บทความวิชาการ

แนวคิดในการแบ่งขอบเขตภารกิจด้านสารสนเทศและด้านไซเบอร์ของหน่วยงานภายในกองทัพบก

The Concepts of Defining Scope of Missions in Information System and Cyber of Royal Thai Army Organizational Structure

มานพ สัมมาขันธ์

ศูนย์ไซเบอร์กองทัพบก แขวงบางขุนพรหม เขตพระนคร กรุงเทพฯ 10200

Manop Summakhan

Army Ciber Center, Royal Thai army

E-mail: manop2334@gmail.com

วันที่รับบทความ : 20 พฤษภาคม 2563
วันที่แก้ไขบทความ : 10 มิถุนายน 2563
วันที่ตอบรับบทความ : 20 มิถุนายน 2563

บทคัดย่อ

จากการพัฒนาทางด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างก้าวกระโดด แม้ว่าจะนำมาซึ่งความเจริญก้าวหน้าและความสะดวกสบายในการดำเนินชีวิตและการประกอบอาชีพ แต่สิ่งที่แฝงมาด้วยคือภัยคุกคามจากผู้ไม่ประสงค์ดี ซึ่งกระทรวงกลาโหมตระหนักถึงความสำคัญในส่วนนี้จึงมีนโยบายให้กองทัพไทยจัดตั้งหน่วยงานรับผิดชอบทางด้านไซเบอร์เป็นการเฉพาะ สำหรับกองทัพบกได้อนุมัติจัดตั้งศูนย์ไซเบอร์กองทัพบกโดยการแปรสภาพหน่วยศูนย์เทคโนโลยีทางทหาร แต่ด้วยขอบเขตภารกิจที่ยังไม่ชัดเจนทำให้การดำเนินงานยังไม่เป็นไปตามเป้าประสงค์ บทความนี้เป็นการเสนอแนวคิดในการแบ่งขอบเขตภารกิจระหว่างหน่วยที่รับผิดชอบงานด้านสารสนเทศกับงานด้านไซเบอร์ โดยใช้แบบจำลอง OSI เป็นเครื่องมือในการอธิบายขั้นตอนการสื่อสารระหว่างคอมพิวเตอร์บนระบบเครือข่าย รวมทั้งใช้ในการวิเคราะห์รูปแบบการโจมตีทางไซเบอร์ที่อาจเกิดขึ้น เพื่อให้หน่วยงานสามารถมองเห็นถึงปัญหาและหนทางแก้ไขได้อย่างชัดเจน ซึ่งจะส่งผลให้กระบวนการทำงานมีประสิทธิภาพมากยิ่งขึ้น

คำสำคัญ: ขอบเขตภารกิจ, ระบบสารสนเทศ, ภัยคุกคามทางไซเบอร์, แบบจำลอง OSI

ABSTRACT

The latest advancements in information technology and wireless communication brought along progress and comfort in our daily lives. However, these developments come potential harms in the form of cyber threats. In response, the Ministry of Defense determined policy for Royal Thai Armed Forces to set up a special unit to be responsible for cyber security. Therefore, the Royal Thai Army had approved the establishment of the Army Cyber Center by transforming the Military Technology Center. With the conflicting scope of missions, nevertheless, causes the operations in cyber security to not meet the goals. This article aims to present the idea of dividing the scope of operations between information systems and cyber systems by using the OSI model as a basis for consideration as well as analyzing potential cyber threats so that the responsible unit can rapidly identify and fix the vulnerabilities, and that results in greater response capabilities.

Keywords: Scope of Missions, Information System, Cyber Threats, OSI Model

บทนำ

การเปลี่ยนแปลงของสภาวะแวดล้อมอันเนื่องมาจากความก้าวหน้าทางเทคโนโลยี ด้านอิเล็กทรอนิกส์และสเปกตรัมแม่เหล็กไฟฟ้า นำไปสู่การพัฒนาและการใช้งานแบบก้าวกระโดดทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยส่งผลกระทบทั้งในระดับบุคคลไปจนถึงระดับประเทศ ซึ่งได้ให้ความสำคัญในการนำเทคโนโลยีมาประยุกต์ใช้ให้เกิดประโยชน์สูงสุดจนเกิดเป็นพลังอำนาจทางไซเบอร์ ในทุกมิติ ทั้งด้านการเมือง เศรษฐกิจ สังคม วิทยาศาสตร์ เทคโนโลยี และการทหาร รวมทั้งยังเคยส่งผลกระทบต่อความมั่นคงของชาติมาแล้วในหลายประเทศ จึงทำให้เห็นว่าโลกของเราเข้าสู่ยุคโลกเสมือนที่ไร้พรมแดนในมิติไซเบอร์ (Cyberspace) อย่างแท้จริง

