The Internet of Things for Munitions Health Management

Matthew Mapleston
Chanza Chanzo Ltd. 30 St Johns Road, Margate, Kent, United Kingdom CT9 1LU
matt@chanzachanzo.com

ABSTRACT

This paper takes a holistic view of Munitions Health Management (MHM) relevant developments across a range of industries and looks at how they may be useful within Defence.

The Internet of Things (IoT) is a widely used term that refers to uniquely identifiable objects and their virtual representations in an Internet-like structure. Tagging objects and people allows them to be managed and inventoried by computers through a multitude of existing technologies.

This paper provides a conceptual introduction to the Internet of Things with examples. This provides the foundation for an examination of the impact IoT could have on defence operations. In particular it focuses on blockchain and smart contract technologies providing critical aspects of security, automation and dependability to IoT and MHM systems.

1 INTRODUCTION

Munition Health Management is about the instrumentation of systems to collect and manage data and generate actionable information. For munitions Safety, Cost and Performance are the key benefits of this approach.

The term 'Internet of Things' describes technologies that embed intelligence, sensing and connectivity into objects. This is happening across a range of industries and has the potential to cause a fundamental transformation of human and indeed machine activities akin to the industrial revolution (Goldman Sachs, 2014).

Munitions Health Management is an Internet of Things implementation and there is a lot to learn from activities within IoT across other domains. This paper provides an introduction to the Internet of Things, a primer if you will, together with selected examples to characterise the main concepts and their status.

2 THE INTERNET OF THINGS

The Internet of Things is thought to be the next industrial revolution. It is expected to contribute nearly $2 Trillion towards the global economy by 2020 (Van Der Meulen, 2013). It will do this by connecting things, people, places and systems, collecting information and adding intelligence where none exists.

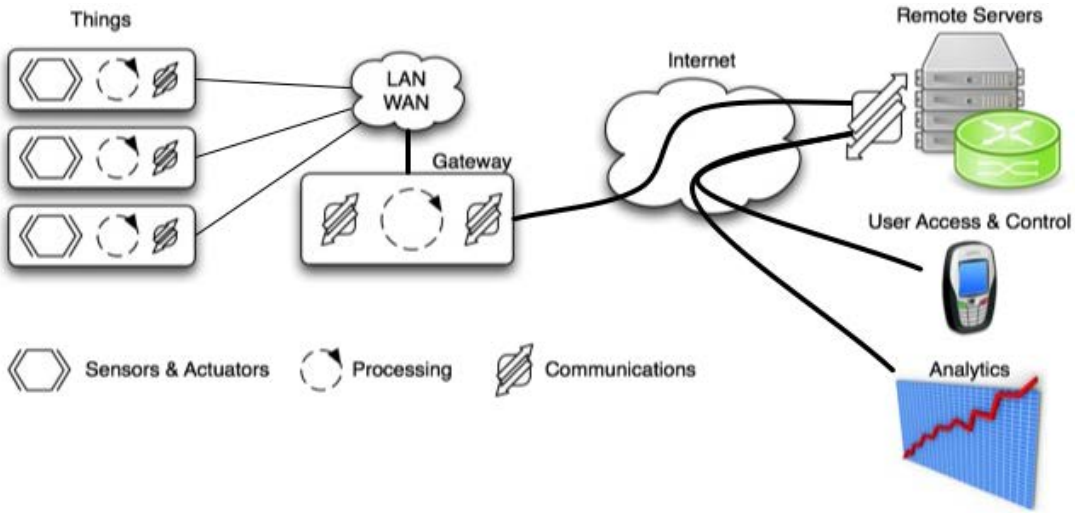
The Internet of Things is the idea that any physical object can connect to the internet and communicate with other objects ("Explainer: What is the 'Internet of Things?' - CNN.com," 2013), that means a world populated by ubiquitous sensors and streams of nano-data (Koomey, 2012) and a dramatic extension of the Internet to enable communication between sensors, actuators and computer networks (Ferber, 2013). The Oxford English Dictionary added a definition for Internet of Things in September 2013:

> "A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data."

