PHYSICAL SECURITY GUIDELINES FOR MALAYSIAN ARMED FORCES FACILITY USING CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

Roslinda Mohamed
Razak Faculty of Technology and Informatic
UTM, Kuala Lumpur, Malaysia
lindaisyahazizan@gmail.com

Hafiza Abas
Razak Faculty of Technology and Informatic
UTM, Kuala Lumpur, Malaysia
hafiza.kl@utm.my

Roslinda Ramli
Faculty of Science and Information Technology
Selangor International Islamic University College
roslinda@kuis.edu.my

Abstract

Physical security is an aspect of security control, especially in terms of prevention and perimeter protection. Physical Security aims to protect the security of documents, staffs, property, buildings and the environment. However, physical security for military buildings is in the middle of a social development area. The military area provides space for irresponsible outsiders to access secrets such as the military daily routine, target building, weapon warehouse, data center and defense operation center. Moreover, outsiders can secretly observe military activities and location of the target buildings. Existing defense systems should be integrated with systems to prevent and protect against all forms of human and natural threats. Therefore, the objective of this study is to propose guidelines for physical security of Malaysian Armed Forces (MAF). Thus, the objective of this study is to propose physical security guidelines for Malaysian Armed Forces (MAF) facilities using Crime Prevention Through Environmental Design (CPTED). For this article, the author applies the convergent-parallel mixed methods approach, that is, the simultaneous collection of qualitative and quantitative data, followed by the combination and comparison of these different data. This approach involves collecting different but complementary data on the same phenomena before conducting an analysis. The results show that the policies contain three components, namely electronic, architectural and organizational. These components are related to six CPTED strategies, namely surveillance and visibility, territoriality, access and escape routes, image and esthetics, target hardening and maintenance. The physical security guidelines that use CPTED must be considered from the beginning of building planning and design. Therefore, this paper proposes the physical security guidelines using CPTED techniques for MAF to improve the physical security objectives.

***Keywords*:** *Physical Security, Guidelines, Crime Prevention through Environmental Design (CPTED).*

1. Introduction

Physical security refers to the protection of workstations, equipment, and all information and software contained therein from theft, vandalism, natural disasters, man-made disasters, and accidental damage (Dunbin Sun, 2021). It is still possible to characterize physical protection as a

security tool aimed at denying unauthorized persons access to buildings, facilities, and services. The best physical security must be balanced with the implementation of crime prevention through environmental design (CPTED). It is well known that most military areas have been caught in the stream of modernization. In the process, most of the tall buildings have been built around the military area. This contributes to the leakage of information to the outside, and there may be an intrusion of outsiders. In addition, the main objective of CPTED is to change the urban environment to deter potential criminals. The concept that the environment can influence human behavior is based on urban planning and environmental psychology. When physical security is in line with CPTED strategies, fewer criminal incursions into military areas occur. CPTED benefits from the opportunity to play a meaningful role in military crime prevention; sustained connections with planning, development, law enforcement, and other local agencies; and new crime prevention and problem-solving initiatives. CPTED can also bring intangible benefits, such as strengthening links between public law enforcement, private security, and urban planners.

Traditional physical security is defined by security measures designed to prevent unauthorized access to facilities, equipment, and resources and to protect employees and property from harm or damage (e.g., sabotage, fraud, or terrorist attacks). In traditional facility, multiple layers of countermeasures such as surveillance, barriers, guards, and access control are used to achieve the goal (3-19.30, Field Manual Physical Security, 2001). This study aims to implement and improve physical security using Crime Prevention Through Environmental Design. Therefore, an overview of the CPTED principles of natural surveillance, natural access control, territorial reinforcement, target hardening, and maintenance (Deutsch, 2018) used in this field study is provided. In another study by Cozens, Saville, & Hillier (2015), CPTED also included activity support. That is, a variety of activities in a given area increases natural public surveillance, which in turn deters criminal activity. Figure 1.1 illustrates the scope of the study.

