ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย
Cyber Warfare Operation RTARF

น.อ.หญิง จินดา สระสมบูรณ์ ร.น.
รองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กองบัญชาการกองทัพไทย

Captain Jinda Sasomboon WRTN.
Deputy Director Military Information Technology Center
Royal Thai Armed Forces Headquarters
Email: jdsasom@hotmail.com

บทคัดย่อ

การวิจัยนี้ เป็นการวิจัยเชิงคุณภาพ ดำเนินการวิจัยโดยการศึกษา รวบรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ ในรูปแบบของคำอธิบายและแผนภาพ ทั้งจากเอกสาร รายงาน ผลการวิจัยที่เกี่ยวข้อง ได้แนวทางในการพัฒนารูปแบบและหลักการปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งการปฏิบัติเชิงรุกและเชิงรับ สำหรับเตรียมการหรือรองรับภัยคุกคามรูปแบบใหม่ที่อาศัยเครือข่ายในการปฏิบัติ รวมทั้งกำหนดบทบาทและโครงสร้างของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ในการปฏิบัติการสงครามไซเบอร์ ซึ่งการปฏิบัติการสงครามไซเบอร์เชิงรุก มีวิธีปฏิบัติประกอบด้วย การหลอกลวงฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามหยุดการให้บริการทางไซเบอร์ การทำลายระบบทางไซเบอร์ฝ่ายตรงข้าม และการเจาะระบบฝ่ายตรงข้าม ส่วนการปฏิบัติการสงครามไซเบอร์เชิงรับ มีวิธีปฏิบัติประกอบด้วย การปกป้องระบบ การทำให้ระบบสามารถระบุตัวตนผู้ใช้งานได้ การกู้คืนหรือการฟื้นคืนระบบ การค้นหาและปิดช่องโหว่ระบบ การปฏิบัติตามข้อกำหนดหรือมาตรฐานทางไซเบอร์ การบำรุงรักษาระบบ รวมถึงการปฏิบัติตามข้อกำหนดต่าง ๆ ทางกฎหมายหรือข้อบังคับทางไซเบอร์ โดยมีฝ่ายต่าง ๆ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ที่เกี่ยวข้องกับการปฏิบัติ คือ ฝ่ายกำลังพล ฝ่ายการข่าว ฝ่ายยุทธการ ฝ่ายส่งกำลังบำรุง ฝ่ายกิจการพลเรือน และฝ่ายสื่อสาร

คำสำคัญ: ปฏิบัติการ, สงครามไซเบอร์

ABSTRACT

This qualitative research was conducted by gathering related information from many reliable resources: related documents, reports and other studies through explanations and diagrams. The research resulted in the guidelines to develop and design the operational principles of military cyber warfare both in offensive and defensive in order to prepare defence for a new form of threat-related to using the networks to operate and to determine the role and the structure of the Royal Thai Armed Forces Headquarters for the cyber warfare operation. The cyber offensive operations were performed by deception, cyber service intrusion, system destruction and system penetration. The cyber defensive operations were performed by system protection, user identification system, system recovery, vulnerability scanning and prevention, the compliance of the cyber rules and standards, system maintenance as well as the compliance of the cyber laws and regulations. The offices under the Royal Thai Armed Forces involved in the operation were Directorate of Joint Personnel, Directorate of Joint Intelligence, Directorate of Joint Operations, Directorate of Joint Logistics, Directorate of Civil Affairs and Directorate of Joint Communications.

Keyword: Cyber Warfare, Cyber Warrior, Malware, Cyber Security

บทนำ

การเตรียมความพร้อมเพื่อปฏิบัติการสงครามไซเบอร์ (Cyber Warfare Operation) พื้นที่การรบที่ 5 เพื่อคุ้มครองปกป้องข้อมูลข่าวสาร บุคคล องค์กร และอธิปไตยของชาติ ต้องดำเนินการอย่างเร่งด่วน โดยกำหนดหลักนโยบายและแนวปฏิบัติทั้งทางยุทธศาสตร์และยุทธวิธีหรือเทคนิควิธี ที่เป็นปัจจัยสำคัญในการพัฒนาความมั่นคงปลอดภัยด้านไซเบอร์ ให้กับกองบัญชาการกองทัพไทย เนื่องจากเป็นยุทธวิธีรูปแบบใหม่ที่มีการนำมาใช้ในการพัฒนากิจการงานด้านการทหาร ทั้งนี้มีหลายประเทศชั้นนำอย่างสหรัฐ รัสเซีย และจีน ต่างใช้เป็นเครื่องมือในการกระทำกับฝ่ายตรงข้าม เพื่อทำลายระบบต่าง ๆ ไม่ว่าจะเป็นระบบการควบคุมการบังคับบัญชา โครงสร้างพื้นฐานสำคัญของประเทศ (Infrastructure) รวมถึงการได้มาซึ่งข้อมูลข่าวสารสำคัญ (Information Critical) หรือการฝังตัวการโจมตีในรูปแบบใหม่ (Root kit) ที่ใช้หลักการเขียนตรรกะทางโปรแกรม (Logical Programming) แทนกำลังพลและยุทโธปกรณ์ทางทหาร (Armament)

