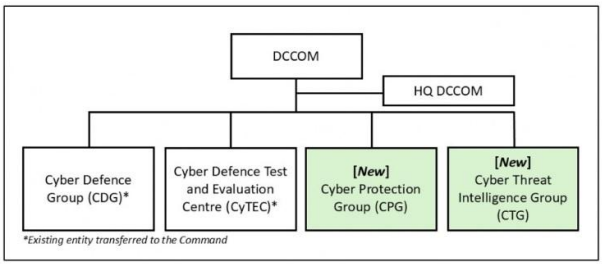
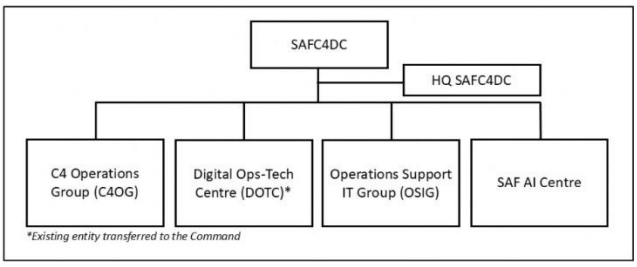
ประเด็น **ยุทธศาสตร์** ฉบับที่ **A19**	**24 มี.ค. 68**	**วิทยาลัยการทัพบก**
ประเด็น **ยุทธศาสตร์กองทัพสิงคโปร์**	**การจัดตั้ง เหล่าที่ 4 ของ กองทัพสิงคโปร์**	
ประเด็นสำคัญ	- **โครงสร้างของกองทัพดิจิทัลและข่าวกรอง (DIS)** **- ลำดับเหตุการณ์ไปสู่เหล่าทัพที่ 4** **- การเตรียมพร้อมของกองทัพไทย**	

Defence Minister Ng Eng Hen with (from left) Commander of SAF C4 and Digitalisation Command Wong Hong Kai; Chief of Defence Force Aaron Beng; Chief of Digital and Intelligence Service Lee Yi-Jin; and Commander of Defence Cyber Command Clarence Cai on March 18. PHOTO: LIANHE ZAOBAO

เมื่อ 18 มี.ค. 68 กองทัพสิงคโปร์เปิดตัวหน่วยงานใหม่อย่างเป็นทางการ โดยมี ดร. Ng Eng Hen รมว.กห.สิงคโปร์เป็นประธาน ได้แก่ Defence Cyber Command (DCCOM) และ SAF C4 & Digitalisation Command (SAFC4 DC) ซึ่งทั้งสองหน่วยถือเป็นเหล่าที่ 4 ของ SAF คือ Digital and Intelligence Service (DIS) เพื่อปกป้องระบบดิจิทัลของประเทศและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ที่สำคัญจากภัยคุกคามทางไซเบอร์ โดย รมว.กห.สิงคโปร์ ระบุว่า ผู้ก่ออาชญากรรมไซเบอร์ได้ปรับปรุงวิธีการของตน ใช้เทคนิคขั้นสูง นอกจากนี้ยังใช้ AI ช่องโหว่แบบ zero-day และมัลแวร์เรียกค่าไถ่ เพื่อโจมตีโครงสร้างพื้นฐานที่สำคัญในภาคส่วนการดูแลสุขภาพ พลังงาน และรัฐบาล

โดย DCCOM จะรวบรวมขีดความสามารถด้านความปลอดภัยทางไซเบอร์ของสิงคโปร์ โดยรวม Cybersecurity Task Force และ Defence Cyber Organization ไว้ภายใต้กองบัญชาการเดียว ในขณะที่ SAFC4DC จะนำ Digital Ops-Tech Centre เข้ามาอยู่ภายใต้การบังคับบัญชาของตน ซึ่งศูนย์ดังกล่าวให้การสนับสนุน SAF ด้วยการผลิตภัณฑ์วิศวกรรมดิจิทัลที่สามารถขับเคลื่อนแนวคิดการต่อสู้ใหม่ ๆ หรือปรับปรุงขั้นตอนการปฏิบัติที่มีอยู่ให้ดีขึ้น รวมทั้ง SAFC4DC จะจัดตั้งศูนย์ AI ร่วมกับ C4 Operations Group ที่มีอยู่ซึ่งทำหน้าที่จัดการเครือข่ายและทรัพยากรเชิงกลยุทธ์ของ SAF รวมถึงขับเคลื่อนการพัฒนาที่เกี่ยวข้องกับระบบ Cloud

