บทคัดย่อ

ชื่อเรื่อง : แนวทางการพัฒนาระบบเทคโนโลยีสารสนเทศทางไซเบอร์เพื่อรองรับภารกิจการบรรเทาสาธารณภัยกองทัพอากาศ

โดย : นาวาอากาศเอก ฐาปนา ม่วงน้อยเจริญ

สาขาวิชา : การปฏิบัติการร่วม/ผสม

อาจารย์ที่ปรึกษาเอกสารวิจัย : **พันเอก**
(ชวลิต ประดิษฐ์นวกุล)
กรกฎาคม ๒๕๖๔

การวิจัยเรื่อง แนวทางการพัฒนาระบบเทคโนโลยีสารสนเทศทางไซเบอร์เพื่อรองรับภารกิจการบรรเทาสาธารณภัยกองทัพอากาศ มีวัตถุประสงค์เพื่อศึกษาพระราชบัญญัติป้องกันและบรรเทาสาธารณภัย แผนป้องกันและบรรเทาสาธารณภัยแห่งชาติ รวมทั้งแนวทางการปฏิบัติที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศด้านไซเบอร์ของกองทัพอากาศ ในการสนับสนุนการใช้ข้อมูลสารสนเทศสำหรับรองรับภารกิจการบรรเทาสาธารณภัยของกองทัพอากาศ และพัฒนาระบบเทคโนโลยีสารสนเทศด้านไซเบอร์ในการบริหารจัดการการบรรเทาสาธารณภัยของกองทัพอากาศ

งานวิจัยนี้เป็นการวิจัยเอกสาร เป็นการศึกษาข้อมูลจากแหล่งข้อมูลทุติยภูมิ ซึ่งเอกสารที่นำมาใช้ในการศึกษาและวิเคราะห์เป็นเอกสารของทางราชการเกี่ยวกับพระราชบัญญัติ ยุทธศาสตร์ นโยบาย แผนแม่บทการบรรเทาสาธารณภัยกองทัพอากาศ และหลักนิยม แนวความคิดการปฏิบัติ เกี่ยวกับเทคโนโลยีด้านไซเบอร์ รวมทั้งระบบเทคโนโลยีสารสนเทศ เพื่อนำมาประยุกต์ใช้ในภารกิจบรรเทาสาธารณภัยของกองทัพอากาศ ภายใต้ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) เพื่อให้เกิดประโยชน์สูงสุดต่อกองทัพอากาศ

ผลการศึกษาและวิเคราะห์เอกสารที่เกี่ยวข้อง พบว่า เทคโนโลยีด้านไซเบอร์ (Cyberspace Operations) การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) และเทคโนโลยีสารสนเทศ เป็นนวัตกรรมใหม่ที่มีความฉลาด และมีการประมวลผลการปฏิบัติที่ถูกต้องรวดเร็วอย่างเป็นระบบ เมื่อนำมาประยุกต์ใช้ร่วมกับแผนแม่บทการบรรเทาสาธารณภัยกองทัพอากาศ จะทำให้เกิดการบริหารข้อมูลที่มีระบบรักษาความปลอดภัยที่ได้มาตรฐาน จะสามารถเพิ่มขีดความสามารถในการปฏิบัติภารกิจบรรเทาสาธารณภัยของ

กองทัพอากาศให้เกิดประสิทธิภาพสูงสุด และยังสามารถบูรณาการใช้ข้อมูลสารสนเทศต่าง ๆ ที่เกี่ยวข้องนี้ร่วมกับหน่วยงานภายนอก เพื่อเพิ่มประสิทธิภาพในการปฏิบัติภารกิจบรรเทาสาธารณภัยของกองทัพอากาศ รวมทั้งเป็นไปตามยุทธศาสตร์กองทัพอากาศ ๒๐ ปี ด้วย

