ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย

โดย

นาวาเอกหญิง จินดา สระสมบูรณ์
รองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร
กรมการสื่อสารทหาร

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๕๗
ประจำปีการศึกษา พุทธศักราช ๒๕๕๗ - ๒๕๕๘

บทคัดย่อ

เรื่อง ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย
ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี
ผู้วิจัย นาวาเอกหญิง จินดา สระสมบูรณ์ **หลักสูตร** วปอ. **รุ่นที่** ๕๗

การวิจัยนี้ เป็นการวิจัยเชิงคุณภาพ ดำเนินการวิจัยโดยการศึกษา รวบรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ ในรูปแบบของคำอธิบายและแผนภาพ รวมทั้งจากเอกสาร รายงาน และผลการวิจัยที่เกี่ยวข้อง ทำการวิเคราะห์ข้อมูลเหล่านั้น ได้แนวทางในการพัฒนารูปแบบและหลักการปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งการปฏิบัติเชิงรุกและเชิงรับ สำหรับใช้ในการเตรียมการ หรือรองรับภัยคุกคามรูปแบบใหม่ที่อาศัยเครือข่ายในการปฏิบัติ นอกจากนี้ยังได้กำหนดบทบาทและโครงสร้างของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย (ศบท.บก.ทท.) ในการปฏิบัติการสงครามไซเบอร์ ทั้งนี้การปฏิบัติการสงครามไซเบอร์เชิงรุก มีวิธีปฏิบัติที่ประกอบด้วยการหลอกลวงฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามหยุดการให้บริการทางไซเบอร์ การทำลายระบบทางไซเบอร์ของฝ่ายตรงข้าม และการเจาะระบบฝ่ายตรงข้าม ส่วนการปฏิบัติการสงครามไซเบอร์เชิงรับมีวิธีปฏิบัติประกอบด้วย การปกป้องระบบ การทำให้ระบบสามารถระบุตัวตนผู้ใช้งานได้ การกู้คืนหรือการฟื้นคืนระบบ การค้นหาและปิดช่องโหว่ระบบ การปฏิบัติตามข้อกำหนดหรือมาตรฐานทางไซเบอร์ การบำรุงรักษาระบบ รวมถึงการปฏิบัติตามข้อกำหนดต่าง ๆ ทางกฎหมายหรือข้อบังคับทางไซเบอร์ โดยมีฝ่ายต่าง ๆ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ที่เกี่ยวข้องกับการปฏิบัติร่วมกัน คือ ฝ่ายกำลังพล ฝ่ายการข่าว ฝ่ายยุทธการ ฝ่ายส่งกำลังบำรุง ฝ่ายกิจการพลเรือน และฝ่ายสื่อสาร

คำนำ

การเตรียมความพร้อมเพื่อปฏิบัติการสงครามไซเบอร์ พื้นที่การรบที่ ๕ เพื่อคุ้มครองปกป้องข้อมูลข่าวสาร บุคคล องค์กร และอธิปไตยของชาติ จึงต้องดำเนินการอย่างเร่งด่วนโดยกำหนดหลักนโยบายและแนวปฏิบัติทั้งทางยุทธศาสตร์และยุทธวิธีหรือเทคนิควิธี ที่เป็นปัจจัยสำคัญในการพัฒนาความมั่นคงปลอดภัยด้านไซเบอร์ ให้กับกองบัญชาการกองทัพไทย การปฏิบัติการสงคราม ไซเบอร์ (Cyber Warfare Operation) จึงกลายเป็นอาวุธหรือเครื่องมือในการปฏิบัติการสงครามในทุกระดับ ตั้งแต่การดำเนินการด้านความขัดแย้งพื้นฐาน สู่การต่อสู้ตั้งแต่ระดับยุทธบริเวณไปจนถึงระหว่างประเทศหรือภูมิภาค เพื่อป้องกันความสับสนในการปฏิบัติ การกำหนดนโยบาย สั่งการ การเตรียมความพร้อม การฝึก และการปฏิบัติการในภาวะสงคราม ทำให้ปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย หรือกองทัพอื่น ยังไม่มีการกำหนดความชัดเจนตั้งแต่ระดับนโยบาย สั่งการ และหลักการปฏิบัติ การวิจัยครั้งนี้ ก็เพื่อศึกษา เสนอแนะ และกำหนดความชัดเจนต่าง ๆ ดังกล่าวข้างต้น ของปฏิบัติการสงครามไซเบอร์ให้สามารถนำไปใช้ประโยชน์ได้กับกองบัญชาการกองทัพไทย

นาวาเอกหญิง

(จินดา สระสมบูรณ์)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๕๗
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเป็นที่ยอมรับว่าเทคโนโลยีสารสนเทศ มีบทบาทสำคัญอย่างยิ่งในกิจกรรมงานต่าง ๆ ไม่เว้นแต่กิจกรรมทางทหาร ดังนั้นการเตรียมความพร้อมเพื่อปฏิบัติการสงครามไซเบอร์ ซึ่งนับว่าเป็นพื้นที่การรบที่ ๕ เพื่อคุ้มครองปกป้องข้อมูลข่าวสาร บุคคล องค์กร และอธิปไตยของชาติ จึงนับว่ามีความสำคัญ และมีความจำเป็นที่ต้องดำเนินการอย่างเร่งด่วนโดยกำหนดหลักนโยบายและแนวปฏิบัติทั้งทางยุทธศาสตร์และยุทธวิธีหรือเทคนิควิธี ที่เป็นปัจจัยสำคัญในการพัฒนาความมั่นคงปลอดภัยด้านไซเบอร์ ให้กับกองบัญชาการกองทัพไทย และประเทศชาติ

การดำเนินการด้านการปฏิบัติการสงครามไซเบอร์ เป็นยุทธวิธีรูปแบบใหม่ที่มีการนำมาใช้ในการพัฒนากิจการงานด้านการทหารมีหลายประเทศชั้นนำอย่างสหรัฐ รัสเซีย และจีน ต่างใช้เป็นเครื่องมือในการกระทำกับฝ่ายตรงข้ามเพื่อทำลายระบบต่าง ๆ ไม่ว่าจะเป็นระบบการควบคุมการบังคับบัญชา โครงสร้างพื้นฐานสำคัญของประเทศ (Infrastructure) รวมถึงการได้มาซึ่งข้อมูลข่าวสารสำคัญ (Information Critical) หรือการฝังตัวการโจมตีในรูปแบบใหม่ (Root kit) ที่ใช้หลักการเขียนตรรกะทางโปรแกรม (Logical Programming) แทนกำลังพลและยุทโธปกรณ์ทางทหาร (Armament) เกิดสนามรบรูปแบบใหม่อย่างที่ไม่คาดคิดมาก่อนว่าจะมีเกิดขึ้นเป็นการรบในพื้นที่ การรบที่ ๕ (Fifth Domain) คือพื้นที่ในระบบเครือข่ายทางการสื่อสารที่เชื่อมโยงกันอย่างไร้ขอบเขตหรือพื้นที่ไซเบอร์ (Cyber Domain) ทดแทน สนับสนุน และเสริมการรบพื้นที่ทางบก (Army Domain) ทางน้ำหรือทางทะเล (Navy Domain) ทางอากาศ (Air Domain) และทางอวกาศ (Space Domain)

ปัจจุบันปฏิบัติการสงครามไซเบอร์ (Cyber Warfare Operation) จึงกลายเป็นอาวุธหรือเครื่องมือในการปฏิบัติการสงครามในทุกระดับ ตั้งแต่การดำเนินการด้านความขัดแย้งพื้นฐาน สู่การต่อสู้ตั้งแต่ระดับยุทธบริเวณไปจนถึงระหว่างประเทศหรือภูมิภาค มีการกระทำทั้งในทางลับและ

เปิดเผย 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) แต่นับว่า ยังมีข้อจำกัดกับการบูรณาการเข้ากับกิจการด้านการทหารในรูปแบบเดิม ที่กำหนดให้ต้องมีการจัดโครงสร้างหน่วย สายการบังคับบัญชา และภารกิจความรับผิดชอบอย่างชัดเจน เพื่อป้องกันความสับสนในการปฏิบัติ การกำหนดนโยบาย สั่งการ การเตรียมความพร้อม การฝึก และการปฏิบัติการในภาวะสงคราม ทำให้ปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย หรือกองทัพอื่น ยังไม่มีการกำหนดความชัดเจนตั้งแต่ระดับนโยบาย สั่งการ และหลักการปฏิบัติ การวิจัยครั้งนี้ ก็เพื่อศึกษา เสนอแนะ และกำหนดความชัดเจนต่าง ๆ ดังกล่าวข้างต้น ของปฏิบัติการสงครามไซเบอร์ให้สามารถนำไปใช้ประโยชน์ได้กับกองบัญชาการกองทัพไทย

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

วัตถุประสงค์ของการวิจัย

๑. ศึกษาและวิเคราะห์หลักปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งการปฏิบัติเชิงรุกและเชิงรับ สำหรับเตรียมการหรือรองรับภัยคุกคามรูปแบบใหม่ที่อาศัยเครือข่ายในการปฏิบัติ

๒. เสนอแนะแนวทางปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย

ขอบเขตของการวิจัย

๑. เน้นการวิจัยด้านการกำหนดรูปแบบและแนวคิดการปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย

๒. การกำหนดบทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบ ความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ รวมถึงปฏิบัติการสงครามไซเบอร์ เฉพาะของกองบัญชาการกองทัพไทย

วิธีดำเนินการวิจัย

การวิจัยนี้ เป็นการวิจัยเชิงคุณภาพ ดำเนินการวิจัยโดยการศึกษา รวบรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ ในรูปแบบของคำอธิบายและแผนภาพ ทั้งจากเอกสาร รายงาน ผลการวิจัยที่เกี่ยวข้อง เพื่อให้ได้แนวทางในการพัฒนารูปแบบปฏิบัติการสงครามไซเบอร์ บทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบ ความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ รวมถึงการปฏิบัติการสงครามไซเบอร์ ที่เหมาะสมกับกองบัญชาการกองทัพไทย

ประโยชน์ที่ได้รับจากการวิจัย

๑. เกิดความเข้าใจในการปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งหลักการปฏิบัติเชิงรุกและเชิงรับ เพื่อใช้เป็นหลักปฏิบัติในการเตรียมความพร้อมทั้งในยามปกติและยามสงครามที่อุบัติขึ้นในยุคเทคโนโลยีสารสนเทศ ขยายตัวครอบคลุมไปทั่วโลก และเชื่อมโยงข้อมูลข่าวสาร บุคคล และองค์กร ด้วยเครือข่ายสังคมออนไลน์

๒. สามารถนำความรู้ที่ได้มาปรับใช้กับปฏิบัติการสงครามไซเบอร์ ของกองบัญชาการกองทัพไทย ทั้งด้านการกำหนดรูปแบบการปฏิบัติการกำหนดโครงสร้างหน่วยงานและความรับผิดชอบต่อการปฏิบัติและการจัดเตรียมกำลังพลรวมถึงยุทโธปกรณ์ที่สำคัญสนับสนุนการปฏิบัติ

บทที่ ๒
การทบทวนวรรณกรรมที่เกี่ยวข้อง

สงครามไซเบอร์ (Cyber Warfare, CW) เป็นสงครามที่ไม่จำกัดพื้นที่ยุทธบริเวณ การทำสงครามเกิดขึ้นไปทั่วระบบเครือข่ายคอมพิวเตอร์ (Computer Network) เป็นสมรภูมิรบ โดยอาศัยเครือข่ายอินเทอร์เน็ต (Internet) ที่เชื่อมโยงไปทั่วโลก (The Internet of Thing) เป็นสนามการทำสงครามไซเบอร์ มีการปล่อยอาวุธที่สำคัญ คือ คำสั่งโปรแกรมที่ประสงค์ร้าย (Malicious Software, Malware) ไปยังเป้าหมาย (Target) ซึ่งมีทั้งแบบมีเป้าหมายชัดเจนและไม่มีเป้าหมายชัดเจน การกระทำ อาจใช้กำลังทางทหาร (Military Force) กำลังพลเรือน (Civil Force) และกำลังประชาชน (People Force) รวมไปถึงกลุ่มคนหรือเครื่องคอมพิวเตอร์ที่เป็นเหยื่อของการควบคุมด้วยโปรแกรมประสงค์ร้าย (BotNet, Robot Network) อาจปฏิบัติได้ทั้งแบบรวมการและแยกการปฏิบัติ เป็นสงครามที่อาจมีคู่กรณีทำสงครามระหว่างกันชัดเจน และไม่ชัดเจน หรืออาศัยการหลอกลวงการโจมตีจากประเทศอื่นที่ไม่ได้เป็นคู่กรณี เป็นฐานการโจมตีฝ่ายตรงข้าม เพื่อปิดบังการการกระทำการ ใด ๆ ของฝ่ายตน หรืออาจกล่าวได้ว่าเป็นสงครามระหว่างแฮกเกอร์ (Hacker Warfare) หรือนักรบไซเบอร์ (Cyber Warrior) ทั้งนี้ผู้วิจัยได้ศึกษาทบทวนวรรณกรรมที่เกี่ยวข้อง โดยกำหนดหัวข้อไว้ ดังนี้

๑. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. สงครามสารสนเทศ

๓. สงครามไซเบอร์

๔. ทฤษฎีและแนวคิดปฏิบัติการสงครามไซเบอร์

๕. ปฏิบัติการสงครามไซเบอร์ในต่างปะเทศ

๖. รายงานการศึกษาวิจัยที่เกี่ยวข้อง

๗. บทสรุป

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

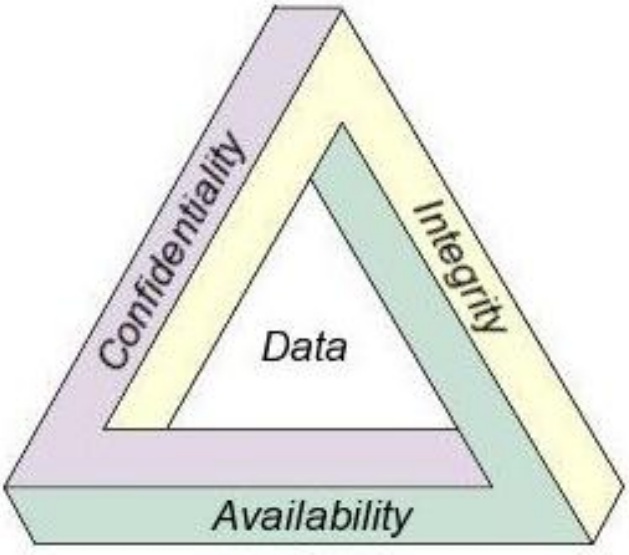
ปัจจุบันเทคโนโลยีสารสนเทศมีการพัฒนาและมีความก้าวหน้าอย่างรวดเร็ว เทคโนโลยีการติดต่อสื่อสารที่สามารถเชื่อมต่อได้อย่างรวดเร็วด้วยระบบเครือข่ายอินเตอร์เน็ต และสามารถส่งข้อมูลได้ในทุกรูปแบบไม่มีข้อจำกัด มีเครือข่ายสังคมออนไลน์ (Social Network) เพื่อให้สามารถเชื่อมต่อถึงกันได้ด้วยความสะดวก แต่ปัญหาในเรื่องของการรักษาความลับ (Confidentiality) เราไม่สามารถล่วงรู้ได้เลยว่ามีบุคคลอื่น ล่วงรู้ข้อมูลเหล่านั้นด้วย หรือมีการแก้ไขความถูกต้องของข้อมูล (Integrity) หรือไม่ และในอนาคตระบบจะมีความพร้อมในการใช้งาน (Availability) มากน้อยเพียงใด หรือที่เรียกว่า CIA Security อธิบายรายละเอียดได้ ดังนี้

๑.๑ ความลับของข้อมูล (Confidentiality, C) คือการรักษาหรือปกปิดเพื่อปกป้องข้อมูลให้เป็นความลับ โดยสามารถเข้าใช้งานได้ เฉพาะผู้ที่ได้รับอนุญาตหรือได้รับสิทธิ์การเข้าถึงเท่านั้น

๑.๒ ความคงสภาพ หรือความสมบูรณ์ของข้อมูล (Integrity, I) เป็นการปกป้องรักษาข้อมูลไว้ ไม่ให้ถูกแก้ไขเปลี่ยนแปลง หรือถูกทำลาย และเป็นการทำให้ข้อมูลมีความน่าเชื่อถือว่าข้อมูลมาจากแหล่งต้นฉบับจริง ไม่ได้ถูกนำไปเปลี่ยนแปลงแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต

๑.๓ ความพร้อมใช้งานของข้อมูล (Availability, A) คือการดูแล รักษาสภาพของข้อมูลให้สามารถเข้าถึงและเรียกใช้งานได้ตลอดเวลา เมื่อต้องการโดยผู้ที่ได้รับอนุญาตเท่านั้น

แผนภาพที่ ๒-๑ CIA Security



การบริหารงานขององค์กรทุกประเภท ทั้งภาครัฐและภาคเอกชน ต่างมีวัตถุประสงค์ของตนเองและมุ่งหวังที่จะทำงานไปให้ถึงเป้าหมายที่วางไว้อย่างดีที่สุด สูญเสียทรัพยากรให้น้อย

ที่สุด แต่การดำเนินการใด ๆ เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้มักจะต้องประสบกับความเสี่ยงที่จะเกิดความผิดพลาด ความเสียหาย ความสูญเปล่าหรือเหตุการณ์ที่ไม่พึงประสงค์ซึ่งอาจเกิดขึ้น มีผลกระทบทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์เป้าประสงค์และเป้าหมายขององค์กร และด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้องค์กรภาครัฐและภาคเอกชน ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดัน ให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสาร มาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย

๒. มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานหลักของประเทศไทย ที่มีหน้าที่ดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ได้จัดทำแผนแม่บทการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งได้กำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของประเทศให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานการบริหารจัดการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศสากล ISO/IEC ๒๗๐๐๑ โดยแบ่งเนื้อหาออกเป็น ดังนี้

๒.๑ นโยบายความมั่นคงขององค์กร

หน่วยงานต้องต้องจัดให้มีนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Security Policy) ของหน่วยงาน เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของหน่วยงาน

๒.๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

เพื่อการบริหารจัดการควบคุมและกำหนดรูปแบบการติดตั้งและใช้งานระบบการรักษาความปลอดภัยสารสนเทศให้ครอบคลุมและมีประสิทธิภาพ

๒.๓ การบริหารจัดการทรัพย์สินขององค์กร

เพื่อให้มีการจัดหมวดหมู่ของสารสนเทศและทรัพย์สินสารสนเทศ ให้มีการรักษาความปลอดภัยที่เหมาะสม รวมถึงจัดทำบัญชีควบคุมให้สามารถตรวจสอบได้ เพื่อป้องกันทรัพย์สินจากความเสียหายที่อาจเกิดขึ้นได้

๒.๔ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

เพื่อเตรียมการจัดหาบุคลากรให้เหมาะสมกับงานด้านความมั่นคงปลอดภัยระบบสารสนเทศ โดยเริ่มจากการกำหนดคุณสมบัติ กำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่แต่ละตำแหน่ง จัดอบรมให้ความรู้ เพิ่มทักษะ และวิธีการแก้ไขปัญหา แก่ผู้ปฏิบัติงานและกำหนดบทลงโทษทางวินัยต่อผู้ฝ่าฝืน

๒.๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

เพื่อให้ผู้รับผิดชอบด้านสารสนเทศและสิ่งแวดล้อมต่าง ๆ เช่น อาคารสถานที่ หรือห้องศูนย์คอมพิวเตอร์ มีการปฏิบัติตามวิธีการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย การถูกขโมย และการก่อกวน หรือแทรกแซงต่อทรัพย์สินสารสนเทศ ของส่วนราชการ และทำให้กิจกรรมการดำเนินงานต่าง ๆ ของหน่วยงานเกิดการติดขัดหรือหยุดชะงัก

๒.๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศองค์กร

เพื่อให้ระบบเครือข่ายและการปฏิบัติงานสารสนเทศ มีการควบคุมจัดการที่เพียงพอ ให้เกิดความปลอดภัยจากการบุกทำลาย และให้ระบบสารสนเทศ มีคุณสมบัติตามที่หน่วยงานกำหนด เช่น มีความลับ ความถูกต้อง และมีความพร้อมในการใช้งาน

