IOT INTEGRATION IN WARFARE: REVOLUTIONIZING MODERN BATTLEFIELD OPERATIONS

Lt Col Rachit Ahluwalia

"Any sufficiently advanced technology is indistinguishable from magic" —Arthur C. Clarke

Abstract

The meteoric rise of IoT has the potential to impact several spheres of humanity, warfighting being one of them. This paper highlights the perspective of IoT implementation in modern battlefield scenarios, analysing its role in augmenting situational awareness, delivering information superiority and supplementing decision support system through comprehensive analysis. While acknowledging the benefits of the technology, the paper also addresses security and ethical concerns associated with IoT in military applications.

Introduction

The present era has been ushered by advancements in Information, communication and technology (ICT). This advancement has impacted the transformation of almost all aspects of society, warfighting being one of them. Contemporary armies across the globe are experimenting to deploy niche technologies into battlefield as force multipliers to gain tactical edge. Out of various new technologies viz AI, robotics, quantum computing, virtual and augmented reality; IoT has been generating immense interest among defence researchers and industry. IoT records an exponential proliferation rate in the domain of emerging computing technologies, with an estimate market revenue of $212 billion worldwide and more than 25 billion devices connected with each other by the year 2027[1]. IoT is an intersection of real-life things/ objects, communication networks and data. It is empowered by plethora of sensors, actuators, identifiers, pervasive information systems, embedded computing, software intelligence and network connectivity. It should not be perceived as any other app on the World Wide Web but as a radical Information Technology enhancement.[2]

IoT harnesses the power of Wireless Sensor Networks (WSNs), RFID, Machine to Machine Communication (M2M) and Control Systems to collect, process and transfer vital info from heterogeneous nodes across time and space. To convert the extracted information into intelligence either localised hardware resources can be employed or geographically dispersed virtual machines over cloud computing.[3] The power of IoT processors is in making informed choices and executing tasks based on what its sensors observe. The range of processing tasks may vary from measuring simple physical parameters viz temperature, humidity, altitude etc to as complex as recognising patterns and extracting weather forecasts using predictive AI algorithms. IoT actuators execute planned actions, post consuming information from sensors that tangibly change the setting. Actuators may perform a trivial task, even as remotely turning on a security light or can accomplish an intricate mission of target identification, tracking and destruction.[4] They can operate on a both sides of the spectrum scale which is significantly smaller and larger than human limits. People may form part of the IoT action loop but it is designed to function autonomously as well.[5]

The meteoric progression of IoT has propelled the deployment of intelligent sensors and actuators in the battlefield, lending it the name Internet of Battlefield Things (IoBT).[6] IoBT is an inventive technology that incorporates WSNs, actuators, portable & ruggedised IoT devices, routers and gateways to create a modern integrated warfighting force with refined operational efficiency.[7] Although it can be argued that IoT technology is not new and has its roots dating back to the work done by Mark Weiser at Xerox PARC in the 1990s, recognising the power of IoT took years of evolution in five key technology domains i.e.

wireless sensors, communication & networking, cloud computing, smart algorithms and digitally controlled actuators.[8]

IoT's Transition to IoBT

The defence sector has been a fountainhead for numerous emerging technologies for ages. Gaining a battlefield edge has always been a driving factor to explore and experiment with radical ideas. Post the first Gulf War one such idea started taking shape when Admiral William Owens, the then Chief of US Naval Operations, introduced the idea of a 'System of Systems' in a research article published under the aegis of the Institute for National Security Studies, United States. He articulated the way data and networks would transform warfighting.[9] This appreciation translated into the concept of 'Network Centric Warfare', which is a convolution of three domains namely physical; where manoeuvres are conducted, producing data from sensors, the info domain; where data is transferred and archived and the cognitive domain, where data is processed and analysed.[10] After more than two decades since this concept was floated, military leaders and defence experts across the world are now sanguine about it's implementation primarily because of IoT technology maturation. Javelin anti-tank missiles and Switchblade loitering missiles which are being extensively used by Ukrainian ground forces to challenge the mighty Russian armour exemplify the successful implementation of IoT technology in the combat zone.[11]