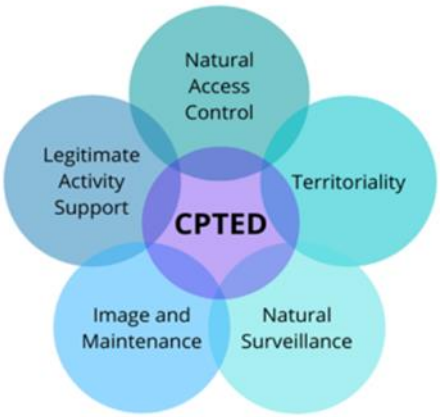

Figure 1.1: Crime Prevention Through Environmental Design Strategic

Physical security design and access control are more than bars on windows, a guard booth, a camera, or a wall. Crime prevention involves the systematic integration of design, technology, and operations to protect three important assets - people, information, and property. Protecting these assets is a major concern and should be considered throughout the design and construction process. The most efficient and cost-effective way to provide security is during the design process. Designers who are to address security and crime must be able to determine security requirements, be knowledgeable about security technologies, and understand the architectural implications of security requirements. The process of designing safety into architecture is known as crime prevention through environmental design (CPTED). It involves designing the built environment to reduce the possibility and fear of predatory crime by stranger. This approach to security design differs from traditional crime prevention practices that focus on preventing access to a crime target

with barrier techniques such as locks, alarms, fences, and gates. CPTED utilizes the capabilities of natural access control, surveillance, and territorial reinforcement. It is possible for natural and normal use of the environment to meet the same security objectives as physical and technical protection methods.

Proper design and effective use of the built environment can lead to a reduction in the fear of crime and the incidence of crime, as well as an improvement in the quality of life in the military zone. Crime decreases when the opportunity to commit a crime is reduced or eliminated. CPTED works by eliminating criminal opportunities in and around your property. This can result in your property being a less attractive target. Lack of maintenance causes people to feel unsafe and feel that undesirable behavior is taking place here. This study can provide guidelines and encourage military departments to design buildings with CPTED in mind. This will ensure that all military personnel are involved in creating and maintaining a safe environment. In addition, it will also ensure the military organization in preparing, reviewing and implementing planning schemes and guidelines CPTED.

This study will have a significant impact on physical security implementation guidelines using Crime Prevention Through Environmental Design (CPTED) for the use of all facilities in Malaysian Armed Forces by incorporating architectural, electronic, and organizational aspects. Through a very humane approach of surveillance and visibility, territoriality, access and escape routes, image and esthetics, target hardening and maintenance, this strategy will contribute to the field of physical security as a whole.

2. Background

Security methods meant to prevent unwanted access to premises, equipment, and resources are referred to as physical security. A strategy or plan of action to protect employees and property from harm or injury is also known as physical security (such as espionage, theft, or terrorist attacks) ("Physical Security," 2016). Important and strategic physical facilities such as the military camp require additional and advanced protection systems due to their important and strategic role. Designing physical security policies through CPTED and security features in MAF buildings and the military environment can reduce opportunities and vulnerability for criminal behavior and help create a sense of community. The goal is to create safe places through limited access to the buildings, good surveillance, and a sense of ownership and responsibility. Therefore, the physical security component installed there must really work and do its job. In the military environment, there are three factors that typically form the basis of a terrorist's decision as to which target to select. The first factor is the type of weapons available to the terrorist. The second factor is the opportunity or vulnerability of the target. And the third factor is the goal or effect the terrorist hopes to achieve through his action (Livingstone, 1982).

There are many examples of military intrusion. It all happens because there is no specific guide for developing a military area (Directorate, S., 2015). One incident in 2000, where Al-Ma'unah was a spiritual Islamist militant group, broke into a Malaysian Army camp early in the morning and stole weapons from an arsenal (The Straits Times, 2015). After a series of incidents, the military has made improvements in opening up military areas. But there still needs to be a guideline for the development of all military fields so that such incidents do not happen again and also because of the advanced new technology, especially in the IR 4.0 era, where intrusion and secrecy have become more advanced.