๒.๗ การควบคุมการเข้าถึง

เพื่อจัดทำบัญชีการกำหนดสิทธิในการเข้าถึงระบบเครือข่าย แก่บุคลากรที่ใช้งานในระบบเครือข่ายและระบบสารสนเทศให้สามารถเข้าถึงข้อมูลคอมพิวเตอร์ และระบบสารสนเทศได้ตามความจำเป็นในการใช้งาน เพื่อรักษาความลับ ความถูกต้องของข้อมูลคอมพิวเตอร์และระบบสารสนเทศ

๒.๘ การจัดการ การหา และการบำรุงรักษาระบบสารสนเทศ

เพื่อให้เจ้าหน้าที่สารสนเทศ ผู้พัฒนาระบบ ผู้จัดหาระบบสารสนเทศ และเจ้าของระบบสารสนเทศ ให้ความสำคัญในการจัดทำระบบความมั่นคงปลอดภัยระบบสารสนเทศทุกระบบที่ได้พัฒนาขึ้น เพื่อลดความเสี่ยงในการถูกโจมตีจากภัยคุกคาม

๒.๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

เพื่อให้เกิดความร่วมมือในการแก้ไขปัญหาจากเหตุการณ์ที่เป็นภัยคุกคามระบบสารสนเทศ และกำหนดแนวทางในการบริหารจัดการเหตุการณ์ที่อาจจะเกิดขึ้นได้

๒.๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกระบวนการดำเนินงาน ความล้มเหลวหรือหายนะที่อาจจะเกิดขึ้นซึ่งมีผลกระทบต่อระบบสารสนเทศ หากเกิดปัญหาต้องมีแนวทางและขั้นตอนการปฏิบัติที่ชัดเจน เพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสมและเกิดความต่อเนื่องในการปฏิบัติงาน

๒.๑๑ การปฏิบัติตามข้อกำหนด

เพื่อให้ผู้ปฏิบัติงานด้านสารสนเทศทุกระดับ คำนึงถึงการปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดในสัญญา ข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และระเบียบปฏิบัติ

แผนภาพที่ ๒-๒ ISO/IEC ๒๗๐๐๑

การรักษาความมั่นคงปลอดภัยสารสนเทศ ให้เป็นไปตามมาตรฐานสากลนั้น จะต้องมีการบริหารจัดการที่เกี่ยวกับการระบุข้อมูลการดำเนินการของทรัพย์สิน (Asset) ด้านความมั่นคงปลอดภัยและการพัฒนาระบบ การจัดทำเอกสาร (Document) นโยบาย (Policy) มาตรฐาน (Standard) ขั้นตอนการปฏิบัติและแนวปฏิบัติ (Process and Best Practices) โดยการดำเนินการประกอบไปด้วยการกำหนดชั้นความลับและความสำคัญของข้อมูล (Classified) การสร้างความ

ตระหนักรู้ (Awareness) และการฝึกอบรม (Training) ทั้งผู้ปฏิบัติและผู้มีส่วนได้ส่วนเสีย ซึ่งถือเป็นการบริหารจัดการด้านความมั่นคงปลอดภัยระบบสารสนเทศที่มีความสำคัญอย่างยิ่ง อีกองค์ประกอบหนึ่งที่มีความสำคัญในการสร้างความมั่นคงปลอดภัยด้านสารสนเทศ คือการกำหนดความเสี่ยง (Risk) ต้องมีการวิเคราะห์ความเสี่ยง (Risk Analysis) การบริหารจัดการความเสี่ยง (Risk Management) วัดผล ประเมิน และลดความเสี่ยงที่จะเกิดขึ้น โดยต้องมีการทบทวนอย่างต่อเนื่องเพื่อหาทางป้องกันและให้มีการดำเนินงานอย่างมีประสิทธิภาพ

สงครามสารสนเทศ

สงครามสารสนเทศ (Information Warfare, IW) เป็นพัฒนารูปแบบของสงคราม ตามยุค ตามสมัย ตามเทคโนโลยีที่เปลี่ยนแปลงไป โดยสงครามข่าวสารในอดีต จะเป็นการปฏิบัติการ ที่เกี่ยวกับข่าวสารทั้งปวง ในรูปแบบการโฆษณา ประชาสัมพันธ์ ชวนเชื่อ ปลุกปั่น ยุยง ปลุกระดม และการปลูกฝังแนวคิดในสื่อต่าง ๆ เช่น ภาพยนตร์ แผ่นป้ายโฆษณา แผ่นพับ หนังสือตำรา หนังสือพิมพ์ และรายการวิทยุ เป็นต้น เข้าสู่ยุคการปฏิบัติการที่เกี่ยวกับข่าวสารบนสื่ออิเล็กทรอนิกส์ ผ่านระบบเครือข่ายคอมพิวเตอร์ในระบบเครือข่ายอินเตอร์เน็ต ที่แพร่กระจายข่าวสารได้ครอบคลุม ทั้งแบบตัวต่อตัว และกลุ่มคนในสังคม รวมถึงให้สามารถกระจายไปทั่วโดยทั้งที่มีเป้าหมายชัดเจนและไม่ชัดเจน ซึ่งเป็นสงครามเงียบในยุคปัจจุบัน มีสายลับลักลอบการเข้าถึงสารสนเทศ เพื่อนำมาใช้ประโยชน์ที่จะกระทำกับฝ่ายตรงข้าม ตัวอย่าง นายเอ็ดเวิร์ด สโนว์เดน (Edward Snowden) ที่ออกมาแฉข้อมูลความพยายามของรัฐบาลสหรัฐอเมริกา ในการดักฟังผู้นำทั่วโลก จนทำให้เกิดความขัดแย้งกับรัฐบาลเยอรมนี ซึ่งรวมถึงความสัมพันธ์ที่ถดถอยของอินโดนีเซียกับออสเตรเลีย ที่มาจากสาเหตุการแอบดักฟังโทรศัพท์เหมือนกัน นอกจากนี้ ในเอกสารที่ นายเอ็ดเวิร์ด สโนว์เดน นำออกมาแฉนั้น ยังอธิบายถึงการที่องค์กรด้านความมั่นคงสหรัฐอเมริกาสนับสนุนเงินทุนจำนวนมาก ให้กับบริษัทชั้นนำต่าง ๆ ที่ให้บริการบนอินเทอร์เน็ต ไม่ว่าจะเป็น Facebook, Twitter, Yahoo, Microsoft และ Apple เพื่อเข้าถึงข้อมูลผู้ใช้บริการทั่วโลก ซึ่งถือเป็นภัยทางความมั่นคงของทุกประเทศทั่วโลก

สงครามสารสนเทศ จึงต้องอาศัยการปฏิบัติการข่าวสารเป็นเครื่องมือที่จำเป็นสำคัญยิ่ง และเป็นส่วนหนึ่งของสงครามจิตวิทยา โดยเฉพาะในยุคเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งสามารถกระทำทั้งในยามปกติและยามสงคราม ทั้งฝ่ายข้าศึกและฝ่ายเดียวกัน รวมถึงฝ่ายเป็นกลางอีกด้วย ทั้งในด้านการเมือง เศรษฐกิจ สังคมจิตวิทยา และการทหาร ในระดับยุทธศาสตร์ ยุทธการ และระดับยุทธวิธี เพราะเป็นเครื่องมือที่มีประสิทธิภาพมากที่สุดที่ส่งผลกระทบในด้านจิตใจ ความรู้สึกนึกคิด ความเชื่อมั่นศรัทธา ทัศนคติทั้งทางบวกและทางลบ ตามวัตถุประสงค์ช่วงระยะเวลาที่รวดเร็ว และแพร่กระจายอย่างไร้ขอบเขต

สงครามไซเบอร์

สงครามไซเบอร์ (Cyber Warfare, CW) เป็นคำที่นิยามขึ้นมาโดย ผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลที่ชื่อ ริชาร์ด เอ. คลาร์ก ในหนังสือที่ชื่อ Cyber War (พฤษภาคม ๒๐๑๐) โดยนิยามว่า "เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก"

Economist อธิบายไว้ว่า "สงครามไซเบอร์ เป็นการกำเนิดสงครามอย่างที่ ๕"

วิลเลียม เจ. ลิน รองรัฐมนตรีว่าการกระทรวงกลาโหม สหรัฐอเมริกา กล่าวว่า “โดยหลักการแล้ว เพนตากอน ได้ยอมรับอย่างเป็นทางการแล้วว่า เป็นเหตุให้เกิดสงคราม ที่กลายเป็นเรื่องอันตรายต่อการปฏิบัติการทหาร ทั้งภาคพื้นดิน อากาศ ทะเล และทางอากาศ”

สงครามไซเบอร์เป็นการปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้าม และต้องทำให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา ซึ่งในช่วงสงครามอ่าวที่สหรัฐโจมตีอิรัก และสงครามอิรักครั้งที่สอง สิ่งที่สหรัฐต้องทำก่อนอื่นคือ ทำลายเครือข่ายคอมพิวเตอร์และอิเล็คทรอนิกส์ของอิรักที่ใช้ควบคุมระบบการยิงของอาวุธ ไม่เพียงแต่กรณีสงครามอิรักเท่านั้น ในการสู้ระบบปัจจุบัน แต่ละฝ่ายต้องหาทางทำลายระบบคอมพิวเตอร์และอิเล็คทรอนิกส์ที่ควบคุมการยิงของอาวุธก่อน

สงครามไซเบอร์ คือการใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำสงคราม สงครามไซเบอร์มีการโจมตีกันหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด เช่น

๑. การโจมตีเว็ป หรือบล็อคเว็ป

๒. การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ต

๓. การเจาะข้อมูลลับ โดยแฮกเกอร์ที่นอกจากได้ข้อมูลลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้

๔. การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้ หรือทำงานไม่แม่นยำ

๕. การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟา ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก

แผนภาพที่ ๒-๓ การปฏิบัติการสงครามไซเบอร์

ที่มา : http://www.clipmass.com/story/๖๑๗๙๒

การใช้คอมพิวเตอร์และอินเตอร์เน็ต เพื่อการทำสงคราม ปัจจุบันมีอยู่ ๘ รูปแบบ คือ

๑. การโจรกรรมทางไซเบอร์

๒. การทำลายเว็ปไซต์

๓. การโฆษณาชวนเชื่อทางอินเตอร์เน็ต (เว็ปไซต์)

๔. การรวบรวมและการล้วงความลับข้อมูล

๕. การกระจายเพื่อให้ปฏิเสธบริการ

๖. การรบกวนเครื่องมือและอุปกรณ์

๗. การโจมตีโครงสร้างระบบสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) พื้นฐานที่สำคัญ

๘. การใช้อุปกรณ์คอมพิวเตอร์หลอกแต่ซ่อนซอฟต์แวร์ไวรัสเอาไว้

กระทรวงกลาโหม สหรัฐ กำหนดให้การรักษาความมั่งคงไซเบอร์ (Cyber Security) คือกระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร ในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทาง

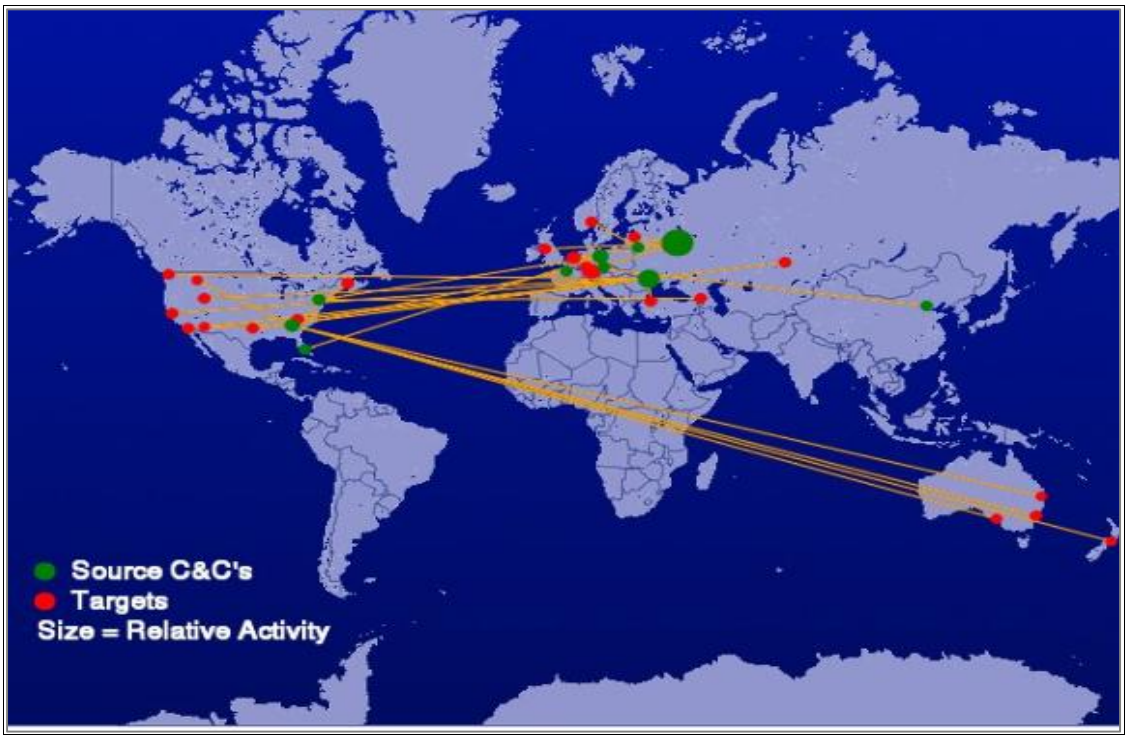
กายภาพ) ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ ส่วนความเสี่ยงของ Cyber Security อาจรวมถึง สิ่งต่างๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้ถือผลประโยชน์ร่วม (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิต และสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญ ของชาติ ต้องอาศัยมาตรการในการรักษาความมั่งคงปลอดภัยไซเบอร์ อย่างการรักษาความลับ (Confidentiality) เป็นมาตรการในการปกปิดข้อมูลข่าวสาร ให้รับทราบได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น การรักษาข้อมูล (Data Integrity) เป็นการเพิ่มความคงทนและความเที่ยงตรงของข้อมูล ที่ถูกจัดเก็บไว้ โดยตรวจสอบการเปลี่ยนแปลงของข้อมูลระหว่างการบันทึกข้อมูล และการสำรองข้อมูล (Back up Data) เป็นหนึ่งในการรักษาความปลอดภัยของข้อมูลข่าวสาร ทำโดยการสำเนา ของไฟล์คอมพิวเตอร์ที่สำคัญ และเก็บรักษาไว้ในที่ตั้งที่อยู่ห่างจากระบบหลักที่ปฏิบัติอยู่ในสภาวะปกติ รวมทั้งที่ตั้งใหม่นั้น ต้องสามารถป้องกันภัยคุกคามในด้านอุบัติภัย และภัยธรรมชาติขนาดใหญ่ นอกจากนี้การให้ความตระหนักด้านการรักษาความปลอดภัยแก่พนักงานในองค์กรให้ทราบถึงผลกระทบที่ตามมาหากองค์กรถูกคุกคามด้านการรักษาความปลอดภัยของไซเบอร์ นั้นยิ่งเป็น สิ่งจำเป็น

สงครามไซเบอร์ คือการขัดกันของกำลังที่ใช้กรอบของไซเบอร์เป็นเครื่องมือ เพื่อให้ได้มาซึ่งการครองความได้เปรียบในห้วงไซเบอร์ (Cyberspace Superiority) บนพื้นที่ปฏิบัติการที่เกี่ยวข้อง ได้แก่ ภาคพื้นดิน ภาคทะเล ภาคอากาศ ภาคอวกาศ และภาคไซเบอร์ ปราศจากการขัดขวางของ ฝ่ายศัตรู การปฏิบัติการทางทหารที่ดำเนินการเพื่อขัดขวางการปฏิบัติงานระบบไซเบอร์และอาวุธ ของฝ่ายตรงข้าม รวมทั้งเพื่อดำรงการปฏิบัติงานระบบไซเบอร์และอาวุธอย่างมีประสิทธิภาพของ ฝ่ายเรา การปฏิบัติการดังกล่าวรวมถึง การโจมตีทางไซเบอร์ (Cyber Attack) การ

ป้องกันทางไซเบอร์ (Cyber Defense) และการแสวงหาประโยชน์จากการสภาพแวดล้อมทางไซเบอร์ (Cyber Operational Preparation of Environment หรือ Cyber Enabling Actions) ดังนี้

๑. การโจมตีทางไซเบอร์ (Cyber Attack) คือ การกระทำใด ๆ ที่ใช้คอมพิวเตอร์ เครือข่าย หรือระบบ รวมทั้งอุปกรณ์ที่เกี่ยวข้อง ซึ่งตั้งใจเป็นภัยคุกคาม ขัดขวาง หรือทำลายระบบทรัพยากร และการทำงานของไซเบอร์ที่สำคัญของศัตรู ผลกระทบที่ต้องการของการโจมตีทางไซเบอร์ไม่จำเป็นต้องจำกัดเพียงระบบคอมพิวเตอร์ และข้อมูลที่เป็นเป้าหมาย ตัวอย่างเช่น การโจมตีต่อระบบคอมพิวเตอร์ ที่ต้องการลิดรอน หรือทำลายโครงสร้างพื้นฐานสาธารณูปโภค หรือขีดความสามารถของระบบบัญชาการและควบคุม (C๒) การโจมตีทางไซเบอร์อาจจะต้องใช้พาหะตัวกลางในการดำเนินการ รวมทั้งอุปกรณ์ต่อเชื่อมต่าง ๆ (Peripheral Devices) เครื่องส่งสัญญาณอิเล็กทรอนิกส์ (Electronic Transmitters) การเข้ารหัส (Embedded Code) หรือเจ้าหน้าที่ปฏิบัติงาน (Operators) กิจกรรมหรือผลกระทบของการโจมตีอาจจะเกิดขึ้นอย่างกระจัดกระจาย เป็นวงกว้าง หรือเป็นเฉพาะพื้นที่ที่เป็นเป้าหมาย ซึ่งถูกใช้แทนที่คำว่า การโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack, CNA) เนื่องจาก การโจมตีทางไซเบอร์นั้นเชื่อมโยงกับกระบวนทัศน์หรือหลักนิยมของการปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations, CNO)

แผนภาพที่ ๒-๔ การโจมตีทางไซเบอร์



ที่มา : http://hackmageddon.com/๒๐๑๓/๐๑/๒๖/a-graphical-world-of-botnets-and-cyber-attacks/

๒. การป้องกันทางไซเบอร์ (Cyber Defense) เป็นการประยุกต์รวมขีดความสามารถและกระบวนการในห้วงไซเบอร์ของหน่วยงานที่เกี่ยวข้อง ในการดำรงขีดความสามารถด้านการตรวจจับ วิเคราะห์และลดภัยคุกคาม/จุดเสี่ยงต่าง ๆ และดำเนินกลยุทธ์ในการเอาชนะศัตรู เพื่อป้องกันเครือข่ายที่กำหนด ปกป้องภารกิจที่สำคัญ และทำให้เกิดอิสระในการปฏิบัติของฝ่ายเรา การป้องกันทางไซเบอร์ รวมถึง การปฏิบัติการเครือข่ายเชิงรุก (Proactive Network Operations) การปฏิบัติการเครือข่าย (Network Operations) ถูกกำหนดโดยกระทรวงกลาโหม สหรัฐ ในการปฏิบัติการ การจัดโครงสร้าง และขีดความสามารถทางเทคนิคสำหรับการปฏิบัติการ และการป้องกันโครงข่ายข้อมูลข่าวสารโลก (Global Information Grid, GIG) การปฏิบัติการเครือข่าย รวมถึงการบริหารจัดการองค์กร (Enterprise Management) การรับรองการทำงานหรือการป้องกันของเครือข่าย (Network Assurance หรือ Network Defense) และการบริหารข่าวสาร (Content Management) การปฏิบัติการเครือข่ายสามารถสนองตอบความต้องการของผู้บังคับบัญชาในการหยั่งรู้สถานการณ์ของข้อมูลข่าวสารโลก เพื่อนำไปสู่การตัดสินตกลงใจในรูปแบบของการ