IoBT should not be looked at with the same lens as that of "just another singular niche technology", rather it engulfs and encompasses a range of many such technologies. Hence comprehending IoBT as an idea is more appropriate and rational.[12] It is the result of the convergence of several intelligent, networked and dynamically constructed devices and technologies that can deliver effects in both physical and virtual space. The goal of IoBT is to administer complex, intelligent systems-of-systems, ubiquitously housing smart sensors and actuators, powered by adaptive learning processes to achieve the Military's strategic and tactical objectives.[13] IoBT grid functions with a varied assortment of sensor nodes wired or wireless, all meshed together. Operations can be coordinated across the network consisting of early warning ground and UAV-based sensors, autonomous weapons, smart soldiers and state-of-the-art command posts. It can perform a dual role of collecting intelligence as well as delivering a kinetic strike. Removing soldiers from the execution loop and placing them in a supervisory position at the highest level, it can enable weapons to assign and engage targets with a high degree of autonomy.[14] It also has the ability to exacerbate the tempo of operations and remove the fog of war.

Advantages Accrued

Future wars will be fought in a highly contested and coercive environment, densely populated by an ensemble of both smart and legacy equipment. This will require accomplishing sprawling responsibilities of collating, corroborating, disseminating and collaborating actionable information with both men and machines.[15] IoBT system can function as an integration platform for these devices and men, helping commanders to shorten the OODA loop and make informed decisions. Some of the advantages that can be accrued by introducing IoT on the battlefield are listed below:-

- **Autonomous Systems**. IoT will act as a catalyst to automate the process of warfighting; from ISR to weapon platforms to Decision Support System all facets of ops can cohesively function without human intervention.

- **Tempo of War**. Increased autonomy in weapon platforms shifts human control from execution to a supervisory role. The process of making a decision to execute the command can be accomplished in split seconds, accelerating the tempo of war.

- **Reduced Attrition**. With the application of remote supervisory oversight better situational awareness and lesser foot on the ground can be achieved, resulting in a lower casualty rate of own troops.

- **Precision Strikes**. Weapons can be guided more precisely to their intended target via an IoT network using both onboard and offboard sensors. Automated control loops outperform soldier-controlled, sight-and-aim weaponry in terms of speed and accuracy. By integrating disparate weapon types IoT increases the enemy’s attack surface.

- **Effective ISR**. Wide-ranging unmanned and dispersed sensors can be meshed together over IoT networks. Additionally, IoT gathers data by monitoring software programs, sniffing networks and accessing databases. Such networks provide a more comprehensive, multi-view and continuous observation of a space, event or activity.

- **Dispels the Fog of War**. During operations when sensors and early warning elements are destroyed or data and sitreps become unreliable, a commander's vision of the events unfolding in front becomes obscured. This fog of war that engulfs decision-making can be dispelled by IoT technology, which constructs dynamic self-healing, adaptive and resilient information sources over secured communication channels. Even amid the melee of battle, better situational awareness can be ensured using these capabilities.

- **Intelligent Processing**. IoT enables sophisticated processing to increase the capacity for human observation. It can spontaneously plan and autonomously execute actions. To ensure that commanders on the battlefield are not overwhelmed by the flow of information, smart processing offers the necessary component for ingesting, filtering, prioritizing, and abstracting it. IoT transforms Data into Info, Info into Awareness, Awareness into Plans and Plans into Action.

- **Agile Logistics**. IoT can supercharge operational logistics by achieving just-in-time and just-in-case supply chains. By convoluting sensors, actuators and monitoring algorithms IoT can keep track of what, where, when, and how much is needed in real-time. Conditioned-based maintenance is another paradigm that can be explored by harnessing IoT technology which can enhance productivity, reduce expenses and improve op reliability.

- **Interfacing Legacy Systems**. IoT networks can join legacy stovepipe systems by using inexpensive sensors, control systems and automatically compiled software. Gateways can be created as an interface between contemporary and legacy platforms to optimally utilise resources at the disposal of theatre commanders.

- **Technology Adaptation**. IoT facilitates quick and inexpensive adaptation of technology because of its ability to introduce new and improved components in existing networks. This facilitates incremental upgrades, distributing the associated costs and enabling continual development to keep abreast with the changing technology paradigm.

Use Cases

With the immense potential that IoT offers for its military usage, its application in tactical battle areas appears to outshine and promises to deliver rich dividends. In network-centric operations scenario, the employability of IoBT can seamlessly and effectively integrate all the available resources at the disposition of the battlefield commander, which can aid in making informed decisions. Some possible application areas are briefly described below.