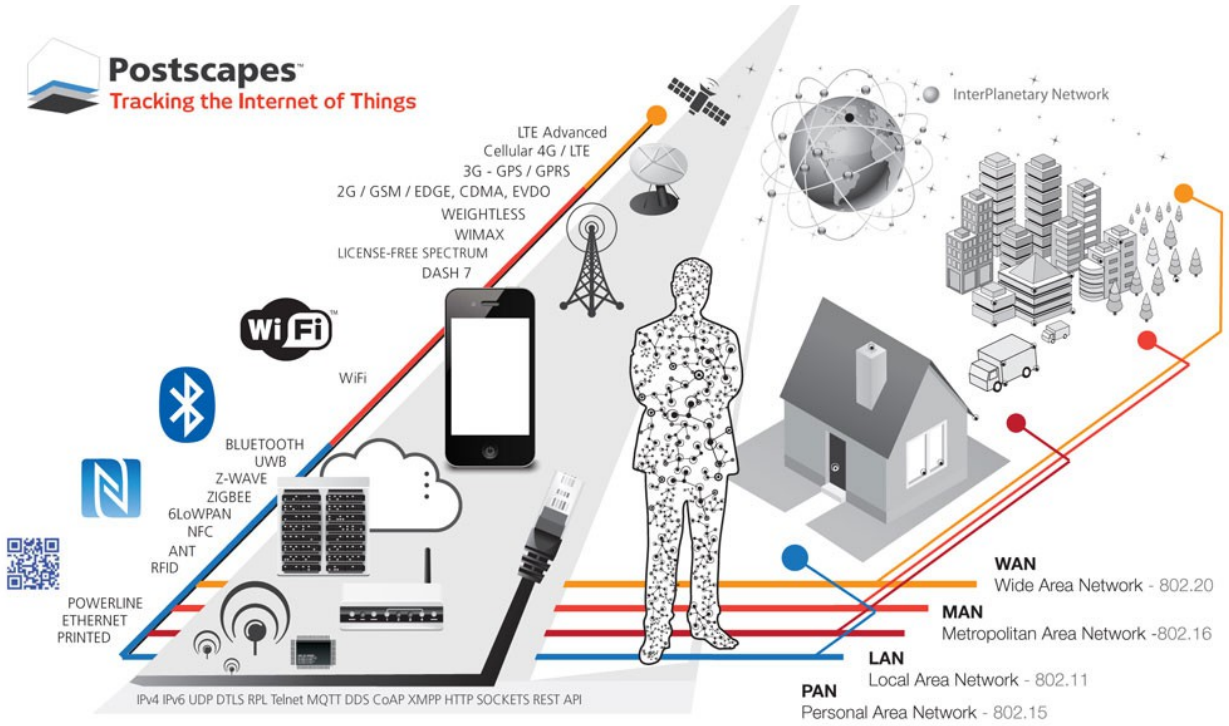
However, it has also been said that the Internet of Things already exists because the number of connected objects exceeded the number of connected humans during 2008/2009 (Evans, 2011). Gartner predict over

thirty billion connected devices of far greater variety by 2020 (Van Der Meulen, 2013) and various reports of market value range from $300 billion to $15 trillion by 2020 (Press, 2014).

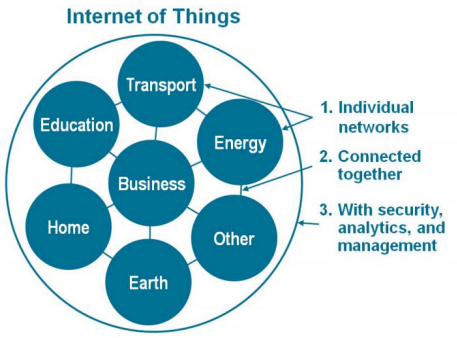
The current general approach to connecting Things to the Internet is shown below. On the left are the 'Things' that are being connected either as new products or retrofits to existing real world objects. These Things feature some form of sensor and/or actuator with embedded processing and communications. These can be characterised as having very small form factors, low electrical and processing power and short distance wireless connections.



These Things often connect to a local hub that filters and concentrates data. Whether a standalone device or an 'app' on a smart phone, hubs provide user interface, sends data over the internet and receives commands from a central control (e.g. the manufacturer). Central controllers aggregate data and use it to manage the Things. The IoT world is very heterogeneous, e.g. there are many network technologies used by IoT systems, many of which are shown in the diagram below ("Internet of Things Technologies-Postscapes," n.d.).



IoT implementations seen so far will lead to loose collections of disparate purpose-built networks. Over time they will converge to form a Network of Networks (Evans, 2011) amplifying the functionality and benefits of each.



3 COMMERCIAL DEVELOPMENTS & TRENDS

At the time of writing there are many examples of the Internet of Things products and services. Here are just a few from various market verticals.

