สมุดปกขาว

หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. ๒๕๖๘

บริการของเรา:

- การป้องกันภัยคุกคามทางไซเบอร์และข่าวกรองภัยคุกคามไซเบอร์
- การฝึกอบรมและพัฒนาบุคลากรด้านไซเบอร์
- การปฏิบัติการทางไซเบอร์และการตอบสนองต่อเหตุการณ์ทางไซเบอร์
- การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII Protection)
- ความร่วมมือด้านไซเบอร์ระหว่างประเทศ

หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย ปกป้องระบบดิจิทัลของชาติ เสริมสร้างขีดความสามารถทางไซเบอร์ รับมือภัยคุกคาม ทันสมัย มั่นคง และยั่งยืน

Contact Us:
0 2572 2251

TABLE OF CONTENTS

TABLE OF CONTENTS

บทสรุปผู้บริหาร - สมุดปกขาว หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. ๒๕๖๘

ในยุคดิจิทัลที่มีการเปลี่ยนแปลงอย่างรวดเร็วและซับซ้อน ภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรงขึ้นอย่างต่อเนื่อง ส่งผลกระทบโดยตรงต่อความมั่นคงของประเทศ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และระบบดิจิทัลที่เกี่ยวข้อง ด้วยเหตุนี้ หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย จึงถูกจัดตั้งขึ้นเพื่อเสริมสร้างขีดความสามารถด้านไซเบอร์ของกองทัพไทย ให้สามารถป้องกันรับมือและตอบโต้ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

สมุดปกขาวฉบับนี้ เป็นเอกสารเชิงยุทธศาสตร์ที่กำหนดกรอบแนวทางในการพัฒนาและเสริมสร้างศักยภาพด้านไซเบอร์ของกองบัญชาการกองทัพไทย **โดยครอบคลุม ๕ มิติหลัก** ได้แก่

๑. สภาพแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นการวิเคราะห์แนวโน้มของภัยคุกคาม ความท้าทาย และโอกาสในการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ

๒. กฎหมายและหลักการสำคัญที่เกี่ยวข้อง ซึ่งกำหนดกรอบกฎหมาย นโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นแนวทางปฏิบัติของหน่วยบัญชาการไซเบอร์ทหาร

๓. กรอบยุทธศาสตร์ ซึ่งเป็นแนวทางและเป้าหมายเชิงยุทธศาสตร์สำหรับการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพไทย

๔. ขีดความสามารถที่ต้องการทางไซเบอร์ ซึ่งกำหนดความสามารถหลักที่จำเป็นสำหรับการปฏิบัติการไซเบอร์ให้เกิดประสิทธิภาพสูงสุด

๕. แผนพัฒนาขีดความสามารถทางไซเบอร์ ซึ่งเป็นการกำหนดแนวทางและมาตรการสำหรับการพัฒนาและยกระดับความสามารถทางไซเบอร์ของกองทัพไทย

๑. สภาพแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์

สถานการณ์ภัยคุกคามทางไซเบอร์มีแนวโน้มทวีความรุนแรงขึ้น เนื่องจากความขัดแย้งระหว่างประเทศ การแข่งขันทางเทคโนโลยี และการดำเนินปฏิบัติการของกลุ่มอาชญากรไซเบอร์ ซึ่งเป้าหมายของการโจมตีไม่ได้จำกัดเฉพาะโครงสร้างพื้นฐานของรัฐเท่านั้น แต่ยังขยายไปถึงภาคเอกชนและประชาชนทั่วไป เทคโนโลยีใหม่ๆ เช่น ปัญญาประดิษฐ์ (AI), การประมวลผลแบบคลาวด์ (Cloud Computing), และเทคโนโลยีควอนตัม (Quantum Computing) ได้เพิ่มขีดความสามารถให้ทั้งฝ่ายป้องกันและฝ่ายโจมตี ทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องที่มีความซับซ้อนมากยิ่งขึ้น

๒. กฎหมายและหลักการสำคัญที่เกี่ยวข้อง

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพไทยต้องอยู่ภายใต้กรอบกฎหมายและหลักการที่ชัดเจน ซึ่งเป็นรากฐานสำคัญในการกำหนดแนวทางปฏิบัติ โดยมีพระราชบัญญัติและแผนปฏิบัติการที่สำคัญ ได้แก่

• พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

• นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕-๒๕๗๐)

• กรอบยุทธศาสตร์กระทรวงกลาโหมด้านไซเบอร์ (พ.ศ. ๒๕๖๖-๒๕๗๐)

• หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ของกองบัญชาการกองทัพไทย

๓. กรอบยุทธศาสตร์สำหรับความมั่นคงปลอดภัยทางไซเบอร์

กรอบยุทธศาสตร์ของกองบัญชาการกองทัพไทยมุ่งเน้นการบูรณาการกำลังพล เทคโนโลยี และกระบวนการปฏิบัติการให้เป็นไปตามมาตรฐานสากล โดยกำหนด **เป้าหมายหลัก ๔ ประการ** ได้แก่

๑) เสริมสร้างขีดความสามารถในการปฏิบัติการทาง ไซเบอร์

• พัฒนาศูนย์ปฏิบัติการร่วมทางไซเบอร์ (JCOC) ให้เป็นศูนย์กลางการบังคับบัญชาและควบคุมปฏิบัติการ

• ยกระดับ ระบบข่าวกรองภัยคุกคามทางไซเบอร์ (CTI)

๒) ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

• พัฒนา Zero Trust Architecture (ZTA) เพื่อเพิ่มความมั่นคงปลอดภัยของระบบดิจิทัล

• บูรณาการ ระบบเฝ้าระวังภัยคุกคามและระบบซ้อมรับมือเหตุการณ์ทางไซเบอร์

๓) เสริมสร้างความร่วมมือระหว่างประเทศ

• แลกเปลี่ยนข้อมูลภัยคุกคามกับพันธมิตร เช่น Cyber Defense Working Group (CDWG)

• เข้าร่วมการฝึกซ้อมทางไซเบอร์ระดับนานาชาติ เช่น Cyber Flag และ Talisman Sabre

๔) พัฒนาขีดความสามารถด้านการปฏิบัติการเชิงรุก (Offensive Cyber Operations: OCO)

• ใช้เทคโนโลยี เช่น Big Data Analytics, Post-Quantum Cryptography (PQC), AI-Driven Cyber Defense

๔. ขีดความสามารถที่ต้องการทางไซเบอร์

การบรรลุเป้าหมายดังกล่าวต้องอาศัยทรัพยากรบุคคล กระบวนการ และเทคโนโลยี

• ทรัพยากรบุคคล (People): พัฒนาโรงเรียนไซเบอร์ทหาร และจัดตั้ง ชุดปฏิบัติการทางไซเบอร์เฉพาะทาง

• กระบวนการ (Process): จัดทำ หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ และบูรณาการระบบเฝ้าระวังภัยคุกคามทางไซเบอร์

• เทคโนโลยี (Technology): ยกระดับ JCOC, Cyber-C2 Technology, Cyber Range & Simulation

๕. แผนพัฒนาขีดความสามารถทางไซเบอร์

เพื่อให้บรรลุเป้าหมายดังกล่าว สมุดปกขาวได้กำหนดแนวทางการพัฒนาใน ๓ ด้านหลัก ได้แก่

๕.๑ การพัฒนาทรัพยากรบุคคล (People)

การพัฒนาทรัพยากรบุคคลทางไซเบอร์มุ่งเน้นการยกระดับองค์ความรู้และทักษะของบุคลากรทางไซเบอร์ผ่านหลักสูตรฝึกอบรมที่ครอบคลุมทุกระดับ ตั้งแต่พื้นฐานจนถึงขั้นสูง เพื่อเตรียมบุคลากรให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์

หลักสูตรแบ่งออกเป็น ๕ กลุ่ม ได้แก่ ๑) หลักสูตรพื้นฐาน สำหรับผู้บริหารและบุคลากรทั่วไป ๒) หลักสูตรระดับกลาง สำหรับผู้ปฏิบัติการไซเบอร์ ๓) หลักสูตรขั้นสูง สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ ๔) หลักสูตรเฉพาะทาง ที่เน้นทักษะเฉพาะ เช่น ข่าวกรองไซเบอร์และการประเมินความเสี่ยง และ ๕) หลักสูตรบริหารงานไซเบอร์ เพื่อพัฒนาทักษะด้านการวางแผนและบริหารศูนย์ปฏิบัติการไซเบอร์

๕.๒ การพัฒนากระบวนการ (Process)