3. Method

For this study, the authors adopt the convergent-parallel mixed-methods approach, i.e., the simultaneous collection of qualitative and quantitative data, followed by the combination and comparison of these different data (W. Creswell & Plano Clark, 2018). This approach involves collecting different but complementary data on the same phenomena before conducting an analysis. Figure 3.1 explains the convergent parallel mixed methods. The results show that the policies

contain 3 components, namely electronic, architectural and organizational. These components are associated with 6 CPTED strategies, namely surveillance and visibility, territoriality, access and escape routes, image and aesthetics, target shielding and maintenance.

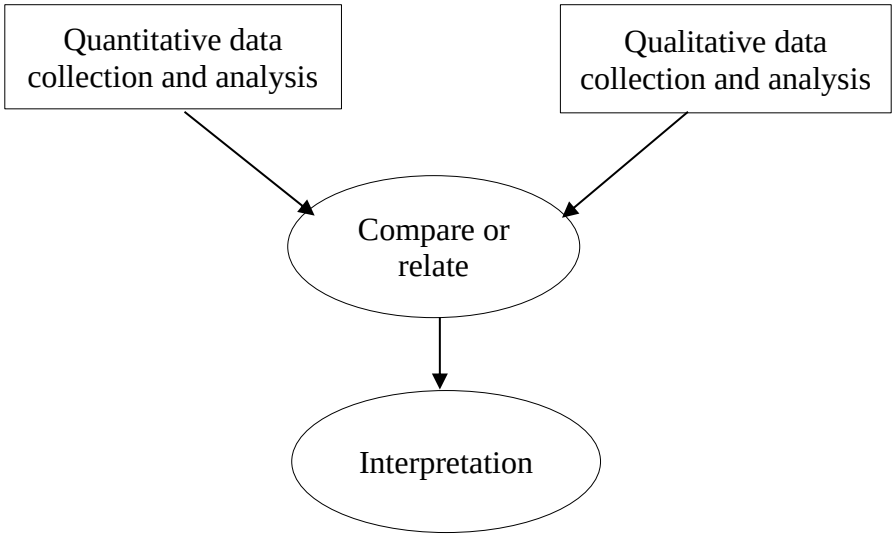

Figure 3.1: The Convergent Parallel Design (John et al., 2018)

3.1 Conceptual Framework

From study analysis to conclusion evaluation, the conceptual framework defines each research process. Figure 3.1 depicts each phase, as well as its anticipated activities and deliverables.

