Internet of Things Centricity of Future Military Operations

Atul Pant*

Since the last decade of the twentieth century, network centricity has profoundly transformed warfighting and the outlook of the military. The next level of the networking ladder is Internet of Things (IoT), which has already started to disruptively change the ways in the civil domain, bringing a considerable autonomy to various processes by linking of a plethora of smart devices that are talking to each other. Militaries, in the near future, are also likely to see similar proliferation of IoT, which will bring a material change to their functioning and conduct of operations. This article analyses various facets and makes assessment of the IoT centricity of future military operations based on the IoT concept, IoT-led future shaping of the things, challenges and developmental trajectories of major powers.

The Internet became a global phenomenon in the last decade of the twentieth century and revolutionised the ways of the world; despite it being a product of the defence world as it was first created during the Cold War era to meet the challenges of communication in the face of ballistic missile threats. A ubiquitous entity today, next logical evolution of the Internet is the Internet of Things (IoT). IoT is the name given to a network of physical devices, vehicles, home appliances and other

* The author is an Indian Air Force officer from the fighter stream, and is presently a Research Fellow at Institute for Defence Studies and Analysis (IDSA). He is a graduate of the Defence Services Staff College, Wellington, and has served in various capacities in the air force, including instructional tenures and staff appointment at Air Headquarters.

ISSN 0976-1004 print

Journal of Defence Studies, Vol. 13, No. 2, April–June 2019, pp. 25–58

items that are embedded with electronics, software, sensors, actuators, etc., for machine-to-machine connectivity, exchanging data and/or being remotely controlled either mutually and autonomously or through computers. Besides, IoT enables heterogeneous electronic gadgets to share information and coordinate actions for stipulated task performance.

The term 'Internet of Things' was coined by Kevin Ashton, a British technology pioneer at Procter and Gamble and Massachusetts Institute of Technology (MIT).[1] The immense possibilities and advantages of the IoT are already being realised in the civil and commercial world; and it is expected that in a decade's time or so, IoT would be commonplace enough to 'disappear' into the background of routine things.

The data network infrastructure for IoT could be cable or wireless technology based—for example, Z-wave, Bluetooth, Wi-Fi and cellular frequencies. The IoT has already been put to immense use in effective monitoring and coordination of manufacturing, supply chains, transportation systems, energy management, banking, healthcare, infrastructure automation, security operations and industrial automation, among other sectors and processes. Writing in the *Scientific American* in 2017, Nir Kshetri stated that there were an estimated 8.4 billion Internet-enabled thermostats, cameras, streetlights, printers, wristwatches and other electronics.[2] In supply chain management, even packages and consignments carry embedded chip-level electronics for automatic tracing during transit. In fact, the year 2017 saw a 31 per cent rise in IoT-connected devices from the year before.[3]

IoT is estimated to reach 30 billion connected devices by 2020,[4] and the potential economic impact is likely to be from $3.9 trillion to $11.1 trillion per year by 2025.[5] These numbers vary from article to article and paper to paper, but all of them agree on the exponential rise in IoT connected devices in future. In the future, IoT is to serve as the base technology for all the automation concepts that are being developed world over, like smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Besides remote sensing, reduced human intervention and remote operation, IoT has also brought in advantages of improved efficiency, accuracy and economic benefit. Paul Fraga-Lamas et al. have shown the all-pervasive future proliferation of IoT very well (see Figure 1).[6]

As in the civil domain, militaries too are now getting more and more dependent on computers, networking and Internet technology. Future militaries would depend a lot on smart devices and systems talking to

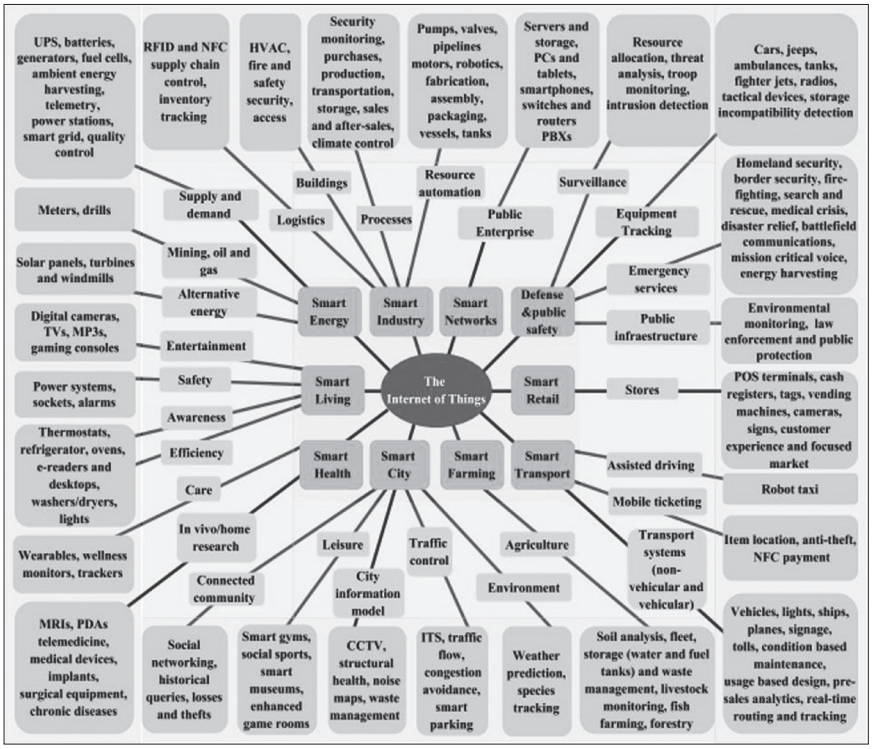

Figure 1 Future Proliferation of the IoT

Source: Paul Fraga-Lamas et al., 'A Review on Internet of Things for Defense and Public Safety', n. 5.

each other and functioning autonomously, also referred to as the 'Internet of Military Things'. Artificial intelligence (AI) and IoT would be the new centricities for military operations. In a previously published paper titled 'Future Warfare and Artificial Intelligence: Visible Path',[7] this author demonstrated the centricity of AI in future warfare; this article is such an attempt to shed light on the centricity of IoT in future military operations.

The next section aims at familiarising the reader with the concept and basic technicalities of IoT. Thereafter, the article looks at how AI and IoT are evolving as complementary technologies, as also highlighting salient vulnerabilities. The network centricity of modern military functioning is portrayed next as well as a discussion on the further evolution to AI and IoT centricity, substantiated with examples of existing functions. The discussion then moves on to the future proliferation of military IoT,

which has been extrapolated with some manifestations, challenges, and trajectories of major world powers, before making an assessment of the future impact of the technology.

Understanding the Technology

In IoT, the connected or networked devices or things that normally function as slaves to a master device, have to either continuously or periodically generate and exchange data with master device, about their state, settings, parameters, sensory inputs, output, etc. The slave devices could be of any type: for example, just sensory devices or object-controlling units. The master device or controller unit queries, receives, analyses, filters, compiles and/or transmits onwards the slave devices' data, or passes any received data or controlling instructions to one or more slave devices connected to it, while coordinating and synchronising their operations where required. In fact, all these processes occur at both the ends, that is, the master device end and slave device end, of the networked devices.

Alerts and warnings are also normally part of information generated, where required, and are provided to humans for intervention or for taking precautions. The master device could be a computer central processing unit (CPU), or a mobile phone or any other customised processing unit, which may be connected through wireless or wired technologies, or may even be remotely located and connected through the Internet. Many of these devices are 'smart' with various levels of AI and are able to coordinate among themselves, serving as masters or slaves as per the requirements of one or more tasks to be performed.

Devices across multiple domains could also be connected to common networks through appropriate protocols, to link up to their complementary devices in other domains. Human control of devices and equipment through the Internet too falls within the ambit of IoT. For customised IoT, virtual, limited home networks for an individual or enterprise could be carved out of the Internet, which connect only few specific devices. In the future, every device is forecasted to be networkable, programmable, trackable and regulated through IoT.[8] Figure 2 depicts the basic principle of IoT and networking of devices for IoT.