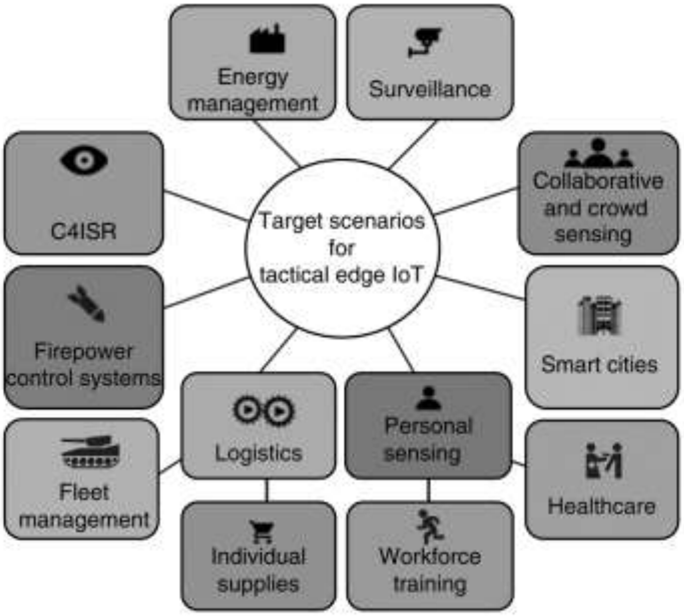

Figure 1: Target Scenarios for Tactical Edge IoT in Defence

Source: https://www.researchgate.net/ profile/Paula-Fraga-Lamas/publication/309404867/figure/fig2/ AS:614078204612624@1523419061829/Promising-target-scenarios-for-defense-and-public-safety.png

- **C4ISR**. An integrated network of IoT sensors deployed across a variety of platforms can provide improved situational awareness in a contested and coercive environment.[16] The amalgamation of ground and aerial sensors, surveillance satellites and also soldiers having a foot on the ground is bound to collect a variety of data. Such information can be filtered, processed, collated, corroborated and conserved in a platform, which regulates critical data transmission up and down the chain of command, allowing better battlefield coordination, command and control.

- **Weapon Control Systems**. The possibility of having an autonomous weapon system and fire control is being explored using sensor networks, machine learning and advanced AI analytics. Such a sensor shooter grid can provision precisely targeted firepower delivery and completely automated responses to attacks in real-time.

- **Op Logistics**. Effective fleet management and efficient shipment tracking can be easily achieved by harnessing smart sensors, RFID tags and M2M communication. Edge IoT devices can augment real-time tracking and provisioning of ordnance, critical supplies, ration and clothing. As consumption patterns are being monitored push model of provisioning supplies based on the inherent priority and necessity can be implemented, greatly improving op efficiency.

- **Man Management**. Wearable IoT sensors can be embedded within combatants' personal equipment like small arms, helmets, clothing, back-pack etc. enabling ubiquitous physical activity tracking and operational data gathering. Using context-aware data to infer and track soldier's health parameters and psychological state during operations in real-time may provide crucial insight and help in taking preventative measures for force conservation.

- **Training**. IoT can also find utility in providing enhanced training and war gaming experience. The IoBT concept can be integrated into military training to create more realistic, adaptive and effective preparation for future operations. Wearable sensors can be exploited to track the physiological and cognitive states of soldiers undergoing training which allows the conveyance of tailored feedback and personal optimisation.

- **Power Management**. Managing power requirements in the theatre of operation remains an underrated area but with the increased introduction of electronic devices in the battlefield, power and energy management will pose some serious challenges in planning and executing future operations. Employing predictive algorithms and real-time IoT data can significantly save military energy effort and help understand usage patterns.

- **Smart Surveillance**. Advanced Audio Visual and seismic sensors along with visual AI and pattern recognition techniques can facilitate the establishment of a smart surveillance and monitoring grid which can span not only over the ground but also the maritime environment. IoT solutions make it possible to sense and forecast ecological conditions thus keeping tabs marine operations over wide areas.

- **Collaborative & Crowd Sensing**. Mobility and manoeuvrability of tactical resources present a unique set of communication challenges in the modern battlefield. Collaborative sensing refers to the process of disseminating sensor data among mobile devices, often using dependable short-range communication.[17] IoT nodes can utilise idle sensors to augment their own sensing needs. Any ad-hoc ISR missions can be facilitated by matching sensors with task assignments. The available sensing and communication resources at the disposition of operational commanders can therefore be optimally utilised.

