BUILDING A CLOUD BASED FRAMEWORK DEFENSE NETWORK: INTERNET OF THINGS APPROACH

BASAKY D. BASAKY, PhD.
Information Technology Department
Salem University Lokoja, Nigeria

&

BAKARE KAREEM
Information Technology Department
Ahmadu Bello University

Abstract

***The exponential growing rate of insecurity in the African nations is disturbing. The many and series of diverse security apparatus but could stem these insecurity. The reasons are clear. We need an up to date system to solve this menace. A cloud-based frame work for National Defense Security Network would be the only solution. The services of a cloud base system are seamlessly changed in a very high speed, less resources for setting up are expend. Other benefits that amount to very low cost is inexhaustible amount of storage space, scalability,* availability, integrity, and confidentiality.**

Introduction

The state of insecurity in Nigeria today is no news to anyone and although, it can be attributed on some factors that have been left unchecked for a long time by both the Government and people of Nigeria but the level of insecurity in the country today is threatening to tear her apart and requires quick, adequate and a new approach to deal with the security challenges plaguing the nation. Apart from food insecurity, financial insecurity, terrorism, health insecurity and others, security failure has eaten deep into the fabrics of the country. The situation in Nigeria since the beginning of this decade in which dozens of militant groups emerged and challenged in the most violent form the authority of the Government; the growing level of urban crime including armed robbery, kidnappings, ritual killings, and cultism; the continuing erosion of the moral authority of religions in which people engage in acts in open defiance of their religious and moral teachings; the culture of impunity that characterizes public affairs; the corruption that is submerging the average Nigerian; and the collapsing social and political institutions in the country over the last few years, more than anything demand for quick and lasting solutions that will at least reduce the security threats facing Nigeria today.

There is general agreement among historians that insecurity have been the core cause of bloodshed in Nigeria and the world at large. Lee, C.H. and Chung, C.W., (2011).

The deep scars that insecurity leaves on people and nations are often obscured by historical accounts that, more often than not, glorify conquest and ignore aggression. One major challenge been faced by Nigerians deserving for more attention as far as security, aping and conflict management is concerned is their effect on everyday life. Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon, D., (2015).

Since the advent of Information Technology, it is assumed to have been of greater advantages than the disadvantages most especially in the area of security. The major challenges

of security in Nigeria include; Terrorism by the Boko Haram in the Northern Nigeria, Kidnapping in the Southern part of Nigeria, armed robbery, pipeline vandalism caused by some Militant group known as the Niger Delta Avengers in the South-South region of the country and Herdsmen killings in some part of the country.

Therefore, the development of a Framework for National Defense Security Network using the Internet of Things approach would impact positively on National Security in Nigeria.
The aim of this study is to develop a Framework for National Defense Security Network using the Internet of Things approach, and the specific objectives include:

1. To find out the various ways in which Information Technology can impact positively on National Security;
2. To determine how National Security can be achieved through Information Technology with emphasis on Internet of Things.

The justification of this work is pre-determined by its objectives. It is however significant, as its developed framework and recommendations would be useful to the military, paramilitary, government, and societies facing enormous security challenges, especially in the face of present security challenges such as

- Insurgences – Boko haram, militants, religious or ethnic wars.
- Insecurity of lives – kidnapping, armed robbery, ritual killings.
- Corruption –Rigging of election, fake licenses, etc.
- Theft –Oil pipeline, public funds or piracy
- Information security – defacing government websites, theft of critical data, Denial of Service attacks.
- Insider threats - Moles within security agencies, disgruntled employees.
- Over-reliance on foreign technology.
- Inadequate regulations: e.g. cyber security and the most recent.
- Farmers/Herdsmen clashes.

One of the significance will broaden our horizon on the use of information technology (Internet of Things) to curb security challenges.

It will stand as a propelling force towards helping the government to achieve maximum success in safe guarding the territory of our dear nation for true development.
This research work is to develop a Framework for National Defense Security Network using the Internet of Things approach. The research intends to focus on Nigeria's security situation.

Related Literature

Here the paper is primarily looking at related works and other theories. A framework work with emphasis on an in-depth, conceptual clarifications and critical review of relevant and relating literatures, its strengths, weaknesses, and the applicability to the research work is done here.

We shall clarify some concepts and review some literature with regards to developing the subject in Nigeria:

- **National Security:** It means security from threats or attacks from people, organizations or countries that impact the well-being of a nation and its citizen as a whole rather than of any specific individuals or within the nation.

- **Information Technology:** This is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.

In May 1999 Nigeria's return to civil rule was accompanied with fresh hopes and latent optimism. This optimism is predicated on the fact that democracy would guarantee freedom, liberty, and equity and enhances security of lives and property, which would indeed repositions development trajectories to sustainability. Regrettably this optimism seems to be a mirage. Nigeria is presently rated as one of the poorest Nations in the world with debilitating youths' unemployment. For instance, Aganga (2009) observed that over ten million Nigerians were unemployed by March 2009 and unemployment is running at around 19.7 percent on average (National Bureau of Statistics Report 2009). This figure geometrically increases yearly with less realistic efforts by the managers of the state to abate the rampaging unemployment problem.

In Nigeria, like many other developing countries, about 70% of the population live in poverty (Otto and Ukpere, 2012). Majority of the population seem to lack access to pipe borne water, health care facilities, electricity and affordable quality education. Amidst these development challenges, the security situation in the country deteriorated drastically. Nigeria's return to democratic rule is threatened by security disaster. Arguably, series of resource based conflict (Niger Delta), ethno-religious crisis (Jos crisis), and communal conflicts persisted. The climax of these security threats is the insurgence of a group called Boko Haram in the Northern Nigeria. Thus, a considerable effort to end the violence and build a sustainable peace to steer the economy to sustainability seems far from realization. The basic questions are: why development has continued to elude Nigeria in spite of numerous amounts of human and material resources? To what extent has security crisis impacted or contributed to development crisis in Nigeria? Is Boko Haram really a threat to development in Nigeria? These pertinent but complex questions needed urgent attention especially now Nigeria is struggling to be among twentieth world developed countries in 202020.

