แนวทางในการบริหารจัดการเครือข่ายของกองทัพบก

ความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร ที่นำมาใช้ในการดำเนินชีวิตประจำวัน มีผลต่อการเปลี่ยนแปลงโลกด้านความเป็นอยู่ สังคม เศรษฐกิจ การศึกษา การแพทย์ เกษตรกรรม อุตสาหกรรม การเมือง ตลอดจนการวิจัยและการพัฒนาต่าง ๆ โดยเฉพาะการต่อเชื่อมกับระบบอินเทอร์เน็ตกำลังมีอัตราเพิ่มขึ้นอย่างต่อเนื่อง ทุกองค์กรต้องมีความจำเป็นติดต่อสื่อสารกับองค์กรทั่วประเทศและทั่วโลก บางองค์กรระบบอินเทอร์เน็ตใช้งานไม่ได้เพียงไม่กี่ชั่วโมงก็ทำให้เกิดความเสียหายกับธุรกิจขององค์กรนั้นอย่างเห็นได้ชัด หลายองค์กรหันมาใช้เทคโนโลยี “e-Commerce” ทำธุรกิจกรรมอิเล็กทรอนิกส์เช่น การให้บริการของธนาคารผ่านทางอินเทอร์เน็ต (ระบบ Internet Banking), ระบบ GFMIS ของรัฐบาล หรือ ระบบการชำระภาษีผ่านทางอินเทอร์เน็ตของกรมสรรพากร,การสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare) เป็นการเปลี่ยนแปลงสู่ยุคของข้อมูลข่าวสาร เพราะความเชื่อที่ว่า หากฝ่ายเรามีข้อมูลข่าวสารที่เหนือกว่าข้าศึก (Information Superiority) จะทำให้เกิด ความตระหนักรู้ในสถานการณ์ (Situation Awareness) ร่วมกันในทุกระดับ ทั้งระดับยุทธศาสตร์ ระดับยุทธการ และระดับยุทธวิธี ทำให้การตัดสินตกลงใจจากส่วนบัญชาการและควบคุมที่สั่งการไปยังหน่วยรบเป็นไปด้วยความถูกต้อง รวดเร็ว และแม่นยำ ก่อให้ความได้เปรียบเหนือข้าศึกมากมายมหาศาล ซึ่งเป็นปัจจัยที่สำคัญที่นำไปสู่ชัยชนะในการทำสงคราม จะเห็นได้ว่าความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร ส่งผลต่อการดำเนินชีวิตและการทำงานในระดับบุคคล จนถึงระดับประเทศ ซึ่งล้วนให้ความสำคัญและนำเทคโนโลยีมาประยุกต์ให้เกิดประโยชน์สูงสุดกับพลังอำนาจของชาติ รวมทั้งสร้างองค์ความรู้ใหม่ในการสร้างพลังอำนาจทางไซเบอร์ในทุกมิติ ทั้งด้านการเมือง เศรษฐกิจ สังคม วิทยาศาสตร์ เทคโนโลยี และการทหาร ส่งผลให้โลกของเราเข้าสู่ยุคโลกเสมือนที่ไร้พรหมแดนในมิติไซเบอร์

ทุกสรรพสิ่งในโลก ยิ่งมีคุณอนันต์ก็จะยิ่งมีโทษมหันต์ ฉันใด ความเจริญก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารยิ่งมีการเจริญก้าวหน้าและมีประโยชน์มากขึ้นเท่าใด

ยิ่งมีโทษติดตามมามากขึ้นเท่านั้น คงไม่มีใครปฏิเสธถึงคุณประโยชน์ของเทคโนโลยีสารสนเทศและการสื่อสาร ส่วนโทษที่เกิดจากเทคโนโลยีสารสนเทศและการสื่อสารโดยตรงแทบมองไม่เห็น แต่ผลที่เกิดจากการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้งานไม่ถูกต้อง หรือนำมาใช้เพื่อผลในทางมิชอบ รวมถึงการนำมาใช้เป็นเครื่องมือทางการทหารนับเป็นภัยที่ใหญ่หลวง ที่กำลังคุกคามความมั่นคงด้านต่างๆ บนไซเบอร์

กองทัพบกเป็นอีกหน่วยงานหนึ่งที่ให้ความสำคัญต่อการนำเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้งานอย่างต่อเนื่อง และได้เริ่มตระหนักถึงภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงขึ้นตามลำดับ จึงได้จัดตั้งหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในการเตรียมความพร้อมรับมือกับภัยคุกคามไซเบอร์ โดยแปรสภาพจากศูนย์เทคโนโลยีทางทหาร ซึ่งเป็นหน่วยขึ้นตรง กรมการทหารสื่อสาร เป็น ศูนย์ไซเบอร์กองทัพบก มีฐานะเป็นหน่วยขึ้นตรงกองทัพบก ในวันที่ 1 ต.ค.59 โดยกรมการทหารสื่อสารเป็นหน่วยปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

กองทัพไทยและกองทัพบกมียุทธศาสตร์เพื่อมุ่งไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations:NCO) และการปฏิบัติการด้านไซเบอร์(Cyber Operations) จึงจำเป็นที่ต้องมีการบริหารจัดการเครือข่ายกองทัพบก เพื่อให้หน่วยงานในกองทัพบกดำเนินการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง(Network Centric Operations:NCO) และการปฏิบัติการด้านไซเบอร์(Cyber Operations) ได้อย่างมีประสิทธิภาพ

ยุทธศาสตร์ของกองทัพไทยและกองทัพบก เพื่อมุ่งไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations:NCO) และการปฏิบัติการด้านไซเบอร์(Cyber Operations) มีดังนี้

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทยและกองบัญชาการกองทัพไทย พ.ศ.2557-2561

ใช้เป็นกรอบและแนวทางในการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพไทย ในส่วนของฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล รวมถึงบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร และเพื่อให้ผู้บริหารระดับสูงและผู้ที่เกี่ยวข้อง ได้ทราบถึงเป้าหมายของโครงการ แผนงานสำหรับการพัฒนาเทคโนโลยีสารสนเทศและสื่อสารกองทัพไทย ประกอบด้วยยุทธศาสตร์ 4 ด้าน ดังนี้

ยุทธศาสตร์ที่ 1 การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารให้มีความมั่นคง ปลอดภัย และมีประสิทธิภาพ

กลยุทธ์/มาตรการ

1.ปรับปรุงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารความเร็วสูง (Broadband) ที่เหมาะสม คุ้มค่า เพื่อให้เชื่อมโยงไปยังส่วนราชการของกองบัญชาการของกองทัพไทย และส่วนราชการที่เกี่ยวข้องทั้งในส่วนกลางและส่วนภูมิภาค

2.จัดตั้งหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันและรับมือภัยทางไซเบอร์อย่างมีประสิทธิภาพ

3.ปรับปรุง/พัฒนาขีดความสามารถโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารเพื่อเตรียมการรองรับสถานการณ์ฉุกเฉินอันเกิดจากการโจมตีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4.สนับสนุนการบูรณาการระบบศูนย์เตือนภัยพิบัติแห่งชาติเพื่อเตรียมความพร้อมสู่อาเซียน

5.ปรับปรุง พัฒนา ระเบียบ ข้อบังคับ ให้สอดคล้องกับการใช้เทคโนโลยีสารสนเทศและการสื่อสาร

ยุทธศาสตร์ที่ 2 พัฒนาระบบเทคโนโลยีสารสนเทศ เพื่อการบูรณาการข้อมูลร่วมกันอย่างมีประสิทธิภาพ

กลยุทธ์/มาตรการ

พัฒนา/ปรับปรุงระบบสารสนเทศ เพื่อสนับสนุนการปฏิบัติงานของหน่วยสนับสนุนการบูรณาการข้อมูลร่วมกันระหว่างกองทัพไทย กับ เหล่าทัพ และส่วนราชการที่เกี่ยวข้อง

รวมทั้งสนับสนุนการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับหน่วยงานภาครัฐ ตามกรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ หรือ TH e-GIF เช่น การบริหารจัดการภัยพิบัติร่วม

