"INTERNET OF THINGS": A NEW PARADIGM FOR MILITARY OPERATIONS

ASHISH GUPTA

Modem warfare has reached a strategic inflection point in the wake of different geo-political challenges, global terrorism menace, different economic challenges, violence emanating from religious radicalisation and internal security challenges. Warfare is no longer the sum total of capabilities, of putting more personnel, capital and technology on the battlefield, but of better situational awareness, contextual knowledge, discerning disposition and homogenised actions. Technological breakthroughs have profoundly altered and shaped the doctrinal, organisational and strategic contours of warfare. History is replete with examples in which adoption and assimilation of enabling technologies and corresponding shifts in doctrine, organisation and strategy have endowed the innovator with the capability to avoid attrition and pursue a form of "decisive" warfare.

Based on the outcome of the Persian Gulf War, which witnessed the use of an impressive array of high-technology weapons that allowed the coalition forces to overwhelm the world's fourth largest army in a remarkably short time, many strategists viewed these developments as revolutionary, spurred through technological breakthroughs rather than part of ordinary evolutionary innovations. At the same time, it is also

Group Captain **Ashish Gupta** is Senior Research Fellow at the Centre for Air Power Studies, New Delhi.

The phrase "Internet of Things (IoT)" has evolved to collectively identify the growing number of smart, connected products, with exponentially expanding opportunities.

important to understand that a revolution is not simply a demonstration of new technological capabilities. The revolutionary process is much more than a technology demonstrator—it is an all encompassing process that requires effective adaptation of such technologies for successful exploitation, corresponding doctrinal and organisational modifications, and willingness to digress from the established ways of doing things.

Information technology has revolutionised the way the warfare is conducted. Once comprising solely mechanical and electrical parts, military hardware has evolved into complex systems by a myriad combinations of various components and functionalities of sensors, microchips, microprocessors, hardware, software, data storage and connectivity. These "smart, connected products", bolstered by advancements and improvements in processing power, device miniaturisation and ubiquitous wireless connectivity, have put warfare on the cusp of an epochal shift, from the conventional to an information-based virtual age. These smart, connected products offer limitless possibilities and opportunities for new functionality, far greater reliability, higher and multifarious product utilisation, and capabilities that cut across, and transcend, the traditional domains of warfare. The changing nature of military hardware is also forcing a rethink of strategic doctrines, a reevaluation of concept of operations and a reassessment of doing things.

Smart, connected military products raise a new set of strategic challenges. The challenges of utilisation of a prodigious amount of new and sensitive data, insertion of new technology into legacy systems, redefining warfare outside the traditional military mindset, and the role of the military leadership in the backdrop of this new paradigm need to be tackled with due diligence. The phrase "Internet of Things (IoT)" has evolved to collectively identify the growing number of smart, connected products, with exponentially expanding opportunities. For exchange of information between people or

things, a virtual or physical connectivity is a prerequisite. The connectivity *per se* is only a conduit and it is the changing nature of the "things" with expanding capabilities and data generation that is ushering in a new era of warfare.

Embedded sensors, intelligent processors, sophisticated software and seamless connectivity in these products, coupled with data analysis and algorithmically induced decision-making capabilities, are driving unfathomable improvements in product functionality and performance.

Over the past 50 years, the information revolution radically reshaped military thinking, concept of operations and strategy. The world is now going to witness another transformation. Before the advent of modern Information Technology (IT), military hardware was predominantly mechanical, and activities in the conduct of warfare such as planning, resource allocation, exchange of instructions and orders were performed using manual modelling, verbal communication and paper processes. Riding of the IT wave, the adoption of IT enabled services in the realm of warfare saw a dramatic increase in the productivity of these activities, in part due to the enhanced ability to capture and analyse a huge amount of data associated with each activity. With increased connectivity and the rise of the internet, an IT-driven renaissance enables better coordination and integration across individual activities. These developments have made the administration, supervision, operation and coordination of military affairs much more productive, result oriented and temporally relevant.

