US DOD and NATO plan Battlefield Internet of Things connecting sensors, wearables, weapons, minitions, platforms and networks for information dominance

The Internet-of-Things is an emerging revolution in the ICT sector under which there is shift from an “Internet used for interconnecting end-user devices” to an “Internet used for interconnecting physical objects that communicate with each other and/or with humans in order to offer a given service”.

The increasing miniaturization of electronics has enabled tiny sensors and processors to be integrated into everyday objects, making them ‘‘smart’’ , such as smart watches, fitness monitoring products, food items, home appliances, plant control systems, equipment monitoring and maintenance sensors and industrial robots. By means of wireless and wired connections, they are able to interact and cooperate with each other to create new applications/services in order to reach common goals. By 2025, it is predicted that there can be as many as 100 billion connected IoT devices or network of everyday objects as well as sensors that will be infused with intelligence and computing capability.

The rapid growth in IOT devices, however will offer new opportunities for hacking, identity theft, disruption, and other malicious activities affecting the people, infrastructures and economy. Some incidents have already

happened, FDA issued an alert about a connected hospital medicine pump that could be compromised and have its dosage changed. Jeep Cherokee was sensationally remote-controlled by hackers in 2015.

The military operations will be significantly affected by widespread adoption of IoT technologies. Analogous to IoT, Military internet of things (MIOT) comprising multitude of platforms, ranging from ships to aircraft to ground vehicles to weapon systems, is expected to be developed. MIoT offers high potential for the military to achieve significant efficiencies, improve safety and delivery of services, and produce major cost savings.

Some of the military applications include fully immersive virtual simulations for soldiers' training; autonomous vehicles; the ability to use smart inventory systems to consolidate warehouses using a web-based delivery and inventory system; and business systems like the Army Strategic Management System to manage energy, utilities and environmental sensors. The military has begun taking steps towards implementing IoT technologies—some troops have been issued with helmets containing built-in monitoring devices to detect potential concussions and other brain injuries.

"With strategy concepts such as "net centric," "information dominance," and the emergence of cyber as an entirely new domain of operations, information always has and will remain central to the military's efficiency and effectiveness. Naturally, IoT technologies and architectures that are designed to move and process information more quickly and in distributed environments seem like natural fits for military applications," write Joe Mariani, Brian Williams, Brett Loubert.

Military Internet of Things

The vision of military internet of things (MIOT) is to realize “anytime, anyplace connectivity for anything, ubiquitous network with ubiquitous computing” in military domain. Commanders make decisions based on real-time analysis generated by integrating Sensors data from unmanned sensors and reports from the field. These commanders shall benefit from a wide range of information supplied by sensors and cameras mounted on the ground, and manned or unmanned vehicles or soldiers.

The DOD has been using IoT in various ways for years, Pellegrino noted, especially for managing its energy usage and physical infrastructure. Connected energy management solutions have allowed the military to reduce total energy consumption by 23 percent since 2002. The military has about 8,000 smart meters installed, with 66 percent of them reporting to an integrated management system. Connected water management has allowed the military to cut portable water use intensity by 27 percent since 2007, he said.

The University of Illinois is leading a $25 million initiative to develop an “internet of battlefield things.” Officials say the initiative aims to have humans and technology work together in a seamless network. They say the initiative will connect soldiers with smart technology in armor, radios, weapons and other objects to give troops a better understanding of battlefield situations and help them assess risks. Experts say future military operations will rely less on human soldiers and more on interconnected technology. They say unmanned systems and machine intelligence advances can be used to improve military capabilities.

Soldiers need a continual flow of information to make the best decisions possible in battle because they are constantly making quick decisions in the face of adverse conditions, UI computer science professor Tarek Abdelzaher said. “You need to

connect to the right sensors, the right cameras, the right devices to collect the right pieces of information," Abdelzaher said.

The present application researches of MIOT are almost limited on how to improve working efficiency in logistic domain using IOT technologies. In future MIOT can be Equipment Maintenance, Smart Bases, Personal Sensing, Soldier Healthcare, Battlefield Awareness, C4ISR and Fire-Control Systems. Joe Mariani, Brian Williams, Brett Loubert categorize IoT applications according to those that aim to improve cost efficiency, those that aim to improve warfighter effectiveness, and rare cases that aim for both.