3.1. Example 1: Consumer products

With its acquisition by Google in early 2014 for a sticker price of USD 3.2bn, Nest Labs Inc. certainly made headlines for being the first large exit of an Internet of Things startup. The Nest Smart Thermostat, premiered only 3 years prior is widely heralded as the best designed and functional smart home appliance yet. Marketed as a self-learning heating and cooling solution, it exhibits a self-learning algorithm on the backend, i.e. Nest's, and now Google's, servers which tries to infer enough information about users' daily

routines to set heating and cooling cycles appropriately. It further is equipped with an array of sensors which allow the device to notice, among other things, presence and movement to adjust predicted state against sensed reality. Due to its connection to the wider internet, the temperature can be adjusted from a smartphone app. With the extension of its product range to include the Nest Protect smoke detector, which integrates seamlessly with the smart thermostat, the system augments its capabilities to use multiple presence and temperature sensors, and to automatically shut down gas ranges should dangerous levels of Carbon-Monoxide or -Dioxide be sensed.

3.2. Health

When the GlowCaps "Smart Pill Bottle" first premiered on the market, the health-care industry started to take note. In the more consumer-geared personal fitness sector, connected products have long played a major role. Spear-headed by the Nike+ system in cooperation with Apple, the benefits of tracking performance have clear to individual athletes. Now, however, the market seems to shift towards more generally health-related devices. GlowCaps utilizes sensors to notice if and when patients take their prescribed medication, and by utilizing a social feedback mechanism are able to drastically increase medication adherence.

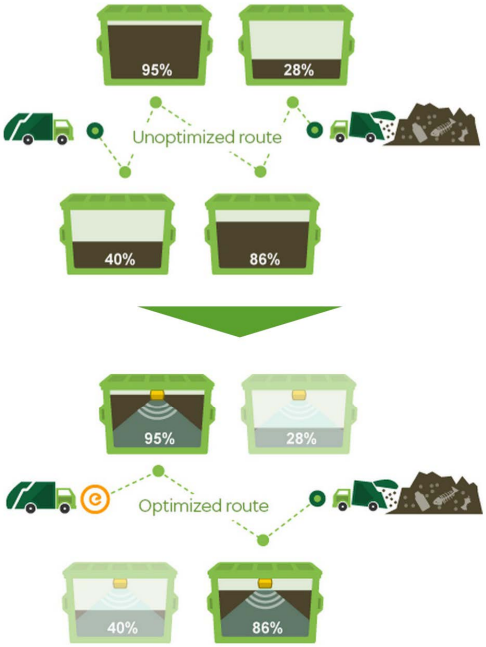
Given previous attempts at "Tele-Health" solutions, which usually are developed in conjunction with established health-care providers or health insurers, the velocity of go-to-market of consumer devices in the health market still seems staggering.

Take for instance the Withings system: starting out as an internet-connected body scale, their family of products now has expanded to include everything from fitness trackers to blood pressure monitors, giving their users a more comprehensive overview over their individual health.

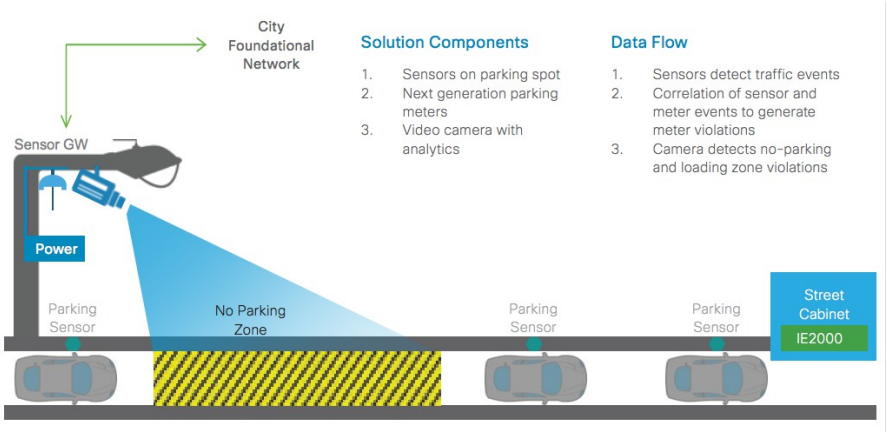
That is not to say that established health-care infrastructure providers aren't utilizing IoT approaches. Players like Alcatel-Lucent or Cisco are aiming to improve efficiencies of in-patient and out-patient care by utilizing better data sharing and facilitating cooperation between individual doctors and nurses.

3.3. Future Cities

The Finish company Enevo ("Enevo Homepage," 2014) developed smart sensors for waste containers to measure fill levels. This data is used to automatically generate schedules and optimised routes for waste collection by not collecting from containers until they need it. They claim up to 50% savings on direct waste collection costs and an elimination of overfilled containers leading to litter. Their system was deployed in 25 countries across Europe and North America with further plans to expand globally (Butcher, 2014).



