sciendo

Land Forces Academy Review
Vol. XXVI, No. 4(104), 2021

EMERGING TECHNOLOGIES AND NATIONAL SECURITY: THE IMPACT OF IoT IN CRITICAL INFRASTRUCTURES PROTECTION AND DEFENCE SECTOR

Petrișor PĂTRAȘCU
"Carol I" National Defence University, Bucharest, Romania
patrascupetrisor@yahoo.com

ABSTRACT

Today's society is increasingly dependent on the facilities offered by new technologies. Thus, emerging technologies play a key role in people's lives, as well as in the functionality and protection of infrastructures that ensure the availability of goods and essential services. Therefore, the exploitation of emerging technologies has become necessary even in the most sensitive sectors of activity, which have significant implications for ensuring national security. Artificial intelligence, Internet of Things, Big Data, robots, drones, machine learning and many more are feasible solutions for the dynamics and optimization of the environment in which they are integrated. The defence sector has also implemented a number of new technologies, integrating state-of-the-art digital systems into the communications architecture that are necessary for carrying out the military operations in a modern battlefield. Although, emerging technologies have a certain degree of uncertainty, they have already been adopted, and today premises are moving towards further innovation and development of emerging technologies by manufacturers that have an increasing interest to integrate them in the key areas of activity. This article provides an analysis of the impact of Internet of Things technologies on national security, in terms of critical infrastructure protection and the defence sector.

KEYWORDS: emerging technologies, IoT, critical infrastructures protection, defence sector

1. Introduction

Nowadays, emerging technologies have become topics of interest in many areas of activity, including essential services. Therefore, the implementation of such technologies in sensitive areas of national security is a real challenge even justified in terms of the defining characteristics of emerging technologies such as for instance the inaccuracy of measuring technology maturity over time. Although there is a certain degree of uncertainty, from the perspective of national security, emerging technologies must be seriously considered both as real opportunities and potential threats. I will analyse further in this article the Internet of Things (IoT) technologies as emerging technologies and their impact on national security from the perspective of critical infrastructure protection and the defence sector. Therefore, the analysis is based on the following questions:

- Are IoT emerging technologies that impact on national security?
- What is the impact of IoT on the functionality and protection of national critical infrastructures?
- What are the adoption of IoT for the defence sector?

DOI: 10.2478/raft-2021-0055
© 2017. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.

The answers to these questions will be found in three sections, using both the analysis of the literature and the transdisciplinary approach in the areas mentioned above.

2. IoT – Emerging Technologies in the Context of National Security

Emerging technologies are identified by a wide range of evolving and disruptive innovations that are relevant to national security through the ability to amplify or impede military activities and other specific intelligence activities in the field of national security (Analytic Exchange Program, 2018). The relevance of technology for security is multiple, and the control of technology as an instrument of national security strategies is particularly important (Mallik, 2004). According to some authors, technological innovation has already surpassed the ability of states to manage the latest developments and potential effects of emerging technologies. In this situation, the solution to manage emerging technologies may arise from new multilateral approaches, involving several actors to develop technical and regulatory solutions (Kavanagh, 2019). In 2015 several studies highlighted that the time of emerging technologies appearance was uncertain and ambiguous. The main features of emerging technologies were also highlighted: radical novelty, relatively fast growth, coherence, prominent impact, uncertainty and ambiguity. Moreover, the impact of these technologies was transposed into the future (Rotolo, Hicks & Martin, 2015). Today, according to Gartner, there are three themes of emerging technology trends, depending on their potential benefits and expected impact. The first theme, Engineering Trust, is based on security, reliability and working practices. The second theme, Accelerating Growth, refers to initiatives that provide opportunities for organizations. In this case, the technological risk must be correlated with the economic risk, in order to meet the short-term objectives of the organization. The third theme, Sculpting Change, supports the fact that risk can be mitigated by influencing change. Thus, the solution is for this change to be accepted as disruptive and for emerging technologies to be held for shaping change and therefore avoiding chaos (Gartner, 2021).

The evolution of digital technologies has made possible the rapid exchange of information for people and organizations, in almost all geographical locations. The growing interest in innovation, in line with the needs of today's society, have fully contributed to the emergence of the digital world. The Internet, through its facilities, has become an essential service in many areas of activity. Today, the lack of the Internet in various situations raises questions, makes communication difficult, disrupts the conduct of activities and generates various effects, especially for those who use it in carrying out their activities. New digital technologies on the other hand are fully contributing to meeting the concrete daily needs of both people and society. In this sense, the artificial intelligence, the Internet of Things, Big Data, Cloud Computing, blockchain, quantum computing, 5G, robotics, drones, 3D printing and others represent the innovative technologies that are part of the reality we live.