In technical terms, some of the critical functions associated with IoT that are important from military IoT point of view are: dynamic service discovery; pervasive computing; and context-aware asset search. Service discovery is the automatic detection of appropriate devices, sensors or

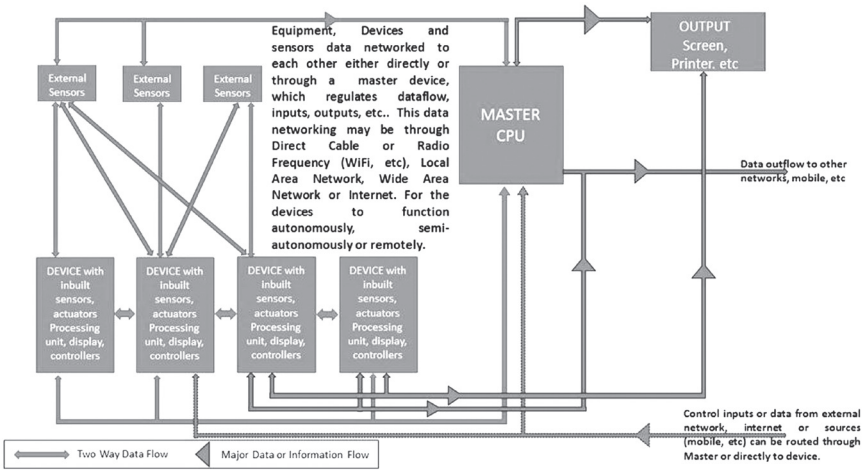

Figure 2 Basic IoT Principle

Source: Author

services offered by various network (or IoT) devices on a computer network to be data linked with, which are needed for executing a particular task or function. Service discovery requires a common language or protocol to allow software agents to make use of one another's services without the need for continuous user intervention.

Pervasive computing is where the computing and data processing takes place to some extent in every connected device and only minimum required data is shared or exchanged over the network. Pervasive computing enables speedier operations. Context-aware search is an intelligent function where the devices or master device would be aware of the purpose for which a device or an asset is being searched over the network, and would make selection of the most suitable asset for the purpose.

Other technological concepts evolving are cloud, cloudlet/fog and edge computing, to increase the processing speed, efficiency, redundancy and security of the IoT. In Fog and Edge computing, the computing takes place at or closer to the periphery of the IoT, rather than in a centralised cloud environment, thereby reducing the requirement of long chain of connectivity, leading to reduced data traffic, speedier operations and reduced chances of disruption of data traffic due to traffic glut or extraneous reasons. Miniaturisation of electronics has provided maximum boost to the IoT concept, where the low volume and

weight advantages have allowed these devices to be fitted at previously unimaginable places. This has also brought about low power requirement to operate the devices. Even 'Internet of nano-things' is now in the field of view and is taking IoT to the next levels.[9]

Complementary AI and IoT

Both AI and IoT are emerging as complementary technologies. Experts have written that IoT shall be functional and useful only with AI, which is how both these are also evolving. At larger scales, where the networks are spread out and intricate and the number of devices is numerous, AI would invariably be required for processing, categorising, fusing and analysing the 'big data' generated. This data would be heterogeneous in nature, generated from various devices and sensors, and for various purposes. As per one article, IoT currently generates more than 2.5 quintillion bytes of data daily with about 9 billion devices connected, which is enough to fill 57.5 billion 32 gigabyte (GB) iPads per day.[10]

Artificial intelligence also enables multidimensional trend assessment in big data environment, which is beyond human capacity. The AI system over IoT would be particularly useful in regulating the operation of devices dynamically by selecting the appropriate devices, analysing their output or transmitted data, regulating their operation to match the conditions and requirements, coordinating and synchronising their actions with other devices, optimally modifying outputs to the environment and other connected assets, realigning goals as necessary, etc. Simultaneous execution of all such operations in a big database environment would be a complex feat. Ajit Jaokar describes the role of AI in IoT as:

> Deep learning algorithms play an important role in IoT analytics. Data from machines is sparse and/or has a temporal element in it. Even when we trust data from a specific device, devices may behave differently at different conditions. Hence, capturing all scenarios for data pre-processing/training stage of an algorithm is difficult. Monitoring sensor data continuously is also cumbersome and expensive. Deep learning algorithms can help to mitigate these risks. Deep Learning algorithms learn on their own allowing the developer to concentrate on better things without worrying about training them.[11]

An interesting corollary to the development of AI and IoT is the development and emergence of 'Ambient Intelligence', which would be a matured electronic environment laden with AI, which evolves when

these technologies have reached some mark and have pervaded into most of the daily use things, maybe in the next decade to decade and a half. In an ambient intelligence world, devices work in concert to support people in carrying out their everyday life activities, tasks and rituals in an easy, natural way, using information and intelligence that is hidden in the network connecting these devices. Being built on an AI and IoT base, Ambient Intelligence would be characterised by pervasive computing, profiling, context awareness and human-centric computer interaction design. A glimpse of it is visible through the present-day mobile phones which are networked and connected, where some of the applications like Google Maps track one's travelling routines and use it to generate best travelling solutions for the person.

Vulnerability of IoT

Another crucial aspect in IoT is the security and protection of the operations and devices connected through IoT. One aspect of this is protection against malevolent intrusion or cyberattacks using malicious software codes to disrupt the cycle of events and damage the connected devices, thereby preventing the task to be performed or having it performed incorrectly. A glaring example of such an attack was the attack by Stuxnet worm, a cyber weapon allegedly developed by the Americans and Israelis,[12] on the Iranian uranium enrichment centrifuges in 2009, which caused the centrifuges to spin faster and continue overspeeding till they were damaged.[13] In another such attack in September 2016, the French telecom provider, OVH, was hit by a distributed denial-of-service (DDoS) attack disrupting telecom services. In one more such incident, half-a-million pacemakers had to be recalled in August 2017 for the fear of hacking.[14]

Attacks could be at micro or macro scales; and at macro scales, these could spell disaster by damaging or putting out of action a large number of critical devices. Even the isolated networks are vulnerable to such attacks where there is a use of flash drives or external memory devices. The Stuxnet attack was on devices which were segregated and isolated from the civil network, where the worm intruded the systems through flash drives. Future IoT, therefore, would need strong security even if it is on insulated networks as the stakes would be high with high cost equipment and devices functioning through IoT.

In IoT, cyberattacks could not only be used for disrupting processes but also for snooping and gathering information unauthorised, for purposes

like industrial spying, etc. Indeed, a lot of the cybersecurity threats over the Internet would be applicable to IoT in one form or the other. Secure IoT is, therefore, of paramount importance. Various features which are likely to enhance security in IoT are segregated network, malware detectors and cleaners, multi-level encryption of data, patchwork and fixes of vulnerabilities in software, use of blockchain technology, etc. In fact, blockchain and IoT are considered to have a synergistic relationship in cybersecurity. Blockchain is an encrypted, distributed computer filing system designed to allow the creation of tamper-proof and real-time records with key based data access, which would bring benefits to the IoT in many ways, from protection against failures and cyberattacks to authentication and increasing reliability of data.[15]

Network Centricity in Modern Military Functioning

Modern militaries have considerable dependence on the electronic networks, both data and communication, for many of their functions. These networks are fast evolving to become the cornerstones of military functioning, and include both operational as well as sustenance functions. Networkcentric concepts of military include operational networks, logistical networks, administrative networks, etc., which primarily focus on information exchange for various needs of the military, like building situational awareness, operational and routine communication, logistical management, imagery transmission and administration. Figure 3 shows a notional depiction of a operational network grid with its various information exchanging entities and data/communication linkages.

Admiral William Owens of the United States (US) Navy called military networks as 'system of systems' in a paper published in 1996.[16] What he referred to was networking of intelligence sensors, command and control systems and precision weapons, all of which enabled enhanced situational awareness, rapid target assessment and distributed weapon assignment. Volumes have already been written about network centric warfare (NCW), a concept that recognises electronic networks hub of warfare and which not only includes the military networks but encompasses even the civil domain networks.