ยุทธศาสตร์ที่ 3 พัฒนาระบบเทคโนโลยีสารสนเทศ สนับสนุนการอำนวยการ การใช้กำลังกองทัพและการยุทธร่วมอย่างมีประสิทธิภาพ

กลยุทธ์/มาตรการ

พัฒนาระบบควบคุมและอำนวยการยุทธร่วม

ยุทธศาสตร์ที่ 4 พัฒนาและส่งเสริมการเรียนรู้ของกำลังพลเพื่อมุ่งไปสู่การพึ่งพาตนเอง

กลยุทธ์/มาตรการ

พัฒนากำลังพลด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานวิชาชีพในระดับสากล เพื่อให้กำลังพลมีขีดความสามารถในการพัฒนาระบบสารสนเทศฯ และหรือพร้อมรับการถ่ายทอดเทคโนโลยีที่ใช้ในการพัฒนาระบบสารสนเทศที่เกิดจากการจ้างพัฒนา เพื่อสนับสนุนการพึ่งพาตนเองด้านเทคโนโลยีสารสนเทศและการสื่อสาร[1]

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารกองทัพบก พ.ศ.2559-2561

ใช้เป็นกรอบและแนวทางในการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพบก ในส่วนของฮาร์ดแวร์ ซอฟแวร์ ระบบเครือข่าย ฐานข้อมูล บุคลากร การรักษาความมั่นคงปลอดภัย การบริหารจัดการ และการบูรณาการระหว่างหน่วยราชการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วย 4 ยุทธศาสตร์ ดังนี้

ยุทธศาสตร์ที่ 1 พัฒนาและบูรณาการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพ

กลยุทธ์/มาตรการ

1.ปรับปรุงโครงสร้างด้านการบริหารจัดการและการปฏิบัติด้านเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพบกให้มีเอกภาพและมีประสิทธิภาพ

2.ปรับปรุงและพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลที่เหมาะสม คุ้มค่า สอดคล้องกับการเปลี่ยนผ่านด้านเทคโนโลยีและการเปลี่ยนผ่านระบบ

อินเทอร์เน็ตโปรโตคอลไปสู่ ยุคที่ 6 (Internet Protocol Version 6 : IPV 6) เพื่อเชื่อมโยงระหว่างหน่วยงานภายในกองทัพบก เหล่าทัพ กองบัญชาการกองทัพไทย กระทรวงกลาโหม และส่วนราชการอื่นที่เกี่ยวข้อง

3.สถาปนาหน่วยปฏิบัติงานด้านไซเบอร์เพื่อป้องกันและรับมือกับภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ

4.ปรับปรุงและพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีความยืดหยุ่น (Resilience) รวมถึงขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยจากภัยคุกคามด้านไซเบอร์ และสถานการณ์ฉุกเฉินอันเกิดจากภัยพิบัติ

5.ปรับปรุงความทันสมัย พัฒนา กฎ ระเบียบ ข้อบังคับ ให้สอดคล้องกับระเบียบ กฎหมาย ภัยคุกคาม รวมถึง การใช้เทคโนโลยีสารสนเทศและการสื่อสาร

ยุทธศาสตร์ที่ 2 พัฒนาระบบเทคโนโลยีสารสนเทศเพื่อบูรณาการข้อมูลร่วมกันอย่างมีประสิทธิภาพ

กลยุทธ์/มาตรการ

1.ปรับปรุง พัฒนา และปรนนิบัติบำรุงระบบสารสนเทศสายงานกำลังพล สายงานข่าว สายงานยุทธการ สายงานส่งกำลังบำรุง สายงานกิจการพลเรือน และสายงานปลัดบัญชีเพื่อสนับสนุนการปฏิบัติงานของหน่วยราชการในกองทัพบกและศูนย์ปฏิบัติการกองทัพบกได้อย่างต่อเนื่อง

2.พัฒนาโปรแกรมประยุกต์ (Application) สำหรับให้บริการประชาชน ตามกรอบยุทธศาสตร์การบูรณาการรัฐบาลอิเล็กทรอนิกส์(e-Government)

3.ปรับปรุง พัฒนาและปรนนิบัติบำรุงระบบภูมิสารสนเทศ(GIS) กองทัพบก ให้สามารถรองรับการใช้งานสนับนุนภารกิจหน่วยราชการในระดับต่างๆ ของกองทัพบก

4.ปรับปรุงและพัฒนาระบบบูรณาการข้อมูลร่วมกันระหว่างหน่วยในกองทัพบก และส่วนราชการอื่นที่เกี่ยวข้อง รวมทั้งสนับสนุนการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับหน่าวยงานภาครัฐ ตามกรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ หรือ Th e-GIF

ยุทธศาสตร์ที่ 3 พัฒนาและบูรณาการระบบเทคโนโลยีสารสนเทศสนับสนุนการอำนวยการและการใช้กำลังทางทหารอย่างมีประสิทธิภาพ

กลยุทธ์/มาตรการ

1.ปรับปรุงและพัฒนาระบบควบคุมบังคับบัญชา (C^4I) กองทัพบก ไปสู่ระบบควบคุม

บังคับบัญชา (C^4ISR) กองทัพบก ตามแผนที่แนวทางการบูรณาการระบบควบคุมบังคับบัญชาของกองทัพไทย

2.ปรับปรุงและพัฒนาระบบฐานข้อมูลสารสนเทศด้านการข่าว ได้แก่ ข้อมูลข่าวกรองภูมิสารสนเทศ(GEOINT) ข้อมูลข่าวกรองทางกายภาพ(IMINT) และข้อมูลข่าวกรองจากแหล่งข่าวเปิด(OSINT) รวมถึง การบูรณาการระบบงานและข้อมูลข่างกรองภายในกระทรวงกลาโหมกับหน่วยงานในประชาคมข่าวกรอง

3.พัฒนาระบบจำลองยุทธ์ของกองทัพบก ที่มีความสอดคล้องรองรับการพัฒนาระบบจำลองยุทธ์ร่วมของกองทัพไทย

4.พัฒนาระบจำลองยุทธ์ทางไซเบอร์(Cyber Range) ของกองทัพบก ที่สามารถบูรณาการใช้งานร่วมกับระบบจำลองยุทธ์ทางไซเบอร์ของกองบัญชาการกองทัพไทยได้อย่างประสานสอดคล้อง คุ้มค่า และเกิดประสิทธิภาพสูงสุด

ยุทธศาสตร์ที่ 4 พัฒนาและส่งเสริมการเรียนรู้ของกำลังพลเพื่อมุ่งไปสู่การพึ่งพาตนเอง

กลยุทธ์/มาตรการ

1.พัฒนากำลังพลด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงการปฏิบัติด้านไซเบอร์ให้เป็นไปตามมาตรฐานวิชาชีพในระดับสากล เพื่อให้กำลังพลมีขีดความสามารถในการพัฒนาระบบสารสนเทศและการสื่อสาร และพร้อมรับการถ่ายทอดเทคโนโลยีที่ใช้ในการพัฒนาระบบที่เกิดจากการจ้างพัฒนา เพื่อการพึ่งพาตนเองด้านเทคโนโลยีสารสนเทศและการสื่อสาร

2.ปรับปรุง พัฒนาหลักสูตรและการจัดการฝึกอบรมเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง การปฏิบัติด้านไซเบอร์ รวมถึงการจำลองยุทธ์ของกองทัพบก เพื่อเสริมสร้างความตระหนักรู้ ความเข้าใจ รวมถึงทักษะการใช้งานได้อย่างถูกวิธีและมีประสิทธิภาพ

3.พัฒนาการจัดการองค์ความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการปฏิบัติงาน เพื่อให้กำลังพลเข้าถึงและเรียนรู้ผ่านเครือข่ายคอมพิวเตอร์และหรือเครือข่ายโทรคมนาคมทหาร เพื่อใช้ในการปฏิบัติงาน รวมทั้งเพิ่มขีดความสามารถของตนเองและหน่วยให้สามารถทำการปรนนิบัติบำรุง ดูแล รักษายุทโธปกรณ์ เครื่องมือระบบเทคโนโลยีสารสนเทศและการสื่อสารได้ด้วยตนเองในอนาคต[2]