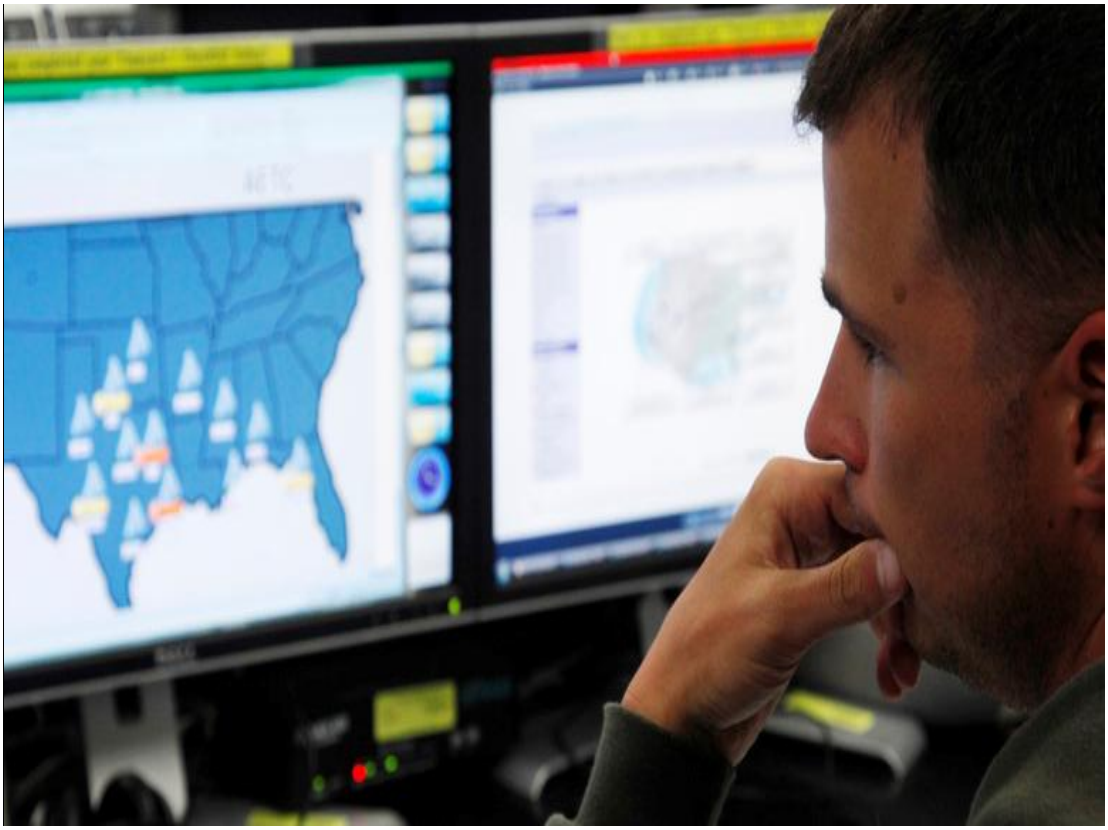
บัญชาการและควบคุม ทั้งนี้การหยั่งรู้สถานการณ์ของข้อมูลข่าวสารโลก ทำได้โดยการบูรณาการทั้งทางเทคนิคและการปฏิบัติการของการบริหารจัดการองค์กร และการป้องกันและกิจกรรมตลอดทุกระดับ การบังคับบัญชา ทั้งระดับยุทธศาสตร์ ระดับยุทธการ และระดับยุทธวิธี เช่น การควบคุมการกำหนดค่า (Configuration Control) มาตรการรับประกันข้อมูลข่าวสาร (Information Assurance Measures) การออกแบบสถาปัตยกรรมความปลอดภัย และการรักษาความปลอดภัยทางกายภาพ (Physical Security and Secure Architecture Design) การตรวจจับการบุกรุก (Intrusion Detection) และการเข้ารหัสข้อมูล (Encryption of Data) ทั้งนี้ เพื่อป้องกันเครือข่ายของ ฝ่ายเดียวกันในด้านการคงสภาพ (Integrity) การพร้อมใช้งาน (Availability) และการรักษาความปลอดภัย (Security) รวมทั้งการป้องกันขีดความสามารถของเครือข่ายของไซเบอร์ฝ่ายเดียวกัน จากการโจมตี การบุกรุก หรือกิจกรรมที่ประสงค์ร้ายต่าง ๆ โดยการดำเนินการเชิงรุกในการค้นหา การสกัดกั้น และการกีดกันการปฏิบัติทางไซเบอร์ของศัตรูต่อภัยคุกคามต่าง ๆ

แผนภาพที่ ๒-๕ การป้องกันทางไซเบอร์

ที่มา : https://cyberarms.wordpress.com/๒๐๑๒/๐๒/๒๐/cyber-cold-war-and-the-need-for-an-offensive-cyber-special-forces-group/

๓. การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ (Cyber Operational Preparation of Environment, C-OPE) เป็นการทำงานภายในห้วงไซเบอร์ในการวางแผน และเตรียมการให้กับการปฏิบัติการทางทหารที่ตามมา โดยอาจรวมถึงการกำหนดระบุข้อมูล การกำหนดตั้งค่าระบบ/เครือข่าย หรือโครงสร้างการเชื่อมต่อทางกายภาพกับระบบหรือเครือข่าย ที่เกี่ยวข้อง เพื่อตรวจสอบช่องโหว่/จุดอ่อนของระบบ รวมถึงการกระทำเพื่อเพิ่มความมั่นใจการเข้าถึง และ/หรือการควบคุมระบบ เครือข่าย หรือข้อมูลในระหว่างการต่อสู้กับภัยคุกคามต่าง ๆ ทั้งนี้ การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ ครอบคลุมการเปิดเผยเครือข่ายคอมพิวเตอร์ (Computer Network Exploitation, CNE) ซึ่ง กระทรวงกลาโหม สหรัฐ หมายถึง การปฏิบัติการ และขีดความสามารถด้านการรวบรวมข่าวกรอง ที่กระทำโดยการใช้เครือข่ายคอมพิวเตอร์ ในการรวบรวมข้อมูลเกี่ยวกับเป้าหมาย หรือระบบ/เครือข่ายข้อมูลข่าวสารอัตโนมัติของศัตรู

แผนภาพที่ ๒-๖ การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์



ที่มาภาพ : http://www.nato.int/cps/en/natolive/news_๗๗๕๑๕.htm

ทฤษฎีและแนวคิดปฏิบัติการสงครามไซเบอร์

๑. การปฏิบัติการสงครามไซเบอร์

การปฏิบัติการสงครามไซเบอร์ ๒ ระดับ คือ การปฏิบัติการสงครามไซเบอร์ระดับยุทธศาสตร์ และการปฏิบัติการสงครามไซเบอร์ระดับปฏิบัติการ ดังนี้

๑.๑ การปฏิบัติการสงครามไซเบอร์ระดับยุทธศาสตร์ คือ การวางแผน อำนวยการควบคุม และสั่งการในระดับนโยบายการจัดทำยุทธศาสตร์การปฏิบัติการสงครามไซเบอร์ รวมถึง

แผนแม่บทความมั่นคงไซเบอร์ และการมีส่วนร่วมในการจัดทำหลักนิยมด้านความมั่นคงไซเบอร์และสงครามไซเบอร์ รวมทั้งการจัดตั้งศูนย์บัญชาการไซเบอร์

๑.๒ การปฏิบัติการสงครามไซเบอร์ระดับปฏิบัติการ คือ เน้นเน้นการรักษาความมั่นคงปลอดภัยสารสนเทศเชิงป้องกัน (Cyber Security) และเตรียมความพร้อมการปฏิบัติการเชิงรุก มีหน้าที่ดำเนินการป้องกัน เฝ้าระวัง วิเคราะห์ ทดสอบ ประเมินผล และแจ้งเตือนภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ เครื่องคอมพิวเตอร์และผู้ใช้งาน ตอบสนองต่อเหตุการณ์ภัยคุกคาม การบุกรุกระบบและการละเมิดการรักษาความมั่นคงปลอดภัยสารสนเทศ กำหนดนโยบาย ระเบียบ แนวปฏิบัติและมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งดำเนินการสร้างความตระหนักรู้ พัฒนาและบริหารจัดการระบบรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานไปจนถึงระดับชาติ ให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพและต่อเนื่อง

๒. แนวความคิดในการปฏิบัติด้านสงครามไซเบอร์

แนวความคิดในการปฏิบัติด้านสงครามไซเบอร์ (ทอ.สหรัฐ) มี ๕ ประการ ได้แก่

๒.๑ การครองไซเบอร์สเปซ (Cyberspace Superiority) คือ การที่ต้องมีความสามารถในการปฏิบัติการบนไซเบอร์สเปซ เหนือกว่าฝ่ายตรงข้ามและต้องป้องกันไม่ให้ฝ่ายตรงข้ามสามารถปฏิบัติการต่าง ๆ บนไซเบอร์สเปซได้เช่นกัน

๒.๒ การโต้ตอบทางไซเบอร์ (Counter-Cyber) เป็นการตอบโต้ฝ่ายตรงข้ามโดยใช้วิธีการปฏิบัติทางไซเบอร์ ๒ รูปแบบ คือ

๒.๒.๑ การโต้ตอบทางไซเบอร์เชิงรุก (Offensive Counter-Cyber, OCC) การปฏิบัติการตอบโต้ทางไซเบอร์เชิงรุก โดยวิธีการทำให้ระบบของฝ่ายตรงข้ามปฏิเสธการให้บริการ (Denial Of Service) การทำลายหรือหลอกลวงความสามารถของศัตรูในการที่จะปฏิบัติการบนไซเบอร์สเปซ ตัวอย่างเช่น สงครามอ่าวเปอร์เซีย ก่อนที่สหรัฐจะใช้กำลังทางทหาร ได้มีการปฏิบัติการทางไซเบอร์ เพื่อโจมตีเครือข่ายเป็นศูนย์กลางการสื่อสารโทรคมนาคมของอิรัก ทำให้ไม่สามารถใช้การสื่อสารโทรคมนาคมได้

๒.๒.๒ การโต้ตอบทางไซเบอร์เชิงรับ (Defensive Counter-Cyber, DCC) การป้องกันการตอบโต้ทางไซเบอร์จากฝ่ายตรงข้าม โดยใช้วิธีการตรวจสอบและสกัดกั้นทำลายหรือลบล้าง กองกำลังทางไซเบอร์ของฝ่ายตรงข้ามที่พยายามจะเจาะหรือโจมตีผ่านไซเบอร์สเปซ เช่น การมีระบบตรวจจับและป้องกันการบุกรุกเครือข่าย (Intrusion Detection/Prevention System) หรือการใช้อุปกรณ์ควบคุมการเข้าถึงประเภทไฟล์วอลล์ (Firewall) โดยมีการตั้งกฎของไฟล์วอลล์ เพื่อควบคุมและป้องกันการถูกโจมตีจากฝ่ายตรงข้ามผ่านทางระบบเครือข่าย

๒.๓ การควบคุมทางไซเบอร์ (Cyberspace Control) คือ ความสามารถในการควบคุมการปฏิบัติต่าง ๆ ในไซเบอร์สเปซ เช่น

๒.๓.๑ การมีอำนาจในการอนุมัติการปฏิบัติการโต้ตอบทางไซเบอร์เชิงรุก

๒.๓.๒ การดำเนินการในการป้องกันทางไซเบอร์จากฝ่ายตรงข้าม

๒.๓.๓ การใช้ยุทธวิธี หรือกลยุทธ์ในการบูรณาการ การปฏิบัติการทางไซเบอร์ร่วมกันกับชาติต่าง ๆ เพื่อเป็นการลดความขัดแย้งที่อาจก่อให้เกิดสงครามไซเบอร์

๒.๔ การปฏิบัติการข้ามพื้นที่ปฏิบัติการ (Cross-Domain Operations) คือ การใช้ปฏิบัติการทางไซเบอร์ เพื่อให้บรรลุผลใน Domain อื่น ๆ เช่น การใช้ปฏิบัติการทางไซเบอร์ เพื่อทำให้เกิดการหยุดชะงักหรือทำลายการป้องกันทางกายภาพ เช่น

๒.๔.๑ การสั่งห้ามหรือการควบคุมระบบ Command control (C๒ link) ของฝ่าย ตรงข้าม

๒.๔.๒ การใช้ปฏิบัติการทางไซเบอร์ ที่ทำให้เกิดการหยุดชะงักการให้บริการหรือการควบคุมระบบสาธารณูปโภค เช่น ไฟฟ้า ประปา นิวเคลียร์

๒.๔.๓ การทำให้เกิดการหยุดชะงักระบบตลาดการเงินหรือระบบเศรษฐกิจ

๒.๕ การพิจารณาการปฏิบัติทางไซเบอร์ (Operational Considerations) สิ่งที่เป็นข้อพิจารณาในการใช้การปฏิบัติการทางไซเบอร์ เช่น

๒.๕.๑ การตรวจสอบให้แน่ใจถึงการกระทำต่าง ๆ ในโลกไซเบอร์ ซึ่งทุกคนมีสิทธิเสรีภาพในการทำกิจกรรมต่าง ๆ แต่ต้องไม่เป็นการสร้างภัยคุกคามให้เกิดขึ้น

๒.๕.๒ ความสามารถครองหรือควบคุมไซเบอร์สเปซได้ ฝ่ายตรงข้ามก็จะปฏิบัติการใด ๆ บนไซเบอร์สเปซได้ลำบาก

๒.๕.๓ การตอบโต้การใช้งานที่เป็นลักษณะประสงค์ร้าย ๆ ของฝ่ายตรงข้ามที่ใช้ ไซเบอร์สเปซ

๒.๕.๔ การแทรกซึมหรือแฝงตัวเข้าถึงระบบต่าง ๆ ของฝ่ายตรงข้าม เช่น การฝัง botnet, Root kit หรือ Trojan horse ที่ช่วยให้สามารถใช้ในการปฏิบัติการไซเบอร์สเปซได้

๓. ยุทธศาสตร์สงครามไซเบอร์แห่งชาติ (National Cyber Warfare Strategy)

ในช่วงเวลาเร่งด่วน สำคัญอันดับแรกการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันเหตุการณ์ความเสียหาย หรือลดผลกระทบจากสงครามไซเบอร์ สำหรับหน่วยงานด้านความมั่นคง และภาคบริการประชาชน เช่น กองทัพ สานักงานตำรวจแห่งชาติ ศาล กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน สานักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด หน่วยงานให้บริการด้านสาธารณสุข หน่วยงานราชการ และหน่วยงานของรัฐ อื่น ๆ ทั้งนี้ต้องร่วมมือกันกำหนดหน้าที่ความรับผิดชอบ การกำกับดูแล และการควบคุมการปฏิบัติ เมื่อประเทศเข้าสู่สงครามไซเบอร์ทั้งที่แบบเป็นทาง (Formal) หรือแบบไม่เป็นทางการ (Informal)

ระยะต่อมาในการกำหนดยุทธศาสตร์สงครามไซเบอร์แห่งชาติ คือ พัฒนาสำหรับหน่วยงานด้านการเงิน การธนาคาร และพาณิชย์อิเล็กทรอนิกส์ เช่น ธนาคาร บริษัทหลักทรัพย์ ประกันภัย ตลาดหลักทรัพย์ ผู้ให้บริการด้านบัตรเครดิต และหน่วยงานภาครัฐที่เกี่ยวข้องกับการตรวจสอบสถาบันการเงิน คู่ขนานกับหน่วยงานด้านสาธารณูปโภคพื้นฐาน เช่น โรงพยาบาลและการสาธารณสุข การผลิตและให้บริการไฟฟ้า การประปา หน่วยงานด้านพลังงาน หน่วยงานด้านการคมนาคมขนส่ง ธุรกิจด้านสายการบิน รวมถึงสำหรับหน่วยงานด้านการสื่อสารและโทรคมนาคม

ระยะปลาย คือ พัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือสร้างความมั่นคงให้กับข้อมูลข่าวสารส่วนบุคคลในเครือข่ายสังคมออนไลน์ และการป้องกันอาชญากรรมไซเบอร์ที่ส่งผลกระทบต่อบุคคล สังคม เศรษฐกิจ อุตสาหกรรม เพราะเหล่านี้คือเหตุ ถ้าเกิดผลกระทบก็นำชาติเข้าสู่สงครามไซเบอร์นั่นเอง

ปฏิบัติการสงครามไซเบอร์ในต่างประเทศ

ปัจจุบันแนวโน้มของภัยคุกคามด้านไซเบอร์ นับวันจะทวีความรุนแรงและเข้มข้นมากขึ้นตามลำดับ ส่งผลกระทบไปในวงกว้างทั้งทางด้านเศรษฐกิจ สังคมจิตวิทยา และความมั่นคงของประเทศ หลายประเทศต่างให้ความสำคัญกับภัยคุกคามด้านไซเบอร์มากขึ้นตามลำดับ โดยเฉพาะประเทศมหาอำนาจ อาทิเช่น สหรัฐอเมริกา ในปี ค.ศ. ๒๐๐๙ ประธานาธิบดี บารัก โอบามา ประกาศว่าระบบพื้นฐานดิจิตอลของสหรัฐอเมริกา “เป็นสินทรัพย์ยุทธศาสตร์ของชาติ” และในเดือนพฤษภาคม ค.ศ.๒๐๑๐ กระทรวงกลาโหม สหรัฐอเมริกา หรือ เพนตากอน (PENTAGON) ได้จัดตั้งกองบัญชาการไซเบอร์ (Cyber Command) นำโดยนายพล คีท บี. อเล็กซานเดอร์ ผู้บริหารของสภาความมั่งคงแห่งชาติสหรัฐอเมริกา เพื่อป้องกันเครือข่ายทหารอเมริกัน และจู่โจมระบบของประเทศอื่นที่เข้ามาโจมตี ภายใต้การควบคุมของผู้บริหารสภาความมั่นคงแห่งชาติสหรัฐ หรือตั้งขึ้นเพียงต้องการป้องการระบบทางทหาร เนื่องด้วยรัฐบาลและระบบพื้นฐานที่เกี่ยวข้อง เป็นความรับผิดชอบหลักตามลำดับของกระทรวงความมั่นคงภายในและบริษัทเอกชน

แผนภาพที่ ๒-๗ ศูนย์ปฏิบัติการไซเบอร์ที่ ๖๒๔ ในมลรัฐเท็กซัส ของกองบัญชาการไซเบอร์ กระทรวงกลาโหม สหรัฐ

ที่มา : http://www.naewna.com/politic/columnist/๖๒๑๔

ในปี ค.ศ. ๒๐๐๘ ระบบคอมพิวเตอร์ระบบหนึ่งของทหารสหรัฐอเมริกาถูกทำลาย อย่างไรก็ตาม Lockheed Martin บริษัทผู้ผลิตอาวุธและอากาศยานรายใหญ่ที่สุดของโลกเพิ่งเปิดเผย

ว่าเป็นเหยื่ออีกรายของการเข้าทำลายระบบเช่นกัน รายงานดังกล่าวถูกจุดประกายให้นำไปสู่การถกเถียงหารือกันแต่ก็ยังเป็นประเด็นอ่อนไหวที่เพนตากอนเลือกที่จะไม่กล่าวถึง รวมทั้งการโจมตีของสหรัฐที่เคยทำมาก่อนหน้า และการให้คำนิยามเมื่อถูกก่อวินาศกรรมบนโลกไซเบอร์ว่าเป็นเรื่องที่ต้องให้ความใส่ใจอย่างมาก เพราะสามารถก่อให้เกิดสงครามได้ อนึ่ง คำถามเหล่านี้ก็เคยเป็นหัวข้อที่สร้างความขัดแย้งภายในกลุ่มของเหล่าทหารมาแล้ว

แนวคิดหนึ่งที่อาจได้รับแรงขับเคลื่อนจากเพนตากอนที่ถือว่ามีลักษณะ “สาสมกัน” หากมีการโจมตีในโลกไซเบอร์และนำไปสู่การล้มตาย ความเสียหาย การทำลาย หรือสร้างความแตกแยก ในระดับสูง อันเป็นสาเหตุของการโจมตีทางทหารตามรูปแบบอาจนำไปสู่การพิจารณาเพื่อ “ใช้กำลัง” เพื่อเป็นการแก้แค้นการกระทำดังกล่าวที่เห็นว่าสมน้ำสมเนื้อกันดี