แต่เทคโนโลยีที่ล้ำสมัย มักมาพร้อมกับภัยคุกคามจากผู้ที่ไม่ประสงค์ดี ดังนั้น ความปลอดภัยทางไซเบอร์ (Cyber Security) เป็นประเด็นที่ถูกกล่าวถึงมากที่สุดในช่วงที่ประเทศไทยกำลังเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัลไทยแลนด์ 4.0 เนื่องจากกลไกการขับเคลื่อนประเทศด้วยระบบดิจิทัลจะต้องมีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มแข็ง แต่จากรายงานข่าวสารในหลายประเทศพบว่า ปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์เพิ่มขึ้นอย่างรวดเร็ว (อินทีวรา จุลชาต, บุญญาภรณ์ วาณิชยชาติ และสาวิตรี ระงับพิษ, 2561) โดยเฉพาะภัยคุกคามที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) ซึ่งในประเทศไทยประกอบด้วย 6 กลุ่ม คือ กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ กลุ่มการเงิน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภค และกลุ่มสาธารณสุข (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2561)

จากแนวโน้มภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงขึ้น รัฐบาลและกระทรวงกลาโหมได้ตระหนักถึงความสำคัญ จึงกำหนดให้ภัยคุกคามด้านไซเบอร์เป็นภัยคุกคามที่มีความสำคัญต่อชาติและได้กำหนดให้การป้องกันภัยคุกคามด้านไซเบอร์เป็นภารกิจที่สำคัญของกระทรวงกลาโหม

กองทัพบกกับภารกิจด้านสารสนเทศและไซเบอร์

กองทัพบกในฐานะหน่วยปฏิบัติหลักด้านความมั่นคงตามกรอบของกระทรวงกลาโหม ได้ให้ความสำคัญต่อการนำเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้งานอย่างต่อเนื่อง และตระหนักถึงภัยคุกคามด้านไซเบอร์ (Cyber Threat) ที่มีความรุนแรงและมีรูปแบบที่หลากหลายมากยิ่งขึ้น ซึ่งท้าทายต่อการปฏิบัติการทางทหารโดยตรง เนื่องจากแนวโน้มด้านเทคโนโลยีทางทหารจะพัฒนาไปสู่การใช้ระบบอัตโนมัติ รวมทั้งระบบควบคุมอุปกรณ์และเครื่องมือทางทหารโดยไม่ใช้คนบังคับ (Unmanned Vehicle/Machine) ซึ่งมีการพัฒนาอย่างต่อเนื่อง ระบบการติดต่อสื่อสารควบคุมและการสั่งการด้วยเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ เพื่อสนับสนุนการตกลงใจในสนามรบ และเพื่อการบริหารงานทั่วไป และในอนาคตจะเข้าสู่ยุคของการปฏิบัติการทางทหารโดยใช้เครือข่ายเป็นศูนย์กลางมากยิ่งขึ้น การสู้รบโดยไม่ใช้อาวุธสังหารจะมีบทบาทในการสร้างความได้เปรียบและจำกัดเสรีในการปฏิบัติของฝ่ายตรงข้ามในรูปแบบต่าง ๆ เช่น การปฏิบัติการข่าวสาร (Information Operations) ไปจนถึงการปฏิบัติการที่เชื่อมโยงบนเครือข่ายคอมพิวเตอร์ (Cyber Operations) ซึ่งในห้วงเวลาที่ผ่านมาได้มีการออกระเบียบกองทัพบกว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศกองทัพบก พ.ศ. 2555 และฉบับปรับปรุง พ.ศ. 2560 ให้หน่วยงานต่าง ๆ ของกองทัพบกยึดถือปฏิบัติ รวมทั้งได้กำหนดแนวทางการพัฒนาการปฏิบัติด้านไซเบอร์ของกองทัพบก เพื่อให้มีความสอดคล้องกับสภาวะแวดล้อมและสถานการณ์ภัยคุกคามทางไซเบอร์

เดิมกองทัพบกมีหน่วยที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ ซึ่งก็คือศูนย์เทคโนโลยีทางทหาร เป็นหน่วยที่ขึ้นตรงกับกรมการทหารสื่อสาร (แผนภาพที่ 1) แต่เมื่อภัยคุกคามทางไซเบอร์ทวีความรุนแรงขึ้น ประกอบกับนโยบายของกระทรวงกลาโหมที่ต้องการให้กองบัญชาการกองทัพไทยและเหล่าทัพมีหน่วยงานรับผิดชอบการปฏิบัติด้านไซเบอร์เป็นการเฉพาะ กองทัพบกจึงได้พิจารณาอนุมัติให้มีการแปรสภาพศูนย์เทคโนโลยีทางทหารเป็นศูนย์ไซเบอร์

