SSC Weekly Focus

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

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
กองบัญชาการกองทัพไทย

บทความวิเคราะห์สถานการณ์ยุทธศาสตร์และความมั่นคงของประเทศรายสัปดาห์ ฉบับที่ ๑๓/๖๖ (๒๓ – ๒๗ ม.ค.๖๖)

ความสำเร็จในการจัดตั้งกองทัพที่ ๔ ของสิงคโปร์

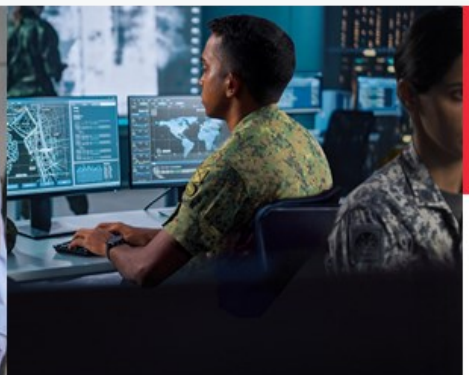
การจัดตั้งกองทัพดิจิทัลและข่าวกรอง (Digital and Intelligence Service: DIS)

เมื่อวันศุกร์ที่ ๒๘ ตุลาคม ๒๕๖๕ กองทัพสิงคโปร์ (Singapore Armed Force : SAF) ได้จัดตั้งกองทัพดิจิทัลและข่าวกรอง (Digital and Intelligence Service : DIS) ขึ้น เพื่อให้ได้ข่าวกรองอย่างทันท่วงที ปกป้องสิงคโปร์จากภัยคุกคาม การโจมตีทางไซเบอร์ และสงครามอิเล็กทรอนิกส์ และมีหน้าที่ปกป้องดูแลดิจิทัลโดเมน (Digital Domain) ในฐานะที่เป็นส่วนหนึ่งของกองทัพสิงคโปร์อย่างบูรณาการ กองทัพดิจิทัลและข่าวกรองจะช่วยเพิ่มความปลอดภัยให้กับกองทัพสิงคโปร์ บูรณาการระบบควบคุมบังคับบัญชา และขีดความสามารถทางไซเบอร์ และมีผลทำให้กองทัพสิงคโปร์มีกำลังพลที่สามารถตอบสนองการปฏิบัติงานด้านดิจิทัลของสิงคโปร์ได้อย่างรวดเร็ว

ลำดับเหตุการณ์สำคัญในการจัดตั้งกองทัพดิจิทัลและข่าวกรอง(Digital and Intelligence Service: DIS)