Architecture-wise military networks are kept isolated from the civil networks by having their own separate cables, nodes, transmitters and terminals for protection of data and information. Also, there is often an air gap maintained with the civil network as far as the terminal and cable layouts are concerned for reducing possibilities of data leak. Within the

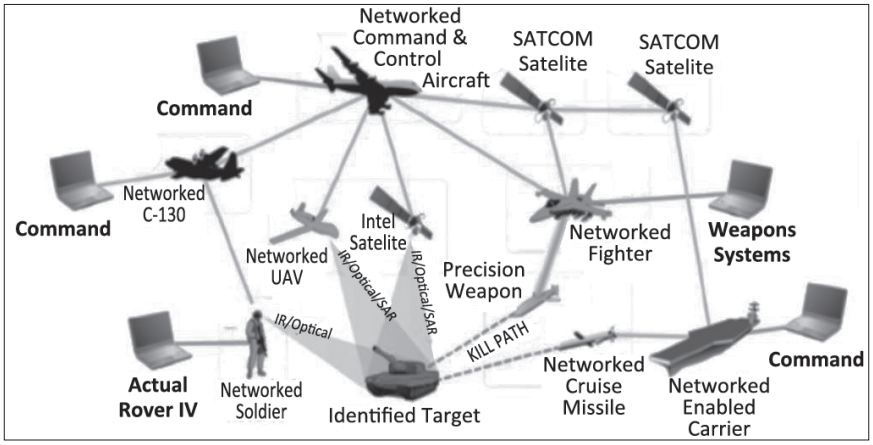

Figure 3 Notional Depiction of Battlespace Network Highlighting the Crucial Links

Source: Adapted from Scalable Network Technologies Inc., 'Software Virtual Networks Integrate Training and Operation of Wireless Net-centric Warfare Systems', *Aerospace and Defence Technology*, 1 October 2008 available at https://www.aerodefensetech.com/component/content/article/adt/tech-briefs/information-sciences/4922, accessed on 4 May 2018.

military networks, various virtual departmental networks are generally carved out, that is, from the common hardware or electromagnetic (EM) spectrum. Almost as a rule, militaries isolate their sensitive networks form other military networks too: for example, operational networks are generally kept detached from logistical and administrative networks involving altogether different set of cabling and hardware to prevent any kind of intrusion or hostile attempts on these. These have redundancies and alternative routings in case of cable or node failures. Software packages and operating systems are customised for military requirements and there is almost always an overlay of encryption on the data communication flowing through these networks.

Modern-day cable networks, in most militaries, are now fibre optic due to high bandwidth and speed requirements. However, field connectivity is generally based on wire or EM spectrum to enable quicker mobilisations and remote connectivity, and also due to difficulties associated with handling bulky and weighty fibre optic cables in field environment. The information linking through data has now reached almost all field-level entities in the advanced militaries, using mediums from satellites to aircraft—such as Airborne Warning And Control System (AWACS)

and Joint Surveillance And Target Attack Radar System (JSTARS)—Unmanned Aerial Vehicles (UAVs), tower-based systems, and so on. The US has also standardised certain such EM data links (with certain communication characteristics) and established nomenclature, such as Link 16 and Link 22. However, the element of IoT is mostly limited to device synchronisation for information and data exchange, though it is increasing incrementally towards envisioned autonomous operations.

The critical role of military data networks was realised during the First Gulf War 1990-91, when networking and information in battlespace led to full-spectrum dominance for the US-led coalition forces over Iraq. The phrase 'full-spectrum dominance' was coined in 1996 by the US Joint Chiefs of Staff, and implies a military entity's achievement of control over all dimensions of the battlespace.[17] Data networking with the coalition forces enabled real-time situation monitoring, including ballistic missile launches, enhanced command and control function, effective and reliable communication, quicker response, shortening of the observe–orient–decide–act (OODA) cycle and radical improvement in other crucial war functions, like information distribution, logistics and mobilisation. An AI-based networked logistics system called Dynamic Analysis and Replanning Tool (DART), which was first IoT concept for military logistics function, was first tried in 1991 during the Gulf War and, as claimed by the Defense Advanced Research Projects Agency (DARPA), it more than paid back its investment.[18] By 2005, the US Department of Defense (DoD) had also established a Global Information Grid (GIG), which networked its warfighters, policymakers and support services globally.[19]

Increased hybridisation of warfare has complicated the matters as the earlier peripheral elements in warfighting have started sharing centre space, and warfighting has expanded into multiple dimensions, like cyberwarfare, information warfare, sub-conventional warfare and others. This has diversified military operations into unconventional regimes of anti-terrorist operations, information dominance, etc., and increased the dependence of militaries on networking for operations further. This dependence is reaching a level where disruption of networks could be catastrophic for military operations.

From Network Centricity to IoT and AI Centricity

The military's dependence on data networking is bound to only increase in the future as their reliance on technologies also increases. Generally,

Figure 4 Notional Depiction of Weapons Grid IoT in Battlespace

Source: Adapted from Alexander Kott, Ananthram Swami, and Bruce J. West, 'The Internet of Battle Things', Cornell University, 2016, available at https://arxiv.org/ftp/arxiv/papers/1712/1712.08980.pdf, accessed on 14 May 2018.

with speeding up of things brought in by the technology, militaries now have shorter time frames available to them for assessing situations, taking decisions, executing tasks, reacting to developments in battlespace, etc. Undoubtedly, this speeding up also calls for optimising logistics and administration, besides the operational activities. With such requirements, more and more military equipment and devices would be networked in future. In future, even things like weapons, transportation platforms, logistical packages and ordnance consignments would be connected to military networks, all having electronics embedded in them, generating and exchanging data, and being controlled and regulated more and more without human intervention, using classical IoT concepts, as covered earlier, like master and slave, dynamic service discovery and pervasive computing. Figure 4 is a notional depiction of such a weapons grid IoT in battlespace.

The number of devices are, in fact, far too many to be depicted in one single diagram. Tapestry Solutions, a Boeing company, mentions on

its website: 'IoT devices can gather more data, facilitate more complex analysis and faster reactions, and reduce human error, delivering more precise and efficient military capabilities, according to a CSIS report, "Leveraging the Internet for a More Efficient and Effective Military".'[20]

Artificial intelligence in the network environment as well as in devices is likely to be one of the core controlling elements of military IoT, performing tasks for military on similar principles as in civil domain. With such pervasion, military functioning and operations in about a decade or so could be termed 'IoT and AI centric', rather than just 'network centric' as is the concept today. Here, the IoT and AI centricity would imply a huge degree of autonomy in the functioning of the connected devices and systems and minimal human intervention towards any task performance.

Some Existing Functions

In the present day too, all the data and information exchange taking place between networked devices can be placed within the regime of IoT to a certain extent, since the devices are synchronysing and coordinating with each other for data exchange; however, the autonomy content, viewed collectively, is yet nascent. Such IoT usage can already be found in almost all the armed forces to some limited extent. Missile or aerial attack threat warnings and alerts are often automatically generated based on the perception of the computer of an air defence system. Terminal air defence systems of the military are usually activated, aimed and triggered by computer systems over networks because, more often than not, an air attack situation develops so fast that humans cannot effectively react to it.

Drones devices too work, to some extent, on the IoT concept for navigation and information transmission, processing and relaying of data; though there are often humans-in-the-loop at crucial places controlling these devices. Automatic intelligence, surveillance and reconnaissance (ISR) and weather monitoring devices in remote and difficult-to-access areas are increasingly becoming common. Security systems based on facial, or iris, or fingerprint or radio-frequency identification (RFID) recognition at military bases and sensitive places are increasingly being employed, with the latest advancement being gait recognition biometrics.[21] The US and other militaries have started employing the technology for many other functions which are covered later in the article.

Electronic warfare (EW) systems also function on the IoT principle,

where the sensors networked to electronic jammers, or flare launchers, automatically trigger these electronic countermeasures on receipt and identification of radar signal. Missile guidance of semi-automatic homing air-to-air missiles is an example of a limited IoT, where the aircraft radar tracks and guides the missiles onto the target automatically.

Military fighter aircraft can increasingly cue each other's systems through data links for target designation while on missions. They can also exchange information or downlink radar, weapon usage and other such data to the mission control rooms for automatic air situation build-up. Telemetered data from the aircraft is mostly used for mission analysis in training establishments. The AN/SPY radar system of the US Army can detect, track and steer guided munitions into as many as 100 targets at a time, entirely autonomously.[22] Another prime example is the Tomahawk Land Attack Missile (TLAM), the US Navy's premier precision strike weapon. The TLAM Block IV variant has a two-way satellite link that allows the missile to be redirected in flight to a new target, or to loiter over a target area, sending footage from its onboard camera to commanders, thereby allowing them to designate new targets as well as assess damage from other strikes.[23]

The IoT-related technology is also being used for military training and simulation. For example, live training 'shoot houses' use cameras, motion sensors and acoustic sensors to track soldiers during training exercises, sending data to mobile devices for trainers who can coach soldiers in real time. Another example is the multiple integrated laser engagement system (MILES), which simulates live infantry combat using blank cartridges and lasers. Similar to laser tag games popular with kids, lasers mounted on weapons send coded signals simulating bullet and when the sensors mounted on a soldier's clothing and equipment receive the laser, they register a hit.[24] These kinds of micro-level or limited IoT applications, where one device is data connected to another to trigger, or monitor or control its operation in military, in fact, are many. Advanced militaries such as the US have also started to employ IoT in some other functions, which are discussed later in the article.