ผลการวิจัยพบว่า เมื่อนำผลการวิเคราะห์มากำหนดแนวทางพัฒนาระบบเทคโนโลยีสารสนเทศด้านไซเบอร์ในการบริหารจัดการบรรเทาสาธารณภัยร่วมกับหน่วยงานที่เกี่ยวข้อง ภายใต้การบริหารข้อมูลที่มีระบบรักษาความปลอดภัยที่ได้มาตรฐาน ประการแรก คือ แนวทางปฏิบัติในการสื่อสารและโทรคมนาคม การติดต่อสื่อสารมีความสำคัญอย่าง มากในการจัดการในภาวะฉุกเฉิน เนื่องจากต้องมีการประสานการปฏิบัติในการจัดการสาธารณภัยอย่างต่อเนื่อง รวมทั้งการแลกเปลี่ยนข้อมูล (Information) ข่าวสาร (Intelligence) เพื่อแจ้งเตือนภัยแก่ประชาชน ประสานงาน ควบคุม สั่งการ และรายงานผลการปฏิบัติงาน ระหว่างหน่วยเผชิญเหตุด้วยกันกับหน่วยงานที่มี หน้าที่สนับสนุนการเผชิญเหตุในด้านต่าง ๆ ประการที่สอง คือ แนวทางการดำเนินการสนับสนุนการปฏิบัติงานในภาวะฉุกเฉิน จำเป็นต้องมีระบบสื่อสารและโทรคมนาคม ทั้งระบบสื่อสารหลัก ระบบสื่อสารรองและ ระบบสื่อสารสำรอง ตลอดจนให้บริการฐานข้อมูลด้านสารสนเทศและการสื่อสารให้สามารถใช้การได้ ในทุกสถานการณ์ ประการที่สาม คือ แผนผนึกกำลังและทรัพยากรเพื่อการป้องกันประเทศเพื่อระดมทรัพยากรด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ประการที่สี่ คือ แผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ ในเรื่องการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ พัฒนาขีดความสามารถในการปกป้องป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยทางไซเบอร์ โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ และเสริมสร้างเครือข่ายความร่วมมือกับทุกภาคส่วนทั้งภายในและภายนอกกองทัพอากาศ และประการสุดท้าย คือ พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั้งภายในและภายนอกกองทัพอากาศ โดยหน่วยงานต้องมีความพร้อมด้านเทคโนโลยีสารสนเทศและการสื่อสาร ในการปฏิบัติตามแผนและ สนับสนุนการดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสารในภาวะปกติ เพื่อให้มีแนวทางดำเนินการ และป้องกันลดผลกระทบ บรรเทาและระงับสถานการณ์ในภาวะไม่ปกติ

ABSTRACT

Title : Guideline to Implementation of Cyber Information Technology in Supporting the Royal Thai Air Force's missions regarding disaster relief

By : Group Captain Tapana Muongnoicharoen

Major Field : Joint Operations

Research Advisor : **Colonel**

(Chavalit Praditnawakul)

July 2021

This research aims to explore the use of information technology : IT in achieving the missions within the Royal Thai Air Force concerning a disaster relief. It would examine through Thailand's Disaster Prevention and Mitigation Acts, a National Disaster Management handbook as well as RTAF's existing plans which include the implementation of cyber technology. Such technology provides key information to cover any missions regarding disaster relief, that could help to deliver the IT system that could manage those aforementioned missions in crisis time.

Also, the study would be represented as a documentary research majorly based on secondary sources such as relevant acts, strategies, policies, and RTAF's master plan. Other significant sources, for instance, RTAF's 20 year Strategy (2018 - 2037) would be an asset in this study when the core value of humanitarian and disaster relief mission needs to be explained.

Considering the data and assessed materials, it reveals that the integration of cyberspace operations, network centric operations and information technology when adapted to the RTAF's master plan in disaster relief could contribute a more successful, systematic and efficient outcome for its missions. It could as well bring a high performance in information management and security system that benefits positive actions during a state

of emergency. This could help RTAF to share information among other working units inside and outside its organization to assure the most efficient outcome in such urgent time.
An analysis to the findings could help to frame an action plan in developing the IT and cyberspace operations in supporting disaster relief's mission with corporation from relevant units, which are

1. Communication and telecommunication could perform a significant role during the state of emergency when multi-coordination is needed. This also brings an exchange, integration and sharing of information and intelligence, in terms of providing a credible source of such events to the civilians.

2. In providing an efficient communication, it is a requirement to build a supportive communication and telecommunication system where the main channel, assisting channel and spares are in its best performance and availability.

3. An action plan for join forces in protecting the nation could bring together the key element of information technology and communication.

4. A national security plan should be setting the agenda focusing a cybersecurity protection, an improvement of cyber operation capability that could prevent threats and a reinforcement of cybersecurity system.

To succeed the plan, it requires a full corporation from RTAF, public and private sectors, and the development in digital infrastructure. This could provide an efficiency, overall accessibility and potential manpower where every unit supports each other as one to perform active roles in a normal time and a role that could help to relieve, mitigate and support the humanitarian assistance in a state of emergency