- จัดทำหลักนิยมการปฏิบัติการร่วมทางไซเบอร์
- พัฒนานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
- เสริมสร้างความร่วมมือกับหน่วยงานทั้งในและต่างประเทศ เช่น Cyber Defense Working Group (CDWG)
- บูรณาการระบบเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ ให้สามารถดำเนินการแบบเรียลไทม์

๕.๓ การพัฒนาเทคโนโลยี (Technology)

- ยกระดับ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ (Joint Cyber Operations Center: JCOC)

• พัฒนาระบบ Cyber-C2 Technology สำหรับการบังคับบัญชาและควบคุมทางไซเบอร์

• สนับสนุน Cyber Range & Simulation สำหรับฝึกซ้อมสถานการณ์ทางไซเบอร์

• เสริมสร้างโครงสร้างพื้นฐาน เช่น Cloud & Edge Computing, Post-Quantum Cryptography (PQC) และ Zero Trust Architecture

แนวทางในอนาคต

การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นปัจจัยสำคัญต่อความมั่นคงของชาติในศตวรรษที่ ๒๑ กองบัญชาการกองทัพไทยจึงมีบทบาทสำคัญในการเสริมสร้างศักยภาพทางไซเบอร์ผ่านการพัฒนาบุคลากร เทคโนโลยี และกระบวนการปฏิบัติการให้ทันสมัยและสอดคล้องกับมาตรฐานสากล

เป้าหมายในระยะยาว ได้แก่

• **ยกระดับ** กองทัพไทยให้สามารถ ป้องกันภัยคุกคามทางไซเบอร์ได้อย่างครอบคลุม

• **สร้าง**ระบบ Cyber Intelligence ที่สามารถคาดการณ์ภัยคุกคามล่วงหน้า

• **ขยาย** ความร่วมมือระหว่างประเทศ ผ่านโครงการฝึกอบรมและการแบ่งปันข้อมูลภัยคุกคาม

• **ปรับปรุง** กฎหมายและนโยบาย ให้สอดคล้องกับภัยคุกคามที่เปลี่ยนแปลงอย่างต่อเนื่อง

สมุดปกขาวฉบับนี้ เป็นแนวทางสำคัญในการเสริมสร้างศักยภาพทางไซเบอร์ของกองบัญชาการกองทัพไทยให้สามารถเผชิญกับภัยคุกคามที่ซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลา การดำเนินการตามแนวทางดังกล่าวจะช่วยให้ประเทศไทยสามารถรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ในระยะยาว และสร้างความเชื่อมั่นให้กับประชาชนและพันธมิตรทั่วโลกว่า ไทยมีศักยภาพในการเผชิญหน้ากับความท้าทายทางไซเบอร์ในศตวรรษที่ ๒๑ อย่างมั่นคงและยั่งยืน

สมุดปกขาว หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. ๒๕๖๘

๑. สภาพแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์

ปัจจุบัน สถานการณ์ภัยคุกคามทางไซเบอร์มีแนวโน้มที่จะทวีความรุนแรงและซับซ้อนขึ้นอย่างต่อเนื่อง ซึ่งเป็นผลมาจากการพัฒนาเทคโนโลยีที่ไม่หยุดยั้งควบคู่กับการขยายตัวของกิจกรรมที่เกี่ยวข้องกับการปฏิบัติการทางไซเบอร์ในทุกมิติ ปัจจัยสำคัญที่ส่งผลให้สถานการณ์ดังกล่าวทวีความรุนแรงขึ้น ได้แก่ ความขัดแย้งทางการเมืองระหว่างประเทศ การแข่งขันด้านเทคโนโลยีระหว่างมหาอำนาจ และการเข้ามามีบทบาทของกลุ่มผู้ที่ไม่หวังดีซึ่งอาศัยช่องโหว่ทางไซเบอร์เป็นเครื่องมือในการโจมตี เป้าหมายของการโจมตีเหล่านี้ไม่ได้จำกัดอยู่เพียงแค่การสร้างความเสียหายต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) หากแต่ยังรวมไปถึงการบ่อนทำลายความเชื่อมั่นของประชาชนที่มีต่อระบบดิจิทัลอีกด้วย ตัวอย่างเช่น กลุ่มผู้โจมตีที่ได้รับการสนับสนุนจากเกาหลีเหนือได้เจาะระบบการเงินและบริษัทเทคโนโลยีเพื่อจัดหาเงินทุนสนับสนุนรัฐบาลของตน นอกจากนี้ การโจมตีที่เกิดขึ้นในสงครามไซเบอร์ระหว่างรัสเซียกับยูเครน ยังสะท้อนให้เห็นถึงผลกระทบทางเศรษฐกิจและการเมืองอันร้ายแรงที่เกิดขึ้นเมื่อมีการโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของแต่ละประเทศ