แผนแม่บทไซเบอร์ กองทัพบก พ.ศ.2560-2564

ใช้เป็นกรอบแนวทางในการเตรียมกำลัง และการใช้กำลังด้านไซเบอร์ในระยะ 5 ปี ทั้งในด้านการจัดหน่วยรับผิดชอบงานด้านไซเบอร์ การเสริมสร้างความพร้อมด้านไซเบอร์ ความต่อเนื่องด้านไซเบอร์และการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพบกทั้งต่อภัยคุกคามทางทหาร(Conventional Theats) ภัยคุมคามที่ไม่ใช่ทหารและภัยคุกคามรูปแบบอื่นๆ(Non-conventional Theats) ประกอบด้วยประเด็นยุทธศาสตร์ 3 ด้าน ดังนี้

ยุทธศาสตร์ที่ 1 การป้องกันเชิงรุกสำหรับการปฏิบัติการในมิติไซเบอร์ของกองทัพไทย มุ่งเน้นไปที่การปฏิบัติการเชิงรุกในลักษณะจำกัดและการโต้ตอบอย่างรวดเร็ว กรณีถูกโจมตีทางไซเบอร์

ยุทธศาสตร์ที่ 2 ผนึกกำลังป้องกันประเทศสำหรับการปฏิบัติการในมิติไซเบอร์ของกองทัพไทย เป็นการสร้างความร่วมมือและบูรณาการขีดความสามารถในการปฏิบัติการในมิติไซเบอร์ในทุกภาคส่วนภายในประเทศเข้าด้วยกันอย่างเป็นระบบ

ยุทธศาสตร์ที่ 3 สร้างความร่วมมือด้านความมั่นคงสำหรับการปฏิบัติการในมิติไซเบอร์ของกองทัพไทย กับประเทศเพื่อนบ้าน ประเทศสมาชิกอาเซียนและมิตรประเทศ ทั้งในระดับภูมิภาคและในระดับโลก

การแบ่งมอบหน้าที่และความรับผิดชอบ

1.กรมการทหารสื่อสาร มีหน้าที่และความรับผิดชอบในการติดตั้งปรนนิบัติบำรุงบริหารจัดการบริการ และกำกับดูแลการใช้งานโครงสร้างพื้นฐานภายในกองทัพบก ทั้งนี้รวมถึงคอมพิวเตอร์และอุปกรณ์ประกอบทุกประเภทที่ใช้งานเชื่อมต่อกับโครงสร้างพื้นฐาน สำหรับการพัฒนาและการใช้งานโปรแกรมประยุกต์บนโครงสร้างพื้นฐานดังกล่าวให้กรมการทหารสื่อสารเป็นหน่วยรับผิดชอบในการกำหนดมาตรฐานการให้คำแนะนำและกำกับดูแลการปฏิบัติของหน่วยต่างๆในกองทัพบก ให้เป็นไปในทิศทางเดียวกัน ตามนโยบายของกองทัพบก

2.ศูนย์ไซเบอร์กองทัพบก มีหน้าที่และความรับผิดชอบในการกำหนดมาตรฐาน ประสานงานและกำกับดูแลรักษาความมั่นคงปลอดภัยระบบสารสนเทศภายในกองทัพบกทุกประเภทรวมทั้งเป็นหน่วยปฏิบัติในการรวบรวมข้อมูลเฝ้าระวังตรวจสอบช่องโหว่ วิเคราะห์

และแจ้งเตือนภัยคุกคามทางไซเบอร์ พร้อมทั้งให้คำแนะนำแก้ไข และฟื้นฟูระบบเมื่อได้รับการร้องขอ

3.หน่วยต่างๆในกองทัพบก มีหน้าที่และความรับผิดชอบในฐานะ ผู้ใช้งานโครงสร้างพื้นฐานระบบสารสนเทศกองทัพบก และ/หรือ เป็นผู้รับผิดชอบในการพัฒนา ติดตั้ง ปรนนิบัติบำรุง กำกับดูแล บริหารจัดการ บริการ และรักษาความมั่นคงปลอดภัยระบบสารสนเทศในความรับผิดชอบของหน่วย ทั้งนี้หน่วยต้องกำหนดเจ้าหน้าที่ผู้รับผิดชอบระบบสารสนเทศประจำหน่วย/พื้นที่รับผิดชอบ โดยปฏิบัติตามวัตถุประสงค์และแนวทางการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบกในส่วนที่เกี่ยวข้องอย่างเคร่งครัด ภายใต้การกำกับดูแลของกรมการทหารสื่อสารและศูนย์ไซเบอร์ของกองทัพบก[3]

การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง(Network Centric Operations:NCO) และการปฏิบัติการด้านไซเบอร์(Cyber Operations) จำเป็นที่ต้องมีการบริหารจัดการเครือข่ายให้มีความชัดเจนในการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง(Network Centric Operations:NCO) และการปฏิบัติการด้านไซเบอร์(Cyber Operations) เพื่อให้เกิดประสิทธิภาพสูงสุด ลดความซับซ้อน และมีมาตรฐานเดียวกันทั้งกองทัพบก

ในปัจจุบันพบว่า การบริหารจัดการเครือข่ายของกองทัพบกยังไม่ได้กำหนดรูปแบบที่ชัดเจน กำหนดเฉพาะรูปแบบการจัดการเครือข่ายในภายในกองบัญชาการกองทัพบกเท่านั้น ซึ่งการจัดการเครือข่ายในกองบัญชาการกองทัพบก กรมการทหารสื่อสารเป็นผู้ให้บริการเครือข่าย ส่วนสนับสนุน กองบัญชาการกองทัพบกเป็นผู้วางระบบเครือข่ายให้กับหน่วยต่างๆ ในกองบัญชาการกองทัพบกประกอบด้วย สำนักงานผู้บังคับบัญชาชั้นสูง กรมยุทธการทหารบก กรมข่าวทหารบก กรมกำลังพลทหารบก กรมส่งกำลังบำรุงทหารบก กรมกิจการพลเรือนทหารบก ศูนย์ปฏิบัติการกองทัพบก หน่วยตรวจโรคที่ 1 ห้องสมุด สำนักงานที่ปรึกษากองทัพบก ศูนย์ไซเบอร์กองทัพบก กรมสารบรรณทหารบก สำนักงานเลขานุการกองทัพบก กรมการเงินทหารบก สำหรับการกำหนดบัญชีผู้ใช้ หน่วยในกองบัญชาการกองทัพบกเป็นผู้กำหนด และส่งรายชื่อให้ศูนย์ไซเบอร์กองทัพบก เพื่อใช้ในการรักษาความปลอดภัยเครือข่าย

จากปัญหาที่พบเกิดจากการที่หน่วยที่เกี่ยวข้องกับเครือข่าย ประกอบด้วย ผู้ให้บริการเครือข่าย ผู้รับบริการเครือข่าย และผู้รักษาความปลอดภัยเครือข่าย ยังไม่ทราบขอบเขตของตนในการบริหารจัดการเครือข่าย และไม่ทราบถึงหน้าที่ของหน่วย ทำให้การบริการจัดการเครือข่ายมีความซ้ำซ้อนกัน ทำให้การปฏิบัติการด้านเครือข่าย และการปฏิบัติงานด้านไซเบอร์ไม่มีประสิทธิภาพ

เพื่อให้การบริหารจัดการเครือข่ายมีประสิทธิภาพ จึงต้องกำหนดขอบเขตของหน่วยที่เกี่ยวข้องกับเครือข่ายประกอบด้วย ผู้ให้บริการเครือข่าย ผู้รับบริการเครือข่าย และผู้รักษาความปลอดภัยเครือข่าย และกำหนดแนวทางในการบริหารจัดการเครือข่ายของกองทัพบก โดยได้ศึกษา แนวคิด ทฤษฎี และแนวทางในการบริหารจัดการเครือข่ายขององค์กรหน่วยงานต่างๆ แล้ว มีแนวทางในการบริหารจัดการเครือข่าย ดังนี้