แผนภาพที่ 1 ผังการจัดหน่วยของกองทัพบก ก่อนการแปรสภาพศูนย์เทคโนโลยีทางทหาร

กองทัพบก และปรับสายการบังคับบัญชาเป็นหน่วยขึ้นตรงกองทัพบก เมื่อ 1 ตุลาคม พ.ศ. 2559 (ศูนย์ไซเบอร์กองทัพบก, 2559) (แผนภาพที่ 2)

ภารกิจหน่วย

หากพิจารณาจากภารกิจของหน่วย ภารกิจของกรมการทหารสื่อสารคือ วางแผน อำนวยการ ประสานงาน แนะนำ และกำกับการในกิจการทั้งปวงที่เกี่ยวกับการสื่อสาร การโทรคมนาคม คอมพิวเตอร์ และอิเล็กทรอนิกส์ สนับสนุนระบบควบคุมบังคับบัญชาและการสื่อสาร ตลอดจนการสงครามข่าวสารของกองทัพบก ซึ่งต่อมาเมื่อมีการแปรสภาพศูนย์เทคโนโลยีทางทหารเป็นศูนย์ไซเบอร์กองทัพบก ภารกิจด้านเทคโนโลยีสารสนเทศจึงถูกโอนให้กรมการทหารสื่อสารเป็นผู้รับผิดชอบ ดังนั้น ในภาพรวมแล้วปัจจุบันกรมการทหารสื่อสารจะดำเนินการเกี่ยวกับโครงสร้างพื้นฐานด้านการสื่อสารและระบบสารสนเทศให้กับหน่วยงานของกองทัพบก เช่น การเชื่อมต่อโครงข่ายการสื่อสารระหว่างกองทัพภาค เป็นต้น

สำหรับศูนย์ไซเบอร์กองทัพบก ได้รับภารกิจใหม่คือ การดำเนินการเกี่ยวกับการปฏิบัติด้านไซเบอร์และการพัฒนาความพร้อมด้านไซเบอร์ของกองทัพบก โดยให้ความสำคัญทางด้านการรักษาความมั่นคงปลอดภัยในส่วนของซอฟต์แวร์ของโครงสร้างพื้นฐานการสื่อสาร เช่น การเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับเครือข่ายอินเทอร์เน็ตของกองบัญชาการกองทัพบก และตอบสนองต่อภัยคุกคามทันทีที่ตรวจพบ ซึ่งการดำเนินงานของศูนย์ไซเบอร์กองทัพบก มีการประชุมหารือและฝึกศึกษาร่วมกันระหว่างศูนย์ไซเบอร์เหล่าทัพและหน่วยงานภายนอกในภารกิจที่เกี่ยวข้องอย่างสม่ำเสมอ เพื่อให้การดำเนินงานเป็นไปในทิศทางเดียวกัน เช่น การประชุมคณะกรรมการความมั่นคงปลอดภัยไซเบอร์กองทัพไทย การประชุมประชาคมไซเบอร์กองทัพไทย และการฝึกร่วมการรักษาความปลอดภัยทางไซเบอร์แบบเป็นหน่วย ซึ่งมีกรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (ทสอ.กห.) และการไฟฟ้านครหลวง (กฟน.) เข้าร่วมฝึกด้วย เป็นต้น

แต่หากพิจารณาจากความหมายของคำว่าระบบสารสนเทศ ซึ่งเป็นงานด้านการพัฒนาระบบงานบนเว็บไซต์

แผนภาพที่ 2 ผังการจัดหน่วยของกองทัพบก หลังการแปรสภาพศูนย์เทคโนโลยีทางทหาร

(Web Application) และเป็นภารกิจที่กรมการทหารสื่อสารได้รับโอนมาจากศูนย์เทคโนโลยีทางทหารนั้น จะแบ่งออกเป็น 3 ระดับ (Tier) (Multitier Architecture, 2561) (แผนภาพที่ 3) คือ

1. Presentation Tier เป็นระดับการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับผู้ใช้งาน เช่น แป้นพิมพ์ จอภาพ เม้าส์ เป็นต้น

2. Application Tier เป็นระบบงานที่ให้บริการสื่อสารระหว่างผู้ใช้งานกับฐานข้อมูล เช่น เครื่องแม่ข่าย (Server)

3. Data Tier เป็นระบบฐานข้อมูล (Data Base) ที่สนับสนุนการทำงานของระบบงาน

แต่ปัจจุบันที่เทคโนโลยีสารสนเทศได้รับการพัฒนาและมีขอบเขตงานที่กว้างขึ้นอย่างมาก ทำให้นิยามของระบบสารสนเทศดังกล่าวอาจครอบคลุมได้ไม่ทั่วถึง จึงมีแนวคิดในการแบ่งแยกภารกิจของทั้งสองหน่วยงานอย่างชัดเจน เพื่อให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดในการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยใช้แบบจำลองเครือข่าย (Network Model) เพื่ออธิบายการทำงานของระบบเครือข่ายในแต่ละชั้น โดยบทความนี้เลือกใช้แบบจำลอง OSI (OSI Model)