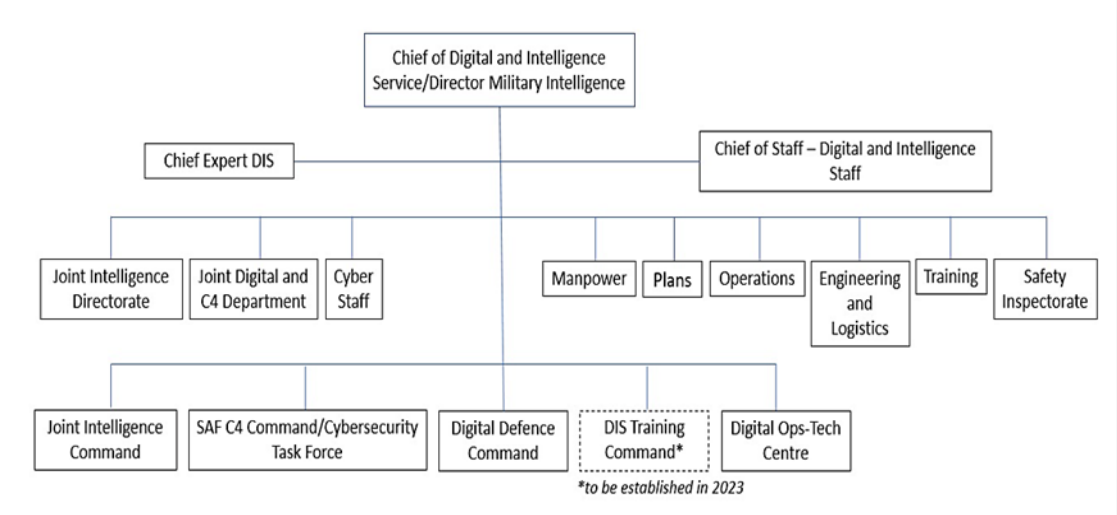
กองทัพสิงคโปร์ได้มีการดำเนินการ[๑] และลำดับเหตุการณ์ที่สำคัญในการเตรียมความพร้อมอย่างรอบด้านก่อนการจัดตั้งเหล่าทัพที่ ๔ ไว้ ดังนี้ **๑) ในปี พ.ศ. ๒๕๕๕** ได้มีการจัดตั้ง C4I Community ซึ่งถือเป็นก้าวสำคัญในการเปลี่ยนแปลงกองทัพให้เป็นกองกำลังที่มีเครือข่ายและมีความรู้ รวบรวมหน่วยระบบบัญชาการและควบคุมหน่วยข่าวกรอง และบุคลากรจากทั่วทั้งกองทัพสิงคโปร์ **๒) ในปี พ.ศ. ๒๕๕๘** กองทัพได้พัฒนาศักยภาพด้วยการ ส่งทีมวิเคราะห์ภาพเข้าร่วมภารกิจแนวร่วมต่อต้านกลุ่มก่อการร้ายไอเอส (Islamic State of Iraq and Syria : ISIS) ในคูเวต **๓) ในปี พ.ศ. ๒๕๖๐** ได้มีการก่อตั้ง “องค์กรป้องกันทางไซเบอร์” (Defense Cyber Organisation : DCO) ขึ้นเพื่อเป็นผู้นำ สนับสนุน และประสานงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพและรัฐบาล **๔) ในปี พ.ศ. ๒๕๖๑** มีโครงการ Cyber Full-time National Service (Cyber NSF) เพื่อดึงดูดและฝึกอบรมกำลังพลที่มีความสนใจ ร่วมเรียนรู้ เพื่อเป็นผู้เชี่ยวชาญด้านไซเบอร์ **๕) ในปี พ.ศ. ๒๕๖๒** ได้มีการพัฒนา[๒] C4X (Command, Control, Communications, Computers) Experts หรือ C4X) โดยเพิ่มด้านเชี่ยวชาญ (Expert) และผู้เชี่ยวชาญด้านการป้องกันไซเบอร์ (Defence Cyber Expert : DCX) เพื่อสนับสนุนการพัฒนาแรงงานทางไซเบอร์ที่มีทักษะสูงและสามารถเสริมสร้างความมั่นคง ปลอดภัยทางไซเบอร์ของสิงคโปร์ **๖) ในปี พ.ศ. ๒๕๖๓** ได้มีการเพิ่มขีดความสามารถด้านข่าวกรอง และการต่อต้านการก่อการร้าย รวมถึงจัดตั้งคณะทำงานด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Task Force) และได้มีการบรรจุ C4I เข้าไปในหลักสูตรโรงเรียนนายร้อย (Officer Cadet School : OCS) และ **๗) วันที่ ๒ มีนาคม ๒๕๖๕** แถลงการณ์โดย Ng Eng Hen รัฐมนตรีว่าการกระทรวงกลาโหมสิงคโปร์ระบุว่า กองทัพสิงคโปร์มีแผนจัดตั้ง “เหล่าทัพที่ ๔” (Fourth service) ซึ่งจะรวบรวมและขยายขีดความสามารถด้านต่าง ๆ ของประเทศในด้านดิจิทัล

โดยได้แต่งตั้งให้ พลตรี Lee Yi-Jin เป็นผู้บัญชาการกองทัพดิจิทัลและข่าวกรอง[๓] มีอายุราชการ ๒๓ ปี ซึ่งเคยได้รับแต่งตั้งในตำแหน่งสำคัญหลายครั้ง เช่น ผู้ช่วยเสนาธิการด้านแผน (Assistant Chief of the General Staff : Plans) และหัวหน้ากลุ่มนโยบายและยุทธศาสตร์ของกระทรวงกลาโหม (Army and Group Chief, Policy and Strategy) ปฏิบัติหน้าที่ผู้บัญชาการคณะทำงานติดตามด้านสุขภาพ (Health Surveillance Task Force) เมื่อปี พ.ศ. ๒๕๖๓ นอกจากนี้ ยังเป็นผู้วางรากฐานในการก่อตั้งกองทัพดิจิทัลและข่าวกรองอีกด้วย



โครงสร้างของกองทัพดิจิทัลและข่าวกรอง (DIS)