การปฏิบัติการสงครามไซเบอร์จึงกลายเป็นอาวุธหรือเครื่องมือในการปฏิบัติการสงครามในทุกระดับ ตั้งแต่การดำเนินการด้านความขัดแย้งพื้นฐานสู่การต่อสู้ตั้งแต่ระดับยุทธบริเวณไปจนถึงระหว่างประเทศหรือภูมิภาค มีการกระทำทั้งในทางลับและเปิดเผย โดยบูรณาการความรู้และเทคโนโลยีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) เทคโนโลยีสารสนเทศและเครือข่าย (Information and Communication Technology) วิศวกรรมอิเล็กทรอนิกส์ (Electronic Engineering) การใช้ข้อมูลตั้งแต่ระดับสัญญาณ (Signal) ตัวอักษร (Character) ข้อมูล (Data) และเนื้อหา (Content) ในสื่อสังคม (Social Media) ที่ได้รวบรวมอยู่ในระบบโปรแกรม (Application) รวมถึงสื่อสังคมออนไลน์ (Social Network) ปัจจุบันปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย หรือกองทัพอื่น ยังมิได้กำหนดความชัดเจนตั้งแต่ระดับนโยบาย สั่งการ และหลักการปฏิบัติ การวิจัยครั้งนี้ ก็เพื่อศึกษา เสนอแนะและกำหนดความชัดเจนต่าง ๆ ดังกล่าวข้างต้น เพื่อให้เกิดแนวคิดในการดำเนินการด้านการปฏิบัติการสงครามไซเบอร์และสามารถนำไปปรับใช้กับกองบัญชาการกองทัพไทย

แม้ว่ากองบัญชาการกองทัพไทย จะมีการเตรียมความพร้อมเรื่องโครงสร้างองค์กรด้านปฏิบัติการสงครามไซเบอร์อยู่ในระดับหนึ่ง คือมีการจัดตั้งกองสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร เพื่อกำหนดยุทธศาสตร์ด้านความมั่นคงไซเบอร์กองทัพไทย กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร และกองพันปฏิบัติการสงครามอิเล็กทรอนิกส์ กรมการสื่อสารทหาร เพื่อดำเนินการด้านการปฏิบัติการสงครามไซเบอร์ แต่ก็ยังขาดรูปแบบและแนวคิดการปฏิบัติการสงครามไซเบอร์ การกำหนดบทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบอย่างชัดเจน การพัฒนาความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ ซึ่งหากมีการบูรณาการและกำหนดนโยบาย รวมถึงแนวปฏิบัติไว้อย่างชัดเจน ก็จะเกิดประโยชน์อย่างสูงสุดต่อการคุ้มครองปกป้องข้อมูลข่าวสาร บุคคล องค์กร รวมถึงอธิปไตยของประเทศ

วัตถุประสงค์ของการวิจัย

1. ศึกษาและวิเคราะห์หลักปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งการปฏิบัติเชิงรุกและเชิงรับ สำหรับเตรียมการหรือรองรับภัยคุกคามรูปแบบใหม่ที่อาศัยเครือข่ายในการปฏิบัติ

2. เสนอแนะแนวทางปฏิบัติการสงครามไซเบอร์ ศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย

ขอบเขตของการวิจัย

1. เน้นการวิจัยด้านการกำหนดรูปแบบและแนวคิดการปฏิบัติการสงครามไซเบอร์ของศูนย์

บัญชาการทางทหาร กองบัญชาการกองทัพไทย

2. การกำหนดบทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบ ความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ รวมถึงปฏิบัติการสงครามไซเบอร์เฉพาะของกองบัญชาการกองทัพไทย