All these technologies mentioned above are also called frontier technologies that benefit from digitalization and connectivity, thereby amplifying their impact when combined (UNCTAD, 2021). Therefore, digital interactions frequently involve large amounts of data, leading to the development of Big Data tools and techniques. The huge volume of data supported by Cloud Computing, the outsourcing of software and hardware components and process automation have significantly contributed to the development of IoT technologies (Shnurenko, Murovana & Kushchu, 2020).

At the same time, a smart IoT system has artificial intelligence that serves the actual goal of automation and adaptation (Ghosh, Chakrabort & Law, 2018). The importance of artificial intelligence for cyber security can also be mentioned here, which can be used for the development of complex algorithms to protect IoT against cyberattacks, including those attacks that are using artificial intelligence (Kuzlu, Fair & Guler, 2021).

In recent years, the rise of IoT technologies has managed to change paradigms and strategies; at first they have been used for smart homes or cars, and now they are used in the most important domains of activity. Thus, IoT is classified as an emerging technology and considered a particularly important tool in combination with other technologies. Within a bibliometric analysis carried out during 2006-2015, the authors (Li, Porter & Suominem, 2018) have analysed, compared and identified IoT as an emerging technology, at the expense of disruptive technology.

The implementation of IoT in both the critical infrastructure sectors and the defence sector, is useful in supporting the achievement of objectives, but there always will be inevitable risks that may affect national security. Therefore, the implementation of IoT technologies in the two areas that are essential for national security has to be a complex process, based on surveys and in-depth research and analysis.

3. The Impact of IoT on the Functionality and Protection of National Critical Infrastructures

Each state protects its critical infrastructure that provides vital goods and services to society. Thus, critical infrastructures are essential systems in the context of national security. For example, the EU approach for the identification, designation and protection of critical infrastructures provide two directions. The first direction is a common one, addressing two European critical infrastructure sectors, namely energy and transport sectors, and the second is an individual one, in which EU Member States establish their national critical infrastructure sectors, such as: health, national security, financial-banking, food and agriculture, information and communication technology, administration and others. There are also two critical infrastructure sectors at national level: energy and transport. In this context, the protection of critical infrastructure, by EU Member States is very important for ensuring national security. Currently, emerging technologies are used in critical infrastructure in order to streamline functionality and to ensure protection against any physical and cyber threats.

Next, I will pay attention to some examples through studies undertaken by several authors on the implementation of IoT technologies in various fields of activity, thus highlighting the importance and need for the adoption of such technologies for the critical infrastructure sectors and subsectors. In the medical field, by adopting advanced technologies, people's health problems can be easily managed and controlled. Through IoT, the vital functions of patients can be monitored anywhere in the world, efficient synchronization between ambulances and the traffic light system can be achieved, intelligent hospitals can be developed, the information exchange between patients and medical staff can be more efficient and telemedicine can sustained, as transmission of information is less expensive than transporting people (Gamage & Madushan, 2020). The development of IoT solutions improves medical assistance, meets the requirements of medical staff, contributes to patient safety and increases operational efficiency in the medical industry (Dang, Piran, Han, Min & Moon, 2019). Also in relation to the medical sector, several authors have analysed the role and importance of IoT during the SARS-COV-2 pandemic.

In fact, the pandemic has been, is and will be a threat to people and society, and for the critical infrastructure, regardless of industry, it is an event transposed into a threat scenario integrated into the structure of the operator's security plan. A group of authors (Nasajpour, Pouriyeh, Parizi, Dorodchi, Valero & Pouriyeh, 2020) have studied a series of implementations of IoT technologies in the fight against COVID-19, dividing them into three phases: diagnosis, quarantine and post-recovery. Thus, portable devices, drones, robots and smartphone applications, contribute significantly to reducing infections, hospitalizations and mortality. Another sector where IoT devices fully justify their usefulness is transportation. Whether we are analysing air, road, naval, rail or urban transport, intelligent systems are increasingly present. Some specialists note the benefits to the traffic system if IoT is integrated into intelligent transport systems (Chand & Karthikeyan, 2018). The usefulness of IoT applications can be seen in traffic monitoring, car theft detection, permanent toll collection system, air pollution monitoring or even the transportation guidance and control systems (Kumar & Dash, 2017). Another sector that has begun to appreciate the IoT technologies is agriculture. If we take into account the estimate that the world population will grow by 25 % in 2050 compared to the current number, as well as the estimate that the urban population will reach 70 %, then food production should double. In addition to food, agricultural crop production is becoming critical for industry and for the economy of many countries. Also, the use of agricultural crops for the production of biofuels and bioenergy adds pressure to the production of agricultural resources. All these agricultural resources are confined to the limitations of agricultural areas, such as temperature, topography, climate, and soil quality. Experts emphasize the role of different technologies, especially IoT, in achieving a more efficient and smarter agriculture in order to meet future expectations. To this purpose, UAV sensors, cloud-computing, communication technology, remote sensing via satellite systems, are elements that can revolutionize the agricultural industry (Ayaz, Ammad-Uddin, Sharif, Mansour & Aggoune, 2019). As for the financial-banking sector, IoT is a growing source of Big Data in terms of information obtained from the physical world, used for financial-banking services, risk management, insurance purposes etc. According to a group of authors (Khanboubi, Boulmakoul & Tabaa, 2019), highlight IoT-based digital trends that have a direct impact on financial services and set out two approaches to these trends with regards to the future of banks. The first approach refers to the replacement of traditional banks, and the second approach is aimed at completing the banks by transforming them into more connected and digitized infrastructures. These are just a few examples of adopting IoT solutions in various critical infrastructure sectors. Moreover, IoT stands next to artificial intelligence, Big Data, cloud computing at the level of cutting-edge technologies that have changed the world.

