



## Cyber Force: การจัดตั้งเหล่าทัพที่ ๔ ของกองทัพอากาศ

ในโลกปัจจุบัน ภัยคุกคามสามารถแทรกซึมในชีวิตประจำวัน ผ่านพื้นที่ไซเบอร์ ข้อมูลข่าวสาร สื่อสังคมออนไลน์ และแพลตฟอร์มดิจิทัล พื้นที่ของความมั่นคงจึงขยายจากโลกทางกายภาพเข้าสู่โลกดิจิทัล และทำให้ประชาชนกลายเป็นส่วนหนึ่งของสนามความขัดแย้งสมัยใหม่ มาเลเซียจึงเริ่มปรับตัวต่อภูมิทัศน์ความมั่นคงที่เปลี่ยนไป ผ่านการเตรียมจัดตั้ง Cyber Force เป็นเหล่าทัพที่ ๔ ต่อจากกองทัพบก กองทัพเรือ และกองทัพอากาศ เพื่อให้สามารถรับมือกับภัยคุกคามที่ไม่ได้เกิดขึ้นเฉพาะในสนามรบ หากแต่อาจเกิดขึ้นได้ทุกที่ ทุกเวลา และใกล้ตัวประชาชนมากกว่าที่เคย

### ภัยคุกคามรูปแบบใหม่กับการจัดตั้งเหล่าทัพที่ ๔

ในเดือนกรกฎาคม ๒๕๖๙ กระทรวงกลาโหมมาเลเซียประกาศว่ากำลังดำเนินการเพื่อจัดตั้ง Cyber Force ให้เป็นเหล่าทัพที่ ๔ ของกองทัพอากาศ (Malaysian Armed Forces) ต่อจากกองทัพบก กองทัพเรือ และกองทัพอากาศ โดย Mohamed Khaled Nordin รัฐมนตรีว่าการกระทรวงกลาโหมมาเลเซีย ระบุว่า การดำเนินการดังกล่าวเป็นสิ่งที่หลีกเลี่ยงได้ยาก เนื่องจากลักษณะภัยคุกคามรูปแบบใหม่ ได้เปลี่ยนจากการต่อสู้ทางกายภาพ ไปสู่การแข่งขันเพื่อครองความได้เปรียบในพื้นที่ไซเบอร์ รวมถึงปรับเปลี่ยนการรับรู้ของประชาชน<sup>๑</sup> ดังนั้นการผลักดัน Cyber Force อย่างเร่งด่วน จึงมีความหมายมากกว่าการจัดตั้งหน่วยงานเพื่อป้องกันการโจมตีระบบคอมพิวเตอร์เพียงอย่างเดียว เพราะนอกจากจะเสริมสร้างความมั่นคงของประเทศ แล้วยังสะท้อนถึงการยกระดับพื้นที่ดิจิทัล ให้เป็นพื้นที่ปฏิบัติการด้านความมั่นคงที่มีความสำคัญควบคู่กับพื้นที่ทางบก ทางทะเล และทางอากาศ

### การเสริมสร้างความมั่นคงด้วยเทคโนโลยีขั้นสูง

การปรับตัวด้านความมั่นคงของมาเลเซียไม่ได้จำกัดอยู่เพียงแค่การเตรียมจัดตั้ง Cyber Force เท่านั้น แต่ครอบคลุมถึงการนำเทคโนโลยีสมัยใหม่เข้ามาเพิ่มขีดความสามารถของหน่วยงานความมั่นคงที่มีอยู่ ทั้ง Artificial Intelligence (AI), Drone, Cyber Defence และ Electronic Warfare<sup>๒</sup> โดยเฉพาะกองทัพอากาศมาเลเซียที่อยู่ระหว่างพัฒนาแนวคิดการปฏิบัติสำหรับระบบ Drone และ Counter-Drone ให้สามารถทำงานร่วมกับยุทธวิธีรูปแบบ

ดั้งเดิมได้อย่างมีประสิทธิภาพ เพื่อรองรับภัยคุกคามรูปแบบใหม่และสถานการณ์ในพื้นที่สีเทา (Grey Zone)<sup>๓</sup> สะท้อนให้เห็นว่าเทคโนโลยีขั้นสูงเหล่านี้ กลายเป็นองค์ประกอบสำคัญที่ช่วยเพิ่มขีดความสามารถของกองทัพอากาศมาเลเซีย นอกจากนี้การเสริมสร้างความมั่นคงด้วยเทคโนโลยีขั้นสูงของมาเลเซียครอบคลุมความมั่นคงในพื้นที่ไซเบอร์ สื่อสังคมออนไลน์ และแพลตฟอร์มดิจิทัล เนื่องจากพื้นที่เหล่านี้ถูกใช้เป็นเครื่องมือในการเผยแพร่ข้อมูล บิดเบือนข้อเท็จจริง ตลอดจนสร้างอิทธิพลทางความคิดและการรับรู้ของประชาชน การพัฒนาขีดความสามารถด้านไซเบอร์ของมาเลเซียจึงมีความสำคัญกับการรับมือปฏิบัติการข้อมูลข่าวสารที่มุ่งแทรกแซงการรับรู้ของประชาชน ซึ่งอาจส่งผลกระทบต่อความเชื่อมั่น ความสัมพันธ์ทางสังคม และเสถียรภาพของรัฐได้ในระยะยาว<sup>๔</sup>

