Thailand SSC focus

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

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
กองบัญชาการกองทัพไทย

เอกสารวิเคราะห์สถานการณ์ยุทธศาสตร์และความมั่นคง ฉบับที่ ๘/๖๕ (๑-๓๑ พ.ค.๖๕)

เหล่าทัพที่ ๔ (Fourth service) “The Digital and Intelligence Service (DIS)” ของกองทัพสิงคโปร์

กองทัพสิงคโปร์ (Singapore Armed Forces: SAF) มีแผนจัดตั้งหน่วยงานใหม่ชื่อว่า “The Digital and Intelligence Service (DIS)” เป็นเหล่าทัพที่ ๔ จากเดิมที่มี กองทัพบก กองทัพเรือ และกองทัพอากาศ ซึ่งเหล่าทัพที่ ๔ นี้มีหน้าที่การทำข่าวกรองที่แม่นยำ ตรงประเด็นและทันเวลาในมิติดิจิทัล (Digital Domain) อีกทั้งยังเชื่อมโยงกับเหล่าทัพอื่นด้วย C4 (Command, Control, Communications, Computers)[๑] เพื่อปฏิบัติการในรูปแบบเครือข่าย อย่างไรก็ตามสิงคโปร์ได้มีการเตรียมความพร้อมก่อนการจะจัดตั้งหน่วยงาน DIS มาตั้งแต่ปี พ.ศ. ๒๕๕๕ ซึ่งถือเป็นก้าวสำคัญในการเปลี่ยนแปลงกองทัพสิงคโปร์ให้เป็นกองทัพที่มีเครือข่ายและมีความรู้ เพื่อรองรับภัยคุกคามรูปแบบใหม่ในอนาคต...

ลำดับเหตุการณ์สำคัญของการพัฒนากองทัพสิงคโปร์ ไปสู่เหล่าทัพที่ ๔[๒]

ภัยคุกคามรูปแบบใหม่จากมิติดิจิทัล สามารถส่งผลกระทบต่อเหตุการณ์ในโลกทางกายภาพได้โดยง่าย ภัยคุกคามดังกล่าวได้เพิ่มขึ้นอย่างต่อเนื่องทั้งในแง่ของขนาด ความซับซ้อนและองค์กร ซึ่งกระทรวงกลาโหมสิงคโปร์ (Ministry of Defence : MINDEF) และกองทัพสิงคโปร์ตระหนักและได้มีการเตรียมความพร้อมด้านโครงสร้างองค์กรและขีดความสามารถของกำลังพลในระบบบัญชาการและควบคุม (Control, Command, Communication, Computer, Intelligence: C4I) นับตั้งแต่การจัดตั้ง C4I Community และวิวัฒนาการเรื่อยมาจนนำมาสู่การเตรียมการจัดตั้งหน่วยงาน “The Digital and Intelligence Service (DIS)” ในไตรมาสที่ ๔ ของปี ๒๕๖๕ ให้มีสถานะเป็นเหล่าทัพที่ ๔ ของกองทัพสิงคโปร์นอกเหนือจากกองทัพบก กองทัพเรือ และกองทัพอากาศ เพื่อให้กองทัพสิงคโปร์สามารถฝึกและปฏิบัติการต่อสู้อย่างเชื่อมโยงกันเป็นเครือข่ายและบูรณาการในการรับมือกับภัยคุกคามทางดิจิทัล โดยมีลำดับเหตุการณ์ที่สำคัญ ในการเตรียมความพร้อมอย่างรอบด้านก่อนการจัดตั้งเหล่าทัพที่ ๔ ดังนี้

๑. ในปี พ.ศ. ๒๕๕๕ ได้มีการจัดตั้ง C4I Community ซึ่งถือเป็นก้าวสำคัญในการเปลี่ยนแปลงกองทัพให้เป็นกองกำลังที่มีเครือข่ายและมีความรู้ โดย C4I Community รวบรวมหน่วย ระบบบัญชาการและควบคุม (C4I) หน่วยข่าวกรอง และบุคลากรจากทั่วทั้งกองทัพสิงคโปร์ ซึ่งรวมถึงนักวิเคราะห์ภาพ (Image Analysts) เจ้าหน้าที่อากาศยานไร้คนขับ (Unmanned Aerial Vehicle Operators: UAV Operators) เจ้าหน้าที่สื่อสาร (Communications Operators) และนักวิเคราะห์ข่าวกรองของกองทัพเรือ (Naval Intelligence Analysts) โดย C4I Community มีความรับผิดชอบหลักในการพัฒนาความสามารถทางวิชาชีพ ความเชี่ยวชาญ และความรู้ของผู้ปฏิบัติงาน[๓]