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ ดำเนินการวิจัยโดยการศึกษา รวบรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ ในรูปแบบของคำอธิบายและแผนภาพ ทั้งจากเอกสาร รายงานผลการวิจัยที่เกี่ยวข้อง เพื่อให้ได้แนวทางในการพัฒนารูปแบบปฏิบัติการสงครามไซเบอร์ บทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบ ความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ รวมถึงการปฏิบัติการสงครามไซเบอร์ ที่เหมาะสมกับกองบัญชาการกองทัพไทย

ประโยชน์ที่ได้รับจากการวิจัย

1. เกิดความเข้าใจในการปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งหลักการปฏิบัติเชิงรุกและเชิงรับ เพื่อใช้เป็นหลักปฏิบัติในการเตรียมความพร้อมทั้งในยามปกติและยามสงคราม ที่อุบัติขึ้นในยุคเทคโนโลยีสารสนเทศ ขยายตัวครอบคลุมไปทั่วโลก และเชื่อมโยงข้อมูลข่าวสาร บุคคล และองค์กร ด้วยเครือข่ายสังคมออนไลน์

2. สามารถนำความรู้ที่ได้มาปรับใช้กับปฏิบัติการสงครามไซเบอร์ ของกองบัญชาการกองทัพไทย ทั้งด้านการกำหนดรูปแบบการปฏิบัติการกำหนดโครงสร้างหน่วยงาน และความรับผิดชอบต่อการปฏิบัติและการจัดเตรียมกำลังพลรวมถึงยุทโธปกรณ์ที่สำคัญสนับสนุนการปฏิบัติ

การทบทวนวรรณกรรม

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในปัจจุบัน เป็นสิ่งที่มีความจำเป็นอย่างมาก เนื่องจากทุกสิ่งทุกอย่างรอบตัวเรา มีความสัมพันธ์กับข้อมูลสารสนเทศในทุก ๆ ด้าน ไม่ว่าจะเป็นเรื่องส่วนตัว หรือเรื่องงานสิ่งต่าง ๆ เหล่านี้ มีการใช้งานที่สะดวกสบายมากขึ้น แต่สิ่งที่ต้องให้ความสนใจและระมัดระวังคือเรื่องของความมั่นคงปลอดภัยด้านสารสนเทศ ใน 3 ด้านคือ การรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) เพื่อเป็นหลักพื้นฐานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในส่วนขององค์กรก็เป็นอีกส่วนหนึ่งที่ต้องให้ความสำคัญในการรักษาความมั่นคงปลอดภัย เพื่อให้เกิดความมั่นใจในการใช้บริการข้อมูลต่าง ๆ ทั้งหน่วยงานเอกชน และหน่วยงานภาครัฐ โดยเฉพาะหน่วยงานภาครัฐ ด้านความมั่นคง ตระหนักรู้และให้ความสำคัญในประเด็น Cyber Security มากขึ้น ทั้งการทำงานในเชิงรับ (Defensive) เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดี ทั้งที่เป็นการกระทำที่มีรัฐบาลสนับสนุน (State Sponsor) หรือเป็นการทำโดยกลุ่มผู้ไม่หวังดีที่ต้องการทำลายชื่อเสียงหรือขโมยข้อมูล และการทำงานเชิงรุก (Offensive) เพื่อการเข้าโจมตีระบบสารสนเทศของประเทศ หรือหน่วยงานอื่น ๆ ทั้งเพื่อให้ได้มาซึ่งข้อมูล และทำลายระบบไม่ให้สามารถใช้งานได้ ซึ่งปัจจุบันประเทศต่าง ๆ เช่น สหรัฐ จีน เกาหลีใต้ ตุรกี ได้มีการจัดหน่วยงานรับผิดชอบการปฏิบัติการด้านไซเบอร์ และสร้างบุคลากรเพื่อเตรียมพร้อมรับมือกับภัยคุกคามในทุกด้าน นอกจากการดำเนินการทางด้านเทคนิค ยังต้องมีการดำเนินการในเรื่องของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นแนวทางในการปฏิบัติให้กับส่วนราชการ หรือหน่วยงานเอกชน ซึ่งถือเป็นการทำด้านกระบวนการ (Process) ต่อมาในการทำในเรื่องบุคลากร (People) การจัดการให้ความรู้ (Knowledge) เพื่อให้สามารถปฏิบัติงานในด้านความมั่นคงปลอดภัยได้อย่างถูกต้อง และมีประสิทธิภาพ สุดท้ายคือเทคโนโลยี (Technology) คือการที่มีระบบ