แบบจำลอง OSI

การสื่อสารระหว่างคอมพิวเตอร์เปรียบได้กับการสื่อสารของมนุษย์ที่ต้องใช้ภาษา และต้องเป็นภาษาเดียวกัน ซึ่งภาษาดังกล่าวเรียกว่าโปรโตคอล (Protocol) เป็นตัวกำหนดขั้นตอนและรูปแบบของข้อมูลที่ใช้ในการสื่อสารระหว่างคอมพิวเตอร์ที่เชื่อมต่อกันเป็นเครือข่าย (อดิศยา เจริญผล, 2561) องค์การมาตรฐานนานาชาติ (The International Organization for Standardization: ISO) ได้ออกแบบจำลองการเชื่อมต่อเครือข่ายแบบเปิด หรือ OSI (Open System Interconnect) โดยมีจุดมุ่งหมายเพื่อให้คอมพิวเตอร์และอุปกรณ์เครือข่ายที่ผลิตโดยบริษัทต่าง ๆ สามารถทำงานร่วมกันได้ แม้ว่าแบบจำลองนี้จะไม่ได้ถูกใช้งานอย่างแพร่หลายเหมือนแบบจำลองชุดอื่น ๆ อย่างเช่น TCP/IP (Transmission Control Protocol) แต่ OSI มีการออกแบบโครงสร้างที่ค่อนข้างสมบูรณ์ ง่ายต่อการใช้อธิบายกลไกการทำงานของโปรโตคอลในเครือข่าย

แผนภาพที่ 3 การแบ่งระดับชั้นของระบบสารสนเทศ

ที่มา: บริษัท ล็อกจิค, 2563

แบบจำลอง OSI แบ่งขั้นตอนการสื่อสารระหว่างคอมพิวเตอร์ออกเป็น 7 ชั้น หรือเลเยอร์ (Layer) (จตุชัย แพงจันทร์, อนุโชต วุฒิพรพงษ์ และอรรณพ ขันธิกุล, 2551) (แผนภาพที่ 4) ประกอบด้วย

เลเยอร์ที่ 1 Physical Layer ทำหน้าที่เชื่อมต่อและส่งสัญญาณทางไฟฟ้าจากผู้ส่งไปยังผู้รับโดยผ่านอุปกรณ์ เช่น สายทองแดง ใยแก้วนำแสง เต้าเสียบ และหัวต่อต่าง ๆ เป็นต้น

เลเยอร์ที่ 2 Data Link Layer ทำหน้าที่รวบรวมและตรวจสอบความถูกต้องของข้อมูล รวมถึงแก้ไขข้อผิดพลาดต่าง ๆ ในระหว่างการรับส่งข้อมูล โดยจะต้องมีการระบุที่อยู่ของอุปกรณ์ต่าง ๆ หรือที่เรียกว่า MAC Address ของอุปกรณ์ที่ใช้ในเลเยอร์นี้ เช่น อุปกรณ์สวิตช์ (Switch) เป็นต้น

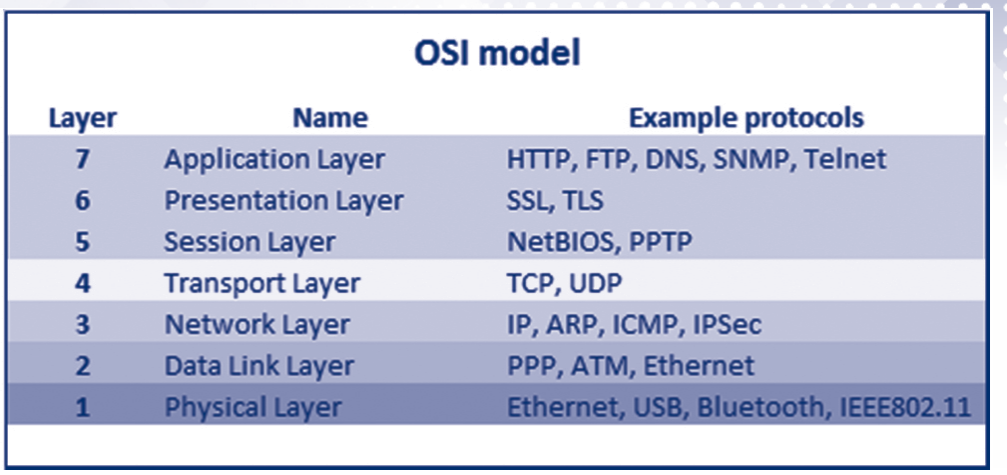
เลเยอร์ที่ 3 Network Layer ทำหน้าที่เลือกหรือกำหนดเส้นทางที่เหมาะสมที่สุดในการส่งผ่านข้อมูลข้ามเครือข่าย โดยจะส่งจากจุดหนึ่งไปยังจุดต่อไปจนถึงปลายทาง (Hop by Hop) ผ่าน Internet Protocol (IP) โดยจะมีการสร้างที่อยู่หรือหมายเลขที่บ่งบอกเฉพาะของคอมพิวเตอร์ที่อยู่ในเครือข่าย (Addressing) ขึ้นมาเพื่อใช้อ้างอิง หรือที่เรียกว่า IP Address