Implementation Challenges

Along with the benefits of employing IoT in the battlefield comes unique challenges. Designing and implementing IoT network in a war-like scenario is a challenging task that necessitates a thorough comprehension of both standard cybersecurity issues and complex ethical issues related to military applications.[18] IoT devices are mandated to operate in harsh hostile conditions muddled with misinformation and deception. Because these networks are deployed in dynamic and hostile battlefield conditions, they are extremely vulnerable to cyber assaults. It is crucial to understand that IoBT networks bring a surfeit of security issues that go beyond traditional IT settings.[19] These networks are made to connect a wide range of equipment from sensors and unmanned vehicles to soldier-worn gadgets.

One of the principal security concerns in IoBT networks is the vulnerability of connected devices. The growth of IoT devices in the military space increases the attack surface and provides enemies with multiple points of entry, as each device has its own set of sensors and communication protocols.[20] IoT enhances defence efforts, but if an IoT system is compromised, it can also intensify harm done by the enemy. IoT components are networked by design, in the event of a single node getting compromised, it could have a cascading effect, jeopardising the others. Safeguarding the integrity of specific IoT nodes does not assure the integrity of the network due to system interdependence and emergent behaviours.[21] Securing these devices requires implementing robust authentication methods, encryption protocols, and regular security upgrades to obviate the threat of unauthorised access and exploitation. Moreover, the issue of data transmission security arises from IoBT network's dependence on wireless communication. Communication routes may be attempted to be intercepted, manipulated, or disrupted by adversaries, endangering the integrity and confidentiality of critical data.[22]

To combat these attacks and guarantee that mission-critical data is secured, it is imperative to implement secure communication protocols and modern encryption standards. Another security threat that defence forces and security agencies should be vary of is identifying and guarding against embedded threats. The hardware components are exported from different countries, and the equipment suppliers maybe located in a specific country but may be utilising manufacturing facilities of another country, therefore, it is quite challenging to govern foreign manufactured components and also determine what constitutes an overseas source.[23]

Given the possible repercussions of security breaches in military operations, ethical considerations in IoBT networks are critical. Privacy and ethical information management become more important because of the colossal volumes of data getting collected and used via sensors and devices. A delicate ethical dilemma is finding a balance between the collection of actionable intelligence and the protection of people's right to privacy, particularly during CI/CT operations and zones where civilians and military coexist.[24] In addition, the introduction of autonomous systems into IoBT networks presents decision-making-related ethical conundrums. For example, split-second choices with big ramifications would be needed for autonomous weapons, smart munitions and drones. To avoid unintentional harm and collateral damage, it is important to make sure that these systems follow moral precepts like discrimination and proportionality.[25] The effect that IoBT sensor networks may have on the civil population is a further ethical consideration. Inadvertently putting civilians in danger might occur when military IoT devices are placed during contested or urban warfare. Minimising damage to civilians, guaranteeing the prudent application of monitoring technologies and integrating moral principles into military policies require detailed study, analysis and planning before making any IoBT deployment.

Way Ahead

To have a future-ready fighting force it is important for nation states to explore and invest in emerging technologies; however, the gestation period for developing and inducting any new combat-ready equipment or system is fairly long. The sluggish pace of progression and related research and development cost are significantly higher as compared to Commercial off-the-shelf (COTS) available devices. IoT devices based on commercially available open-source and proprietary technologies are developing rapidly. It is possible to acquire and deploy technology in a quicker timeframe by using COTS IoT devices. The promise of system dependability, reliability, security, redundancy, portability and consistency in the theatre of battle can be achieved by tweaking these devices to military-grade specifications and standards.[26] Presently commercial IoT technology is substantially ahead of the defence IoT. Focussed efforts from government and industry optimising commercial investment to meet specific needs of defence forces is the need of the hour. Stakeholders involved in national security should engage with both industry and academia to stay updated with the rapidly evolving technological landscape, given the widespread availability of commercial IoT solutions.

Handling the colossal volume of data that IoBT sensor network can churn during active operations will require data filtering, refining and processing within the network. Such processing methodology also extends elastic multi-vantage multi-modal authentication of the IoT device's health and threats. Another idea that's garnering a lot of attention is CPDDS or the Design for Cyber-Physical Data-Driven Systems. Broadly stating, it is an embedded system in which computing units use feedback loops to connect with sensors and actuators in the real-world environment as well as each other. Applications for CPDDS can be found in vital infrastructure, including the distribution of fuel, water, electricity grid and transportation. In IoBT unmanned autonomous systems can be designed using this principle.[27] CPDDS can ensure information assurance encompassing verifiable safety, dependability and credibility. Assurance is also necessary for the system as a whole to guarantee the accuracy and security of decisions that follow, as well as for the interconnection of the networks, which frequently need to transfer data over poor communication channels.