Now, IT has become an indispensible appendage to all military activities. Proliferation of IT in military related products is remarkably variegated and prolific. Embedded sensors, intelligent processors, sophisticated software and seamless connectivity in these products, coupled with data analysis and algorithmically induced decision-making capabilities, are driving unfathomable improvements in product functionality and performance. This wave of IT-driven transformation has the potential to be bigger than its predecessors, triggering even more innovation, operational enhancements

The alloying of intelligence and connectivity gives rise to an entirely new set of product functionality and capabilities in four core areas: monitoring, control, optimisation and autonomy.

and tactical utilisation. Smart, connected products offer a whole new set of technological solutions to some of the challenges in modern warfare.

Smart, connected products are made by an amalgam of three core elements: physical components, "smart" components, and connectivity components. Smart components focus on value addition and capability enhancement of the physical components, while connectivity amplifies the capabilities of the smart components. The end result is the evolution of a dynamic process of value addition and improvement. The product's mechanical and electrical parts are termed as physical components while *smart* components are fabricated by using sensors, microprocessors, data storage, controls, software, embedded operating systems and enhanced user interface. In many products, software is increasingly used to emulate the functionalities of some hardware components or for enabling a single physical device to undertake multi-tasking at various levels. *Connectivity is achieved by using* components capable of interfacing/ interacting with the environment, medium or other devices by using ports, antennae, and protocols enabling wired or wireless connections.

MODERN WARFARE AND INTERNET OF THINGS

The alloying of intelligence and connectivity gives rise to an entirely new set of product functionality and capabilities in four core areas: monitoring, control, optimisation and autonomy. A capability developed in one area is in itself an enabler and energiser, and functions as a stepping stone for the next level, ultimately leading to the desired goal. For example, monitoring capabilities are the bedrock for successful command and control operations, optimisation and autonomy.

- **Monitoring:** Smart, connected products facilitate comprehensive monitoring of the pace and magnitude of operations and even subtle

changes in the external environment are recorded through sensors and external data sources. By analysing and synthesising data, the user is alerted to change/ modify circumstances or performance. Monitoring also gives an insight into the product's operating characteristics, its history and its utilisation. Intelligence, Surveillance and Reconnaissance (ISR) operations have always been the mainstay of military operations. ISR operations provide valuable inputs and data which support planning, decision-making and mission accomplishment.

In some cases, such as in air defence operations, monitoring is the core element of mission accomplishment. Air defence systems are made up of a set of sensors and a set of kill vehicles, collectively called a weapon system. While sensors are used to detect incoming targets, kill vehicles are assigned to destroy targets. Air defence weapon systems designed with smart products will be capable of controlling themselves in a coordinated manner. Based on a pre-evaluated threat threshold, the smart components monitor the evolving air situation and alert operators in advance if the threat reaches a pre-defined threshold. The sensors continuously monitor the assigned area, exchange information laterally with other sensors and allocate weapons to targets based on vicinity and kill probability.

- **Control:** Smart, connected products can be controlled through remote commands or algorithms that are built into the device or reside in the product cloud. Algorithms are rules that direct the product to respond to specified changes in its condition or environment. Control through software embedded in the product allows the customisation of product performance to a degree that previously was not effective or often even possible. The same technology also enables users to control and optimise their interaction with the product in many new ways.[1]
- **Optimisation:** The monitoring data garnered from smart, connected products and capacity to control product functionality allows optimisation of product performance in unthinkable ways—a capability

1. Michael E. Poter and James E. Heppelmann, "How Smart, Connected Products Are Transforming Completion," *Harvard Business Review*, November 2014, p.64.

acquisition not possible with earlier technology. Smart products, using algorithmic architecture and data analytics of in-use or historical data, offer improved efficiency and utilisation. In radar, for instance, a local microcontroller can adjust polarisation on every revolution during the rains. The radiated power can be adjusted to not only improve radar performance but minimise its impact on the efficiency of power generating components.

