team recommends the Army establish a campaign of learning to accelerate the adoption of commercial experience and best practices in a time-phased, risk-based approach (Fig. 3.1). Broadly, the immediate, or “crawl,” option is characterized by commercial technology and practices that are directly applicable to Army applications with little customization. Intermediate, or “walk,” options may be thought of as those that are extensions of commercial technology with some customization that is technically straightforward for the Army operational environment. Finally, the long term, or “run,” options are those that call for a specific Army solution due to the unique nature of the Army mission and operational and security requirements.

	Crawl (0-5 yrs)	Walk (5-10 yrs)	Run (>10 yrs)
Source	COTS	COTS and Army	Army
Key Impact	Readiness, Cost Savings	Situational Understanding	Combat Effectiveness
Approach	Use COTS	Develop Analytics Framework	Fund Research
Example Application	Power by the Hour / Smart Forts	IoTINT	Enhancing Autonomous Combat Operations

Figure 3.1 Campaign of Learning for Military IoT

3.1 IMMEDIATE OPPORTUNITIES

Industry is focused on business outcomes. Customers want efficiency in delivery of products and services which is driving innovation and broadening the applications of IoT. Cheaper sensors enable real-time or near real-time monitoring of key performance parameters, and advances in analytics allow industry to get more precise information about customers, their equipment, and patterns of use that impact performance.

3.1.1 POWER BY THE HOUR

An industry approach referred to as “Power by the Hour” can and is being used to continuously tune performance on a per asset basis to manage performance, which is driving changes to business models. The concept is, rather than sell a capital asset like jet engines or elevators, industry is selling a service, power, based on availability of the asset or service.

Two industry examples clearly describe the concept: General Electric (GE) and ThyssenKrupp. GE has implemented a “Power by the Hour” model with jet engines and locomotives to improve asset performance management, optimize service, and manage their supply chain effectively

using IoT. The asset, e.g., a jet engine, is fully instrumented and performance data is collected from sensors while in flight. When the airplane lands, the data is downloaded and analyzed. GE also creates a digital twin, or model, of each engine that's used to integrate and analyze the data. The tool allows them to predict when maintenance will be required for an individual engine, effectively plan for that maintenance, and ultimately improve operational time. GE has reported operational efficiencies resulting from avoiding engine removals for maintenance and has also implemented a similar IoT-enabled approach for diesel engines on trains. There too, the results have saved money, such as minimizing fuel consumption and emissions per trip by optimizing speed and horsepower based on train weight, rail topology, and locomotive data (Fig. 3.2). Specific savings cited by the company include 32,000 gallons fuel per locomotive and 174,000 tons emissions decreased per year.

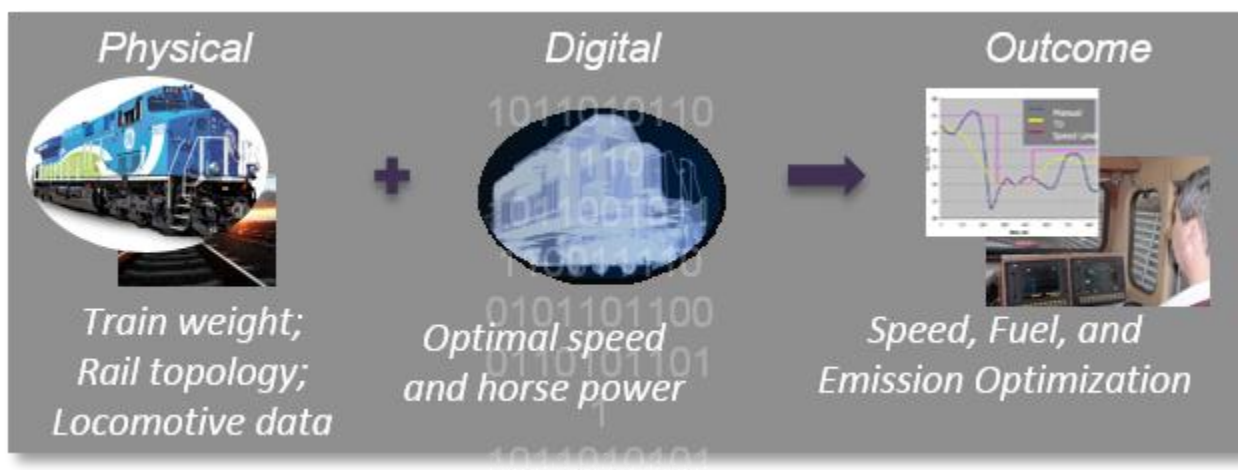


Figure 3.2 Power by the Hour Methodology for Locomotives

Working with Microsoft, ThyssenKrupp (TK) has developed a similar solution for elevators, connecting thousands of sensors to analyze their systems and improve maintenance. Like GE, TK has developed a business model enabled by IoT to sell a service rather than the elevators themselves. In this case, the monitoring of sensors is done while the systems are on-line, and they alert when maintenance is required. The improvements in maintenance reduce downtime and maximize the availability of the service.

The concept of using IoT data has expanded into the commercial trucking industry and is being used as a market discriminator by companies such as Navistar. Navistar has provided many of the Army's MRAPs, so it's not hard to envision expanding the Navistar approach to all current Army equipment. However, the study team also found that the Army has requested some of the IoT capabilities be removed or disabled in the trucks it has purchased.

The study team couldn't identify any existing Army applications of "Power by the Hour." However, the Army can take advantage of the industry's advances in IoT, cloud computing, and data analytics in the near term to achieve cost savings and improved readiness. Army railroad

operations present a potential pilot opportunity to apply “Power by the Hour,” including the digital twin concept, to demonstrate cost savings and readiness improvements.

3.1.2 SMART CITIES

Smart Cities utilize multiple technologies to improve the performance of health, transportation, energy, education, and water services leading to higher levels of services and security to their citizens. In 2015, the Administration announced a new “Smart Cities” initiative to help communities improve city services. The initiative will invest \$160M in federal research dollars as well as leverage technology collaborations, and a key strategy involves creating testbeds for IoT applications.⁶ While the idea of increasing efficiencies through tagging, improved sensors, integrated management systems, or networking isn’t new, IoT offers new opportunities to leverage technology, sensors, and data analytics at scale.

Industry has projected savings and benefits of Smart Cities in several specific application areas reaching hundreds of millions of dollars within the next decade.⁷ These savings could be even greater because the possible applications to city services could easily expand. Traffic management systems increase revenues through management of tolls, parking enforcement, and congestion penalties. Conservation can be encouraged through smart grids that adjust rates during peak hours and water metering systems that find and encourage repairs of leaks. Recycling and reduction of waste can be incentivized through a “pay as you throw” adjustment to solid waste management charges. One current IoT application, GE Intelligent Lighting, integrates cameras with sensors, e.g. acoustics, to enhance public safety, security, and operational efficiencies. The technology has already been deployed in four U.S. cities to address issues like gunshot location identification, parking enforcement, and reduction of vehicle-pedestrian accidents.

Key elements of Smart Cities are already being implemented in more than twenty cities around the world. Cities such as Columbus, New York City, Barcelona, Copenhagen, London, Rio de Janeiro, and Singapore already excel at harnessing technology to run more efficiently and offer opportunities to learn how to apply commercial technologies at scale. While the Army has applied improved metering and networking to achieve improvements in energy and water management, there are many new opportunities presented by the advances in IoT for efficiencies and cost savings. The Army has the opportunity in the near term to leverage government, academic, and industry investment to create an IoT technology platform. The U.S. Army Installation Management Command (IMCOM) oversees Army posts and other locations that have many of the same challenges facing U.S. cities, thereby offering the opportunity to create Smart Forts that leverage the Smart Cities initiatives to achieve cost savings within the institutional Army.

⁶ White House press release, 14 September 2015, “Fact Sheet: Administration Announces New Smart Cities Initiative to Help Communities Tackle Local Challenges and City Services.”

⁷ Automatic Identification and Mobility (AIM) and RAIN RFID.

3.1.3 NATIONAL TRAINING CENTER (NTC) TEST BED

As the study team met with industry, it became apparent that there's an ubiquitous flow of data from IoT devices. Data gathering with AT&T, the Radio Frequency Identification (RFID) Council, GE, Microsoft, and Pacific Northwest Laboratory revealed the things that comprise the 'T' in IoT will always be capable of transmitting. For example, take the case of automobiles: the 4g and 5g networks require creating a separate identification for IoT data from all other uses of the cell network. On the networks, IoT data is billed at significantly lower rates than all other cell traffic. This approach has been agreed upon in the international cell community and by the automotive community. The result is that any commercial vehicle recently produced is enabled to tell where it is in geo-space, how it is performing, and how its operator is performing. That's a significant development for the Army. Under Presidential Directive 13693 (March 2015), government agencies operating a fleet of at least 20 motor vehicles will:

Improve agency fleet and vehicle efficiency and management by:... (iii) collecting and utilizing as a fleet efficiency management tool... agency fleet operational data through deployment of vehicle telematics at a vehicle asset level for all new passenger and light duty vehicle acquisitions and for medium duty vehicles where appropriate; (iv) ensuring that agency annual asset-level fleet data is properly and accurately accounted for in a formal agency Fleet Management System and any relevant data is submitted to the Federal Automotive Statistical Tool reporting database, the Federal Motor Vehicle Registration System, and the Fleet Sustainability Dashboard (FleetDASH) system.⁸

In other words, GSA fleets will be IoT enabled, and this means that any GSA vehicle, as well as any privately-owned vehicle operated by a Soldier (to include his family), Army civilian, or vendor that supports the Army, will be a source of IoT data.

Taking the ubiquitous data stream a step further, IoT sensors are small enough now to be embedded in the threads that are woven into fabric, a feature already used in consumer products such as towels at commercial gyms. These and other applications currently under development force the Army to think about its (Blue) operational security (OPSEC), adversary (Red) OPSEC, and friendly (Gray) influence on OPSEC. To that end, the study team postulated three areas for investigation:

1. Blue OPSEC 1 – Managing and protecting data emanating from the Army and friendly (Blue) forces by monitoring and manipulating IoT data streams from commercial, military, and Soldier sources. In the near term, the Army should work to influence IoT standards, and work to change policy to maintain control of its data stream. In the far term, the Army should adopt full encryption and develop an on/off capability for IoT to maintain security.