Traditional cyber security measures involve implementing access control mechanisms and network security protocols at physical and network layers. However, transposing a similar template for IoBT devices will require hardware modifications and firmware updates making it inefficient with respect to both time and cost. SDN i.e. Software Defined Networking is a novel technique to overcome these issues. It provides an agile framework to efficiently and effectively manage large networks. SDN tends to separate control and data planes thus injecting flexibility into the network.[28] This augment in creating network layer security systems which are flexible and dynamic. The method of least privilege should be adopted while designing access control system for IoBT devices, as it negates the asymmetric nature of access control violations. The scale of the network and severe resource constraints pose unique challenges that IoBT devices must function under; therefore it is necessary to evaluate the conservative approach of host vs network-based defences. Due to their very nature IoT devices are unable to support end-point security protection. Hence deployment of an Intrusion detection system yields better dividends than employing legacy anti-viruses and firewalls on an IoBT network.

Ethical issues pertaining to use and misuse of IoBT necessitate the adoption of accommodative doctrine and policies, ensuring that the country exploits technological benefits while preventing the prospective for damage to the civil populace. In a democracy this will require consent of the people who consume or are subjected to the technology.[29] Transparency, accountability and security are some of the tenants that consent is built upon and cannot exist without. It is also necessary to preserve the integrity and security of the supporting data of an IoT system. This includes the history of its own processing activities and perceived results of those activities in addition to the extracted data. Records of disclosure statements, reviews, audits, and patches/ updates are a few examples of collateral information. Preserving the authenticity of the data demands not just keeping it safe but also ensuring it is properly recorded, saved and archived.

Conclusion

IoT is an innovative technology that should be harnessed to increase military operational efficacy and efficiency. IoBT is a network of sensors, actuators, wearables and portable IoT equipment that uses state-of-the-art computing to link soldiers with smart technology and build an integrated, coherent, and cohesive fighting force. Since it is a loosely coupled integration of numerous key technological components, harnessing the potential of IoBT in the modern battlefield requires a through understanding of the opportunities and challenges being presented by it. From the commander's perspective, IoBT can be alluded to as a smart and adaptive common operating platform that can accomplish Network Centricity and augment as a force multiplier on the battlefield.

IoT systems and devices will need to function independently in the modern battlefield to reduce the cognitive strain on warfighting soldiers and prevent human error brought on by coercive environments. On the other hand, little study has been done on how to allow IoBT systems and devices to function independently while yet being aware of their surroundings and able to make wise choices. The focus area for modernizing the IoBT should be on decision process multipliers, underlying technology interactions and scientific cross-technology experimentation.

The review has highlighted the potential benefits of implementing contemporary IoT concepts in military settings, while also acknowledging the unique challenges posed by tactical battlefield environments and adversarial conditions. These issues and challenges merit attention and require smart innovative solutions to ensure successful implementation of IoT technology in military operations.

****

Lt Col Rachit Ahluwalia was commissioned in Corps of Signals in March 2003. He holds an Mtech Degree in Computer Science and is pursuing PhD in IoT. The officer is currently posted at MILIT, Pune as Instructer Class 'A'.

NOTES

1 Satyajit Sinha, "State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally," *IoT Analytics*, January 26, 2024, https://iot-analytics.com/number-connected-iot-devices/.

2 Somayya Madakam, R. Ramaswamy, and Siddharth Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications* 03, no. 05 (January 1, 2015): 164–73.

3 Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* 29, no. 7 (September 1, 2013): 1645–60.

4 Abdelzaher, Tarek, Nora Ayanian, Tamer Basar, Suhas Diggavi, Jana Diesner, Deepak Ganesan, Ramesh Govindan, et al. "Toward an Internet of Battlefield Things: A Resilience Perspective." *Computer* 51, no. 11 (November 1, 2018): 24–36.

5 Zhu, Lin, Suryadipta Majumdar, and Chinwe Ekenna. "An invisible warfare with the internet of battlefield things: A literature review." *Human Behaviour and Emerging Technologies* 3, no. 2 (November 29, 2020): 255–60.

6 Poltronieri, Filippo, Laurel Sadler, Giacomo Benincasa, Timothy Gregory, John M. Harrell, Somiya Metu, and Christine Moulton. "Enabling Efficient and Interoperable Control of IoBT Devices in a Multi-Force Environment," October 1, 2018.