หรืออุปกรณ์ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ช่วยในการป้องกันการบุกรุก หรือใช้ในการโจมตี (Hacking) เครือข่ายอื่น ๆ ในระบบสงครามไซเบอร์ การกำหนดหน่วยความรับผิดชอบมีความจำเป็นอย่างสูง เพื่อเป็นการเตรียมความพร้อมทั้งความรู้ความสามารถกำลังพล และอาวุธยุทโธปกรณ์ ที่เหมาะสมต่อการปฏิบัติการสงครามไซเบอร์

ผลการวิจัย

การปฏิบัติการสงครามไซเบอร์ของศูนย์บัญชาการทางทหาร (ศบท.) กองบัญชาการกองทัพไทย ผู้วิจัยได้ดำเนินการตามขั้นตอนของการวิจัย ได้ผลการวิจัยสำหรับการปฏิบัติการสงครามไซเบอร์ ดังนี้

1. นโยบายและแนวปฏิบัติของปฏิบัติการสงครามไซเบอร์

ปฏิบัติการสงครามไซเบอร์ เป็นการปฏิบัติการโดยใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายเป็นหลัก เกิดการปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations, CNO) จากการศึกษารวบรวมข้อมูลผู้วิจัยจึงกำหนดการปฏิบัติที่สำคัญ แบ่งออกเป็น ๒ ด้าน คือ การปฏิบัติการไซเบอร์เชิงรุก (Cyber Offensive Operations) และการปฏิบัติการไซเบอร์เชิงรับ (Cyber Defensive Operations) โดยมีฝ่ายต่าง ๆ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ที่เกี่ยวข้องกับการปฏิบัติคือ ฝ่ายกำลังพล ฝ่ายการข่าว ฝ่ายยุทธการ ฝ่ายส่งกำลังบำรุง ฝ่ายกิจการพลเรือน และฝ่ายสื่อสาร

1.1 การปฏิบัติการสงครามไซเบอร์เชิงรุก มีวิธีปฏิบัติประกอบด้วย การหลอกลวงฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามหยุดการให้บริการทางไซเบอร์ การทำลายหรือรบกวนระบบต่าง ๆ และการเจาะระบบฝ่ายตรงข้าม

1.2 การปฏิบัติการสงครามไซเบอร์เชิงรับ มีวิธีปฏิบัติประกอบด้วย การปกป้องระบบ การทำให้ระบบสามารถระบุตัวตนผู้ใช้งานได้ การกู้คืนหรือการฟื้นคืนระบบ การค้นหาและปิดช่องโหว่ระบบ การปฏิบัติตามข้อกำหนดหรือมาตรฐานทางไซเบอร์ การบำรุงรักษาระบบ รวมถึงการปฏิบัติตามข้อกำหนดต่าง ๆ ทางกฎหมายหรือข้อบังคับทางไซเบอร์

2. กระบวนการปฏิบัติการสงครามไซเบอร์สำหรับการปฏิบัติภายในและภายนอก ดังนี้

2.1 การปฏิบัติการสงครามไซเบอร์ ที่ต้องปฏิบัติภายใน (Internal Cyber Warfare Operation) ประกอบด้วย การประเมินและการตรวจสอบ (Evaluations & Audits) การพิสูจน์ การตรวจสอบ และการรับรอง (Verification, Validation & Certification) การทดสอบการเจาะระบบ และการค้นหาช่องโหว่ (Penetration Testing & Vulnerability Scanning) การตรวจจับและป้องกันการบุกรุก (Intrusion Detection & Prevention) การรักษาความปลอดภัยส่วนบุคคล การฝึกอบรม และการสร้างความตระหนัก (Personnel Security, Training & Awareness) การสืบสวน (Forensics) การควบคุมการเข้าถึง (Access Control) การกู้คืนภัยพิบัติ (Disaster Recovery) การบริหารจัดการการปฏิบัติการ (Operations Management) การเข้ารหัส (Encryption) และนโยบายและกระบวนการ (Policies & Procedures)

2.2 การปฏิบัติการสงครามไซเบอร์ ที่ต้องปฏิบัติภายนอก (External Cyber Warfare Operation) ประกอบด้วย การโจรกรรมข้อมูล (Hacking) การแทรกการโจมตีผ่านทางช่องโหว่ (Vulnerability Injections) การพัฒนามัลแวร์และสปายแวร์ (Malware & Spyware Development) การเฝ้าระวังเครือข่ายและข่าวกรอง (Network Surveillance & Intelligence) และการบริการและการตรวจจับช่องโหว่ (Service & Vulnerability Detection)