การประยุกต์ใช้ “สงครามตามแบบ” บนโลกไซเบอร์นั้น มียุทธศาสตร์สำคัญที่สะท้อนให้เห็นถึง “หลักการสงครามไซเบอร์” ของสหรัฐฯ และพันธมิตรในการสร้างนโยบายทางด้านความมั่นคงใหม่ โดยองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (NATO) ได้ริเริ่มทำเมื่อปีที่ผ่านมา ซึ่งน่าจะเป็นการรวมกลุ่มเพื่อปรึกษาหารือร่วมกันเพื่อการโจมตีศัตรูบนโลกไซเบอร์หรือผู้ก่อวินาศกรรมด้านสารสนเทศ เจ้าหน้าที่กระทรวงกลาโหมเชื่อว่าการโจมตีทางคอมพิวเตอร์เป็นเรื่องที่ต้องใช้ความเชี่ยวชาญอย่างมากและจำเป็นต้องได้รับความช่วยเหลือจากรัฐบาลในด้านทรัพยากร เช่น การใช้ขีปนาวุธในการจู่โจมด้านเทคโนโลยี อาทิ เครือข่ายเชื่อมโยงระบบสายส่งพลังงาน น่าจะได้รับการพัฒนาโดยมีรัฐเป็นผู้สนับสนุน

พลอากาศตรี Charles Dunlap (เกษียณอายุราชการแล้ว) และอาจารย์แห่ง Duke University law school ได้กล่าวว่า “Act of war” คือ วลีทางการเมือง ไม่ใช่คำที่ใช้ใน ทางกฎหมาย ซึ่งเห็นว่าการโจมตีทางไซเบอร์นั้นมีความรุนแรงพอ ๆ กับการโจมตีด้วยอาวุธ หรือที่ทหารมักเรียกว่าเป็น “การใช้กำลัง” (use of force)

James Lewis ผู้เชี่ยวชาญด้านความมั่นคงทางคอมพิวเตอร์ แห่งศูนย์ศึกษายุทธศาสตร์ระหว่างประเทศ ซึ่งเป็นที่ปรึกษาให้แก่ทีมบริหารของประธานาธิบดีโอบามา กล่าวว่า ในปัจจุบันเจ้าหน้าที่กระทรวงกลาโหมกำลังประเมินว่าการโจมตีทางไซเบอร์ประเภทใดที่ถือเป็น “การใช้กำลัง” ขณะที่นักวางแผนทางด้านการทหารหลายรายเชื่อว่า มาตรการในการ “เอาคืน” หรือ “แก้แค้น” ดังกล่าว ควรต้องระบุให้ชัดถึงความเสียหาย ความพยายาม และสาเหตุของการโจมตีนั้นด้วย

ตัวอย่าง ถ้ามีการก่อวินาศกรรมระบบคอมพิวเตอร์ทำให้เกิดเหตุขัดข้องจนต้องปิดตัวลง เช่น ในด้านการค้า ถ้ามีการขัดขวาง หรือปิดล้อมทางเดินเรือ ก็สามารถพิจารณาได้ว่า ท่าทีดังกล่าวมีลักษณะต้องการ ก่อสงคราม สามารถตัดสินใจให้ใช้มาตรการ “เอาคืน” เพื่อโต้ตอบกลับไปได้เลย

นายกรัฐมนตรี เดวิด คาเมรอน ระบุว่าการโจมตีในโลกไซเบอร์ถือเป็น “ภัยคุกคามสมัยใหม่” อย่างสำคัญที่เราต้องเผชิญ ส่วนรัฐบาลอังกฤษระบุว่าสงครามไซเบอร์จำลอง จะช่วยพัฒนาระบบแลกเปลี่ยนข้อมูลข่าวสารด้านภัยคุกคามระหว่างอังกฤษกับสหรัฐ หน่วยงานที่มีส่วนร่วมในเกมสงครามไซเบอร์ครั้งนี้มีทั้ง MI๕ หน่วยข่าวกรองของอังกฤษ และสำนักงานสอบสวนกลาง FBI ของสหรัฐ ในอนาคตองค์กรเหล่านี้จะผนึกกำลังเป็นเครือข่ายกับหน่วยงานลักษณะเดียวกันของประเทศ อื่น ๆ ด้วย

ปัญหาเรื่องสงครามไซเบอร์เริ่มเป็นภัยคุกคามต่อสหรัฐมากขึ้นเรื่อย ๆ โดยลีออน พาเนตตา รัฐมนตรีว่าการกระทรวงกลาโหมของสหรัฐเคยออกมาเตือนว่าสหรัฐอาจจะพบกับการโจมตีไซเบอร์ครั้งใหญ่โดยไม่รู้ตัว (เขาใช้คำว่า Cyber-Pearl Harbor) ในอีกไม่ช้า และช่วงไม่กี่เดือนที่ผ่านมาเราก็เริ่มเห็นความพยายามของรัฐบาลสหรัฐในการรับมือภัยคุกคามใหม่นี้ เช่น การเพิ่มจำนวนบุคลากรใน “กองกำลังไซเบอร์” ของเพนตากอนจาก ๙๐๐ เป็น ๔,๐๐๐ ตำแหน่ง ซึ่งมุมมองของรัฐบาลโอบามาต่อ “ความมั่นคงไซเบอร์” คือ สาธารณูปโภคและโครงสร้างพื้นฐานสำคัญ ๆ ของประเทศ เช่น ระบบไฟฟ้า ระบบการควบคุมการบินและจราจร ระบบกำจัดขยะและของเสีย โครงข่ายโทรคมนาคม ไปจนถึงโรงไฟฟ้านิวเคลียร์ ซึ่งปัจจุบันถูกควบคุมโดยระบบคอมพิวเตอร์ทั้งหมด ซึ่งอาจเป็นเป้าหมายของศัตรูหรือคนที่ไม่หวังดีต่อสหรัฐ ใช้วิธีการโจมตีทางอิเล็คทรอนิกส์ เช่น การแฮ็ก หรือปล่อย ไวรัสเวิร์ม โจมตีจนระบบเหล่านี้ใช้งานไม่ได้ ส่งผลกระทบต่อเศรษฐกิจและความมั่นคงของประเทศ

ภัยความมั่นคงจากระบบเครือข่ายกลายเป็นปัญหาระดับชาติของรัฐบาลทั่วโลก และกลายเป็นความขัดแย้งระดับประเทศอยู่บ่อยครั้ง โดยกรณีที่โดดเด่น คือการกีดกันของสหรัฐต่ออุปกรณ์เครือข่ายจากบริษัทจีน Huawei และ ZTE ด้วยเหตุผลว่ากลัวจีนวาง “ประตูลับ” (backdoor) เข้าไปล้วงข้อมูลจากหน่วยงานของสหรัฐที่ใช้งานอุปกรณ์เครือข่ายยี่ห้อเหล่านี้

อินเดียเป็นประเทศล่าสุดที่ออกมาตรการป้องกันภัยจากอุปกรณ์เครือข่ายยี่ห้อต่างประเทศ โดยคณะรัฐมนตรีของอินเดียได้แสดงความเป็นกังวลในประเด็นนี้ต่อกระทรวง

โทรคมนาคมของอินเดีย (Department of Telecommunications) และทางกระทรวงก็ประกาศตั้งแล็บทดสอบคุณภาพด้านความปลอดภัยของอุปกรณ์เครือข่าย ทั้งจากประเทศจีน (Huawei และ ZTE) กับจากสหรัฐอเมริกา (Cisco) และยุโรป (Alcatel)

ประเทศจีนมีการจัดตั้ง “ไซเบอร์บลูทีม (Cyber Blue Team)” ขึ้นมา มีเป้าหมายเพื่อเป็นกลไกในการฝึกฝนเพื่อป้องกันความมั่นคงทางอินเตอร์เน็ต และโฆษกกลาโหมจีน Geng Yansheng กล่าวว่า จีนเป็นเหยื่อจากการโจมตีทางไซเบอร์ และไซเบอร์บลูทีม ของกองทัพปลดปล่อยประชาชนพยายามจะสร้างหน่วยความมั่นคงทางอินเตอร์เน็ตให้แข็งแกร่งขึ้น ปัจจุบันความปลอดภัยทางอินเตอร์เน็ตกลายเป็นประเด็นสากลไปแล้ว มันไม่ใช่เรื่องที่ส่งผลกระทบแค่เพียงสังคมในระดับพลเมืองอีกต่อไป แต่ยังส่งผลไปยังมิติทางทหารด้วย

แผนภาพที่ ๒-๘ ไซเบอร์บลูทีม (Cyber Blue Team)

ที่มา : http://www.siamintelligence.com/china-measure-on-yber-war/

นอกจากนี้ประเทศจีนสร้างเครือข่ายคอมพิวเตอร์รหัสลับเชิงควอนตัมรายแรกในโลก เป็นระยะทางไกล ๑,๘๓๐ กิโลเมตร ระหว่างกรุงปักกิ่งและเซี่ยงไฮ้ ซึ่งในทางทฤษฎีถือเป็นระบบป้องกันแฮคเกอร์คุกคามที่มีความปลอดภัยมากที่สุดในโลก และเร็ว ๆ นี้ จีนจะมีเครือข่าย

คอมพิวเตอร์ป้องกันการแอบดักข้อมูลหรือล้วงความลับ แสดงถึงมาตรการเด็ดขาดกำจัดภัยเงียบในสงครามไซเบอร์กับสหรัฐอเมริกา และ The Economist เขียนว่า จีนมีแผนที่จะ “เป็นเจ้าแห่งสงครามสารสนเทศ ในกลางศตวรรษที่ ๒๑” พวกเขายังเขียนว่า ประเทศอื่นกำลังจัดการอย่างเดียวกัน ในสงครามทางอินเตอร์เน็ต อาทิ รัสเซีย อิสราเอล เกาหลีเหนือ นอกจากนั้น อิหร่านยังอ้างว่าจะเป็นกองทัพไซเบอร์ที่ใหญ่ที่สุดเป็นอันดับ ๒ ของโลก เจมส์ กอสเลอร์ ผู้เชี่ยวชาญระบบรักษาความปลอดภัยรัฐบาล กังวลว่า สหรัฐอเมริกา ขาดแคลนผู้เชี่ยวชาญระบบรักษาความปลอดภัยคอมพิวเตอร์อย่างมาก ประมาณว่ามี ๑,๐๐๐ คน ที่ผ่านคุณสมบัติในประเทศในทุกวันนี้ แต่พวกเขาต้องการผู้เชี่ยวชาญถึง ๒๐,๐๐๐ - ๓๐,๐๐๐ คน

ประเทศอังกฤษ ได้ก่อตั้งศูนย์ปฏิบัติการรักษาความปลอดภัยทางไซเบอร์ขึ้น โดยมีศูนย์กลางอยู่ที่สำนักงานใหญ่ด้านการสื่อสารและคมนาคมของประเทศ

ประเทศจีน มีแผนจะพัฒนาไปเป็น “ประเทศเจ้าแห่งสงครามไซเบอร์” ภายในกลางศตวรรษที่ ๒๑ ประเทศอิหร่าน ที่อีกไม่ช้าจะขอเป็น “กองทัพไซเบอร์ใหญ่สุดเป็นลำดับ ๒ ของโลก” ไม่รวมถึง รัสเซีย อิสราเอล และเกาหลีเหนือ ที่ต่างดำเนินการในลักษณะเดียวกันกับหลายประเทศ ที่กล่าวมา เพื่อมิให้ตกขบวนในยุคที่โลกกำลังหันมาทำการยุทธ์แนวใหม่กันทางอินเตอร์เน็ต

ประเทศเอสโตเนีย (Estonia) เป็นการโจมตีทางไซเบอร์ที่เริ่มขึ้นเมื่อ ๒๗ เม.ย. ค.ศ. ๒๐๐๗ ระบบโทรคมนาคม อินเตอร์เน็ต ไฟฟ้า คมนาคม ซึ่งถือเป็นระบบสารสนเทศโครงสร้างพื้นฐานถูกโจมตี ใช้การไม่ได้ จากการโจมตีทางไซเบอร์ โดยเชื่อว่าเป็นการโจมตีจากรัสเซีย หลังจากที่เอสโทเนียได้ทำการย้ายอนุเสาวรีย์วีรบุรุษสงครามในเมือง Tallinn และการเข้ามามีบทบาทในภูมิภาคของ EU วิธีการโจมตีเป็นแบบการกระจายการโจมตี แล้วทำให้ระบบหยุดบริการ (Distributed Denial of Dervice, DDoS) การเปลี่ยนหน้าเว็บไซต์มีการวิเคราะห์กันว่าเป็นการโจมตีที่มีภาครัฐ เป็นผู้สนับสนุน (State sponsored) การโจมตีทางไซเบอร์ดังกล่าว ส่งผลให้ประเทศเอสโทเนีย ซึ่งถือเป็นประเทศชั้นนำด้านการนำเทคโนโลยี และระบบสารสนเทศ เข้ามาช่วยเพิ่มประสิทธิภาพในการทำงาน เกิดผลกระทบในวงกว้าง และมีการกล่าวกับว่าการโจมตีดังกล่าว เป็นการทำสงครามไซเบอร์ของโลกเป็นครั้งแรก (Cyber War I)

ประเทศเกาหลีใต้ (South Korea) เมื่อวันที่ ๒๐ มี.ค. ค.ศ.๒๐๑๓ ซึ่งเป็นวันครบรอบสงครามเกาหลี เครื่องคอมพิวเตอร์จำนวนมากของในเกาหลีใต้ ๓ แห่ง รวมทั้งธนาคารถูกโจมตีใช้การไม่ได้ และเว็บไซต์หน่วยงานราชการรวมถึงเว็บไซต์ของประธานาธิบดีเกาหลีใต้ ถูกเปลี่ยนหน้าเว็บไซต์ จากการวิเคราะห์หาแหล่งที่มาการโจมตีพบว่า มีความเกี่ยวข้องกับ ประเทศเกาหลีเหนือ และยังมีรายงานว่าระบบธนาคาร ก็ได้รับผลกระทบจากการโจมตี

ประเทศเกียร์กีซ (Kyrgyz) เมื่อ วันที่ ๑๔ ธันวาคม ค.ศ.๒๐๐๗ เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศเกียร์กีซ ถูกโจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโทเนีย

นี่เองจึงเป็นจุดพลิกผันให้ปัจจุบันนี้ “สงครามไซเบอร์” ซึ่งมุ่งโจมตี หรือ ก่อวินาศกรรมกันทางสื่อสารสนเทศ กำลังอุบัติขึ้นมา

ในวงการทหารสมัยใหม่ มองว่า ไซเบอร์สเปซ (Cyberspace) คือสนามรบในสงครามไซเบอร์ (Cyber Warfare) ที่ “สารสนเทศ” (Information) กำลังกลายเป็นอาวุธที่สามารถนำมาใช้ในการโจมตีฝ่ายตรงข้ามได้โดยไม่ต้องทำสงครามในรูปแบบเดิม ๆ ดังตัวอย่างที่เห็นได้ชัดเจนจากปรากฏการณ์ “Arab Spring” เป็นปรากฏการณ์การใช้เครือข่ายสังคมออนไลน์โซเชียลเน็ตเวิร์ค เช่น Facebook และ Twitter สร้างกระแสต่อต้านรัฐบาล มีผลกระทบเต็ม ๆ ต่อการบริหารงานของรัฐบาล และ มีผลกระทบต่อภาพลักษณ์ของผู้นำในระดับประเทศ

รายงานการศึกษาวิจัยที่เกี่ยวข้อง

สงครามสารสนเทศ การศึกษาระบบรักษาความปลอดภัยสำหรับเครือข่ายข้อมูลข่าวสารของกองทัพอากาศไทย (วัชรพงศ์ ธรรมรักษ์, งานวิจัยเฉพาะกรณี ตามหลักสูตรวิทยาศาสตรมหาบัณฑิต (การบริหารโทรคมนาคม) วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์ พ.ศ.๒๕๔๔) นโยบายผู้บัญชาการทหารอากาศ ประจำปีพุทธศักราช ๒๕๕๘ ด้านกำลังพลให้ทบทวนและกำหนดความต้องการกำลังพลทั้งเชิงปริมาณและเชิงคุณภาพให้สอดรับกับกรอบงบประมาณประจำปีที่กองทัพอากาศได้รับ ตลอดจนจัดทำแผนการสรรหาและเลือกสรรกำลังพลให้มีความเหมาะสมใน ทุกสายวิทยาการที่มีการปฏิบัติการที่ใช้เครือข่ายเป็น

ศูนย์กลาง เพื่อให้บรรลุวิสัยทัศน์กองทัพอากาศ โดยมุ่งพัฒนากำลังพลที่ปฏิบัติงานด้านสงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับตามมาตรฐานสากล และด้านเทคโนโลยีสารสนเทศและการสื่อสาร พัฒนาขีดความสามารถ การปฏิบัติการด้านสงครามไซเบอร์

กองทัพบกกับความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ (Army and National Cyber Security) (ฤทธี อินทราวุธ, http://km.rta.mi.th/newkm/index.php/menu-km๖/๔-army-and-national-cyber-security) กล่าวว่า สงครามไซเบอร์สิ่งท้าทายความร่วมมือในอนาคตของอาเซียน

นโยบายรัฐมนตรีว่าการกระทรวงกลาโหม พลเอก ประวิตร วงษ์สุวรรณ พัฒนากิจการอุตสาหกรรมป้องกันประเทศ โดยบูรณาการขีดความสามารถของภาครัฐและเอกชน รวมทั้งใช้ประโยชน์จากความร่วมมือในกลุ่มประเทศสมาชิกอาเซียนเพื่อนำไปสู่การพึ่งพาตนเองในการผลิตอาวุธยุทโธปกรณ์รายการที่จำเป็น พัฒนากิจการวิทยาศาสตร์และเทคโนโลยีเพื่อการป้องกันประเทศให้ทัดเทียมกับประเทศในภูมิภาค และสามารถสนับสนุนการพึ่งพาตนเองของอุตสาหกรรมป้องกันประเทศ โดยร่วมมือกับทุกภาคส่วนทั้งในและต่างประเทศ รวมทั้งพัฒนาเทคโนโลยีสารสนเทศการสื่อสารและกิจการอวกาศ โดยเน้นให้เกิดการบูรณาการ ความเป็นมาตรฐานความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในกระทรวงกลาโหม และความสามารถในการรับมือกับสงครามไซเบอร์

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทย และกองบัญชาการกองทัพไทย พ.ศ.๒๕๕๗ – ๒๕๖๑ พันธกิจ ด้านเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทยในการเพิ่มขีดความสามารถในการรักษาความปลอดภัยระบบสารสนเทศ เพื่อลดและป้องกันภัยคุกคามในรูปแบบของ “สงครามไซเบอร์” (Cyber Warfare)

สรุป

ความรักษาความมั่นคงปลอดภัยด้านสารสนเทศในปัจจุบัน เป็นสิ่งที่มีความจำเป็นอย่างมาก เนื่องจากทุกสิ่งทุกอย่างรอบตัวเรา มีความสัมพันธ์กับข้อมูลสารสนเทศในทุก ๆ ด้าน ไม่ว่าจะเป็นเรื่องส่วนตัว หรือเรื่องงานสิ่งต่าง ๆ เหล่านี้ มีการใช้งานที่สะดวกสบายมากขึ้น แต่สิ่งที่ต้องให้ความสนใจและระมัดระวังคือเรื่องของความมั่นคงปลอดภัยด้านสารสนเทศ ใน ๓ ด้านคือ การรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งานของ