⁸ Planning for Federal Sustainability in the Next Decade; Executive Order 13693 of March 19, 2015; <https://www.gpo.gov/fdsys/pkg/FR-2015-03-25/pdf/2015-07016.pdf>; pp. 3-4.

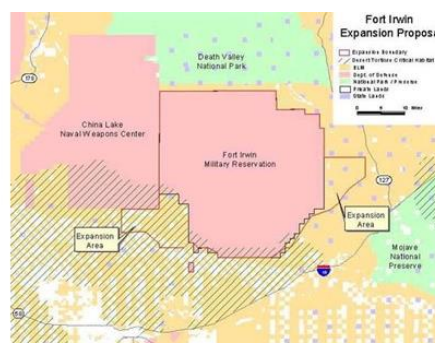
2. Blue OPSEC 2 – Using IoT to shape the environment by monitoring and manipulating IoT data streams from commercial, Blue, and Gray sources to effect local actions and support Blue operations. In the near term, the Army should monitor IoT data streams to identify patterns. In the far term, the Army could work to influence patterns of life.
3. Red OPSEC – Using data to disrupt Red operations by monitoring and manipulating IoT data streams from civilian and government sources to influence, disrupt, and shape Red operations. In the near term, the Army should monitor data patterns and identify vulnerabilities to spoofing and injecting disruptive phenomena or actions. In the far term, the Army could use what it's learned to disrupt Red's ability to conduct operations and to influence civilian populations.

The Army has a unique opportunity to begin work in these areas. The study team found that AT&T had recently upgraded the cell network at Ft. Irwin, CA to the latest 4g/5g capability. The network supports NTC scoring and tracking of a Brigade Combat Team's (BCT) play during the BCT's exercise rotation at NTC. Thus, the Army has access to a robust, well-defined tracking and scoring system operating over a robust and well-defined commercial 4g/5g network. In other words, a unique laboratory to investigate how the Army can leverage IoT (Fig. 3.3).

NTC conducts 10 to 11 BCT evolutions/year

- Maneuver data is recorded over a ATT 4G/5G cell network
- OPFOR uses same network to exercise operations against Blue force
- Significant log platform data is recorded on platform and downloaded post operation
- Opportunity exist to create an Analytic Test Bed while anonymizing datasets

Army Analytics Group has the ability to fuse data and conduct deep learning across massive, integrated data sets



The function of the Analytical Test bed is merging NTC blue and red operations and log data to include LIA log mesh net

- Forming Situational Understanding and determining the analytics needed and not the OER
- Informing the requirements process
- The development of tactics and techniques to exploit IoT without impacting the tempo of BCT experience in the NTC

Figure 3.3 NTC and IoT

On visiting the NTC, the study team learned that the exercising BCT was restricted from using their cell phones while in the operational “box,” but that the NTC’s simulated opposing forces could use their cell phones to target the BCT. None of the tracking and scoring data was analyzed beyond that required to train and grade the BCT in the box. Given that 11 of 13 BCTs from the Army train at the NCT every year, the amount of data that can be harvested to inform the Army of how to capitalize on the IoT is rich and deep.

Leveraging the data at NTC will require a new and unique approach to realize the full benefit. The study team believes the Army Analysis Group (AAG) in Fairfield, CA is a viable candidate to take on this task. AAG would need to capture all tracking and scoring data, the relevant cell traffic to the NTC operation, then filter out non-relevant cell data, and develop the necessary analytics to determine the baseline. Once the baseline is established, the full power of IoT can be explored. This can range from allowing Soldiers to use their non-government devices during the exercise, to engaging more robust cyber operations.

IoT will affect the warfighter from phase 0 – OPSEC starts long before movement to contact – through phase 4 – the ability to target and avoid being targeted – requiring the Army to start data collection, analysis and exploitation at home station, continue through deployment, and through the BCT's return to home station.

There are legal challenges that must be dealt with in this environment to assure that Soldiers don't inadvertently violate statutes on data collection and use. IoT has changed the speed and ease with which data can be accumulated, analyzed, and acted upon. The Army needs to gain an understanding on how to make it a force multiplier. The study team believes NTC offers the best opportunity to initiate that effort.

3.2 INTERMEDIATE OPPORTUNITIES

Commercial industry's motivation to advance IoT is centered on providing convenience for customers and cost savings for business, both of which are considered by the study team as short-term opportunities for leveraging IoT technology. Another effect of a future environment where everything's connected will be the development of new types of products and services. This will take longer to mature, but IoT sensors will proliferate from cars to appliances, goods, and clothing. IoT will also produce transformation in business processes (Fig. 3.4).

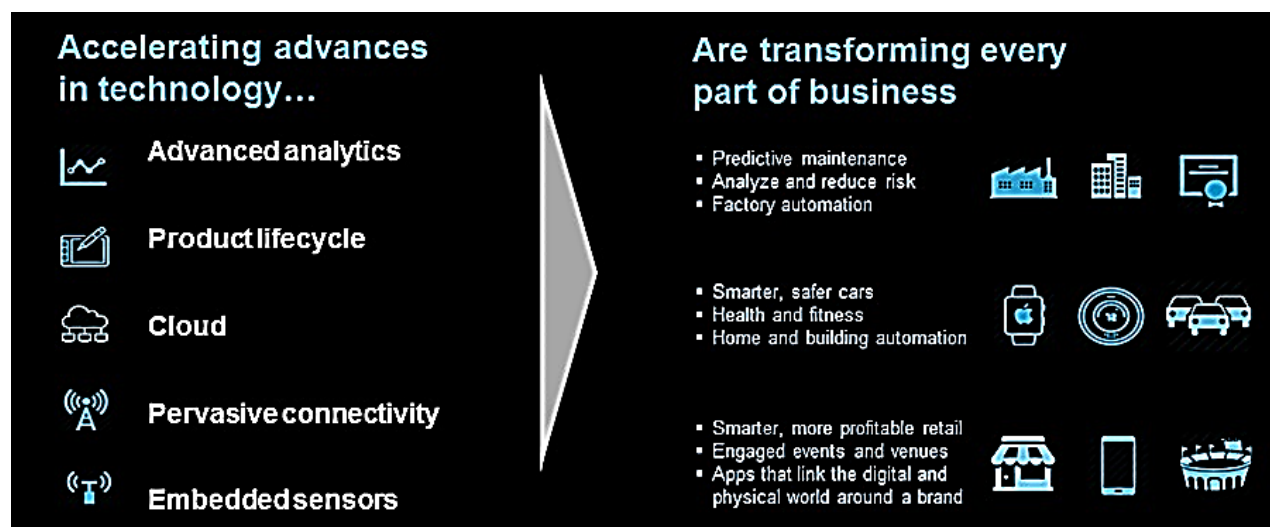


Figure 3.4 IoT Creating Value

In terms of a military application, the translation between commercial and Army-specific opportunities are straight forward: buildings translate to installations, smarter cars to Army fleet vehicles, and health monitoring to improved Soldier readiness. But there are special considerations for the military application that the Army must understand before adopting IoT. For example, there will exist the potential of using IoT sensors for gathering intelligence, surveillance, and reconnaissance (ISR) data. The Army will need a strategy to guard against adversaries exploiting IoT to gain an edge over U.S. forces.

3.2.1 INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) VIA IOT

Future military engagement will include precision operations in smart Megacities where IoT sensors will likely be in place providing everyday convenience to consumers and enabling government to run the city more efficiently. The Army needs to be prepared to leverage the existing IoT infrastructure for ISR and other military applications to enhance situational awareness and situational understanding. Furthermore, combining information from the IoT network with other available intelligence will provide an increased level of situational awareness. The study team adopted the notion that intelligence from IoT data (IoTINT), when fused with other intelligence sources, leads to better situational awareness and understanding for Soldiers operating in megacities.

Know your adversary: IoT data (“IoTINT”), when fused with other intelligence data, leads to better situational awareness and understanding for soldiers operating in megacities.

IoT data can provide information such as:

- Vehicle position and location, traffic control, vehicle occupancy
- Building occupancy, occupant location, appliance status, stock (food, etc.) inventory, sewer contents
- Disease trends, medical stock inventory

The information can provide detailed knowledge of the inner workings of a city, or at a much finer level of granularity, the routine of a single individual. In the case of a military action requiring precise strike capability, IoT surveillance can provide the warfighter with information such as the best ingress and egress for a structure, the pattern of life around a target location, and the differentiation of adversary forces hiding among the civilian population.

IoTINT can benefit in both the planning and execution stages of an Army operation (Fig. 3.5). In terms of planning, IoT sensors provide information on the state of the city. For example, data from household devices provides information on when people are present, data from hospitals provides a status on the health of the community, etc. During the execution phase of an operation, data traffic of IoT sensors provides real-time information on, for example, where

individuals are moving within a building. In both stages, IoTINT enhances situational awareness and understanding.

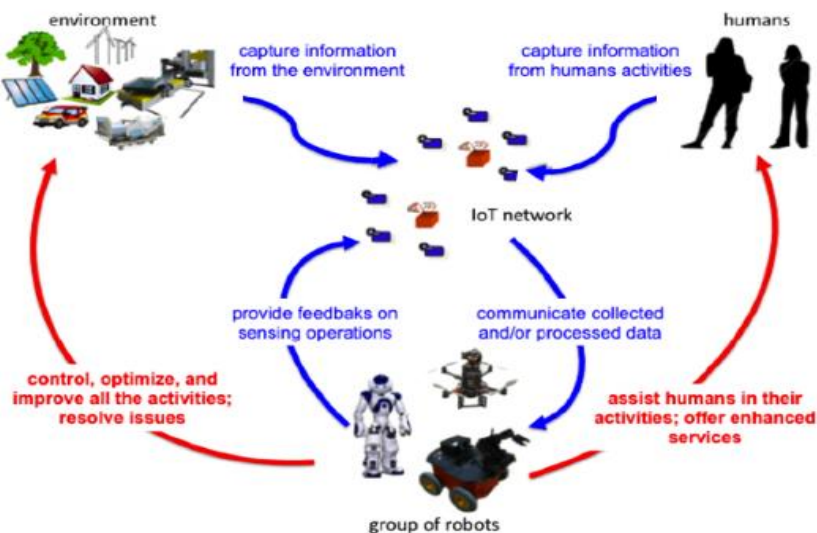


Figure 3.5 IoTINT for Situational Awareness and Understanding

3.2.2 DISRUPTING AND CONTROLLING RED AND GREY IOT SYSTEMS

As IoT increasingly becomes part of the fabric of a smart megacity, the city will become more dependent on IoT devices and networks. Army operations could be assisted by disrupting adversary or 'red' IoT systems and monitoring or controlling civilian 'grey' systems. For example, transportation, building, water and sewer systems, electric and power, and industrial systems can all be enlisted to alter patterns of life in ways that benefit Army operations. Three areas for further study include:

- Determining the value of maneuver capability within adversary's IoT
- Distorting the adversary's situational understanding and manipulating their actions
- Using IoT to influence local populations

The Army needs to examine what advantages may be gained by manipulating the infrastructure of cities. These need to be weighed against risks taken and/or advantages given to adversaries. Further, the analysis needs to be conducted in the context of doctrinal and legal guidelines.

