sciendo

Land Forces Academy Review
Vol. XXIV, No 4(96), 2019

FROM THE IOT TO THE IOBT. THE PATH TO SUPERIOR SITUATIONAL UNDERSTANDING

Florin POPESCU
Ministry of National Defence, Bucharest, Romania
popescuveve@gmail.com

ABSTRACT

In order to maintain and improve its competitive advantage, the ability of 21st-century armies to recognize, anticipate, adapt and manipulate IoT on the future battlefield is important. The explosive growth of innovation in the commercial sector which utilizes the integration of cloud computing, mobile communications, sensor data collection networks and artificial intelligence is a major challenge for the military. A new concept, still untapped, called the Battlefield Things Internet (IoBT) comes from here.

KEYWORDS: IoT, IoBT, situational understanding, common operational image, cloud computing

1. Introduction

"Internet of Battlefield Things" (IoBT) is from a technological or logical point of view a branch of the Internet of Things. This uses the same smart units as IoT, but the main reason for IoBT is to incorporate these systems in operating methods that go beyond basic warnings.

Interventions are well-designed and managed processes that use sensible devices to create smart sources of records that exchange the competitive advantage of operations. It improves "operational intelligence" and performs extra deliberate interventions with greater predictable results. Measures are well-designed and controlled systems that use sensitive tools to build intelligent record sources that share operations' competitive advantage. This improves' operational intelligence' and carries out more strategic measures with more predictable results.

This study was the outcome of an office analysis that examined various new technology information sources and was initially intended to raise awareness of the evolution toward a new technology among military leaders and scientists. The writer had this goal as he assumes that digitization is most likely to result in a radical transformation of military operations.

2. Proliferation of Internet of Things (IoT)

The Internet of Things, officially abbreviated IoT represents a global interconnected network of smart devices to communicate each other, resulting data flows through intelligent processes.

Kevin Ashton, co-founder of MIT Auto-ID Center, was the first scientist that mentioned about the concept of IoT (Internet of Things) in a presentation he done for Procter & Gamble (P&G) in 1999. Aiming to highlight the radio frequency ID (RFID) in P&G's board attention, Professor Ashton called his speech "Internet of Things" to incorporate a new trend: *the internet* (Ashton, 2009).

DOI: 10.2478/raft-2019-0034

The book written by MIT professor Neil Gershenfeld, entitled "When Things Start to Think", published in 1999, did not use the exact term, but came up with a clear vision of the direction of IoT.

Although Ashton stated the first time the concept of Internet of Things, the idea of interconnected devices have the origins in 1970s. It is expected that the Internet of Things (IoT) will revolutionize the way we live our lives, with many consumers already enjoying the benefits of IoT. But, the benefits of IoT will not be limited to individual benefits, but large organizations will be able to streamline their complex processes through improved automation, releasing employees from other additional tasks.

IoT is boosting rapidly and specialists expect that IoT is going to influence all our lives in coming decades, conducting to a smart world that 20 years ago seemed to be a science fiction.

Figure no. 1: *IoT network sensors*
(Source: Keeley, 2017)

Recent studies estimate that in 2020 IoT is going to reach approximately 50 billion connected devices. The economic impact is expected to be $11.1 trillion by 2025 (Manyika et al., 2005). By and large, IoT will allow automation of everything around us. The expansion of IoT and its applications are exposed in Figure no. 2.

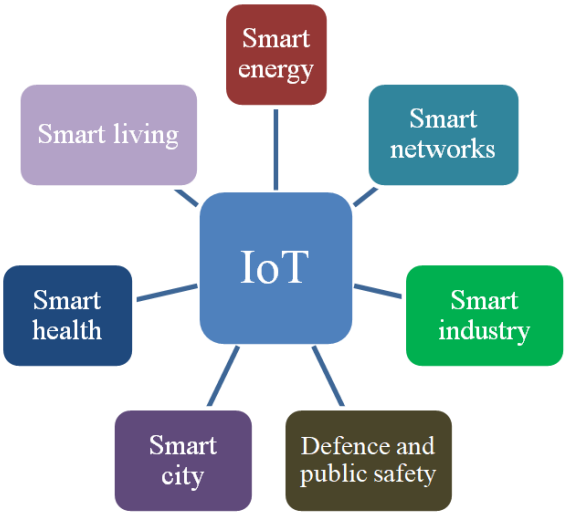

Figure no. 2: *The expansion of IoT and its applications*

IoT represents the convergence of several interdisciplinary domains (Figure no. 3):