ข้อมูล (Availability) เพื่อเป็นหลักพื้นฐานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในส่วนขององค์กรก็เป็นอีกส่วนหนึ่งที่ต้องให้ความสำคัญในการรักษาความมั่นคงปลอดภัย เพื่อให้เกิดความมั่นใจในการใช้บริการข้อมูลต่าง ๆ ทั้งหน่วยงานเอกชน และหน่วยงานภาครัฐ โดยเฉพาะหน่วยงานภาครัฐ ด้านความมั่นคง ก็ให้ความสำคัญในเรื่องของ Cyber Security มากขึ้น ทั้งการทำงานในเชิงรับ (Defensive) เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดี ทั้งที่เป็นการกระทำที่มีรัฐบาลสนับสนุน (State Sponsor) หรือเป็นการทำโดยกลุ่มผู้ไม่หวังดีที่ต้องการทำลายชื่อเสียง หรือขโมยข้อมูล และการทำงานเชิงรุก (Offensive) เพื่อการเข้าโจมตีระบบสารสนเทศของประเทศ หรือหน่วยงานอื่น ๆ ทั้งเพื่อให้ได้มาซึ่งข้อมูล และทำลายระบบไม่ให้สามารถใช้งานได้ ซึ่งปัจจุบันประเทศต่าง ๆ ได้มีการจัดหน่วยงานด้านไซเบอร์ขึ้นมาทำงานด้านนี้ ทั้งประเทศสหรัฐ จีน เกาหลีใต้ เป็นต้น นอกจากการดำเนินการทางด้านเทคนิค ยังต้องมีการดำเนินการในเรื่องของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นแนวทางในการปฏิบัติให้กับส่วนราชการ หรือหน่วยงานเอกชน ซึ่งถือเป็นการทำด้านกระบวนการ (Process) ต่อมาในการทำในเรื่องบุคคลากร (People) การจัดการให้ความรู้ (Knowledge) เพื่อให้สามารถปฏิบัติงานในด้านความมั่นคงปลอดภัยได้อย่างถูกต้อง และมีประสิทธิภาพ สุดท้ายคือ เทคโนโลยี (Technology) คือ การที่มีระบบหรืออุปกรณ์ในด้านการ รักษาความมั่นคงปลอดภัยสารสนเทศ ช่วยในการป้องกันการบุกรุก หรือใช้ในการโจมตี (Hacking) เครือข่ายอื่น ๆ ในระบบสงครามไซเบอร์ การกำหนดหน่วยความรับผิดชอบมีความจำเป็นอย่างสูง เพื่อเป็นการเตรียมความพร้อมทั้งความรู้ความสามารถกำลังพล และอาวุธยุทโธปกรณ์ ที่เหมาะสมต่อการปฏิบัติการสงครามไซเบอร์

บทที่ ๓

การพัฒนาปฏิบัติการสงครามไซเบอร์

การใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำสงคราม หรือมักเรียกกันว่าสงครามไซเบอร์ มีการโจมตีกันหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด เช่น การโจมตีเว็บ หรือบล็อคเว็บ การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ต การเจาะข้อมูลลับโดย แฮกเกอร์ ที่นอกจากได้ข้อมูลลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้ การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้ หรือทำงานไม่แม่นยำ ไปจนถึงการโจมตีโครงสร้างพื้นฐาน (Infrastructure Attacking) เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมผ่านระบบเครือข่าย โดยระบบคอมพิวเตอร์ (Computer Network Controller) ซึ่งเป็นจุดอ่อนต่อการโจมตีมาจากฝ่าย ตรงข้ามหรือผู้ไม่ประสงค์ดี สงครามไซเบอร์จึงเป็นการปฏิบัติที่มีความสลับซับซ้อน ผู้วิจัยจึงได้ศึกษาการพัฒนาปฏิบัติการสงครามไซเบอร์ โดยกำหนดหัวข้อไว้ ดังนี้

๑. รูปแบบปฏิบัติการสงครามไซเบอร์
๒. แนวโน้มปฏิบัติการสงครามไซเบอร์
๓. ความพร้อมของกำลังพลและหน่วยงานต่อปฏิบัติการสงครามไซเบอร์
๔. ข้อจำกัดในการดำเนินการ

รูปแบบปฏิบัติการสงครามไซเบอร์

การปฏิบัติการสงครามไซเบอร์ (Cyber Warfare Operation) มีอยู่ด้วยกัน ๕ รูปแบบ ได้แก่

๑. Cyberspace Superiority คือ การครอง Cyberspace หรือการที่ต้องมีความสามารถ ในการปฏิบัติการสงครามไซเบอร์บน Cyberspace เหนือกว่าฝ่ายตรงข้าม และต้องป้องกันไม่ให้ ฝ่ายตรงข้ามสามารถปฏิบัติการสงครามไซเบอร์ต่างๆ บน Cyberspace ได้เช่นกัน

๒. Counter-Cyber เป็นการตอบโต้ฝ่ายตรงข้ามโดยใช้วิธีการปฏิบัติสงครามไซเบอร์ใน ๒ รูปแบบ คือ

๒.๑ Offensive Counter-Cyber (OCC) การปฏิบัติการตอบโต้ทางไซเบอร์เชิงรุก โดยวิธีการทำให้ระบบของฝ่ายตรงข้ามปฏิเสธการให้บริการ (Denial Of Service, DoS) การทำลายหรือหลอกลวงความสามารถของศัตรูในการที่จะปฏิบัติการบน Cyberspace เช่น สงครามอ่าวเปอร์เซีย ก่อนที่สหรัฐจะใช้กำลังทางทหาร ได้มีการปฏิบัติการทางไซเบอร์เพื่อโจมตีเครือข่ายของ AT&T ซึ่งเป็นศูนย์กลางการสื่อสารโทรคมนาคมของอิรัก ทำให้ไม่สามารถใช้การสื่อสารโทรคมนาคมได้

๒.๒ Defensive Counter-Cyber (DCC) การป้องกันการตอบโต้ทางไซเบอร์ จากฝ่ายตรงข้าม โดยใช้วิธีการตรวจสอบและสกัดกั้นทำลายหรือลบล้าง กองกำลังทางไซเบอร์ ของฝ่ายตรงข้ามที่พยายามจะเจาะหรือโจมตีผ่าน Cyberspace เช่น การมีระบบตรวจจับและป้องกันการบุกรุกเครือข่าย (Intrusion Detection/Prevention System, IDS/IPS) หรือการใช้อุปกรณ์ควบคุมการเข้าถึงประเภทไฟล์วอลล์ (Firewall) โดยมีการตั้งกฎของไฟล์วอลล์ เพื่อควบคุมและป้องกันการถูกโจมตีจากฝ่ายตรงข้ามผ่านทางระบบเครือข่าย

๓. Cyberspace Control คือความสามารถในการควบคุมการปฏิบัติสงครามไซเบอร์ต่าง ๆ ใน Cyberspace เช่น

๓.๑ การมีอำนาจในการอนุมัติการปฏิบัติการโต้ตอบทางไซเบอร์เชิงรุก

๓.๒ ดำเนินการในการป้องกันทางไซเบอร์จากฝ่ายตรงข้าม

๓.๓ การใช้ยุทธวิธี หรือกลยุทธ์ในการบูรณาการ การปฏิบัติการทางไซเบอร์ร่วมกันกับชาติต่าง ๆ เพื่อเป็นการลดความขัดแย้งที่อาจก่อให้เกิดสงครามไซเบอร์

๔. Cross-Domain Operations คือการใช้ปฏิบัติการทางไซเบอร์เพื่อให้บรรลุผลใน Domain อื่น ๆ กองทัพสหรัฐแบ่งพื้นที่การรบออกเป็น ๕ พื้นที่/โดเมนคือ Land, Sea, Air, Space และ Cyberspace เช่น

๔.๑ การใช้ปฏิบัติการทางไซเบอร์ เพื่อทำให้เกิดการหยุดชะงักหรือทำลายการป้องกันทางกายภาพ (กล้องวงจรปิด CCTV, Sensor ตัวจับการบุกรุก เป็นต้น)

๔.๒ การสั่งห้ามหรือการควบคุมระบบ Command Control (C2 Link) ของฝ่ายตรงข้าม

๔.๓ การใช้ปฏิบัติการทางไซเบอร์ที่ทำให้เกิดการหยุดชะงักการให้บริการ หรือการควบคุมระบบสาธารณูปโภค เช่น ไฟฟ้า ประปา และนิวเคลียร์

๔.๔ การทำให้เกิดการหยุดชะงักระบบตลาดการเงินหรือระบบเศรษฐกิจ

๕. Operational Considerations สิ่งที่เป็นข้อพิจารณาในการใช้ปฏิบัติการทาง ไซเบอร์ เช่น

๕.๑ การตรวจสอบให้แน่ใจถึงการกระทำต่าง ๆ ในโลกไซเบอร์ ซึ่งทุกคนมีสิทธิเสรีภาพในการทำกิจกรรมต่าง ๆ แต่ต้องไม่เป็นการสร้างภัยคุกคามให้เกิดขึ้น

๕.๒ ถ้าเราสามารถครอง หรือควบคุม Cyberspace ได้ฝ่ายตรงข้ามก็จะปฏิบัติการใด ๆ บน Cyberspace ได้ลำบาก

๕.๓ การตอบโต้การใช้งานที่เป็นลักษณะประสงค์ร้าย ของฝ่ายตรงข้ามที่ใช้ Cyberspace

๕.๔ การแทรกซึมหรือแฝงตัวเข้าถึงระบบต่าง ๆ ของฝ่ายตรงข้าม เช่น การฝัง botnet, Root kit, หรือ Trojan horse ที่ช่วยให้สามารถใช้ในการปฏิบัติการ Cyberspace ได้

แนวโน้มปฏิบัติการสงครามไซเบอร์

เป้าหมายในการปฏิบัติการสงครามไซเบอร์ มีแนวโน้มการโจมตีเป้าหมาย ระบบต่าง ๆ ดังนี้

๑. ระบบเครือข่ายคอมพิวเตอร์ทางทหาร (Military Networks) เป็นเป้าหมายหลักที่ จะถูกโจมตี เพื่อดึงข้อมูล เฝ้าตรวจ และทำลายเพื่อไม่ให้สามารถใช้งานได้

๒. ระบบบริหารจัดการของหน่วยงานภาครัฐและเว็บไซต์ (Government Systems and Websites) เป็นเป้าหมายเพื่อทำให้ระบบบริหารจัดการที่ใช้ในการบริหารประเทศล่ม และเสียหายไม่สามารถใช้งานได้ เกิดความชะงักงันในการดำเนินการ ที่จะส่งผลให้ประชาชนเกิดความ ไม่พอใจ และสร้างความเสียหายต่อทั้งระบบทางด้านสาธารณูปโภค เช่น ระบบไฟฟ้า ประปา ระบบการ

โทรคมนาคมต่าง ๆ อีกสิ่งหนึ่งซึ่งเป็นช่องทางในการให้ข้อมูลข่าวสาร และให้บริการต่าง ๆ ต่อประชาชน คือ เว็บไซต์ ก็จะเป็นส่วนที่จะถูกโจมตีได้เช่นกัน ทั้งเปลี่ยนแปลงหน้าจอเว็บไซต์ (Web Defacement) เพื่อทำให้หน่วยงานขาดความน่าเชื่อถือ ที่จะเข้าไปใช้บริการ หรือถูกเจาะระบบ (Hacking) เพื่อไปดึงข้อมูลที่สำคัญต่าง ๆ ทั้งข้อมูลของหน่วยงาน และข้อมูลของผู้เข้ามาใช้บริการ

๓. สถาบันการเงินและสินเชื่อ (E-commerce and Financial Institutes) เป็นส่วนที่สำคัญที่จะตกเป็นเป้าหมาย

๔. บริษัทผู้ให้บริการโทรคมนาคม (Telecommunication Companies)

๕. อื่น ๆ (Other) เช่น ระบบอาวุธทางไซเบอร์ (Cyber Weapons) ซึ่งแบ่งได้เป็น ๒ กลุ่ม คือ

๕.๑ Software Based Weapons เพื่อไม่ให้มีความพร้อมในการใช้งาน (Availability) หรือลดประสิทธิภาพความสามารถในการใช้งาน (Capability)

๕.๒ Hardware Based Weapons ความมุ่งหมายเช่นเดียวกับ Software Based Weapons รวมถึงการทำให้การผลิตมีค่าใช้จ่ายที่สูงขึ้น จากการต้องซ่อมแซมแก้ไข (Cost of Manufacturing)

ตัวอย่าง การปฏิบัติการสงครามไซเบอร์ระหว่างปาเลสไตน์ กับ อิสราเอล เมื่อวันที่ ๒๘ กันยายน พ.ศ. ๒๕๔๓ แฮกเกอร์วัยรุ่นชาวอิสราเอล ได้โจมตีเว็บไซต์ของกลุ่มฮิลบัลเลอะและฮามาส ในเลบานอน ซึ่งเรียกกลุ่มนี้ว่า Cyber Jihad จากปาเลสไตน์ หรือกลุ่มแฮกเกอร์ที่มีในอิสราเอล เช่น Mossad, Wizel, Israel Hackers Unit, Israeli Internet Underground, Small Mistake, Analyzer และ ViRii เป็นต้น

ยุทธวิธีและกลยุทธ์ที่กลุ่มแฮกเกอร์ชาวอิสราเอล นิยมใช้ เช่น การไปลงทะเบียนเว็บไซต์ด้วยการสะกดคำที่ผิด จาก Hamas.com เป็น hamas.org ทำการ Propaganda, การโจมตีเว็บไซต์จำนวนมาก การส่งอีเมล์ จำนวนมากต่อวัน

ส่วนของปาเลสไตน์ ก็มีกลุ่มของแฮกเกอร์ที่มีความชำนาญ เช่น กลุ่ม G-Force Pakistan, Dr.Nuker, Pakistani Hackerz Club เป็นต้น ซึ่งเป้าหมายในการโจมตีประเทศอิสราเอล ก็คือ ทหาร ธนาคาร สถาบันการศึกษา หน่วยงานราชการ บริษัทที่ใช้บริการระบบโทรคมนาคม และสถาบันแลกเปลี่ยนเงินตรา

การปฏิบัติการสงครามไซเบอร์ระหว่างอิหร่าน กับ สหรัฐอเมริกา ที่มีการพัฒนากระบวนการให้ยากต่อการตรวจจับภัยคุกคามต่าง ๆ ต่อสหรัฐ เพื่อให้มีผลกระทบในทุกภาคส่วน ทั้งเศรษฐกิจ ความมั่นคง การเมือง และสังคม

การปฏิบัติการสงครามไซเบอร์ระหว่างจีน คิวบา กับ สหรัฐอเมริกา มีวิศวกร นักคอมพิวเตอร์ เจ้าหน้าที่เทคนิค จำนวน ๑,๑๐๐ คน แบ่งออกเป็น ๓ กลุ่ม เข้าไปทำงานในบริษัทางด้านโทรคมนาคมของอเมริกา

การปฏิบัติการสงครามไซเบอร์ระหว่างอินเดีย และ ปากีสถาน โดยเกิดขึ้นครั้งแรก เมื่อเดือน พฤษภาคม พ.ศ.๒๕๕๒ เป้าหมายที่ศูนย์วิจัย Bhabha Atomic เรื่องการเปิดเผยข้อมูลเกี่ยวกับการทดสอบนิวเคลียร์ผ่านทางอีเมล์ โดยการปลอมแปลงเว็บไซต์ (Web Defacement) ในส่วนของกลุ่มแฮกเกอร์ปากีสถาน ก็มีเป้าหมายที่ Guirat Governmant, Ministry Of External Affairs เป็นต้น ซึ่งกลุ่มแฮกเกอร์ที่มีชื่อเสียงอาทิเช่น AIC, Gforce Pakistan, Silver Lords

จากตัวอย่างการปฏิบัติการสงครามไซเบอร์ของประเทศต่าง ๆ ที่กล่าว จะเห็นว่าเป็นไปตามแนวโน้มปฏิบัติการสงครามไซเบอร์ตามเป้าหมายข้างต้น

ความพร้อมของกำลังพลและหน่วยงานต่อปฏิบัติการสงครามไซเบอร์

กระทรวงกลาโหม

ในส่วนของราชการทหาร นายกรัฐมนตรี/รัฐมนตรีว่าการกระทรวงกลาโหม ได้อนุมัติหลักการให้จัดตั้งศูนย์ปฏิบัติการไซเบอร์กลาโหมขึ้น โดยกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ เตรียมจัดตั้งหน่วยงานด้านไซเบอร์โดยตรง (Cyber Command) เพื่อขึ้นมารองรับการปฏิบัติงานความมั่งคงปลอดภัยของประเทศ จากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ โดยศูนย์ปฏิบัติการไซเบอร์กลาโหม (Cyber Operations Center, COC) จะเป็นแกนหลักในด้านการพัฒนาบุคลากรด้านนี้ให้กับกำลังพลสังกัดกระทรวงกลาโหม โดยจะมีห้องปฏิบัติการสำหรับการฝึกปฏิบัติด้านสงครามไซเบอร์ (Cyber Warfare) รวมถึงการสร้างภาคีเครือข่าย ประชาคม ทั้งภาครัฐและเอกชน เพื่อเสริมสร้างศักยภาพของประเทศด้านไซเบอร์ในการรับมือกับภัยคุกคามจากสงครามไซเบอร์

กองบัญชาการกองทัพไทย

ตามมติสภากลาโหม ครั้งที่ ๕/๒๕๕๖ เรื่อง ภัยคุกคามด้านไซเบอร์ ได้กำหนดให้กองบัญชาการกองทัพไทย นำข้อมูลไปศึกษาและพิจารณาแนวทางการดำเนินการจัดตั้งหน่วยไซเบอร์ขึ้นมารับผิดชอบภัยคุกคามด้านไซเบอร์เป็นการเฉพาะ โดยใช้การปรับเกลี่ยอัตราที่มีอยู่ให้เกิดประโยชน์สูงสุด ดังนั้นทางกองบัญชาการกองทัพไทย จึงจัดตั้งหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกันและรับมือกับภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ เพิ่มขีดความสามารถในการรักษาความปลอดภัยระบบสารสนเทศ เพื่อลดและป้องกันภัยคุกคามในรูปแบบของ “สงครามไซเบอร์” (Cyber Warfare) โดยมีหน่วยงานที่รับผิดชอบ คือ กรมยุทธการทหาร และ กรมการสื่อสารทหาร

กองทัพบก

ได้มีนโยบายและอนุมัติหลักการให้ ศูนย์เทคโนโลยีทางทหาร (ศทท.) ดำเนินการปรับปรุงภารกิจและโครงสร้างการจัดหน่วย โดยเพิ่มเติมภารกิจด้านการปฏิบัติการสงครามไซเบอร์ และปรับสายการบังคับบัญชาจากเดิม เป็นหน่วยขึ้นตรงกรมการทหารสื่อสาร มาเป็นหน่วยขึ้นตรงกองทัพบก (นขต.ทบ.) เพื่อเตรียมรองรับการปฏิบัติงานความมั่งคงปลอดภัยด้านไซเบอร์ ที่ส่งผลกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ โดยเฉพาะความมั่นคงทางการทหาร และการรักษาความสงบเรียบร้อยภายในประเทศ รวมถึงการปฏิบัติการที่ประสานสอดคล้องกับกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพต่าง ๆ ตลอดจนรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations, NCO) โดยแนวความคิดเบื้องต้นในการเตรียมการดำเนินการพัฒนาปรับปรุงภารกิจ โครงสร้างการจัดหน่วย และการพัฒนาศักยภาพของกำลังพล ให้มีคุณวุฒิการศึกษา คุณลักษณะ ขีดความสามารถ ประสบการณ์ และความถนัดเฉพาะด้านที่สอดคล้องกับตำแหน่งหน้าที่การงาน (put the right to the right job) เพื่อให้การปฏิบัติภารกิจที่ได้รับมอบเป็นไปอย่างมีประสิทธิภาพ โดยเน้นการปรับเกลี่ย โยกย้าย และการบรรจุกำลังพลด้านปฏิบัติการเป็นหลักมากกว่างานทางธุรการ ในสัดส่วนไม่น้อยกว่า ๗๐ : ๓๐ สำหรับในด้านการปรับปรุงโครงสร้างการจัดหน่วย โดยแปรสภาพ กองการสงครามสารสนเทศ เป็น กองปฏิบัติการไซเบอร์ (Cyber Operations Division) ซึ่งจะเป็นหน่วยปฏิบัติการด้านไซเบอร์เชิงรุก (Cyber Offensive Operation) โดยจะดำเนินการด้านการตรวจสอบสภาพแวดล้อมของภัยคุกคาม การวางแผนควบคุม