3.2.3 RESEARCH AND DEVELOPMENT (R&D) IN IOT

Companies like IBM, Intel, and Cisco are investing billions of dollars in IoT to establish themselves as leaders in the emerging industry. While these and other corporations across the

globe are working to shape R&D and industry standards, the U.S. government lacks representation among decision-making consortia.

Government agencies do recognize the potential impact of IoT, particularly regarding cyber security. For example, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has made several awards to advance the security of digital identify for IoT devices. Organizations including the NSA and the Army Research Laboratory also have similar programs, for both defensive and offensive cyber. The Defense Advanced Research Projects Agency (DARPA) has initiated Leveraging the Analog Domain for Security (LADS) program, which seeks to make use of the analog emissions of IoT devices in cyber procedures.

None of the current R&D efforts delivers IoTINT capability for the Army. To rectify the situation, the Army should seize on the opportunity to influence the direction of existing R&D efforts to move them in directions that are relevant to the Army. It could also advocate for the creation of new R&D efforts focused specifically on combat use of IoTINT. To accomplish these ends, the Army would likely have to serve as transition partner for new efforts.

3.3 LONG TERM OPPORTUNITIES

Beyond reducing costs and developing new products, services and techniques, longer-term opportunities for leveraging IoT technology focus on the use of IoT data and data fusion⁹ to produce exponential increases in the effectiveness of systems using IoT. The Army can likewise fuse IoT data to enhance its combat capability. There are also significant opportunities to improve installation operations through situational awareness for increased safety and reduction of operational costs.

3.3.1 IOT AS INPUT TO BIG DATA ANALYTIC ENGINES

The fusion of IoTINT data and information from existing sources of intelligence is an objective that fits within the broad goal of fusing data from diverse sources. The most recent Army Doctrine Publication on Intelligence (ADRP 2-0) defines fusion as simply “consolidating, combining, and correlating information together.” This doctrine also defines a related term— all-source intelligence—as, “the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations.” From a functional

⁹ The most common model in data fusion is the one developed by the Joint Directors of Laboratories (JDL; and Llinas et al., 2004). The model provides a hierarchical functional description of fusion comprised of four levels, which are as follows:

- Level-0, or Data Assessment, encompasses the pre-processing necessary to transform raw data in the form of signals, pixels, etc., into an observable object. This is typically an entity resolution or data association problem.
- Level-1, or Object Assessment, is the estimation and prediction of an object’s state.
- Level-2, or Situation Assessment, is the estimation and prediction of relations among objects.
- Level-3, or Impact Assessment, is the estimation and prediction of the effects of the observed object(s) on situations of interest.

perspective, fusion is an opportunity to transform data into useful, actionable knowledge. Knowledge generation can take relatively low-value data (often created in high volumes) and translate them into higher-value knowledge (that is usually much lower in volume/size). The Army's experience with Real-Time Regional Gateway (RTRG) is an example of the use integration and fusion of various information types to produce actionable intelligence.

Advances in Big Data analytics indicate there will be increasing data fusion capabilities. Big Data generally refers to the so-called "V" capabilities that will transform today's limited databases into ones that can handle most or all the following demands (Fig. 3.6):

- Large Volumes of data (petabytes and higher) that hold a
- Variety of data types, searchable with high
- Velocity, which can be accessed virtually, through a browser or smartphone or both while ensuring a
- Veracity that satisfies the need to be able to trust the data

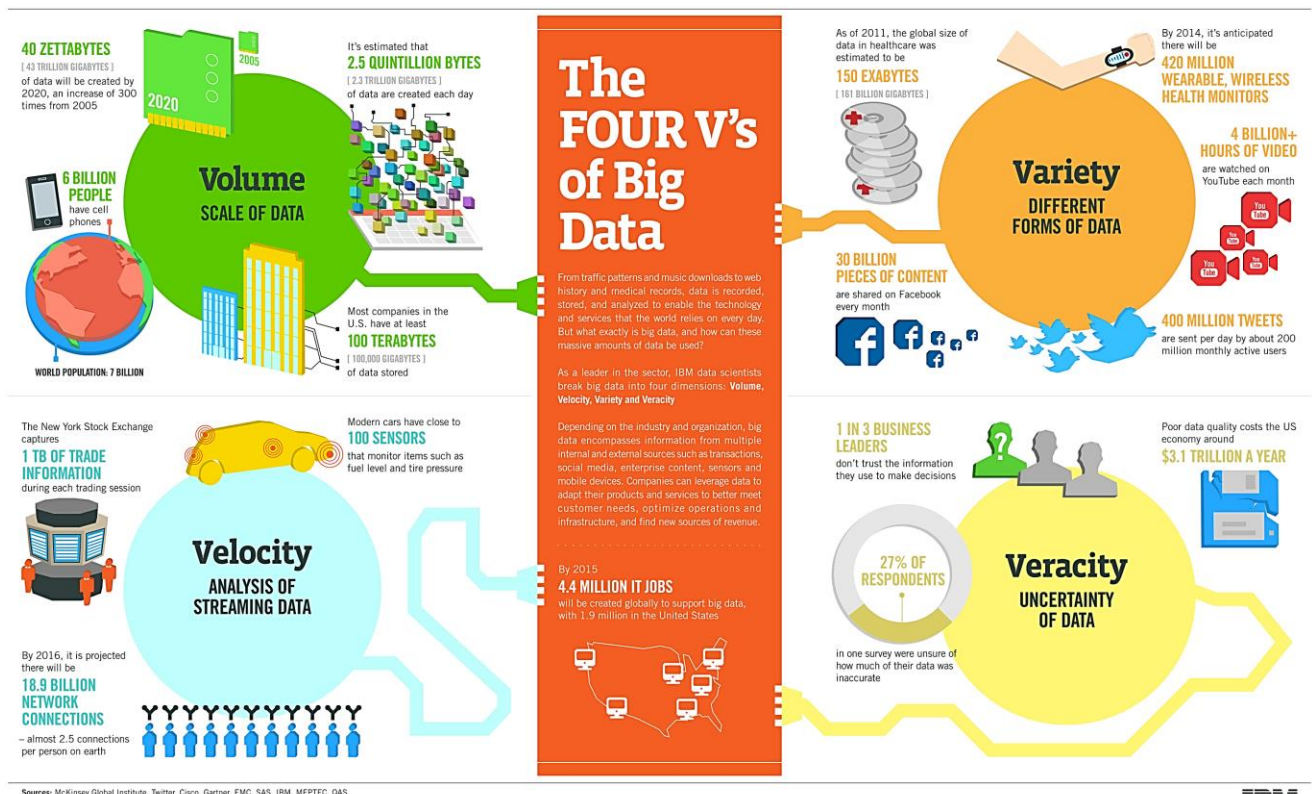


Figure 3.6 Four V's of Big Data (McKinsey Global Institute)

Commercial companies and government contractors are entering the Big Data marketplace and are forming a new wave of collaboration and competition in the field of data exploitation. Their

efforts are generating new data fusion capabilities in the various intelligence functions, which, in turn, are leading to the development of advanced warning and forecasting tools for use by decision-makers. There's a specific cloud architecture model focused on providing data/analytic services needed.

3.3.2 COMMERCIAL, INTELLIGENCE COMMUNITY, AND ARMY SOLUTIONS

Over the last decade, commercial information technology leaders in industry have moved to distributed database architectures and schemas such as Apache Hadoop¹⁰ that embrace distributed storage, unstructured data, and reliance on cheaper commodity equipment. This commercial trend toward more scalable, so-called NoSQL or non-relational database designs is likely to benefit the Army. In fact, the intelligence community has been developing and testing these designs. The Army Chief Information Officer/G6 and G2/ Deputy Chief of Staff for Intelligence and Security, along with similar offices in the Navy, have been advocating these ideas and incorporating them into programs of record and other initiatives. Specifically, both Army Network Command and Army Intelligence Command envision adopting and adapting the distributed cloud approach being developed and tested by the Intelligence Community. The goal is to have a capability that can be leveraged to handle the volume and variety of data at the proper velocity, i.e., "speed of need."

¹⁰ A collection of open-source software utilities that facilitate using a network of many computers to solve problems.

4 CROSS-CUTTING

Implementation of IoT in the Army crosses various operational and logistical boundaries. For example, acquisitions, policy, and cybersecurity involve HQDA, TRADOC, Materiel Command, and various warfighter functions.

4.1 POLICY

IoT is developing outside of the military without regard to military equities. The continued absence of any detectible participation in the IoT standards groups by any DoD activity will create challenges for the Army (and DoD). NIST participates in international activities, but not at the level that industry does. As a result, standards are as general as possible to assure industry equities are covered.

The effect on the Army is that Soldiers are buying IoT-enabled devices such as performance trackers, smart phones, entertainment devices, and automobiles, and bringing them into the military space. Moreover, GSA is requiring that any GSA-leased vehicle is IoT enabled unless the acquiring agency specifically asks for the device to be disabled. That means that most non-tactical GSA leased vehicles (sedans, trucks, busses, etc.) are IoT devices.

