บทคัดย่อ

ชื่อเรื่อง : แนวทางการพัฒนาระบบบริหารจัดการภัยคุกคามทางไซเบอร์ของ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ ศูนย์บัญชาการทางทหาร

โดย : นาวาอากาศเอก อานนท์ เชิญธงไชย

สาขาวิชา : วิทยาศาสตร์ เทคโนโลยี และนวัตกรรม ทางด้านความมั่นคงและการทหาร

อาจารย์ที่ปรึกษาเอกสารวิจัย : **นาวาอากาศเอก**

(ศีพัฒน์ นามวัฒน์)

สิงหาคม ๒๕๖๓

การวิจัยในครั้งนี้มีวัตถุประสงค์เพื่อศึกษาทบทวน โครงสร้าง รูปแบบ ระบบบริหารจัดการ ปัญหาและอุปสรรค ของระบบการทำงานของเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมาและแนวโน้มการพัฒนาในอนาคต สำหรับนำมาประยุกต์ใช้ในการออกแบบพัฒนาระบบบริหารจัดการภัยคุกคามทางไซเบอร์ของ ศรซ.ศบท. เพื่อกำหนดแนวทางการพัฒนาตั้งแต่ระดับนโยบายและการนำไปสู่การปฏิบัติของหน่วยงานหลักที่สำคัญของ ศรซ.ศบท. อีกทั้งเป็นการเตรียมสร้างเป็นนวัตกรรมระบบฯ ต้นแบบ (Innovation Prototype) ให้สามารถพัฒนาต่อยอดได้อย่างสอดคล้องตามสถานการณ์หรือบริบททางไซเบอร์ของประเทศต่อไป

วิธีดำเนินการวิจัย ผู้วิจัยใช้กระบวนการวิจัยเชิงคุณภาพ (Qualitative Research) แบบวิจัยเอกสาร (Documentary Research) และการสัมภาษณ์เชิงลึก (In-depth Interview) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) ที่ได้มาจากการสัมภาษณ์กลุ่มเป้าหมาย ได้แก่ ผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ และผู้ปฏิบัติที่มีหน้าที่เกี่ยวข้องโดยตรง รวมทั้งใช้ข้อมูลทุติยภูมิ (Secondary Data) ที่ได้จากการศึกษาหลักการ แนวคิด ทฤษฎีทางด้านความมั่นคงปลอดภัยไซเบอร์จากการทบทวนวรรณกรรมที่เกี่ยวข้อง พร้อมทั้งได้มีการนำแนวคิดการบริหารจัดการสมัยใหม่เป็นเครื่องมือในการวิเคราะห์เพื่อให้สามารถค้นพบแนวทางการพัฒนาตามวัตถุประสงค์ของงานวิจัยที่กำหนด

ผลการวิจัยพบว่า แนวทางพัฒนาระบบบริการจัดการระบบบริหารจัดการภัยคุกคามทางไซเบอร์ของ ศรช.ศบท. เป็นการได้แนวทางที่ครอบคลุมทุกด้านตามหลักการบริหาร ตั้งแต่ กำลังพล กระบวนการในการบริหารจัดการ จากการผนึกกำลัง ประสานความร่วมมือในทุกส่วนที่เกี่ยวข้องอย่างบูรณาการ โดยใช้ทรัพยากรทางด้านไซเบอร์ที่มีเทคโนโลยีสูงตามมาตรฐานสากลให้เกิดความคุ้มค่าด้านงบประมาณ ตลอดจนสามารถปรับปรุงพัฒนาให้สอดคล้องกับบริบทของกองทัพไทยและระดับประเทศต่อไปได้ในอนาคต

ทั้งนี้หน่วยงานไซเบอร์ในกองทัพไทยต้องเตรียมความพร้อมของ กำลังพล กระบวนการและพัฒนาต่อยอดจากเทคโนโลยีที่มีอยู่ในการปฏิบัติการร่วมกันในการบูรณาการให้มีประสิทธิภาพอย่างจริงจัง ตามกลยุทธ์ที่วิจัยได้ จำนวน ๔ ด้าน ซึ่งประกอบด้วย กลยุทธ์เชิงรุก กลยุทธ์เชิงรับ กลยุทธ์เชิงแก้ไข และกลยุทธ์เชิงป้องกัน แต่ละกลยุทธ์ควรต้องมีการปฏิบัติที่ประสานสอดคล้องกันทั้งในระดับนโยบายและการนำไปสู่การปฏิบัติให้เป็นไปอย่างมีประสิทธิภาพ เป็นพื้นฐานสำคัญสำหรับเตรียมการบูรณาการกับหน่วยงานภาคส่วนอื่นของประเทศในการปฏิบัติการร่วมในสถานการณ์วิกฤตระดับประเทศต่อไป

ABSTRACT

Title : Cyber Security Management Systems Guidelines for the Royal Thai Armed Forces Joint Cyberspace Operations Center

By : Group Captain Arnon Choenthongchai

Major Field : Science Technology and Innovation of military security

Research Advisor : GP.Capt

(Sipat Namwat)

August 2020

The purpose of this research is to study and review the current obstacles of cyber security management systems and recommend the future development guidelines for the Joint Cyber Space Operations Center (JCOC) under the Military Operations Center (MOC). The guidelines will be considered from the policy level to the operational level in the JCOC. They will be used to provide an innovation prototype that can be further developed in accordance with Thailand's cyber situations or contexts.

In method, the researcher used qualitative approach by documentary research and in-depth interview using primary data obtained from interviewees who are experts and have direct responsibilities. The researcher will also include the use of secondary data derived from the studying of the principles, concepts, theories of cyber security from relevant literature reviews with the introduction of modern management concepts as an analytical tool in order to be finding the appropriate development guidelines in accordance with the research objectives

The result of the research shows that Guideline for Development Cyber Security of Royal Thai Armed Forces Joint Cyberspace Operations Center Management Systems is cover all aspects according to management principles, from personnel to management processes. From synergies collaboration in all areas related highly integrated by using high-tech cyber resources to meet international standards to create value as well as able to improve and develop in accordance with the context of the Thai military and the national level in the future.

In this regard, the cyber divisions in the Thai Armed Forces must prepare the personnel, process and develop further from the existing technology in the joint operation in order to effectively integrate seriously. According to the research strategy, there are 4 aspects which consist of proactive strategies, preventive strategies, responsive strategies, and passive strategies. Each strategy should have consistent practices at both the policy level and operational level. It is an important to coordinate with other agencies of the country in the joint operations at the national level.

.