3. รูปแบบที่เหมาะสมของปฏิบัติการสงครามไซเบอร์ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ฝ่ายต่าง ๆ มีหน้าที่ โดยสรุป ดังนี้

3.1 ฝ่ายกำลังพล มีหน้าที่เกี่ยวกับการสรรหากำลังพล พัฒนากำลังพล ที่มีความสามารถในด้านการปฏิบัติการสงครามไซเบอร์ ทั้งที่เป็นข้าราชการ และจากบุคคลพลเรือน รวมถึงให้มีการฝึกฝนและเรียนรู้วิธีการและเทคนิคการทำสงครามไซเบอร์แบบใหม่ ๆ เพื่อเตรียมความพร้อมให้กับกำลังพลสามารถรับมือกับการปฏิบัติการสงครามไซเบอร์

3.2 ฝ่ายการข่าว มีหน้าที่ในการจัดทำข้อมูลทำเนียบกำลังรบทางด้านการปฏิบัติการสงครามไซเบอร์ของประเทศเพื่อนบ้าน การข่าวกรองการปฏิบัติการสงครามไซเบอร์ที่เกิดขึ้นในภูมิภาคต่าง ๆ ของโลก และวาดภาพสนามรบทางไซเบอร์

3.3 ฝ่ายยุทธการ มีหน้าที่กำหนดยุทธศาสตร์และหลักนิยมการปฏิบัติการสงครามไซเบอร์ ให้กับแต่ละฝ่ายที่ปฏิบัติงานในศูนย์บัญชาการทางทหาร

3.4 ฝ่ายส่งกำลังบำรุง มีหน้าที่จัดหาความต้องการ และยุทโธปกรณ์ที่ใช้ในการปฏิบัติการสงครามไซเบอร์

3.5 ฝ่ายกิจการพลเรือน มีหน้าที่ประสานงานกับหน่วยงานภาครัฐและเอกชน ที่มีความรู้ความสามารถในการปฏิบัติงานด้านไซเบอร์ เมื่อเกิดการทำสงครามทางไซเบอร์ การปิดช่องทางการเชื่อมต่อเครือข่ายในระดับประเทศ และการปฏิบัติการจิตวิทยาและประชาสัมพันธ์ ให้กับประชาชนและฝ่ายตรงข้าม

3.6 ฝ่ายสื่อสาร มีหน้าที่จัดการสื่อสาร เครื่องมือและกำลังพล เพื่อรองรับการปฏิบัติการสงครามไซเบอร์ การปฏิบัติการด้านการป้องกันไซเบอร์ และสนับสนุนการปฏิบัติการด้านการโจมตีทางไซเบอร์

4. มาตรการส่งเสริมการปฏิบัติที่มีประสิทธิภาพ

4.1 การปฏิบัติที่สอดคล้องกันระหว่างฝ่ายยุทธการ ที่ต้องกระทำต่อฝ่ายตรงข้าม และฝ่ายสื่อสารที่ต้องปกป้องฝ่ายเราและสนับสนุนการปฏิบัติฝ่ายยุทธการ รวมถึงการให้กองบัญชาการกองทัพไทยสนับสนุนการปฏิบัติศูนย์บัญชาการทางทหาร

4.2 เทคโนโลยีและยุทโธปกรณ์ที่ใช้ในการปฏิบัติการสงครามไซเบอร์ที่ต้องมีอย่างเหมาะสมสำหรับการปฏิบัติการ

ข้อเสนอแนะ

1. การปฏิบัติการสงครามไซเบอร์ มีความสลับซับซ้อนทั้งในการกำหนดขอบเขตการปฏิบัติ และวิธีการปฏิบัติ ในสถานการณ์ที่ไม่สามารถกำหนดเป้าหมายการโจมตีได้ด้วยวิธีการลาดตระเวนหาข่าวหรือการสอดแนม จึงจำเป็นต้องอาศัยกำลังพลหรือบุคลากรเฉพาะทางที่มีความรู้ความสามารถทางด้านการรักษาความมั่นคงไซเบอร์ ระบบเครือข่ายคอมพิวเตอร์ และการบริหารจัดการฐานข้อมูล รวมถึงการพัฒนาโปรแกรม ประกอบกับความคิดสร้างสรรค์ การส่งเสริมความก้าวหน้า รวมถึงผลตอบแทนที่เป็นแรงจูงใจ จึงต้องกำหนดขึ้นในระดับนโยบายของหน่วยงาน และให้สามารถตอบสนองได้อย่างเป็นรูปธรรม จะเกิดประโยชน์สูงสุดต่อการเตรียมความพร้อมต่อการปฏิบัติการสงครามไซเบอร์ทั้งปัจจุบันและอนาคต

