Thailand SSC focus

Strategic Studies Center
National Defence Studies Institute
Royal Thai Armed Forces Headquarters

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
กองบัญชาการกองทัพไทย

เอกสารวิเคราะห์สถานการณ์ยุทธศาสตร์และความมั่นคง ฉบับที่ ๖/๖๔ (๑-๓๑ มี.ค.๖๔)

การปรับปรุงขีดความสามารถทางไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ

ความก้าวหน้าทางเทคโนโลยีทางด้านไซเบอร์ได้มีการพัฒนาไปอย่างรวดเร็ว ผลจากภัยคุกคามทางไซเบอร์ส่งผลให้ประเทศต่าง ๆ ต้องมีการพัฒนาภายในหน่วยงาน พัฒนาบุคลากรให้มีความทันสมัย เพิ่มศักยภาพและยกระดับหน่วยงานให้สามารถแข่งขันกับองค์กรอื่น ๆ รวมถึงการพร้อมรับมือกับภัยคุกคามทางเทคโนโลยีทุกรูปแบบ และถือเป็นความเร่งด่วนในการบริหารจัดการสำหรับองค์กรต่าง ๆ ซึ่งกระทรวงกลาโหมสหรัฐฯ ก็ได้มีความเคลื่อนไหวในการพัฒนากำลังพลมาอย่างต่อเนื่อง เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามและสร้างความได้เปรียบในการแข่งขันให้กับประเทศในระยะยาว จึงมีความจำเป็นที่จะต้องฟื้นฟูกำลังพลที่มีในปัจจุบันให้มีความพร้อมในระดับสูงเพื่อสอดรับกับยุคแห่งการเปลี่ยนแปลงทางไซเบอร์

ข้อมูลทั่วไป

ในปัจจุบันภัยคุกคามความมั่นคงทางไซเบอร์ที่กระทบต่อความมั่นคง และความก้าวหน้าทางเทคโนโลยีที่มีการพัฒนาไปอย่างรวดเร็วได้เข้ามามีบทบาทสำคัญในการเปลี่ยนแปลงโลก ความรวดเร็วทำให้การติดต่อสื่อสาร การรับส่ง และการเข้าถึงข้อมูลเป็นไปอย่างไร้ขีดจำกัด[๑] เห็นได้จากในช่วงที่ผ่านมา พบข่าวมัลแวร์ (Malware) และภัยคุกคามทางไซเบอร์หลากหลายประเภทเพิ่มมากขึ้นทำให้เห็นว่าภัยคุกคามทางไซเบอร์มีการพัฒนาไปอย่างรวดเร็วและส่งผลกระทบในวงกว้างมากขึ้น

จากสถานการณ์และการเปลี่ยนแปลงของโลกอย่างรวดเร็วส่งผลต่อความมั่นคงของนานาประเทศในหลายมิติ รวมทั้งประเทศไทย มีสิ่งบ่งชี้ว่าความมั่นคงของชาติได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ในหลายมิติ เช่น ผลกระทบต่อความน่าเชื่อถือทางเศรษฐกิจ สังคม การเมือง รวมไปถึงความสงบเรียบร้อยและความมั่นคงในประเทศ นอกจากนั้นเมื่อมีความก้าวหน้าและพึ่งพาไซเบอร์มากเพียงใด ยิ่งเพิ่มโอกาสเสี่ยงที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงของชาติจากไซเบอร์มากขึ้นอย่างหลีกเลี่ยงไม่ได้[๓]

การปรับปรุงขีดความสามารถทางไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ

เมื่อวันที่ ๒๑ - ๒๗ ก.พ.๖๔ ที่ผ่านมา[๒] เป็นช่วงสัปดาห์ที่วิศวกรของกระทรวงกลาโหมสหรัฐฯ ที่แสดงถึงความพยายามในการพัฒนากำลังพลด้านวิศวกรรมที่หลากหลายเพื่อเพิ่มความเข้าใจ ความสนใจในวิศวกรรม และเทคโนโลยี เนื่องจากกำลังพลด้านไซเบอร์ของกองทัพมีความสำคัญต่อการปกป้องความมั่นคงของชาติ ซึ่ง John Marx รักษาการผู้อำนวยการใหญ่ด้านความทันสมัยทางไซเบอร์ สำนักงานปลัดกระทรวงกลาโหมสหรัฐฯ ได้กล่าวไว้ในสัปดาห์วิศวกรที่ผ่านมาว่า การปรับปรุงขีดความสามารถทางไซเบอร์ภายในกระทรวงกลาโหมมีเป้าหมายสำคัญ ๓ ด้าน ได้แก่

เป้าหมายแรก การพัฒนาความสามารถในแผนการพัฒนา การปรับใช้ระบบปฏิบัติการทางไซเบอร์ รวมถึงความสามารถในการเตรียมพร้อม และตอบสนองต่อสถานการณ์ด้านภัยคุกคามทางไซเบอร์ ระบบโครงสร้างพื้นฐานที่สร้างขึ้นเพื่อรองรับการโจมตีทางไซเบอร์ประเภทต่าง ๆ ในปัจจุบัน ความสามารถในการจัดการกับภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นในสภาพแวดล้อมของการปฏิบัติงาน เป็นต้น