๒. ในปี พ.ศ. ๒๕๕๘ กองทัพได้พัฒนาศักยภาพด้วยการส่งทีมวิเคราะห์ภาพเข้าร่วมภารกิจแนวร่วมต่อต้านกลุ่มก่อการร้ายไอเอส (Islamic State of Iraq and Syria : ISIS) ในคูเวต[๔]

๓. ในปี พ.ศ. ๒๕๖๐ ได้มีการก่อตั้ง Defense Cyber Organisation (DCO) เพื่อเป็นผู้นำและประสานงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพ และ การเปิดตัวคำสั่ง SAF C4 ซึ่งเป็นการผสานรวม C4 และความสามารถในการป้องกันทางไซเบอร์[๕]

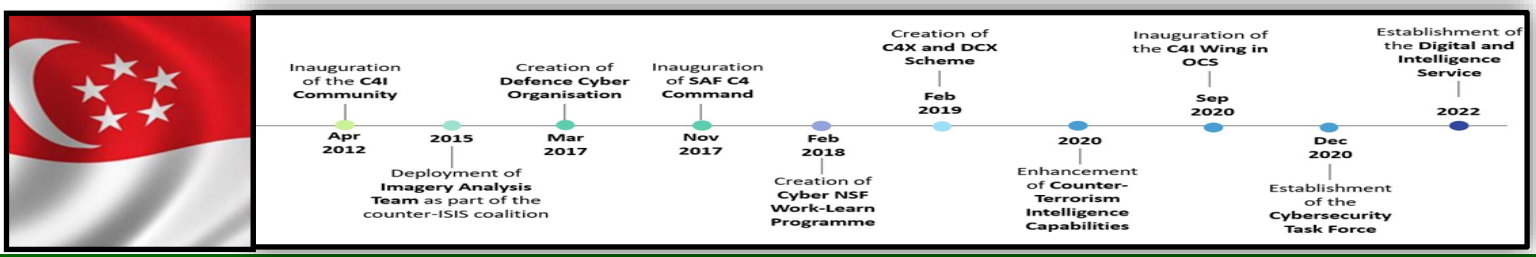
๔. ในปี พ.ศ. ๒๕๖๑ มีโครงการ Cyber Full-time National Service (Cyber NSF) เพื่อดึงดูดและฝึกอบรมกำลังพลที่มีความสนใจร่วมเรียนรู้ เพื่อเป็นผู้เชี่ยวชาญด้านไซเบอร์ หลังจากจบหลักสูตรแล้วกำลังพลจะได้รับมอบหมายให้มีบทบาทรับผิดชอบต่าง ๆ เพื่อปกป้องเครือข่ายและระบบภายในกระทรวงกลาโหมและกองทัพสิงคโปร์[๖]

๕. ในปี พ.ศ. ๒๕๖๒ ได้มีการพัฒนา C4X โดยเพิ่มด้านความเชี่ยวชาญ (Expert) และผู้เชี่ยวชาญด้านการป้องกันไซเบอร์ (Defence Cyber Expert : DCX) เพื่อสนับสนุนการพัฒนาแรงงานในโลกไซเบอร์ที่มีทักษะสูงและสามารถเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของสิงคโปร์

๖. ในปี พ.ศ. ๒๕๖๓ ได้มีการเพิ่มขีดความสามารถด้านข่าวกรอง และการต่อต้านการก่อการร้าย รวมถึงจัดตั้งคณะทำงานด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Task Force) และได้มีการบรรจุ C4I เข้าไปในหลักสูตรโรงเรียนนายร้อย (Officer Cadet School : OCS)

๗. ในปี พ.ศ. ๒๕๖๕ มีการเตรียมจัดตั้ง The Digital and Intelligence Service (DIS) ที่จะมีสถานะเป็นเหล่าทัพที่ ๔ เพื่อช่วยให้กองทัพสามารถปกป้องสิงคโปร์จากภัยคุกคามทางดิจิทัลได้มีประสิทธิภาพมากขึ้น

ทั้งนี้ การเตรียมความพร้อมจากการจัดตั้งหน่วยงานที่เกี่ยวกับด้านดิจิทัลและการพัฒนากำลังพลให้มีความรู้เท่าทันเทคโนโลยีที่มีการเปลี่ยนแปลงไป ถือเป็นความพยายามในการรักษาความมั่นคงของประเทศจากภัยคุกคามใหม่ในอนาคต



บทวิเคราะห์

จากการที่กองทัพสิงคโปร์ได้เตรียมจัดตั้ง DIS ให้มีสถานะเป็นเหล่าทัพ แสดงว่าสิงคโปร์ได้เล็งเห็นความสำคัญของภัยคุกคามทางดิจิทัล โดยการจัดตั้ง DIS ได้ส่งผลดีต่อกองทัพสิงคโปร์ แต่ก็ก่อให้เกิดความท้าทายต่อภูมิภาคด้วยเช่นกัน