2. การปฏิบัติการสงครามไซเบอร์จะต้องเป็นความร่วมมือระหว่างหน่วยงานทหาร หน่วยงานด้านความมั่นคง หน่วยงานภาครัฐ พลเรือน เอกชน และสถาบันการศึกษา

3. การจัดให้มีศูนย์ปฏิบัติการทดสอบการปฏิบัติการสงครามไซเบอร์ เพื่อให้สามารถดำเนินการได้อย่างแม่นยำตามขอบเขตของฝ่ายยุทธการกำหนด และเพื่อลดความผิดพลาดในการปฏิบัติที่อาจจะเกิดขึ้นได้เมื่อฝ่ายตรงข้ามปฏิบัติการตอบโต้

4. การส่งเสริมงานวิจัยและพัฒนางานตามแผนงานโครงการของการปฏิบัติการสงครามไซเบอร์ ระบบเครือข่ายคอมพิวเตอร์ การพัฒนาโปรแกรม สำหรับเป็นเครื่องมือในการปฏิบัติการสงครามไซเบอร์ทั้งเชิงรับและเชิงรุก ต้องได้รับการสนับสนุนอย่างจริงจัง รวมถึงต้องปรับปรุงขั้นตอนการปฏิบัติงานการวิจัยและพัฒนางานแผนงานโครงการไม่ให้เกิดความยุ่งยาก

ซับซ้อน ลดการดำเนินการทางธุรการหรือทางเอกสาร ให้เหมาะกับผู้ทำการวิจัยและพัฒนา รวมถึงผู้ปฏิบัติงานโครงการ

บรรณานุกรม

รหัสลับสงครามไซเบอร์ เข้าถึงได้จาก http://www.lokwannee.com/web2013/?p=101022

ริชาร์ด เอ. คลาร์ก และ โรเบิร์ต คเนค. **สงครามไซเบอร์ (CYBER WAR)**. สำนักพิมพ์มติชน กุมภาพันธ์, 2555

สงครามไซเบอร์ เข้าถึงได้จาก http://www.dstd.mi.th/board/index.php?topic=893.0

สงครามไซเบอร์ (Cyber Warfare) เข้าถึงได้จาก http://www.rtarf.mi.th/pdf/712557.pdf

Computer Network Operations เข้าถึงได้จาก https://www.nsa.gov/careers/career__fields/netopps.shtml

Cyberwarefare in the Umited States เข้าถึงได้จาก http://en.wikipedia.org/wiki/Cyberwarfare__in__the__United__States

Herbert S. Lin. **Offensive Cyber Operations and the Use of Force** เข้าถึงได้จาก http://jnslp.com/wp-content/uploads/2010/08/06__Lin.pdf

Cyber Warfare Operation RTARF

Captain Jinda Sasomboon WRTN.
Deputy Director Military Information Technology Center
Royal Thai Armed Forces Headquarters
Email: jdsasom@hotmail.com

ABSTRACT

This qualitative research was conducted by gathering related information from many reliable resources: related documents, reports and other studies through explanations and diagrams. The research resulted in the guidelines to develop and design the operational principles of military cyber warfare both in offensive and defensive in order to prepare defence for a new form of threat-related to using the networks to operate and to determine the role and the structure of the Royal Thai Armed Forces Headquarters for the cyber warfare operation. The cyber offensive operations were performed by deception, cyber service intrusion, system destruction and system penetration. The cyber defensive operations were performed by system protection, user identification system, system recovery, vulnerability scanning and prevention, the compliance of the cyber rules and standards, system maintenance as well as the compliance of the cyber laws and regulations. The offices under the Royal Thai Armed Forces involved in the operation were Directorate of Joint Personnel, Directorate of Joint Intelligence, Directorate of Joint Operations, Directorate of Joint Logistics, Directorate of Civil Affairs and Directorate of Joint Communications.

Keyword: Cyber Warfare, Cyber Warrior, Malware, Cyber Security

Preface

The preparation for Cyber Warfare Operations, the battlefield area 5 to protect information, citizen, the organization and the sovereignty must have been urgently carried out by setting the policy and the guidelines of strategy, artifice and technique that were basic factors to develop the cyber security for the Royal Thai Armed Forces since it was a new artifice to develop the military affairs. Many of the world's leading countries such as the United States of America, Russia and China had performed such operations to attack their antagonists' command control system and infrastructure, access to critical information or made a root-kit attack by logical programming instead of the armament.