The impact on OPSEC and the conflicts that arise when data is accumulated by Army activities that may be subject to Title 50 restrictions (collection on U.S. persons) have yet to be assessed. The study team observed examples of new street lights that capable of collecting images of activities within their viewing radius. These street light systems are in use in cities such as New York and are being aggressively marketed to other cities. The companies involved operate under the business plan that the technology monitors the space out to 35 feet and there are services to be provided (i.e., sold) covering that space (video, sound, Wi-Fi, etc.). These devices offer an opportunity to change how perimeter and internal security are managed, provided that any Title 50 issues are resolved. The study team found no guidance advising or directing installations in the application of such technologies on post.

4.2 CYBERSECURITY CONSIDERATIONS

The study team was tasked to assess the potential risks that would stem from the Army's adoption of IoT. Because IoT is an extension of cyberspace,¹¹ the Army's use of IoT will require mitigating and managing the attendant cybersecurity risks.¹² Through its visits and

¹¹ Cyberspace is defined by DoD Joint Publication 1-02 as A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

¹² Cybersecurity is defined by DoD Joint Publication 1-02 as Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

investigations, the study team identified several areas of cybersecurity concern with respect to the institutional and operational Army's adoption of IoT.

4.2.1 RISK ANALYSIS: AN EXAMPLE

Using IoT may bring some needed capability that supports Army missions, but it may also give an adversary some capabilities to disrupt or degrade these missions. Thus, as the Army considers the use of IoT for various missions, one of the factors it will need to assess is the attendant cybersecurity risk. In the end, the Army is unlikely to be able to eliminate all IoT cybersecurity risk. Rather, it should systematically seek to increase the adversary workload required to degrade Army missions.

For example, we can define risk as a function of the following variables:

$$\text{Risk} = F(\text{Vulnerability}, \text{Exploit}, \text{Impact}, \text{Intent})$$

where the variables are:

- **Vulnerability.** An adversary will seek to identify one or more flaws in the system that he can exploit for his purposes. These flaws could be the result of errors in design, implementation, configuration, or misuse of the system. The Defense Science Board's Resilient Military Systems and the Advanced Cyber Threat¹³ characterized cyber adversaries into three broad categories: (1) those able to exploit known vulnerabilities in systems, (2) those able to discover previously unknown vulnerabilities in systems, and (3) those able to create vulnerabilities in systems. Generally, a greater number of vulnerabilities causes risk to increase.
- **Exploit.** Next, the adversary must be able to design and carry out an attack that takes advantage of one or more of the system vulnerabilities. Some exploits may be inexpensive to create and execute. In fact, they may be found prepackaged and ready to use on the Internet. Others may be quite expensive to develop and may be highly tuned to specific systems. As the cost of creating and executing exploits decreases, the risk increases.
- **Impact.** Successful exploitation of the vulnerability has a negative impact on the rightful user of the system. If the impact of successful exploitation is low, the risk is also low, and vice versa. From an Army perspective, these impacts can be characterized according to their severities, such as "mission kills" where the Army can no longer accomplish some mission that relies on the device, or "catastrophic kills" which impacts Soldier safety or the overall integrity of the Army system.
- **Intent.** If an adversary has the means but little motivation to exploit the system, then the risk is lower than if the adversary has significant motivation. Intent can change with

¹³ <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

time, so use of a system may present low risk during a time when an adversary has little motivation to attack it and high risk some time later when an adversary is more motivated to attack.

As an example, we might consider the use of an IoT-enabled vehicle. The feasibility of hijacking such vehicles leading to potentially catastrophic consequences have been reported in the press.¹⁴ The risk presented by such a vehicle depends on who is using the vehicle and for what purpose. The study team developed a notional approach to assessing risk of using an IoT-enabled vehicle for two types of users: a private citizen and a Soldier (Fig. 4.1). Even though the vulnerabilities inherent in the IoT-enabled vehicles and the ease with which exploits can be developed might be similar, the risk from a cyber-attack against a commercial automobile used by a private citizen (the first row) may be relatively low, because although vulnerabilities and exploits exist, and the impact might be catastrophic for the rightful user, adversaries may have little motivation to execute the exploit. On the other hand, risk from a similar cyber-attack against an Army vehicle might be higher, especially in later phases of conflict, primarily because the impact of successful attack might be higher, and the adversary could have much greater motivation to launch the attack.

Scenario	Vulnerability	Exploit	Impact	Intent	Risk
Cyber-attack against privately owned IOT-enabled automobile	Insufficient protection of wireless interfaces, insufficient intra-vehicle network isolation, lack of data integrity checking	Insert malformed packets on to vehicle networks, insert resident implants on vehicle computers.	Misinformation presented to driver, malicious control of critical vehicle systems (e.g. brakes), leading potentially to vehicle crashes and passenger injuries	Not clear that criminals have found a way to “monetize” these types of attacks.	Low-Medium
Cyber-attack against IOT-enabled Army vehicle	Similar to above	Similar to above	Similar to above, but also includes mission kill, platform kill, lack of confidence in ability to achieve mission, general confusion, etc.	Phase 0: Low, but could be used to lead to confusion Phase 1-4: Could be quite high, seen as an attractive alternative to kinetic engagement	Phase 0: Low-High Phase 1-4: High

Figure 4.1 Cyber Attack on Vehicles: Risk Comparison (Notional Example)

¹⁴ A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway – With Me in It,” Wired, July 21 2015, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>.

Users of IoT-enabled devices need to assess risk this way to make reasoned trades between the capabilities brought by IoT and the inherent cybersecurity risks they impose.

4.2.2 BROAD CATEGORIES OF IOT CYBERSECURITY RISK FACING THE ARMY

There are three broad categories of risk to Army missions that can be brought about by successful cyber exploitation: loss of confidentiality (the adversary can access Army data), loss of integrity (the adversary can distort Army data) and loss of availability (the adversary can make Army data inaccessible to the Army when it is needed). The study team made the following observations regarding these risk categories:

- Confidentiality. Network service providers are working to ensure customer IoT data flowing over their core networks are encrypted from the point that they enter the core network, through the network, and into that part of the network that provides analytic services. However, at the “edge” of the network, e.g. inside a vehicle or within a facility, the data are usually unencrypted, thereby subject to exfiltration and exploitation. The same is true for the data once they enter the analytic cloud in which they are processed. At present, the data need to be unencrypted to be processed efficiently.
- Integrity. Because IoT data collected by sensors and subsequently processed are typically not cryptographically signed, an adversary could modify or corrupt the data in ways that could go undetected. Provenance of the data (i.e. how data are collected and processed through the system) is usually not tracked either, and so the Army would have limited ways of determining the relative trustworthiness of IoT data.
- Availability. Although some elements of commercial networks are designed to be resilient to both fault tolerance and malicious denial of service, there are some adversary techniques (e.g. jamming a communication link with RF energy) against which commercial networks are not well-protected. Additionally, the edge networks themselves are not well-protected against denial of service.

There's a high prevalence of vulnerabilities in IoT devices. Hewlett Packard reported 70% of IoT devices are vulnerable to attack.¹⁵ Devices tested included mainly household items (TVs, thermostats, door locks, etc.), and the vulnerabilities included insufficient authorization (permitting control of the devices by unauthorized parties) and lack of sufficient encryption.

4.2.3 SOFTWARE SECURITY

In addition to these concerns about data, protecting the software running on processors within IoT devices can be challenging for several reasons. First, unlike the software running on

¹⁵ HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack, 29 July 2014. <http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.V8WTAnpb51Y>

conventional servers and desktop machines, the software running in embedded devices is often not cryptographically signed and checked, making it easier for adversaries to insert malicious versions of software into such devices (the Hewlett Packard report provides confirmation of this problem). Second, it's usually more difficult to update the embedded software because network connectivity is intermittent or disadvantaged, meaning that for long periods of time, processors can be running unpatched software in which vulnerabilities are widely known to be present. Finally, standard protection tools (e.g. virus detection, intrusion prevention) are often not available or not installed in embedded systems.

4.2.4 RECOMMENDED PATH FORWARD

The risk mitigation strategy would address the elements of cybersecurity addressed above, e.g. understanding and reducing the number of vulnerabilities in IoT devices used in support of Army missions, assessing and increasing the cost of adversary exploitation of vulnerabilities that remain, and decreasing the impact of successful exploitation on Army mission. For the most part, commercial best practices including "good hygiene" (e.g. installing security patches, good user training, etc.) can address the least capable threats. With respect to mid and higher tier threats against its IoT applications, the Army should consider employing the following cybersecurity technology:

- End-to-end encryption. Data should be encrypted at the earliest possible point, ideally before it even leaves the sensor. The data should remain encrypted for as long as possible, i.e. until the end-user or systems process the data. The data should not be decrypted and re-encrypted along the way. Access to cryptographic keys should be limited and well-understood.
- Cryptographic signatures on data. Individual data elements should be signed cryptographically, which would make it much more difficult for an adversary to change the data between the time they are created and the time they are used.
- Cryptographic provenance tracking of data. Individual data elements should be tracked through the system to identify where the data were created and what processing has been applied to them. This technique permits both end users and end systems to understand what has happened to the data as it has flowed through the system and to assess the data's trustworthiness. Provenance tracking data should also be cryptographically signed to make it more difficult for an adversary to modify the data.
- Cryptographic signatures on software. All software should be cryptographically signed when it is developed, and these signatures should be checked by the end systems before the software is loaded and run. Signing software and checking those signatures makes it much more difficult for adversaries to insert malicious code into systems.
- Techniques to randomize/diversify software. To the extent possible, randomization should be introduced into the software that does not change its functionality but that

does make it harder for an adversary to reverse engineer and to develop exploits against the software. Not all randomization and diversification techniques increase adversary workload, and some incur costly overhead, so trades need to be made to provide meaningful increases to adversary workload at manageable costs.

- Use of anti-jam waveforms for critical communications. Commercial IoT wireless communication relies on the assumption that all devices within the RF environment will adhere to spectrum allocation assignments. RF interference in such cases is usually caused by misconfiguration. Army IoT systems will need to operate in the presence of adversary jamming, so critical RF communication links will need to use waveforms that are difficult for the adversary to jam.
- Use of low-probability-of-detection waveforms. Commercial systems seek to limit unintended RF emissions to minimize interference with other systems and conserve power. The Army often operates in environments where it seeks to severely limit or eliminate RF emissions entirely in those environments.
- Progressive use of security measures depending on the threat condition. Though vendors have generally not provided built-in provisions for evolving threat conditions, such as “due to imminent contact with the enemy, stop sending routine device status updates and non-critical software upgrades,” the Army could seek to configure its IoT devices to operate in this manner, trading some amount of capability for increased security during periods of high threat.