มาตรฐานการสื่อสารข้อมูล

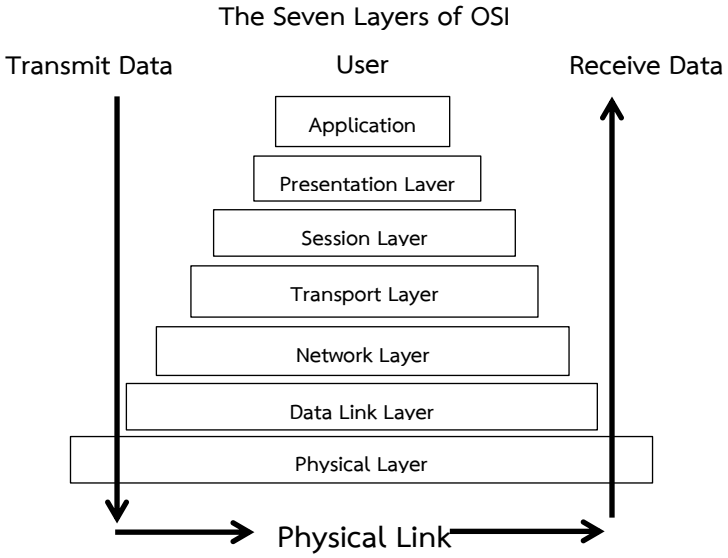
OSI Model คือ องค์ประกอบ ที่สามารถพัฒนาขึ้นมาเพียงชั้นเดียวจากจำนวน 7 ชั้นแล้วนำไปใช้งานร่วมกับชั้นอื่นที่มีการพัฒนาไว้แล้วโดยหลักการแต่ละชั้นจะติดต่อกับชั้นในระดับเดียวกันที่อยู่บนเครื่องอีกเครื่องหนึ่ง

Open Systems Interconnection (OSI)

จัดตั้งและกำหนดโดย องค์การกำหนดมาตรฐานสากล หรือ ISO (International Standards Organization) เริ่มนำมาใช้งานราว ๆ กลางปี ค.ศ. 1970 และใช้อ้างอิงมาจนถึงปัจจุบัน จุดมุ่งหมายเพื่อเปิดช่องทางให้ข้อมูลที่เก็บอยู่ในระบบคอมพิวเตอร์หนึ่ง ๆ รับส่งไปยังคอมพิวเตอร์ที่เป็นระบบเดียวกันหรือต่างระบบได้โดยอิสระ ไม่ขึ้นกับผู้ผลิตสร้างการทำงานที่เป็นระบบเปิด (Open System)

แนวคิดของการกำหนดมาตรฐานเป็นแบบชั้นสื่อสาร (layers) คือ

1.ชั้นสื่อสารแต่ละชั้นถูกกำหนดขึ้นมาตามบทบาทที่แตกต่างกัน
2.แต่ละชั้นสื่อสารจะต้องทำหน้าที่ตามที่ได้รับมอบหมายอย่างดียิ่ง
3.แต่ละฟังก์ชั่นในชั้นสื่อสารใดๆจะต้องกำหนดขึ้นมาโดยใช้แนวความคิดใน ระดับสากล เป็นวัตถุประสงค์หลัก[4]



รูปที่ 1 โครงสร้างการสื่อสารข้อมูลใน OSI Model[5]

OSI Model ประกอบด้วยการทำงาน 7 Layer แต่ละ Layer ทำงาน ดังนี้

Layer ที่ 7 Application Layer เป็นชั้นที่อยู่บนสุดของขบวนการรับส่งข้อมูล ทำหน้าที่ในการเชื่อมต่อข้อมูลระหว่างผู้ใช้งานกับโปรแกรมใช้งาน โดยจะแบ่งคำสั่งต่างๆ ที่ผู้ใช้กำหนดผ่านทางเมนู หรือการคลิกเมาส์ ส่งให้โปรแกรมใช้งาน ซึ่งโปรแกรมใช้งานจะไปเรียกฟังก์ชันที่ให้บริการจากระบบปฏิบัติการอีกต่อหนึ่ง ดังนั้นคำสั่งหรือข้อมูลที่ผู้ใช้ส่งมาให้จะต้องถูกต้องตามกฎเกณฑ์ของระบบปฏิบัติการนั้นๆ หากมีข้อผิดพลาดฟังก์ชั่นที่เรียกใช้งานก็จะแจ้งกลับมายังโปรแกรม และ โปรแกรมใช้งานก็จะแสดงข้อความการผิดพลาดให้กับผู้ใช้อีกต่อหนึ่ง ลักษณะการทำงานส่วนใหญ่ในชั้นนี้ได้แก่ การระบุตำแหน่งของเครื่องคอมพิวเตอร์ปลายทาง การกำหนดสิทธิ ในการเข้าถึงข้อมูล ตัวอย่างเช่น การเข้าใช้งานในระบบ E-Mail การถ่ายโอนไฟล์ในเครือข่าย

Layer ที่ 6 Presentation Layer เป็นชั้นที่ทำหน้าที่เป็นส่วนติดต่อระหว่างชั้น Application และ Session ให้เข้าใจกัน โดยจะเป็นการสร้างขบวนการย่อยๆ ในการทำงานระหว่างกัน และ จัดรูปแบบการนำเสนอข้อมูลในการสื่อสารให้เข้าใจกันได้ เช่น การแปลงรหัสข้อมูล การเข้ารหัส (Encrypt) และ ถอดรหัสข้อมูล (Decrypt)

Layerที่ 5 Session Layer เป็นชั้นที่ทำหน้าที่สร้างส่วนติดต่อ (Session) ในการสื่อสารข้อมูล โดยกำหนดจังหวะในการรับ-ส่งข้อมูลว่าจะทำงานในแบบผลัดกันส่ง (Half Duplex) หรือ ส่งรับพร้อมกัน (Full Duplex) โดยจะสร้างเป็นส่วนของชุดข้อมูลโต้ตอบกัน

Layer ที่ 4 Transport Layer ทำหน้าที่แบ่งข้อมูลที่มีขนาดใหญ่เกินมาตรฐานการรับ-ส่งออกเป็นส่วนย่อยๆ ให้เหมาะสมกับการทำงานทางฮาร์ดแวร์ของอุปกรณ์ในระบบเครือข่ายตามมาตรฐานที่ใช้งาน

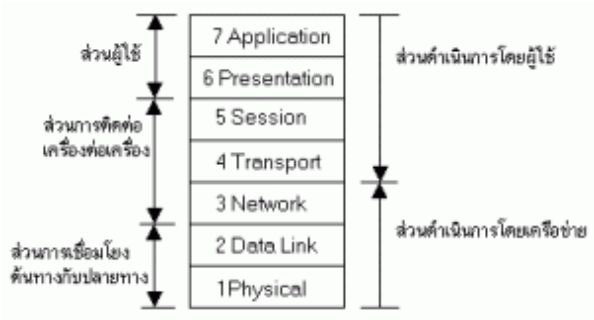
Layer ที่ 3 Network Layer ทำหน้าที่เชื่อมต่อและกำหนดเส้นทางในการรับส่งข้อมูลผ่านระบบเครือข่าย โดยจะนำข้อมูลในชั้นบนที่ส่งมาในรูปของ Package หรือ Frame ซึ่งมีเพียงแอดเดรสของผู้รับ – ผู้ส่ง ลำดับการรับ – ส่งข้อมูล และส่วนของข้อมูล นอกจากนี้ยังทำหน้าที่ในการสถาการเชื่อมต่อในครั้งแรก (Call Setup) และ การยกเลิกการติดต่อ (Call Clearing)

Layer ที่ 2 Datalink Layer ทำหน้าที่ในการจัดเตรียมข้อมูลในการเชื่อมต่อให้กับอุปกรณ์ทางฮาร์ดแวร์ โดย หลังจากที่ได้รับข้อมูลจากชั้น Network Layer ที่กำหนดเส้นทางในการติดต่อมาให้ ก็จะทำการสร้างคำสั่งที่จะใช้ควบคุมฮาร์ดแวร์ในการติดต่อ และทำการตรวจสอบข้อผิดพลาดในการรับ-ส่งข้อมูล เพื่อให้ข้อมูลที่รับ-ส่งกันตรงกับมาตรฐานการรับ-ส่งข้อมูลในระดับฮาร์ดแวร์ เช่น มาตรฐานอีเธอร์เน็ต (Ethernet) มาตรฐานโทเค็นริง (Token Ring) ฯลฯ

