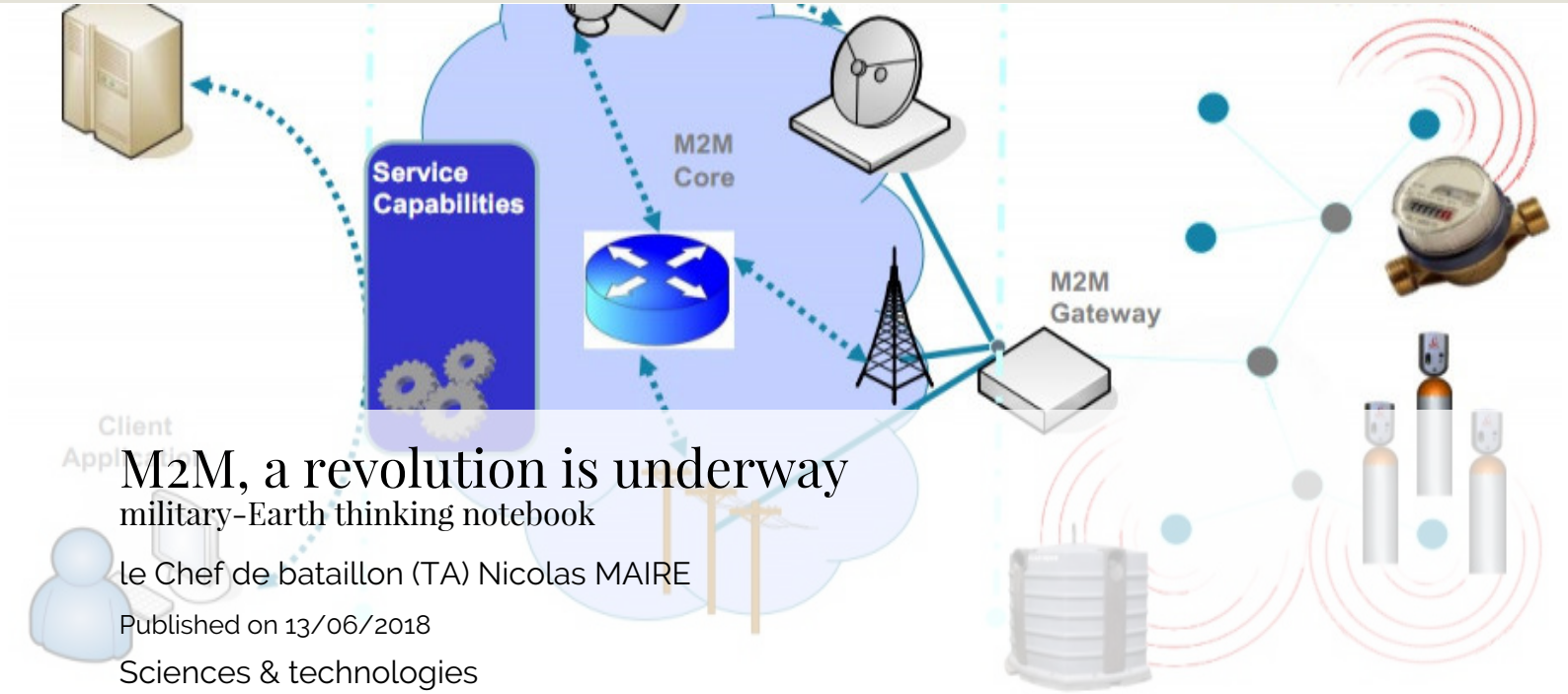

M2M, a revolution is underway

military-Earth thinking notebook

le Chef de bataillon (TA) Nicolas MAIRE

Published on 13/06/2018

Sciences & technologies

A technology based on communicating objects capable of acting autonomously, "M2M" is likely, according to experts, to change our way of life in the years to come. Its potential applications in the armed forces are such that they are likely to very quickly become a major part of the operational activity of forces, which is why it is important to carry out an in-depth reflection on their use as soon as possible in order to derive optimal efficiency from them.

A technological revolution. This is how specialists describe the advent of "machine to machine" (M2M), atechnology that extends the Internet beyond the traditional world of computers to create an Internet of Things, a world where intelligent devices communicate, exchange and act wirelessly in an autonomous way.

The explosive growth of the M2M market in recent years illustrates the extraordinary value of such technology. In 2012, the Orange phone operator sold ten times more M2M SIM cards than even the most optimistic forecasts predicted. According to the analyst firm Infonetics Research, M2M revenue is expected to grow from nearly $15 billion in 2012 to $31 billion in 2017. Estimates even predict the construction of some 212 billion connected objects by 2020.

But the stakes are not only economic: as M2M offers major prospects for the evolution of our way of life, the number of applications in all fields is almost infinite and the armed forces should benefit greatly from this upheaval. This is why the military institution must now undertake an in-depth reflection in order to anticipate the massive advent of a new era in the world's armed forces.This is why the military institution must think deeply about this now in order to anticipate the massive advent of very close to the M2M Internet in units and ensure that this phenomenon is consistent with its needs, organization and ethics, and does not become counterproductive.