Levels and Gravity of Security Crisis in Nigeria

Many people have done research on Implications for National Development in the discourse of security in Nigeria, Okorie (2011), Jega (2002), Salawu (2010), Onyishi (2011), Ezeoha (2011), Lewis (2002), have identified several causes of security crisis in Nigeria that pose grave consequences to national development. Chief among them is ethno-religious conflicts that tend to have claim many lives in Nigeria. By "ethnic-religious", it means a situation in which the relationship between members of one ethnic or religious and another of such group in a multiethnic and multi-religious society is characterized by lack of cordiality, mutual suspicion and fear, and a tendency towards violent confrontation (Salawu, 2010).

Since independence, Nigeria appears to have been bedeviled with ethno-religious conflicts. Over the past decades of her Nationhood, Nigeria has experience a palpable intensification of religious polarization, manifest in political mobilization, sectarian social movements, and increasing violence (Lewis 2002). Ethnic and religious affiliations determine who gets what in Nigeria; it is so central and seems to perpetuate discrimination. The return to civil rule in 1999 tends to have provided ample leverage for multiplicity of ethno-religious conflicts.

A work coauthored by Uhunmawuangho and Epelle, (2011), contended that democracy has increased the culture of impunity in some people while political differences are believed to have fuelled some of the violence that have erupted.

Theoretically what this is talking of is that poverty and unemployment increases the number of people who are prepared to kill or be killed for a given course at token benefit, Salawu, (2010).

It could predispose one to engaging in illicit activities that would undermine security of the environment.

Today in the country a systemic and political corruption seems to have added another dimension of violent conflicts which has relegated all the policies existing for security and eroded National values. Corruption is bad not because money and benefits change hands, and not because of the motives of participants, but because it privatizes valuable aspects of public life, bypassing processes of representation, debate, and choice (Thompson in Graflambsdorff 2001).

Boko Haram as a Threat to National Security in Nigeria

Boko Haram is a religious Islamic sect that came into the limelight in 2002 when the presence of the radical Islamic sect was first reported in Kanama (Yobe state) and also in Gwoza (Borno state). “Boko Haram,” which in the local Hausa language means “Western education is forbidden,” officially calls itself “Jama’atul Alhul Sunnah Lidda’wati wal Jihad,” which means “people committed to the propagation of the Prophet’s teachings and jihad”(Meehan and Speier 2011).

Seeing beyond religious explanations, Boko Haram could be arguably described as a “home-grown” terrorist group that romances with some desperate politicians in the North. There are conceptions that the sect enjoys effective support from some well-to-do individuals, religious leaders, allies, admirers of their ideology and highly placed politicians in the North who claim to be Nigerians but are clandestinely working against the State. For instance, Lister, (2012), observed that it is no longer a sect of Islamic fanatics but has the support of disgruntled politicians and their paid thugs (Adagba, Ugwu and Eme, 2012). Recently, revelations and security investigations into the activities of the sect tend to affirm that the group is also sponsored from within the country. This simultaneously transpire within the period when a serving Senator from the North is on trial for aiding the activities of Boko Haram. Thus, a senior official of Boko Haram allegedly granted an interview detailing how the sect had been on the payroll of a few governors of the North (Adagba etal, 2012). Thus, Boko Haram seems to be a destructive political tool with a cosmetic pretension of being religious.

This indiscriminate and sporadic bombing seem to make Northern Nigeria increasingly unsafe and has compelled most non-indigenes of the region to relocate especially the Igbos. This phobia of being attacked especially in cities like Kano, Kaduna, Maiduguri, Jalingo and Yola was responsible for the exodus of people from the North to other parts of the country as witnessed in the last few months. Not surprisingly, cities are experimenting with innovative approaches to preventing crime and countering extremism.

The most successful are improving intelligence gathering, strengthening policing and community outreach, and investing in new technologies to improve urban safety. Such cities are said to deploy 'agile security': data-driven and problem-oriented approaches that speed up decision-making and design in environmental changes to limit insecurity.

Detecting Crime before it Happens Using Agile Security

Agile security measures start with the premise that many types of crime, radicalization and terrorism are non-random and even predictable. With some exceptions, they tend to cluster in time, space and among specific population groups. The massive increase in computing power and advances in machine learning have made it possible to sift through huge quantities of data related to crime and terrorism, to identify underlying correlations and causes. The harnessing and processing of these data flows is crucial to enabling agile security in cities.

A precondition of agile security is connected urban infrastructure. When city authorities, private firms and civic groups have access to real-time data - whether generated by crime-mapping platforms, gunshot-detection systems, CCTVs or smart lights - they can get better at detecting crime before it occurs.

A growing array of crime prevention tools are not only connected to the cloud, they are also running off deep neural networks. As a result, public authorities are more easily reading license plates, running facial recognition software, mapping crime and terrorist networks and detecting suspicious anomalies. Some of these technologies are even processing data within the devices themselves, to speed up crime-fighting and terrorist prevention capabilities.

Another critical feature of agile security is leadership, especially in the law enforcement sector.

A growing number of metropolitan police are adopting problem-oriented policing practices and focusing on hotspots to deter and control crime. Across North America and Western Europe, police, counter-terrorism and emergency responders have set up fusion centres that stream multiple datasets from across a wide range of sources, from city sensors to cybercrime units in private companies. Across the Americas, the Middle East and Asia, police are also investing in machine learning tools to predict when and where crime will occur, known in the business as real-time epidemic-type aftershock sequence (ETAS) crime forecasting.