Cisco's City Parking system (Cisco, 2014) connects parking spaces to the Internet of Things to ultimately make cities greener and more liveable. An ITS America report showed that up to 30% of traffic on the roads of cities in the USA are those circling around looking for parking spaces. Sensing the availability of parking spaces and intelligently managing and communicating over the Internet of Things greatly reduces that figure by guiding parkers directly to the nearest free space. In addition, the system can guide enforcement officers to cars overdue on their fees and no parking zone violations.



Smart meters are the next generation of gas and electricity meters that offer a range of intelligent features including real-time display of energy use, accurate billing and easier switching of provider. Most smart meters at the time of writing use GMS/GPRS (mobile phone) signals to send information back to the supplier. The UK Government's policy is that most consumers will have smart meters installed by energy companies by 2020 (UK Government, 2014). and have awarded contracts with a value of £2.4 billion to roll out 53 million electricity and gas smart meters (Davey, 2013).

3.4. Transport/AutomotiveAutonomous, Self-learning cars

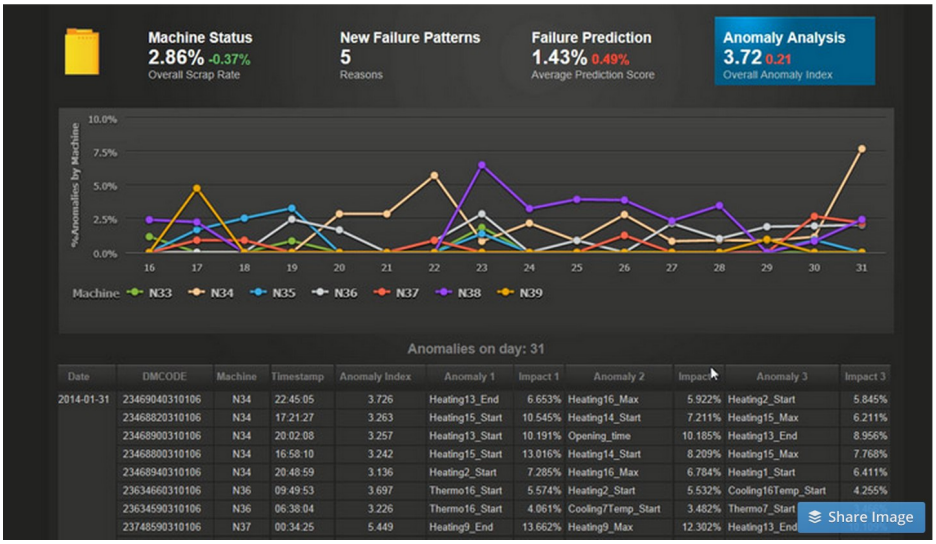
Automotive systems have a big impact on everyone's lives. They give us freedom of movement and influence many aspects of urban planning. They also are responsible for many deaths through road traffic accidents, generate air pollution, consume much energy and time.

Telematics on fleet cars and haulage vehicles have been common place for many years. Telematic monitoring of all cars is improving the efficiency maintenance regimes through diagnostics and prognostics. Telematics are also being used to reward careful driving with lower insurance premiums by measuring driving style, journey times and lengths and changing driver behaviour on the way (Boggan, 2012).

MIT Media Lab have conducted research into various aspects of automotive systems, positing that cars should behave like horses in old western films (Rose, 2014) where the cowboy wobbles out of the saloon and whistles for his horse that takes him home while he sleeps. Taking this further, cars could wander off and self-park miles from the city to return in time to carry their owner home. Google (Thrun, 2010) and Oxford University ("Mobile Robotics Group | Department of Engineering Science, University of Oxford," n.d.) have made this a reality using sensors and actuators in cars and 'big data' about other cars, roads and urban spaces to drive around without direct human control.