Layer ที่ 1 Physical Layer เป็นชั้นล่างสุดของแบบจำลอง OSI Model และเป็นชั้นที่มีการเชื่อมต่อจริงทางกายภาพ ในชั้นนี้จะเป็นส่วนที่ใช้กำหนดคุณสมบัติทางกายภาพของอุปกรณ์ที่จะนำมาเชื่อมต่อกัน เช่น จะใช้ขั้วต่อสัญญาณแบบใด ใช้การรับ-ส่งข้อมูลแบบใด ความเร็วในการรับ-ส่งข้อมูลที่จะใช้เป็นเท่าใด ข้อมูลในชั้นนี้จะอยู่ในรูปของสัญญาณทาง

ไฟฟ้าแบบดิจิตอลคือมีระดับสัญญาณ 0 หรือ 1 หากมีปัญหาในการรับ-ส่งข้อมูลทางฮาร์ดแวร์ เช่น สายรับ-ส่งข้อมูลขาด หรือ อุปกรณ์ในเครือข่ายชำรุดเสียหาย ก็จะทำการตรวจสอบและส่งข้อมูล ความผิดพลาดไปให้ชั้นอื่นๆ ที่อยู่เหนือขึ้นไปรับทราบ[6]

เราสามารถแบ่งส่วนการทำงานของสถาปัตยกรรมรูปแบบ OSI ได้ง่าย ๆ จากรูปด้านล่าง โดยด้านซ้ายมือซึ่งจัดแบ่ง Layer ทั้ง 7 ชั้นออกเป็น 3 ส่วนคือส่วนของผู้ใช้งาน ส่วนการติดต่อระหว่างเครื่องต่อเครื่อง และส่วนการเชื่อมโยงต้นทางกับปลายทาง สำหรับในทางขวามือของรูปจะเป็นการจัดแบ่งลักษณะ การสื่อ สารออกเป็น 2 ส่วนคือส่วนดำเนินการโดยผู้ใช้งาน และอีกส่วนหนึ่งเป็นการดำเนินการโดยเครือข่าย



รูปที่ 2 สถาปัตยกรรมรูปแบบ OSI แบ่งแยกตามส่วนการทำงาน[7]

ในการรับส่งข้อมูลใน OSI Model ได้กำหนด Protocol คือ ชุดของกฎที่ควบคุมการสื่อสารระหว่างคอมพิวเตอร์ในเครือข่ายในแต่ละ Layer ตามภาพด้านล่าง

OSI Reference Model		OSI Protocols
7	Application	CMIP,DS,FTAM,MHS,VTP
6	Presentation	Presentation Service/Presentation Protocol
5	Session	Session Service/Session Protocol
4	Transport	TP0,TP1,TP2,TP3,TP4,TP5
3	Network	CONP/CMNS,CLNP/CLNS,IS-IS,ES-IS
2	Datalink	IEEE802.2,IEEE802.3,IEEE802.5,FDDI,X.25
1	Physical	IEEE802.2,IEEE802.3,IEEE802.5,FDDI,X.25 Hardware Hardware Hardware Hardware

รูปที่ 3 ชุดโปรโคตอล OSI ที่ทำงานในแต่ละ Layer[8]

โปรโตคอล TCP/IP (Transmission Control Protocol / Internet Protocol)
เป็นมาตรฐานที่เกิดขึ้นก่อนการกำหนดมาตรฐาน OSI MODEL และมีการใช้งานแพร่หลายบนเครือข่ายอินเทอร์เน็ต นอกจากนี้ยังไม่ต้องเสียค่าลิขสิทธิ์ในการใช้ จึงทำให้เป็นมาตรฐานถือว่ามีการใช้งานมากที่สุดในปัจจุบัน[9]

มาตรฐาน TCP/IP จะแบ่งการรับ-ส่งข้อมูลเป็น 4 ชั้น เมื่อเปรียบเทียบกับแบบอ้างอิง OSI Model 7 ชั้น

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS,DHCP,FTP,HTTPS,IMAP,LDAP,NTP,POP3 RTP,RTSP,SSH,SIP,SMTP,SNMP,Telnet,TFTP
	Presentation Layer	JPEG,MIDI,MPEG,PICT,TIFF
	Session Layer	NetBIOS,NFS,PAP,SCP,SQL,ZIP
Transport Layer	Transport Layer	ICP,UDP
Internet Layer	Network Layer	ICMP,IGMP,IPsec,IPv4,IPv6,IPX,RIP
Network Layer	Data Link Layer	ARP,ATM,CDP,FDDI,Frame Relay, HDLC,MPLS,PPP,STP,Token Ring
	Physical Layer	Bluetooth,Ethernet,DSL,ISDN ,802.11,WiFi

รูปที่ 4 แสดงความแตกต่างของ TCP/IP,OSI Model และProtocols ในแต่ละ Layer

จากรูปจะเห็นว่า
ชั้น Application ของ TCP/IP จะเสมือนรวม ชั้น Applicationชั้น Presentation และชั้น Session เข้าเป็นชั้นเดียวกันโดยมีหน้าที่เป็นส่วนในการติดต่อระหว่างผู้ใช้งานกับ ส่วนบริการต่างๆ เช่น การโอนย้ายไฟล์ (FTP), การรับส่งจดหมายอิเล็กทรอนิกส์ (SMTP) หรือบริการในการควบคุมเครื่องระยะไกล (Telnet)
ชั้น Transport ของ TCP/IP จะทำหน้าที่เช่นเดียวกับ Transport ของ OSI Model คือจัดเตรียมข้อมูลในการรับ-ส่ง เพื่อควบคุมการรับ-ส่งข้อมูลให้มีเสถียรภาพเชื่อถือได้ รวมทั้งการตัดแบ่งข้อมูลเป็นส่วนย่อย
ชั้น Internet จะทำหน้าที่เช่นเดียวกับชั้น Network ของ OSI Model ในการเลือกเส้นทางการส่งข้อมูลรวมทั้งสร้างสภาวะการเชื่อมต่อ และ สภาวะยกเลิกการเชื่อมต่อ

ชั้น Host to Network จะทำหน้าที่แปลง IP Address เป็นหมายเลขประจำตัวทางฮาร์ดแวร์ของอุปกรณ์เครือข่าย เพื่อใช้ในการรับ-ส่งข้อมูลในระดับกายภาพ รวมทั้งการสร้างสัญญาณไฟฟ้าสำหรับการรับ-ส่งข้อมูลตามมาตรฐานทางฮาร์ดแวร์ที่ใช้ เช่น ระบบอีเธอร์เน็ต หรือ โทเค็นริง ซึ่งจะคล้ายกับการรวม ชั้น Data Link และชั้น Physical ของ OSI Model เข้าด้วยกัน[9]

แบบอ้างอิงการบริหารเครือข่าย ISO

องค์การมาตรฐานนานาชาติ ISO ได้กำหนดแบบอ้างอิงการบริหารเครือข่ายเพื่อเป็นแนวทางสำหรับการบริหารเครือข่ายอย่างเป็นระบบ ซึ่งแบบอ้างอิงประกอบด้วย 5 หัวเรื่อง ดังนี้

1.การบริหารประสิทธิภาพ (Permanance Management) : จุดประสงค์ของการบริหารประสิทธิภาพของเครือข่าย ก็เพื่อให้อุปกรณ์เครือข่ายทำงานได้อย่างเต็มประสิทธิภาพและมี Bandwidth (Bandwidth คือ การวัดความเร็วในการส่งข้อมูลของอินเทอร์เน็ต ซึ่งโดยมากเรามักวัดความเร็วของการส่งข้อมูลเป็น bps (bit per second)) เพียงพอต่อการบริหารประสิทธิภาพเครือข่ายนั้น จะเกี่ยวข้องกับการมอนิเตอร์ การประเมินการปรับค่าคอนฟิกต่างๆ เพื่อให้การใช้ Bandwidth และทรัพยากรอื่นๆมีประสิทธิภาพ ซึ่งจะเกี่ยวข้องกับการทำบัญชีคอมพิวเตอร์และอุปกรณ์เครือข่าย การตรวจวัดรายงานวิเคราะห์ปริมาณการใช้(Utilization) และอัตราส่งผ่านข้อมูล(Throughout) ของอุปกรณ์เครือข่ายต่างๆ เช่น ลิงค์ ฮับ สวิตซ์ เราท์เตอร์ โฮส และไฟร์วอลล์ เป็นต้นไปจนถึงเส้นทางข้อมูลผ่านอุปกรณ์เครือข่ายต่างๆ