Defensive Architecture

To be truly effective, agile security requires making pinprick changes to the built environment to deter and design out threats of crime and terrorism. Deterrence may involve the use of defensive architecture such as smart cameras, street lights, anti-vehicular systems, blast walls and strategically placed forest canopy. The goal is to reduce the opportunities for perpetrators to target would-be victims or to do damage.

Efforts to design out threats of crime and terrorism also involve making physical changes to the environment, including building low-rise buildings, building green spaces and community centres, promoting mixed communities and targeting renewal measures in neighbourhoods that exhibit concentrated disadvantage. Investments in high-quality public goods and social cohesion can help prevent crime and radicalization.

A final requirement of agile security is that it avoids curbing civil liberties, whether intentionally or unintentionally. At a minimum, municipal governments need to find ways to consult with city residents to discuss the motives and implications of new technologies. This means undertaking consultations, especially in the most vulnerable communities.

Local authorities must also develop criteria related to personal data access, retention and redress, and encourage algorithmic transparency where possible.

An unmanned aerial vehicle (UAV), commonly known as a drone, is an aircraft without a human pilot aboard. UAVs are a component of an unmanned aircraft system (UAS); which

include a UAV, a ground-based controller, and a system of communications between the two. The flight of UAVs may operate with various degrees of autonomy: either under remote control by a human operator or autonomously by onboard computers.

Compared to manned aircraft, UAVs were originally used for missions too "dull, dirty or dangerous" for humans. While they originated mostly in military applications, their use is rapidly expanding to commercial, scientific, recreational, agricultural, and other applications, such as policing, peacekeeping, and surveillance, product deliveries, aerial photography, agriculture, smuggling, and drone racing.

UAV innovations started in the early 1900s and originally focused on providing practice targets for training military personnel. UAV development continued during World War I, when the Dayton-Wright Airplane Company invented a pilotless aerial torpedo that would explode at a preset time.

According to Bruce Schneier, 2015 all disruptive technologies upset traditional power balances, and the Internet is no exception. The standard story is that it empowers the powerless, but that's only half the story. The Internet empowers everyone. Powerful institutions in the Sahel of Africa might be slow to make use of that new power, but since they are powerful, they can use it more effectively. Governments and corporations have woken up to the fact that not only can they use the Internet; they can control it for their interests. Unless we start deliberately debating the future we want to live in, and the role of information technology in enabling that world, we will end up with an Internet that benefits existing power structures and not society in general.

There is need to create terrorists' online platform, a model that people can use to defeat terrorism. In the fight against terrorism, we should migrate from military analogue to digital to defeat terrorism. We should create terror channels in the Sahel with the vision to tackle terror and create innovative ideas in the fight against terrorism. With the use of social media and others, the internet is crucial if we must defeat terrorists in the Sahel of Africa on online first.

Despite increasing international recognition of the threat posed by terrorists' use of the Internet in recent years in the Sahel of Africa, there is currently no global instrument specifically to address this pervasive facet of terrorist activity. Moreover, there is limited online action to defeat, restrict and control terrorists through the use of the Internet in the Sahel. Terrorism, in all its manifestations, affects us all. The use of the Internet to further terrorist purposes disregards national borders, amplifying the potential impact on victims. The United Nations Security Council recently unanimously backed a West African force which is not enough to combat militant groups in the Sahel region. The internet is crucial in the fight against terrorists in Africa.

Military action alone will not defeat terrorism in Africa. The United Nations and government at all levels in the Sahel of Africa should engage internet providers to streamline and monitor streaming issues online. There must be gathering of intelligence of streaming online issues in Africa. United Nations must defeat terrorists online first before it engages terrorists in military confrontation. Experts must be recruited and trained for streaming intelligence gathering online in the Sahel of Africa. The fight against terrorism starts from the internet.

We must collectively defeat terrorism online before any military action. Intelligence gathering of streaming videos, blogs, text messages, internet relay, chat channels and others in Sahel of Africa are crucial in the fight against terrorists in Africa. As part of new approach to fight terrorism, African countries should invest in sophisticated surveillance technology and share information on a range of law enforcement and security matters, including terrorism. African

countries should been exchanging and sharing information on terrorism. African countries should share intelligence on terror cases tied to Africa with United Nations Security Council -- evidence like internet addresses used in a suspected identity of terror attack, "addresses that are traced to the African terrorists, for both the suspected attackers and potential victims." There should be special internet security team aimed at West African networks and apparently originating from IP addresses in Africa. There should be Office of Internet Security in West Africa.

The fight against terror in West Africa should involve all areas of the drone dome, Internet and online services, including social networking venues, websites that post terror activities, Internet news groups and Internet Relay Chat channels.

Methodology

A proposed model designed for the Proposed Internet of Things (IoT) Framework for National Defense and Security

Roadmap of the Devices and Applications in the Proposed Internet of Things (IoT) Security Framework and the overview of the most promising IoT scenarios, are depicted in Figure 1.