เลเยอร์ที่ 4 Transport Layer ทำหน้าที่แบ่งข้อมูลให้พอเหมาะกับการใช้งานในแต่ละเลเยอร์ เช่น แบ่งข้อมูลในส่วนของเลเยอร์บนให้เหมาะกับการจัดส่งลงไปในเลเยอร์ล่าง เป็นต้น

เลเยอร์ที่ 5 Session Layer ทำหน้าที่ควบคุมการส่งผ่านข้อมูลการสื่อสารจากต้นทางไปยังปลายทางให้มีความสอดคล้องกัน การสื่อสารที่เกิดขึ้นช่วงขณะใดขณะหนึ่งเรียกว่า Session เลเยอร์นี้จะรับผิดชอบเกี่ยวกับการสร้าง Session ควบคุมการแลกเปลี่ยนข้อมูล และยกเลิก Session เมื่อสิ้นสุดการสื่อสาร

เลเยอร์ที่ 6 Presentation Layer ทำหน้าที่แสดงผลในรูปแบบที่ผู้ใช้งานมองเห็น เช่น รูปภาพบนจอมอนิเตอร์ รวมถึงการส่งข้อมูลที่มีการเข้ารหัส (Encoding) เนื่องจากคอมพิวเตอร์แต่ละเครื่องอาจใช้วิธีการเข้ารหัสที่ต่างกัน เช่น บางเครื่องอาจใช้การเข้าหัสแบบ ASCII (American Standard Code for Information Interchange) แต่บางเครื่องอาจใช้การเข้ารหัสแบบ EBCDIC (Extended

แผนภาพที่ 4 แบบจำลอง OSI



OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

ที่มา: สารานุกรมเสรี, 2561

Binary Coded Decimal Interchange Code) ดังนั้น ในเลเยอร์นี้จะทำการแปลงข้อมูลให้อยู่ในรูปแบบมาตรฐาน ส่วนทางเครื่องผู้รับจะแปลงกลับไปเป็นรูปแบบที่คอมพิวเตอร์เครื่องนั้นเข้าใจ

เลเยอร์ที่ 7 Application Layer ทำหน้าที่เชื่อมต่อระหว่างโปรแกรมประยุกต์ของผู้ใช้งานกับกระบวนการการสื่อสารผ่านเครือข่าย เช่น Web Browser, Email และ FTP เป็นต้น

และส่วนที่อยู่ถัดจากเลเยอร์ที่ 7 คือ ผู้ใช้งาน (User) ซึ่งเป็นผู้ส่งคำสั่งผ่านโปรแกรมประยุกต์ไปยังเลเยอร์ที่ 7

การสื่อสารระหว่างคอมพิวเตอร์ในเครือข่าย จะเริ่มจากการที่ผู้ใช้งานมีข้อมูลที่ต้องการส่งไปยังผู้ใช้งานอีกคนหนึ่ง โดยข้อมูลนั้นจะส่งผ่านจากเลเยอร์ที่ 7 ไปจนถึงเลเยอร์ที่ 1 จากนั้นข้อมูลจะถูกแปลงเป็นสัญญาณเพื่อส่งผ่านสายสัญญาณหรือสื่อกลางที่เชื่อมระหว่างคอมพิวเตอร์จนถึงเครื่องผู้รับ ส่วนกระบวนการรับข้อมูลจะดำเนินไปในทางกลับกันคือ จะเริ่มต้นรับข้อมูลจากเลเยอร์ที่ 1 และส่งต่อไปเรื่อย ๆ จนถึงเลเยอร์ที่ 7 จากนั้นจะส่งต่อให้โปรแกรมประยุกต์ของผู้ใช้งานต่อไป (แผนภาพที่ 5) ซึ่งหลักการรับส่งข้อมูลนี้คล้ายกับการรับส่งจดหมายทางไปรษณีย์ที่ข้อมูลจะถูกบรรจุลงในซองจดหมาย จ่าหน้าที่อยู่ของผู้รับและผู้ส่ง จากนั้นหย่อนซองจดหมายลงในตู้ไปรษณีย์ และระบบขนส่งทำการขนย้ายจดหมายไปตามที่อยู่ผู้รับจนกระทั่งผู้รับได้รับข้อมูลและเปิดอ่านข้อความ

ภัยคุกคามทางไซเบอร์ตามแบบจำลอง OSI

แบบจำลอง OSI นอกจากจะทำให้เข้าใจการสื่อสารของข้อมูลในระบบเครือข่ายแล้ว ยังทำให้ทราบถึงรูปแบบการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นในแต่ละเลเยอร์ โดยช่องโหว่ของระบบเครือข่ายสามารถอธิบายได้ดังนี้ (Lee Hazell, 2557)