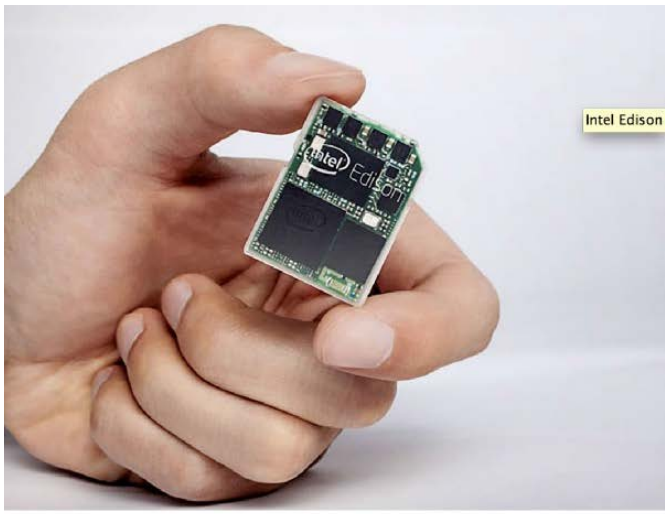
3.5. Industrial Products

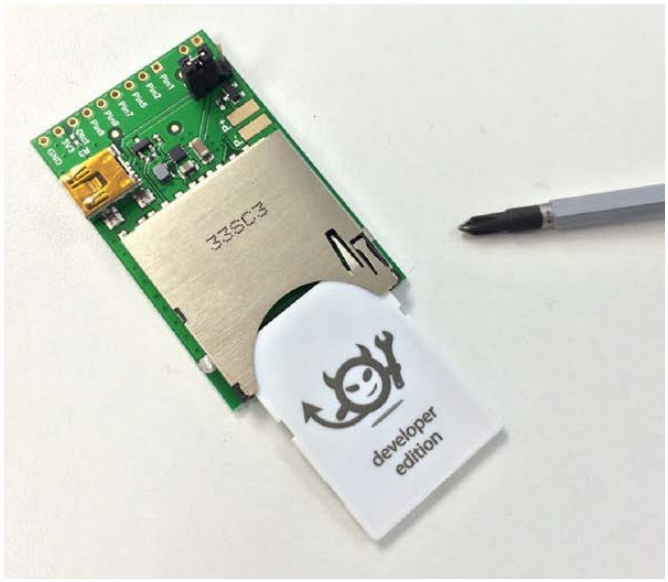
IBM offer a range of business analytics software including predictive maintenance and quality systems that proactively detect failure patterns. It integrates and analyses sensor data including usage and wear both in real-time and historical. It provides actionable information through predictive modelling, decision management, workflows and dashboards ("IBM - Predictive Maintenance and Quality," 2014).



3.6. Hardware Technology

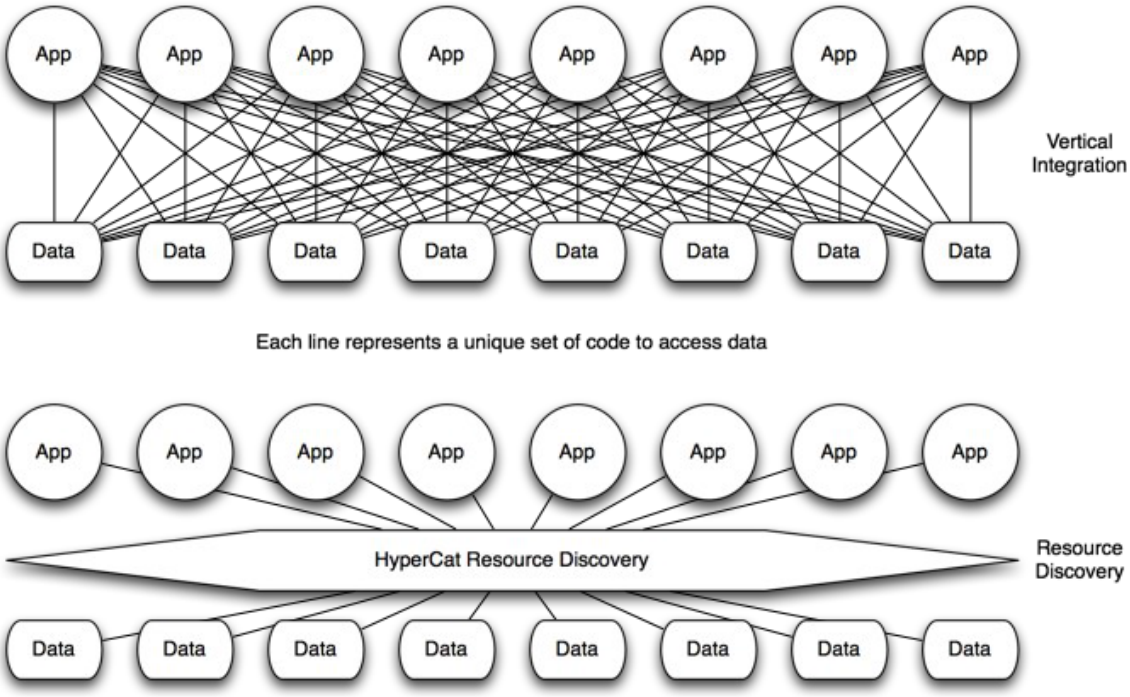
Miniaturisation of computing hardware continues at pace. In particular the two main processor manufacturers are in a competitive race to produce new products aimed at the Internet of Things and wearable devices. Hand-in-hand with miniaturisation is a drive for energy efficiency which is driven by new uses for computers within the Internet of Things area. Examples of this type of hardware are Edison from Intel (Shah, 2013) and the ARM based Imp (Smith, 2013) both shown below.