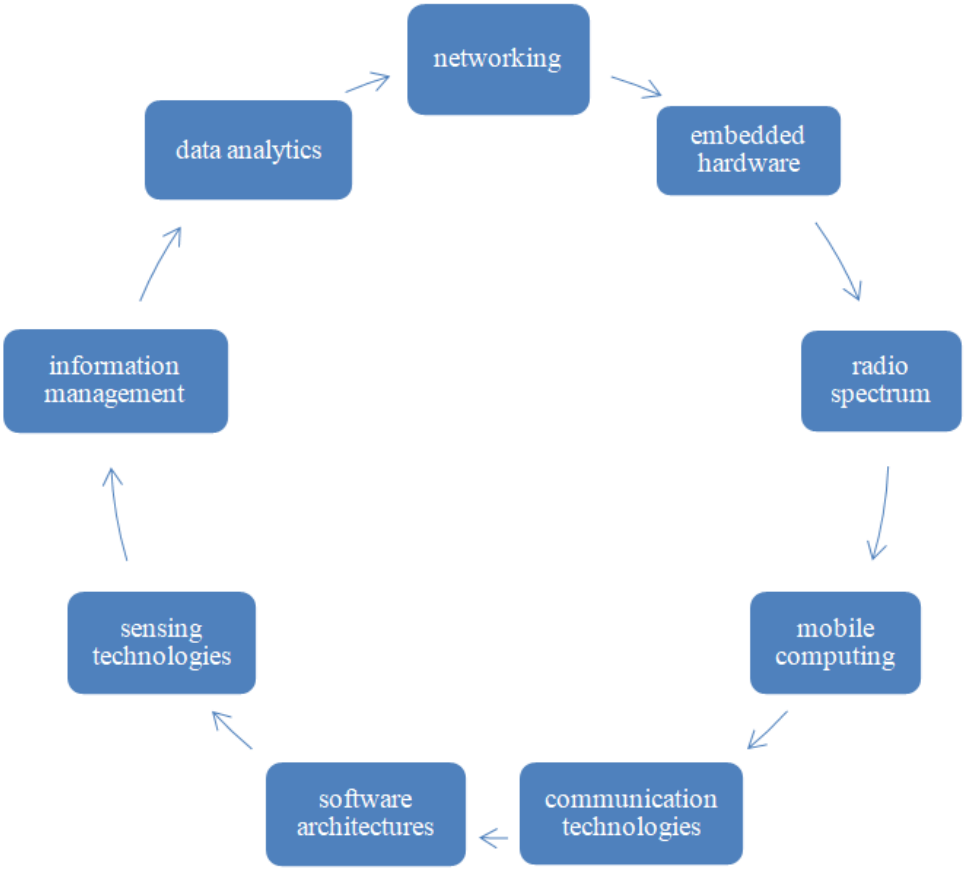

Figure no. 3: *Internet of Things (IoT) – interdisciplinary domains*

3. The Path from the IoT to the IoBT

Although the term Internet of Things (abbreviated IoT) entered the lexicon in 1999, since then, there has been a proliferation of related terms, such as Web of Things (WoT) and Internet of Things Medical (IoMT) and so on. With the publication of *Human Digital Immortality: Where Human Old Dreams and New Technologies Meet* (Popescu & Scarlat, 2017), a new concept came to my attention. This is the concept of "Internet of Battlefield Things" (IoBT), in translation "the Internet of Things on the battlefield".