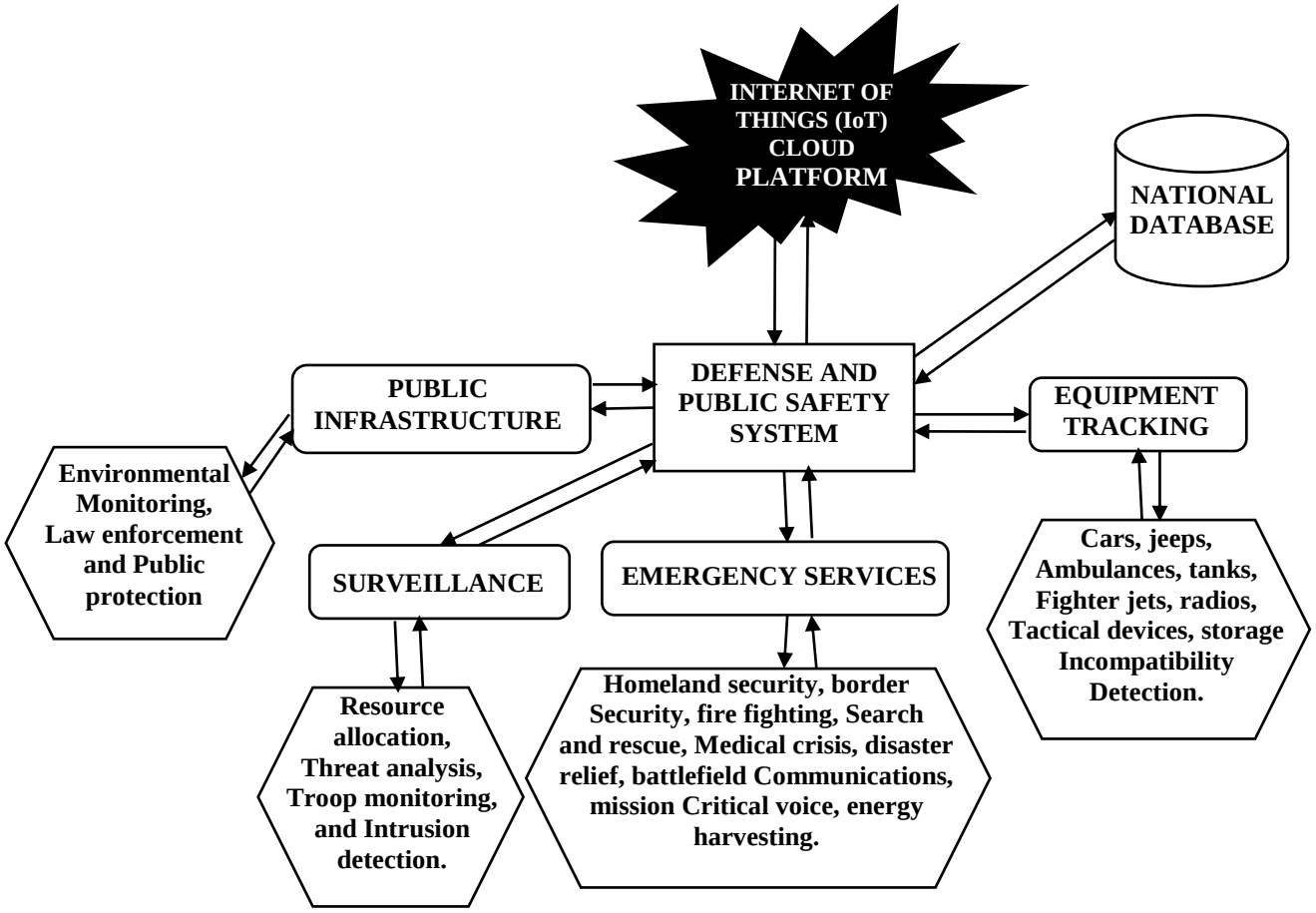

Figure 1: Roadmap of the Devices and Applications in the Proposed Internet of Things (IoT) Security Framework.

Target Scenarios for Mission-Critical IoT

Until now, the deployment of IoT-related technologies for defense and public safety has been essentially focused on applications for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), and fire-control systems. This is driven by a predominant view that sensors serve foremost as tools to gather and share data, and create a more effective Command and Control (C2) of assets. IoT technologies have also been adopted in some applications for logistics and training, but their deployment is limited and poorly integrated with other systems.

Besides, IoT functionalities are useful for establishing advanced situational awareness in the area of operations. Commanders make decisions based on real-time analysis generated by integrating Sensors data from unmanned sensors and reports from the field. These commanders benefit from a wide range of information supplied by sensors and cameras mounted on the ground, and manned or unmanned vehicles or soldiers. These devices examine the mission landscape and feed data to a forward base. Some of the data may be relayed to a Command Center where it is integrated with data from other sources.

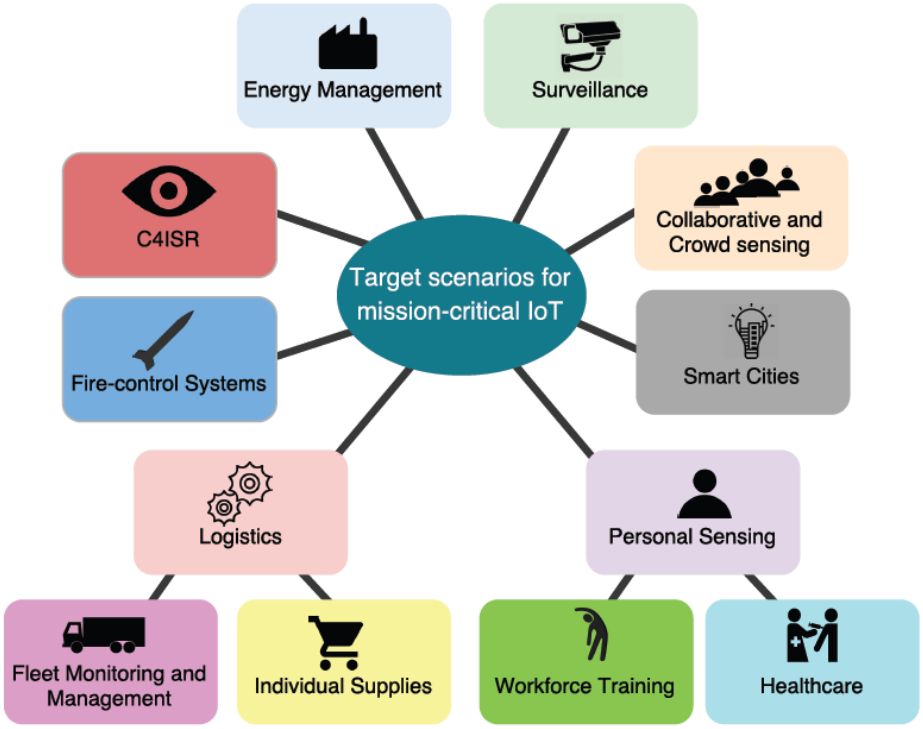

Figure 2. Promising target scenarios for defense and public safety.
Source: www.mdpi.com/journal/sensors.