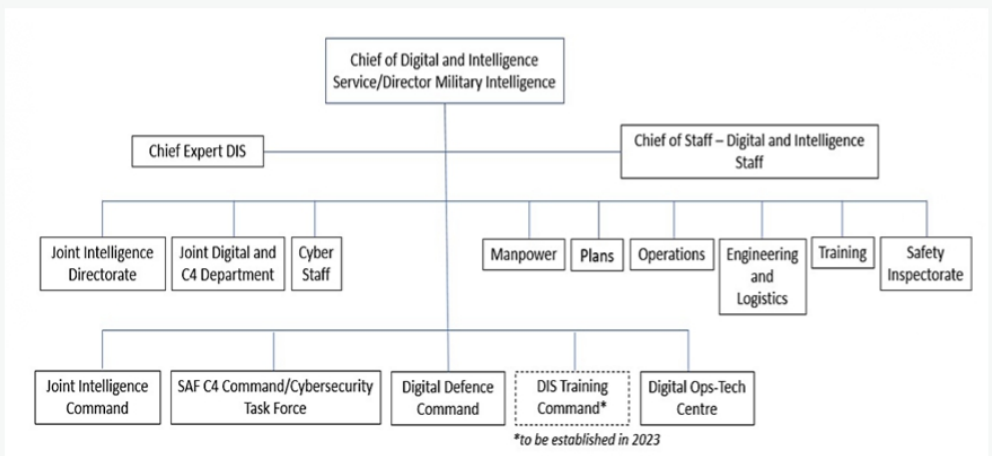




หน่วยงานใหม่ของกองทัพสิงคโปร์ (Singapore Armed Forces: SAF) ที่จัดตั้ง ชื่อว่า “The Digital and Intelligence Service (DIS)” เป็นเหล่าทัพที่ 4 จากเดิมที่มี กองทัพบก กองทัพเรือ และกองทัพอากาศ ซึ่งเหล่าทัพที่ 4 นี้มีหน้าที่การทำข่าวกรอง ที่แม่นยำ ตรงประเด็น และทันเวลาในมิติดิจิทัล (Digital Domain) อีกทั้งยังเชื่อมโยงกับเหล่าทัพอื่นด้วย C4 (Command, Control, Communications, Computers) เพื่อปฏิบัติการในรูปแบบเครือข่าย ซึ่งถือเป็นก้าวสำคัญในการเปลี่ยนแปลงกองทัพสิงคโปร์ให้เป็นกองทัพที่มีเครือข่ายและมีความรู้เพื่อรองรับภัยคุกคามรูปแบบใหม่ในอนาคต

โครงสร้างของกองทัพดิจิทัลและข่าวกรอง (DIS)

กองทัพดิจิทัลและข่าวกรอง"มีผู้บัญชาการกองทัพดิจิทัลและข่าวกรอง (Chief of Digital and Intelligence Service : CDI) เป็นผู้บังคับบัญชา มีหัวหน้าฝ่ายเสนาธิการ (Chief of Staff - Digital and Intelligence Staff. COS-DS) และหัวหน้าผู้เชี่ยวชาญ (Chief Expert DS: CXDI) ให้คำแนะนำ มีหน่วยขึ้นตรง ประกอบด้วย กรมเสนาธิการไซเบอร์ กรมข่าวร่วม กรมดิจิทัล และระบบควบคุมบังคับบัญชาร่วม มี 4 กองบัญชาการ ได้แก่ กองบัญชาการข่าวกรองร่วม กองบัญชาการควบคุมบังคับบัญชา/กองกำลังเฉพาะกิจรักษาความมั่นคงปลอดภัยไซเบอร์ กองบัญชาการป้องกันดิจิทัล และกองบัญชาการฝึกกองทัพดิจิทัลและข่าวกรอง และ 1 ศูนย์ปฏิบัติการทางเทคนิคดิจิทัล