2.การบริหารข้อผิดพลาด (Fault Management) : จุดประสงค์ของการบริหารข้อผิดพลาดของเครือข่าย คือ การเฝ้าระวัง การเก็บล็อก(Log) การแจ้งเตือน การตรวจเช็ค และการแก้ไขข้อผิดพลาดต่างๆ ที่เกิดขึ้นในเครือข่าย ซึ่งขั้นตอนนี้จะมีบางส่วนที่คาบเกี่ยวกับการบริหารประสิทธิภาพเครือข่าย แต่ข้อแตกต่างก็ คือ การบริหารข้อผิดพลาดนั้นจะเน้นที่การแก้ปัญหา หรือข้อผิดพลาดของเครือข่ายได้ทันเวลา เช่น สัญญาณขาด สวิตซ์เสีย และเราท์เตอร์เสีย เป็นต้น ในขณะที่การบริหารประสิทธิภาพจะเน้นที่ประสิทธิภาพการใช้งานเครือข่ายโดยรวม

3.การบริหารคอนฟิกกูเรชัน (Configulation Management) : การบริหารค่าคอนฟิกกูเรชันต่างๆ ของอุปกรณ์ในเครือข่าย เช่น หมายเลข IP เวอร์ชันของซอฟแวร์ที่ใช้ในแต่ละเซิร์ฟเวอร์ ค่าคอนฟิกของเราท์เตอร์ สวิตซ์ ผังการเชื่อมต่อของอุปกรณ์ต่างๆ เป็นต้น

4.การบริหารบัญชีผู้ใช้ (Accounting Management) : การควบคุมการใช้งานทรัพยากรเครือข่ายของผู้ใช้งาน ซึ่งอาจใช้เพื่อการเก็บค่าบริการ ฟังก์ชันอาจรวมถึงการจัดการบัญชีผู้ใช้ การพิสูจน์ทราบตัวตน การกำหนดสิทธิ และการควบคุมการเข้าถึงทรัพยากรต่างๆ เป็นต้น

5.การบริหารการรักษาความปลอดภัย(Security Management) : การควบคุมการเข้าใช้ทรัพยากรเครือข่ายให้เป็นไปตามนโยบายที่เรากำหนดไว้[10]

มาตรฐานการรักษาความปลอดภัยของข้อมูล

ระบบรักษาความปลอดภัยของข้อมูลของพาณิชย์อิเล็กทรอนิกส์จึงต้องมีมาตรการดังต่อไปนี้

1. การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization) คือ การระบุ ตัวบุคคลที่ติดต่อว่าเป็น บุคคลตามที่ได้กล่าวอ้างไว้จริง และมีอำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง (เปรียบเทียบได้กับการแสดงตัวด้วยบัตรประจำตัวซึ่งมีรูปติดอยู่ด้วย หรือการใช้ระบบล็อคซึ่งผู้ที่จะเปิดได้จะต้องมีกุญแจอยู่เท่านั้น เป็นต้น)

2. การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้ หรือส่งผ่านทางเครือข่ายโดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้ (เปรียบเทียบได้กับการปิดผนึกซองจดหมาย การใช้ซองจดหมายที่ทึบแสง การเขียนหมึกที่มองไม่เห็น เป็นต้น)

3. การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบไม่ได้ (เปรียบเทียบได้กับ การเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบขึ้น เป็นต้น)

4. การป้องกันการปฏิเสธ หรือ อ้าง ความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆที่เกี่ยวข้อง หรือ การป้องกันการอ้างที่เป็นเท็จว่าได้ รับหรือ ส่งข้อมูล (เปรียบเทียบได้กับการส่งจดหมายลงทะเบียน เป็นต้น)[11]

จากการศึกษา การบริหารจัดการเครือข่าย และการใช้งานเครือข่าย ตามแบบอ้างอิงการบริหารเครือข่าย ISO, มาตรการการรักษาความปลอดภัยของข้อมูล, มาตรฐาน OSI(Open System Interconnection)และโปรโตคอล TCP/IP (Transmission Control Protocol/ Internet Protocol) โดยทำการวิเคราะห์และสังเคราะห์โดยเปรียบเทียบแนวทางในการบริหารจัดการเครือข่ายตามมาตรฐานต่างๆ ที่ได้ศึกษา กับ OSI Model และหน้าที่ของผู้ให้บริการเครือข่าย ผู้รับบริการเครือข่าย ผู้รักษาความปลอดภัยเครือข่าย เพื่อให้ง่ายแก่การวิเคราะห์และสังเคราะห์ จึงได้ทำเป็นตารางเปรียบเทียบ ดังนี้

ตารางวิเคราะห์และสังเคราะห์การบริหารจัดการเครือข่าย

	แนวทางบริหารจัดการเครือข่าย	แบบอ้างอิงการบริหารเครือข่าย ISO	มาตรการการรักษาความปลอดภัยของข้อมูล	มาตรฐาน OSI	TCP/IP	สถานะ
1	การบริหารประสิทธิภาพ (Permanance Management) เกี่ยวข้องกับการมอนิเตอร์ การประเมิน การปรับค่าคอนฟิกต่างๆ เพื่อให้การใช้แบนด์วิธและทรัพยากรอื่นๆ มีประสิทธิภาพ การทำบัญชีคอมพิวเตอร์และอุปกรณ์เครือข่าย การตรวจวัดรายงานวิเคราะห์ปริมาณการใช้(Utilization) และอัตราส่งผ่านข้อมูล(Throughout) ของอุปกรณ์เครือข่ายต่างๆ เช่น ลิงค์ ฮับ สวิตช์ เราท์เตอร์ โฮส และไฟร์วอลล์ เป็นต้นไปจนถึงเส้นทางข้อมูลผ่านอุปกรณ์เครือข่ายต่างๆ	/		Layer1, 2 และ 3	Layer1 และ 2	ผู้ให้บริการเครือข่าย

(ต่อ)ตารางวิเคราะห์และสังเคราะห์การบริหารจัดการเครือข่าย

แนวทางบริหารจัดการเครือข่าย		แบบอ้างอิงการบริหารเครือข่าย ISO	มาตรการการรักษาความปลอดภัยของข้อมูล	มาตรฐาน OSI	TCP/IP	สถานะ
2	การบริหารข้อผิดพลาด (Fault Management) ดำเนินการ การเฝ้าระวัง การเก็บล๊อก(Log) การแจ้งเตือน การตรวจเช็ค และการแก้ไขข้อผิดพลาดต่างๆ ที่เกิดขึ้นในเครือข่าย เน้นที่การแก้ปัญหา หรือข้อผิดพลาดของเครือข่ายได้ทันเวลา เช่น สัญญาณขาด สวิตซ์เสีย และเราท์เตอร์เสีย	/		Layer1 และ 2	Layer1	ผู้ให้บริการเครือข่าย
3	การบริหารคอนฟิกกูเรชัน (Configulation Management) : การบริหารค่าคอนฟิกกูเรชันต่างๆ ของอุปกรณ์ในเครือข่าย เช่น หมายเลข IP เวอร์ชันของซอฟแวร์ที่ใช้ในแต่ละเซิร์ฟเวอร์ ค่าคอนฟิกของเราท์เตอร์ สวิตซ์ ผังการเชื่อมต่อของอุปกรณ์ต่างๆ เป็นต้น	/		Layer1 และ 2	Layer1	ผู้ให้บริการเครือข่าย
4	การบริหารบัญชีผู้ใช้ (Accounting Management) : การควบคุมการใช้งานทรัพยากรเครือข่ายของผู้ใช้งาน การพิสูจน์ทราบตัวตน การกำหนดสิทธิ และการควบคุมการเข้าถึงทรัพยากรต่างๆ เป็นต้น	/		Layer3	Layer2	ผู้ให้บริการเครือข่าย

