GlobalData.

Thematic Research: Aerospace and Defense

GDDEF-TR-S007

17 May 2019

Internet of Military Things

Internet of Military Things

The Internet of Things (IoT) in the defense industry, also known as the Internet of Military Things (IoMT) or Internet of Battlefield Things (IoBT), is the effort to develop interconnected entities that will be able to carry out multiple military and security tasks or missions.

IoMT is an enabler that will revolutionize the collection, analysis and flow of information, and thereby decision-making, as well as supporting a more intelligent interaction between humans, networks, and interfaces in an increasingly dynamic battlespace.

Advanced military forces have been investing in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems and infrastructure in order to analyze and disseminate data. IoMT aims to take this process to a higher level by better exploiting and optimizing the use of a larger volume of the collected data.

Some might wonder what the difference is between the currently available systems and platforms connected on various command and control (C2) backbones. The main difference is scale, as IoMT will allow for a much wider network, able to offer game-changing capabilities.

The ability to further connect currently scattered systems or networks into a larger integrated network will further revolutionize the tempo of operations in a number of ways. Among other things, it will reduce the time required between collecting and analyzing intelligence, planning an operation, executing it, securing the objective and restarting the sequence. That sequence does not only include front-line forces, but the entire military organization, including logistics, support, and staff units.

IoMT is in its early stages, as the underlying technologies that will effectively support its use in real combat scenarios, as well as the infrastructure design, are still under development. Commercial-off-the-shelf (COTS) technologies and cooperation between the Armed Forces and either private entities or universities and research organizations will allow the smooth introduction of the technology.

Developing major military enablers is a long-term process. IoMT is receiving, and will continue to receive, R&D funding from government funds, with the aim of developing an end product, contrary to many of the civilian market IoT products and solutions.

Leaders

Leading companies in C4ISR, cybersecurity, autonomy, and other related fields, will be part of the IoMT revolution. They include Northrop Grumman, Boeing, Lockheed Martin, Thales, BAE Systems, L3 Harris Technologies, Leonardo DRS, and Airbus.

Inside

- Players
- Trends
- Value chain
- Industry analysis
- Companies section

Report type

- **Single theme**
- Multi-theme
- Sector Scorecard

clientservices.thematic@globaldata.com
+44 (0) 207 406 6764

Contents

Technology briefing

GlobalData's defines IoT as the use of connected sensors and actuators to control and monitor the environment, the things that move within it, and the people that act within it.

To the above definition one could add that IoT in general, and IoMT specifically, is about optimizing the use of things and acquiring accurate data in order to deliver truly informed decision-making and get the best value for money from the processes involved.

The US Department of Defense (DoD) developed IoMT to enable such capabilities as part of the Third Offset Strategy. This strategy was conceived in an effort to develop and use disruptive technologies that would maintain US military supremacy against the growing capabilities employed by major competitors (e.g. China and Russia), which have a strong physical presence on the internet and have shown willingness to perpetrate cyberattacks.

IoMT structures can take many forms. Starting from the lowest level, it could be a self-contained environment like a building or buildings (e.g. warehouses or depots) where the databases for equipment and stock of a depot are fed directly to a central hub.

IoMT structures can also take the form of local environments. In this case, the data collected by a group of military depots could be accessed by a UK Ministry of Defence (MoD) supervising authority. This would allow the availability of items to be assessed real-time and procurement procedures to be initiated at an earlier stage, thus reducing gaps in support or production.

That concept could also take place on a global level. In such a case, data collected from sensors and systems deployed worldwide could be fed to central command echelons in real-time, allowing informed decisions to be taken rapidly.

In the early 2000s the US Army deployed Blue Force Tracker systems with its forces in Iraq. It was a big step forward in operations through advanced C2, as it provided a tactical picture of the area of operations to certain echelons of command, down to the platoon level.

To better understand the rationale behind IoMT, it would help understand where we are now. Military and security services around the world tend to create stovepipes. That is, each service has its own means of collecting, analyzing and disseminating information, its own means of delivering fire, its own decision-making process, and (in general) its own way of doing things. The lessons learned from combat operations have made it clear that the lack of communication between these stovepipes results in failures, often at the cost of human lives.

Joint capabilities were seen as the solution to this problem. However, despite the efforts that have been made so far, jointness has only been implemented to a limited extent. For example, higher echelons of command may have a picture from the area of operations, but units of the same armed forces or allies are still not fully capable of exchanging data, thus failing to exploiting their full range of capabilities. In this case, the picture a soldier sees through their night-vision goggles, or that is acquired from an electro-optical/infra-red (EO/IR) sensor onboard an unmanned aerial vehicle (UAV), cannot always be transmitted to all platforms in the loop.

Similarly, integrating swarms of unmanned systems into a manned platforms environment is still a challenge, not only in terms of connecting them but also carrying out complex-mission scenarios, involving the use of sensors and weapons, their guidance to the target, and their ability to learn.

These examples highlight the problems associated with the current infrastructure. The available computer networks are not fully interconnected, as result of gaps in application programming interface (API) management and transmission control protocol/internet protocol (TCP/IP) networks, which allow safe communication between things and data transfer.

Therefore, data and intelligence collected from sensors cannot always be disseminated in real-time to all the echelons of command, horizontally or vertically, which then lack the ability to respond proactively. That problem is magnified during combat operations, since the modern battlefield is highly dynamic and the "fog of war" still covers every aspect of operations, albeit for a different set of reasons than it did years, decades, or even centuries ago.

IoMT is an enabler that brings together previously divided networks of things. Therefore, its operation is based on the existence of well-established, modern and secure communications networks.