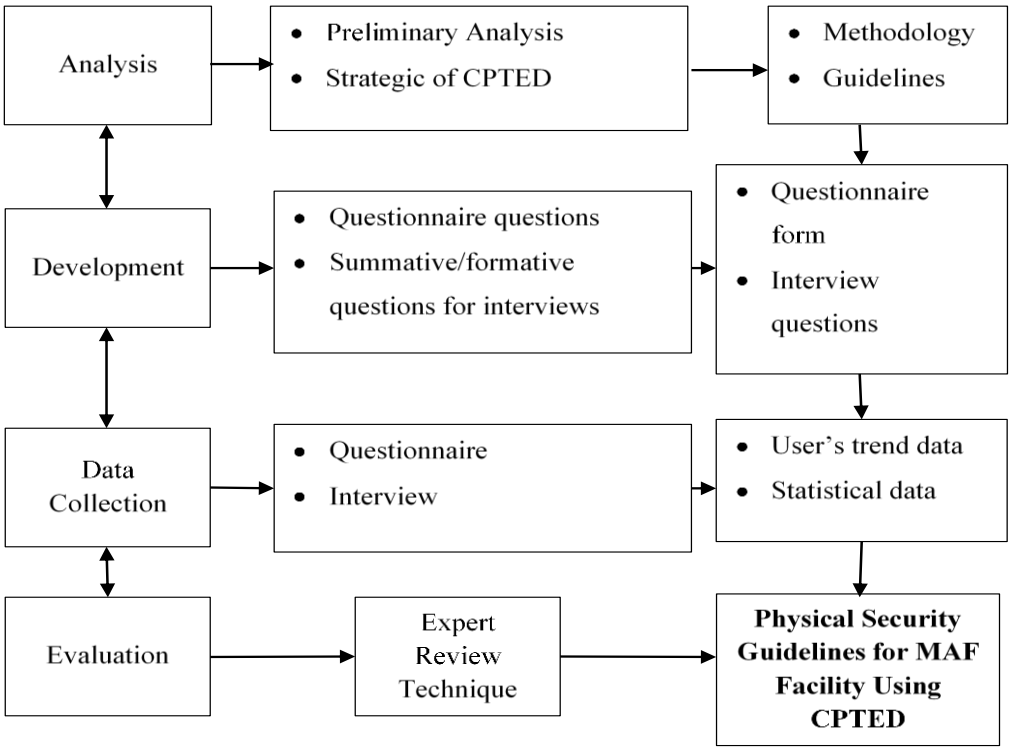

Figure 3.1: Conceptual Framework

3.1.1 Phase 1: Preliminary study

Preliminary study is a study that conducted to refine the research intervention and evaluate its acceptability (Smith et al., 2015). In phase 1 of the research process, Preliminary study is conducted to identify the research problem, research purpose and scope. The information from the literature review will be used to answer the research question, "What are the current physical security issues in the MAF facility without 100% implementation of CPTED strategy?" and "How are the three components of electronics, architecture, and organization related to CPTED strategies?". In this phase, a Preliminary Study survey is conducted among the military personnel of Malaysian Armed Forces working in the main guard of camp 11 Infantry Brigade using the study Cross-Sectional (Kumar, 2016). Military personnel will be given questionnaires to complete and collect on the same day. In addition to the questionnaires, the military personnel are also asked about their opinions and problems with the development of the camp's surroundings. The data collected through the questionnaire will then be entered into Google Forms to perform statistical calculations and create graphs. This preliminary study helps to advance the literature review that was conducted and provides a good overview of the challenges that were encountered and what can be incorporated into current practice.

3.1.2 Guideline Design and Development

Phase 2 develops the proposed physical security policies for the MAF facility using CPTED. The physical security policy phases are shown in Figure 3.2. Guideline's design and development, in which the initial guidelines are validated by experts consisting of university lecturers and a MAF security officer. In this phase, the validation of the guidelines will be conducted in two (2) rounds so that the guidelines can be developed thoroughly.

