CHAPTER I
INTRODUCTION

1.1 Background

In the digital era defining the 21st century, it's clear that the evolution of cyberspace has become a crucial aspect of national defense and security worldwide. Indonesian National Armed Forces, as a primary pillar of the nation's defense, is not immune to the significant impacts of this change. Cyber incidents globally have profoundly highlighted the importance of cyber protection in safeguarding national sovereignty and security.

Cyberattacks on critical infrastructure, such as electricity, water, and transportation systems in various countries, have heightened awareness of potential threats to similar infrastructures in Indonesia. Such cyberattacks can cause serious disruptions in military and civilian operations, threatening national stability. The theft of data and intelligence by foreign nations or cyber groups has become a serious concern. Incidents like the theft of weapon designs, strategic plans, or other secret military data have increased the need for enhanced cyber security within the Indonesian National Armed Forces to protect critical information.

Terrorists are increasingly utilizing cyberspace to communicate, recruit, and coordinate attacks. Cyberattacks on military websites or the spread of propaganda damaging the Indonesian National Armed Forces reputation have become a major concern in counter-terrorism efforts. Information warfare in cyberspace has become a significant tool in geopolitical conflicts. The manipulation of information, spread of fake news, and disinformation campaigns necessitate the Indonesian National Armed Forces ability to identify, counter, and disseminate accurate information. In response to these evolving cyber trends and incidents worldwide, the Indonesian National Armed Forces continues to enhance its cyber capabilities and awareness, including establishing cyber units, training personnel, and collaborating with national and international cyber

agencies. Cyber protection and the ability to counter cyber threats have become integral to Indonesia's national defense and security strategy in this digital era, where warfare relies not only on conventional military strength but also on cyber skills, artificial intelligence, and global terrorism networks.

A recent example of cyber challenges faced by the military is the cyberattack aimed at the Armed Forces of Ukraine. In 2017, from the first day of the war, Ukrainian government service sites were inaccessible due to Distributed Denial of Services (DDoS) attacks, including websites belonging to the parliament, government, Ministry of Foreign Affairs, and other state institutions. The "Hermetic Wiper" data-wiping malware was found on hundreds of Ukrainian government computers. Days before, Ukrainians received fake text messages informing them that ATMs were offline. Many citizens rushed to withdraw money, leading to panic and uncertainty. The cyberattacks, suspected to be from Russia, targeted Ukrainian military communication devices, causing serious disruptions in communication and military operation coordination. Ukraine accused Russia of these cyberattacks, including malware and DDoS attacks targeting military communication systems, such as phones and internal networks. This disrupted command and control capabilities, complicating troop movements and reducing the effectiveness of military operations. These attacks demonstrate how cyber power can be used to disrupt military infrastructure and affect military operations' performance. They also highlight the importance of cyber protection in facing modern threats, as well as efforts needed to identify and address cyberattack perpetrators. Integrating technology, terrorism, and cyber challenges, militaries worldwide must continue to adapt and develop robust cyber capabilities to protect national interests and maintain security in this complex digital era.

Cyber education at the Military Academy through the Defense Electronics Engineering Diploma IV (D-IV) Program has been well integrated into the curriculum. The Supporting Competence courses, particularly Basic Technology Knowledge, provide a platform for future military officers to understand important aspects of cyberspace. This course, worth 2 Semester Credit Units, teaches relevant basic cyber knowledge.

Topics in this course range from cyber law, data security, hacking and ethical hacking, to understanding cyber threats and effective cyber defense strategies. Understanding cyber law helps cadets respect rules and ethics in technology usage. Meanwhile, knowledge about data security and hacking techniques provides deep insights into how to protect data and identify potential attacks. Through this structured curriculum, Military Academy cadets are well-prepared to face the increasingly complex cyber challenges of the modern era, ensuring the continuity of national security.

Important lessons for the military, especially the Indonesian Army, from cyber incidents include increasing awareness of cyber threats, mastering cyber technology and security, and developing rapid and effective response capabilities. International collaboration is key in information exchange and joint efforts against cyberattacks. Protecting confidential information and understanding cyber terrorism threats need to be enhanced, while capabilities in information warfare are also important to influence public opinion and foreign policies. In this complex digital era, these lessons become an integral part of national defense and security strategy to protect national interests.