### บทวิเคราะห์: ภาพสะท้อน Cyber Force ของมาเลเซีย

การเตรียมจัดตั้ง Cyber Force เป็นเหล่าทัพที่ ๔ ของมาเลเซีย ไม่ใช่เพียงการปรับโครงสร้างทางทหารแบบใหม่เท่านั้น หากแต่สะท้อนถึงการเปลี่ยนโครงสร้างการนิยามภัยคุกคามรูปแบบใหม่ของรัฐปัจจุบัน จากเดิมที่ความมั่นคงให้ความสำคัญกับการปกป้องดินแดน อธิปไตย และพรมแดนทางกายภาพ ไปสู่การนิยามที่ครอบคลุม การปกป้องพื้นที่ไซเบอร์ ข้อมูลข่าวสาร และการรับรู้ของประชาชน นำมาสู่บทวิเคราะห์ภาพสะท้อน ๒ ประเด็น ดังนี้

๑) การผนึกกำลังป้องกันทางไซเบอร์ระหว่างภาคความมั่นคง เนื่องจากในปัจจุบันโครงสร้างพื้นฐานและพื้นที่ดิจิทัล เชื่อมโยงกับ



หลายภาคส่วน มาเลเซียจึงจำเป็นต้องพัฒนา Cyber Force ควบคู่กับการสร้างกลไกความร่วมมือระหว่างภาคส่วนต่าง ๆ อย่างไรก็ตาม ความท้าทายสำคัญ คือ ความแตกต่างของภารกิจ วัฒนธรรมองค์กร และระดับการเข้าถึงข้อมูลที่มีชั้นความลับ ระหว่างกองทัพ หน่วยงานพลเรือน และภาคเอกชน ซึ่งถือเป็นการขยายภาคความมั่นคงเข้าสู่พื้นที่ทางสังคมเพื่อสร้างความไว้วางใจระหว่างรัฐกับประชาชน เพราะเมื่อพื้นที่ดิจิทัลที่ประชาชนใช้ในชีวิตประจำวัน กลายเป็นพื้นที่ปฏิบัติการด้านความมั่นคง การเฝ้าระวังและการป้องกันภัยของรัฐอาจถูกตั้งคำถามถึงขอบเขตและความเหมาะสมของการใช้อำนาจได้ ดังนั้น ความท้าทายของ Cyber Force จึงไม่ได้อยู่เพียงการพัฒนาขีดความสามารถทางเทคโนโลยี แต่รวมถึงการสร้างกลไกที่ทำให้ตัวแสดงซึ่งมีบทบาทแตกต่างกันสามารถทำงานร่วมกันได้ เพราะท้ายที่สุดแล้ว ความมั่นคงทางไซเบอร์ไม่ได้ขึ้นอยู่กับความเข้มแข็งของกองทัพเพียงอย่างเดียว แต่ขึ้นอยู่กับความไว้วางใจระหว่างรัฐ กองทัพ และสังคม

**๒) การเตรียมความพร้อมด้านนโยบายและกฎหมายที่เกี่ยวข้องด้านไซเบอร์** ความสำคัญของ Cyber Force สะท้อนการเปลี่ยนกระบวนทัศน์ของความมั่นคงมาเลเซีย จากภัยคุกคามที่มีพื้นที่ชัดเจนไปสู่ภัยที่ไร้พรมแดน อย่างไรก็ตาม การเปลี่ยนผ่านดังกล่าวย่อมสร้างโจทย์ใหม่เกี่ยวกับอำนาจหน้าที่ และการแบ่งบทบาทระหว่างกองทัพกับหน่วยงานพลเรือน เนื่องการบังคับใช้กฎหมายที่มีอยู่เดิม อาจนำไปสู่ช่องว่างความรับผิดชอบเมื่อเผชิญเหตุการณ์จริง หากขาดการกำหนดขอบเขตการใช้อำนาจที่ชัดเจน ขณะเดียวกัน ความเร็วแบบก้าวกระโดดของเทคโนโลยีเป็นอีกหนึ่งอุปสรรคสำคัญ เพราะเทคนิคการโจมตีรูปแบบใหม่สามารถเปลี่ยนแปลงได้เร็วกว่ากระบวนการร่างกฎหมาย และการปรับนโยบายของรัฐ ส่งผลให้กฎระเบียบที่มีอยู่อาจไม่ครอบคลุมต่อสถานการณ์ที่เกิดขึ้น ดังนั้น ความท้าทายของมาเลเซียจึงไม่ใช่เพียงการสร้างตัวบทกฎหมายรองรับการจัดตั้ง Cyber Force แต่คือการสร้างกรอบนโยบายและกฎหมายที่มีความชัดเจน เพียงพอต่อการกำหนดอำนาจและความรับผิดชอบ ขณะเดียวกันต้องมีความยืดหยุ่นเพียงพอต่อการปรับตัวตามเทคโนโลยี และรูปแบบของภัยคุกคามรูปแบบใหม่ที่เปลี่ยนแปลงอย่างเป็นพลวัต ซึ่งถือเป็นเงื่อนไขสำคัญต่อประสิทธิภาพของ Cyber Force ในระยะยาว