Real-time monitoring of data on equipment condition and its operational capability enables operators to optimise its utilisation by performing preventive maintenance and accomplishing repairs remotely, thereby reducing product down time and need for onsite repair teams. Even when onsite repair requirement is indispensible, advance information about failed components and instructions to accomplish the repairs reduces costs, reduces down time and improves spare management.

- **Autonomy:** *By smart* monitoring adaptive control and functionality optimisation capabilities, the smart, connected products can achieve a previously unattainable level of autonomy. Products equipped with sophisticated components and processes are capable of interacting with their environment, self-diagnosing their own service needs, optimising their output and adapting to operators' preferences. Autonomy not only reduces the continual presence of operators but improves operational safety in dangerous environments and facilitates operations in remote locations. Autonomous products can also self-synchronise and coordinate with other products and systems, producing results far exceeding the sum total of individual capabilities. The value of these capabilities can grow exponentially as more and more products become connected.

A whole gamut of technologies is driving the Internet of Things (IoT) evolution. IoT is no longer confined to the traditional range of physical devices. The amalgam of traditional devices, human operators and smart devices in varying temporal and spatial domains, greatly expands the scope of application of IoT. IoT takes the outside physical information as a sensing

foundation to realise identification of things, carry out dynamic sensing of environmental information, connect with other devices, and then builds a network by using various wired and wireless network communication technologies to achieve information transmission. After sensing, a connection needs to be realised for distributed data sharing by integrating sensing subnets with existing networks. IoT uses high-performance computing technology to achieve intelligent data management and decision-making. Based on the results from the decision-making process, the control of things and the environment is realised.

The data collection process of IoT is mainly through the control of various sensing devices to collect information on the surrounding environment and transfer the data through the corresponding network protocols.

- **Identification Technology:** For application of IoT, the basic requirement is recognition of things by assigning to each device, a globally unique value for its unambiguous identification. There are many coding rules, such as the Electronic Product Code (EPC) which uses Radio Frequency Indentification (RFID) technology, IP version 4 (IPv4) and IP version 6 (IPv6) which are based on the Transmission Control Protocol/Internet Protocol (TCP/IP). For the realisation of the full potential of IoT and seamless connectivity, mapping and compatibility issues between different coding methodologies need to be resolved. RFID is a non-contact identification technology for automatic identification of targets and collection of data through its radio frequency signals. TCP / IP based IPv4 and IPv6 technology is capable of meeting the requirement of a vast number of devices in IoT.
- **Sensing Technology:** Data acquisition in the form of generation, access, transmission, processing and application is an important component of IoT. In IoT, depending upon the type of sensing devices (RFID, infrared devices, TCP/IP-based devices, global positioning system devices), real-time data in various forms are acquired. The data collection process of IoT is mainly through the control of various sensing devices to collect

information on the surrounding environment and transfer the data through the corresponding network protocols.

- **Communication and Network Integration Technology:** The transmission of sensing data in IoT mainly relies on network and communication technology The network level of IoT is not limited to the traditional and single network structure but is spread over different types of networks, such as the internet, 2G/3G mobile communications networks, and broadcasting and television networks. It involves wired, wireless, mobile and other means of access, unification of heterogeneous network addresses, conversion, packet format, routing options and other issues.
- **Intelligent Information Processing Technology:** The key technology in IoT is how to transform physical sensing data into logic data. Intelligent information processing technology integrates intelligent computation, data mining, optimised algorithm and machine learning, and after processing and analyses of the data, the results are delivered to the intended user.