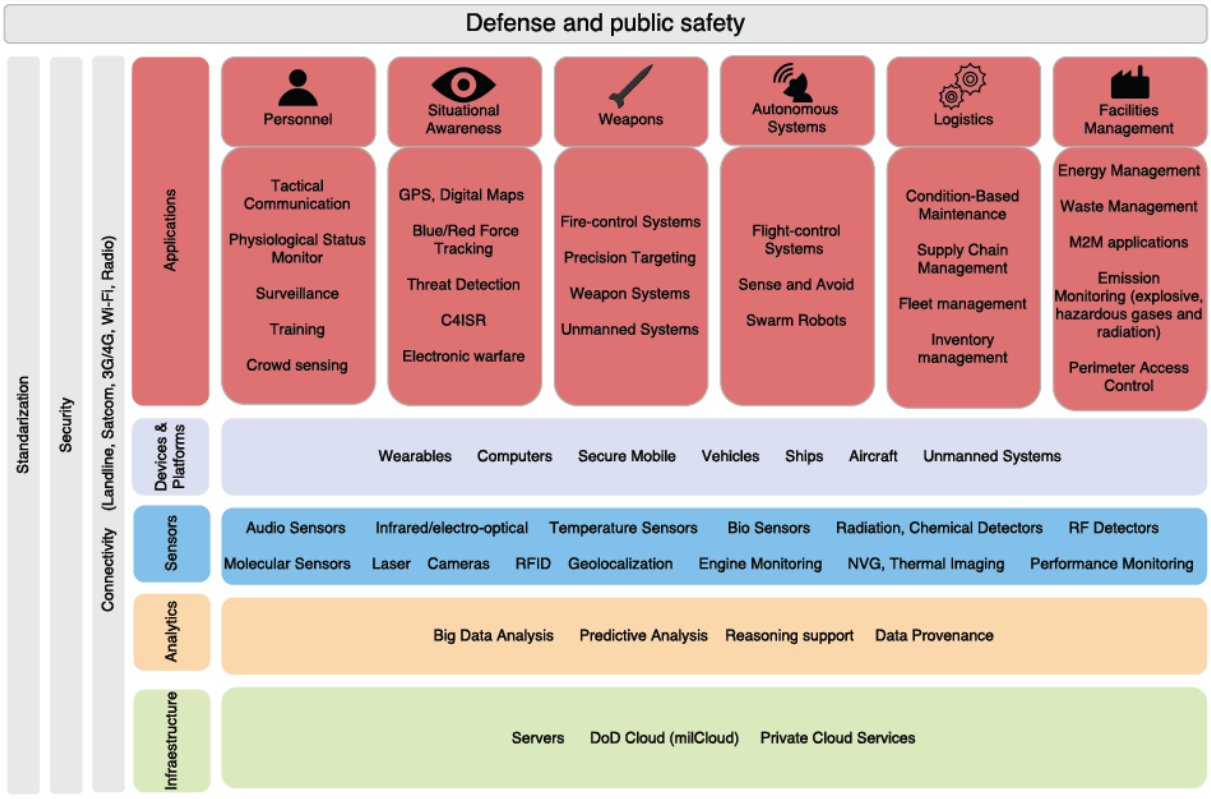

Figure 3: Defense and public safety technology stack.
Source: www.mdpi.com/journal/sensors.

C4ISR

C4ISR systems use millions of sensors deployed on a range of platforms to provide advanced situational awareness. Radar, video, infrared or passive RF detection data are gathered by surveillance satellites, airborne platforms, UAVs (Unmanned Aerial Vehicles), ground stations, and soldiers in the field. These data are delivered to an integration platform that analyzes them and delivers information up and down the chain of command. These platforms provide a Common Operational Picture (COP) allowing for enhanced coordination and control across the field.

High-level military echelons are provided with comprehensive situational awareness through central operations centers, which receive data feeds from platforms. Lower levels (i.e., platoon, soldiers) also have access to the data in their area. In the case of combat pilots, they receive prioritized data feeds integrated with data from their own sensor systems.

Fire-Control Systems

In fire-control systems, end-to-end deployment of sensor networks and digital analytics enable fully automated responses to real-time threats, and deliver firepower with pinpoint precision.

Munitions can also be networked, allowing smart weapons to track mobile targets or be redirected in flight. Prime examples are the Tomahawk Land Attack Missile (TLAM) and its variants, navy's precision strike standoff weapons for attack of long range, medium range and tactical targets. Furthermore, the military has invested in the use of long endurance UAVs to engage high-value targets and introduce multi-UAVs applications.

Logistics

Logistics is an area where multiple low-level sensors are already being used in defense. Currently, their deployment remains constrained to benign environments with infrastructure and human involvement. The military can deploy some IoT technologies in non-combat scenarios in order to improve back-end processes. For example, RFID tags would be used to track shipments and manage inventories between central logistics hubs.

In the following subsections, we describe examples that belong to two main categories: fleet management and individual supplies.