Future Macro-Level Military IoT

In future, IoT at macro and micro scales, or functioning over the wide military networks, is what is envisaged to be the cornerstone of military functioning. Contemporary and future battlespace environments, shaped by advanced technology, call for integrated approach to warfighting by

all the forces, that is, surface, air and maritime forces, though the extent of their participation would depend on the nature of battlespace, whether it is over land, over sea or both, and the nature of operation. Currently, outer space too is within the span of battlespace as space-based assets now play a significant role in communication and imaging and are, therefore, very much in the ambit of being targeted.

Future warfare is also going to be multi-domain, which essentially implies expansion of battlespace. Numerous articles and papers have appeared in the last few years on how the warfare is evolving into multi-domain warfare, where elements of different domains would be simultaneously engaged in prosecution of war. A US Army Training and Doctrine Command document defines the multi-domain battle operational framework as one that includes all domains, spanning to include space and cyberspace, as well as the EM spectrum and information environment.[25] This nature of the battlespace also points towards future centricity of data networking in warfare, where it would serve as the nervous system of military operations. A blog of the US Army Training and Doctrine Command mentions General Mark Milley, Chief of Staff of the Army, ordering creation of an experimental combat unit known as the Multi-Domain Task Force of the US Army in 2016, equipped with futuristic technology weapons and equipment, including robotics, to study its effectiveness and survivability in future battle environments.[26]

Broadly, the macro-level IoT for the military in future would be established on the similar lines as in the civil domain, but with differences in the software, connected devices and systems, linkages and frequencies, etc. They are likely to be following similar principles of cloud, cloudlet, fog, edge and pervasive computing, dynamic service discovery, and contextual search, as the IoT pervasion, data generation and traffic and processing power increases. These would be segregated from the civil networks and some of the sensitive operational networks would be isolated and insulated from even other friendly military networks.

The military IoT would also need to follow some exclusive software layer and encryption protocols specifically for military, over and above the data-sharing protocols, for data and communication security, which are as such followed in sensitive and classified communications in militaries and are akin to encryption protocols followed by the bank servers. This would be primarily to prevent breaches and intrusions into the IoT networks. While speaking on an IoT-based ballistic missile defence system, J.D. Hammond, Director of Operational Command

and Control, Lockheed Martin, observed: 'It takes data from hundreds of sensors, radars and satellites and translates that data into a common language for the missile defense systems to interact and engage the threat.'[27]

The IoT is likely to be used either keeping human-in-the-loop or human-on-the-loop during future military conflicts in weapons utilisation, especially where lethal autonomous weapon systems (LAWS) and other autonomous robotic machines are also pitched in combat. An example of human-in-the-loop through IoT is the offensive missions flown by the Predator unmanned combat aerial vehicle (UCAV) in the operations against terrorists in Afghanistan, where most of the mission is executed by the Predator autonomously, except for launch of the missile, which is remotely triggered by the human operator who is mission-in-charge and may be sitting hundreds of miles away but is connected to the UCAV through a radio wave data network through a satellite or another relay UAV, thus keeping human-in-the loop. In cases where the UCAV would take a decision autonomously to launch the weapon after ascertaining the right target, but such launch could be vetoed by the human mission-in-charge remotely, will be the human-on-the-loop.

Networking and computerisation have a major role to play in integration of forces in battlespaces and, in fact, networking would be the key element enabling integration of warfare in future. Interoperability would be enabled by systems operating on common networking protocols and, at places, sharing the data hardware too. The criticality of networking and NCW invariably forms a part of generally all modern military doctrines. Future networking for integrated operations would require common or shared networking between the forces even in the battlespaces, which invariably would continue to happen.[28]

The future battlespace would be dominated by autonomous equipment and combat systems, including robotic drones, tanks, guns, mine-laying vehicles, sea vessels, EW equipment, etc., and support systems comprising radars, lasers, sonic sensors and imagery systems. These unmanned systems would be key components of integrated operations. The vital enabler and a necessity for coherent and coordinated operation of these battlespace assets would be IoT in the battlespace.

In future conflict scenarios, for coordination and synchronised action, all combat and non-combat entities in the battlespace would be generating and exchanging data on their state, serviceability status, position, sensor inputs, etc., over the IoT with central computers and

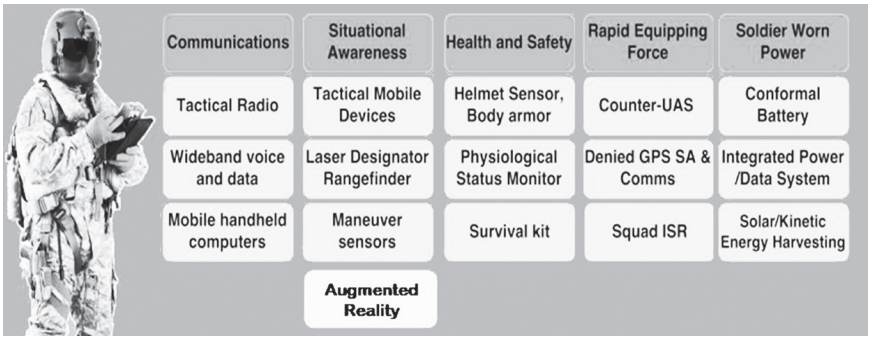

Figure 5 Future Networked Soldier

Source: Adapted from Paul Fraga-Lamas et al., 'A Review on Internet of Things for Defense and Public Safety', n. 5.

monitoring systems and with other battlespace entities. As a result, there would be an enormous increase in automatic data generation and traffic over these military networks, making direct human control of assets practically impossible; and without the assets being controlled automatically and functioning concertedly, the success of operations would be very difficult.

The Networked Soldier

Soldiers and manned equipment/vehicular platforms would be data linked for communication, control and information exchange, which would be automatic as well as manual. The soldiers would not only be networked for communication, position and logistics/weapon state, but also the future technology would enable a soldier to be wired with sensors to automatically monitor his vital medical and health markers, and take a decision when a soldier needs rest or replacement, what is the state of health of a battalion, when will their biorhythm be at peak to plan any activity (such as an offensive) and so on. Augmented reality to increase soldier's awareness would be again an IoT function. He could digitally call for artillery and air support using just a handheld device pointing at the target, where the rest of the needed information would be automatically sensed and uploaded on IoT. Western armies are already using similar devices.[29] Figure 5 depicts such a future soldier.

In future aerial missions, manned and unmanned aircraft could be flying in formations, linked and coordinated through IoT. Such experiments are already underway. These would actually lead to the expensive manned or unmanned military systems being replaced by the

cheaper autonomous systems. The IoT would be the base technology for drone swarming, which is likely to be a key weapon for future warfare in most of the scenarios like deserts, jungles and urban areas. Pairing of ISR devices to specific missions through IoT in insurgent or insurgent-infested areas is likely to become an effective tool for the military for countering the menace.

Artificial intelligence and IoT-integrated battlespace environment technology will enable maintaining real-time situational awareness and scenario building during military campaigns, especially where there are fast-changing scenarios, shorter response times available, large number of entities in the battlespace, and huge data traffic. This would also enable the commanders and higher echelons to see an integrated battle picture as well as specific sectors, along with ambient elements such as weather and presence of chemicals, and enable them to focus on more critical areas and visualise scenarios more realistically using virtual reality in 3D.

Lethal Autonomous Weapon Systems (LAWS)

Integrating the combat systems also brings in the aspect of autonomy of the lethal combat systems or LAWS powered by AI, which would be one major aspect of military IoT. It is envisaged by the experts that in spite of the intense debate surrounding LAWS and opposition from a major faction of scientists and defence architects, the offensive LAWS would eventually find a place in the military operations. A recent statement by Robert O. Work, the 32nd US Defense Secretary, on the Third Offset Strategy of the US,[30] and China's change in position in 2016 on autonomous weapon systems, from emphasising on human-in-the- loop to responsible use of LAWS[31] more or less confirm the future induction of LAWS into militaries.