Some of the applications of MIoT are:

1. Military Equipment Logistics – IoT can be huge enabler of efficiency, visibility and military equipment in the right hands at right time. Deploying radio frequency identification tags and standardized barcodes to track individual supplies down to the tactical level could provide real-time supply chain visibility and allow the military to order parts and supplies on demand. The ability to use smart inventory systems to consolidate warehouses using a web-based delivery and inventory system.
2. Equipment Maintenance: The harsh conditions and extended deployments put extensive wear and tear on equipment. IoT can enable enhanced equipment maintenance and management through monitoring, optimizing and appropriately allocating various resources and processes such as manpower, material, financial resources and maintenance personnel.
3. Smart Bases that incorporate commercial IoT technologies in buildings, facilities, etc., force protection at bases as well as maritime and littoral environments, health and personnel monitoring, monitoring and Justin-time equipment maintenance.

4. Personal Sensing, Soldier Healthcare – The combination of IoT sensors (temperature, blood pressure, heart rate, cholesterol levels and blood glucose) through body area networks will allow the health of the soldier to be monitored in real time. Soldiers can be alerted of abnormal states such as dehydration, sleep deprivation, elevated heart rate or low blood sugar and, if necessary, warn a medical response team in a base hospital.
5. Battlefield Awareness – Situational awareness encompasses a wide range of activities in the battlefield to gain information on enemy's intent, capability and actual position. IoT can enable a vital role by collecting, analyzing, and delivering the synthesized information in real time for expeditious decision making. IoT can enhance Battlefield Awareness from global, to company, platoon and squad commanders down to single soldiers level.
6. Fire-Control Systems: In fire-control systems, end-to-end deployment of sensor networks and digital analytics enable fully automated responses to real-time threats, and deliver firepower with pinpoint precision. Munitions can also be networked, allowing smart weapons to track mobile targets or be redirected in flight.
7. Other use cases for IoT include fully immersive virtual simulations for soldiers' training; autonomous vehicles;and business systems like the Army Strategic Management System to manage energy, utilities and environmental sensor.

Vulnerability of Military Internet of Things

Security equipment is also vulnerable to exploitation by politically and criminally motivated hackers. Security

researchers Runa Sandvik and Michael Auger gained unauthorized access to the smart-rifle's software via its WiFi connection and exploited various vulnerabilities in its proprietary software. The TP750 was tricked into missing the target and not firing the bullet. Recently IoT devices are themselves used for attacks such as when an internet-connected fridge was used as a botnet to send spam to tens of thousands of Internet users.

Military IoT networks will also need to deal with multiple threats from adversaries, said Army's John Pellegrino deputy assistant secretary of the Army for strategic integration, including physical attacks on infrastructure, direct energy attacks, jamming of radiofrequency channels, attacks on power sources for IoT devices, electronic eavesdropping and malware.

DARPA has launched Leveraging the Analog Domain for Security (LADS) Program for developing revolutionary approaches for securing Military Internet of things. LADS will develop a new protection paradigm that separates security-monitoring functionality from the protected system, focusing on low-resource, embedded and Internet of Things (IoT) devices.

US Army's Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA)

US Army's Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA)

Through its Internet of Battlefield Things (IoBT) Collaborative Research Alliance, the Army has assembled a team to conduct basic and applied research involving the explosive growth of interconnected sensing and actuating technologies that include distributed and mobile communications, networks of information-driven devices, and artificially intelligent

services, and how ubiquitous “things” present imposing adversarial challenges for the Army. Alliance members leading IoBT research areas include UIUC, University of Massachusetts, University of California-Los Angeles and University of Southern California. Other members include Carnegie Mellon University, University of California Berkeley and SRI International.

The ability of the Army to understand, predict, adapt, and exploit the vast array of internet worked things that will be present of the future battlefield is critical to maintaining and increasing its competitive advantage. The explosive growth of technologies in the commercial sector that exploits the convergence of cloud computing, ubiquitous mobile communications, networks of data-gathering sensors, and artificial intelligence presents an imposing challenge for the Army. These Internet of Things (IoT) technologies will give our enemies ever increasing capabilities that must be countered, but commercial developments do not address the unique challenges that the Army will face in using them.