4. The Impact of IoT Adoption on the Defence Sector

In general, emerging technologies are questionable when they are about to be adopted for the defence sector. The persistence and interest of manufacturers to develop emerging technologies in the defence sector is increased. Instead, decision-makers and military experts appreciate the potential benefits, but also have reservations about their specific vulnerabilities and risks. However, for many years, the defence sector has shown a growing interest in adopting IoT solutions.

The use of IoT offers many benefits including increased efficiency, greater automation, reduced human error, low costs and a large amount of data collected and analysed, even if there have been implemented much more stringent privacy policies and security standards the defence

sector (Crelier, 2019). At first, they have been tested mainly for the non-combat areas, for logistics, communications, medical or research and surveillance systems. Subsequently, according to a group of specialists (Fraga-Lamas, Fernández-Caramés, Suárez-Albela, Castedo & González-López, 2016), these solutions cover a much larger area, including the combat zone, being developed for C4ISR systems, fire control systems, smart city-specific operations and others.

Currently, if we look from the perspective of operational areas, there is a growing interest in the adoption of IoT in each of the five areas – terrestrial, air, maritime, space, cyberspace, including a holistic approach, such as Joint all Domain Operation (JADO). Moreover, the interconnectivity and compatibility with other emerging technologies further increases the interest for the implementation IoT. The role artificial intelligence in IoT technologies is an eloquent example. Data from sensors and other smart devices is a tremendous amount of information, which is analysed, sorted, filtered and processed, some of them already using the Big Data concept. The results of these processes are getting implemented into both predictable and actionable intelligence, in accordance with the requirements of strategic, operational and tactical level information.

Also, artificial intelligence (AI) represents a topical issue for the defence sector. The unique features of AI are particularly important for national security. Therefore, AI may be integrated into many applications, thereby improving IoT in order to optimize performance (Sayler, 2019). Artificial intelligence algorithms used in military systems in areas such as Big Data, logistics, object detection and cybersecurity reveal particularly important areas of the defence sector, with a key role in ensuring national security and deployment of a military operations in the modern warfare (Bistron & Piotrowski, 2021). For example, the logistics field includes a large amount of data and information on transport, distribution, equipment, maintenance, ammunition and much more. Some authors note that the IoT can reduce the response time of providing logistics and also improve the speed of actions (Wang, Cao, Shen & Zheng, 2018). Other authors propose a conceptual model called the Military Supply Chain Cyber Implications Model (M-SCCIM), based on IoT technologies and smart contracts to facilitate supply chain activities (Sobb & Turnbull, 2020). Smart contracts are programs stored on a blockchain that run only when predetermined conditions are met.

Therefore, IoT solutions are diverse and provides benefits to military activities, being used in the most important fields, both in time of peace and in warfare. But in return, there are many risks and vulnerabilities caused by the integration of such technologies in the defence sector. The defence infrastructure sector represents a target for cyber attackers, especially those supported by state and non-state actors. Their cyber-attacks aim, on the one hand, to disable and disrupt services, and on the other hand, to remain as long as possible in software systems and related networks, without being discovered, in order to steal as much data and classified information as possible. Consequently, cybersecurity measures are essential in the defence sector, in order to ensure the confidentiality, availability and integrity of IoT technologies.

5. Conclusions

In general, emerging technologies have a significant impact on the sectors where they have been implemented, including on critical infrastructure and the defence sector. First, the benefits of emerging technologies that are already being exploited are greatly appreciated and many activities are being automated and optimized. Secondly, the expected advantages of the technologies that are in the process of designing and testing represent a real interest for national security,

being classified as new technologies that can influence essential goods and services and the conduct of military operations in the modern warfare. Third, the interoperability and connection of several types of emerging technologies greatly increase the functionality and protection of critical infrastructure, as well as superiority in the planning and conduct of military operations. Moreover, the architecture of military systems and networks could play a critical role in the IoT security challenge even though some specific properties of IoT are already successfully implemented in critical infrastructures. Last but not least, the adoption of IoT technologies in the defence sector and critical infrastructure should consider the associated security risks so that cyber-attacks do not be a threat to national security.