เป้าหมายที่สอง การพัฒนาขีดความสามารถสำหรับการปฏิบัติการทางไซเบอร์ และการควบคุมแถบคลื่นแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) เพื่อสนับสนุนวัตถุประสงค์เชิงกลยุทธ์ในระดับชาติ ซึ่งจะช่วยให้กระทรวงกลาโหมสหรัฐฯ สามารถบรรลุข้อได้เปรียบด้านข้อมูลในทุกพื้นที่ปฏิบัติการ (Operation Domain)

เป้าหมายที่สาม เพื่อสนับสนุนสองประการแรก คือการสร้างความเชี่ยวชาญด้านไซเบอร์และควบคุมแถบคลื่นแม่เหล็กไฟฟ้าที่ไม่มีใครเทียบได้ทั่วโลก เพื่อแก้ไขปัญหาการขาดทีมงานผู้เชี่ยวชาญด้านนวัตกรรมการสร้างสรรค์ ซึ่งต้องอาศัยความเข้าใจการขับเคลื่อนด้วยความรู้ที่กว้างขวางเกี่ยวกับซอฟต์แวร์ ซึ่งทำให้ระบบที่ซับซ้อนสามารถทำงานได้ และต้องมีผู้ที่เข้าใจถึงขีดจำกัดของซอฟต์แวร์อย่างแท้จริง จึงจะมีส่วนทำให้เป้าหมายทั้งสองประการแรกสามารถบรรลุได้ นอกเหนือจากภารกิจหลักทั้งสามนี้ กระทรวงกลาโหมสหรัฐฯ ยังสนับสนุนการสรรหาบุคลากรที่มีความสามารถพิเศษในโลกไซเบอร์ ตลอดจนบุคลากรที่มีความสามารถที่มีความเข้าใจซอฟต์แวร์ที่ซับซ้อนได้เป็นอย่างดี และสามารถสร้างผลงานที่ยอดเยี่ยมได้ ซึ่งถือเป็นความสามารถของกระทรวงกลาโหมสหรัฐฯ ในการมีระบบที่สามารถต้านทานการโจมตีทางไซเบอร์ และบรรลุข้อได้เปรียบด้านข้อมูลในสนามรบ

บทวิเคราะห์

จากเป้าหมายของการปรับปรุงขีดความสามารถทางไซเบอร์ให้ทันสมัยภายในกระทรวงกลาโหมสหรัฐฯ ทำให้เห็นถึงการกำหนดแนวทางของการวางแผนป้องกันด้านไซเบอร์ในอนาคตโดยให้ความสำคัญกับนวัตกรรมทางเทคโนโลยีและการพัฒนาขีดความสามารถใหม่ ตลอดจนการพัฒนาขีดความสามารถของกำลังพลในงานด้านไซเบอร์เพื่อให้มีประสิทธิภาพที่ดีขึ้น สามารถตอบสนองต่อความท้าทายทั้งในปัจจุบัน และอนาคต ซึ่งหากปราศจากการฟื้นฟูการพัฒนาและการเตรียมความพร้อม อาจทำให้สหรัฐฯ เผชิญกับความท้าทายจากภัยคุกคาม และการปกป้องอธิปไตยทางไซเบอร์ทั้งจากตัวแสดงที่เป็นรัฐ และไม่ใช่รัฐ

ประเทศที่มีเทคโนโลยีระดับสูงอย่างจีน รัสเซีย และญี่ปุ่น ที่ผ่านมาทั้งสามประเทศก็ตกอยู่ในพื้นที่ของการถูกก่ออาชญากรรมทางไซเบอร์ ซึ่งปัญหาอาจเกิดจากความบกพร่องของระบบ หรือความปลอดภัยทางไซเบอร์ที่ยังไม่เพียงพอ และจากประเด็นที่เกิดขึ้นนี้ก็ทำให้แต่ละประเทศ รวมทั้งกองทัพ หันมาให้ความสำคัญกับการปรับปรุงระบบให้มีประสิทธิภาพมากขึ้น โดยได้มีการใช้เงินลงทุนที่เพิ่มสูงขึ้นเพื่อพัฒนาระบบฮาร์ดแวร์ และซอฟต์แวร์ทางไซเบอร์ รวมถึงการพัฒนาบุคลากรของกองทัพด้านไซเบอร์ให้มีความพร้อมสำหรับการป้องกันการถูกโจมตีดังกล่าว แสดงให้เห็นว่าอนาคตการแข่งขันในมิติของไซเบอร์จะมีความสำคัญและมีความจำเป็นต่อกองทัพเป็นอย่างยิ่ง