IoT-centric operations, like network-centric warfare, will enable a shift from attrition-centric warfare to a war-fighting style characterised by expeditious decision-making, versatile networked command and control, and self-synchronisation. IoT will accelerate the process of attainment of information superiority, better awareness and understanding of the battle space rather than simply more raw data. With the emergence of new challenges to national security, the changing nature of global terrorism and an ever-growing reliance on network-centric operations, the intelligence agencies have to trawl through vast amounts of data to identify subtle and specific signatures to determine the magnitude and timing of conditioned responses**.** In modern warfare, the key to successful operations is an immediate and appropriate response to fleeting signatures, and a detour from the time-consuming routine monitoring processes. The consequences of not dealing effectively with these challenges are potentially profound. IoT enabled forces, acting with speed, precision, and reach, achieve the massing of effects versus the massing of forces. The results that follow are the rapid

foreclosure of enemy courses of action and the shock of closely coupled events. [2] One of the potential strengths of IoT-centric warfare will be to offset a disadvantage in numbers, technology, or position.

BATTLEFIELD AWARENESS AND IOT

Carl von Clausewitz had stated, "The great uncertainty of all data in war is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which in addition, not infrequently—like the effect of fog or moonshine—gives to things exaggerated dimensions and unnatural appearance."[3] Situational Awareness (SA) encompasses a wide range of activities on the battlefield to gain information about the enemy's intent, his capability and actual position. Throughout military history, seeking of higher ground for an insightful perception of the battlefield has been the holy grail of warfare. Over recent years, aerial and space reconnaissance assets are being increasingly used to gain SA and thereby penetrate the fog of war. The main determinant of effectiveness in these operations is the speed of delivery of the relevant information. IoT can play a vital role in raising situational awareness by collecting, analysing and delivering the synthesised information in real-time for expeditious decision-making for appropriate military action. Defining SA in the realm of IoT requires understanding of SA from the perspective of the fact that SA is highly dependent on the following three factors:

Carl von Clausewitz had stated, "The great uncertainty of all data in war is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which in addition, not infrequently—like the effect of fog or moonshine—gives to things exaggerated dimensions and unnatural appearance."

- The perception of the elements in the environment within a volume of time and space.

2. Neil Couch and Bill Robins, "Big Data for Defence and Security," Royal United Services Institute for Defence and Security Studies, Occasional Paper, September 2013, p.1.
3. Clausewitz, *On War* (Project Gutenberg), Chapter II Section 24. Available online at http://www.gutenberg.org/ ebooks/1946?msg=welcome_stranger. Accessed on April 16, 2015.

- The comprehension of their meaning and/or comprehension of the current situation.
- The projection of their status in the near future.

Perception is the key to all SA because operators perceive the environment differently. Perception, in turn, impacts how each individual comprehends, and acts upon information. Comprehension is the ability to take disjointed elements from the perception phase and understand what their meaning and significance are to the greater whole. Projection is the ability to predict future actions, at least, in the near term; this is achieved from the knowledge that is obtained from perception and comprehension. IoT enabled devices can enhance the level of perception by adding an objective functionality to a complex and abstruse set of data. The chaotic war-time environmental signatures and stimuli are organised to fit in the human cognitive process for comprehension.

Today, *Battlefield Situational Awareness (BSA) can be enhanced* by leveraging real-time and untethered interactions among combatants, decision-makers and machines. Unification of Command, Control, Communications, Computers, Information, Surveillance, Reconnaissance (C4ISR) systems, sensors, video, voice, data collaboration and secure mobile computing is delivering transformative and emancipator battlefield capabilities. IoT technologies can conjure up an integrated battlefield awareness system for monitoring, planning and reacting to threats as they emerge. An IoT enabled wearable device will transform a war-fighter in the field into a communications node, capable of gathering and transmitting data back to analytics and command centres. The lateral and vertical exchange of information of the battlefield between aerial and space-based sensors, Unmanned Aerial Vehicles (UAVs), monitoring and communication devices, radars and wearable devices will provide real-time assessment of evolving operational requirements that help a military commander use assets effectively in deterring, and responding to, threats.