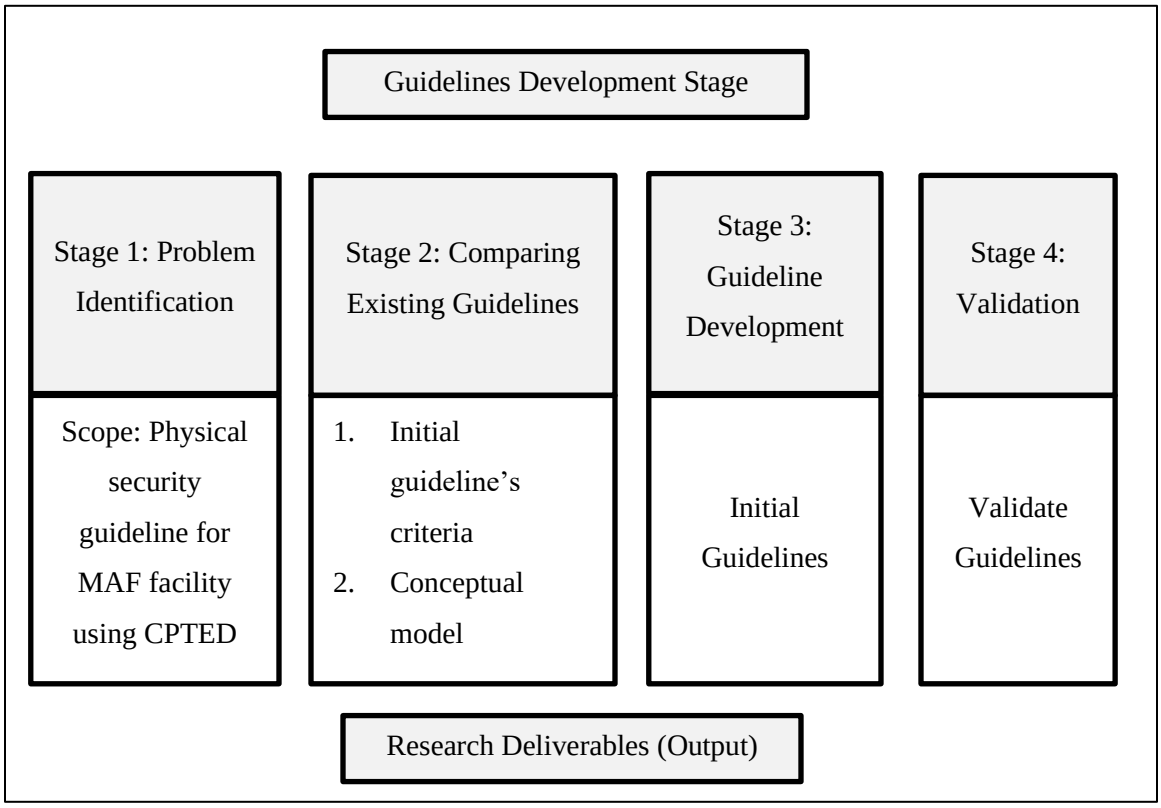

Figure 3.2: Guideline Development Stage

3.1.3 Phase 3: Guidelines Validation

The validation of the guidelines is done in two (2) rounds using the expert review technique where each physical security criterion is reviewed by experts using strategic CPTED criteria and the criteria he experts' approval are developed into physical security guidelines for MAF facilities using CPTED. Table 3.3 shows the validation criteria for the guidelines that align CPTED strategies with the 3 components of the guidelines.

Table 3.3: Validation Criteria

Guideline Component / CPTED Strategy	**Electronic**	**Architecture**	**Organizational**
Surveillance and visibility	Electronic access and intrusion detection; electronic surveillance	Architectural design and layout; circulation control; site planning and landscaping	Security Guards

Territoriality	Alarm and electronic monitoring and control; electronic detection	Architectural design and layout; circulation control; site planning and landscaping	Security Guards
Access and escape routes	Alarm and electronic monitoring and control; electronic detection	Architectural design and layout; signage; site planning and landscaping	Security Guards
Image and aesthetics		Architectural design and layout; signage	
Target hardening	Alarm and electronic monitoring and control; electronic detection	Circulation control; site planning and landscaping	
Maintenance	Manpower	Manpower	Manpower

3.1.4 Phase 4: Reporting

In this phase, the results of each phase are summarized in a full report. The purpose of the project report is to confirm that the project objectives have been achieved. All findings obtained in each phase will be forwarded to the appropriate departments of the MAF. Conducting a detailed study will provide good input to the MAF to establish guidelines for physical security using CPTED in each building of the military compound.

4. Findings

Each CPTED strategy employs a slightly different method to send a clear message to criminals that a responsible person is nearby and their activities are not welcome. Each of the 6 CPTED strategies has been broken down into 3 components, electronic, architectural, and organizational. The result is that all CPTED strategies overlap in the 3 components. Figure 4.1 below shows the overlap of the 3 components. The three components support each other in creating the physical security policies for the MAF facility using CPTED.