Weapon systems like autonomous drone swarms being developed by the US, China and Russia, which fall under the purview of LAWS, also corroborate the fact.[32] As such, the reduction in response time and shortening of the OODA cycle that the LAWS would bring in would be an inescapable necessity to retain the combat edge over military adversaries. Other advantages like reduction in own casualties and avoidance of exposing forces to increasingly lethal battlespaces would also be reasons for the militaries to opt for development and deployment of LAWS. These, in turn, would bring in much-required asymmetry in the military might vis-à-vis the adversary, a key ingredient for military victory. For such use and effectiveness, LAWS would be working on IoT

for synchronised fire and manoeuvre. All these aspects are increasing the relevance of IoT and are indicative of the fact that battlespaces would see almost complete IoT-based operations in one-and-a-half to two decades.

An integrated approach to warfare implies complementarily integrating the warfare resources of all available forces for their optimal utilization to achieve war objectives. This approach also signifies interoperability of warfare means of all the forces. Interoperability means the utilisability and use of one force's assets and warfighting resources by other forces, including tasking, controlling and operation of equipment or platform. Interoperability of warfare means has been kept as an important element in the modern doctrines of the armed forces, though integration of forces is yet to materialise for most of the militaries in its true sense. Also, some forces still keep interoperability concept limited in scope and restricted to a few aspects of military activities in their doctrines. Even the civil resources are included in the concept as far as integration is concerned.

Combat systems in battlespaces are one facet of military requirements. As covered earlier, interrelated with the integrated and speedier warfare, there will also be a requirement of well-coordinated and optimised battlespace support functions like logistics and transportation, which again would be IoT based. In the time frame of one-and-a-half to two decades, there would be a prevalence of AI as a design feature in most of the military systems. It would be an enabler for autonomous operation of the systems, also bringing in seamless functionality of heterogeneous military systems operating in different domains through IoT.

Military Operations Other than War (MOOTW)

MOOTW are non-combat military operations and mainly comprise humanitarian assistance and disaster relief (HADR) and peacekeeping. In both, the IoT devices would find immense employability. Multiple autonomous drones, linked to rear base camps, could be launched to identify the places where help like rescue or supply of food is required, and then pinpointed rescue or relief supply effort could be launched, reducing the wasted missions. Also, exposure to danger could be reduced for the rescue party. Similar would be advantages in HADR in contaminated zones. Similarly, in peacekeeping operations, IoT devices patrolling disturbed areas would provide a safer and more effective option.

The IoT military systems, both combat and non-combat, coupled with other advanced technologies like AI will also bring about downsizing

of the forces since most of the tasks and duties shall be automatically executed by the systems exchanging information and data over the IoT. When soldiers are replaced by robotic machines in battlespaces, the costs of maintaining militaries would reduce as: first, the costs of designing the autonomous systems are reducing rapidly so these systems are envisaged to be cheaper in future; and second, the maintenance costs of a fleet of machines would be lower than maintenance costs of personnel due to lower recurring costs like pay, kitting, healthcare and retirement benefits, making these preferable for both militaries and governments. A recent example is China which has announced a downsizing of the People's Liberation Army (PLA) to below 1 million, where the vacuum created would be filled by high-end military systems.[33] Others too may start following suit in the years to come.

Challenges

Connectivity in Battlespaces

The IoT in military would have its challenges though, some of them similar as for the civil IoT and some unique in nature arising out of the military and battlespace environment. As discussed earlier, in military IoT, the field or end-point connectivity would be mostly through radio waves on which data could be superimposed. With high data flow rate required for IoT to function, the radio wave spectrum would have to be from ultra-high frequency (300 kilohertz–3 gigahertz) or super-high frequency (3–30 gigahertz) and millimetric waves (30–300 gigahertz), which would restrict the radio wave propagation to line of sight, and obstacles in the battlespace like hillocks, dunes and mountains would prevent the propagation of these waves. Maintaining IoT connectivity would thus require considerable effort. The silver lining to this issue is that these frequency bands are already in use for military equipment and satellite communication. Millimetric waves, to some extent, can enable high data rates, but suffer from atmospheric attenuation and weather degradation (rain, humidity, etc.), which in battlespace environments could become a serious shortcoming.

Use of satellites, drones, balloons and additional relay equipment may provide connectivity to some shadow areas but these would increase the costs and efforts. Some of the IoT vehicles, systems and weapons could themselves be designed as relays too, and enable connectivity to the devices which may be out of range or in shadow areas. The systems

would have to cater for multiple redundancies to cater for failures as well as have multiple channel connectivity, for a single channel of connectivity may be insufficient for a dynamic and EW-dominated situation of battlespaces.

High bandwidth data transmission would have to be built into all the back-up transmission means for high rate of data transmission and glitch-free operations, especially where there is data traffic convergence. Data hygiene and data validation in such an environment would be significant challenges. The IoT connectivity to undersea vehicles will be difficult, which will have a short range when submerged, due to propagation characteristics of the radio waves. With convergences brought about by a large number of connected machines and smart mobile devices at the nodal points, there will also be an increasing demand for network capacity over the limited EM spectrum available to support these data-hungry devices, and providing the same in the battlespace environment would be another challenge. The system would also have to have an AI-based data optimisation for best results where the data traffic is restricted or limited due to bandwidth limitations, which may often be encountered in a dynamic war scenario.

Powering Devices

For IoT operations, a number of devices are likely to be battery powered, while a fewer would be fuel powered. Wearable batteries could be mechanical movement recharged or thermally recharged. Providing power to robotic entities needing long-duration independent sustenance in the battlespace would be an issue. A reliable solution does not exist as of now. Power optimisation, low power design for long-duration operations as well as battery weight reduction are the areas that need research focus, and much is underway already. Power supply would especially be a critical issue in remote and difficult regions, and also in a variety of weather conditions, for example, in very low temperature conditions which reduce battery life. While solar or wind power is an option, these would be subject to constraints of weather and other factors. Recharging or replacing the batteries in a battlespace environment will need serious consideration.

Design

Additional challenges would transpire from the hostile and destructive military action that these systems have to be designed to face. Military

systems have to be designed catering for battlefield ruggedness, high stress, rough usage, weather and environment proofing and water proofing, and also have to have robust fail-safe mechanisms. They follow the military standards generally referred to as 'Mil Standard' which loosely indicates a tougher build. As compared to the civil domain, this kind of designing involves more rigorous testing and much stricter performance guarantees, which not only takes more time to ensure but also increases the time lag for the product to come out. For example, the US DoD specifies Mil-Standard-1678 as a general standard for fibre optic cables on military mobile vehicles used in air, land and sea applications for data transmission.[34]

For effective operations in military environment and battlespaces, military standards design would be looked at for all IoT devices and components, like nodes, relay sets, transmitters, cables and power packs, which would incur higher costs. Commercial off-the shelf (COTS) components for military systems, however, are being recommended by many for use to contain the costs and ensure easy replaceability, but these may not be fit for all the places, especially in battlespace environments. The use of COTS components shall therefore vary from system to system and place to place. For very low-cost devices like self-sacrificial drones, the cheaper costs may outweigh ruggedness.

Standardisation

IoT will call for certain standardisation of design features of the combat and non-combat data systems and protocols so that these can successfully exchange data with heterogeneous systems present on the network and be able to synchronise with other systems in varying battlespace environments. Allocating Mac addresses or similar identification addresses to each and every entity in the network is a simple example. Using databases of multiple heterogeneous devices and their synchronisation (with different functioning attributes of different devices) for optimal functioning, fault or malfunction identification, generating alternative courses of action, would be a humongous challenge associated with the military IoT.

Though cloud design has some heterogeneity accommodation incorporated, it would still require a powerful AI support for rapid processing. It is likely to pose major difficulty for militaries which rely on import of weapons and equipment for defence use due to differences in software of these systems. A recent article mentions: '…the DoD

continues to struggle with interoperability. While the military has deployed a wide range of IoT-related technologies, many are developed in segregated "stovepipes" which makes it difficult to communicate across other systems.'[35] Creating tactics for employing such IoT-based systems would be another challenge by itself, catering for multiple contingencies like systems being put out of action during battle or component failures of systems.

EW and Cyber Threat Environment

Future military conflicts are likely to take place in a dense EW and cyberwarfare environment. Military devices connected to and functioning through the IoT would also be vulnerable to these attacks and their functioning could be degraded so as to thwart missions. Large number of links to establish would also provide multiple intrusion points for attacks. All kinds of EM transmissions are giveaways of devices' position, which makes them vulnerable to hostile actions, besides allowing the enemy to judge the deployments.