INTELLIGENCE AND OPERATIONS

For many intelligence experts, automated analysis technology is the top Intelligence, Surveillance and Reconnaissance (ISR) priority. In the military realm, data comes from a number of sources and platforms. It is varied and increasingly 'unstructured', with large quantities of imagery and video generated every day. It has been commented that data in military operations, "has reached an inflection point in data deluge. We are now in danger of data asphyxiation and decision paralysis."[4] The collected data need to be sieved through the mesh of perceived objectives and goals to perform real analysis rather than exhaustive culling of raw data. IoT enabled devices can be used as predictive tools capable of providing coherent and actionable sets of data. IoT devices are capable of performing semantic and pragmatic data analysis to which experts can then apply their experience, intuition and human judgment.

IoT will usher in a new era of efficiency, visibility and availability of military equipment in the right hands at the right time. It will be a huge enabler of creating efficiencies and unprecedented end-to-end visibility in every logistics activity and transaction.

APPLICATION OF INTERNET OF THINGS IN MILITARY EQUIPMENT LOGISTICS

The proliferation of data generated from connected devices and sensors will have an enormous impact on military equipment logistics processes and the way logistics oriented decisions are made. IoT will usher in a new era of efficiency, visibility and availability of military equipment in the right hands at the right time. It will be a huge enabler of creating efficiencies and unprecedented end-to-end visibility in every logistics activity and transaction. Gen Dennis J Reimer, chief of the staff of the army, famously said, "There will not be a revolution in military affairs unless there is a revolution in military logistics." A loose consensus is slowly developing to recognise the Revolution in Military Logistics (RML) as a necessary precondition of the Revolution in Military Affairs (RMA). For RML, the focus needs to be on:

4. Couch and Robins, n.2, p.10.

- **More Accurate and Timely Visibility of Demands:** IoT will further serve this demand by exploiting real-time information connectivity and auto communication by products of their status, health and requirements.
- **Quicker, More Responsive Processes:** Timely, integrated and predictive support even in unforeseeable conditions, as the products will accurately provide the information in real-time.
- **Increased Support From Afar:** During split-based operations conditions, by sustaining the force from dispersed geographical locations, as with IoT products, blow by blow performance evaluation would be possible.
- **Reduced Footprint:** By limiting the extent and magnitude of logistics support forces from the active theatre, attrition would be reduced.

Every smart equipment in the logistics chain, from intelligent storage to transportation to fitment and, finally, being declared operationally suitable, will give off streams of useful real-time data. By leveraging IoT in the logistics process, it will be possible to:

- Collect data coherently across the whole spectrum of military equipment to predict future demand accurately.
- Create efficient shipments and optimisation.
- Prioritise the components' availability.
- Initiate procurement processes by studying the consumption pattern and inventory held.

IOT AND CASUALTY MITIGATION

The care of war casualties, both during their service and as veterans, is the lynchpin of military ideology. Changes in battlefield medical technologies, evacuation of the seriously wounded from the battlefield and assisting those in need of physical and mental succour have profoundly changed the treatment of wounded and injured soldiers. Without proper care of the wounded, the morale of the troops would suffer. IoT is capable of fuelling tremendous growth and improvement in the provision of health care services to military personnel by improved monitoring, driving better outcomes, consistency of care, and enhancing the domain knowledge of

medical experts. IoT can combine human intelligence and diligence with technology advancements to deliver enhanced results. The personalised medical devices and mobile health care applications that make up IoT, have been increasingly making forays in the defence health care programmes. IoT can be further exploited to holistically improve all aspects of health care by not only managing health, but by disease prevention and fitness promotion. To bolster health care for defence personnel, leveraging the potential of IoT and adoption of IoT driven systems and processes, along with patient participation and subsequent data analysis, will change the way health services are delivered. IoT will continue to evolve fast, leading to impactful and positive changes in the realm of military forces.