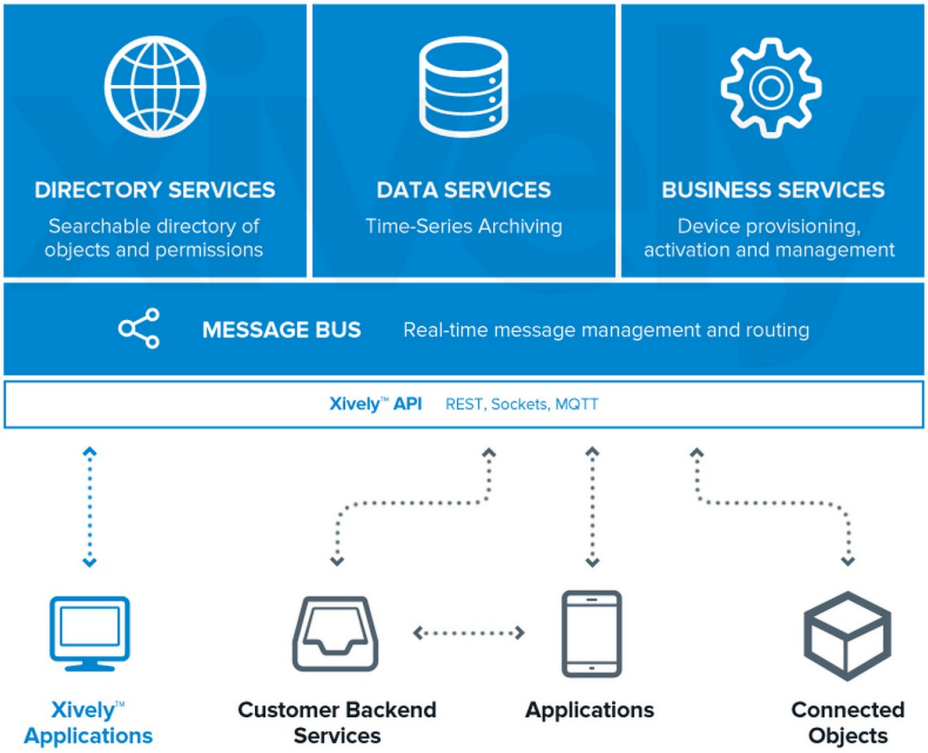


3.7. Data & Software

In order for the Internet of Things to be fully realised technology must be developed to avoid vertical data streams creating silos of inoperable data and services. HyperCat was developed to enable the discovery of resources by applications without source-specific code (Beart, 2014). HyperCat is a new media type for the web allowing servers to list catalogues of resources. It is designed to make discovery of IoT services and assets easier (1248, 2014; Beart, 2014).



A commercial example of this approach can be found with Xively in their cloud service (Xively, 2014).



4 BLOCKCHAINS

The above introduction to IoT and examples of its implementation all share three challenges: Security, Autonomy and Dependability.

The millions of IoT being connected to the internet form a tempting target for hackers for example to form massive botnets used for significant Distributed Denial of Service attacks. IoT devices are infected with malware that when triggered collectively swamp target computers with massive amounts of network traffic. The scale of recent attacks is sufficient to bring down all internet activity for a small country (Woolf, 2016) and significantly impact even the USA (Nixon et al., 2016).

Simple automation is evident in all IoT devices starting from collecting data to controlling a local system. Difficulties of human management and control of millions of devices and associated networks will require more automation within devices and at higher levels of abstraction e.g. a company providing millions of energy meters would not be able to manage individual meters without significant automation.

IoT devices must be dependable because they must provide value to the consumer, support health critical functions, protect personal data or are integral parts of critical national infrastructure. Increasingly, dependability rests on software due to its complexity (it's hard to write it well) and its attack vectors as a connected device.

Each of these challenges can be addressed through Blockchains and Smart Contracts.

Block-chain technologies are a key enabler of IoT; invented in 2008 to enable crypto-currency systems where digital tokens of value can be sent anonymously over open networks without any trusted intermediary. The most popular crypto-currency holds £32.9 Billion of capital on the open internet, has not been successfully hacked in its nearly 10 years of existence and cannot be switched off while the internet is available. These technologies can be used to create autonomous organisations through decentralized, secure execution of logic and smart contracts between digital entities. In the near future enterprises will hold smart contracts responsible for many times the value of crypto-currencies. They are the solution to key issues in the development of IoT systems and therefore inherently essential elements of autonomous last mile resupply.