การปฏิบัติ และการปฏิบัติการไซเบอร์ โดยจะมีแผนการบรรจุและพัฒนากำลังพลที่มีความรู้ความเชี่ยวชาญ และได้รับการฝึกฝนด้านการปฏิบัติการไซเบอร์ ปฏิบัติหน้าที่เป็นนักรบไซเบอร์ (Cyber Warriors) อยู่ในชุดปฏิบัติการไซเบอร์ (Cyber Operation Teams, COT) และชุดเตรียมพร้อมเผชิญเหตุฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Teams, CERT) เป็นหน่วยปฏิบัติการและเตรียมจัดตั้ง กองรักษาความปลอดภัยด้านไซเบอร์ (Cyber Security Division) ซึ่งเป็นหน่วยปฏิบัติการด้านไซเบอร์เชิงรับ (Cyber Defensive Operations) ดำเนินการด้านระเบียบการรักษาความปลอดภัยสารสนเทศ การป้องกัน เฝ้าระวัง ตรวจสอบช่องโหว่ โดยใช้เครื่องมือระบบตรวจหาการบุกรุก (Intrusion Detection System, IDS) และระบบป้องกันการบุกรุก (Intrusion Protection System, IPS) รวมถึงการกู้คืนสภาพเมื่อถูกโจมตี (Recovery) ตลอดจนการพัฒนาโปรแกรมและเครื่องมือต่าง ๆ เพื่อรองรับงานด้านไซเบอร์ นอกจากนี้ยังได้เตรียมการด้านการพัฒนาเทคโนโลยีและนวัตกรรมต่าง ๆ ด้านไซเบอร์ โดยแสวงความร่วมมือกับหน่วยงานต่างๆ ทั้งภายในและภายนอกกองทัพ ทั้งภาครัฐและองค์กรเอกชนในด้านวิชาการ การวิจัยพัฒนา (R&D) การสัมมนา เชิงปฏิบัติการ (Workshop) และการฝึกปฏิบัติต่างๆ โดยเฉพาะการฝึกซ้อมแผนเผชิญเหตุด้านไซเบอร์ (Cyber Incident Action Plan Exercise) การฝึกซ้อมแผนฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Exercise) การฝึกซ้อมการปฏิบัติการไซเบอร์ (Cyber Operations Exercise) และการฝึกจำลองสงครามไซเบอร์ (Cyber Warfare Simulation Exercise) เป็นต้น

กองทัพเรือ

มีกองสงครามอิเล็กทรอนิกส์ และกองสงครามไซเบอร์ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ รับผิดชอบ ซึ่งจะพัฒนาขีดความสามารถในการรักษาความปลอดภัยสารสนเทศ ตามแนวคิด Defense-in-Depth ตั้งแต่เครือข่ายคอมพิวเตอร์แม่ข่าย (Server) ไปจนถึงคอมพิวเตอร์ปลายทาง (Endpoint) มีแนวทางการใช้งาน ระเบียบ มาตรการ เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ มีระบบจำลองการฝึกปฏิบัติการสงครามไซเบอร์ในส่วนการตรวจจับ (Sensor) การเฝ้าติดตาม (Monitor) และการจัดเก็บข้อมูล (Log) สามารถนำผลการฝึกไปใช้ประโยชน์ ในการศึกษาวิเคราะห์และพัฒนาขีดความสามารถของกำลังพล ด้านปฏิบัติการเครือข่ายคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ

กองทัพอากาศ

มีนโยบายให้ ทบทวนและกำหนดความต้องการกำลังพลทั้งเชิงปริมาณและเชิงคุณภาพ ให้สอดรับกับกรอบงบประมาณประจำปีที่กองทัพอากาศได้รับ ตลอดจนจัดทำแผนการสรรหา และการเลือกสรรกำลังพลให้มีความเหมาะสมในทุกสายวิทยาการที่มีการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง เพื่อให้บรรลุวิสัยทัศน์กองทัพอากาศ โดยมุ่งพัฒนากำลังพลที่ปฏิบัติงานด้านสงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์ มีการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ โดยเฉพาะการกระตุ้นและพัฒนากำลังพลด้านไซเบอร์ให้มีความพร้อมในการปฏิบัติการด้านไซเบอร์ ทั้งเชิงรุกและเชิงรับตามมาตรฐานสากล

ข้อจำกัดในการดำเนินการ

การพัฒนาปฏิบัติการสงครามไซเบอร์ มีข้อจำกัดในเรื่องของความรู้กำลังพล ที่ต้องได้รับการอบรมและศึกษาทั้งทางทฤษฎีและทางปฏิบัติเกี่ยวกับเครื่องคอมพิวเตอร์ ระบบเครือข่าย ระบบโทรคมนาคมและการสื่อสาร การเข้ารหัสและถอดรหัส เพื่อที่จะได้นำมาประยุกต์ใช้ในการปฏิบัติสงครามไซเบอร์ รวมทั้งในแง่ของกฎหมาย ยังไม่มีการออกกฎหมาย เพื่อรองรับการปฏิบัติการสงครามไซเบอร์ที่ชัดเจน อาจจะทำให้หน่วยปฏิบัติหรือผู้ปฏิบัตินั้นไม่สามารถปฏิบัติได้อย่างเต็มที่ ตามที่ได้รับมอบหมาย ส่วนในด้านของเทคโนโลยี เครื่องมือที่ทันสมัยในการใช้เป็นอาวุธทางด้านการปฏิบัติการสงครามไซเบอร์ ก็ยังมีราคาแพง และกลุ่มผู้ผลิตก็ยังไม่ได้เปิดเผยออกมา เนื่องจากเทคโนโลยีส่วนใหญ่มาจากประเทศมหาอำนาจ เช่น สหรัฐ อังกฤษ และรัสเซีย เป็นต้น

สำหรับกองบัญชาการกองทัพไทย การพัฒนาปฏิบัติการสงครามไซเบอร์ นับว่ายังอยู่ในระดับที่สามารถดำเนินการได้อย่างจำกัด อันเนื่องมาจากข้อกำหนดการปฏิบัติของหน่วยงานที่ต้องเป็นไปตามสายบังคับบัญชาที่ยังต้องได้รับการพัฒนาในเรื่องการบูรณาการของหน่วยต่างๆ ที่เกี่ยวข้องทั้งในส่วนอำนวยการ ส่วนปฏิบัติ และส่วนสนับสนุนการปฏิบัติ รวมไปถึงข้อกำหนดการปฏิบัติการทางทหารด้านสงครามไซเบอร์กับภาคการเมือง ภาคพลเรือน และภาคเอกชน

บทที่ ๔

ปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย

ปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย มุ่งเน้นการปฏิบัติของศูนย์บัญชาการทางทหาร (ศบท.) โดยผู้วิจัยได้กำหนดแนวทางการปฏิบัติไว้ตามหัวข้อ ดังนี้

๑. นโยบายและแนวปฏิบัติการปฏิบัติการสงครามไซเบอร์

๒. รูปแบบที่เหมาะสมของปฏิบัติการสงครามไซเบอร์

๓. มาตรการส่งเสริมการปฏิบัติที่มีประสิทธิภาพ

นโยบายและแนวปฏิบัติการปฏิบัติการสงครามไซเบอร์

การปฏิบัติสงครามไซเบอร์ เป็นการปฏิบัติการโดยใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายเป็นหลัก เกิดการปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations, CNO) จากการศึกษารวบรวมข้อมูลผู้วิจัยจึงกำหนดการปฏิบัติที่สำคัญ แบ่งออกเป็น ๒ ด้าน คือ

๑. การปฏิบัติการไซเบอร์เชิงรุก (Cyber Offensive Operations) ประกอบด้วย การปฏิบัติสำคัญ ๒ แนวทางคือ การโจมตีทางเครือข่ายคอมพิวเตอร์ของฝ่ายตรงข้าม (Computer Network Attack, CNA) และการเจาะแอบเอาข้อมูลจากเครือข่ายคอมพิวเตอร์ของ ฝ่ายตรงข้าม (Computer Network Exploitation, CNE) โดยมีวิธีปฏิบัติการสงครามไซเบอร์ ดังนี้

๑.๑ การหลอกลวง (Deception)

๑.๒ การปฏิเสธ (Denial)

๑.๓ การทำลาย (Destruction)

๑.๔ การเจาะระบบ (Exploitation)

๒. การปฏิบัติการไซเบอร์เชิงรับ (Cyber Defensive Operations) มีการปฏิบัติสำคัญคือ การปกป้องทางเครือข่ายคอมพิวเตอร์ (Computer Network Defense, CND) โดยมีวิธีปฏิบัติการสงครามไซเบอร์ ดังนี้

๒.๑ การปกป้อง (Guard)

๒.๒ การระบุตัวตน (Identify)

๒.๓ การกู้คืน (Recover)

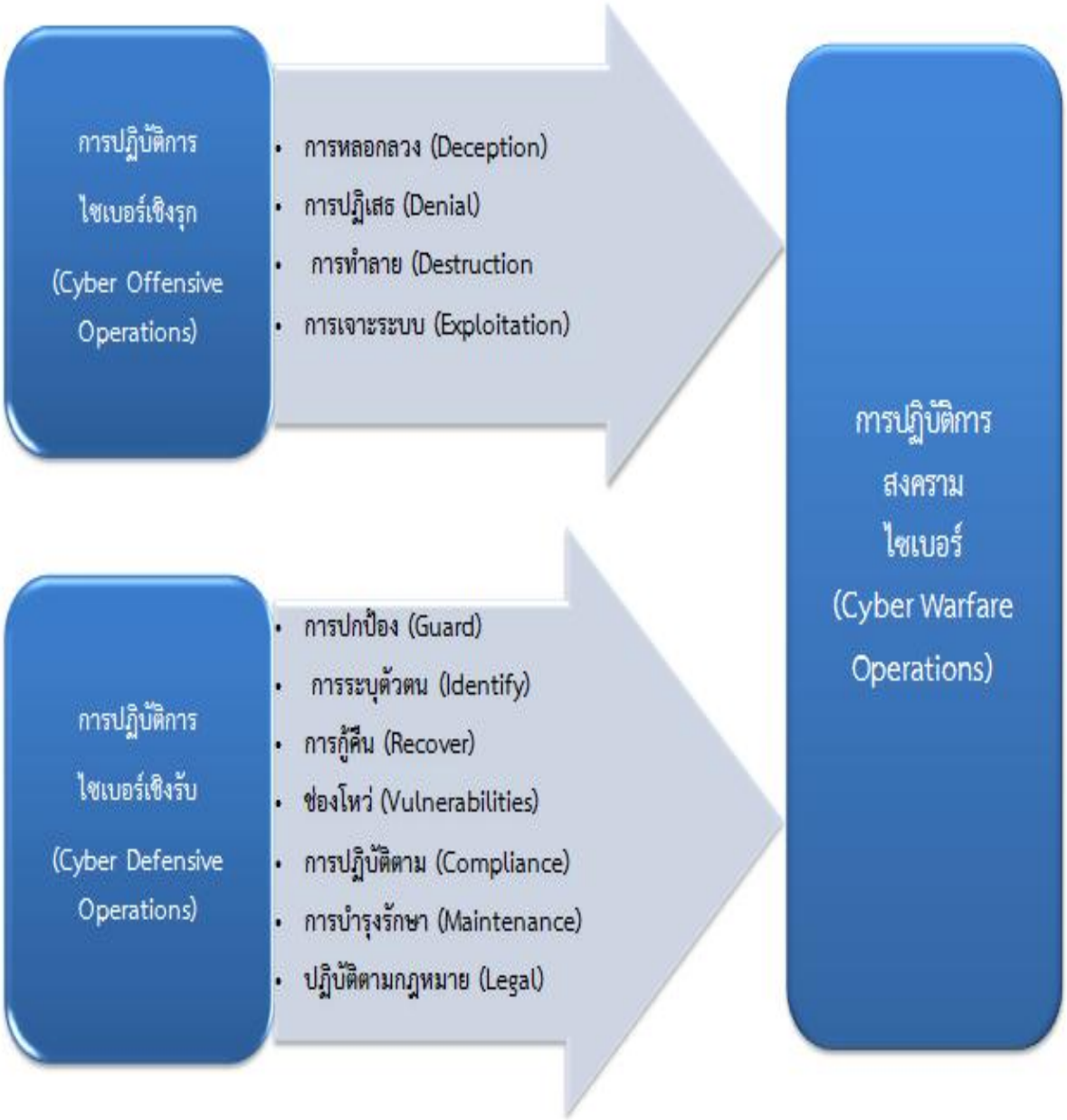
๒.๔ ช่องโหว่ (Vulnerabilities)

๒.๕ การปฏิบัติตาม (Compliance)

๒.๖ การบำรุงรักษา (Maintenance)

๒.๗ ปฏิบัติตามกฎหมาย (Legal)

แผนภาพที่ ๔-๑ นโยบายและแนวปฏิบัติการปฏิบัติการสงครามไซเบอร์



จากการปฏิบัติการไซเบอร์ที่สำคัญ ๒ ด้าน กำหนดแนวปฏิบัติให้กับส่วนงานที่เกี่ยวข้อง ๔ ส่วน โดยมีส่วน ส่วนสร้างความตระหนักในสถานการณ์ทางไซเบอร์ (Cyber Security Awareness) สำคัญ ทำหน้าที่เชื่อมโยงกับส่วนอื่น ๆ ดังนี้

๑. ส่วนปฏิบัติการเครือข่ายไซเบอร์ (Cyber Network Operations) มีหน้าที่ โดยกำหนดเป็นแนวปฏิบัติสำหรับการปฏิบัติการสงครามไซเบอร์ ดังนี้

๑.๑ วางแผนและวิศวกรรมเครือข่ายคอมพิวเตอร์

๑.๒ ติดตั้งและปฏิบัติงานเครือข่ายคอมพิวเตอร์

๑.๓ บำรุงรักษาเครือข่ายคอมพิวเตอร์

๑.๔ บริหารจัดการข้อมูลสารสนเทศให้มีความมั่นคงปลอดภัย

๑.๕ ป้องกันการบริการเครือข่ายคอมพิวเตอร์

๑.๖ เฝ้าระวังเครือข่ายคอมพิวเตอร์

๑.๗ บำรุงรักษาการสร้างความตระหนักรู้การปกป้องและภัยคุกคามไซเบอร์

๒. ส่วนสงครามไซเบอร์ (Cyber War) มีหน้าที่ โดยกำหนดเป็นแนวปฏิบัติสำหรับการปฏิบัติการสงครามไซเบอร์ ดังนี้

๒.๑ กำหนดและวิเคราะห์ข้อมูลเครือข่ายคอมพิวเตอร์

๒.๒ ศึกษาและกำหนดคุณสมบัติของภัยคุกคามไซเบอร์

๒.๓ ติดตาม เป้าหมาย และเจาะระบบฝ่ายตรงข้าม

๒.๔ เตรียมการกำหนดและใช้แนวทางการปฏิบัติการไซเบอร์กับฝ่ายตรงข้าม และแจ้งเตือน

๒.๕ สนับสนุนในการสร้างความตระหนักรู้การปกป้องและภัยคุกคามไซเบอร์

๒.๖ ปฏิบัติการป้องกันไซเบอร์โดยทันที

๒.๗ ช่วยตรวจสอบและวิเคราะห์ลักษณะการโจมตีของฝ่ายตรงข้าม

๓. ส่วนสนับสนุนไซเบอร์ (Cyber Support) มีหน้าที่ โดยกำหนดเป็นแนวปฏิบัติสำหรับการปฏิบัติการสงครามไซเบอร์ ดังนี้

๓.๑ การตรวจสอบช่องโหว่ ทดสอบและประเมินผล

๓.๒ การตรวจสอบการรักษาความปลอดภัยภัยคุกคามพื้นฐาน

๓.๓ การแก้ไขช่องโหว่และรักษาความปลอดภัย

๓.๔ ค้นหาโครงสร้างของโปรแกรมประสงค์ร้าย

๓.๕ โจมตีช่องโหว่ในที่ตั้งที่กำหนด

๓.๖ การตอบโต้ข่าวกรอง

๓.๗ การสืบสวนทางไซเบอร์

๓.๘ การบังคับใช้กฎหมาย

๓.๙ การวิจัยและพัฒนาทางไซเบอร์

๓.๑๐ การพัฒนาการฝึกทางไซเบอร์

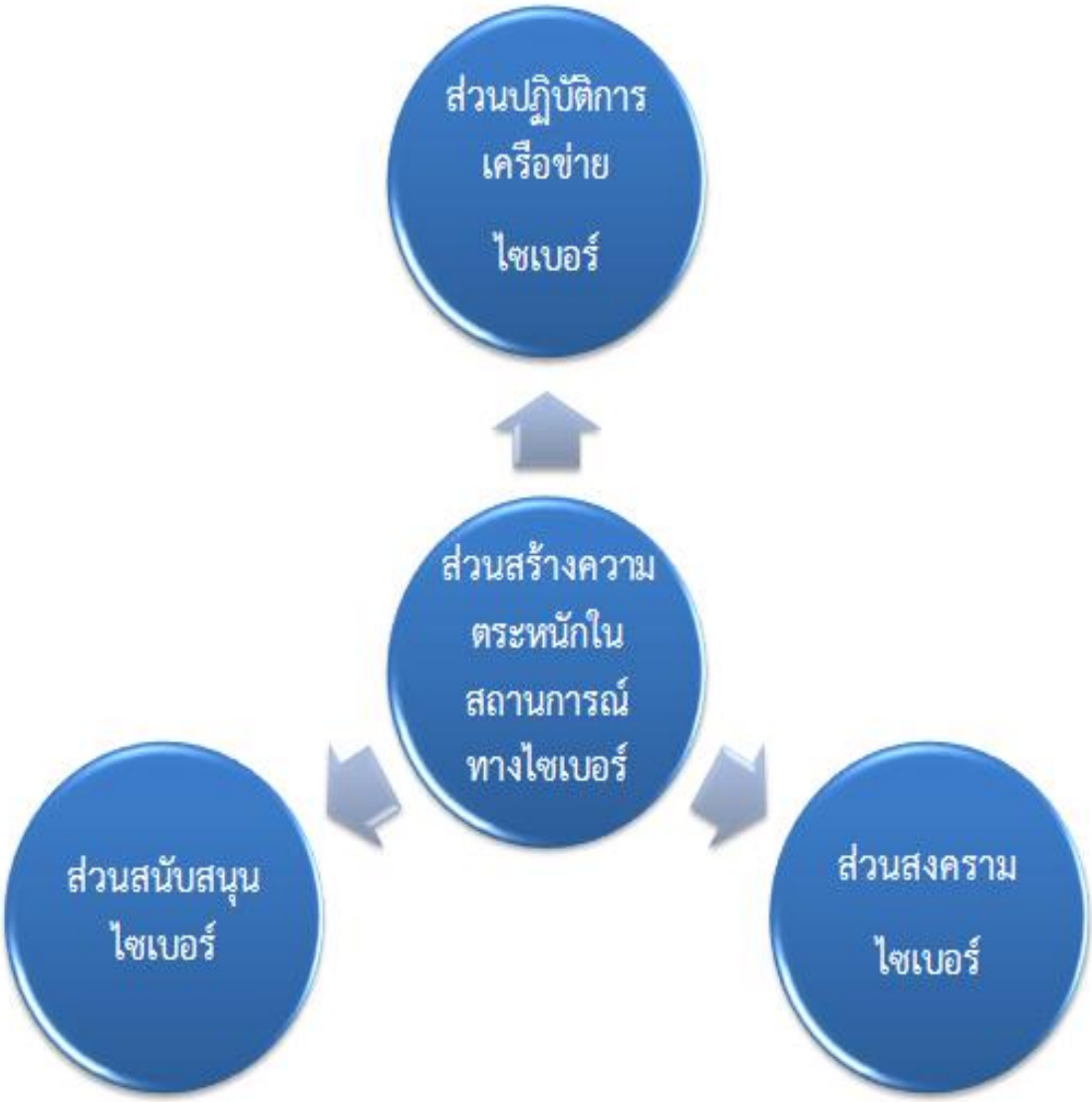
๔. ส่วนสร้างความตระหนักในสถานการณ์ทางไซเบอร์ (Cyber Security Awareness)

๔.๑ การทำให้ไซเบอร์เกิดความเข้าใจและใช้งานได้อย่าง Friendly

๔.๒ การสร้างความตระหนักต่อปฏิบัติการไซเบอร์และสถานการณ์ของฝ่ายตรงข้าม

๔.๓ การปฏิบัติการไซเบอร์พิเศษ

แผนภาพที่ ๔-๒ การเชื่อมโยงการปฏิบัติการสงครามไซเบอร์ในส่วนงานต่าง ๆ



จากนโยบายและแนวปฏิบัติการปฏิบัติการสงครามไซเบอร์ ผู้วิจัยกำหนดกระบวนการปฏิบัติการสงครามไซเบอร์ เพื่อให้ส่วนงานต่าง ๆ ในการปฏิบัติสงครามไซเบอร์ได้ ๒ กลุ่มการปฏิบัติ คือ

๑. การปฏิบัติการสงครามไซเบอร์ ที่ต้องปฏิบัติภายใน (Internal Cyber Warfare Operation) ดังนี้