ภัยคุกคามด้านความมั่นคงทางไซเบอร์ ส่งผลกระทบต่อกองทัพในกลุ่มประเทศอาเซียน และประเทศไทยด้วย เนื่องจาก ๑) การทำงานของระบบไซเบอร์ได้ถูกพัฒนาให้สามารถสร้างความเสียหายต่อข้อมูลอย่างรุนแรง และส่งผลกระทบในวงกว้างมากขึ้น ๒) มีความซับซ้อนในการติดตามถึงผู้กระทำความผิด จึงทำให้การจับกุมผู้กระทำความผิดทำได้ยาก และ ๓) มีความยุ่งยากในการเฝ้าระวัง และป้องกันสำหรับการรับมือกับภัยคุกคามดังกล่าว ดังนั้น จึงจำเป็นต้องอาศัยความรู้เฉพาะทางด้านไซเบอร์ของกำลังพลในกองทัพเป็นอย่างมาก เนื่องจาก ปัญหาการถูกโจมตีทางไซเบอร์มักเกิดจากการขาดการบริหารระบบเครือข่ายที่ดี และขาดความเข้าใจในกระบวนการทำงานของระบบไซเบอร์ ซึ่งจากผลกระทบดังกล่าวอาจส่งผลต่อความเชื่อมั่นในการใช้งานเทคโนโลยีด้านความมั่นคง และอาจสร้างความเสียหายเกินกว่าที่กองทัพจะสามารถรับมือได้

ข้อเสนอแนะต่อกองทัพ

ภัยคุกคามด้านความมั่นคงทางไซเบอร์จะมีความสำคัญและจำเป็นอย่างยิ่งต่อกองทัพในอนาคต ดังนั้น เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามดังกล่าว กองทัพควรดำเนินการ ดังนี้

๑) กองทัพควรสนับสนุนการพัฒนากำลังพลด้านไซเบอร์เพื่อแก้ไขปัญหาการขาดแคลนกำลังพลที่มีความรู้ ความสามารถด้านไซเบอร์ในหลายหน่วยงาน จึงควรจัดทำ “ประชาคมความมั่นคงทางไซเบอร์ (Cyber Defense Community)” เพื่อเป็นการรวมผู้เชี่ยวชาญในการพัฒนาขีดความสามารถ เพื่อเตรียมความพร้อมรับมือกับภัยคุกคามในทุกรูปแบบ และสามารถดึงกลุ่มผู้เชี่ยวชาญทางไซเบอร์มาเพื่อใช้แก้ปัญหาทางไซเบอร์ได้

๒) กองทัพควรสนับสนุนการบริหารระบบเครือข่ายทางไซเบอร์ รวมถึงการสนับสนุนระบบฐานข้อมูล และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีประสิทธิภาพที่สูงขึ้น เพื่อรองรับการเผชิญกับภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงของชาติ

๓) กองทัพควรส่งเสริมการแสวงหาประโยชน์ด้านองค์ความรู้จากผู้เชี่ยวชาญทางไซเบอร์ โดยอาศัยความร่วมมือจากหน่วยงานต่าง ๆ ทั้งภายใน และภายนอกกองทัพ ซึ่งจะเป็นประโยชน์ในการแลกเปลี่ยนความรู้จากการได้ปฏิบัติร่วมกัน เพื่อให้กำลังพลได้เพิ่มพูนความรู้ความเข้าใจถึงการทำงานของระบบทางไซเบอร์มากขึ้น

ข้อมูลอ้างอิง

[๑] เอกสารศึกษาเฉพาะกรณี (Case Study) เรื่อง ปัญญาประดิษฐ์ (Artificial Intelligence: AI) กับจุดเปลี่ยนของสงครามในอนาคต พิมพ์ครั้งที่ ๑ กรุงเทพฯ ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, ๒๕๖๓.

[๒] https://www.defense.gov/Explore/News/Article/Article/2512764/cyber-workforce-vital-to-protecting-national-security/

[๓] เอกสารศึกษาเฉพาะกรณี เรื่อง แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พิมพ์ครั้งที่ ๑ – กรุงเทพฯ ศูนย์ศึกษายุทธศาสตร สถาบันวิชาการป้องกันประเทศ, ๒๕๖๐.

เพื่อประโยชน์ในการพัฒนา SSC Focus กรุณาส่งข้อคิดเห็นของท่านมายัง คณะผู้จัดทำ (ศศย. สปท.) T/F : ๐ ๒๒๗๕ ๕๗๑๕ - ๑๖

๑. ท่านสนใจประเด็นใดเพิ่มเติม/เห็นว่าควรศึกษาเพิ่มเติม

☐ การเมือง ☐ เศรษฐกิจ ☐ สังคม ☐ วิทยาศาสตร์/เทคโนโลยี ☐ การทหาร ☐ พลังงาน/สิ่งแวดล้อม

☐ อื่น ๆ .....

๒. ข้อเสนอแนะเพิ่มเติม

.....

บทวิเคราะห์โดย กองภูมิภาคศึกษา ศูนย์ศึกษายุทธศาสตร์ฯ