Blockchains have been considered for use in defence (Barnas, 2016) particularly for data integrity, asset provenance and resilient communications – key components of logistics. Barnas does not however consider the promise of decentralised, deterministic computing commonly called smart contracts. Ethereum, an implementation of a blockchain with smart contract capability (Diedrich, 2016; Ethereum Foundation, n.d.), is the leading-edge of this technology.

Blockchains are decentralised, highly-secure computing; moving away from centralised or federated architectures is vital if autonomous systems of systems are to be realised as indicated by recent developments around IoT. It turns the approach to cyber-security on its head moving away from the fortress approach which gains trust from a core entity. The ADO removes the need for secret credentials segregating insiders from outsiders – it is a trustless network; it allows reliable data exchange and logic code execution on an unreliable network where some participants cannot be trusted.

Blockchains and Smart Contracts enable decentralized computing that shares data, state and code with all nodes within a peer to peer network, building on heterogeneous network systems. It has no central point of failure therefore no downtime, disappearing servers or hanging applications can occur.

The underlying principles are:

- peer to peer network of software nodes (decentralization)
- an immutable record of events and transactions (block-chain)

- digital identities maintaining anonymity (asymmetric key encryption)
- implicit trust without intermediary (consensus)
- deterministic, cyber-hard code (smart contracts)

Decentralisation: a network of cooperating software nodes each share a consistent state and history making the network very robust against failure. This is achieved securely and efficiently using techniques such as blockchains and merckle trees (see below). External events, new smart contracts and data updates enter the network as transitions from current state which are verified then shared with all nodes. This ensures that there is no single point of failure because every node must agree with the overall 'Truth' to continue to be part of the network. It is extremely difficult to change history in order to justify any alternative truth.

Block-chain: The block-chain is an ordered, back-linked, append-only list of blocks of data that forms the backbone of the network. A block is a data structure constructed from a set of changes to logic code, trigger inputs and computation results/state transitions that occurred over a short time interval. This data is passed through a cryptographic hash to generate a fingerprint of its data. This fingerprint, a timestamp and the fingerprint of the last accepted block are then combined by another cryptographic hash to generate the overall block fingerprint.

A cryptographic hash is a one way mathematical algorithm that converts any input data into a unique fixed length signature; the input data cannot be found from its signature. For example, the string "Hello World" hashes to A591A6D40BF420404A011733CFB7B190D62C65BF0BCDA32B57B277D9AD9F146E; the string "Hello World!" hashes to 2DDDC2BB86F352EA34213F067371C3EEA9EDAB97001BEE9AA5047DF583B739BA; and a digital mpeg file of a film would hash to a similar unique 64 character signature.

As a consequence each new block is appended onto a chain of all former blocks in time order. Any change to a block (even one bit) completely changes its fingerprints invalidating all subsequent block fingerprints calculated from it. This creates a historical record hard chained together making any tampering evident throughout the network. It is also very, very hard for adversaries to access and compute an alternative chain quickly enough to overtake the consensus supporting the original blockchain. This chain of blocks creates an immutable record of events and database of code and state. The whole chain is efficiently shared between many nodes in network and verified every time a new block is added. Any attempt to tamper with the record of events or the database of code and state is immediately evident within network because the hash results no longer stack up (literally). This creates the cyber-hard, fault tolerant backbone of autonomous system-of-systems behaviour.

Asymmetric Key Encryption: Every node, user, platform, asset may have a digital entity on the blockchain represented by a unique identity. This identity is based on a public key generated from a private key. The public key can be shared over the network and used to encrypt messages and verify identity. The use of public keys to generate digital identity is also a useful source of anonymity in the digital world further hardening against cyber-attack; the right approach makes it impossible for anyone gaining unauthorised access to the ledger to work out the identity, location or behaviours of real-world assets.

Consensus: Each time a transition is created it is checked by multiple Validator nodes for correct format and adherence to basic rules. Validated transitions are shared across the network and kept in a pool. At intervals of time a block combines transitions from the pool into a new block to be added to the blockchain. This is carried out by multiple Endorser nodes in parallel competing to calculate a block that is accepted by a majority of nodes as the Truth. This version of byzantine fault tolerance maintains ADO's decentralized blockchain instead of using a central trusted intermediary.

Smart Contracts: Building on guaranteed execution and trust without intermediary, smart contracts encode agreements in logic code baked into the blockchain. They can be thought of as an 'if this then that' state machine that produces repeatable outcomes for any set of inputs. Once committed they can be relied

upon to execute once the defined triggers are met. The only way to stop a smart contract would be for the coordinating authority to reset the whole network to a previous snapshot.