What is the M2M?

The principle of "machine to machine" can be described as the association of information and communication technologies (ICT) with "intelligent" and communicating objects allowing the latter to interact, without the intervention of a human operator, with an information system.

At present, M2M does not correspond to a well-established standard but rather represents a different concept and set of systems, each designed to meet a specific need. Originally used in remote monitoring or telemetry survey operations, M2M has been undergoing a very significant expansion in recent years through the development of "smart technology" stamped systems: robotics, home automation[1], road traffic supervision, management of stocks, logistics flows or vehicle fleets...

An M2M system consists of at least three key elements:

- wireless sensors or a radio identification system (RFID)[2],
- one or more wireless communication media,
- one or more autonomous software system(s) designed to enable a network element to interpret the data and, where appropriate, to make a decision and respond to the data.

MIT's Technology Review[3] (MassachusettsInstitute of Technology) magazineranked the concept of wireless sensor networks among the top ten new technologies that will change our way of life: it consists of a large number of nodes (the micro-sensors), scattered over a geographical area (called a "sensor field"), capable of autonomously collecting, transmitting and relaying environmental data. These data are routed to a "collection point" or data sink (connected to the Internet or to a particular information system) for exploitation (see diagram on previous page).

Radio identification is a method of storing and retrieving data remotely using markers (consisting of a chip and antenna) and readers. These readers, connected to an information system, can provide a record of the data collected on the markers as they pass by (principle of the cashier passing a bar code in front of the reader at her cash desk).

Finally, there are many wireless communication standards that can transmit data to their point of use: for example, sensor networks can be based on short-range communication technologies such as Wi-Fi, Bluetooth or IEEE 802.15.4. On a larger scale, if it is not possible to carry information on a wired medium, other wireless technologies such as those derived from mobile telephony (3G, LTE, etc.) or radio or satellite links can still be used.

The reduction in the size and cost of sensors, the wide range of existing sensor types (thermal, optical, acoustic, etc.) and the constant evolution of wireless technologies have considerably broadened the scope of applications for M2M systems in general and sensor networks in particular. At the heart of these almost unlimited possibilities are jobs for the armed forces likely to respond to certain problems of modern conflicts or to improve the effectiveness of their actions in operations.

Armed forces at the heart of the technological debate

As was the case for ARPANET(Advanced Research Projects Agency Network), the precursor of the Internet, GPS and UAVs, the armed forces, mainly American, have been at the heart of the development of M2M systems. Efficient, quick to implement, inexpensive, highly flexible and fault-tolerant, sensor networks in particular have many advantages to offer in the context of certain missions.

Simple applications were thus immediately found to make this new technology profitable: sensors for intrusion detection, movement detection or to carry out contamination control of an area... One of the first successes of M2M for several years in the armed forces is the geolocation system [4]: whatever their name, these systems allow to automatically report the geografic position of combatants or friendly vehicles in the field and to display them on a digital cartographic support.

However, the armed forces have so far only scratched the surface of the possibilities offered by M2M systems, and the possibilities for using these technologies seem almost unlimited.

In 2012, four researchers from the Universities of Podgorica (Montenegro) and Belgrade (Serbia) published the results of a study[5] on possible military applications of sensor networks. The inventory of such applications includes systems equipped with portable acoustic sensors (EARS: Early Attack Reaction System) or onboard aerostats (AAP: Aerostat Acoustic Payload) to detect combat zones or establish the starting point (azimuth and distance) of a shot, permanent sonar systems for submarine detection (ASW: Anti Submarine Warfare) and even an improbable "intelligent" minefield where sensor-equipped mines are able to move in leaps and bounds to get under the tracks of an approaching armoured vehicle or to autonomously reorganise the mine network after an explosion. There is nothing far-fetched about this incredible idea, since it has been the subject of work by the very serious Defense Advanced Research Projects Agency (DARPA) for several years now.the agency of the US Department of Defense in charge of research and development of new technologies for military use.

In the same spirit, there is also the ambitious project of the US Army in the field of personal equipment for infantrymen: Future Force Warrior. This will improve the efficiency of the existing equipment, but above all it will integrate numerous functionalities. In the long term, the soldier will benefit, among other things, from more effective and lighter ballistic protection and NBC protection integrated into an air-conditioned and hermetically sealed full-face helmet. Above all, however, it will be transformed into a single network of autonomous sensors: biometric sensors will collect information on the soldier's physiological state (body temperature, hydration level, heart rate, etc.), a GPS will provide his position, while multi-optical cameras on his clothing and weapon will enable him to film what he sees around him. All this data will then pass through a mini-computer inserted in the suit (which will act as a data sink) before being transmitted via a protected satellite link to an information system for processing.