REFERENCES

Analytic Exchange Program (2018). *Emerging Technology and National Security*, 6, available at: http://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf.

Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A., & Aggoune, E.M. (2019). Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk. *IEEE Access, Vol. 7*, 129551-129583.

Bistron, M., & Piotrowski, Z. (2021). Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens. *Electronics, Vol. 10, Issue 7*, 871. https://doi.org/10.3390/electronics10070871.

Chand, V., & Karthikeyan, J. (2018). Survey on The Role of IoT in Intelligent Transportation System. *Indonesian Journal of Electrical Engineering and Computer Science, Vol. 11, No. 3*, 936-941.

Crelier, A. (2019). *Trend Analysis: The Challenges of Scaling the Internet of Things*. Center for Security Studies (CSS), ETH Zurich, available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190827_AC_TA_The%20Challenges%20of%20Scaling%20the%20Internet%20of%20Things%20Cyber-Reports.pdf.

Dang, L.M., Piran, M.J., Han, D., Min, K., & Moon, H. (2019). A Survey on Internet of Things and Cloud Computing for Healthcare. *Electronics, Vol. 8, Issue 7*, 768.

Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors, Vol.16, Issue 10*, 1644, https://doi.org/10.3390/s16101644.

Gamage, R., & Madushan, R. (2020). A Review on Applications of Internet of Things (IOT) in Healthcare. *Journal of the American Society for Information Science and Technology*.

Gartner (2021). *3 Themes Surface in the 2021 Hype Cycle for Emerging Technologies*. Available at: https://www.gartner.com/smarterwithgartner/3-themes-surface-in-the-2021-hype-cycle-for-emerging-technologies.

Ghosh, A., Chakrabort, D., & Law A. (2018). Artificial Intelligence in Internet of Things. *CAAI Transactions on Intelligence Technology*, 208-218.

Kavanagh, C. (2019). *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?*. Available at: https://carnegieendowment.org/files/WP_Camino_Kavanagh___New_Tech_New_Threats.pdf.

Khanboubi, F., Boulmakoul, A., & Tabaa, M. (2019). Impact of Digital Trends using IoT on Banking Processes. *Procedia Computer Science, Vol. 151*, 77-84.

Kumar, N.M., & Dash, A. (2017). The Internet of Things: An Opportunity for Transportation and Logistics. *International Conference on Inventive Computing and Informatics (ICICI 2017)*, 194-197.

Kuzlu, M., Fair, C., & Guler O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity. *Discover Internet of Things 1, 7*. https://doi.org/10.1007/s43926-020-00001-4.

Li, M., Porter, A.L., & Suominen, A. (2018). Insights into relationships between disruptive technology/innovation and emerging technology: A bibliometric perspective. *Technological Forecasting and Social Change, Vol. 129*, 285-296.

Mallik, A. (2004). *Technology and Security in the 21st Century: a Demand-side Perspective*. Oxford University Press Inc., New York.

Nasajpour, M., Pouriyeh, S., Parizi, R.M., Dorodchi, M., Valero, M., & Pouriyeh, S. (2020). Internet of Things for Current COVID-19 and Future Pandemics: an Exploratory Study. *Journal of Healthcare Informatics Research, 4*, 325-364.

Rotolo, D., Hicks, D., & Martin, B.R. (2015). What is an emerging technology? *Research Policy, Vol. 44, Issue 10*, 1827-1843.

Sayler, K. (2019). *Artificial Intelligence and National Security*: A Congressional Research Service Report. R45178, available at: https://crsreports.congress.gov/product/details?prodcode=R45178.

Shnurenko, I., Murovana, T., & Kushchu, I. (2020). *Artificial Intelligence: Media and Information Literacy, Human Rights and Freedom of Expression*. UNESCO IITE and TheNextMinds.

Sobb, T.M., & Turnbull, B. (2020). Assessment of Cyber Security Implications of New Technology Integrations into Military Supply Chains. *2020 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 21–21 May 2020, 128-135.

UNCTAD. (2021). *Technology and Innovation Report 2021*. Available at: https://unctad.org/system/files/official-document/tir2020_en.pdf

Wang, J., Cao, L., Shen, Y., & Zheng, G. (2018). Research on Design of Military Logistics Support System Based on IoT. *2018 Prognostics and System Health Management Conference (PHM-Chongqing)*, Chongqing, China, 829-832.