โอกาสของกองทัพสิงคโปร์ ดังนี้

สำหรับกองทัพสิงคโปร์การจัดตั้งหน่วย DIS จะเสริมสร้างให้กองทัพดำเนินงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น เนื่องจาก DIS จะผสานรวมความสามารถของกองทัพสิงคโปร์ให้แน่นแฟ้นยิ่งขึ้น เพื่อจัดการกับภัยคุกคามด้านความมั่นคงต่างๆ ซึ่งรวมถึง ภัยคุกคามจากมิติดิจิทัล ซึ่งการที่ DIS มุ่งเน้นเฉพาะเจาะจงในการตระหนักถึงศักยภาพของเทคโนโลยีดิจิทัลที่เกิดขึ้นใหม่ เช่น คลาวด์ (Cloud) วิทยาศาสตร์ข้อมูล (Data Science) และปัญญาประดิษฐ์ (Artificial Intelligence : AI) สิ่งเหล่านี้จะช่วยเสริมสร้างความมั่นคงให้กับกองทัพสิงคโปร์ นอกจากนี้ การเติบโตและเสริมสร้างทรัพยากรมนุษย์ก็มีส่วนสำคัญในการทำให้ DIS สามารถขยายกำลังคนด้านดิจิทัลและหน่วยข่าวกรองได้ด้วยการเสริมสร้างการพัฒนาทางวิชาชีพ การสรรหาบุคลากร และโอกาสทางอาชีพ ทั้งนี้การจัดตั้ง DIS มีความสอดคล้องกับแนวคิดเรื่องการป้องกันประเทศแบบเบ็ดเสร็จ (Total Defence Themes) สำหรับในปี พ.ศ. ๒๕๖๕ คือ **การร่วมกันทำให้สิงคโปร์ให้แข็งแกร่ง “Together We Keep Singapore Strong”** โดยสิงคโปร์ได้เพิ่มการป้องกันประเทศด้านดิจิทัล (Digital Defence) เข้าเป็นส่วนหนึ่งของการป้องกันประเทศแบบเบ็ดเสร็จ (Total Defence) เมื่อปี ๒๕๖๒ จากเดิมที่มีการป้องกันประเทศเฉพาะด้านการทหาร พลเรือน เศรษฐกิจ สังคม และจิตวิทยา ซึ่งการจัดตั้ง DIS จะมีบทบาทในการ ๑) ทำข่าวกรองที่แม่นยำ ตรงประเด็น และทันเวลาในมิติดิจิทัล ๒) เชื่อมโยงกับเหล่าทัพอื่นด้วย C4 (command, control, communications, computers) เพื่อปฏิบัติการในรูปแบบเครือข่าย ๓) รับผิดชอบในการป้องกันทางดิจิทัลให้กองทัพ ผ่านการป้องกันทางไซเบอร์และการปกป้องเครือข่ายและระบบอิเล็กทรอนิกส์ของกองทัพตลอดจนการป้องกันประเทศด้านจิตวิทยา เพื่อเสริมสร้างความมุ่งมั่นและความยืดหยุ่นของกำลังพลในการปฏิบัติการ

ความท้าทายของสิงคโปร์จากการจัดตั้ง DIS

๑. เกิดความหวาดระแวงในภูมิภาค เมื่อกองทัพสิงคโปร์มีความแข็งแกร่งทางด้านดิจิทัลมากขึ้น อาจเป็นเหตุผลให้เกิดบรรยากาศความหวาดระแวงด้านความมั่นคง (Security Dilemma) และความไม่ไว้เนื้อเชื่อใจระหว่างกันกับบางประเทศในภูมิภาค

๒. การพัฒนาอาวุธสมัยใหม่ร่วมกับต่างประเทศ โดยวัตถุประสงค์หลักของกองทัพสิงคโปร์ คือ การปรับเปลี่ยนไปสู่กองทัพยุคที่สาม (The 3rd Generation SAF) กองทัพสิงคโปร์ได้ปรับปรุงรูปแบบกองทัพ ด้วยการลดกำลังพล และใช้เทคโนโลยีเข้ามาทดแทนกำลังพล โดยเฉพาะอากาศยานไร้คนขับ ปัญญาประดิษฐ์ วิทยาการหุ่นยนต์ (Robotics) และการบูรณาการเครือข่ายอย่างเต็มรูปแบบ โดยอาจพัฒนาอาวุธสมัยใหม่ร่วมกับต่างประเทศ อันจะเห็นได้จากการฝึกทวิภาคีระหว่างสหรัฐฯ และสิงคโปร์ ที่มีการใช้เทคโนโลยีแบบบูรณาการของทั้งสองประเทศที่อาจสร้างความกังวลกับประเทศในภูมิภาคได้[๗]