CONCLUSION

This paper set out to introduce and characterise emerging Internet of Things concepts and technologies providing relevant examples. Mapping these to defence capabilities highlights some risks and opportunities which must be managed to maintain military capability in the medium to long-term. It is our intention to maintain an overview of Internet of Things developments and understand their impact on defence capability both positive and negative.

5 REFERENCES

1248, 2014. 1248.io Wiki [WWW Document]. URL http://wiki.1248.io/doku.php (accessed 9.4.14).

Barnas, N.B., 2016. Blockchains in National Defense: Trustworthy Systems in a Trustless World. Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama.

Beart, P., 2014. Hyper/Cat in 15 Minutes.

Boggan, S., 2012. The little black box that could save you a fortune on your car insurance... Mail Online.

Butcher, M., 2014. Enevo Sensor-based waste collection system. Techcrunch.

Cisco, 2014. Cisco Smart+Connected City Parking - Cisco Systems [WWW Document]. URL http://www.cisco.com/web/strategy/smart_connected_communities/city_parking.html (accessed 9.14.14).

Davey, R.H. (MP) E., 2013. Award of Smart Meters DCC Licence - Written statements to Parliament - GOV.UK [WWW Document]. URL https://www.gov.uk/government/speeches/award-of-smart-meters-dcc-licence (accessed 9.16.14).

Diedrich, H., 2016. Ethereum: blockchains, digital assets, smart contracts, decentralized autonomous organizations.

Enevo Homepage [WWW Document], 2014. URL http://www.enevo.com/ (accessed 9.14.14).

Ethereum Foundation, n.d. Devcon2: Ethereum in 25 Minutes.

Evans, D., 2011. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything (Whitepaper). Cisco Internet Business Solutions Group.

Explainer: What is the “Internet of Things?” - CNN.com [WWW Document], 2013. URL http://edition.cnn.com/2012/12/04/business/leweb-parallax-internet-things (accessed 8.15.14).

Ferber, S., 2013. How the Internet of Things Changes Everything [WWW Document]. Harv. Bus. Rev. URL http://blogs.hbr.org/2013/05/how-the-internet-of-things-cha/ (accessed 8.15.14).

Goldman Sachs, 2014. The Next Industrial Revolution: Moving from B-R-I-C-K-S to B-I-T-S.

IBM - Predictive Maintenance and Quality [WWW Document], 2014. URL http://www-03.ibm.com/software/products/en/predictive-maintenance-quality (accessed 9.13.14).

Internet of Things Technologies- Postscapes [WWW Document], n.d. URL http://postscapes.com/internet-of-things-technologies (accessed 9.4.14).

Koomey, J., 2012. The Computing Trend that Will Change Everything [WWW Document]. MIT Technol. Rev. URL http://www.technologyreview.com/news/427444/the-computing-trend-that-will-change-everything/?p1=BI (accessed 8.15.14).

Mobile Robotics Group | Department of Engineering Science, University of Oxford [WWW Document], n.d. . Mob. Robot. Group. URL http://mrg.robots.ox.ac.uk/ (accessed 9.4.14).

Nixon, A., Costello, J., Wikholm, Z., 2016. Flashpoint - An After-Action Analysis of the Mirai Botnet Attacks on Dyn. Flashpoint.

Press, G., 2014. Internet of Things By The Numbers: Market Estimates And Forecasts. Forbes.

Rose, D., 2014. Enchanted objects: design, human desire, and the Internet of things, First Scribner hardcover edition. ed. Scribner, New York, NY.

Shah, A., 2013. Intel chases Internet of things with new chips, software. Computerworld.

Smith, T., 2013. Little devil: Electric Imp is an Internet of Things Wi-Fi PC-ON-AN-SD-CARD • The Register. The Register.

Thrun, S., 2010. Official Google Blog: What we're driving at [WWW Document]. Off. Google Blog. URL http://googleblog.blogspot.co.uk/2010/10/what-were-driving-at.html (accessed 9.4.14).

UK Government, 2014. Smart meters - Helping households to cut their energy bills - Policies - GOV.UK [WWW Document]. URL https://www.gov.uk/government/policies/helping-households-to-cut-their-energy-bills/supporting-pages/smart-meters (accessed 9.4.14).

Van Der Meulen, R., 2013. Gartner Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets.

Woolf, N., 2016. Massive cyber-attack grinds Liberia's internet to a halt. The Guardian.

Xively, 2014. What is Xively - Xively [WWW Document]. What Xively. URL https://xively.com/whats_xively/ (accessed 9.26.14).