Fleet Monitoring and Management

Fleet monitoring can be represented by aircraft and ground vehicle fleets with on-board sensors that monitor performance and part status. For example, they track vehicle status and subsystems, and indicate when resupplying low-stock items (i.e., fuel or oil) is needed. Sensors would issue alerts, potentially reducing the risk of fatal failures. The aim is to facilitate condition-based maintenance and on-demand ordering of parts, reduce maintenance staff, and decrease unanticipated failures or unnecessary part replacements. Although IoT deployment carries up-front costs, it can enable significant long-term savings by transforming business processes across logistics. Defense has an opportunity to take advantage in the auto and industrial sectors, and exploit performance data on existing data links, like Blue Force Tracker transponders (already in place on many military vehicles) to limit new security risks. By extension, IoT-connected vehicles could also share information, for example, about available spare parts.

Real-time fleet management includes geolocation, status monitoring, speed and engine status, total engine hours, fuel efficiency, and weight and cargo sensors. Besides, when tracking shipments, the position and status of the containers can be monitored to identify potential problems.

Regarding aircraft, modern jet engines are equipped with sensors that produce several terabytes of data per flight. This information combined with in-flight data can improve engine performance to reduce fuel costs, detect minor faults or shorten travel duration . Furthermore, it enables preventive maintenance resulting in a long lifecycle (slowing or preventing breakage) and less downtime spent in repairs. The flight data can be tracked in real-time by operators and analysts on the ground.

Individual Supplies

The deployment of RFID tags, sensors and standardized barcodes allow for tracking individual supplies. IoT provides real-time supply chain visibility (whether it is being shipped, transferred, deployed, consumed), and allows the military to order supplies on demand and simplify logistics management for operational units. This smarter procurement of goods avoids delays caused by out-of-stock parts or inventory-carrying costs. Likewise, it can increase accountability, enhance mission reliability, reduce losses and theft of military equipment, and help with the time criticality on the military maintenance.

At the soldier level, tracking is useful in order to follow a proactive approach to logistics or to meet operational requirements. Soldier material (e.g., water, food, batteries or bullets) can be monitored with alerts issued for a necessary resupply. Aggregate data (e.g., groups of soldiers, companies, battalions, etc) might also be studied for further enhancements of supply

for tactical and emergency units. The analytics might be focused on considering environment, body type, and consumption, among other variables.

Smart Cities Operations

In denied area environments, existing IoT infrastructures could be reused in military operations. Ambient sensors can be used to monitor the existence of dangerous chemicals. Sensors monitoring human behavior may be used to assess the presence of people acting in a suspicious way. Leveraging information provided by pre-existing infrastructures might be critical. Several security issues may arise, such as equipment sabotage or deceptive information. The authors of categorize such attacks into four areas: (1) system architecture, firewalls, software patches; (2) malware, security policies and human factors; (3) third-party chains and insider threat; and (4) database schemas and encryption technologies.

Personal Sensing, Soldier Healthcare and Workforce Training

Body-worn devices are increasingly available, fitness trackers enable monitoring of physical activity along with vital signs. This information has an obvious value for the users, but there is also a significant potential in examining aggregate values of communities. Body-worn sensors, when deployed on a community scale, offer information to support C4ISR. We have to distinguish between participatory and opportunistic sensing. The last one may be of particular relevance for under-cover personnel involved in reconnaissance missions in urban environments. Technologies for monitoring both workforce and their surroundings could aid when inferring physical or psychological states as well as assessing the risk of internal injury based on prior trauma. Soldiers can be alerted of abnormal states such as dehydration, sleep deprivation, elevated heart rate or low blood sugar and, if necessary, warn a medical response team in a base hospital. These wide range of health and security monitoring systems, enables an effective end-to-end soldier health system, including re-provisioning of health services when needed.

The previously referred applications, and others yet-to-be imagined, could be part of the equipment of the soldiers of the future. A likely evolution of such equipment can be seen in Figure 4 below.

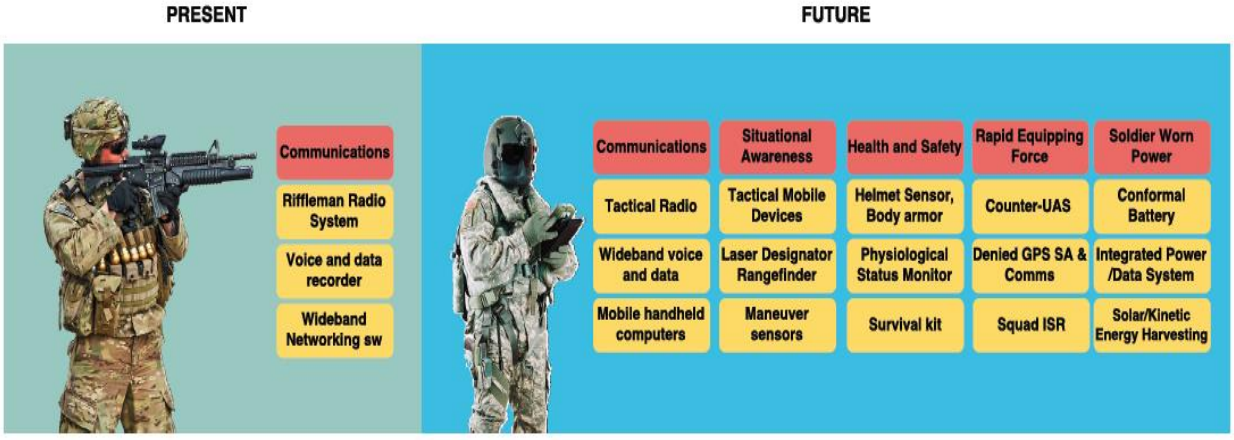

Figure 4: Soldiers of today and the future.
Source: www.mdpi.com/journal/sensors.

Collaborative and Crowd Sensing

Collaborative sensing involves sharing sensing data among mobile devices combined with robust short range communications. IoT nodes would be able to utilize placement or other sensors to supplement their own sensing methods. Once security issues (such as trust and authentication) are resolved, the information can be made available to the users. Long-term maintenance of IoT services yield multiple benefits, such as trend or fault detection. Individual sensor parameters must be considered to assign a particular relevance to a given reporting device and its feedback can be improved upon data fusion approaches.