ลำดับเหตุการณ์สำคัญของการพัฒนากองทัพสิงคโปร์ ไปสู่เหล่าทัพที่ 4

จัดตั้งหน่วยงาน “The Digital and Intelligence Service (DIS)” ให้มีสถานะเป็นเหล่าทัพที่ 4 ของกองทัพสิงคโปร์ เพื่อให้กองทัพสิงคโปร์สามารถฝึกและปฏิบัติการต่อสู้ อย่างเชื่อมโยงกันเป็นเครือข่ายและบูรณาการในการรับมือกับภัยคุกคามทางดิจิทัล โดยมีลำดับเหตุการณ์ที่สำคัญ ในการเตรียมความพร้อม ก่อนการจัดตั้งเหล่าทัพที่ 4 ดังนี้

พ.ศ. 2555 ได้มีการจัดตั้ง C4I Community ซึ่งถือ เป็นก้าวสำคัญในการเปลี่ยนแปลงกองทัพให้เป็นกองกำลังที่มี เครือข่ายและมีความรู้ 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 มีความรับผิดชอบหลักในการพัฒนา ความสามารถทางวิชาชีพ ความเชี่ยวชาญ และความรู้ของผู้ปฏิบัติงาน

พ.ศ. 2558 กองทัพได้พัฒนาศักยภาพด้วยการ ส่งทีมวิเคราะห์ภาพเข้าร่วมภารกิจแนวร่วมต่อต้านกลุ่มก่อการร้าย ไอเอส (Islamic State of Iraq and Syria: ISIS) ในคูเวต

พ.ศ. 2560 ได้มีการก่อตั้ง Defense Cyber Organization (DCO) เพื่อเป็นผู้นำและประสานงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพ และการเปิดตัวคำสั่ง SAF C4 ซึ่งเป็นการผสานรวม C4 และความสามารถในการป้องกันทางไซเบอร์

พ.ศ. 2561 มีโครงการ Cyber Full-time National Service (Cyber NSF) เพื่อดึงดูดและฝึกอบรมกำลังพลที่มีความสนใจ ร่วมเรียนรู้ เพื่อเป็นผู้เชี่ยวชาญด้านไซเบอร์ หลังจากจบหลักสูตรแล้ว กำลังพลจะได้รับมอบหมายให้มีบทบาทรับผิดชอบต่าง ๆ เพื่อปกป้องเครือข่ายและระบบภายในกระทรวงกลาโหมและกองทัพสิงคโปร์

พ.ศ. 2562 ได้มีการพัฒนา C4X โดยเพิ่มด้าน ความเชี่ยวชาญ (Expert) และผู้เชี่ยวชาญด้านการป้องกันไซเบอร์ (Defense Cyber Expert: DCX) เพื่อสนับสนุนการพัฒนาแรงงาน ในโลกไซเบอร์ที่มีทักษะสูงและสามารถเสริมสร้างความมั่นคง ปลอดภัยทางไซเบอร์ของสิงคโปร์

พ.ศ. 2563 ได้มีการเพิ่มขีดความสามารถด้านข่าวกรอง และการต่อต้านการก่อการร้าย รวมถึงจัดตั้งคณะทำงานด้านความปลอดภัย ทางไซเบอร์ (Cybersecurity Task Force) และได้มีการบรรจุ C4I เข้าไปในหลักสูตรโรงเรียนนายร้อย (Officer Cadet School: OCS)