The ability of 21st century armies to understand, predict, adapt and exploit IoT on the future battlefield is essential to maintaining and increasing its competitive advantage. The explosive growth of technologies in the commercial sector that exploit the convergence of cloud computing, mobile communications, sensor data collection networks and artificial intelligence is a major challenge for the military. From here comes a new concept, still untapped, called the Internet of Battlefield Things (IoBT) (Zhu et. al., 2018). The main objective of the Internet of Battlefield Things (IoBT) could be to provide situational awareness of the battlefield using a network of inter-connected analytical sensors and devices. The sensors could detect the enemy's movement and then transmit the information in real time to analysts, allowing them to make tactical decisions regarding positioning, avoidable areas or crossing a certain area.

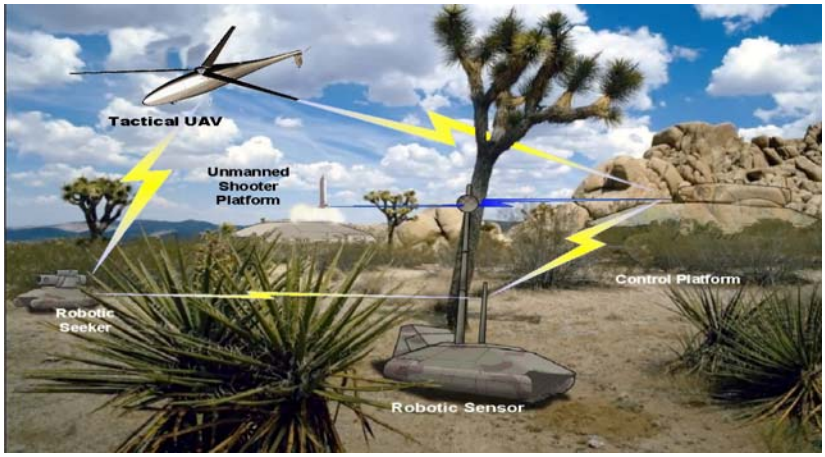

Figure no. 4: *Network of sensors and analytical devices*
(Source: West, 2017)

The modern capabilities of detecting the enemy and high precision weapons force the military to have high mobility and quick decision making. To do this, we need to have information from different sources in real time to be able to be disseminated promptly with all units involved in the operation, and one of the ways to solve this problem is to use Internet based Battle Things (IoBT) solutions.

The use of the concept of Internet of Things (IoT) in the armies of many countries of the world will become a technological trend, a kind of indicator of the modernity and innovation of their armed forces. With the advent of new technologies, the range of tasks and capabilities of military "smart devices" is rapidly expanding. It can be said that the IoT will begin to penetrate all possible aspects of military operations, starting from solving the most difficult tasks of detecting and destroying the high precision enemy to the end with monitoring the physical state of a particular service. Today, the potential areas of the "military" use of IoT technologies already include logistical support for troops, monitoring the current situation instead of a confrontation for different levels of military personnel (top commanders, unit commanders, separate fighter), medical assistance (on the field) and in a regular situation). Also, IoT devices could be widely used in various military personnel training programs in virtual combat mode.

Figure no. 5: *Connecting the military with intelligent technologies*
(Source: Stone, 2018)

The next decade will bring radical changes in the military sphere regarding military operations approaches and everything that goes with them, from military logistics to the direct hit of the enemy. All technical devices that will be in operation will need to be connected to a common system, starting with the UAV sensor and ending with a portable device in the soldier's ammunition. Moreover, the focus is precisely on unification not in a unit or separate type of troops, but between all the armed forces. It is assumed that integration into the global network will give commanders the opportunity to quickly make decisions regarding the conduct of offensive, defensive and other actions in the theater of operations.

4. IoBT Functionalities in Defence

Defense carry on to force innovation using advanced sensors, surveillance and reconnaissance drones, satellite conversation and has invested substantially in mobile technologies, together with tactical mobility for warriors. Defense these days has the opportunity to take advantage of the advantages of IoT with the aid of partnering with the non-public area and adopting IoT-enabled business practices that think about the technological peculiarities of tactical systems.

