
# BRIEFING NOTES

BN-52-Emerging technology and military application-May2021

## PUBLIC POLICY FRAMEWORK FOR INTERNET-OF-BATTLEFIELD THINGS (IOBT)

Authors: Mehdi Taheri[1] and Kash Khorasani[2]
1 Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
2 Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

## SUMMARY

- Internet-of-battlefield-things (IoBT) systems will significantly change the future of modern warfare. These systems will improve performance of war-fighters, provide them with real-time information, guide and protect them, and will decrease the collateral damages caused by military operations.
- Combination of artificial intelligence (AI) and IoBT will result in emergence of adversarial devices and agents that can have fairly high complexity, endurance, and speed that will overwhelm conventional combat forces. Consequently, one needs to develop intelligent IoBT systems to fight adversarial IoBTs.
- One needs to take precautions in developing IoBT systems to address existing concerns and challenges such as security and privacy issues, ethics and liability, and resiliency and reliability of these systems. Hence, one needs to develop an IoBT public policy framework to ensure that the implemented IoBT systems have a high level of reliability, resiliency, and performance in highly dynamic and evolving battlefield environments.


## CONTEXT

- In order to provide armed forces with ISR and situational awareness information on the ground, seas, and in air by using a large number of sensors, the command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems have been developed [1].
- However, effectiveness of C4ISR systems can be improved by developing a network of interconnected devices that share their sensor information for decision making purposes. Consequently, the connection among various devices in the system would potentially enable combat forces to utilize the received information to make more timely and better decisions in complex and confusing environments of combat zones [1].
- Artificial Intelligence (AI) and connected autonomous things in the context of internet-of-battlefield-things (IoBT) are shaping and revolutionizing the future of military combats and modern warfare. Autonomous intelligent things or agents will fight adversarial autonomous intelligent things at a fast pace that would otherwise be beyond human capabilities.
- IoBT technology provides armed forces with strategic war assets in the highly dynamic battle zones. Moreover, IoBT connects combat subordinate forces to the command and control centers, provides war-fighters with real-time information of the battlefield, and this technology can reduce the collateral damage and human loss that are caused by military offences and attacks.
- The effectiveness and performance of IoBT systems rely on the underlying communication networks that connect various devices in the system. Moreover, these communication networks will be the target of adversarial cyber-physical attacks.

- Consequently, in order to carry out collaborative missions and operations by utilizing IoBT and in presence of adversarial cyber-physical attacks, the communication networks should be adaptive, versatile, and resilient.
- Adversaries will execute cyber-physical attacks to disable or disturb the IoBT system and communication network [2]. The type of cyberattacks could vary from spreading very generic, cheap malwares such as ransomwares that disrupt fairly simple computer assets to highly sophisticated malwares such as Stuxnet. Moreover, adversaries are capable of imposing disruption to the exchange of information among devices in the IoBT by performing Distributed Denial of Service (DDoS) cyberattacks on the communication networks.
- Given that intelligent IoBT systems will fight other intelligent adversarial devices, the future warfare will be far more complex than today's human operated missions and operations in both pace and scale [2]. Hence, AI-empowered and intelligent IoBT systems should carry out the task of monitoring adversarial cyber-physical attacks in the system as well as responding to and circumventing the potential cyberattacks [2].
- IoBT systems communicate a large amount of information with one another, and this calls for developing methodologies to authenticate the information source. The authentication methodology would then assure that the command and control center and combat forces received data are not false data and fake messages that generated by the enemy. In [3], an authentication model based on the Public Key Infrastructure (PKI) and digital signature has been proposed, which can be integrated into the existing IoBT systems.
- By utilizing a combination of PKI and digital signatures, IoBT devices will be capable of transmitting encrypted data to one another and obtain digital identities. Hence, the source of all the exchanged information can be verified and validated in order to improve the reliability and trust in IoBT systems [3]. One of the most important factors that should be taken into account is the data latency that is imposed by the authentication methods. The data latency factor is crucial since it has a major impact on military operations and the speed of decision making for taking a specific action against the enemy.
- There are several technical research that have been conducted to address security and privacy problems in IoT and IoBT systems, which indicate the rapid advancement in this field. However, due to the above rapid advancements in IoT and IoBT cyber security, the existing public policy frameworks and efforts could fall behind and fail to address the new challenges and concerns in this field. Moreover, advances in the cyber security research do designate topics and important technical issues that public administrators and policymakers should incorporate into their decision-making processes.
- Although there are several technical solutions to the challenging problems in developing IoBT systems, public policy frameworks have yet to be developed. A public policy framework can provide directions to fully address technical and legal problems, such as network specifications, resiliency requirements, level of reliability, authentication

problems, security issues, liability concerns, and ethical considerations in development of IoBT systems.

## CONSIDERATIONS AND RECOMMENDATIONS

- In the first step for developing a public policy framework for IoBT, one must identify and model the impact of various policies and decisions on the combat forces and their commanders as representing the main users of this technology [4]. Second, one needs to interpret and discover consequences of armed forces' preferences from the output of IoBT systems.
- Moreover, public values, which are considered as as "ethics, desired traits, characteristics of consequences that matter, guidelines for action, priorities, value trade-offs, and attitudes towards risk," should be considered in the decision-making processes and public policy development [4]. In the context of IoBT, public values should be determined by armed forces. Moreover, in view of public values of armed forces in the IoBT public policy framework should ultimately result in creation and implementation IoBT based on their perspectives. Hence, public values should be incorporated into the decision-making processes.
- Subsequent to identifying public values and preferences one needs to organize them and come up with their evaluation methods. Various objectives should be considered in order to evaluate and rank users' preferences [4]. For instance, security issues and resiliency of IoBT systems are among the most important values that should be considered within the considered policies.

## REFERENCES


[1] M. J. Farooq and Q. Zhu, " On the secure and reconfigurable multi-layer network design for critical information dissemination in the internet of battlefield things (IoBT)," *2018 IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2618--2632.

[2] Theron, Paul and Kott, Alxander, " When Autonomous Intelligent Goodware Will Fight Autonomous Intelligent Malware: A Possible Future of Cyber Defense," *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*, 2019, pp. 1-7.

[3] Ivan Vulic, Radomir Prodanovic, Tot Ivan, Bogićević Dušan, " Model for authenticating the Internet of Military Things and Internet of Battlefield," *2020, 10th International Conference on Information Society and Technology, Kopaonik, Serbia*.

[4] Smith, Kane J and Dhillon, Gurpreet and Carter, Lemuria, " User values and the development of a cybersecurity public policy for the IoT," *International Journal of Information Management*, vol. 56, 2021.