Cyber red teaming of specific IoT components and systems in an Army mission context would provide an independent assessment of how well the Army had reduced its cybersecurity risk. Cyber red teams take an adversary perspective, looking for vulnerabilities and demonstrating exploits that can have maximum impact at the lowest possible cost while matching known adversary strengths, weaknesses, CONOPS and TTPs. The National Defense Authorization Act specifically calls out the need for the evaluation of cyber vulnerabilities of major weapon systems.¹⁶ This same process could be used to detect and assess the impact of cyber vulnerabilities in IoT components and systems. Because the Army’s IMCOM manages day-to-day operations of Army installations, and because these installations are in some cases already using IoT technology, they could be used as test beds to measure the extent to which adversaries of varying skill and resource levels can impact Army missions.

¹⁶ See Section 1647 of <https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf>.

5 FINDINGS AND RECOMMENDATIONS

Based on its data gathering and analyses, the study team developed findings in five categories:

1. Army is not taking full advantage of industrial advances in IoT for warfighter effectiveness and cost savings:
 - a. Industry is investing and implementing IoT at an exponential rate
 - b. Success in industrial deployment of IoT is due to the reduced cost of deployment, advancements in cloud computing, and data analytics
 - c. Industry is using standards bodies to develop interoperability of IoT and there is no evidence of Army participation in these bodies
2. Army does not have IoT system level requirements that are needed for adoption on the battlefield and in the Army industrial base
3. There are cyber and network connectivity challenges that the Army has not yet solved
 - a. Current commercial IoT does not provide sufficient cyber security for critical Army missions
 - b. Some battlefield environments offer limited network connectivity
4. IoT issues cross policy and legal boundaries that must be resolved for Army applications
5. Army can harvest data and develop analytics that identify improvements of warfighter effectiveness:
 - e. NTC and other sources to inform on uses and defenses for IoT enabled things to include an EW environment
 - f. IMCOM as it permeates posts, camps, and stations (government and non-government sources)
 - g. AMC installations for the Army industrial base (depots, arsenals, ammunition storage facilities, and ocean ports)
 - h. MEDCOM as it pertains to Soldier performance

To address these findings, the study team made the following recommendations:

1. AMC: identify the appropriate platform to implement power by the hour using Army railroad as an initial pilot to demonstrate cost savings and readiness improvements
2. AMC and IMCOM: expand existing efforts in depots and smart forts by utilizing smart cities technologies for cost savings, and efficiencies
3. MEDCOM: identify Soldier performance data that are important for battlefield awareness
4. G3/5/7 and OGC: update policies for both legal and implementation issues required to utilize IoT
5. DUSA: task AAG to create an analytics framework for experimentation for knowledge, acceptance, and development of DOTML-PF that will:
 - d. Support Blue on Blue and Blue on Red analysis for a tactical analysis (SME: FORSCOM, MEDCOM)
 - e. Support Blue on Blue and Red on Blue, OPSEC assessments (SME: FORSCOM, MEDCOM, and AMC)
 - f. Inform requirements process across all Army (SME: TRADOC and ASA(ALT))
6. TRADOC: define requirements for IoT systems and have representation on R&D programs related to IoT
7. G6: actively participate in IoT commercial standards bodies to represent the Army's interest
8. ARL: advocate and co-fund (e.g. with DARPA or IARPA) research programs around
 - a. offensive use of adversary's IoT (blue on red/grey)
 - b. adapting the analytics from IoT to disadvantaged (intermittent connectivity, low data rate) networks
9. ASA (ALT), CIO-G6, G3/5/7, AMC, & ARCYBER: include IoT considerations in Army cyber resiliency efforts
10. ARCYBER: develop a risk mitigation strategy for inclusion of IoT in military operations and platforms
11. ARCYBER: conduct adversarial cyber red teaming using IMCOM smart forts as test beds

APPENDIX A – TERMS OF REFERENCE



SECRETARY OF THE ARMY
WASHINGTON
JAN 04 2016

Dr. James Tegnalia
Chairman, Army Science Board
101 Army Pentagon
Washington, DC 20310

Dear Dr. Tegnalia:

I request the Army Science Board (ASB) conduct a study entitled "The Military Benefits and Risks of the Internet of Things." The study will determine the advisability of the Army applying the commercial practice of networking civilian physical systems into a military analog of the "internet of things (IOT)." An IOT moves beyond the exchange of information in cyber space to the networking of operating systems of physical objects.

The study team's tasks shall include, but not be limited to, the following:

- a. Establish which military functions and systems should be networked into an integrated tactical network. As a minimum, the assessment should include systems necessary to provide a comprehensive situation awareness assessment to the military formation. Given such a situational awareness capability, which other military systems should be networked in order to exploit the situation awareness achieved?
- b. Address the vulnerability of such a concept, including risk as a function of the level of integration, and recommend architectures that minimize this vulnerability.
- c. Assess the performance implications of such an integration and the tradeoffs between performance and vulnerability.
- d. Assess the process for determining, on a continuing basis, via Red Teaming and other techniques, the balance of performance improvement and vulnerability.

This study should make use of relevant studies performed by Department of Defense science boards and the National Research Council. Specifically, the study should apply and extend relevant findings and recommendations of the following:

- a. Army Science Board studies on cyber vulnerability and electronics countermeasures.
- b. Navy Studies Board network vulnerability study.
- c. Defense Science Board cyber vulnerability study and autonomy study.

-2-

The study team should consult with the research and development community on the state of defense technology, and also with the U.S. Army Training and Doctrine Command (TRADOC) on the doctrine, tactics, and training in place for networking operating systems of military hardware. The study team should also consult with the commercial sector on the status, advantages, and disadvantages of the commercial IOT.

The study should provide an independent report of its deliberations, findings, and recommendations, as well as cooperate with and provide its results to the parent ASB study on "Disruptive Innovative Concepts for the Future Army."

The Commanding General, TRADOC is the sponsor of this effort. The G-3/5/7 will assist the study team in accessing classified information up to Top Secret and including Sensitive Compartmented Information and Special Access Programs. The Board will provide a briefing and report with findings and recommendations by September 30, 2016 to me and the Chief of Staff, Army.

The study will operate in accordance with the Federal Advisory Committee Act and DoD Directive 5105.4, "DoD Federal Advisory Committee Management Program." I do not anticipate that this study will need to go into any "particular matters" within the meaning of Title 18 United States Code Section 208, nor will it cause any member to be placed in the position of acting as a procurement official.

Sincerely,

A handwritten signature in black ink, reading "Eric K. Fanning". The signature is fluid and cursive, with the first letters of each word being capitalized and prominent.

Eric K. Fanning
Acting

APPENDIX B – STUDY TEAM MEMBERS

Gisele Bennett, PhD., Chair (Georgia Tech)

Marc Zissman, PhD., Vice Chair (MIT-LL)

Members

COL (Ret). William Crowder (LMI)
Mary Crannell (Idea Sciences)
Sid Dalal, PhD. (AIG)
Chris Yu, PhD. (Draper)
Jasper Lupo, PhD. (ARA)

Evelyn Mullen, P.E. (Los Alamos)
Isaac Porche, PhD. (RAND)
Mary Anne Yates, PhD. (Argonne)
Susan Myers, PhD. (ManTech)

Leonard Braverman, PhD. and Jim Tegnalia, PhD., Senior Advisors

Jeffrey Isaacson, PhD., ASB Integration Team Liaison

MAJ Jeremy Harlan, Study Manager

Mark Swiatek, Tech Writer/Editor

Areas of Expertise

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

APPENDIX C – LINES OF INQUIRY AND VISITATIONS

Lines of inquiry for data collection began with the following 21 questions that were sent to each individual and/or organization prior to the interview. The intent was to establish a baseline of preparatory material and to provide the context of the study for each visit or teleconference, reducing the need for introductory and expository remarks and maximizing time spent on topics advancing the concept of military IoT.

1. How can we exploit IoT for situational awareness in training?
2. How can we exploit IoT for situational awareness (Business Intel/Analytics)?
3. What do you see as possible uses in humanitarian relief?
4. How does IoT insert into Army Ops?
5. What level did you focus your IoT approach?
6. How are these companies creating business case?
7. How does IoT help automation?
8. What experiments have you conducted to determine your IoT approach?
9. How has IoT helped, or how do you envision it will help your operations?
10. How does this help reduce the cost of supporting your business line?
11. What do you worry about in protecting data and what data do you protect?
(confidentiality, integrity, availability, and privacy)
12. What testing did you do to assure IoT would in your business?
13. If you launch a field trial, what did you learn?
14. How are these companies dealing with authentication?
15. What commercial technologies can be leveraged?
16. What does a IoT system look like to you?
17. Does your IoT approach exploit machine learning?
18. Does your IoT approach employ machine to machine communications or Machine to cloud communications?
19. Do you provide your own communications infrastructure, or do you rely on third party infrastructure?
20. What were your first steps in using IoT?
21. What are the main impediments to implementing IoT commercially?

The Study Team conducted the following visitations and teleconferences, grouped by category (DoD/USG Agency, Private Industry, and Academic/Research Institution) and listed in chronological order.