The U.S. Army Research Laboratory (ARL) has established an Enterprise approach to address the challenges resulting from the Internet of Battlefield Things (IoBT) that couples multi-disciplinary internal research with extramural research and collaborative ventures. ARL intends to establish a new collaborative venture (the IoBT CRA) that seeks to develop the foundations of IoBT in the context of future Army operations. The Collaborative Research Alliance (CRA) will consist of private sector and government researchers working jointly to solve complex problems. The overall objective is to develop the fundamental understanding of dynamically-composable, adaptive, goal-driven IoBTs to enable predictive analytics for intelligent command and control and battlefield services.

For the purposes of this CRA, an Internet of Battlefield Things (IoBT) can be summarized as a set of interdependent and interconnected entities (e.g. sensors, small actuators,

control components, networks, information sources, etc.) or “things” that are: dynamically composed to meet multiple mission goals; capable of adapting to acquire and analyze data necessary to predict behaviors/activities, and effectuate the physical environment; selfaware, continuously learning, autonomous, and autonomic, where the things interact with networks, humans, and the environment in order to enable predictive decision augmentation that delivers intelligent command and control and battlefield services.

The IoBT is the realization of pervasive computing, communication, and sensing where everything will be a sensor and potentially a processor (i.e. increased number of heterogeneous devices, connectivity, and communication) where subsequent information is of a scale unseen before. The battlespace itself will consist of active red (enemy), blue (friendly), and gray (non-participant) resources, where deception will be the norm, the environment (e.g. megacities and rural) will be dynamic, and ownership and other boundaries will be diverse and transient.

These IoBT characteristics all translate into increased complexity for the warfighter, particularly because current, commonly available, interconnected “things” will exist in the battlefield and be increasingly intelligent, obfuscated, and pervasive. These IoBT characteristics all translate into increased complexity for the warfighter, requiring situation-adaptive responses, selective collection/processing and real time sensemaking over massive heterogeneous data.

The objective of the IoBT CRA is to develop the underlying science of pervasive, heterogeneous sensing and actuation to enhance tactical Soldier and Mission Command autonomy, miniaturization, and information analytic capabilities against adversarial influence and control of the information battlespace; delivering intelligent, agile, and resilient decisional overmatch at significant standoff and op-tempo.

The IoBT CRA consists of three main research areas: Device/Information Discovery, Composition, and Adaptation to establish theoretical foundations that facilitate goal-driven discovery, adaptation, and composition of devices and data at unprecedented scale, complexity, and rate of acquisition; Autonomous & Autonomic Actuation Enabling Intelligent Services to advance the theory and algorithms for complexity and nonlinear dynamics of real-time actuation and robustness with a focus on autonomic system properties (e.g. self-optimizing, self-healing and self-protecting behaviors); and Distributed Asynchronous Processing and Analytics of Things to enrich the theory and experimental methods for complex event processing, with compact representations and efficient pattern evaluation.

Distributed and Collaborative Intelligent Systems (DCIST) Collaborative Research Alliance (CRA)

Through its Distributed and Collaborative Intelligent Systems (DCIST) Collaborative Research Alliance (CRA), the Army will perform enabling basic and applied research to extend the reach, situational awareness, and operational effectiveness of large heterogeneous teams of intelligent systems and Soldiers against dynamic threats in complex and contested environments and provide technical and operational superiority through fast, intelligent, resilient and collaborative behaviors. Alliance members include the University of Pennsylvania as the lead research organization. Individual research area leads are MIT and Georgia Tech. Other consortium members are University of California San Diego, University of California Berkeley and University of Southern California.

DCIST concentrates its research into three main areas: distributed intelligence, led by MIT, where researchers will establish the theoretical foundations of multi-faceted distributed networked intelligent systems combining autonomous

agents, sensors, tactical super-computing, knowledge bases in the tactical cloud, and human experts to acquire and apply knowledge to affect and inform decisions of the collective team; heterogeneous group control, let by Georgia Tech, to develop theory and algorithms for control of large autonomous teams with varying levels of heterogeneity and modularity across sensing, computing, platforms, and degree of autonomy; and adaptive and resilient behaviors, led by the University of Pennsylvania, to develop theory and experimental methods for heterogeneous teams to carry out tasks under the dynamic and varying conditions in the physical world. In addition to these three main research areas, research will be pursued along three underlying research themes in Learning, Autonomous Networking, and Cross Disciplinary Experimentation.