ในอนาคต สถานการณ์ภัยคุกคามทางไซเบอร์มีแนวโน้มทวีความรุนแรงมากขึ้น เนื่องจากการพัฒนาเทคโนโลยีสมัยใหม่ซึ่งสามารถถูกนำมาใช้เป็นอาวุธในการโจมตีไซเบอร์ได้ ตัวอย่างเช่น การประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพื่อเพิ่มประสิทธิภาพในการโจมตี การสร้างมัลแวร์ที่สามารถปรับตัวเข้ากับสภาพแวดล้อมของเป้าหมายได้ และการพัฒนาเครื่องมือโจมตีที่สามารถเจาะระบบได้ในหลากหลายแพลตฟอร์ม นอกจากนี้ ปัญญาประดิษฐ์ยังถูกนำมาใช้เพื่อสร้างข้อมูลเท็จที่มีความซับซ้อนและน่าเชื่อถือ ซึ่งส่งผลกระทบโดยตรงต่อความมั่นใจของประชาชนที่มีต่อข้อมูลข่าวสาร การผสมผสานเทคโนโลยีขั้นสูงเข้ากับกลยุทธ์การโจมตีทางไซเบอร์รูปแบบใหม่ยังส่งผลให้การโจมตีสามารถก่อให้เกิดผลกระทบได้ในวงกว้างและเกิดขึ้นอย่างรวดเร็วมากยิ่งขึ้น อีกหนึ่งประเด็นที่น่ากังวลคือ ภัยคุกคามที่พุ่งเป้าไปยังเทคโนโลยีคลาวด์ (Cloud) ซึ่งในปัจจุบันได้กลายเป็นโครงสร้างพื้นฐานที่สำคัญของระบบสารสนเทศ แนวโน้มของการโจมตีระบบคลาวด์ยังคงเพิ่มสูงขึ้น โดยเฉพาะอย่างยิ่งในกรณีที่องค์กรขาดมาตรการป้องกันที่เพียงพอ เช่น การโจมตีแบบแรนซัมแวร์ (Ransomware) ที่มุ่งเป้าไปที่ฐานข้อมูลสำคัญในระบบคลาวด์ หรือการใช้ระบบคลาวด์เป็นช่องทางแพร่กระจายมัลแวร์ซึ่งสามารถก่อให้เกิดความเสียหายในวงกว้าง ขณะเดียวกัน ช่องโหว่ในห่วงโซ่อุปทาน (Supply Chain) ยังคงเป็นประเด็นสำคัญเช่นกัน ตัวอย่างเช่น กรณีที่หน่วยงานด้านความมั่นคงปลอดภัยบางแห่งดำเนินการอัปเดตซอฟต์แวร์ผิดพลาด ส่งผลกระทบต่อระบบคอมพิวเตอร์ทั่วโลก ซึ่งหลายประเทศยังคงพึ่งพาอาศัยอยู่

ภัยคุกคามทางไซเบอร์ยังคงเป็นความท้าทายสำคัญที่ทุกประเทศต้องเผชิญต่อไป ด้วยเหตุนี้ การป้องกันที่มีประสิทธิภาพและการปรับตัวให้ทันต่อภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว จะเป็นปัจจัยสำคัญในการรักษาความมั่นคงและเสถียรภาพของประเทศ ด้วยตระหนักถึงความสำคัญของประเด็นดังกล่าว กระทรวงกลาโหมจึงได้จัดตั้งหน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทยขึ้นในปีงบประมาณ พ.ศ. ๒๕๖๘ เพื่อเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ทั้งนี้ การดำเนินงานของหน่วยบัญชาการ ไซเบอร์ทหารครอบคลุมภารกิจในหลายด้าน ได้แก่ การจัดตั้งกองกำลังรบทางไซเบอร์ การฝึกปฏิบัติและการซ้อมรบ การพัฒนาศักยภาพของบุคลากรผ่านการเสริมสร้างทักษะและองค์ความรู้ การลงทุนในเทคโนโลยีที่ทันสมัย ตลอดจนการสร้างความร่วมมือกับมิตรประเทศ เพื่อให้มั่นใจว่าหน่วยงานดังกล่าวสามารถปกป้องผลประโยชน์ของชาติและรักษาเสถียรภาพความมั่นคงของประเทศได้อย่างมีประสิทธิภาพและยั่งยืน