DoD and other Government Agencies

1. Communications Electronics Command, Software Engineering Center, (Mr. Michael Crapanzano, 18 February 2016, Aberdeen Proving Ground, MD)
2. Army G8, (COL George Lewis, 26 February 2016, Pentagon, VA)
3. Fires Center of Excellence (Mr. Matt Merrick, 2 March 2016, Teleconference)

4. Army Material Command, Technology Requirements Integration Office (Mr. Tom Pedigo, 15 March 2016, Huntsville, AL)
5. Army Research Laboratory (Dr. Joe Mait, 29 March 2016, Adelphi, MD)
6. Mad Scientist (TRADOC Sponsored Conference, 21-22 April 2016, Phoenix, AZ)
7. National Security Agency, Laboratory for Telecommunication Sciences (Mr. Brad Martin, 26 April 2016, College Park, MD)
8. Army G2 (SES Patricia Guitard, 10 May 2016, Pentagon, VA)
9. Research, Development and Engineering Command (Mr. Michael Stanka, 12 May 2016, Aberdeen Proving Ground, MD)
10. PEO C3T (Ms. Jennifer Zbozny, COL William Sheehy, 12 May 2016, Aberdeen Proving Ground, MD)
11. National Training Center (COL Matthew Moore, 16-17 May 2016, Fort Irwin, CA)
12. Army Cyber Command (LTC Jonathan Burnett, 25 May 2016, Fort Belvoir, VA)
13. Logistics Innovation Agency (Mr. David Mitchem, 25 May 2016, Fort Belvoir, VA)
14. PM Position, Navigation and Timing (SES Kevin Coggins, 1 June 2016, Pentagon, VA)
15. Army CIO/G6 (MG Garrett Yee, 1 June 2016, Pentagon, VA)
16. Army Analytics Group (Dan Jensen, 7 June 2016, Fairfield, CA)
17. I Corps G2 (COL Robert Dixon, 9 June 2016, Fort Lewis, WA)
18. Cyber Center of Excellence (COL Laroy Peyton, 15 June 2016, Fort Gordon, GA)
19. Assistant Secretary of the Army for Strategic Innovation (SES Dr. John Pellegrino, 27 June 2016, Pentagon, VA)
20. Combined Arms Center/Mission Command Center of Excellence (SES Richard Parker, Mr. Robert Dehaan, 28-29 June 2016, Fort Leavenworth, KS)
21. Department of Homeland Security (Mr. Daniel Massey, 7 July 2016, Teleconference)
22. Defense Advanced Research Projects Agency, LADS Program (Dr. Keromytis, Ms. Mary Denz, 12 July 2016, Washington, DC)

Private Industry

1. Google (Dr. Vint Cerf, Chief Internet Evangelist, 26 February 2016, Reston, VA)
2. Oshkosh (Mr. Mike Ivy, 15 March 2016, Huntsville, AL)
3. Intelligent Communities Forum (Dr. Robert Bell, 8 April 2016, Teleconference)
4. AT&T World Headquarters and IoT Foundry (Mr. Chris Smith, Mr. Carl Tegen, Mr. Gary Langston, Mr. Terry White, Mr. Greg Dimond, Mr. Chris Sambar, Mr. Mobeen Khan, Dr. Tina Hampton, Dr. Usha Mohan, 12 April 2016, Dallas, TX)
5. McLane Industries (Mr. Drayton McLane, 13 April 2016, Temple, TX)
6. Microsoft (Dr. Arjimand Samuel, Mr. Mik Wimbrow, 15 April 2016, Redmond, WA)
7. AT&T Drive Studio (Dr. Usha Mohan, 20 April 2016, Atlanta, GA)
8. IBM (Mr. Milan Patel, Mr. Peter Allor, Mr. Sky Matthews, 21 April 2016, Atlanta, GA)
9. Amazon Web Services (Mr. Adam Ginsburg, 26 April 2016, Herndon, VA)
10. General Electric (Ms. Maria Peace, 23 May 2016, Teleconference)
11. RAIN Alliance (Mr. Steve Halliday, 7 June 2016, Napa, CA)
12. General Electric (Mr. Chip Cotton, 8 June 2016, San Ramon, CA)
13. AIG (Dr. Sid Dalal, 21 June 2016, New York, NY)

14. General Motors Connected Cars (Ms. Susan Smyth, 25 July 2016, Teleconference)

Research Institutions

1. George Washington University (Dr. Joe Pelton, 29 March 2016, Washington, DC)
2. Massachusetts Institute of Technology (Dr. Sanjay Sarma, 5 April 2016, Cambridge, MA)
3. Massachusetts Institute of Technology, Lincoln Laboratory (Dr. Marc Zissman, 5 April 2016, Lexington, MA)
4. Massachusetts Institute of Technology, SENSEable Cities Laboratory (Ms. Erin Baumgartner, 6 April 2016, Cambridge, MA)
5. Pacific Northwest National Laboratory (Mr. Mark Greaves, 10 June 2016, Seattle, WA)

APPENDIX D – ASB APPROVED BRIEFING WITH FINDINGS AND RECOMMENDATIONS

Findings and recommendations were adopted by the ASB membership in plenary session at the University of California, Irvine, on 28 July 2016.



Army Science Board



The Military Benefits and Risks of the Internet of Things July 28, 2016

UNCLASSIFIED

Army Science Board

1



Impact of Technology on the World



UNCLASSIFIED

Army Science Board

2



Impact of Technology on the Army

Industrial Revolution

- Machine Gun
 - Reshaped conflict and removed the horse: improved **Fires**
- Steam/ Reciprocal Engine
 - Reshaped movement and removed Sail/Horse: improved **Maneuverability**
- Jet Engine
 - Reshaped travel and shrank the time boundaries: facilitates **Force Projection**

Communication Revolution

- Telegraph/Telephone/Radio
 - Accelerated decision time: increased **Warfighter Effectiveness**
- Internet
 - Reshaped information flow and changed the news cycle and data analytics: improved **Situational Awareness**

Internet of Things – Melding of the two

- Explodes available data from devices and has the opportunity to improve **Situational Awareness, Cost, Readiness, and Combat Operations**

IoT has the potential to be as big a game changer as prior technology advancements

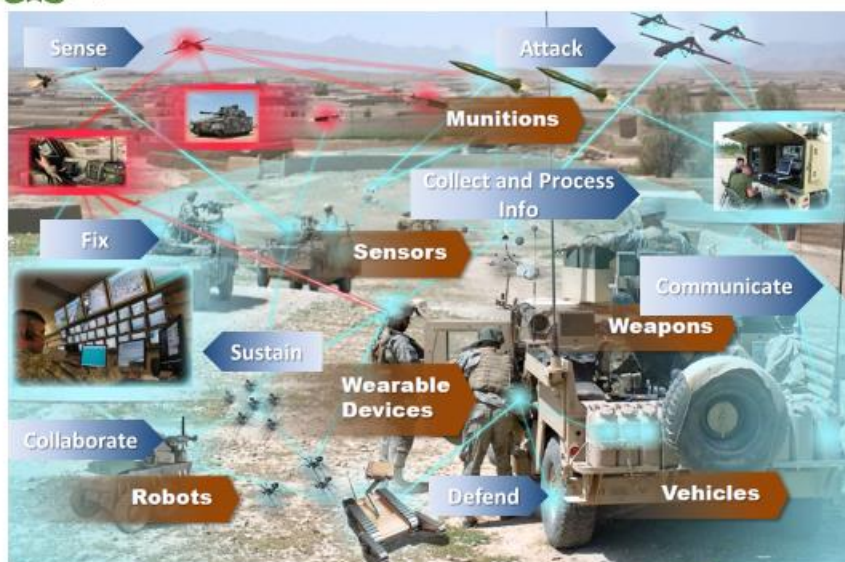
UNCLASSIFIED

Army Science Board

3



Military IoT – Overlay for combat arms



Dr. Pellegrino – AFCEA presentation 2016

UNCLASSIFIED

Army Science Board

4



Roadmap



Introduction

- Study Team
- Terms of Reference
- Visits
- Definition and Relevance
- Use Cases (Crawl, Walk, Run)
- Cross-Cutting Considerations
- Findings and Recommendations

UNCLASSIFIED

Army Science Board 5



Study Team

Chair – Dr. Gisele Bennett (Georgia Tech)

Vice-Chair – Dr. Marc Zissman (MIT-LL)

Panel Members

COL (Ret). William Crowder (LMI)	Evelyn Mullen, P.E. (Los Alamos)
Mary Crannell (IdeaSciences)	Dr. Isaac Porche (RAND)
Dr. Sid Dalal (AIG)	Dr. Mary Anne Yates (Argonne)
Dr. Chris Yu (Draper)	Dr. Susan Myers (ManTech)
Dr. Jasper Lupo (ARA)	

Senior Advisors – Dr. Leonard Braverman and Dr. Jim Tegnalia

Integration Team Liaison – Dr. Jeff Isaacson

Study Manager – Maj Jeremy Harlan

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, Intelligence

UNCLASSIFIED

Army Science Board 6



Terms of Reference

Sponsor: CG TRADOC

Excerpt from TOR:

"The study will determine the advisability of the Army applying the commercial practice of networking civilian physical systems into a military analog of the internet of things (IoT). An IoT moves beyond the exchange of information in cyber space to the networking of operating systems of physical objects."

- Our study addressed three key questions:
 - How is IoT transforming our world?
 - What are the opportunities for the Army?
 - What are the consequences of doing nothing?

Past studies did not focus on IoT as a system

- Army Science Board – cyber vulnerability and electronics countermeasures
- Navy Studies Board – network vulnerability study
- Defense Science Board – cyber vulnerability study and strategic surprise

UNCLASSIFIED

Army Science Board 7



Visits and Interviews

Industry

Google-Vint Cerf
Oshkosh
AT&T-IoT Foundry,
AT&T Connected Cars Foundry
Drayton McLane
Microsoft
IBM
Amazon Web Services
General Electric
RAIN
General Motors
AIG

Government/Military

CECOM
Army G8-COL Lewis
Fires Center of Excellence
Army Materiel Command
Army Research Labs
Mad Scientist
NSA
Army G2
RDECOM
PEO C3T
National Training Center, Fort Irwin
ARCYBER
Logistics Innovation Agency
PM-Position, Navigation and Timing
Army G6
Army Analytics Group
Office of General Council
I Corps G2
Pacific Northwest National Labs
Deputy Assistant Secretary of the Army for
Strategic Innovation
CAC-T
Mission Command Center of Excellence
DHS
DARPA

Academia

George Washington University-Joe Pelton
MIT-Dr. Sanjay Sarma
MIT Lincoln Laboratory
MIT SENSEable Cities
Intelligent Communities Forum

UNCLASSIFIED

Army Science Board 8



What is IoT and Why Is IoT Important?

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**.*

- How is IoT different?
 - Very large scale (2020 est.: 20 Billion devices, 200 Billion tags)
 - Totally pervasive (all over the world)
 - All things connected (even threads in clothes)
 - Very low cost (pennies per tag)
 - Data analytics
- Why is industry investing?
 - Customers want efficiency (e.g. better control of HVAC system, automatic product delivery)
 - Industry uses analytics to get more precise information about their customers

*ISO/IEC JTC1 definition

UNCLASSIFIED

Army Science Board 9



Why is IoT Important to the Army?