กองทัพดิจิทัลและข่าวกรอง[๖] มีผู้บัญชาการกองทัพดิจิทัลและข่าวกรอง (Chief of Digital and Intelligence Service : CDI) เป็นผู้บังคับบัญชา มีหัวหน้าฝ่ายเสนาธิการ (Chief of Staff – Digital and Intelligence Staff: COS-DS) และหัวหน้าผู้เชี่ยวชาญ (Chief Expert DIS : CXDI) ให้คำแนะนำ มีหน่วยขึ้นตรง ประกอบด้วย กรมเสนาธิการไซเบอร์ กรมข่าวร่วม กรมดิจิทัล และระบบควบคุมบังคับบัญชาร่วม มี ๔ กองบัญชาการ ได้แก่ กองบัญชาการข่าวกรองร่วม กองบัญชาการควบคุมบังคับบัญชา/กองกำลังเฉพาะกิจรักษาความมั่นคงปลอดภัยไซเบอร์ กองบัญชาการป้องกันดิจิทัล และกองบัญชาการฝึกกองทัพดิจิทัลและข่าวกรอง และ ๑ ศูนย์ปฏิบัติการทางเทคนิคดิจิทัล



บทวิเคราะห์จากการจัดตั้งกองทัพดิจิทัลและข่าวกรอง (DIS) ของสิงคโปร์

๑. ทำให้สามารถจัดทำข่าวกรองที่ถูกต้อง แม่นยำ ทันต่อเวลา เพื่อแจ้งเตือนล่วงหน้า และสนับสนุนการตกลงใจในการปฏิบัติการทางทหาร และยกระดับความรู้ด้านดิจิทัลของกำลังพลในกองทัพให้สามารถตอบสนองความต้องการในการปฏิบัติงานด้านดิจิทัลของสิงคโปร์ได้อย่างรวดเร็ว เพื่อเป็นการยกระดับการทำงานด้านความมั่นคงทางไซเบอร์ของกองทัพ

๒. ทำให้สามารถปกป้องเครือข่าย พรมแดนดิจิทัลของกองทัพ ตลอดจนสร้างระบบนิเวศทางดิจิทัลของประเทศที่แข็งแกร่งขึ้นในรัฐบาลหน่วยงานด้านความมั่นคง และภาคส่วนสำคัญของเศรษฐกิจ

๓. เป็นการสร้างโอกาสในการพัฒนาเทคโนโลยีสมัยใหม่ทางดิจิทัลร่วมกับต่างประเทศเพิ่มมากขึ้น โดยกองทัพสิงคโปร์มีเป้าหมายหลัก คือ การปรับเปลี่ยนไปสู่กองทัพยุคที่สาม (The 3rd Generation SAF) ปรับปรุงรูปแบบกองทัพ ใช้เทคโนโลยีเข้ามาทดแทนกำลังพล เช่น อากาศยานไร้คนขับ ปัญญาประดิษฐ์ วิทยาการหุ่นยนต์ (Robotics) เป็นต้น

ข้อเสนอแนะ: กองทัพไทยควรพิจารณาดำเนินการ ดังนี้

๑. ด้านบุคลากร : ไทยควรผลิตและสร้างบุคลากรให้มีความชำนาญ รวมทั้งเสริมทักษะและขีดความสามารถด้านดิจิทัลเพื่อให้รู้เท่าทันและรองรับภัยคุกคามทางไซเบอร์ที่มีพัฒนาการอย่างต่อเนื่อง

๒. ด้านเทคโนโลยี : ไทยควรเตรียมพร้อมทางด้านเทคโนโลยีทั้ง (Hardware) โครงสร้างพื้นฐาน อุปกรณ์ เครื่องมือและเทคโนโลยีรวมทั้งด้าน (Software) โปรแกรมต่าง ๆ และระบบปฏิบัติการที่มีความทันสมัยและมีประสิทธิภาพ

๓. ด้านประสิทธิภาพ : ไทยควรมีการบูรณาการและประสานการทำงานร่วมกันระหว่างเหล่าทัพและหน่วยงานด้านความมั่นคงอื่น ๆ ให้มีการเชื่อมโยงเครือข่าย และประสานการปฏิบัติการข่าวกรองผ่านระบบไซเบอร์ รวมถึงการรับมือเมื่อมีเหตุการณ์ถูกโจมตีหรือป้องกันภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้น

อ้างอิง

[๑] ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. (๒๕๖๕). เหล่าทัพที่ ๔ (Fourth service) “The Digital and Intelligence Service (DIS)” ของกองทัพสิงคโปร์. https://www.sscthailand.org/uploads_ssc/research_20220606165450463311959 6.pdf

[๒] https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latestreleases /article-detail/2012/april/2012apr02-News-Releases-02178

[๓] The Straittimes. (2022). https://www.straitstimes.com/singapore/saf-s-digital-and-intelligence-service-formed-to-safeguard-s-pore-against-digital-threats.

[๔] Blockdit. (2565). https://www.blockdit.com/posts/6369d380d23092f52fd048be.