The combination of IoT sensors will allow significantly improved measurement and monitoring methods of vital functions (temperature, blood pressure, heart rate, cholesterol levels, blood glucose, etc). Implantable wireless identifiable devices could be used to store health records that could save a patient's life in emergency situations. Edible, biodegradable chips could be introduced into the body and used for guided action. Things are more and more integrated within the human body. It is expected that body area networks can be formed and that they will communicate with treating physicians and emergency services.

IOT AND DEPLOYMENT/ MOBILISATION

Real-time route optimisation of all types of forces, equipped with IoT enabled devices, can be done by studying the steady stream of data generated during movements. The enabling automated capability to support rapid deployment of forces and to furnish accurate and timely data to manage the deployment conundrum has a bearing on operational efficiency and efficacy. The automated planning, organising, coordinating, and controlling of deployment activities will provide optimum, cost-effective and need-based solutions to the movement/deployment of both equipment and personnel, from origin to destination. For example, a system with IoT enabled devices will be able to plan and execute air movement as well as design and analyse force packages by real-time estimation of airlift requirements for a given

Modern aviation equipment with high technology integration requires managing and monitoring each component throughout the entire life-cycle process from its design, prototype fabrication, mass production, integration with other components, and maintenance.

deployment list, maintenance of pre-planned contingency packages, and by automated generation of individual aircraft load plans.

EQUIPMENT MAINTENANCE AND IOT

The core of military operations comprises resources—the combined human and physical assets necessary to perform at peak levels. In today's military Services, keeping military equipment major end items in mission capable condition has been a tremendous challenge in theatres of operation. The harsh conditions, extended deployments and stretching of the limits of their capabilities have put extensive wear and tear on equipment. The perennial operational readiness requirement of equipment throughout all the branches of the military Services is stretching the existing maintenance resources and practices to the limit. Many diverse and complex factors affect equipment maintenance, such as the battlefield environment, equipment condition, maintenance resources, technical level of personnel, etc. Therefore, it is of great significance to use advanced IoT technology for advanced equipment maintenance and management.

By using IoT, visualisation techniques and automatic identification technology, with a combination of computer platforms, databases, supervision of the maintenance personnel and material in important links, the nodes and parts of the maintenance process, can be effectively implemented. The safety management system with intelligent decision-making and automatic monitoring based on IoT will be capable of combining, optimising and appropriately allocating various resources and processes such as manpower, material, financial resources, information, technology, management level and equipment maintenance objects. For example, modern aviation equipment with high technology integration requires managing and monitoring each component throughout the entire

life-cycle process from its design, prototype fabrication, mass production, integration with other components, and maintenance.

IoT achieves automatic and intelligent information collection, transmission, processing and connections between objects through a variety of sensing equipment.[5] The management and process monitoring systems, based on IoT technology, can effectively improve the management efficiency of the equipment maintenance materials. The traceability of management behaviour and spare management information can be achieved by means of convenient, fast and accurate acquisition of raw materials.

IOT IN AEROSPACE AND AVIATION

IoT can help to improve the safety and security of products and services by protecting them from counterfeiting. Aviation maintenance, for example, is marred by the problem of Suspected Unapproved Parts (SUPs). A SUP is an aircraft part that is not guaranteed to meet the requirements of an approved aircraft part (e.g. the part does not conform to the strict quality requirements). Thus, SUPs pose a great risk of undermining the capability of a mission critical aircraft to meet its objective. SUPs can seriously violate the maintenance and security standards, leading to accidents or incidents. This problem can be solved by introducing electronic pedigrees for certain categories of aircraft parts, which document their origin and safety-critical events during their life-cycle (e.g., modifications). By storing these pedigrees within a decentralised database as well as on RFID tags, which are securely attached to aircraft parts, an authentication (verification of digital signatures, comparison of the pedigree on RFID tags and within the database) of these parts can be performed, for example, prior to installing them within an aircraft. Thus, the safety and security of an aircraft can be significantly improved. The 'on-condition' wireless monitoring of the aircraft by the use of intelligent devices with sensing capabilities available within the cabin or outside and connected to the aircraft monitoring systems is another emerging application area that forms the basis for ubiquitous

5. H. Sundmaeker, et al., "Vision and Challenges for Realizing the Internet of Things," IoT European Research Cluster (European Union, 2010).