๓. การยกระดับความร่วมมือความมั่นคงปลอดภัยทางไซเบอร์กับประเทศมหาอำนาจ อันจะเห็นได้จากการลงนามบันทึกความเข้าใจสามฉบับเมื่อเดือนสิงหาคม พ.ศ. ๒๕๖๔ ระหว่างสิงคโปร์และสหรัฐฯ เพื่อยกระดับการทำงานร่วมกันระหว่างหน่วยงานด้านการเงิน หน่วยงานด้านความมั่นคงทางไซเบอร์ และกองทัพ ซึ่งหากมีเหล่าทัพที่ ๔ อาจทำให้เกิดความร่วมมือต่าง ๆ เพิ่มมากขึ้น อย่างไรก็ตาม การยกระดับความร่วมมือนั้นเป็นที่น่าจับตามองเพราะอาจส่งผลกระทบทางอ้อมต่อภูมิภาคได้[๘]

ข้อเสนอแนะต่อกองทัพ

The Digital and Intelligence Service (DIS) จะส่งเสริมให้กองทัพสิงคโปร์มีประสิทธิภาพมากขึ้นในการปกป้องประเทศจากภัยคุกคามที่มีความซับซ้อนมากขึ้นในอนาคต สำหรับประเทศไทยได้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ เพื่อกำหนดนโยบาย มาตรการ แนวทาง ในการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐ และภาคเอกชน ในส่วนของกองทัพไทยและเหล่าทัพ ก็มีการจัดตั้งหน่วยงานด้านการป้องกันภัยคุกคามทางไซเบอร์ อาทิ (๑) ศูนย์ไซเบอร์ กห. (๒) ศูนย์ไซเบอร์ทหาร ทท. (๓) ศูนย์ไซเบอร์ ทบ. และ ทอ. และ (๔) กองสงครามไซเบอร์ ทร. เป็นต้น ดังนั้นเพื่อให้กองทัพสามารถรับมือกับภัยคุกคามด้านไซเบอร์ได้อย่างมีประสิทธิภาพ จึงมีข้อเสนอแนะให้กับกองทัพใน ๓ ประเด็น ดังนี้

๑) *ด้านบุคลากร* : กองทัพควรผลิตและสร้างบุคลากรให้มีความชำนาญ รวมทั้งเสริมทักษะและขีดความสามารถด้านดิจิทัลโดเมนเพื่อให้รู้เท่าทันและรองรับภัยคุกคามทางไซเบอร์ที่มีพัฒนาการอย่างต่อเนื่อง อาทิ การจัดหลักสูตรเฉพาะในการพัฒนากำลังพล เป็นต้น

๒) *ด้านเทคโนโลยี* : กองทัพควรเตรียมพร้อมทางด้านเทคโนโลยีทั้ง (Hardware) โครงสร้างพื้นฐาน อุปกรณ์ เครื่องมือและเทคโนโลยี รวมทั้งด้าน (Software) โปรแกรมต่าง ๆ และระบบปฏิบัติการที่มีความทันสมัยและมีประสิทธิภาพ เพื่อรองรับกับภัยคุกคามทางไซเบอร์ในทุกรูปแบบ

๓) *ด้านประสิทธิภาพ* : กองทัพควรมีการบูรณาการและประสานการทำงานร่วมกันระหว่างเหล่าทัพและหน่วยงานด้านความมั่นคงอื่น ๆ ให้มีการเชื่อมโยงเครือข่ายและบูรณาการการทำงานระหว่างกัน เพื่อประสานการปฏิบัติการด้านไซเบอร์ให้มีประสิทธิภาพ ในเรื่องการข่าวกรองผ่านระบบไซเบอร์ รวมถึงการรับมือเมื่อมีเหตุการณ์ถูกโจมตี หรือภัยคุกคามทางไซเบอร์

อ้างอิง

[๑] https://www.nia.go.th/news/page/304/

[๒] Fact Sheet: Timely Establishment of Digital and Intelligence Service, www.mindef.gov.sg

[๓] Fact Sheet: SAF C4I Community, www.mindef.gov.sg

[๔] SAF's Participation in the Counter-ISIS Coalition , www.mindef.gov.sg

[๕] Fact Sheet: SAF C4 Command Integrates C4 and Cyber Defence Capabilities, www.mindef.gov.sg

[๖] Written Reply by Minister for Defence Dr Ng Eng Hen to Parliamentary Question on the Cyber NSF Scheme and Cyber Military Experts Scheme, www.mindef.gov.sg

[๗] สิงคโปร์และสหรัฐฯ ขยายความร่วมมือด้านความมั่นคงทางไซเบอร์, https://ipdefenseforum.com

[๘] กองทัพสิงคโปร์และสหรัฐฯ เข้าร่วมการฝึกสะเทินน้ำสะเทินบกระหว่างการฝึกซ้อมกะรัต พ.ศ. 2563, https://ipdefenseforum.com

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