พ.ศ. 2565 มีการเตรียมจัดตั้ง The Digital and Intelligence Service (DIS) ที่จะมีสถานะเป็นเหล่าทัพที่ 4 เพื่อช่วยให้กองทัพสามารถปกป้องสิงคโปร์จากภัยคุกคามทางดิจิทัลได้มีประสิทธิภาพมากขึ้น

การที่กองทัพสิงคโปร์ได้เล็งเห็นความสำคัญของภัยคุกคามทางดิจิทัล โดยการจัดตั้ง DIS ได้ส่งผลดีต่อกองทัพสิงคโปร์ แต่ก็ก่อให้เกิดความท้าทายต่อภูมิภาคด้วยเช่นกัน ซึ่งการจัดตั้งหน่วย DIS จะเสริมสร้างให้กองทัพดำเนินงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น เนื่องจาก DIS จะผสานรวมความสามารถของกองทัพสิงคโปร์ให้แน่นแฟ้นยิ่งขึ้น เพื่อจัดการกับภัยคุกคามด้านความมั่นคงต่างๆ รวมถึงภัยคุกคามจากมิติดิจิทัล การเติบโตและเสริมสร้างทรัพยากรมนุษย์ก็มีส่วนสำคัญในการทำให้ DIS สามารถขยายกำลังคนด้านดิจิทัล และหน่วยข่าวกรองได้ด้วยการเสริมสร้างการพัฒนาทางวิชาชีพ การสรรหา บุคลากร และโอกาสทางอาชีพ ทั้งนี้การจัดตั้ง DIS มีความสอดคล้องกับแนวคิดเรื่องการป้องกันประเทศแบบเบ็ดเสร็จ (Total Defence Themes)

การเตรียมพร้อมของกองทัพไทย

จะเห็นได้ว่ากองทัพสิงคโปร์ได้มีการพัฒนาให้ทันกับสถานการณ์ของโลกที่เกิดขึ้น การเตรียมพร้อมรับสถานการณ์จากภัยคุกคามจึงเป็นเรื่องที่จำเป็น กองทัพไทยจึงควรมีการพัฒนาหลายด้านเพื่อเสริมสร้างความมั่นคงให้กับกองทัพ ทั้งด้านบุคลากร ซึ่งกองทัพควรผลิตและสร้างบุคลากรให้มีความชำนาญ รวมทั้งเสริมทักษะและขีดความสามารถด้านดิจิทัลโดเมน อาทิ การจัดหลักสูตรเฉพาะในการพัฒนากำลังพล ในด้านเทคโนโลยีควรเตรียมพร้อมทางด้านเทคโนโลยีทั้ง (Hardware) โครงสร้างพื้นฐาน อุปกรณ์ เครื่องมือและเทคโนโลยี รวมทั้งด้าน (Software) โปรแกรมต่าง ๆ และระบบปฏิบัติการที่มี ความทันสมัยและมีประสิทธิภาพ รวมถึงด้านประสิทธิภาพที่ควรมีการบูรณาการและประสานการทำงานร่วมกันระหว่างเหล่าทัพ และหน่วยงานด้านความมั่นคงอื่น ๆ ให้มีการเชื่อมโยงเครือข่ายและบูรณาการการทำงานระหว่างกัน เพื่อประสานการปฏิบัติการด้านไซเบอร์ให้มี

ประสิทธิภาพในเรื่องการข่าว กรองผ่านระบบไซเบอร์ รวมถึงการรับมือเมื่อมีเหตุการณ์ถูกโจมตี หรือ ภัยคุกคามทางไซเบอร์

พ.อ.สุเทพ ยั่งยืน
อจ.อก.สมย.วทบ.

อ้างอิง

https://www.sscthailand.org/uploads_ssc/research_20220606165450463311959 6.pdf
https://www.infoquest.co.th/2022/179585
https://www.ryt9.com/s/iq37/3303454