Currently, there is no specific laboratory for cyber practice at the Military Academy, so cadets must use the available computer laboratories for practicals, although this may not be entirely adequate for more in-depth cyber practical exploration. Practical topics like Social Engineering, Python Keylogger, and Wifi Security remain an important part of the curriculum, despite facility limitations. This situation also raises relevant legal and technical considerations for cyber practice activities by cadets. Despite facing challenges in terms of ideal laboratory facilities, the Department of Mathematics, Science, and Technology and the Director of Education Staff at the Military Academy strive to provide relevant knowledge and skills in the cyber field to cadets. They continue to develop a structured curriculum and practicals that offer a strong understanding of urgent cyber security issues. With hopes that better cyber laboratory facilities will be available in the future, the Military Academy remains committed to producing military officers ready to face modern cyber challenges.

In the context of previous research conducted by various researchers, such as the development of a web-based Odoo Point of Sale Application documentation module at PT Belant Persada (Gustiani et al., 2018), related research shows results from the development of ICT-Based Learning Project Management Using the Accelerated SAP Method on Odoo ERP (Supriyono & Sutiah, 2019). The implementation of an ERP-based information system using Odoo software at PT.X demonstrates the potential and advantages of Odoo ERP as a reliable platform in various applications (Perdanakusuma et al., 2020). The proposed research uses the Odoo ERP framework to design a Cyber Learning System at the Military Academy Magelang. The main goal is to support cyber learning for cadets at the Military Academy. By utilizing technology proven efficient in previous research, it aims to create a modern, effective, and relevant educational system for current military education needs.

1.2 Problem Statement

Cyber education at the Military Academy is not just an addition, but an integral part of preparing military officers for the digital era. In response to rapid technological advancements and contemporary demands, the curriculum at the Military Academy has effectively integrated cyber learning materials. This aims to provide a strong foundation for cadet officers, preparing them to understand and tackle the increasingly complex challenges of cyberspace. One concrete effort is through the Supporting Competence courses. Topics like Basic Technology Knowledge are carefully designed, ensuring that cadets not only receive information but also a deep understanding of the important aspects of cyberspace. This ensures that they are equipped with relevant and up-to-date basic cyber knowledge. The following is a formulation of the problem that can be observed.

a. What are the relevant materials and learning techniques to be developed in the ODOO platform?
b. How is the design of materials and learning techniques for Basic Cyber Knowledge studies at the Military Academy?

c. How to conduct testing of materials and learning techniques for Basic Cyber Knowledge studies at the Military Academy?

1.3 Scope of the Problem

The scope of this research includes:

a. Utilizing the Odoo ERP application as a platform for cyber learning and modifying it with Python programming language.
b. Using a dedicated server to install a Linux system and creating a practice website from Odoo ERP for testing SQL injection techniques.
c. Cadets will use client computers to try SQL injection attack techniques.
d. Cadets will use a server to examine how to protect against SQL injection attacks.
e. The research period is from June to December 2023.

1.4 Research Objectives

Based on the problem statement outlined above, the objectives of this research are:

a. To identify the materials and learning techniques related to Basic Cyber Knowledge studies at the Military Academy.
b. To design effective materials and learning techniques suitable for Basic Cyber Knowledge studies at the Military Academy.
c. To test the designed materials and learning techniques on Basic Cyber Knowledge studies at the Military Academy.

1.5 Benefits of the Research

The expected benefits of this research are:

a. Development of Relevant Learning Materials. The results of this research will contribute to identifying and developing learning materials relevant to Basic Cyber Knowledge studies in the Basic Technology Knowledge course at the Military Academy.
b. Improvement of Learning Design. This research will design effective

learning plans in line with Basic Cyber Knowledge studies at the Military Academy. Thus, the research outcomes will assist in developing better learning methods to face increasingly complex cyber challenges.

c. Enhancement of Cyber Security. With a focus on testing and evaluating learning designs, this research will provide the necessary insights to understand the effectiveness and response to SQL injection attacks. This will aid in enhancing cyber security within the Military Academy environment and offer valuable knowledge to cadets in facing future cyber threats.

d. Contribution to Academic Literature. The findings of this research will contribute to academic literature in the fields of education and cyber security. The discoveries can serve as references and guides for future research in developing innovative and effective learning approaches for similar topics in military institutions and other educational bodies.