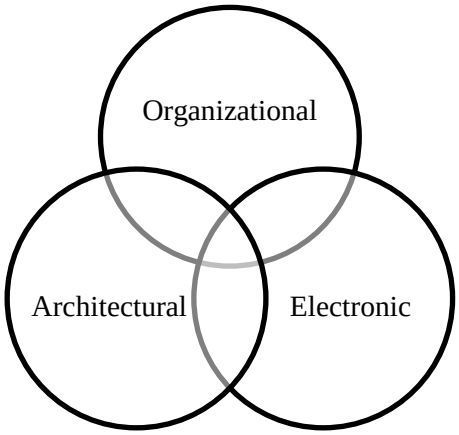

Figure 4.1: Overlapping 3 Component

The total of 38 respondents in this study are military personnel of the 11th Brigade Infantry, who are involved in the aspect of security of information, facilities and the environment. It is very important to study their understanding and implementation of CPTED as they are the main group of implementers of this policy. Based on the findings, strategic management can effectively determine the future implementation of CPTED in all military camps. Figure 4.2 shows the percentage of understanding and importance of these 3 components to them, 51% of the respondents indicated these 3 components are important to the success of this guideline. 29% of respondents indicated that only 2 components made a good guideline. There are 11 military personnel, meaning the equation of 30% states that if only 1 component out of 3 components is implemented, the implementation of this guideline may be sufficient. This shows that understanding the importance of CPTED to the information, buildings, and environment of military areas is paramount.

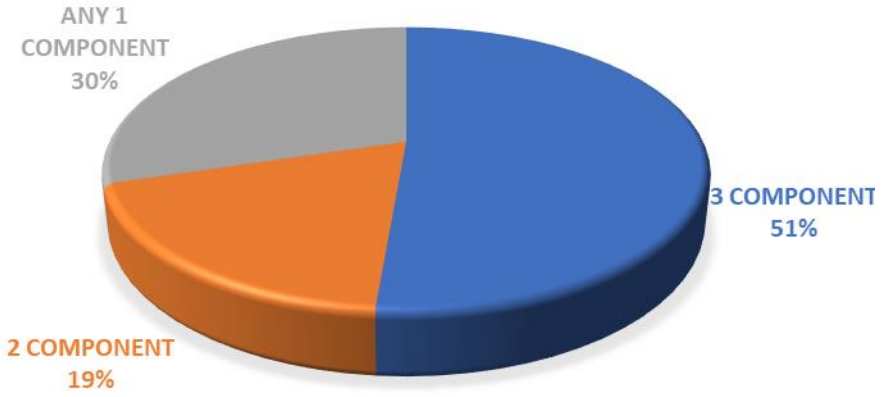

Figure 4.2: Percentage of Respondent

5. Conclusions

The goal of this physical security guidance for MAF facilities using CPTED is to influence and inform decisions about the design and management of the built environment so that our military camps, buildings, and personnel are safer and therefore more sustainable. It is also capable of solving physical security problems for the MAF facility. Security planning and management

involves many, sometimes competing, objectives or measures. This guidance primarily attempts to avoid repeating the same ideas in the many different sections. Therefore, no single detailed CPTED strategy or principle should be followed in isolation from the others. The best approach is based on understanding and applying the entire 6 strategic CPTED ideas, which are divided into the 3 components of Architecture, Electronics, and Organization. This makes it easier for an organization to formulate the criteria that must be in place to ensure that its physical security measures are successful. Successful implementation of the CPTED strategy in development requires planning at various levels, from overall design to documentation of the finer details, and staff with management must be aware of their responsibilities and the importance of physical security in their organization.

6. Future Works

It is clear that the implementation of CPTED in buildings or environments of military areas has reached the 50% level. However, it is hoped that the percentage of CPTED implementation can be further increased if there is consistent guidance to support the IR 4.0 plan in the future.

The first is the possible application of the method for CPTED based on the IoT. The Internet of Things (IoT) refers to a system of computing devices, objects, mechanical and digital machines, animals, or humans that are connected by unique identifiers (UIDs) and can transmit data over a network without requiring human-to-human or human-to-computer interaction (Rosencrance et al., 2019). Many researchers have proposed using IoT as a solution for physical security where an application program interface (API) is used to connect smart devices to the online access control system and grant access to those who are authorized ((Ouaddah et al., 2016), (Andaloussi et al., 2018), (Bandara et al., 2016), (Ashibani et al., 2017), (Z. Khan et al., 2017), (Ravidas et al., 2019), (Fysarakis et al., 2018) and (Greaves & Coetzee, 2017)). The readings from each sensor were used to assess the risk of crime at a particular location. For this experiment, sensors such as an acoustic sensor, a light sensor, and an ultrasonic sensor were used. The purpose of the sensor is to report any changes and environmental factors in the real-world. A light sensor was used to measure the brightness of an area. An acoustic sensor and an ultrasonic sensor were used to measure the status of the floating population in the area. These two factors can be used to determine if the area in question is an environment where the criminal activities of suspects can be monitored.