The U.S. Army's operational competitive advantage in a multi-domain battle will be realized through technology dominance, said ARL Director Dr. Philip Perconti.

NATO task group to examine applicability of IoT to Military

These IoT networks will need to deal with multiple threats from adversaries, Pellegrino said, including physical attacks on infrastructure, direct energy attacks, jamming of radiofrequency channels, attacks on power sources for IoT devices, electronic eavesdropping and malware.

NATO has set up RTO task group (IST-147) that would select a scenario to examine applicability of IoT to military operations including base operations, situational awareness, boundary surveillance including harbour, energy management, and etc. It shall also access the risk of applying IoT technologies in the scenario. Based on this risk assessment, models for security and trust management that address the most significant risks will be proposed. Mitigation measures may

include: Managing identity, credentials and rights of IoT devices and users; Object level protection and trust; and Assessment of available or emerging commercial security solutions. It shall also define an IoT architecture or architectures that might be used in military situations taking into account existing IoT architectures used in other domains.

Challenges and Requirements for Military internet of things (MIOT)

There is great potential for IoT technologies to revolutionize modern warfare, leveraging data and automation to deliver greater lethality and survivability to the warfighter while reducing cost and increasing efficiency. However the successful development and deployment of IoT technologies across the military requires many challenges to be solved:

1. In contrast to commercial deployments that mainly focus on systems with fixed sensors/devices Military internet of things (MIOT) shall consist of large number of mobile things such as UAVs, Aircrafts, tanks e.t.c. The mobile IoT paradigm invalidates many of the assumptions of traditional wireless sensor networks, especially with regards to wireless technologies and protocols. In particular, mobile IoT devices would find it quite difficult to connect with each other and other components of the IoT network in the presence of mobility, intermittent connectivity and RF link variability.
2. Deployment Features: One of the biggest constraints in a battlefield environment is power consumption. IoT devices are likely to be powered by batteries or solar power, and charged on-the-move from solar panels, trucks, or even by motion while walking. In either case, they should last for extended periods of time (at least for the duration of the mission). Therefore, devices and

sensors need to be power-efficient.

3. Challenges related to reliability and dependability, especially when IoT becomes mission critical. Equipment should fulfill the requirements imposed and be compliant with the considerations from military standards (e.g., MIL-STD 810G, MIL-STD 461F, MIL-STD-1275). IoT devices should be ruggedized and prepared to operate under extreme environmental conditions.
4. Security challenges related to co-existence and interconnection of military and civilian IoT networks. Security concerns are the main issue holding back the military's use of the Internet of Things. Some potential adversaries have advanced cyber and electronic warfare capabilities, and everything connected to the Internet is potentially vulnerable to attack.
5. Node Capture Attacks: In a node capture attack, the adversary can capture and control the node or device in IoT via physically replacing the entire node, or tampering with the hardware of the node or device.
6. Electronic Warfare: Another challenge to IoT implementation is that it makes systems vulnerable to electronic warfare. Most IoT technologies communicate wirelessly on radio frequencies. Adversaries can use relatively unsophisticated methods like RF jamming to block these signals, rendering the devices unable to communicate with backbone infrastructure.
7. Information management challenges for military application of IoT – trustworthiness, pedigree, provenance, and enabling military commanders and missions to benefit from IoT generated information.

IoT can serve the warfighter better with more intelligence and more ways to coordinate actions amongst themselves. In 20 years the IoT will be ubiquitous, Yet for the Army and wider military to make the most of IoT, it will need to rely on heterogeneous and flexible networks that continue to operate in environments with spotty connectivity, and don't place

burdens on soldiers, said Pellegrino, deputy assistant secretary of the Army for strategic integration.

Pellegrino said some connected devices will be intelligent, and others will be “marginally intelligent” but that connectivity will spread everywhere, from munitions to weapons, robotics, vehicles and wearable devices. All of these devices will generate an enormous amount of data, he said, and the military needs to figure out how to make that data useful.