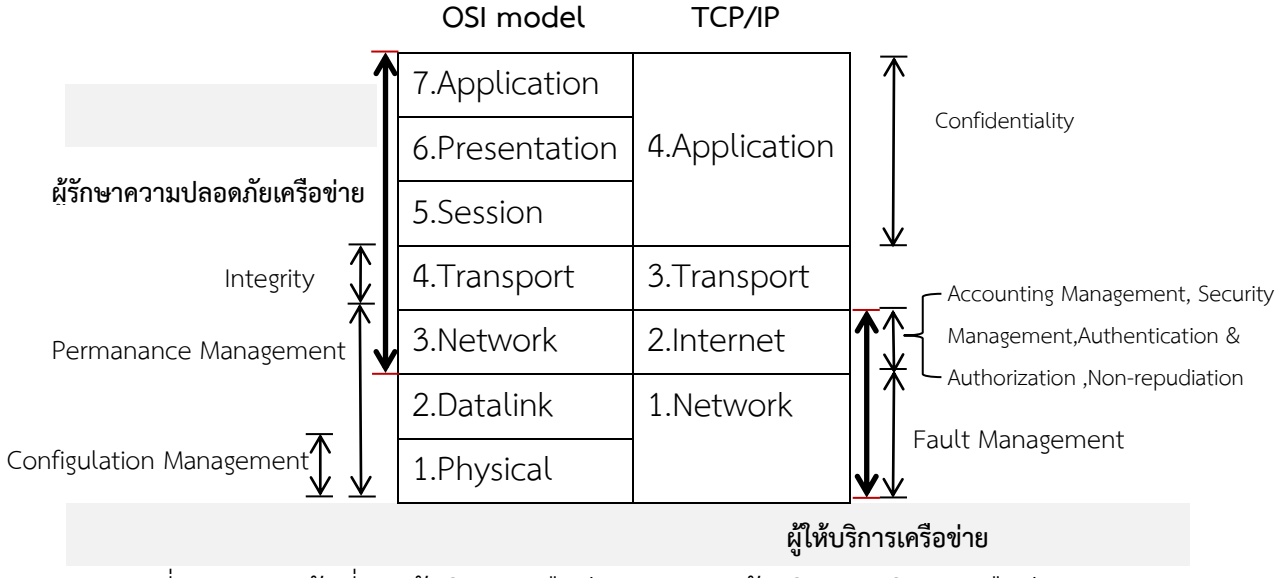
(ต่อ)ตารางวิเคราะห์และสังเคราะห์การบริหารจัดการเครือข่าย

แนวทางบริหารจัดการเครือข่าย		แบบอ้างอิงการบริหารเครือข่าย ISO	มาตรการการรักษาความปลอดภัยของข้อมูล	มาตรฐาน OSI	TCP/IP	สถานะ
5	การบริหารการรักษาความปลอดภัย (Security Management) : การควบคุมการเข้าใช้ทรัพยากรเครือข่ายให้เป็นไปตามนโยบายที่เรากำหนดไว้	/		Layer3	Layer2	ผู้รักษาความปลอดภัยเครือข่าย
6	การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization) คือ การระบุ ตัวบุคคลที่ติดต่อว่าเป็น บุคคลตามที่ได้กล่าวอ้างไว้จริง และมีอำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง		/	Layer3	Layer2	ผู้รักษาความปลอดภัยเครือข่าย
7	การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้ หรือส่งผ่านทางเครือข่ายโดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้		/	Layer5,6 และ7	Layer4	ผู้รักษาความปลอดภัยเครือข่าย
8	การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบ)ไม่ได้		/	Layer4	Layer3	ผู้รักษาความปลอดภัยเครือข่าย

(ต่อ)ตารางวิเคราะห์และสังเคราะห์การบริหารจัดการเครือข่าย

	แนวทางบริหารจัดการเครือข่าย	แบบอ้างอิงการบริหารเครือข่าย ISO	มาตรการการรักษาความปลอดภัยของข้อมูล	มาตรฐาน OSI	TCP/IP	สถานะ
9	การป้องกันการปฏิเสธ หรือ อ้างความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆที่เกี่ยวข้อง หรือการป้องกันการอ้างที่เป็นเท็จว่าได้รับหรือ ส่งข้อมูล		/	Layer3	Layer2	ผู้รักษาความปลอดภัยเครือข่าย

จากการวิเคราะห์และสังเคราะห์การบริหารจัดการเครือข่าย และการใช้งานเครือข่าย ตามแบบอ้างอิงการบริหารเครือข่าย ISO, มาตรการการรักษาความปลอดภัยของข้อมูล, มาตรฐาน OSI(Open System Interconnection)และโปรโตคอล TCP/IP (Transmission Control Protocol/ Internet Protocol) พบว่า แนวทางในการบริหารจัดการเครือข่ายตามมาตรฐานที่ได้ศึกษาเมื่อเปรียบเทียบกับ OSI Model สามารถแบ่งหน้าที่ในการบริหารจัดการเครือข่ายตาม Layer ตามภาพด้านล่าง



รูปที่ 5 แสดงหน้าที่ของผู้บริหารเครือข่ายตามแบบอ้างอิงการบริหารเครือข่าย ISO, มาตรการการรักษาความปลอดภัยของข้อมูล, มาตรฐาน OSI และโปรโตคอล TCP/IP

จากภาพสรุปได้ ดังนี้

1.ผู้ให้บริการเครือข่าย บริหารจัดการในส่วนของ Layer 1-3 มีหน้าที่ Configulation Management, Fault Management, Permanance Management, Accounting Management, Security Management,Authentication & Authorization ,Non-repudiation

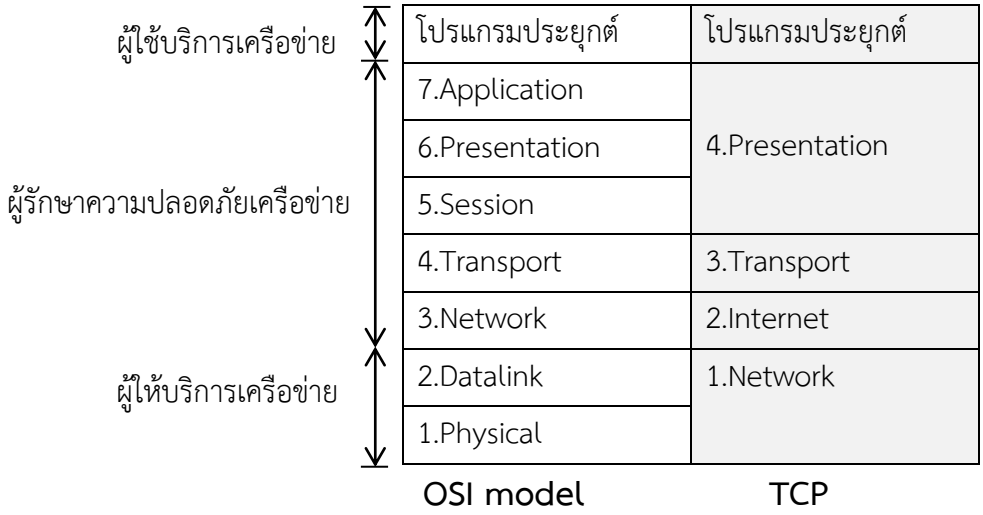
2.ผู้รักษาความปลอดภัยเครือข่าย บริหารจัดการในส่วนของ Layer 3-7 มีหน้าที่ Permanance Management, Accounting Management, Security Management,Authentication & Authorization ,Non-repudiation, Integrity, Confidentiality

บทสรุปและข้อเสนอแนะ

จากผลการศึกษาข้างต้น จึงได้เสนอแนวทางในการบริหารจัดการเครือข่ายกองทัพบก โดยใช้ OSI model มากำหนดขอบเขตของผู้ให้บริการเครือข่าย ผู้รับบริการเครือข่าย และผู้รักษาความปลอดภัย และกำหนดแนวทางในการบริหารจัดการเครือข่ายกองทัพบก

จะพบว่าใน layer 3 เป็นงานของผู้ให้บริการเครือข่ายและผู้รักษาความปลอดภัยเครือข่าย ซึ่งใน server มี software ที่ทำหน้าที่ Permanance Management, Accounting Management อยู่แล้ว จึงเห็นควรให้ผู้รักษาความปลอดภัยเครือข่ายบริหารจัดการตั้งแต่ layer 3-7 สำหรับผู้ใช้บริการเครือข่าย และจากการที่กำลังพลในกองทัพบกมีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยเครือข่ายในกองทัพบกมีหลายระดับ จึงให้บริหารจัดการเฉพาะในเรื่องของ Accounting Management, Authentication & Authorization ซึ่งอยู่เหนือ layer 7 โดยสามารถอธิบายได้ ดังนี้