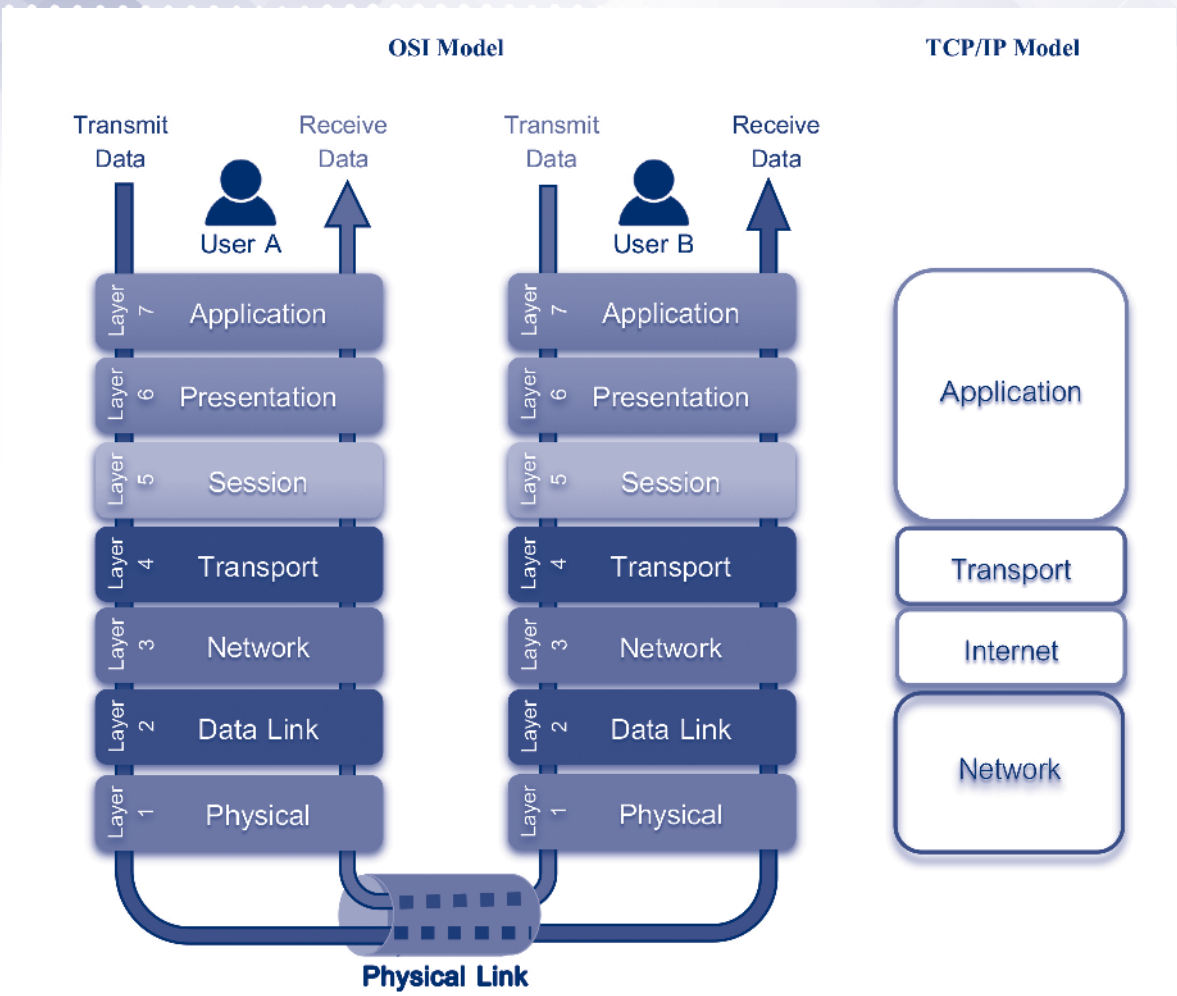
เลเยอร์ที่ 1 Physical Layer มักพบการโจมตีที่มุ่งทำให้ระบบเครือข่ายล้มเหลว ซึ่งวิธีการโจมตีอาจทำได้โดยการตัดสายเคเบิล ใช้อุปกรณ์ตัดสัญญาณไวไฟ หรือโจมตีด้วย DDoS (Distributed Denial of Service) เพื่อให้เครื่องแม่ข่ายไม่สามารถให้บริการได้อีก