๑.๑ การประเมินและการตรวจสอบ (Evaluations & Audits)

๑.๒ การพิสูจน์ การตรวจสอบ และการรับรอง (Verification, Validation & Certification)

๑.๓ การทดสอบการเจาะระบบ และการค้นหาช่องโหว่ (Penetration Testing & Vulnerability Scanning)

๑.๔ การตรวจจับและป้องกันการบุกรุก (Intrusion Detection & Prevention)

๑.๕ การรักษาความปลอดภัยส่วนบุคคล การฝึกอบรม และการสร้างความตระหนัก (Personnel Security, Training & Awareness)

๑.๖ การสืบสวน (Forensics)

๑.๗ การควบคุมการเข้าถึง (Access control)

๑.๘ การกู้คืนภัยพิบัติ (Disaster Recovery)

๑.๙ การบริหารจัดการการปฏิบัติการ (Operations Management)

๑.๑๐ การเข้ารหัส (Encryption)

๑.๑๑ นโยบายและกระบวนการ (Policies & Procedures)

๒. การปฏิบัติการสงครามไซเบอร์ ที่ต้องปฏิบัติภายนอก (External Cyber Warfare Operation)

๒.๑ การโจรกรรมข้อมูล (Hacking)

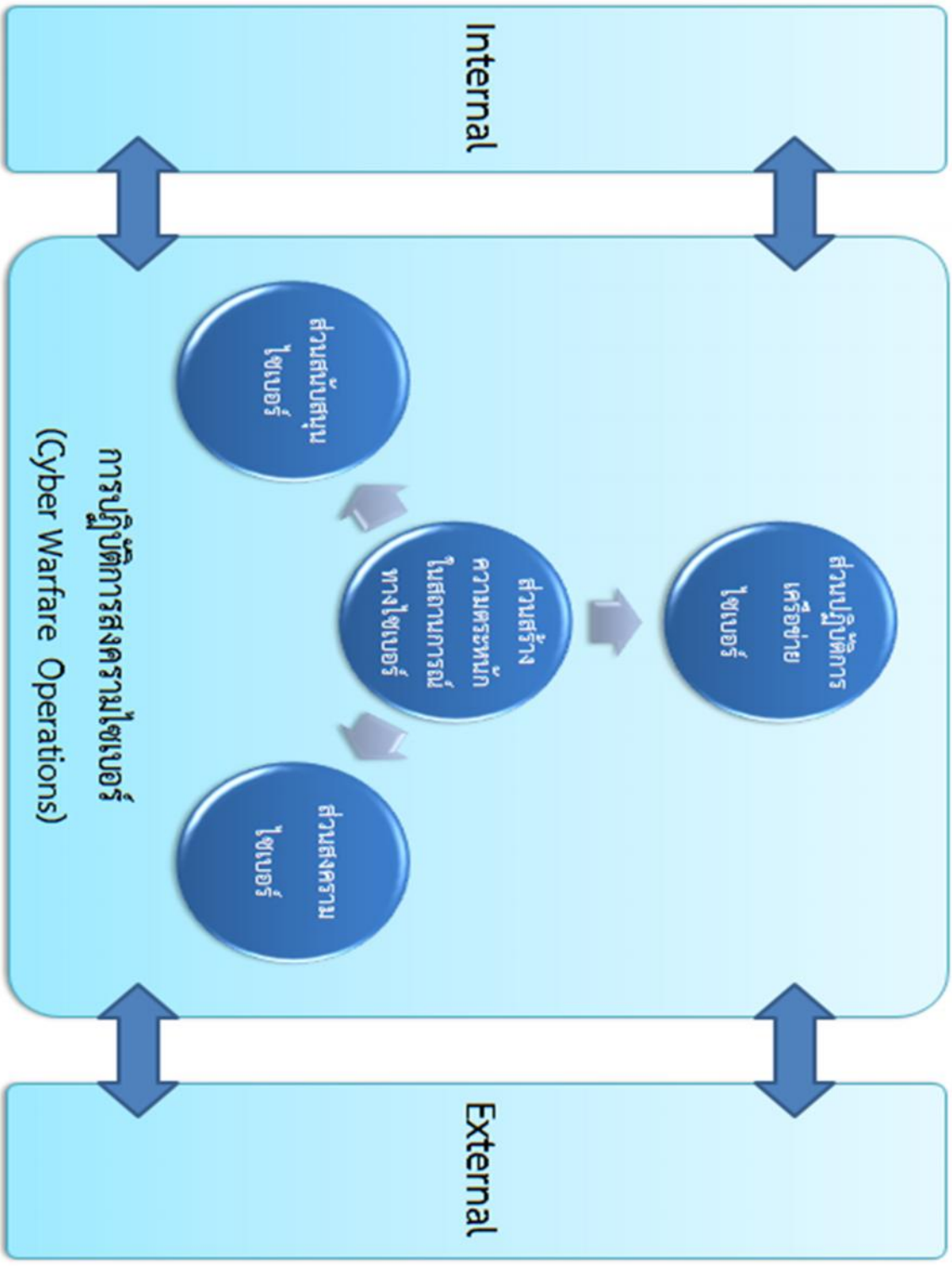
๒.๒ การแทรกการโจมตีผ่านทางช่องโหว่ (Vulnerability Injections)

๒.๓ การพัฒนา มัลแวร์ และ สปายแวร์ (Malware & Spyware Development)

๒.๔ การเฝ้าระวังเครือข่าย และข่าวกรอง (Network Surveillance & Intelligence)

๒.๕ การบริการ และการตรวจจับช่องโหว่ (Service & Vulnerability Detection)

แผนภาพที่ ๔-๓ กระบวนการปฏิบัติการสงครามไซเบอร์



รูปแบบที่เหมาะสมของปฏิบัติการสงครามไซเบอร์

รูปแบบที่เหมาะสมของการปฏิบัติการสงครามไซเบอร์ แบ่งออกตามฝ่ายต่าง ๆ ที่ปฏิบัติงานในศูนย์บัญชาการทางทหาร ได้ดังนี้

๑. ฝ่ายกำลังพล (ฝกพ.)

มีหน้าที่เกี่ยวกับการสรรหากำลังพลที่มีความสามารถในด้านการปฏิบัติการสงครามไซเบอร์ ทั้งที่เป็นข้าราชการ และจากบุคคลพลเรือน โดยการสอบคัดเลือก ซึ่งผู้สมัครต้องมีคุณสมบัติที่เหมาะสม มีความรู้สามารถในเรื่องของระบบเครือข่ายคอมพิวเตอร์ การใช้งานอุปกรณ์และโปรแกรมทั้งในด้านการโจมตี (Offensive) และการป้องกัน (Defensive) รวมถึงการพัฒนากำลังพลที่ปฏิบัติงานด้านสงครามไซเบอร์ ให้มีความรู้ความสามารถที่ทันสมัย และปฏิบัติงานได้อย่างมีประสิทธิภาพ เช่น การจัดหาทุนการศึกษาเฉพาะทางและส่งกำลังพลเข้ารับการศึกษา ทั้งภายในและภายนอกประเทศ จัดหาวิทยากรที่มีความรู้ความสามารถจากเอกชน เข้ามาอบรมให้กับกำลังพล เพื่อฝึกฝนและเรียนรู้วิธีการและเทคนิคการทำสงครามไซเบอร์แบบใหม่ ๆ เพื่อเตรียมความพร้อมให้กับกำลังพลสามารถรับมือกับสงครามไซเบอร์ที่โจมตีเข้ามา

๒. ฝ่ายการข่าว (ฝขว.)

มีหน้าที่ในการจัดทำข้อมูลทำเนียบกำลังรบทางด้านการปฏิบัติการสงครามไซเบอร์ของประเทศเพื่อนบ้าน ประกอบด้วย หน่วยงาน กำลังพล และอาวุธยุทโธปกรณ์ทางด้านไซเบอร์ เป็นต้น มีหน้าที่หาข่าวกรองการปฏิบัติการสงครามไซเบอร์ที่เกิดขึ้นในภูมิภาคต่าง ๆ ของโลก เพื่อให้ผู้บังคับบัญชา สามารถทราบข่าว และตกลงใจในการวางแนวทางการปฏิบัติสงครามไซเบอร์ของศูนย์บัญชาการทางทหารต่อไป วาดภาพสนามรบทางไซเบอร์

๓. ฝ่ายยุทธการ (ฝยก.)

มีหน้าที่กำหนดยุทธศาสตร์ และหลักนิยมการปฏิบัติการสงครามไซเบอร์ ให้กับแต่ละฝ่ายที่ปฏิบัติงานในศูนย์บัญชาการทางทหาร เพื่อจะได้มีหลักในการปฏิบัติที่เป็นไปในแนวทางเดียวกัน มีการวางแผนการปฏิบัติการสงครามไซเบอร์ ในขั้นต่าง ๆ ของแผนป้องกันประเทศ พร้อมทั้งจัดการฝึกร่วมกับเหล่าทัพต่าง ๆ ในการปฏิบัติการสงครามไซเบอร์

๔. ฝ่ายส่งกำลังบำรุง (ฝกบ.)

มีหน้าที่จัดหาความต้องการ และยุทโธปกรณ์ที่ใช้ในการปฏิบัติการสงครามไซเบอร์ ที่มีประสิทธิภาพ เพื่อสนองต่อความต้องการของฝ่ายต่าง ๆ

๕. ฝ่ายกิจการพลเรือน (ฝกร.)

มีหน้าที่ประสานงานกับหน่วยงานภาครัฐ และเอกชน ที่มีความรู้ความสามารถในการปฏิบัติงานด้านไซเบอร์ เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (MICT) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ องค์การมหาชน (ETDA) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) บริษัทผู้ให้บริการอินเทอร์เน็ต (ISP) เช่น True, TOT และ CatTelecom เป็นต้น เพื่อประสานงานเมื่อเกิดการทำสงครามทางไซเบอร์ ทั้งการขอใช้บุคลากร และอุปกรณ์ทางไซเบอร์ เพื่อช่วยในการทำสงคราม การปิดช่องทางการเชื่อมต่อเครือข่ายในระดับประเทศ ฝ่ายกิจการพลเรือนยังมีหน้าที่ในการปฏิบัติการจิตวิทยาและประชาสัมพันธ์ ให้กับประชาชนและฝ่ายตรงข้าม เมื่อเกิดเหตุการณ์ขึ้น (Information Operation, IO)

๖. ฝ่ายสื่อสาร (ฝสส.)

มีหน้าที่จัดการสื่อสาร เครื่องมือและกำลังพล เพื่อรองรับการปฏิบัติการสงครามไซเบอร์ แบ่งออกเป็น

๖.๑ การปฏิบัติการด้านการโจมตี (Offensive)

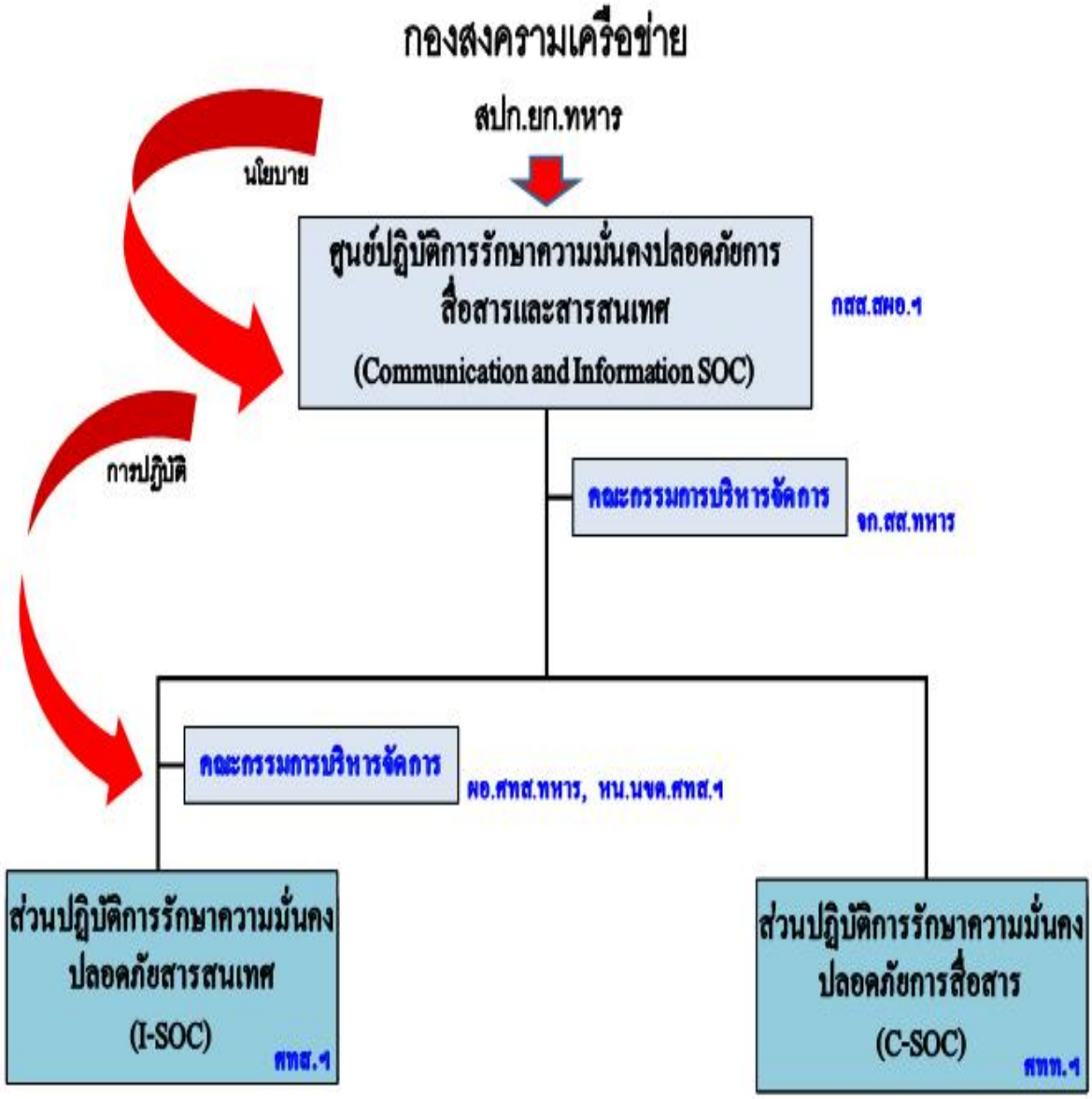
๖.๒ การปฏิบัติการด้านการป้องกัน (Defensive)

แผนภาพที่ ๔-๔ ศูนย์บัญชาการทางทหารที่เกี่ยวข้องกับการปฏิบัติการปฏิบัติการสงครามไซเบอร์

มาตรการส่งเสริมการปฏิบัติที่มีประสิทธิภาพ

๑. การปฏิบัติที่สอดคล้องกันระหว่างฝ่ายยุทธการ ที่ต้องกระทำต่อฝ่าตรงข้าม และฝ่ายสื่อสาร ที่ต้องปกป้องฝ่ายเราและสนับสนุนการปฏิบัติฝ่ายยุทธการ รวมถึงการให้กองบัญชาการกองทัพไทย สนับสนุนการปฏิบัติศูนย์บัญชาการทางทหาร

แผนภาพที่ ๔-๕ การปฏิบัติที่สอดคล้องกันระหว่างฝ่ายยุทธการและฝ่ายสื่อสาร



๒. เทคโนโลยีและยุทโธปกรณ์ที่ใช้ในการปฏิบัติการสงครามไซเบอร์ ดังนี้

๒.๑ เครื่องมือ Reconnaissance Tools ใช้ในการค้นหาข้อมูลทั่วไป เพื่อนำข้อมูลเหล่านั้นมาใช้ในการวางแผนการปฏิบัติ เช่น จากในเว็บไซต์ การตรวจสอบ Domain Name System (DNS) การค้นหาจากเครื่องมือที่ประเภท Search Engine เช่น Google และ Yahoo เป็นต้น

๒.๒ เครื่องมือ Scanning Tools เป็นเครื่องมือที่ใช้ในการค้นหาข้อมูลเกี่ยวกับสิ่งแวดล้อมของเป้าหมาย และระบบที่ใช้พร้อมรายละเอียด เช่น การเปิดใช้งาน Port ต่าง ๆ อย่างเครื่องมือ เช่น Nmap, Nessus, และ Acunetix เป็นต้น

๒.๓ เครื่องมือ Access and Escalation Tools เป็นเครื่องมือที่ใช้ในการเข้าถึง สิทธิ์การใช้งานระบบ การเพิ่มสิทธิ์การเข้าถึง เครื่องมือในการเข้าถึงรหัสผ่าน (Password Tools) เช่น Hydra, Cain & Able เป็นต้น ใช้เครื่องมือที่สามารถเจาะระบบผ่านทางช่องโหว่ที่ตรวจพบ (Metasploit)

๒.๔ เครื่องมือ Exfiltration Tools เป็นเครื่องมือที่ใช้ในการขโมยข้อมูล เช่น การขโมยผ่านทางอุปกรณ์จัดเก็บข้อมูลขนาดเล็กแต่สามารถจัดเก็บข้อมูลได้ปริมาณมาก เช่น Flash drive, Micro SD สามารถนำไปดึงข้อมูลในเครื่องคอมพิวเตอร์ของฝ่ายตรงข้าม ด้วยโปรแกรมที่ฝังตัวอยู่

๒.๕ เครื่องมือ Sustainment Tools เครื่องมือที่ใช้ในการเข้าถึงระบบ ที่มีช่องโหว่ให้สามารถกลับมาใช้งานเข้าถึงได้ในภายหลัง เช่น การเพิ่มสิทธิ์ในการเข้าถึง การทำประตูหลัง (Backdoor)

๒.๖ เครื่องมือ Assault Tools เป็นเครื่องมือที่ใช้ในการยึดเครื่องคอมพิวเตอร์ ของฝ่ายตรงข้าม เพื่อใช้เป็นเครื่องในการทำ Botnet ส่งไปโจมตีทำให้ระบบของฝ่ายตรงข้ามหยุด การให้บริการ (Denial of Service, DoS)

๒.๗ เครื่องมือ Obfuscation Tools เป็นเครื่องมือที่ใช้ในการปกปิด และลบร่องรอยการเข้ามาในระบบหรือเครือข่ายของฝ่ายตรงข้าม เช่น Location และ Log

บทที่ ๕

สรุปและข้อเสนอแนะ

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ ดำเนินการวิจัยโดยการศึกษา รวบรวมข้อมูล ที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ ในรูปแบบของคำอธิบายและแผนภาพ ทั้งจากเอกสาร รายงาน ผลการวิจัยที่เกี่ยวข้อง เพื่อให้ได้แนวทางในการพัฒนารูปแบบการปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย โดยกำหนดขอบเขตการปฏิบัติของศูนย์บัญชาการทางทหารที่เหมาะสม โดยมีวัตถุประสงค์ของการวิจัย ดังนี้

๑. ศึกษาและวิเคราะห์หลักปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งการปฏิบัติเชิงรุกและเชิงรับ สำหรับเตรียมการหรือรองรับภัยคุกคามรูปแบบใหม่ที่อาศัยเครือข่ายในการปฏิบัติ

๒. เสนอแนะแนวทางปฏิบัติการสงครามไซเบอร์ ศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย

สรุป

นโยบายและแนวปฏิบัติการปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งหลักการปฏิบัติเชิงรุก และหลักการปฏิบัติเชิงรับ จะเป็นหลักปฏิบัติในการเตรียมความพร้อมทั้งในยามปกติและยามสงคราม ที่อุบัติขึ้นในยุคเทคโนโลยีสารสนเทศ ขยายตัวครอบคลุมไปทั่วโลก และเชื่อมโยงข้อมูลข่าวสาร บุคคล และองค์กร ด้วยเครือข่ายสังคมออนไลน์ ดังนี้

๑. การปฏิบัติการสงครามไซเบอร์เชิงรุก มีวิธีปฏิบัติประกอบด้วย การหลอกลวงฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามหยุดการให้บริการทางไซเบอร์ การทำลายทางไซเบอร์ฝ่ายตรงข้าม และการเจาะระบบฝ่ายตรงข้าม ส่วนการปฏิบัติการสงครามไซเบอร์เชิงรับ มีวิธีปฏิบัติประกอบด้วย การปกป้องระบบ การทำให้ระบบสามารถระบุตัวตนผู้ใช้งานได้ การกู้คืนหรือการฟื้นคืนระบบ การค้นหาและปิดช่องโหว่ระบบ การปฏิบัติตามข้อกำหนดหรือมาตรฐานทางไซเบอร์ การบำรุงรักษาระบบ รวมถึงการปฏิบัติตามข้อกำหนดต่าง ๆ ทางกฎหมายหรือข้อบังคับทางไซเบอร์