Connected "things" can include digital soldiers equipped with wearable devices, the sensors that form part of modern soldier systems or onboard systems, weapons systems (e.g. remotely-operated weapon stations or

ROWS), unmanned X vehicles (where X stands for either ground (UGVs), aerial (UAVs), surface (USVs), or underwater (UUVs)), munitions, infrastructure (buildings, networks, storage, etc.), actuators, computers, and many other things. These are the edge devices; in other words, the ones that are on the frontline (to use a common military term).

The operational advantages of setting up such a backbone are immense. However, the big impact comes from the combination of IoMT with artificial intelligence (AI) technologies like machine learning. IoT machines that incorporate AI have the ability to learn through the detection of patterns found in data. Through such sequences, edge devices can provide data analytics that will be predictive, prescriptive, and adaptive.

Until now we have seen AI used within an edge device, rather than forming part of an integrated IoT infrastructure. However, this is currently changing, and the defense market will witness a new era in the analytics and decision-making domains, where mesh networks will replace edge ones. Mesh networks are wirelessly connected to each other to extend radio signals through routing, relaying, and proxying to and from end-users. That reduces dead-zones and allows data to be transferred faster, without loss of data packages.

Such big capabilities always come at a cost and spending on IoMT operations and maintenance (O&M) will have to be clearly defined. That will help potential customers make an informed decision on their overall ability not only to acquire an IoMT infrastructure but also to maintain and upgrade it. Since this technology is still in its infancy, available cost information is limited, so manufacturers and governments will have to work on absorbing cost increases to make their solutions more affordable.

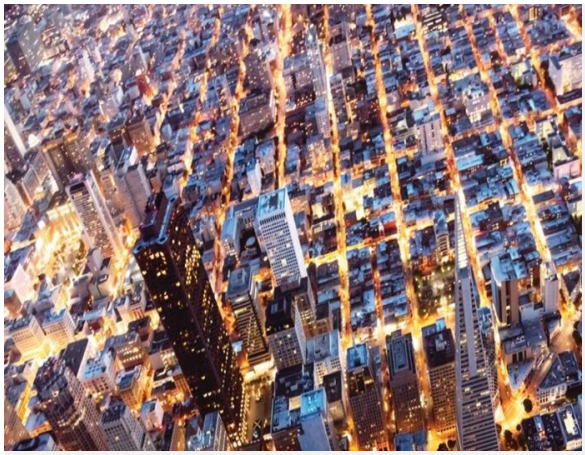
Pilot programs are a good way for government organizations to learn as much as possible on the actual acquisition and sustainment costs of IoMT, as well the utility of the technology. Small in scope, they will provide the necessary proof of concept and feasibility. Therefore, military leaders and acquisition officials will have a larger range of actual data upon which they can make informed decisions. The downsides of pilot programs include: their size, as small implementations may not reveal potential costs associated with larger acquisition and development projects; and the underlying technology and integration issues that arise when many different subsystems have to interconnect on the same platform or network.

Finally, it should be noted that, despite the advantages offered, IoMT comes with inherent dangers related to cyber-warfare and electronic warfare, as everything is connected on a network. Devices and software are provided and supported by a number of manufacturers. Data is coming from a variety of sources as well. These represent risks that must be secured. Therefore, everything should be ruggedized and protected according to military standards. NATO's standardization agreements (STANAGs) are an example of how common standards can be adopted and how a regional or transnational organization can benefit its member-states.

Manufacturers and data providers will have to undergo security audits, according to new standards that will be adopted by defense ministries and organizations. Implementation of new procedures will lead to additional costs, in terms of manufacturing, support, and training.

Most importantly, IoMT will require cooperation between allies on an international level. Despite the existence of military alliances, such as NATO, where standardization is a core element in the force structuring process, maintaining the alliance's integrity will not be easy. An example of this is the political frictions between the US and some EU countries over the development of their 5G networks by Chinese companies. European countries assume that security risks imposed by the use of Chinese technology either need to be proven or can be manageable. At the same time, China is subsidizing the products and R&D of its tech giants, such as Huawei and ZTE, making them very affordable to customers.

About GlobalData



4,000 of the world's largest companies make better and more timely decisions thanks to our unique data, expert analysis and innovative solutions delivered through a single platform.

GlobalData is one of the world's leading providers of company operational data and strategic analysis, providing detailed information on tens of thousands of companies globally. Our highly qualified team of Analysts, Researchers, and Solution Consultants use proprietary data sources and various tools and techniques to gather, analyze and represent the latest and the most reliable information essential for businesses to sustain a competitive edge. Data is continuously updated and revised by large teams of research experts, so that it always reflects the latest events and information. With a large dedicated research and analysis capability, GlobalData employs rigorous primary and secondary research techniques in developing unique data sets and research material for this series and its other reports. GlobalData offers comprehensive geographic coverage across world's most important sectors, focusing particularly on energy and healthcare.

Contact us

If you have any more questions regarding our research, please contact us:

RESEARCH

Cyrus Mewawalla
Head of Thematic Research
cyrus.mewawalla@globaldata.com
+44 (0) 207 936 6522

CLIENT SERVICES

clientservices.thematic@globaldata.com
+44 (0) 207 406 6764

Disclaimer

The data and analysis within this report is driven by GlobalData from its own primary and secondary research of public and proprietary sources and does not necessarily represent the views of the company (or companies) covered.

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that GlobalData delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such GlobalData can accept no liability whatsoever for actions taken based on any information that may subsequently prove to be incorrect.