Cyber warfare operations became a weapon or a tool used in every level of warfare from preliminary conflicts to war zone conflicts and to international or regional conflicts, disclosed or undisclosed. The cyber warfare was operated depending on the integration of knowledge and information security, information and communication technology, electronic engineering, signal usage, font character, data, content in social media appeared in application and social network. At presently, the policy, the command and the operational guideline of the cyber warfare operation by the Royal Thai Armed Forces Headquarters and others were vaguely defined. Therefore, this research aimed to study and bring forward apparent policies, commands and operations to trigger the concept for the cyber warfare operations that could be applied by the Royal Thai Armed Forces Headquarters.

Though having prepared the organizational structure for the cyber warfare operation such as the Cyber Warfare Command under Directorate of Joint Operations to determine the cyber security strategy of the Thai Armed Forces, the Cyber Security Command, the Military Technology Center and Electronic Warfare Battalion, the Directorate of Joint Communications to perform the cyber warfare operations, the Royal Thai Armed Forces Headquarters still lacked the principles and concepts of the cyber warfare operation, the clear definition of role and structure of the authorities and the availability improvement of the troops for the cyber warfare operation. Were the integrations, policies and guidelines set, it would maximize the benefits to ensure protection for information, people, organizations and sovereignty.

Objectives

1. To study and analyze the military cyber warfare operations both in offensive and defensive to prepare for a new form of threat relying on networks to operate.

2. To bring forward the guidelines of the cyber warfare operations for the Military Command Center, the Thai Royal Armed Forces Headquarters.

Scope of Research

1. The research focused on the system and the concept of the cyber warfare operations

of the Military Command Center, the Thai Royal Armed Forces Headquarters.

2. The research focused on defining roles and the structure of the responsible offices, the availability of troops against the cyber warfare operations as well as the cyber warfare operations, particularly for the Thai Royal Armed Forces Headquarters.

Research Methodology

This qualitative research was studied by gathering related information from the reliable resources: related documents, reports and other studies through explanations and diagrams. The purpose was to create the guideline to develop and design the operational principles of military Cyber Warfare, the roles and the structure of the related offices and the availability of troops for the cyber warfare operation, as well as the cyber warfare operation suitable for the Royal Thai Armed Forces Headquarters.

Research Benefits

1. Understanding the military cyber warfare operations in both offensive and defensive that were regarded as the practice principles in both peacetime and wartime that probably occurred in the information technology era that was now overwhelming the globe and connected information, individuals and organizations together via the social networks.

2. Applying knowledge to the cyber warfare operations of the Royal Thai Armed Forces Headquarters in framing the operational system and the structure of the office and its responsibility for the operation and preparation of troops and equipment in support.

Literature Review

Presently, the information security protection must have been prioritized since everything both personal and impersonal around was related to information technology. Though this technology resulted in more convenience, there were 3 things of information security that needed attention which are confidentiality, integrity and availability. Those three were the basic rules of security to protect information. Furthermore, the organizations both in public and private sectors must have prioritized the security of information to ensure the confidence in providing information services. Especially, the public security-related offices should have been aware of the importance of cyber security issues both in defensive operation to prevent from any antagonists supported by state sponsor or malicious groups that aim to discredit or penetrate information, and in offensive operations to hack another country's or organization's information system and destroy the system. Many countries, such as the United States of America, China, South Korea and Turkey, had established the organizations responsible for the cyber operations and prepared their people for threat in every aspect. Apart from the technical practice, it was necessary to exercise the policies on information security protection as the guideline for government offices or private organizations. Exercising the

policy was regarded as the process operations. Concerning people, they should have been equipped with knowledge so that they were capable of performing accurately security services. Lastly, technology was a system or a tool for information security protection, assisting intrusion prevention and hacking other networks. Amidst the cyber warfare, it was necessary to establish specialized organizations to prepare knowledgeable and skillful troops and suitable equipment enough for the cyber warfare operation.

Results

After researching on the cyber warfare operation of the Military Command Center, the Royal Thai Armed Forces Headquarters, the results were as follows.