The transformation of actionable and reliable knowledge and creation of perceptions from the large amount of data generated by the physical devices and human sensors requires further research and standardisation.

sensor networks. The nodes in such a network will be used for detecting various conditions such as pressure, vibrations, temperature, etc. The data collected gives access to customised usage trends, facilitates maintenance planning, allows condition-based maintenance, reduces maintenance and waste, and can be used as an input for evaluating and reducing energy consumption during aircraft operations.[6]

CHALLENGES OF IOT

It has been succinctly commented that "IoT describes a splendiferous future: a dynamic and universal network where billions of identifiable 'things' (e.g., devices, people, applications, services, etc.) are communicating with one another anytime and anywhere; things become context-aware, are able to configure themselves and exchange information, and show 'intelligent/cognitive' behaviour when exposed to a new environment and unforeseen circumstances; intelligent decision-making algorithms will enable appropriate rapid responses, revolutionizing the ways business values are generated." [7]

However, the present is not without challenges and tribulations, and the current research and developments, though promising, are still far from realisation of the envisaged vision. The diverse, heterogeneous and time dependent data generated by IoT enabled devices and resources is a major hurdle for the aggandisation of IoT. The transformation of actionable and reliable knowledge and creation of perceptions from the large amount of data generated by the physical devices and human sensors requires further research and standardisation. IoT requires efficient mechanisms and methods that can handle a large amount of data and respond to the identified phenomena and events arising from the environment in a timely fashion. Furthermore, security and privacy issues and the trust and reliability of the

6. Ibid.
7. Ibid.

data are also important for IoT-based applications and services, especially those in the military domain. Some of the major challenges are given below:

- **Inherent Dynamism and Complexity of IoT:** In the military realm, most of the data generated is transient in nature, with high spatiotemporal dependencies. While analysis of data for meaningful inferences is possible, the pervasiveness and volatility of the environments require continuous monitoring and updates. This inherent dynamicity becomes a challenging issue when scalability, diversity and network/resource constraints are taken into consideration. The challenge in the future will be further exacerbated in the wake of the mobility and ubiquity of IoT enabled military hardware providing real-time data streaming. The issues of dynamicity and complexity will have a significant impact on many aspects of military operations such as data and resource access services, and maintenance, data analysis, aggregation and mining.[8] Further research, refinement and consolidation for coherent data processing mechanisms are required to address these issues.
- **Scalability of IoT Resources:** Creating domain knowledge models from data garnered from a large number of IoT entities, devices and their related data is critical for data engineering and knowledge harvesting. The data generated during military operations is an expected outcome of different processes, so meaningful interpretation needs to be associated with domain knowledge of resources and entities. Many military specific applications have been developed to maintain own domain knowledge, but interoperability with cognitive layouts of human operators and algorithmic understanding of other IoT devices is an issue. The granularity of the data is another important issue; the completeness and unambiguity of the data will result in expansion of the domain knowledge realm. The data handling in the military environment is more challenging and fraught with technical difficulties due to the magnitude of data generated by corresponding resources, the continuous changes in the state of the resources and data, and the

8. Payam Barnaghi, Wei Wang, Cory Henson and Kerry Taylor, "Semantics for the Internet of Things: Early Progress and Back to the Future," p.16. Available online at http://knoesis.org/library/download/IJSWIS_SemIoT.pdf. Accessed on April 17, 2015.

The trustworthiness of these resources is another key issue which involves the capability of sensors to produce accurate and reliable data and its functioning in a changing environmental condition.

volatility of the environments.[9] A more efficient mechanism on information search and retrieval, indexing query and information access will be required to address these issues.