Finally, the importance of the logistics chain in modern conflicts is now well known: adding M2M capabilities to a logistics information system could probably significantly improve its efficiency. Radio-identification packages could automate and optimise the tracking and management of food, medicine or spare parts stocks. Fuel sensors could also be integrated into each vehicle to collect information on consumption, range, range

and transmission to the logistics unit. This would make it possible to automate periodic logistics messaging and to anticipate refuelling phases. In the same vein, one could even imagine a system of sensors on weapons, magazines and magazine carriers that would transmit data to the information system.This would enable the information system to receive data on ammunition consumption in order to constantly improve resupply procedures, but also to have a real-time assessment of a unit's combat readiness.

However, while these technologies, which are particularly in vogue, seem likely to represent a significant added value for the armed forces, it is nevertheless necessary to be reasonable and aware of the limits to their use in operations and elsewhere.

Artificial intelligence and the human mind

As was already the case with the use of armed drones, the introduction of technologies that supplant man for certain tasks gives rise to an ethical debate when it comes to their application in combat. The soldier in war has the right to give death. That is a fact. If he has this power, this great responsibility, it is because he accepts in return that he can be killed by his enemy. If we follow this ethical reasoning, does a drone pilot in Florida have the right to open fire on his enemies in Afghanistan knowing that they, in return, can never threaten his life? Similarly, tomorrow, will we be allowed to put in place armed systems that will automatically fire on any intruder who enters a perimeter and is detected by presence sensors? No matter how sophisticated a system is, it will never do more than apply the rules defined by the extremely complex algorithms that set it up. No matter how sophisticated an artificial intelligence may be, it will never be able to accurately copy the patterns of thought, reflection or sensitivity of individual human beings. Thus, the human being must remain at the centre of decision-making: M2M systems, if deployed, should only be used as tools to amplify efficiency or as decision support tools. They must lighten the tasks of collecting and processing information in order to improve the procedures in force, but in no way supplant human beings in the cycle of analysis and choice of actions to be taken.

In addition to the obvious security and confidentiality issues inherent in the circulation of potentially sensitive information over wireless links that are highly vulnerable to eavesdropping, interception orIn addition to the obvious security and confidentiality problems inherent in the circulation of potentially sensitive information over wireless links that are highly vulnerable to eavesdropping, interception or intrusion, another problem could be linked to the massive arrival of such systems in the armed forces, a problem that is not only of concern to the European Union but also to the international community.This problem has already been encountered with the considerable development of information systems in recent years: that of information literacy. If WIS[6] have made it possible to improve the overall effectiveness of the various levels of command, it is above all because significant efforts have been made in their use and the discipline that this entails. As the capabilities offered by computer networks make it easy to generate information and disseminate it to as many people as possible, a phenomenon of information overload quickly emerged: Information was everywhere where it should be, but especially where it should not be, and everyone was wasting considerable time finding useful information in the midst of a continuous flow of superfluous information. Too much information kills information, it is often said... If this phenomenon has been relatively curbed, it is thanks in particular to theIf this phenomenon has been relatively curbed, it is thanks in particular to the creation of information management units and the establishment of strict rules for the use of the systems. It is then easy to imagine that

these information flows will grow exponentially with the development of a multitude of sensor networks and M2M assemblies. It will therefore be necessary to ensure their proper use and parameterisation: not only will these systems have to collect data, but above all they will have to interpret them correctly in order to deliver useful information (and not raw data) to the right person.

What's next?

Tomorrow may present the armed forces with an even greater challenge than the digitization of the battle space and the advent of information systems within command structures. M2M systems have the potential to become remarkable decision support tools and fabulous levers to boost efficiency. The sine qua non condition for effective integration is to carry out an in-depth reflection today on the definition of the perimeter that we want to give to these systems. What are our needs? What can these systems do for us? What are their limits? What limits will we impose on their use for ethical reasons? The arrival of M2M is an inevitable phenomenon. If it is to be a success for armies, these questions must be answered as soon as possible. Before others decide for us.

1] All the techniques that allow the automation of the home (comfort, security, energy).

[2] Radio Frequency IDentification

[3] http://www2.technologyreview.com/featured-story/401775/10-emerging-technologies-that-will-change-the/2/

4] e.g. BFT (Blue Force Tracker) / ePLRS (enhanced Position Location Reporting System) / MTS (Movement Tracking System)

[5] "A Survey of Military Applications of Wireless Sensor Networks"(P. Durišić, Z. Tafa, G. Dimić and V. Milutinović).

6] OIS: operational information systems.

Saint-cyrien of the promotion "De la France combattante" (1997-2000), graduated from the War School (20th promotion), the Chief of Battalion(TA) MAIRE has spent almost all his career in the Signals Army. This year, he is studying at Télécom Bretagne for a Master's degree in "mobile networks and services" before joining the 53rd Signal Regiment in the summer of 2014 to take up the position of Head of BOI.

Title : le Chef de bataillon (TA) Nicolas MAIRE

Author (s) : le Chef de bataillon (TA) Nicolas MAIRE

Release date 23/05/2018