1. Policy and Guideline for the Cyber Warfare Operation

The cyber warfare was operated through the computer and the network resulted in Computer Network Operations (CNO). According to the study, the operations were divided into 2 types; Cyber Offensive Operations and Cyber Defensive Operations. The offices under the Royal Thai Armed Forces involved in the operations were Directorate of Joint Personnel, Directorate of Joint Intelligence, Directorate of Joint Operations, Directorate of Joint Logistics, Directorate of Civil Affairs and Directorate of Joint Communications

1.1 Cyber Offensive Operations were deception, cyber service intrusion, system destruction and system penetration

1.2 Cyber Defensive Operations were system protection, user identification system, system recovery, vulnerability scanning and prevention, the compliance of the Cyber rules and standards, system maintenance as well as the compliance of the Cyber laws and regulations

2. Internal Cyber Warfare Operation and External Cyber Warfare Operation

2.1 Internal Cyber Warfare Operations were comprised of evaluations & audits, verification, validation & certification, penetration testing & vulnerability scanning, intrusion detection & prevention, personnel security, training & awareness, forensics, access control, disaster recovery, operation managements, encryption and policies & procedures.

2.2 External Cyber Warfare Operations were comprised of hacking, vulnerability injections, malware & spyware development, network surveillance & intelligence and service & vulnerability detection.

3. The structure for cyber warfare operation of the Military Command Center, the Thai Royal Armed Forces Headquarters was performed by the following directorates and duties.

3.1 Directorate of Joint Personnel was responsible for recruiting and developing troops capable of cyber warfare operation regardless of an officer or just a citizen. Moreover, it had to provide training and new technique for the troops to be able to handle the cyber warfare operation.

3.2 Directorate of Joint Intelligence was responsible for arranging information about the

neighbouring cyber warfare forces and gathering intelligence on the cyber warfare operations in any regions across the world, as well as plotting the cyber battlefield.

3.3 Directorate of Joint Operations was responsible for designing the strategy and the principles of the cyber warfare operation for other directorates under the Military Command Center.

3.4 Directorate of Joint Logistics was responsible for supplying any necessary equipment for the cyber warfare operation.

3.5 Directorate of Joint Civil Affairs was responsible for coordinating with public and private sectors qualified with the ability for the cyber operations, the shutdown of the domestic networks, the psychological acts and the public relations to citizen and antagonists in case the cyber warfare arose.

3.6 Directorate of Joint Communications was responsible for providing accurate communication, equipment and troops for the cyber warfare operation, the cyber defense operation and the support for the cyber offensive operation.

4. Promoting Measures for Effective Operation

4.1 There should have been the consistent cooperation between the Directorate of Joint Operations that act directly on an antagonist and the Directorate of Joint Communications, a supporter that also coordinated with the Royal Thai Armed Forces Headquarters, to support the operations of the Military Command Center.

4.2 Technology and equipment used in the cyber warfare operations must have been appropriately provided.

Suggestions

1. Cyber warfare operations can be complicated in specifying its scope and operation method. Under the situation where targets cannot be locked by patrol or spy, it is necessary to rely on people specialized in cyber security protection, network system and database management, program development combined with creativity, progress and good incentives. Those factors have to be written in the policy that can be substantially exercised. It will maximize the benefits for the preparation for the cyber warfare operations in both the present and the future.

2. Cyber warfare operations must be cooperated among the military offices, the security offices, the public sectors, the citizen, the private sectors and the educational institutions.

3. The Test Center for the cyber warfare operations should be established in order to practice accurate operations consistently with the scopes determined by the directorate of joint operations and reduce the operational mistakes to the least which might occur due to antagonists' counter-attack.

4. Research promotion and development, cyber warfare operations, project plan, and program development regarded as tools for the cyber offensive operations and the cyber

defensive operations must be pragmatically promoted. Moreover, the research development procedures and the project plan procedures have to be loosened, less complicated. Administrative and documentary procedures should be loosened to suit researchers, developers and project practitioners.

Bibliography

http://www.lokwannee.com/web2013/?p=101022. Secret Code of Cyber War.

Richard A.Clark and Robert Knake. **Cyber War.** Matichon Publisher, February, 2012.

http://www.dstd.mi.th/board/index.php?topic=893.0. **Cyber Warfare**.

https://www.nsa.gov/careers/career__fields/netopps.shtml. **Computer Network Operations.**

http://en.wikipedia.org/wiki/Cyberwarfare__in__the__United__States.**Cyber Warfare in the United States**.

http://jnslp.com/wp-content/uploads/2010/08/06__Lin.pdf. Herbert S. Lin, **Offensive Cyber Operations and the Use of Force**.