Use of directional beams, laser transmission, etc., along with security techniques, like low probability of intercept (LPOI) transmission and burst transmissions, will have to be developed for use in battlespaces for IoT too. Electronic jamming and spoofing of signals could be a major problem, preventing functioning of systems or exchange of data feed. An example was Russians thwarting a drone swarm attack on their airbase in Syria on 5 January 2018 using missiles as well as EW means.[36]

There is a possibility of improperly secured IoT data traffic being tapped by an adversary to glean sensitive information or identify tactics. Pascal Geenens, Europe, Middle East and Africa region security evangelist at Radware, says:

> Military branches have long been heavy technology users. They have also had a technology procurement model based on an outdated approach and xenophobic buying behavior…Seemingly innocuous cameras, sensors and other IoT devices pervade the military, but are just as rife with security issues as any on the planet. Once demonstrable vulnerabilities are validated, how much would a government pay to regain control of weapons or other crucial resources?[37]

Reducing vulnerability of EW systems, which in future battlespaces could be in large numbers, would probably be one of the big challenges for IoT-based military operations. The IoT devices will have to have

the redundancies, countermeasures and counter-countermeasures for such attacks.

There is also a risk of intrusion or degrading of the function of devices and weapons linked through IoT by bug implanting or tampering of circuits, as only few of the nations like the US and China have the integrated circuits (chips) fabrication (manufacture) facility, who may design circuits to 'bug' or trapdoor the hardware and software for backdoor entry for interfering with the devices functioning. Military devices being imported or designed based on imported chips or circuits are rather vulnerable. Though certification is generally taken from the vendor to that effect, these are almost impossible to catch as the circuits or the line replacement units are provided in sealed condition and the importers generally have no understanding of the circuitry inside.

Threats from non-nuclear electromagnetic pulse (NNEMP) weapons would be a considerable worry as it could render a large number of connected systems and weapons temporarily unusable or permanently damaged, degrading the combat capability drastically. Not just the combat systems but also the support IoT networks, such as logistics, could be affected so as to impede the missions. Though fibre optic cables provide protection against EM pulse, in the battlespaces, EM pulse would technically be very difficult to counter as any kind of exposed metallic part of circuit or wires makes the devices vulnerable to EM pulse damage despite protective measures like caging.

Conventional Aspect

The possibility of network disruption also calls for conventional warfighting capability to be retained by the militaries, putting intense pressure on them to expand their arena into multiple domain technology-intensive battlespace environment, while furthering their conventional fighting capability too. Since military budgets are limited and so is human technical capability, it would require some extraordinary brain-wracking to find a solution to this future issue of training the military men, and of balancing the conventional and robotic warfighting capabilities. Negotiating ethical aspects of using autonomous weapon systems in combat, which is already coming under much debate and criticism, would be another challenge.

Since there are likely to be regular evolutions with newer concepts of connectivity, software and application layering and data-sharing protocols in IoT taking place quite frequently in future, which may at

times require additional hardware and face software compatibility issues, upgrading a vast number of devices, weapons, platforms, etc., held with the military to newer system and protocols will be a further challenge. Garnering funds for such changes would be equally challenging for most militaries too. There will also be requirement for a plan for backport hardware support to older versions of the operating system, as well as a plan for regular software updates for the devices to function smoothly and seamlessly. Though the AI based would be a self-healing IoT network, troubleshooting and fault handling or repair in remote and battlespace environment would be other crucial issues that would need to be catered for. This can be quite challenging in military environments, but needs to be part of the overall strategy.

Reading the Present Trajectories

United States

Internet and the idea of IoT have emanated from the US, which has been using the IoT concept in myriad forms for various military requirements for quite some time. Presently, the Americans are also in the forefront in the development of IoT for military. The US has used networked sensors since the Cold War era for monitoring nuclear missile launch threat, including satellite-based sensors that generate alerts automatically. They were also the first to demonstrate to the world the centricity of modern military power on the data and information networks during Operation Desert Storm in 1991. The US DoD's current approach to maintaining asymmetry in military might against other major powers is centered on the Third Offset Strategy, which hovers around advancing the military technologies based on AI and IoT.

DARPA is, in fact, working on an AI-based autonomous offensive system called Collaborative Operations in Denied Environment (CODE), where multiple drones would carry out entire missions on their own by assessing environments and situations in real time, often engaging targets on their own.[38] The US Army is working with defence contractors to help it integrate and use IoT solutions in daily operations. Lockheed Martin, for instance, is providing assistance on using machine learning to automate decision-making.[39]

The US Air Force (USAF) conducted a design project in April 2017 on turning the USAF bases into smart bases through IoT. The report of the study group envisages every activity at the air force bases, from

personal to official to operational, to be regulated automatically through IoT. It envisages extensive use of networked static sensors (like security camera or acoustic) and mobile smart devices (like perimeter security drones), or personal gadgets like mobile phones to wearable devices like smart watches, at the air force bases, enabling monitoring of activities to distribution of information.[40] The US apparently has a classified communication network line spanning 48,000 miles, which is being used in missile defence and battle coordination scenarios,[41] signifying the US venture into IoT. The logistics agency is also using IoT-based RFID for trans-shipment of goods and telemetry on the aircraft for monitoring the fuel requirements of bases.[42] The US military is already using the RFID tags for tracking shipments.

Writing in the *Internet of Business*, Nicholas Fearn mentions USAF's efforts in deploying IoT for maintenance of fighter jets, where the internal sensors would automatically communicate to the logistics support systems the maintenance requirements and right spares and equipment can be made available at right time saving time and costs.[43] According to Gopal Singh, writing in the *International Journal of Scientific Research Engineering & Technology*, the DoD has been using IoT concepts in improving their warfare systems.[44] SEAWEB is another IoT-based application for the US Navy. It is composed of persistent nodes, anchored to the ocean floor and floating at various depths for the purpose of collecting and identifying underwater acoustic signals (for example, submarine). Once a node is triggered, collected data is exfiltrated to floating devices for further transmission.[45]

China

China's military modernisation trajectory is similar to that of the US. It has not only established an elaborate, countrywide fiber optic network, but is also expanding the civil connectivity to its neighbours. It is also a hub of computer hardware, including the fabrication of integrated circuits for computers, which gives it a distinct advantage of self-reliance in developing computer-based systems. Anhui Sinonet and Xonglong Science and Technology Co. Ltd., designs, produces and markets networking equipment, security sensors, integrated systems and automatic control products throughout China. In June 2017, the Chinese military listed Beijing Sinonet Science and Technology Co., a subsidiary of Anhui Sinonet, as contractor for IoT project, with an aim to establish an IoT control network and information service platform

for military supplies and fuel oil for the country's new war zone combat system.[46]

In March 2018, an IoT-based omni-surveillance system called Sharp Eyes was commissioned in 50 cities (and is going to be installed in all of China). It has facial recognition and vehicle number plate reading features and can identify the blacklisted personnel and vehicles in a normal city crowd by instantly comparing them with existing database and alert the security personnel.[47] By some estimates, there will be about 200 billion connected devices by 2020 in the world, and 95 per cent of those devices will be manufactured in China.[48] Little is available otherwise on China's military IoT in open source. China's advancements in development of autonomous UAVs, including drone swarms and other robotic weapons and equipment, are all broadly on similar lines to that of the US, and drawing the parallels, their trajectory of developing IoT-based military capability can be visualised to be similar. China has also created a PLA Strategic Support Force, with one of the main aims being to undertake operations in the cyber, EW and space regimes, which will be based on an IoT foundation.

Others

Most of the significant world powers have a similar vision of the future evolution of militaries and warfare, and their programmes are on similar trajectories. Information available in the open domain through news reports, articles and papers reveals that almost all these nations are pursuing development of advanced and intelligent weaponry, with data linking and network centricity as focal functional concept. Concepts of integration and interoperability, though much emphasised, are at present nascent with most militaries in practicality; however, there is increasing effort for these to be corporealised due to evolving multi-domain battlespaces, which in future, as is very well realised, will need multidimensional action. Similar developments keep coming to light towards having command and control structures, battlespace monitoring set-ups, logistical supply chains and other real-time functions for sustaining integration and interoperability. These are again being developed with AI and network centricity. Border security systems of countries like Israel and South Korea, which are IoT and AI based, are already functional. Networking is now an ongoing process in the modern military set-ups and most of the militaries have fairly matured local area and wide area network connectivity for routine work. IoT applications

are still very limited in nature for most functions of the militaries but are evolving.