Main functionalities of IoT for defense are presented in Figure no. 6.

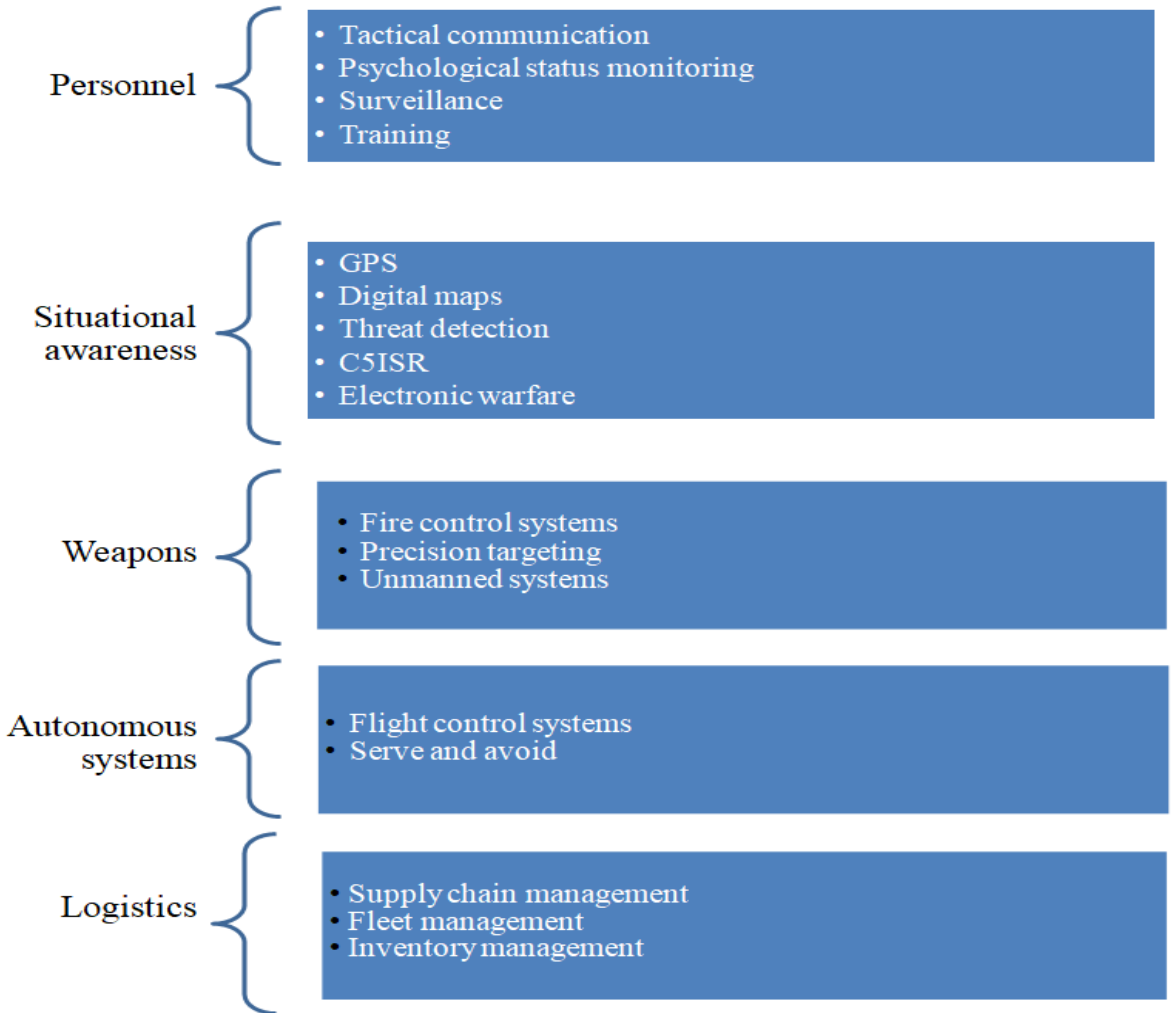

Figure no. 6: *IoT functionalities*

Smart devices embedded into soldiers body could offer information for future C5ISR systems. Consequently, C5ISR systems will be able to use data flows from millions of sensors on mounted on both, human body soldiers bodies and a variety of platforms, Surveillance satellites, UAVs (Unmanned Aerial Vehicles, in order to provide sophisticated situational awareness.