DOD Logistics programs and operations totaled \$84B in FY2000, accounting for 1/3 of budget

Improved Warfighter Effectiveness

- Situational Awareness: Blue SA of Blue, Blue SA of Red and Grey
- Better mission command (C2) and autonomy
- Fight more effectively in Red and Grey environment
- Soldier performance

Reduced Cost

- Efficiencies in maintenance, readiness, facilities management, logistics

UNCLASSIFIED

Army Science Board 10



Roadmap

- Introduction
 - Study Team
 - Terms of Reference
 - Visits
 - Definition and Relevance
- ➔ Use Cases (Crawl, Walk, Run)
 - Cross-Cutting Considerations
 - Findings and Recommendations

UNCLASSIFIED

Army Science Board 11



Campaign of Learning for Military Use of IoT

	Crawl (0-5 yrs)	Walk (5-10 yrs)	Run (>10 yrs)
Source	COTS	COTS and Army	Army
Key Impact	Readiness, Cost Savings	Situational Understanding	Combat Effectiveness
Approach	Use COTS	Develop Analytics Framework	Fund Research
Example Application	Power by the Hour / Smart Forts	IoTINT	Enhancing Autonomous Combat Operations



Some commercial IoT investments are ready to be harvested now

UNCLASSIFIED

Army Science Board 12



“Power By The Hour” IoT Changing Business Models: Crawl

GE Digital: Asset performance management, service optimization, supply chain management

- Key concept: sell power not engines (planes, trains)
- Key concept: create digital twin of important asset for predictive or condition based management of individual assets



ThyssenKrupp and Microsoft developed a solution to connect thousands of sensors and systems in its elevators to improve maintenance and “up time”

- Key concept: sell availability of service not commodity
- Key concept: elevators self-alert when maintenance is required

Industry is focused on business outcomes: per asset model, continuously tuned. Process is scalable and adaptable – periodic data downloads possible to enable operational security.

UNCLASSIFIED

Army Science Board 13



“Power By The Hour” IoT Changing Business Models: Crawl

Airplane engines

Recent successes ...



GE90

120

removals saved



CFM56

40

removals saved



Water wash

\$7M/yr

fuel savings at one GE90 operator

Industry has demonstrated success:

- improved reliability
- reduced manpower and engine replacements
- fuel cost savings



Train: Minimized fuel consumption and emissions – generated per trip.

- **32K gallons/locomotive**
- **174K tons emissions decreased per year**

Know thyself

- IoT used in Power by the Hour can be utilized for cost savings and improve readiness*
- Digital twin can be used for virtual test bed

* ASB FY 2015 Strategies to Optimize Army Operating and Generating Forces for 2025 and Beyond

UNCLASSIFIED

Army Science Board 14



SMART Cities: Efficiencies in Operations and Cost Reductions: Crawl



Smart Cities utilize multiple technologies to improve the performance of health, transportation, energy, education, and water services leading to higher levels of services and security to their citizens.

UNCLASSIFIED

Army Science Board 15



SMART Cities: Efficiencies in Operations and Cost Reductions: Crawl

Current Army savings*



Industry Projected Savings and Benefits:**

- Traffic management - \$100B in revenue by 2020 (management of tolls and congestion penalties)
- Smart grids - \$200B-\$500B per year by 2025 (adjust rates for peak energy use)
- Water conservation through reduction of water leaks
- Increase in recycling through "pay as you throw"

Opportunities for the Army to further leverage industrial applications of IoT

* Dr. John Pellegrino – AFCEA presentation 2016

** Automatic Identification and Mobility (AIM) and RAIN RFID

UNCLASSIFIED

Army Science Board 16



SMART Cities: Efficiencies in Operations and Cost Reductions: Crawl

Key elements are already being implemented in more than 20 cities, including private and government investments

- Smart Cities Initiative (9/14/15 – White House announcement)
 - \$35M in grants, \$10M investments in research infrastructure (NSF, NIST)
 - \$70M + \$45M investments in safety, environment, energy, climate, transportation, health (DHS, DOT, DOE, DOC, EPA)
- GE Intelligent Lighting (integrating cameras plus sensors, e.g. acoustics) deployed in 4 cities to enhance public safety, security, operational efficiencies
- Columbus, NYC, Chicago, Barcelona, Copenhagen, London, Rio, and Singapore and other cities (20+) already excel in harnessing technology to run more efficiently



Smart Cities can be utilized for cost savings, sustainment, and an integrated technology platform. Army can leverage investments and track outcomes for use in Smart Forts

UNCLASSIFIED

Army Science Board 17



Campaign of Learning for Military Use of IoT

	Crawl (0-5 yrs)	Walk (5-10 yrs)	Run (>10 yrs)
Source	COTS	COTS and Army	Army
Key Impact	Readiness, Cost Savings	Situational Understanding	Combat Effectiveness
Approach	Use COTS	Develop Analytics Framework	Fund Research
Example Application	Power by the Hour / Smart Forts	IoTINT	Enhancing Autonomous Combat Operations



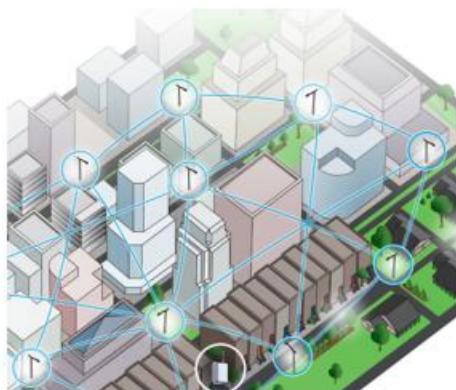
Some commercial IoT investments are ready to be harvested now

UNCLASSIFIED

Army Science Board 18



IoT Data in Megacities Will Have Significant Warfighting Value: Walk



Valuable IoT Data Types

- Vehicles: vehicle position, location, traffic control, vehicle occupancy
- Buildings: Occupancy, occupant location, appliance status, stock (food, etc.) inventory, sewer contents
- Medical: Disease trends, medical stock inventory

Warfighting Questions That Could Be Answered

- Best way to ingress and egress
- Know target locations and patterns of life
- Differentiation of red vs grey

Know your adversary:

IoT data ("IoTINT"), when fused with other intelligence data, lead to better situational awareness for Soldiers operating in megacities

UNCLASSIFIED

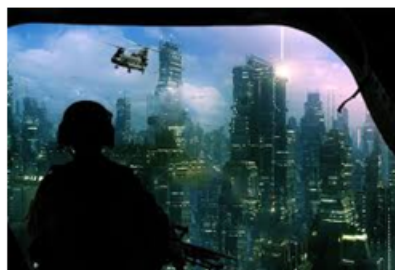
Army Science Board 19



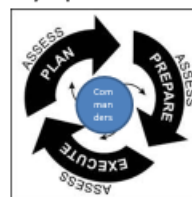
IoTINT Helps Both in Planning and Execution

Planning: Data traffic of IoT sensors provides information on the 'state' of the city:

- Data from household devices provides information on when people are present
- Data from hospitals provides state of community



Army Operations Process



Execution: Data traffic of IoT sensors provides real-time information on where individuals are moving within a building

- Real-time data to provide information for ingress/egress

Using IoTINT has the potential to improve planning and execution of Army urban operations

UNCLASSIFIED

Army Science Board 20



Combat Use of IoTINT Research

- Significant IoT research efforts already underway, e.g.
 - DARPA: “Leveraging the Analog Domain for Security” Program
 - DHS S&T: R&D focused on security for automotive, building, and medical devices
 - NSA and ARL have related efforts
- However, none of these will deliver Army combat IoTINT capability
- Army has opportunities to:
 - Influence the direction of existing R&D efforts to move them in directions relevant to the Army
 - Advocate for the creation of new R&D efforts focused on combat use of IoTINT
 - Serve as transition partner for these new efforts

* Consistent with the DSB 2015 Summer Study on Strategic Surprise Recommendation #15.

UNCLASSIFIED

Army Science Board 21



Combat Value of Disrupting and Controlling Red and Grey IoT Systems

- Megacity operations will become increasingly dependent on IoT networks and devices
 - Army operations could be assisted by disrupting “red” IoT systems and controlling “grey” IoT systems, e.g.
 - Transportation systems
 - Building systems
 - Water/sewer systems
 - Electrical/power systems
 - Industrial systems
 - Challenges
 - Technical
 - Doctrinal
 - Legal
 - Key questions:
 - What value might this bring to the Army?
 - Related: What value might this same capability bring to US adversaries?
- 



- Determine value of maneuver capability within adversary's IoT
- Distort the adversary's understanding and manipulate their actions
- Use IoT to influence Grey

UNCLASSIFIED

Army Science Board 22



IoTINT and IoT Disruption Can Enhance Autonomous Operations in Megacities: Run



Autonomous JLTV

Manned Stryker

UNCLASSIFIED

Army Science Board 23



IoTINT and IoT Disruption Can Enhance Autonomous Operations in Megacities



Autonomous JLTV

Manned Stryker

- Autonomous systems will have their own sets of sensors which provide a baseline situational awareness
- IoTINT provides extended real-time situational awareness using non-organic sensors
- Process IoT data (and local sensor data) within the autonomous system – data fusion at the edge
- IoTINT will enhance operations for both Soldiers and unmanned systems*

IoT exploitation and attack enable Kinetic and Non Kinetic effects

* Reference 2016 ASB Studies on Fires, RAS, Soldier Enhancement

UNCLASSIFIED

Army Science Board 24



Roadmap

- Introduction
 - Study Team
 - Terms of Reference
 - Visits
 - Definition and Relevance
- Use Cases (Crawl, Walk, Run)
- ➡ Cross-Cutting Considerations
- Findings and Recommendations