An Assessment

IoT is increasingly becoming a commonplace technology in the civil world where it has started to optimise and streamline things. It is forecasted to proliferate in every sector, in about a decade to decade-and-a-half's time, to an extent where almost every main gadget shall be functioning through IoT. It would probably not even be realised as 'existing' by common users, but would disappear as a background facility, like electricity in present times.

As covered earlier, conceptual change in military operations network centricity has taken primacy since the 1991 Gulf War, though the concept of IoT was extremely limited then by modern standards. Even then, the IoT-based application, DART, is considered to have more than paid off in optimising the logistic coordination of the coalition forces. Network centricity has now become the mantra of successful military operations. Presently, conventional wars are considered unlikely in the face of nuclear overhang. Military operations now, and in future, are likely to be short, precise, integrated, limited objective guided and effect based, with short OODA cycles, due to multidimensional, unrestricted and hybrid character imparted to conflicts by the advancing technology.

We have seen in the narrative how in the future battlespaces, use of robotic systems and intelligent weapons linked and controlled through military IoT would underwrite the success of military operations, specially in the places where the risk or lethality is high. Going forward, IoT would be the foundation for integration of multidimensional forces and resources in military operations and it would be equally applicable to offence and defence. The Space component would also be crucial in providing data linking and redundancy for IoT. Artificial intelligence would be one of the key ingredients of the military systems and weapons, whether these are surface, aerial or underwater systems. Cost-effective AI technology, like drone swarms, would find high employment in the operations for bringing in efficiency and out-of-proportion results vis-à-vis the costs. These systems and weapons would invariably be integrated through IoT.

Prevailing technologies, software and networking concepts, data generation and sharing protocols, and the security concepts which are in use or being developed for IoT in civil domain, would form

the framework or basis for the military IoT too, though the military domain IoT would have some of its own peculiarities and challenges. Frequent software and hardware upgradations or add-ons due to newer technologies, often leading to major changes software modules as well as equipment utilisation concept, and early obsolescence and replacements of weapons and equipment, is likely to be the future order. Organisations such as militaries need time to adapt to technological changes due to their multifarious manifestations and frequent changes may pose some operose challenges.

Success in future military operations would depend a lot on how effectively the IoT-based systems are employed and how well these function. Cyberattacks and EW/NNEMP weapons could wipe away the advantages in one go in the battlespaces. There are, however, constraints in employing weapons like NNEMP as these could considerably damage own systems also. Dependence on these weapons would bring considerable uncertainty and unpredictability to warfare and would make deployment of forces quite complicated. These challenges would put immense pressure on the military commanders and higher echelons. Thus, militaries would have to be proficient in using advanced systems and weapons on the one hand, and they would not be able to shed their conventional warfighting skills on the other.

However, skilling the soldiers in technology may not be very difficult a proposition as with sophisticated civil technology becoming commonplace, the technological awareness of the personnel is much better, and the younger generation is really not discomfited by new technology. Besides, in future, the technically qualified are only likely to be selected for soldiering. Developing and adopting new tactics involving the connected devices would be a difficult task for the forces, which may see frequent changes with rapidly emerging newer devices and systems.

The world's major powers—the US, China and Russia—have officially acknowledged the role of AI in future military operations and have charted road maps for development of AI-powered warfare systems, including LAWS. The US is leading in the research on advanced AI systems, but China and Russia are also not too far behind. European nations, Israel, South Korea and a few others have also made substantial progress in the field. Other powers like India and South Africa are following suit. Military IoT is being developed on an equal footing as AI by the powers so as to realise the full advantages of the AI. Their forces are heading towards more integrated approaches to warfare and military

operations, where IoT will have a key role. There are teething problems of bringing together heterogeneous IoT devices presently, which even the US is facing; however, as data-sharing protocols are maturing, these would evolve over time for easy integration and coherent functioning of the devices.

Future coalitions of forces, as the Western powers are quite often seen to do, would be more readily effected by IoT. But, it would be a challenge as it would require sharing protocols and information of IoT devices, which would amount to compromising the systems, which even the friendly forces may not be comfortable with. Probably adding another layer of shell protocols in data sharing in such cases where data access between various networks is regulated would be an answer. Current agreements on communication and data sharing, like Communication Interoperability and Security Memorandum of Agreement (CISMOA)—a legal framework of the US that enables the transfer of critical, secure and encrypted communications between weapon platforms to facilitate 'interoperability'—may need to be revisited to cover the future IoT requirements.

Artificial intelligence and IoT shall render maintaining large manned militaries futile. China has already announced downsizing of its army to under a million, compensating reduction by technology. Similar downsizing of conventional forces can easily be foreseen for all the major powers of the world in about a decade or so. This would bring in a rebalancing of the power equations between the traditional rivals due to reduced force levels and higher level of transparency brought about by the IoT systems, though these are likely to increase the asymmetry between the powerful and others. Such asymmetry and transparency would contribute to increasing the stability in the regions and reduce the armed confrontations and insurgencies.

Overall, the present trends and rate of advancement of technology indicate rapid growth in the AI and IoT in the military systems, leading to a radical transformation to the concept and nature of the military operations driven by the AI and IoT. The changes are already visible as the military systems that are coming out have more and more intelligent and autonomous components. Major transformations may be seen in a decade to decade-and-a-half. The LAWS are likely to be the future weapon systems, though debates on the ethics and accountability of actions and such use of force shall carry on long into the future. The futility of the customary military systems is now becoming evident.

Forces would eventually transform and adapt to the new technology in spite of often-heard reluctance. There is a certain amount of uncertainty on the trajectory on how these would evolve due to uncertainty of how the AI would evolve. The IoT, however, would be the key enabler for future AI-regulated military activities and operations. The time may vary somewhat but the transformations are inevitable.

Notes

1. Kevin Ashton, 'That "Internet of Things" Thing', *RFID Journal*, 22 June 2009, available at http://www.rfidjournal.com/articles/view?4986, accessed on 13 May 2018.
2. Nir Kshetri, 'Using Blockchain to Secure the "Internet of Things"', *Scientific American*, 10 March 2018, available at https://www.scientificamerican.com/article/using-blockchain-to-secure-the-internet-of-things/, accessed on 16 May 2018.
3. Reuben Jackson, 'Why IoT Needs the Blockchain, and Blockchain Needs IoT', *Hackernoon*, 21 January 2018, available at https://hackernoon.com/why-iot-needs-the-blockchain-and-blockchain-needs-iot-896725b349c4, accessed on 17 May 2018.
4. 'Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in billions)', *Statista*, available at https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, accessed on 17 May 2018.
5. Paula Fraga-Lamas, Tiago M. Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo and Miguel González-López, 'A Review on Internet of Things for Defense and Public Safety', *Sensors*, 5 October 2016, available at https://www.mdpi.com/1424-8220/16/10/1644/pdf, accessed on 3 May 2018.
6. Ibid.
7. Atul Pant, 'Future Warfare and Artificial Intelligence: Visible Path', Institute for Defence Studies and Analyses (IDSA) Occasional Paper, July 2018, available at https://idsa.in/occasionalpapers/future-warfare-and-artificial-intelligence-49, accessed 17 May 2018.
8. Andy Hobsbawm, 'The Internet of Things: What Role will Humans Play?', *The Guardian*, 6 February 2014, available at https://www.theguardian.com/media-network/media-network-blog/2014/feb/06/internet-of-things-humans-smart, accessed on 24 April 2018.
9. Saumya Sharma, 'What is the Internet of Nano-things, and What are Its Uses?', *Tech Target: IoT Agenda*, December 2018, available at https://internetofthingsagenda.techtarget.com/answer/What-is-the-internet-of-nano-things-and-what-are-its-uses?track=NL-1843&ad=924953&s

rc=924953&asrc=EM_NLS_105575035&utm_medium=EM&utm_source=NLS&utm_campaign=20181225_Internet%20of%20nano-things%20takes%20IoT%20to%20a%20smaller%20scale, accessed on 4 January 2018.