The CIA and Defense Information Security Agency (DISA) are working with commercial companies to bring the cloud and software to secure government networks. Thus, the infrastructure for dealing with the data volume of tactical IoT applications is, potentially, already in place.

“All of these devices are going to be performing a massive variety of tasks,” Pellegrino said, including recommendations on where and when to attack and defend, and which of them will need to be coordinated.

New technologies required to power IoT

State-of-the-art (SOA) sensors use active electronics to monitor the environment for the external trigger, consuming power continuously and limiting the sensor lifetime to durations of months or less. In addition, it increases the cost of deployment, either by necessitating the use of large, expensive batteries or by demanding frequent battery replacement. It also increases Warfighter exposure to danger.

DARPA’s N-ZERO program intends to extend the lifetime of remotely deployed communications and environmental sensors from months to years, by supporting projects that demonstrate the ability to continuously and passively monitor the environment, waking an electronic circuit only upon the detection of a specific trigger signature. DARPA’s N-ZERO

program can also enable the future billions of Internet of Things (IoT) devices that shall be deployed ‘everywhere’ and to be accessed ‘any time’ from ‘anywhere’.

For more information on DARPA N-ZERO:http://idstch.com/home5/international-defence-security-and-technology/technology/energy/darpa-s-n-zero-program-will-allow-unattended-wireless-sensor-network-monitoring-for-years/

Flexible Networks

Wireless Sensor Networks shall play major part in another revolution that is in IoT although other communication techniques are also used in IoT. The future billions of Internet of Things (IoT) devices shall be deployed ‘everywhere’ and to be accessed ‘any time’ from ‘anywhere’, anything from large buildings, industrial plants, planes, cars, machines, any kind of goods. WSN technology shall also be employed in smart cities for applications in smart grid, smart water, intelligent transportation systems, and smart homes.

Pellegrino notes that the battlefield situations the military operates in “range from the moderately stable to very high dynamic situations.” To support IoT, the military’s networks will need to be flexible and interactive, he said, and still work despite limited bandwidth, intermittent connectivity and with a large number of devices on the network.

The arrangement of those networks needs to be done “totally autonomously,” he said. The military’s partners may be changing depending on the mission, and connected devices will need to work across networks with different network equipment and configurations.

“To achieve changing objectives with multiple complex tradeoffs, we have got to have highly adaptive management and organization leading to action, with no burden on the soldier, either cognitive or physical burden,” Pellegrino said.

DARPA has been experimenting with “mobile ad hoc networks,” designed to form a self creating and self healing mesh of communication nodes, with setup time measured in minutes instead of days. DARPA envisions networks of more than 1,000 nodes providing individual soldiers with streaming video from drones and other sensors, radio communications to higher headquarters, and advanced situational awareness of other soldiers’ location and status.

DARPA’s Revolutionary Approach “LADS” for IoT Security

DARPA, the Department of Defense’s Advanced Research Projects Agency, issued a call for “innovative research proposals” for the Leveraging the Analog Domain for Security (LADS) Program. The program is directing $36 million into developing enhanced cyber defense through analysis of involuntary analog emissions, including things like “electromagnetic emissions, acoustic emanations, power fluctuations and thermal output variations.”

The program will explore technologies to associate the running state of a device with its involuntary analog emissions across different physical modalities including, but not limited to, electromagnetic emissions, acoustic emanations, power fluctuations and thermal output variations. This will allow a decoupled monitoring device to confirm the software that is running on the monitored device and what the current state of the latter is (e.g., which instruction, basic block, or function is executing, or which part of memory is being accessed).

for more information on DARPA LADS: http://idstch.com/home5/international-defence-security-and-technology/cyber/darpa-launched-lads-program-secure-military-internet-things-miot-cyber-attacks-adversaries-hackers-terrorists/

References and resources also include:

- http://www.fedtechmagazine.com/article/2016/05/internet-things-battlefield-needs-be-flexible-army-official-says
- https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-military-defense-industry.html
- https://researchfunding.duke.edu/internet-battlefield-things-iobt-collaborative-research-alliance-cra
- https://www.eurekalert.org/pub_releases/2017-10/uarl-bit100417.php