UNCLASSIFIED

Army Science Board 25

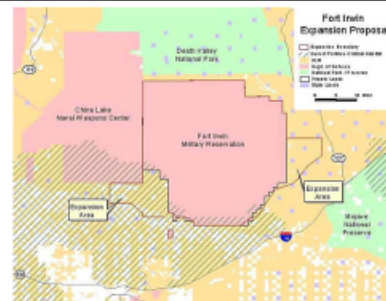


NTC Data and IoT Creating an Analytics Framework Today

NTC conducts 10 to 11 BCT evolutions/year

- Maneuver data is recorded over an ATT 4G/5G cell network
- OPFOR uses same network to exercise operations against Blue force
- Significant log platform data is recorded on platform and downloaded post operation
- Other data recorders could be added

Army Analytics Group (AAG) has the ability to fuse data and conduct deep learning across massive, integrated data sets



The opportunity exists to create an Analytical Framework by merging NTC blue and red operations and log data to include LIA log mesh net, while anonymizing datasets and incorporating EW effects

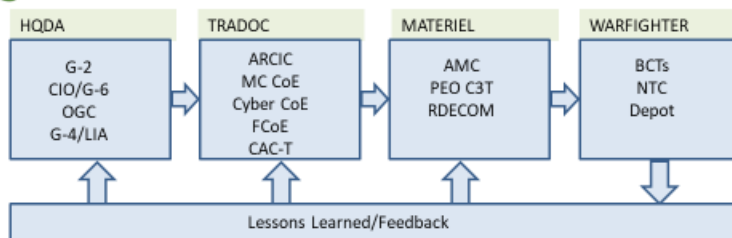
- Forming Situational Understanding and determining the analytics needed without revealing sources
- Informing the requirements process
- The development of tactics and techniques to exploit IoT without impacting the tempo of BCT experience in the NTC

UNCLASSIFIED

Army Science Board 26



Cross-Cutting Considerations Policy and Requirements



Because the Army has not yet developed a vision and strategy to use IoT:

- Acquisition community has no requirements, therefore there is no program plan to integrate IoT technology into any platform or product
- Requirements community has no experience with IoT systems, therefore isn't writing requirements
- The Army CoEs have not adopted and internalized the impact of IoT
- The warfighter does not have IoT enabled combat capability

UNCLASSIFIED

Army Science Board 27



Cross-Cutting Consideration Cyber Security Risk

Risk = F(Vulnerability, Exploit, Impact, Intent)

Example



Scenario	Vulnerability	Exploit	Impact	Intent	Risk
Cyber attack against automobile	Insufficient protection of wireless interfaces, insufficient intra-vehicle network isolation, lack of data integrity checking	Insert malformed packets on to vehicle networks, insert resident implants on vehicle computers.	Misinformation presented to driver, malicious control of critical vehicle systems (e.g. brakes), leading potentially to vehicle crashes and passenger injuries	Not clear that criminals have found a way to "monetize" these types of attacks.	Low-Medium
Cyber attack against Army vehicle (notional)	Similar to above	Similar to above	Similar to above, but also includes mission kill, lack of confidence in ability to achieve mission, general confusion, etc.	Phase 0: Low, but could be used to lead to confusion Phase 1-4: Could be quite high, seen as an attractive alternative to kinetic engagement	Phase 0: Low-High Phase 1-4: High

Risk to Army in most phases of conflict is likely much higher than risks faced in commercial IoT cyber attacks

UNCLASSIFIED

Army Science Board 28



Consequences of Doing Nothing

Cede the IoT Battlespace to the enemy!

- Successful adversary exploitation of our IoT systems
- Overpayment for maintenance systems (e.g. vehicles)
- Waste in the management of buildings and infrastructure
- Unacceptably low readiness due to inefficient maintenance
- Limited situational awareness leading to ineffective Army urban operations

UNCLASSIFIED

Army Science Board 29



Roadmap

- Introduction
 - Study Team
 - Terms of Reference
 - Visits
 - Definition and Relevance
- Use Cases (Crawl, Walk, Run)
- Cross Cutting Considerations
- ➡ Findings and Recommendations

UNCLASSIFIED

Army Science Board 30



Findings

1. Army is not taking full advantage of industrial advances in IoT for warfighter effectiveness and cost savings:
 - a) Industry is investing and implementing IoT at an exponential rate
 - b) Success in industrial deployment of IoT is due to the reduced cost of deployment, advancements in cloud computing, and data analytics
 - c) Industry is using standards bodies to develop interoperability of IoT and there is no evidence of Army participation in these bodies
2. Army does not have IoT system level requirements that are needed for adoption on the battlefield and in the Army industrial base
3. There are cyber and network connectivity challenges that the Army has not yet solved
 - a) Current commercial IoT does not provide sufficient cyber security for critical Army missions
 - b) Some battlefield environments offer limited network connectivity

UNCLASSIFIED

Army Science Board 31



Findings

5. IoT issues cross policy and legal boundaries that must be resolved for Army applications
6. Army can harvest data and develop analytics that identify improvements of warfighter effectiveness:
 - a) NTC and other sources to inform on uses and defenses for IoT enabled things to include an EW environment
 - b) IMCOM as it permeates posts, camps, and stations (government and non government sources)
 - c) AMC installations for the Army industrial base (depots, arsenals, ammunition storage facilities, and ocean ports)
 - d) MEDCOM as it pertains to Soldier performance

UNCLASSIFIED

Army Science Board 32



Recommendations

1. AMC: identify the appropriate platform to implement power by the hour using Army railroad as an initial pilot to demonstrate cost savings and readiness improvements
2. AMC and IMCOM: expand existing efforts in depots and smart forts by utilizing smart cities technologies for cost savings, and efficiencies
3. MEDCOM: identify Soldier performance data that are important for battlefield awareness
4. G3/5/7 and OGC: update policies for both legal and implementation issues required to utilize IoT
5. DUSA: task AAG to create an analytics framework for experimentation for knowledge, acceptance, and development of DOTML-PF that will:
 - a) Support Blue on Blue and Blue on Red analysis for a tactical analysis (SME: FORSCOM, MEDCOM)
 - b) Support Blue on Blue and Red on Blue, OPSEC assessments (SME: FORSCOM, MEDCOM, and AMC)
 - c) Inform requirements process across all Army (SME: TRADOC and ASA(ALT))

UNCLASSIFIED

Army Science Board 33



Recommendations

6. TRADOC: define requirements for IoT systems and have representation on R&D programs related to IoT
7. G6: actively participate in IoT commercial standards bodies to represent the Army's interest
8. ARL: advocate and co-fund (e.g. with DARPA or IARPA) research programs around
 - a) offensive use of adversary's IoT (blue on red/grey)
 - b) adapting the analytics from IoT to disadvantaged (intermittent connectivity, low data rate) networks
9. ASA (ALT), CIO-G6, G3/5/7, AMC, & ARCYBER: include IoT considerations in Army cyber resiliency efforts
10. ARCYBER: develop a risk mitigation strategy for inclusion of IoT in military operations and platforms
11. ARCYBER: conduct adversarial cyber red teaming using IMCOM smart forts as test beds

UNCLASSIFIED

Army Science Board 34



“By 2025, you will not be able to avoid being connected”



UNCLASSIFIED

Army Science Board 35

APPENDIX E – GLOSSARY OF TERMS, ABBREVIATIONS, AND ACRONYMS

ABCT	Armored Brigade Combat Team	GAO	General Accounting Office
AD	Active Duty	GF	Generating Force
ALT	Acquisition, Logistics and Technology	GoCo	Government-owned, Contractor-operated
AMAF	Annual MOS Availability Factors	HQDA	Headquarters, Department of the Army
AMMH	Annual Maintenance Man-Hours	IDA	Institute for Defense Analysis
AO	Area of Operations	IPT	Indirect Productive Time
AOAP	Army Oil Analysis Program	JPADS	Joint Precision Air Drop System
AOR	Area of Responsibility	LMI	Logistics Management Institute
APOE	Aerial Point of Embarkation	LOGCAP	Logistics Civil Augmentation Program
AR	Army Regulation	LOGSA	Logistics Support Activity
ARFORGEN	Army Force Generation	M&RA	Manpower and Reserve Affairs
ASA	Assistant Secretary of the Army	MACOM	Major Army Command (obsolete)
ASB	Army Science Board	MARC	Manpower Allocation Requirements Criteria
ASIOE	Associated Support Items of Equipment	MOD	Ministry of Defence (UK)
AWPS	Army Workload Performance System	MOS	Military Occupational Specialty
BCT	Brigade Combat Team	MS ³	Manpower Staffing Standard System
BOIP	Basis of Issue Plan	MTDA	Modification Table of Distribution and Allowance
BOIPFD	Basis of Issue Plan Feeder Data	MTOE	Modified Table of Organization and Equipment
CAB	Combat Aviation Brigade	OCS	Operational Contract Support
CAB (M)	Combat Aviation Brigade (Medium)	OF	Operating Force
CBM	Condition Based Maintenance	OMS/MP	Operational Mode Summary/Mission Profile
CBM+	Condition Based Maintenance Plus	OSD	Office of the Secretary of Defense
CG	Commanding General	PEO	Program Executive Officer
CMICS	Civilian Manpower Integrated Costing System	PM	Program Manager
COCOM	Component Commander	PMCS	Preventative Maintenance Checks and Services
CONOP	Concept of Operations	POE	Port of Embarkation
CSA	Chief of Staff of the Army	RC	Reserve Component
CSS	Combat Service Support	RDECOM	Research, Development and Engineering Command
CULT	Common User Land Transportation	RIF	Reduction in Force
DCS	Deputy Chief of Staff	ROI	Return on Investment
DoD	Department of Defense	S&T	Science and Technology
DPAMMH	Direct Productive Annual Maintenance Man-Hours	SBCT	Stryker Brigade Combat Team
EIS	Enterprise Information Systems	Sec Army	Secretary of the Army
FFRDC	Funded Research and Development Centers	SIPT	Supportability Integrated Process Team
FILO	First in, Last Out	STEM	Science, Technology, Engineering and Math
FMSWEB	Army Force Management Support Agency	TEU	Twenty-Foot Equivalent Units
FOB	Forward Operating Base	TOE	Table of Organization and Equipment
FTE	Full-Time Equivalent	TOR	Terms of Reference
FY	Fiscal Year	TRADOC	Training and Doctrine Command
G1	Personnel	USAFMSA	U.S. Army Force Management Support Agency
G3	Operations	USAMAA	U.S. Army Manpower Analysis Agency
G4	Logistics	USTRANSCOM	U. S. Transportation Command