### ข้อเสนอแนะต่อกองทัพไทย

๑) กองทัพไทยควรให้ความสำคัญกับการพัฒนาขีดความสามารถในการรับมือภัยคุกคามรูปแบบใหม่ โดยการศึกษาการเตรียม

ความพร้อมด้านนโยบายและกฎหมายที่เกี่ยวข้องด้านไซเบอร์ของมาเลเซียดังที่กล่าวมาแล้วและความจำเป็นของไทยในการจัดตั้งเหล่าทัพไซเบอร์ตามรูปแบบของมาเลเซีย โดยศึกษาความเหมาะสมของโครงสร้างการบัญชาการที่สามารถเชื่อมโยงการปฏิบัติระหว่างเหล่าทัพและหน่วยงานที่เกี่ยวข้องในปัจจุบันให้เกิดประสิทธิภาพสูงสุด ให้เกิดการประสานงานร่วมกัน ลดความซ้ำซ้อนระหว่างหน่วยงาน

๒) ในการรับมือกับภัยคุกคามทางไซเบอร์ กองทัพไทยควรมองเป็นโอกาสในการพัฒนาให้เป็นพื้นที่นำร่องสำหรับการผลักดันให้เป็น Smart Border Security โดยไม่จำเป็นต้องเริ่มจากการลงทุนระบบขนาดใหญ่ แต่เลือกพื้นที่ที่มีปัญหาการลักลอบและการเคลื่อนย้ายข้ามแดนสูง เช่น แนวแม่น้ำโก-ลก แล้วทดลองบูรณาการ Drone AI ระบบเฝ้าตรวจ และข่าวกรองภาคสนาม เข้ากับการปฏิบัติของหน่วยที่รับผิดชอบ เพื่อสร้างภาพสถานการณ์ร่วมและลดข้อจำกัดของการลาดตระเวนด้วยกำลังพลเพียงอย่างเดียว

๓) การรับมือกับภัยคุกคามรูปแบบใหม่ โดยบูรณาการความร่วมมือกับต่างประเทศ เช่น การใช้กลไกความร่วมมือไทย-มาเลเซียเป็นช่องทางทดลองและพัฒนา แทนการสร้างกลไกใหม่ขึ้นมาซ้ำซ้อน โดยผลักดันเรื่อง Smart Border Security ซึ่งอาจทำร่วมกับฝ่ายมาเลเซียที่กำลังใช้ Drone และ AI เพิ่มประสิทธิภาพการควบคุมชายแดนเพื่อสร้างความมั่นคงอย่างต่อเนื่อง ผ่านคณะกรรมการชายแดนทั่วไป ไทย-มาเลเซีย (General Border Committee: GBC) คณะกรรมการชายแดนส่วนภูมิภาคไทย-มาเลเซีย (Regional Border Committee: RBC) และคณะกรรมการร่วมว่าด้วยความร่วมมือด้านความมั่นคง ไทย-มาเลเซีย (Joint Working Committee on Security Cooperation: JWC-SC) ในการหารือประเด็นความร่วมมือด้านความมั่นคงชายแดน อาชญากรรมข้ามชาติ และการป้องกันทางไซเบอร์

### อ้างอิง

- <sup>๑</sup> Free Malaysia Today. (2026). Cyber force to be 4th service branch of armed forces. Free Malaysia Today
- <sup>๒</sup> The Star. (2025). Armed Forces cyber command base to be launched in November. The Star
- <sup>๓</sup> The Star. (2026). Defence Ministry working on establishing cyber force as fourth service branch. The Star
- <sup>๔</sup> The Sun. (2026). Cyber force could guard Malaysia's digital front door: Experts. The Sun.

๗ ก.ย. ๖๕



www.sscthailand.org



๖๒ ถนนวิภาวดีรังสิต แขวงดินแดง เขตดินแดง กรุงเทพฯ ๑๐๕๐๐



sscthailand



sscthailand