เลเยอร์ที่ 2 Data Link Layer จะเป็นการโจมตีที่อุปกรณ์สวิตช์ที่ไม่ได้ตั้งค่าอย่างปลอดภัย รูปแบบการโจมตีที่พบ เช่น MAC Flooding ซึ่งเป็นการส่ง MAC Address ปลอมเข้าไปเป็นจำนวนมาก จนทำให้พื้นที่เก็บข้อมูลในอุปกรณ์สวิตช์เต็ม หรือ ARP Poisoning ที่เป็นการโจมตีช่องโหว่ของโปรโตคอล ARP

เลเยอร์ที่ 3 Network Layer รูปแบบการโจมตีที่พบจะเป็น DDoS เพื่อขัดขวางการส่งผ่านข้อมูลข้ามเครือข่าย

เลเยอร์ที่ 4 Transport Layer มักพบการสแกนพอร์ต

แผนภาพที่ 5 แบบจำลอง OSI เปรียบเทียบกับแบบจำลอง TCP/IP



(Port Scanning) เพื่อสำรวจหาช่องโหว่ในระบบ

เลเยอร์ที่ 5 Session Layer เลเยอร์ที่ 6 Presentation Layer และเลเยอร์ที่ 7 Application Layer มักพบการโจมตีช่องโหว่บนโปรแกรมประยุกต์ที่เกิดจากความผิดพลาดในการพัฒนาตัวโปรแกรม รูปแบบการโจมตีที่พบ เช่น SQL Injection ซึ่งเป็นการแอบใส่คำสั่ง SQL ผ่านทาง Web Application เพื่อโจมตีระบบฐานข้อมูล

การแบ่งภารกิจในเลเยอร์ 3

เมื่อพิจารณาถึงภารกิจของกรมการทหารสื่อสารและศูนย์ไซเบอร์กองทัพบกจะพบว่า กรมการทหารสื่อสารรับผิดชอบกำกับดูแลในส่วนของเลเยอร์ 1-2 เพราะเกี่ยวเนื่องกับระบบฮาร์ดแวร์ และการโจมตีทางไซเบอร์ที่พบจะเป็นลักษณะของการโจมตีทางกายภาพ สำหรับศูนย์ไซเบอร์กองทัพบกรับผิดชอบกำกับดูแลในส่วนของเลเยอร์ 3-7 ซึ่งภัยคุกคามจะเป็นลักษณะของการโจมตีระบบซอฟต์แวร์ โดยศูนย์ไซเบอร์กองทัพบกมีการเฝ้าระวังและป้องกันภัยคุกคามทางไซเบอร์ตลอด 24 ชั่วโมงทุกวัน มีการตรวจสอบการใช้งานอินเทอร์เน็ตของกำลังพลเพื่อตรวจหาและดักจับโปรแกรมประสงค์ร้าย หรือมัลแวร์ (Malware) รวมถึงพฤติกรรมที่เข้าข่ายการบุกรุกต่อระบบเครือข่ายภายใน เช่น DDoS, SQL Injection และการสแกนพอร์ต เป็นต้น หากตรวจพบการโจมตีดังกล่าว ศูนย์ไซเบอร์กองทัพบกจะส่งทีมตอบสนองเหตุการณ์ภัยคุกคามทางไซเบอร์

(Computer Security Incident Response Team: CSIRT) เพื่อทำการแก้ไขปัญหาทันที นอกจากนี้ยังมีการกำหนดวงรอบการทดสอบเจาะระบบเพื่อค้นหาช่องโหว่ (Penetration Testing) และการประเมินความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ (Vulnerability Assessment) ของระบบเครือข่ายภายในกองทัพบกด้วย

อย่างไรก็ตาม ในส่วนของเลเยอร์ 3 ถึงแม้จะเป็นการกำหนดเส้นทางการส่งผ่านข้อมูลข้ามเครือข่าย แต่ต้องอาศัยอุปกรณ์ในการเชื่อมต่อซึ่งก็คือ Router หรืออุปกรณ์สวิตช์ เลเยอร์ 3 (Switch Layer 3) ดังนั้น ในการปฏิบัติที่ผ่านมาจึงเป็นหน้าที่ของกรมการทหารสื่อสารในการติดตั้งและตั้งค่าอุปกรณ์ รวมถึงการกำหนด IP Address และบัญชีผู้ใช้งาน แต่เนื่องจากกำลังพลมีการเปลี่ยนแปลงตำแหน่งบ่อยครั้ง ทำให้บัญชีผู้ใช้งานประจำ IP Address นั้น ๆ มีการเปลี่ยนแปลงอยู่เสมอ เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ ทีม CSIRT ของศูนย์ไซเบอร์กองทัพบกจึงไม่สามารถดำเนินการได้ทันที เพราะต้องติดต่อประสานขอข้อมูล IP Address และบัญชีผู้ใช้งานจากกรมการทหารสื่อสาร