OSI model/TCP/IP



บทสรุปและข้อเสนอแนะ

1. จากการศึกษาเราสามารถกำหนดขอบเขตของผู้ให้บริการเครือข่าย ผู้รับบริการเครือข่าย และผู้รักษาความปลอดภัยเครือข่าย ได้ ดังนี้

   1.1 ผู้ให้บริการเครือข่าย มีขอบเขตบริหารจัดการเครือข่ายใน layer 1-2

   1.2 ผู้รักษาความปลอดภัยเครือข่าย มีขอบเขตบริหารจัดการเครือข่ายใน layer 3-7

   1.3 ผู้ใช้บริการเครือข่าย มีขอบเขตบริหารจัดการเครือข่ายเหนือ layer 7

2. แนวทางในการบริหารจัดการเครือข่ายกองทัพบก ดำเนินการ ดังนี้

   2.1 ผู้ให้บริการเครือข่าย บริหารจัดการใน OSI layer 1-2 มีหน้าที่

2.1.1 การบริหารประสิทธิภาพ (Permanance Management) : จุดประสงค์ของการบริหารประสิทธิภาพของเครือข่าย ก็เพื่อให้อุปกรณ์เครือข่ายทำงานได้อย่างเต็มประสิทธิภาพและมีแบนด์วิธเพียงพอต่อการบริหารประสิทธิภาพเครือข่ายนั้นจะเกี่ยวข้องกับการมอนิเตอร์ การประเมิน การปรับค่าคอนฟิกต่างๆ เพื่อให้การใช้แบนด์วิธและทรัพยากรอื่นๆ มีประสิทธิภาพ ซึ่งจะเกี่ยวข้องกับการทำบัญชีคอมพิวเตอร์และอุปกรณ์เครือข่าย การตรวจวัดรายงานวิเคราะห์ปริมาณการใช้(Utilization) และอัตราส่งผ่านข้อมูล(Throughout) ของอุปกรณ์เครือข่ายต่างๆ เช่น ลิงค์ ฮับ สวิตช์ เราท์เตอร์ โฮส และไฟร์วอลล์ เป็นต้นไปจนถึงเส้นทางข้อมูลผ่านอุปกรณ์เครือข่ายต่างๆ

2.1.2 การบริหารข้อผิดพลาด (Fault Management) ดำเนินการ การเฝ้าระวัง การเก็บล๊อก(Log) การแจ้งเตือน การตรวจเช็ค และการแก้ไขข้อผิดพลาดต่างๆ ที่เกิดขึ้นในเครือข่าย เน้นที่การแก้ปัญหา หรือข้อผิดพลาดของเครือข่ายได้ทันเวลา เช่น สัญญาณขาด สวิตช์เสีย และเราท์เตอร์เสีย

2.1.3 การบริหารคอนฟิกกูเรชัน (Configulation Management) : การบริหารค่าคอนฟิกกูเรชันต่างๆ ของอุปกรณ์ในเครือข่าย เช่น หมายเลข IP เวอร์ชันของซอฟแวร์ที่ใช้ในแต่ละเซิร์ฟเวอร์ ค่าคอนฟิกของเราท์เตอร์ สวิตช์ ผังการเชื่อมต่อของอุปกรณ์ต่างๆ เป็นต้น

2.2 ผู้รักษาความปลอดภัยเครือข่าย บริหารจัดการใน OSI Layer 3-7 มีหน้าที่

2.2.1 การบริหารการรักษาความปลอดภัย (Security Management) : การควบคุมการเข้าใช้ทรัพยากรเครือข่ายให้เป็นไปตามนโยบายที่เรากำหนดไว้

2.2.2 การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้ หรือส่งผ่านทางเครือข่ายโดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้

2.2.3 การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบไม่ได้

2.2.4 การป้องกันการปฏิเสธ หรือ อ้าง ความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆที่เกี่ยวข้อง หรือ การป้องกันการอ้างที่เป็นเท็จว่าได้ รับหรือ ส่งข้อมูล

2.3 ผู้ใช้บริการเครือข่าย บริหารจัดการใน OSI layer เหนือ layer 7 มีหน้าที่

2.3.1 การบริหารบัญชีผู้ใช้ (Accounting Management) : การควบคุมการใช้งานทรัพยากรเครือข่ายของผู้ใช้งาน การพิสูจน์ทราบตัวตน การกำหนดสิทธิ และการควบคุมการเข้าถึงทรัพยากรต่างๆ เป็นต้น

2.3.2 การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization) คือ การระบุ ตัวบุคคลที่ติดต่อว่าเป็น บุคคลตามที่ได้กล่าวอ้างไว้จริง และมีอำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง

3. เพื่อให้การบริหารจัดการเครือข่ายกองทัพบกมีประสิทธิภาพ ควรแยกงานด้านสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ออกจากกัน โดยการใช้มาตรฐาน OSI(Open System Interconnection) และแบบอ้างอิงการบริหารเครือข่าย ISO โดยการกำหนดขอบเขตงานด้านสารสนเทศ ที่ OSI layer 1-2 และการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ OSI layer 3-7 โดยกำหนดหน้าที่ ดังนี้

3.1 ผู้ให้บริการเครือข่าย

3.1.1 ติดตั้งปรนนิบัติบำรุงบริหารจัดการบริการ และกำกับดูแลการใช้งานโครงสร้างพื้นฐานภายในกองทัพบก ทั้งนี้รวมถึงคอมพิวเตอร์และอุปกรณ์ประกอบทุกประเภทที่ใช้งานเชื่อมต่อกับโครงสร้างพื้นฐาน

3.1.2 กำหนดมาตรฐาน ให้คำแนะนำและกำกับดูแลการปฏิบัติของหน่วยต่างๆ ของกองทัพบกในการพัฒนาและการใช้งานโปรแกรมประยุกต์บนโครงสร้างพื้นฐาน ให้เป็นไปในทิศทางเดียวกัน ตามนโยบายของกองทัพบก

3.2 ผู้รับบริการเครือข่าย

3.2.1 เป็นผู้ใช้งานโครงสร้างพื้นฐานระบบสารสนเทศกองทัพบก

3.2.2 เป็นผู้รับผิดชอบโครงสร้างพื้นฐานในการพัฒนา ติดตั้ง ปรนนิบัติบำรุง กำกับดูแล บริหารจัดการ บริการ และรักษาความมั่นคงปลอดภัยระบบสารสนเทศในความรับผิดชอบของหน่วย

3.2.3 กำหนดเจ้าหน้าที่ผู้รับผิดชอบระบบสารสนเทศประจำหน่วย/พื้นที่รับผิดชอบ โดยปฏิบัติตามวัตถุประสงค์และแนวทางการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบกในส่วนที่เกี่ยวข้องอย่างเคร่งครัด ภายใต้การกำกับดูแลของผู้ให้บริการเครือข่าย และผู้รักษาความปลอดภัยเครือข่าย

3.2.4 การพัฒนาและการใช้งานโปรแกรมประยุกต์บนโครงสร้างพื้นฐาน ภายใต้การกำกับดูแลของผู้ให้บริการเครือข่าย

3.2.5 การบริหารบัญชีผู้ใช้ (Accounting Management)

3.2.6 การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization)

3.3 ผู้รักษาความปลอดภัยเครือข่าย

3.3.1 กำหนดมาตรฐาน ประสานงานและกำกับดูแลรักษาความมั่นคงปลอดภัยระบบสารสนเทศภายในกองทัพบกทุกประเภท

3.3.2 รวบรวมข้อมูลเฝ้าระวังตรวจสอบช่องโหว่ วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ พร้อมทั้งให้คำแนะนำแก้ไข และฟื้นฟูระบบเมื่อได้รับการร้องขอ

3.3.3 ติดตั้งปรนนิบัติบำรุงบริหารจัดการบริการ และกำกับดูแลการใช้งานเครื่องแม่ข่าย (Server)