IoT can ease ad-hoc mission-focused Intelligence, Surveillance and Reconnaissance (ISR) via pairing sensors with mission assignments. Thus, sensors and sensor platforms would not have to be burdened with excessive equipment to handle mission scenarios on their own.

Surveillance

Security cameras and sensors, combined with sophisticated image analysis and pattern recognition software, ease remote facility monitoring for security threats. In the case of marine and coastal surveillance, using different kinds of sensors integrated in planes, unmanned aerial vehicles, satellites and ships, make possible to control the maritime activities and traffic in large areas, keep track of fishing boats, and supervise environmental conditions and dangerous oil cargos.

Other examples can be the monitoring of hazardous situations: combustion gases and preemptive fire conditions to define alert zones, monitoring of soil moisture, vibrations and earth density measurements to detect dangerous patterns in land conditions or earthquakes, or distributed measurement of radiation levels in the surroundings of nuclear power stations to generate leakage alerts.

Operational Requirements

The exceptional advantage of this paper is that it is cloud based security that enhances the current military has unique operational requirements. Security, safety, robustness, interoperability challenges, as well as bureaucratic and cultural barriers, stand in the way of the broad adoption of new IoT applications. In this Section a set of operational requirements grouped by capabilities (represented in Figure 5) are assessed in order to cover the scenarios previously discussed.

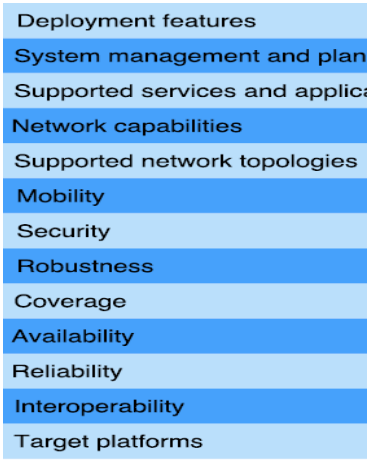

Figure 5: Operational requirement and Capabilities assessed to cover mission-critical scenarios. Source: www.mdpi.com/journal/sensors.

Implementation and Analysis

Military Architecture with Six Layers

A generic IoT architecture is presented, and it introduces an IoT daemon consisting in three layers with automation, intelligence and zero-configuration: Virtual Object, Composite Virtual Object, and Service layer. An example of the possible military architecture to be used can be seen in Figure 6.

The process of sensing consists in collecting data from objects within the network, and sending them back to a data warehouse, a database or a cloud system, to be analyzed and act. Four main classes of IoT services can be categorized:

i. Identity-related services: these services are employed to identify objects, but are also used in other types of services.
ii. Information Aggregation services: these services collect and summarize raw measurements.
iii. Collaborative-Aware services: these services act on top the Information Aggregation services and use the obtained data to make decisions.
iv. Ubiquitous services: these collaborative-aware services function anytime to anyone, anywhere.

Most existing applications provide the first three types of services. The ultimate goal are the ubiquitous services. Semantic analysis is performed after sensing to extract the corresponding knowledge. It includes discovering, resources usage and information modeling. Thereafter, recognizing and analyzing data to take proper decisions within the service. This is supported by semantic web technologies such as the Resource Description Framework (RDF), the Web Ontology Language (OWL), or Efficient XML Interchange (EXI), adopted as a recommendation.

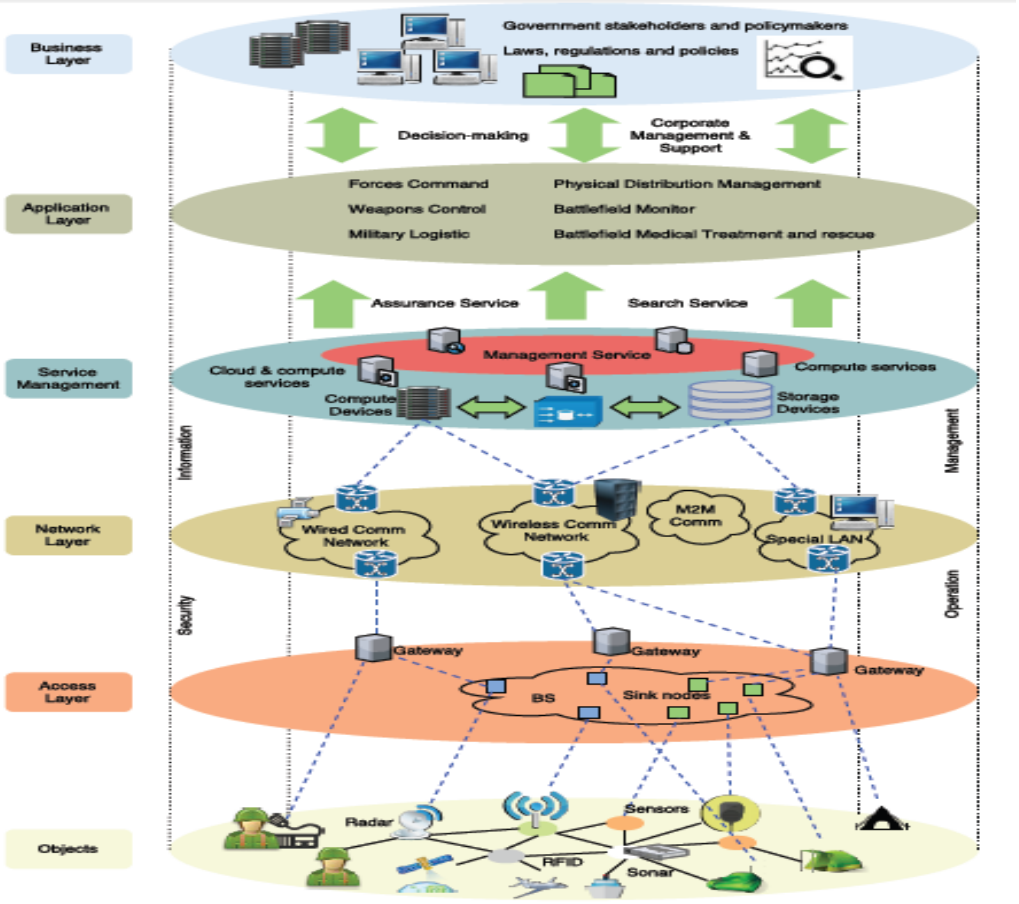

Figure 6. Example of military architecture with six layers.
Source: www.mdpi.com/journal/sensors.