ดังนั้น เพื่อให้การปฏิบัติงานมีประสิทธิภาพ การตั้งค่าอุปกรณ์ในเลเยอร์ 3 รวมถึงการเก็บรวบรวมบัญชีผู้ใช้งานควรเป็นภารกิจของศูนย์ไซเบอร์กองทัพบก เพื่อใช้สนับสนุนการปฏิบัติให้กับทีม CSIRT ในการดำเนินการแก้ไขปัญหาและพิสูจน์หลักฐานทางไซเบอร์ให้กับหน่วยงานของกองทัพบกได้รวดเร็วยิ่งขึ้น นอกจากนี้หากต้องการประสิทธิภาพสูงสุดในการรักษาความมั่นคงปลอดภัยให้กับเครือข่ายภายใน ควรมีการจำกัดจำนวนเส้นทางเชื่อมต่อกับอินเทอร์เน็ต เปรียบเหมือนการผ่านเข้าออกหน่วยงานทหารที่ต้องผ่านกองรักษาการณ์เพื่อตรวจหาและเฝ้าระวังภัยคุกคามตลอด 24 ชั่วโมง แต่หากมีทางเข้าออกจำนวนมาก การเฝ้าระวังยิ่งทำได้ลำบาก ดังนั้น ควรกำหนดให้เครือข่ายภายในมีเส้นทางเชื่อมต่อกับอินเทอร์เน็ตให้น้อยที่สุด

สรุป

การแบ่งขอบเขตภารกิจของแต่ละหน่วยงานให้เกิดประสิทธิภาพและประสิทธิผล หากยึดเพียงความหมายของคำนิยามที่ระบุในภารกิจหน่วย อาจเกิดความไม่ชัดเจนของหน้าที่ความรับผิดชอบ ส่งผลให้การปฏิบัติงานมีความซ้ำซ้อน เกิดความล่าช้า และอาจไม่ทันต่อเหตุการณ์ นอกจากนี้อาจเกิดความสับสนในการระบุปัญหา ข้อขัดข้อง หรือประเภทของภัยคุกคามที่อาจเกิดขึ้นในแต่ละขั้นตอนของการปฏิบัติงานด้วย ดังนั้น แต่ละหน่วยควรพิจารณาเลือกหลักทฤษฎีหรือแบบจำลองที่เหมาะสมกับหน่วยงานของตน และนำมาใช้อ้างอิงในการวางแผน การปฏิบัติงาน การประเมินผล และการทบทวนกระบวนการปฏิบัติงานของหน่วยงาน เพราะจะทำให้การแบ่งขอบเขตหน้าที่มีหลักการที่ชัดเจน สอดคล้องกับภารกิจ และสนับสนุนการปฏิบัติของหน่วย ส่งผลให้การดำเนินงานมีประสิทธิภาพมากยิ่งขึ้น รวมถึง ลดข้อผิดพลาด ข้อขัดข้องในการปฏิบัติงานของหน่วย และเป็นไปตามนโยบายของผู้บังคับบัญชากองทัพบก กระทรวงกลาโหม และรัฐบาล ที่ชัดเจน และส่งผลต่อการรักษาความมั่นคงแห่งชาติด้านไซเบอร์ (Security Ciber) ต่อไป

บรรณานุกรม

อินทีวรา จุลชาต, บุญญาภรณ์ วาณิชยชาติ และสาวิตรี ระงับพิษ. “ความปลอดภัยไซเบอร์และเทคโนโลยีบล็อกเชน”, วารสารเทคโนโลยีป้องกันประเทศ. 7 (30), เมษายน-มิถุนายน 2561. หน้า 42-43.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. “การประชุมแนวนโยบายการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ”. (เอกสารประกอบการประชุมแนวนโยบายการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ. 2561).

ศูนย์ไซเบอร์กองทัพบก. “ประวัติศูนย์ไซเบอร์กองทัพบก”. (ออนไลน์). เข้าถึงได้จาก: https:// cyber.rta.mi.th/about.php, 2559.

“Multitier architecture”. (ออนไลน์). เข้าถึงได้จาก : https://en.wikipedia.org/wiki/Multitier_architecture, 2561.

ธีระยุทธ ทองเครือ. “สถาปัตยกรรมเว็บเซอร์วิส”. (ออนไลน์). เข้าถึงได้จาก: https://dev.cs.kku.ac.th/ws/slide/chapter%201.pdf, 2561.

อดิศยา เจริญผล. “Network Model”. (ออนไลน์). เข้าถึงได้จาก: http://www.ict.up.ac.th/ adisayac/231341/Network%20Model.pdf, 2561.

จตุชัย แพงจันทร์, อนุโชต วุฒิพรพงษ์ และ อรรณพ ขันธิกุล, บรรณาธิการ. เจาะระบบ Network 2nd Edition. (นนทบุรี: ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์, 2551). หน้า 39-47.

Lee Hazell. “Network Vulnerabilities and the OSI Model”. (ออนไลน์). เข้าถึงได้จาก: https:// cybersecuritynews.co.uk/network-vulnerabilities-and-the-osi-model, 2557.