The second is the possible use of drones. Historically, such drones were first used by military services, but nowadays these drones with IoT addition are also used a lot in civilian applications such as infrastructure inspection, public safety, traffic control, agriculture and crop health monitoring, which gives us some advantages. The use of UAVs in construction industry is a cost-effective solution (N. Mohamed, 2014) as UAVs can maneuver flexibly in most boring, dirty, difficult and even dangerous places. This makes the proposed solution a unique one. These IoT-enabled drones can fly over the objects with precise flight altitude and capture the best quality images with a high-resolution camera, which are then further processed via machine algorithms and IoT-like applications to update the progress of each construction site, whether it is connected or not. For unconnected construction sites, the number of drones can be increased and work in a master-slave combination (F. Mohammed, 2019) to update the results, while for connected construction sites, the update can be done using a proper flight plan (F. Mohammed, 2019). Figure 6 show military facilities after applying the IoT element in any physical security environment to ensure no intrusion into restricted areas.

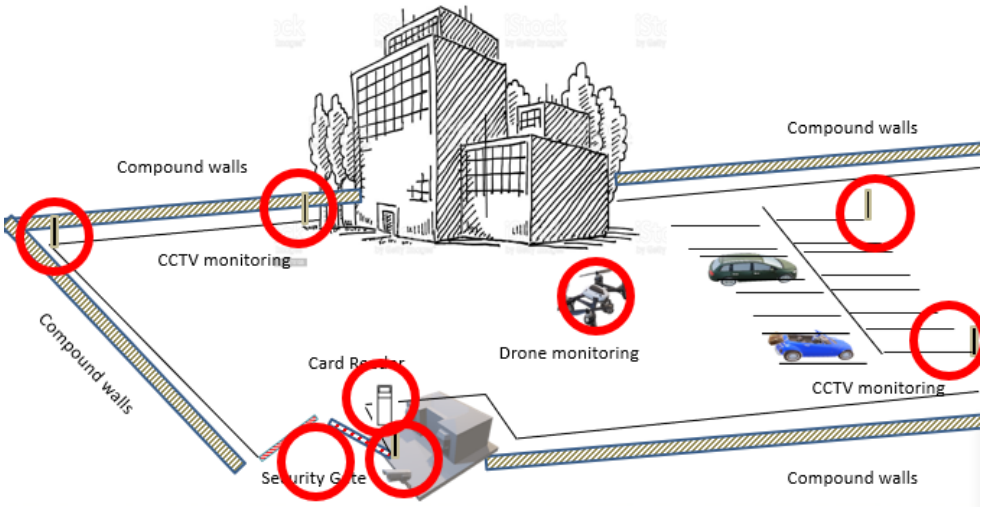

Figure 6: IoT in Military Facilities

Acknowledgement
We would like to thank Universiti Teknologi Malaysia, Selangor International Islamic University College and Malaysian Armed Forces.

References

Bruneau, M, Chang, S, Eguchi, R., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., Winterfelt, D. "A Framework to Qualitatively Assess and Enhance the Seismic Resilience of Communities" by Earthquake Spectra Journal Vol. 19, No. 4: 733-752, Earthquake Engineering Research Institute, 2003.

Critical Infrastructure Resilience Final Report and Recommendations by National Infrastructure Advisory Council (NIAC), Washington, DC: NIAC, 2009.