โดยมีฝ่ายต่าง ๆ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ที่เกี่ยวข้องกับการปฏิบัติ คือ ฝ่ายกำลังพล ฝ่ายการข่าว ฝ่ายยุทธการ ฝ่ายส่งกำลังบำรุง ฝ่ายกิจการพลเรือน และฝ่ายสื่อสาร

๒. การใช้การปฏิบัติการสงครามไซเบอร์ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ฝ่ายต่าง ๆ มีหน้าที่ โดยสรุป ดังนี้

๒.๑ ฝ่ายกำลังพล มีหน้าที่เกี่ยวกับการสรรหากำลังพล พัฒนากำลังพลที่มีความสามารถในด้านการปฏิบัติการสงครามไซเบอร์ ทั้งที่เป็นข้าราชการ และจากบุคคลพลเรือน รวมถึงให้มีการฝึกฝนและเรียนรู้วิธีการและเทคนิคการทำสงครามไซเบอร์แบบใหม่ ๆ เพื่อเตรียมความพร้อม ให้กับกำลังพลสามารถรับมือกับการปฏิบัติการสงครามไซเบอร์

๒.๒ ฝ่ายการข่าว มีหน้าที่ในการจัดทำข้อมูลทำเนียบกำลังรบทางด้านการปฏิบัติการสงครามไซเบอร์ของประเทศเพื่อนบ้าน การข่าวกรองการปฏิบัติการสงครามไซเบอร์ที่เกิดขึ้น ในภูมิภาคต่าง ๆ ของโลก และวาดภาพสนามรบทางไซเบอร์

๒.๓ ฝ่ายยุทธการ มีหน้าที่กำหนดยุทธศาสตร์ และหลักนิยมการปฏิบัติการสงครามไซเบอร์ ให้กับแต่ละฝ่ายที่ปฏิบัติงานในศูนย์บัญชาการทางทหาร

๒.๔ ฝ่ายส่งกำลังบำรุง มีหน้าที่จัดหาความต้องการ และยุทโธปกรณ์ที่ใช้ในการปฏิบัติการสงครามไซเบอร์

๒.๕ ฝ่ายกิจการพลเรือน มีหน้าที่ประสานงานกับหน่วยงานภาครัฐ และเอกชนที่มีความรู้ความสามารถในการปฏิบัติงานด้านไซเบอร์ เมื่อเกิดการทำสงครามทางไซเบอร์ การปิดช่องทางการเชื่อมต่อเครือข่ายในระดับประเทศ และการปฏิบัติการจิตวิทยาและประชาสัมพันธ์ให้กับประชาชนและฝ่ายตรงข้าม

๒.๖ ฝ่ายสื่อสาร มีหน้าที่จัดการสื่อสาร เครื่องมือและกำลังพล เพื่อรองรับการปฏิบัติการสงครามไซเบอร์ การปฏิบัติการด้านการป้องกันไซเบอร์ และสนับสนุนการปฏิบัติการด้านการโจมตีทางไซเบอร์

ข้อเสนอแนะ

๑. การปฏิบัติการสงครามไซเบอร์ มีความสลับซับซ้อนทั้งในการกำหนดขอบเขตการปฏิบัติ และวิธีการปฏิบัติ การไม่สามารถกำหนดเป้าหมายการโจมตีได้ด้วยวิธีการลาดตระเวนหาข่าว หรือการสอดแนม จึงจำเป็นต้องอาศัยกำลังพลหรือบุคลากรเฉพาะทางที่มีความรู้ความสามารถทางด้านการรักษาความมั่นคงไซเบอร์ ระบบเครือข่ายคอมพิวเตอร์ และการบริหารจัดการฐานข้อมูล รวมถึงการพัฒนาโปรแกรม ประกอบกับความคิดสร้างสรรค์ การส่งเสริมความก้าวหน้า รวมถึงผลตอบแทนที่เป็นแรงจูงใจ จึงต้องกำหนดขึ้นในระดับนโยบายของหน่วยงาน และให้สามารถตอบสนองได้อย่างเป็นรูปธรรม จะเกิดประโยชน์สูงสุดต่อการเตรียมความพร้อมต่อการปฏิบัติการสงครามไซเบอร์ทั้งปัจจุบันและอนาคต

๒. การปฏิบัติการสงครามไซเบอร์จะต้องเป็นความร่วมมือกันทั้งทหาร หน่วนงานอื่นภาครัฐ พลเรือน เอกชน และสถาบันการศึกษา

๓. การจัดให้มีศูนย์ปฏิบัติการทดสอบการปฏิบัติการสงครามไซเบอร์ เพื่อให้สามารถดำเนินการได้อย่างแม่นยำตามขอบเขตของฝ่ายยุทธการกำหนด และเพื่อลดความผิดพลาดในการปฏิบัติที่อาจจะเกิดขึ้นได้เมื่อฝ่ายตรงข้ามปฏิบัติการตอบโต้

๔. การส่งเสริมงานวิจัยและพัฒนา งานตามแผนงานโครงการ ของการปฏิบัติการสงครามไซเบอร์ ระบบเครือข่ายคอมพิวเตอร์ การพัฒนาโปรแกรม สำหรับเป็นเครื่องมือในการปฏิบัติการสงครามไซเบอร์ทั้งเชิงรับและเชิงรุก ต้องได้รับการสนับสนุนอย่างจริงจัง รวมถึงต้องปรับปรุงขั้นตอนการปฏิบัติงานการวิจัยและพัฒนา งานแผนงานโครงการ ไม่ให้เกิดความยุ่งยากซับซ้อน ลดการดำเนินการทางธุรการหรือทางเอกสารให้เหมาะกับผู้ทำการวิจัยและพัฒนา รวมถึงผู้ปฏิบัติงานโครงการ

ประวัติย่อผู้วิจัย

ชื่อ นาวาเอกหญิง จินดา สระสมบูรณ์

วัน เดือน ปีเกิด ๘ พฤศจิกายน ๒๕๐๑

ประวัติการทำงาน รองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย

ผู้วิจัย นาวาเอกหญิง จินดา สระสมบูรณ์ **หลักสูตร** วปอ. **รุ่นที่** ๕๗

ตำแหน่ง รองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร

ความเป็นมาและความสำคัญของปัญหา

การเตรียมความพร้อมเพื่อปฏิบัติการสงครามไซเบอร์ พื้นที่การรบที่ ๕ เพื่อคุ้มครอง ปกป้องข้อมูลข่าวสาร บุคคล องค์กร และอธิปไตยของชาติ จึงต้องดำเนินการอย่างเร่งด่วนโดย กำหนดหลักนโยบายและแนวปฏิบัติทั้งทางยุทธศาสตร์และยุทธวิธีหรือเทคนิควิธี ที่เป็นปัจจัย สำคัญในการพัฒนาความมั่นคงปลอดภัยด้านไซเบอร์ ให้กับกองบัญชาการกองทัพไทย เนื่องจาก การดำเนินการด้านการปฏิบัติการสงครามไซเบอร์ เป็นยุทธวิธีรูปแบบใหม่ที่มีการนำมาใช้ในการ พัฒนากิจการงานด้านการทหารมีหลายประเทศชั้นนำอย่างสหรัฐ รัสเซีย และจีน ต่างใช้เป็นเครื่อ มือในการกระทำกับฝ่ายตรงข้ามเพื่อทำลายระบบต่าง ๆ ไม่ว่าจะเป็นระบบการ ควบคุมการบังคับ บัญชา โครงสร้างพื้นฐานสำคัญของประเทศ (Infrastructure) รวมถึงการได้มาซึ่งข้อมูลข่าวสาร สำคัญ (Information Critical) หรือการฝังตัวการโจมตีในรูปแบบใหม่ (Root kit) ที่ใช้หลักการเขียน ตรรกะทางโปรแกรม (Logical Programming) แทนกำลังพลและยุทโธปกรณ์ทางทหาร (Armament)

การปฏิบัติการสงครามไซเบอร์ (Cyber Warfare Operation) จึงกลายเป็นอาวุธหรือ เครื่องมือในการปฏิบัติการสงครามในทุกระดับ ตั้งแต่การดำเนินการด้านความขัดแย้งพื้นฐาน สู่การ ต่อสู้ตั้งแต่ระดับยุทธบริเวณไปจนถึงระหว่างประเทศหรือภูมิภาค มีการกระทำทั้งในทางลับและ เปิดเผย โดยบูรณการความรู้และเทคโนโลยีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) เทคโนโลยีสารสนเทศและเครือข่าย (Information and Communication Technology) วิศวกรรมอิเล็กทรอนิกส์ (Electronic Engineering) การใช้ข้อมูลตั้งแต่ระดับสัญญาณ (Signal) ตัวอักษร (Character) ข้อมูล (Data) และเนื้อหา (Content) ในสื่อสังคม (Social Media) ที่ ได้รวมอยู่ในระบบโปรแกรม (Application) รวมถึงสื่อสังคมออนไลน์ (Social Network) แต่นับว่ายังมี ข้อจำกัดกับการบูรณาการเข้ากับกิจการด้านการทหารในรูปแบบเดิม ที่กำหนดให้ต้องมีการจัด โครงสร้างหน่วย สายการบังคับบัญชา และภารกิจความรับผิดชอบอย่างชัดเจน เพื่อป้องกันความ

สับสนในการปฏิบัติ การกำหนดนโยบาย สั่งการ การเตรียมความพร้อม การฝึก และการปฏิบัติการในภาวะสงคราม ทำให้ปฏิบัติการสงครามไซเบอร์ของกองบัญชาการกองทัพไทย หรือกองทัพอื่นยังไม่มีการกำหนดความชัดเจนตั้งแต่ระดับนโยบาย สั่งการ และหลักการปฏิบัติ การวิจัยครั้งนี้ ก็เพื่อศึกษา เสนอแนะ และกำหนดความชัดเจนต่าง ๆ ดังกล่าวข้างต้น ของปฏิบัติการสงครามไซเบอร์ให้สามารถนำไปใช้ประโยชน์ได้กับกองบัญชาการกองทัพไทย

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

วัตถุประสงค์ของการวิจัย

๑. ศึกษาและวิเคราะห์หลักปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งการปฏิบัติเชิงรุกและเชิงรับ สำหรับเตรียมการหรือรองรับภัยคุกคามรูปแบบใหม่ที่อาศัยเครือข่ายในการปฏิบัติ

๒. เสนอแนะแนวทางปฏิบัติการสงครามไซเบอร์ ศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย

ขอบเขตของการวิจัย

๑. เน้นการวิจัยด้านการกำหนดรูปแบบและแนวคิดการปฏิบัติการสงครามไซเบอร์ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย

๒. การกำหนดบทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบ ความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ รวมถึงปฏิบัติการสงครามไซเบอร์ เฉพาะของกองบัญชาการกองทัพไทย

วิธีดำเนินการวิจัย

การวิจัยนี้ เป็นการวิจัยเชิงคุณภาพ ดำเนินการวิจัยโดยการศึกษา รวบรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ ในรูปแบบของคำอธิบายและแผนภาพ ทั้งจากเอกสาร รายงาน ผลการวิจัยที่เกี่ยวข้อง เพื่อให้ได้แนวทางในการพัฒนารูปแบบปฏิบัติการสงครามไซเบอร์ บทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบ ความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ รวมถึงการปฏิบัติการสงครามไซเบอร์ ที่เหมาะสมกับกองบัญชาการกองทัพไทย

ผลการวิจัย

ปฏิบัติการสงครามไซเบอร์ของศูนย์บัญชาการทางทหาร (ศบท.) กองบัญชาการกองทัพไทย ผู้วิจัยได้ดำเนิการตามขั้นตอนของการวิจัย ได้ผลการวิจัยสำหรับการปฏิบัติการสงครามไซเบอร์ ดังนี้

๑. นโยบายและแนวปฏิบัติการปฏิบัติการสงครามไซเบอร์

การปฏิบัติสงครามไซเบอร์ 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

๑.๑ การปฏิบัติการสงครามไซเบอร์เชิงรุก มีวิธีปฏิบัติประกอบด้วย การหลอกลวงฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามหยุดการให้บริการทางไซเบอร์ การทำลายทางไซเบอร์ฝ่ายตรงข้าม และการเจาะระบบฝ่ายตรงข้าม

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

๒. กระบวนการปฏิบัติการสงครามไซเบอร์ สำหรับการปฏิบัติภายในและภายนอก ดังนี้

๒.๑ การปฏิบัติการสงครามไซเบอร์ ที่ต้องปฏิบัติภายใน (Internal Cyber Warfare Operation) ประกอบด้วย การประเมินและการตรวจสอบ (Evaluations & Audits) การพิสูจน์ การ

ตรวจสอบ และการรับรอง (Verification, Validation & Certification) การทดสอบการเจาะระบบและการค้นหาช่องโหว่ (Penetration Testing & Vulnerability Scanning) การตรวจจับและป้องกันการบุกรุก (Intrusion Detection & Prevention) การรักษาความปลอดภัยส่วนบุคคล การฝึกอบรมและการสร้างความตระหนัก (Personnel Security, Training & Awareness) การสืบสวน (Forensics) การควบคุมการเข้าถึง (Access control) การกู้คืนภัยพิบัติ (Disaster Recovery) การบริหารจัดการการปฏิบัติการ (Operations Management) การเข้ารหัส (Encryption) และนโยบายและกระบวนการ (Policies & Procedures)

๒.๒ การปฏิบัติการสงครามไซเบอร์ ที่ต้องปฏิบัติภายนอก (External Cyber Warfare Operation) ประกอบด้วย การโจรกรรมข้อมูล (Hacking) การแทรกการโจมตีผ่านทางช่องโหว่ (Vulnerability Injections) การพัฒนา มัลแวร์ และ สปายแวร์ (Malware & Spyware Development) การเฝ้าระวังเครือข่าย และข่าวกรอง (Network Surveillance & Intelligence) และการบริการ และการตรวจจับช่องโหว่ (Service & Vulnerability Detection)

๓. รูปแบบที่เหมาะสมของปฏิบัติการสงครามไซเบอร์ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ฝ่ายต่าง ๆ มีหน้าที่ โดยสรุป ดังนี้

๓.๑ ฝ่ายกำลังพล มีหน้าที่เกี่ยวกับการสรรหากำลังพล พัฒนากำลังพล ที่มีความสามารถในด้านการปฏิบัติการสงครามไซเบอร์ ทั้งที่เป็นข้าราชการ และจากบุคคลพลเรือน รวมถึงให้มีการฝึกฝนและเรียนรู้วิธีการและเทคนิคการทำสงครามไซเบอร์แบบใหม่ ๆ เพื่อเตรียมความพร้อมให้กับกำลังพลสามารถรับมือกับการปฏิบัติการสงครามไซเบอร์

๓.๒ ฝ่ายการข่าว มีหน้าที่ในการจัดทำข้อมูลทำเนียบกำลังรบทางด้านการปฏิบัติการสงครามไซเบอร์ของประเทศเพื่อนบ้าน การข่าวกรองการปฏิบัติการสงครามไซเบอร์ที่เกิดขึ้นในภูมิภาคต่าง ๆ ของโลก และวาดภาพสนามรบทางไซเบอร์

๓.๓ ฝ่ายยุทธการ มีหน้าที่กำหนดยุทธศาสตร์ และหลักนิยมการปฏิบัติการสงครามไซเบอร์ ให้กับแต่ละฝ่ายที่ปฏิบัติงานในศูนย์บัญชาการทางทหาร

๓.๔ ฝ่ายส่งกำลังบำรุง มีหน้าที่จัดหาความต้องการ และยุทโธปกรณ์ที่ใช้ในการปฏิบัติการสงครามไซเบอร์

๓.๕ ฝ่ายกิจการพลเรือน มีหน้าที่ประสานงานกับหน่วยงานภาครัฐ และเอกชน ที่มีความรู้ความสามารถในการปฏิบัติงานด้านไซเบอร์ เมื่อเกิดการทำสงครามทางไซเบอร์ การปิดช่องทางการเชื่อมต่อเครือข่ายในระดับประเทศ และการปฏิบัติการจิตวิทยาและประชาสัมพันธ์ให้กับประชาชนและฝ่ายตรงข้าม

๓.๖ ฝ่ายสื่อสาร มีหน้าที่จัดการสื่อสาร เครื่องมือและกำลังพล เพื่อรองรับการปฏิบัติการสงครามไซเบอร์ การปฏิบัติการด้านการป้องกันไซเบอร์ และสนับสนุนการปฏิบัติการด้านการโจมตีทางไซเบอร์

๔. มาตรการส่งเสริมการปฏิบัติที่มีประสิทธิภาพ

๔.๑ การปฏิบัติที่สอดคล้องกันระหว่างฝ่ายฝ่ายยุทธการ ที่ต้องกระทำต่อฝ่ายตรงข้าม และฝ่ายสื่อสาร ที่ต้องปกป้องฝ่ายเราและสนับสนุนการปฏิบัติฝ่ายยุทธการ รวมถึงการให้กองบัญชาการกองทัพไทย สนับสนุนการปฏิบัติศูนย์บัญชาการทางทหาร

๔.๒ เทคโนโลยีและยุทโธปกรณ์ที่ใช้ในการปฏิบัติการสงครามไซเบอร์ที่ ต้องมีอย่างเหมาะสมสำหรับการปฏิบัติการ

ข้อเสนอแนะ

๑. การปฏิบัติการสงครามไซเบอร์ มีความสลับซับซ้อนทั้งในการกำหนดขอบเขตการปฏิบัติ และวิธีการปฏิบัติ การไม่สามารถกำหนดเป้าหมายการโจมตีได้ด้วยวิธีการลาดตระเวนหาข่าว หรือการสอดแนม จึงจำเป็นต้องอาศัยกำลังพลหรือบุคลากรเฉพาะทางที่มีความรู้ความสามารถทางด้านการรักษาความมั่นคงไซเบอร์ ระบบเครือข่ายคอมพิวเตอร์ และการบริหารจัดการฐานข้อมูล รวมถึงการพัฒนาโปรแกรม ประกอบกับความคิดสร้างสรรค์ การส่งเสริมความก้าวหน้า รวมถึงผลตอบแทนที่เป็นแรงจูงใจ จึงต้องกำหนดขึ้นในระดับนโยบายของหน่วยงาน และให้สามารถตอบสนองได้อย่างเป็นรูปธรรม จะเกิดประโยชน์สูงสุดต่อการเตรียมความพร้อมต่อการปฏิบัติการสงครามไซเบอร์ทั้งปัจจุบันและอนาคต

๒. การปฏิบัติการสงครามไซเบอร์จะต้องเป็นความร่วมมือกันทั้งทหาร หน่วนงานอื่นภาครัฐ พลเรือน เอกชน และสถาบันการศึกษา

๓. การจัดให้มีศูนย์ปฏิบัติการทดสอบการปฏิบัติการสงครามไซเบอร์ เพื่อให้สามารถดำเนินการได้อย่างแม่นยำตามขอบเขตของฝ่ายยุทธการกำหนด และเพื่อลดความผิดพลาดในการปฏิบัติที่อาจจะเกิดขึ้นได้เมื่อฝ่ายตรงข้ามปฏิบัติการตอบโต้

๔. การส่งเสริมงานวิจัยและพัฒนา งานตามแผนงานโครงการ ของการปฏิบัติการสงครามไซเบอร์ ระบบเครือข่ายคอมพิวเตอร์ การพัฒนาโปรแกรม สำหรับเป็นเครื่องมือในการปฏิบัติการสงครามไซเบอร์ทั้งเชิงรับและเชิงรุก ต้องได้รับการสนับสนุนอย่างจริงจัง รวมถึงต้องปรับปรุงขั้นตอนการปฏิบัติงานการวิจัยและพัฒนา งานแผนงานโครงการไม่ให้เกิดความยุ่งยากซับซ้อน ลดการดำเนินการทางธุรการหรือทางเอกสารให้เหมาะกับผู้ทำการวิจัยและพัฒนา รวมถึงผู้ปฏิบัติงานโครงการ