Conclusion

This article examined how the defense industry can leverage the opportunities created by the commercial IoT transformation.

In order to perform the study, we propose significant scenarios such as: C4ISR, fire-control systems, logistics, smart cities operations, personal sensing, soldier healthcare and workforce training, collaborative and crowd sensing, energy management, and surveillance.
Based on the operational requirements, we proposed the architecture, technologies and protocols that address the most significant capabilities.

Commercial IoT still faces many challenges, such as standardization, scalability, interoperability, and security. Researchers working on defense have to cope with additional issues posed by tactical environments, and the nature of operations and networks. There are three main differences between Defense/PS IoT and the present method of combating warfare: the complexity of the deployments, the resource constraints (basically the ones related to power consumption and communications), and the use of centralized cloud-based architectures.

Beyond the earliest military IoT innovations, complex battlefields will require additional research advances to address the specific demands.
We can conclude that the military and first responders should establish a testbed for identifying and experimenting with technologies that could remodel the way missions are accomplished, and which would serve as a link between warfighters in the field and IoT developers.

Recommendations

The following recommendations were obtained from the analysis of the previous sections:

i. Introduce rapid field testing (testbed): the military should consider creating a dedicated technology comprising military personnel in a live training environment to experiment with technologies and get real end-user feedback early in the development process.
ii. The military can to a certain extent, take advantage of civilian mobile waveforms such as 4G/5G LTE. Nevertheless, those advances will need to be paired with military-specific communications architectures (e.g., multiband radios with scarce bandwidth, MANET topologies and defensive countermeasures).
iii. Use Platform as a Service (PaaS) to deliver web-based services without building and maintaining the infrastructure, thereby creating a more flexible and scalable framework to adjust and update the systems.
iv. Realize a comprehensive trust framework that can support all the requirements of IoT for the military. In military environments, policies will likely be contextual and transient, conflated by inter-organizational and adversarial interactions.

References

Alderson, A. (2015).Sports tech—Fitness trackers. Eng. Technol. 10, 84–85.

Atzori, L.; Iera, A.; Morabito, G.(2010). The internet of things: A survey. Comput. Netw. 54, 2787–2805.

Business Insider (BI) Intelligence (2015). The Internet of Things: Examining How the IoTWill Affect theWorld; Technical Report; Business Insider: New York, NY, USA.

Calhoun, G.L.; Draper, M.H. (2015). Display and Control Concepts for Multi-UAV Applications. In Handbook of Unmanned Aerial Vehicles; Springer: Dordrecht, The Netherlands; pp. 2443–2473.

Chang, J.M.; Ho, P.C.; Chang, T.C. (2014). Securing BYOD. IT Prof. , 16, 9–11.

Ericsson. Ericsson Mobility Report on the Pulse of the Networked Society; Technical Report; Ericsson: Stockholm, Sweden, November 2015.

Fraga-Lamas, P., et al (2016). A Review on Internet of Things for Defense and Public Safety. Sensors 2016, 16, 1644; doi:10.3390/s16101644. www.mdpi.com/journal/sensors.

Fraga-Lamas, P., et al (2016). Evolving Military Broadband Wireless Communication Systems: WiMAX, LTE and WLAN. In Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23–24 May 2016; pp. 1–8.

Instrumented-Multiple Integrated Laser Engagement System (I-MILES). (2016). Available online: https://www.cubic.com/Global-Defense/Training-Systems-and-Solutions/Ground-Combat-Training/Multiple-Integrated-Laser-Engagement-System .

International Telecommunication Union Radiocommunication Sector (ITU-R) (2015). Radiocommunication Objectives and Requirements for Public Protection and Disaster Relief (PPDR); Technical Report ITU-R M.2377-0; ITU: Geneva, Switzerland.

Jaimes, L.G.;Vergara-Laurens, I.J.; Raij, A. A (2015). Survey of incentive techniques for mobile crowd sensing. IEEE Internet Things J. 2, pp. 370–380.

Kantarci, B.; Mouftah, H.T. (2014). Trustworthy sensing for public safety in cloud-centric internet of things. IEEE Internet Things J., 1, pp. 360–368.

Lee, H.; Yoo, S.; Kim, Y.W. (2016). An energy management framework for smart factory based on context-awareness. In Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 31; pp. 685–688.

Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; Aharon, D(2015). The Internet of Things: Mapping the Value beyond the Hype; Technical Report; McKinsey Global Institute: Washington, DC, USA, .

Shunk, D. (2015). Ethics and the enhanced soldier of the near future. Mil. Rev. 2015, 95, 91–98.

U.S. Department of Defense (2015). Annual Energy Management Report; Technical Report; Office of the Assistant Secretary of Defense (Energy, Installations, and Environment): Washington, DC, USA,.

Wang, P.; Ali, A.; Kelly,W. (2015). Data security and threat modeling for smart city infrastructure. In Proceedings of the International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7; pp. 1–6. 61. Cirani, S.; Picone, M. Wearable computing for the internet of things. IT Prof. 17, 35–41.