De Boer, J. Resilience and The Fragile City Retrieved Feb 2017 from Our World: https://ourworld.unu.edu/en/resilience-and-the-fragile-city, 2017

Ettouney and Alampalli. Infrastructure Health in Civil Engineering: Theory and Components Boca Raton, FL: CRC Press, 2012.

F. Mohammed, I. Ahmed, N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Opportunities and challenges of using UAVs for Dubai Smart city," in Proceedings of the 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–4, Dubai, UAE, April 2014.

Irina Matijosaitiene, Urban Planning and Design for Terrorism Resilient Cities, Journal of Sustainable Architecture and Civil Engineering,2016

Justice, M. of. (2005). National Guidelines for Crime Prevention Part 2: Implementation Guide. In City

Khalid, E. I., Abdullah, S., Hanafi, M. H., Said, S. Y., & Hasim, M. S. (2019). The consideration of building maintenance at design stage in public buildings. Facilities, F-04-2018-0055. https://doi.org/10.1108/F-04-2018-0055

Matthew M. Car, Urban Hostility: CPTED, Hostile Architecture, and the Erasure of Democratic Public Space, 2020

Menichelli, F. (2014). Technology, context, users: A conceptual model of CCTV. Policing, 37(2), 389–403. https://doi.org/10.1108/PIJPSM-06-2013-0055

Natural Hazards Mitigation Saves: An Independent Study to Assess the Future Savings from Mitigation Activities: Volume 1 - Findings, Conclusions, and Recommendations by National Institute of Building Sciences Report, Washington, DC: MMC, 2005.

N. Mohamed, J. Al-Jaroodi, I. Jawhar, and S. Lazarova-Molnar, "A service-oriented middleware for building collaborative UAVs," Journal of Intelligent & Robotic Systems, vol. 74, no. 1-2, pp. 309–321, 2014.

Omrany, H., & Marsono, A. (2016). Optimization of Building Energy Performance through Passive Design Strategies. British Journal of Applied Science & Technology, 13(6), 1–16. https://doi.org/10.9734/bjast/2016/23116

Paul Cozens1, Terence Love2, A Review and Current Status of Crime Prevention through Environmental Design (CPTED), 2015

Perimeter Security. (2016, April 9). In Wikipedia, the free encyclopedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Perimeter_Security&oldid=714468410.

Physical Security, Headquarters, Department of the US Army,2010

Prevatt, J. S. (1998). Crime Prevention Through Environmental Design (CPTED) and the role of facilities planning in force protection. 163

Queensland, C. (2007). Crime Prevention through Environmental Design guidelines for Queensland Part a: Essential features of safer places.

Ray, M. (2017). Local government. Retrieved September 28, 2019, from https://www.britannica.com/topic/local-government

Rouse, M. (2017). Security. Retrieved September 27, 2019, from https://searchsecurity.techtarget.com/definition/security

University, S. (2016). HIPAA Security: Facilities Security Policy | University IT. https://uit.stanford.edu/security/hipaa/facilities-security-policy

Vasileios Mavroeidis, Kamer Vishi, A Framework for Data-Driven Physical Security and Insider Threat Detection, 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)

Virgilito, D. (2014). A Physical Security Policy Can Save Your Company Thousands of Dollars. Retrieved December 25, 2019, from https://resources.infosecinstitute.com/physical-security-policy-can-save-company-thousands-dollars/

Wang, X., & Wang, Y. (2018). An office intelligent access control system based on RFID. In Proceedings of the 30th Chinese Control and Decision Conference, CCDC 2018 (pp. 623–626). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CCDC.2018.8407206

Wang, Z., & Liu, X. (2017). Analysis of burglary hot spots and near-repeat victimization in a large Chinese city. ISPRS International Journal of Geo-Information, 6(5). https://doi.org/10.3390/ijgi6050148

Zou, B., Yang, M., Guo, J., Wang, J., Benjamin, E. R., Liu, H., & Li, W. (2018). Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation. Progress in Nuclear Energy, 104, 8–15. https://doi.org/10.1016/j.pnucene.2017.08.006