7 Feng, Yuan, Menglin Li, Chengyi Zeng, and Hongfu Liu. "Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective." *Entropy* 22, no. 10 (October 16, 2020).

8 Alexander Kott, Ananthram Swami, and Bruce J. West, "The Internet of Battle Things," *Computer* 49, no. 12 (December 1, 2016): 70–75.

9 Owens, William A. "The Emerging U.S. System-of-Systems." *Strategic Forum*, February1, 1996. https://www.questia.com/library/journal/1G1-130124286/the-emerging-u-s-system-of-systems.

10 Zheng, Denise E., and William A Carter. *Leveraging the Internet of Things for a More Efficient and Effective Military*. Rowman & Littlefield, 2015.

11 Leigh Kaplan, "Loitering Munitions in Ukraine and Beyond - War on the Rocks," War on the Rocks, April 21, 2022, https://warontherocks.com/2022/04/loitering-munitions-in-ukraine-and-beyond/.

12 Stephen Russell, Tarek Abdelzaher, and Niranjan Suri, "Multi-Domain Effects and the Internet of Battlefield Things," November 1, 2019.

13 Reza Tadayoni, Anders Henten, and Morten Falch, "Internet of Things — The battle of standards," November 1, 2017.

14 Alberts, David S., John J. Garstka, and Frederick P. Stein. "Network Centric Warfare: Developing and Leveraging Information Superiority.," February 1, 2000.

15 Neag, Mihai-Marcel, and George Mogoş. "Challenges and Opportunities of the Network-Centric Warfare on the National Defense System of Romania." *Land Forces Academy Review* 25, no. 1 (March 1, 2020): 15–21.

16 Ming-Jing, Lu. "Conceive on Modeling Platform in Training Simulation System of C4SIR." Jisuanji Fangzhen, January 1, 2013.

17 Sejun Song et al., "Effective Opportunistic Crowd Sensing IoT System for Restoring Missing Objects," June 1, 2015.

18 Alexander Kott, David S. Alberts, and Cliff Wang, "Will Cybersecurity Dictate the Outcome of Future Wars?," Computer 48, no. 12 (December 1, 2015): 98–101

19 Lin Zhu, Suryadipta Majumdar, and Chinwe Ekenna, "An invisible warfare with the internet of battlefield things: A literature review," *Human Behavior and Emerging Technologies* 3, no. 2 (November 29, 2020): 255–60.

20 Pedro Miguel Sánchez Sánchez et al., "SpecForce: A Framework to Secure IoT Spectrum Sensors in the Internet of Battlefield Things," *IEEE Communications Magazine* 61, no. 5 (May 1, 2023): 174–80.

21 U. Rahamathullah and E. Karthikeyan, "A lightweight trust-based system to ensure security on the Internet of Battlefield Things (IoBT) environment," *International Journal of System Assurance Engineering and Management*, September 3, 2021.

22 Federico Mancini and Frank T. Johnsen, "A Novel IoBT Security Assessment Framework: LoRaWAN Case Study," January 1, 2020, https://ffipublikasjoner.archive.knowledgearc.net/handle/20.500.12242/2909.

[23] Sharjeel Riaz et al., "Malware Detection in Internet of Things (IoT) Devices Using Deep Learning," *Sensors* 22, no. 23 (November 29, 2022): 9305.

[24] Rita Francese, Maria Frasca, and Michele Risi, "Are IoBT services accessible to everyone?," *Pattern Recognition Letters* 147 (July 1, 2021): 71–77.

[25] Fiona Carroll, Ana Calderon, and Mohamed Mostafa, "Ethics and the Internet of Everything: A Glimpse into People's Perceptions of IoT Privacy and Security," in *Springer eBooks*, 2012, 3–29.

[26] Pradhan, Manas, Fahrettin Gokgoz, Nico Bau, and Daniel Ota. "Approach towards application of commercial off-the-shelf Internet of Things devices in the military domain," December 1, 2016.

[27] Niggemann, Oliver, Gautam Biswas, John S. Kinnebrew, Hamed Khorasgani, Sören Volgmann, and Andreas Bunte. "Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control.," January 1, 2015, 185–92.

[28] Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." *IEEE Communications Magazine* 51, no. 2 (February 1, 2013): 114–19.

[29] Draetta, Laura, and Caroline Rizza. "The 'silence of the chips' concept: towards an ethics(-by-design) for IoT." *International Journal of Information Ethics* 22 (December 1, 2014): 23–31.