- **Quality, Trust, and Reliability of Data:** The data, after observation and measurement, is provided by different sensory devices designed to perform a myriad operations. However, the quality of observations and measurements can change over time, for example, changes in the environment, faults in devices, or errors in device settings. As with any sensor, IoT enabled military sensors are not entirely impervious to inaccurate and erroneous measurements, thereby affecting the quality, viability and veracity of data generated. Detection of anomalies, filtering out erroneous measurements and accepting data within the acceptable threshold can help in detecting errors and processing of data conforming to various operational requirements. The trustworthiness of these resources is another key issue which involves the capability of sensors to produce accurate and reliable data and its functioning in a changing environmental condition. Design adoptable sensors, with high reliability attributes, environment independent functionality, fitted with robust feedback and verification mechanisms can bridge the trust deficit.
- **Interpretation and Perception of Data:** The data received from various sensors is a key enabler for developing situation-aware applications that can intelligently respond to corresponding changes in operational conditions. Perception is the key to human intelligence and experience. Providing interpretation capabilities and analytics methods to sensors to process and elucidate changes in the battlefield will provide the military commanders with comprehension capabilities to take disjointed elements from the perception phase and understand their broader meaning and significance. However, sensor perception has additional

9. Ibid.

challenges such as integration and fusion of data from different sources, description of the events for cognitive understanding, risk threshold calculation, real-time processing of the data, and quality and dynamicity of the outputs. The research is this field needs to develop solutions that can efficiently query and access data from various sensors, geographically distributed, with different assigned roles. The requirement of situation recognition, anomalies detection and pattern association with existing knowledge to create higher-level abstractions or new knowledge are some of the challenges which need to be tackled.[10]

The research is this field needs to develop solutions that can efficiently query and access data from various sensors, geographically distributed, with different assigned roles.

- **Security and Privacy:** In the battlefield, the IoT enabled sensors will be used to describe the operational environment, the status of weapons, the location of mission critical assets, combatant deployment and other activities. This calls for mechanisms to provide and guarantee the security and privacy of data. While sharing and communicating the IoT data, encryption and verification measures for meeting the desired security levels and privacy requirements are a must. As data is shared over the communication networks and can be shared among myriad users and devices, it is paramount to regulate access control through authentication and authorisation. Security and privacy imperatives in the IoT domain are central to the development and consolidation of reliable and efficient solutions in support of military operations.

CONCLUSION

Smart, connected military products will have a transformative effect on the quality, efficiency and effectiveness of military operations. Increased situational awareness, better understanding of equipment performance, improved maintenance practices, and better heath care support to combatants will create opportunities for mission accomplishment, reduced

10. Ibid.

What distinguishes the victors is their grasp of information—not only from the mundane standpoint of knowing how to find the enemy while keeping him in the dark, but also in doctrinal and organisational terms.

attrition and casualty containment. The contours of the future conflicts will be shaped in part by how these technological advances are assessed and adopted. Yet, in the context of warfare, technology is an enabler but does not govern it. It is not technology *per se*, but rather the organisation of technology that is important. What distinguishes the victors is their grasp of information—not only from the mundane standpoint of knowing how to find the enemy while keeping him in the dark, but also in doctrinal and organisational terms. [11] History demonstrates that changes of this magnitude do not occur without being accompanied by a fundamental change in the way war is conducted.[12] The forays made by IoT in the warfare realm are a culmination of the advances in computerised information and telecommunications technologies. These advances, when married to related innovations in management and organisational theory, will inevitably have a profound impact on the means and ends of armed conflict.

11. Peter L. Hays, Brenda J. Vallance and Alan R. Van Tassell, *American Defense Policy* (London: John Hopkins University Press, 1997), p.567.
12. Norman C. Davis, *In Athena's Camp: Preparing for Conflict in the Information Age* (Rand National Defence Research Institute, 1997), p.79.