10. Ajit Jaokar, 'Data Science for Internet of Things (IoT): Ten Differences from Traditional Data Science', *KD Nuggets*, September 2016, available at https://www.kdnuggets.com/2016/09/data-science-iot-10-differences.html, accessed on 10 May 2018.
11. Ibid.
12. David Kushner, 'The Real Story of Stuxnet', *IEEE Spectrum*, 26 February 2013, available at https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, accessed on 27 April 2018.
13. David E. Sanger, 'Stuxnet Worm was Perfect for Sabotaging Centrifuges', *The Hindu*, 20 November 2010, available at http://www.thehindu.com/todays-paper/tp-opinion/Stuxnet-worm-was-perfect-for-sabotaging-centrifuges/article15697946.ece, accessed on 6 May 2018.
14. Naresh Persaud, '2018 Prediction: Securing IoT-connected Devices will be a Major Cybersecurity Challenge', *CSO*, 22 December 2017, available at https://www.csoonline.com/article/3244467/internet-of-things/2018-prediction-securing-iot-connected-devices-will-be-a-major-cybersecurity-challenge.html, accessed on 20 May 2018.
15. Khwaja Shaik, 'Why Blockchain and IoT are Best Friends', *IBM*, 12 January 2018, available at https://www.ibm.com/blogs/blockchain/2018/01/why-blockchain-and-iot-are-best-friends/, accessed on 9 May 2018.
16. William A. Owens, 'The Emerging U.S. System-of-Systems', *Internet Archive: Wayback Machine,* 6 February 1996, available at https://web.archive.org/web/20100105160638/http://www.ndu.edu/inss/strforum/SF_63/forum63.html, accessed on 2 May 2018.
17. US Department of Defense (DoD), Joint Chiefs of Staff, 'Joint Vision 2010', *Internet Archive: Wayback Machine,* 2010, p. 25, available at https://web.archive.org/web/20161224220150/http:/www.dtic.mil/jv2010/jv2010.pdf, accessed on 14 May 2018.
18. Stephan De Spiegeleire, Matthijs Maas and Tim Sweijs, 'Artificial Intelligence and the Future of Defence', *The Hague Centre for Strategic Studies*, 2017, available at https://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf, accessed on 15 May 2018.
19. 'Global Information Grid (GIG)', GlobalSecurity.org, available at https://www.globalsecurity.org/intell/systems/gig.htm, accessed on 26 December 2018.

20. IoT for Military Asset Management (Part I): A Deep Dive into Problems of the Past and how Tapestry's Sensor Integration Platform, ESI, Can Help, *Tapestry Solutions*, available at https://www.tapestrysolutions.com/2017/12/19/esi-and-the-iot-in-the-military-part-i-problems-from-the-past-and-how-the-internet-of-things-is-transforming-dod-supply-chain-management/, accessed on 18 May 2018.
21. Jordan Kenny, 'Artificial Intelligence Footstep Recognition System could be Used for Airport Security', *University of Manchester*, 29 May 2018, available at https://www.manchester.ac.uk/discover/news/ai-footstep-recognition-system-could-be-used-for-airport-security/, accessed on 5 September 2018.
22. Ibid.
23. Ibid.
24. Ibid.
25. US Army Training and Doctrine Command, 'Multi-domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040', December 2017, available at http://www.tradoc.army.mil/MultiDomainOps/docs/MDB_Evolutionfor21st.pdf, accessed on 29 April 2018.
26. Ibid.
27. Lockheed Martin, 'IOT is Transforming Modern Warfare', available at https://www.lockheedmartin.com/en-us/news/features/2017/internet-of-things-transofrming-modern-warfare.html, accessed on 21 May 2018.
28. Denise E. Zheng and William A. Carter, 'Leveraging the Internet of Things for a More Efficient and Effective Military', Centre for Strategic and International Studies, September 2015, available at https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf, accessed on 26 April 2018.
29. 'Warfighter Information Network-Tactical (WIN-T)', General Dynamics, available at https://gdmissionsystems.com/en/communications/warfighter-information-network-tactical, accessed on 28 December 2018.
30. Zachary Cohen, 'US Risks Losing Artificial Intelligence Arms Race to China and Russia', *CNN*, 29 November 2017, available at https://edition.cnn.com/2017/11/29/politics/us-military-artificial-intelligence-russia-china/index.html, accessed on 9 March 2018.
31. Bedavyasa Mohanty, 'Lethal Autonomous Dragon: China's Approach to Artificial Intelligence Weapons', 15 November 2017, available at https://www.orfonline.org/expert-speak/lethal-autonomous-weapons-dragon-china-approach-artificial-intelligence/, accessed on 20 April 2018.
32. US DoD, 'Department of Defense Announces Successful Micro-drone Demonstration', Press Release, 9 January 2017, available at https://www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-

demonstration/, accessed on 16 March 2018; and 'China Launches Record-breaking Drone Swarm', *The Economic Times,* 11 June 2017, available at https://economictimes.indiatimes.com/news/international/world-news/china-launches-record-breaking-drone-swarm/articleshow/59095002.cms, accessed on 20 April 2018.

33. Adam Ni, 'Why China is Trimming its Army', *The Diplomat*, 15 July 2017, available at https://thediplomat.com/2017/07/why-china-is-trimming-its-army/, accessed on 5 April 2018.
34. Mark Beranek, 'MIL-STD-1678 Department of Defense Standard Practice Fiber Optic Cabling Systems Requirements and Measurements', *IEEE Xplore*, 2015, available at https://ieeexplore.ieee.org/document/7356617/, accessed on 8 May 2018.
35. 'IoT for Military Asset Management (Part I): A Deep Dive into Problems of the Past and How Tapestry's Sensor Integration Platform, ESI, can Help', *Tapestry Solutions*, 19 December 2017, available at https://www.tapestrysolutions.com/2017/12/19/esi-and-the-iot-in-the-military-part-i-problems-from-the-past-and-how-the-internet-of-things-is-transforming-dod-supply-chain-management/, accessed on 25 May 2018.
36. Excerpts taken from Facebook page of the Ministry of Defence of the Russian Federation, 8 January 2018, available at https://www.facebook.com/mod.mil.rus/posts/2031218563787556, accessed on 12 February 2018.
37. Nicholas Fearn, 'US Army is Using IoT Tech and Data to Transform Warfare', *Internet of Business*, 20 January 2017, available at https://internetofbusiness.com/us-army-iot-warfare/, accessed on 29 May 2018.
38. DARPA, 'Collaborative Operations in Denied Environment', available at https://www.darpa.mil/program/collaborative-operations-in-denied-environment, accessed on 28 March 2018.
39. Fearn, 'US Army is Using IoT Tech and Data to Transform Warfare', n. 37.
40. 'Air Force CyberWorx Report 17-002: Air Force Smart Bases', Air Force CyberWorx™, 2017, available at http://www.dtic.mil/dtic/tr/fulltext/u2/1042768.pdf, accessed on 2 June 2018.
41. 'IOT is Transforming Modern Warfare', n. 27.
42. Zheng and Carter, 'Leveraging the Internet of Things for a More Efficient and Effective Military', n. 28.
43. Nicholas Fearn, 'US Air Force Mulls IoT Deployment', *Internet of Business*, 29 March 2016, available at https://internetofbusiness.com/us-air-force-mulls-iot-deployment/, accessed on 29 May 2018.
44. Gopal Singh, 'Internet of Things Advancement in Defence', *International Journal of Scientific Research Engineering & Technology*, 2015, available at http://www.ijsret.org/pdf/EATHD-15012.pdf, accessed on 1 June 2018.

45. Andrew R. Belding, 'In-Network Processing on Low-Cost IoT Nodes for Maritime Surveillance', Naval Postgraduate School Monterey, California, March 2017, available at http://www.dtic.mil/dtic/tr/fulltext/u2/1045800.pdf, accessed on 26 April 2018.
46. 'Chinese Military Lists Beijing Sinonet Science and Technology as Contractor for IoT Project', *Yicai Global,* 20 June 2017, available at https://yicaiglobal.com/news/chinese-military-lists-beijing-sinonet-science-and-technology-contractor-iot-project, accessed on 16 May 2018.
47. Simon Denyer, 'China's Watchful Eye', *The Washington Post*, 7 January 2018, available at https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.5617205bfc6e, accessed on 13 March 2018.
48. Kaelyn Lowmaster, 'China's Insidious Surveillance Army: The Internet of Things', *The Hill*, 21 November 2017, available at http://thehill.com/opinion/cybersecurity/361300-chinas-insidious-surveillance-army-the-internet-of-things, accessed on 17 May 2018.