All these data flows integrated into a common platform could provide information up and down to chain of command at different levels.

Eventually, all these networks will be able to provide a Common Operational Picture (COP) for high-level military echelons in order to gain extensive situational awareness.

In fire control systems, end-to-end sensor networks and digital analytics enable real time threats and firepower with high precision.

Logistics is an environment that already uses multiple low-level sensors in security. Their implementation is currently restricted to stable areas with facilities and human involvement. For non-combat scenarios, the military has already implemented several IoT systems to boost back-end processes. For example, RFID tags were used to track shipments between central logistics hubs and to manage inventories. We define examples belonging to two main categories in the following subsections: fleet management and individual supplies. Surveillance cameras and sensors, together with advanced image analysis and pattern recognition technology, allow remote monitoring of security threats. In the case of marine and coastal surveillance, the use of various types of sensors mounted in aircraft, unmanned aerial vehicles, satellites and ships makes it possible for large areas to monitor maritime movements and traffic.

5. Conclusions: Toward a Superior Situational Understanding

Future military operations must specifically rely on integrated soldiers to achieve superior defense capabilities. The IoBT would associate soldiers with smart technology to give troops an "extra sensory" experience, provide superior understanding of the situation, equip fighters with predictive powers, provide better risk management and gain common insights. Naturally, the military's use of smart devices is already an unsustainable process. Unlike "civilians", however, IoBT systems are exposed to more serious risks as a result of participation in war confrontations between various parties. It takes a large cooperation initiative between governments, industry and the scientific community to bring IoT to the military truth. It is necessary to continue advancement in the technological fields, IT, computer engineering. Many philosophical questions, however, remain about the opposition, continuity of operations, or disaggregation of the ability to implement a military IOBT.

REFERENCES

Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*. Alpharetta, GA, SUA.

Gershenfeld, N. (1999). *When Things Start to Think*. Canada: Fitzhenry & Whiteside Ltd.

Keeley, P. (2017). *Understanding the Explosion of IoT and Its Impact*, available at: https://www.fortinet.com/blog/industry-trends/understanding-the-explosion-of-iot-and-its-impact.html, accessed on 16 September 2019.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2005). *The Internet of Things: Mapping The value beyond the Hype.* Technical Report, Washington, DC, USA: McKinsey Global Institute.

Popescu, F., & Scarlat, Cz. (2017). Human Digital Immortality: Where Human Old Dreams and New Technologies Meet. In Anabela Mesquita, A., *Research Paradigms and Contemporary Perspectives on Human-Technology Interaction* (pp. 266-282). Pennsylvania, USA: IGI GlobalDesseminator of Knowledge.

Stone, A. (2018). The internet of battlefield things will depend on modernized networks. *C4ISRNET – Media for the Intelligence Age Military*, available at: https://www.c4isrnet.com/special-reports/military-it-modernization/2018/08/03/the-internet-of-things-will-depend-on-modernized-networks/, accessed on 19 October 2019.

West, N. (2017). Military Continues to Design War Matrix With "Internet Of Battlefield Things". *The Daily Coin*, available at: https://thedailycoin.org/2017/07/21/ military-continues-design-war-matrix-internet-battlefield-things/, accessed on 12 October 2019.

Zhu, J., McClave, E., Pham, Q., Polineni, S., Reinhart, S., Sheatsley, R., & Toth, A. (2018). *A Vision toward an Internet of Battlefield Things (IoBT): Autonomous Classifying Sensor Networkby.* US Army Research Laboratory.