๒. กฎหมายและหลักการสำคัญต่าง ๆ ที่เกี่ยวข้อง

ความมั่นคงปลอดภัยทางไซเบอร์จำเป็นต้องอาศัยการพัฒนาแผนงานที่สอดคล้องกับยุทธศาสตร์ระดับชาติ เช่น แผนการพัฒนาทางไซเบอร์เพื่อความมั่นคง กระทรวงกลาโหม (พ.ศ. ๒๕๖๖-๒๕๗๐) ซึ่งกำหนดแนวทางเสริมสร้างศักยภาพการป้องกันประเทศไว้อย่างชัดเจน รวมถึงการอ้างอิงถึงยุทธศาสตร์ทหารด้านสงครามไซเบอร์ ที่มุ่งบูรณาการทรัพยากรไซเบอร์เพื่อให้เกิดประสิทธิภาพสูงสุด นอกจากนี้ หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ ยังมีบทบาท

สำคัญในการกำหนดกรอบแนวทางที่ชัดเจนสำหรับการตอบสนองต่อภัยคุกคามทางไซเบอร์ และสนับสนุนให้เกิดการจัดตั้ง หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย อันมีเป้าหมายเพื่อเสริมสร้างความพร้อมในการปฏิบัติการทางไซเบอร์ทั้งในมิติของการเตรียมกำลังและการใช้กำลังทางไซเบอร์อย่างมีประสิทธิภาพ ท่ามกลางบริบทที่ความมั่นคงปลอดภัยทางไซเบอร์กลายเป็นรากฐานสำคัญของการป้องกันประเทศ

๒.๑ **กฎหมายที่เกี่ยวข้อง**

๒.๑.๑ พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. ๒๕๕๑

๑) มาตรา ๑๕ กองทัพไทยมีหน้าที่เตรียมกำลัง การป้องกันราชอาณาจักรและดำเนินการเกี่ยวกับการใช้กำลังทหารตามอำนาจหน้าที่ของกระทรวงกลาโหมมีผู้บัญชาการทหารสูงสุดเป็นผู้บังคับบัญชารับผิดชอบ

๒) มาตรา ๑๖ ให้อำนาจกองทัพไทยในการจัดตั้งคณะกรรมการหรือคณะอนุกรรมการ ตลอดจนมอบหมายบุคคลใดๆ เพื่อพิจารณาเรื่องที่เกี่ยวกับแผนรักษาเอกราชและผลประโยชน์แห่งชาติ รวมถึงการปฏิบัติการทางทหารร่วมกับทุกส่วนราชการ (ตามที่ระบุในมาตรา ๑๗)

๓) มาตรา ๑๗ กำหนดโครงสร้างของกองทัพไทยว่าประกอบด้วย กองบัญชาการกองทัพไทย, กองทัพบก, กองทัพเรือ, กองทัพอากาศ และส่วนราชการอื่นตามที่กำหนดโดยพระราชกฤษฎีกา

๔) มาตรา ๑๘ ระบุให้กองบัญชาการกองทัพไทยมีหน้าที่ควบคุม อำนวยการสั่งการและกำกับดูแลการดำเนินงานของทุกเหล่าทัพ ในการเตรียมกำลังเพื่อการป้องกันราชอาณาจักรและปฏิบัติการใช้กำลังทหารภายใต้อำนาจหน้าที่ของกระทรวงกลาโหมให้เกิดประสิทธิภาพสูงสุด โดยมีผู้บัญชาการทหารสูงสุด เป็นผู้บังคับบัญชารับผิดชอบ

๕) มาตรา ๒๙ กำหนดโครงสร้างการฝึกและการศึกษาของทหารและข้าราชการพลเรือนในสังกัดกระทรวงกลาโหมให้เป็นไปตามนโยบายที่กระทรวงกลาโหมกำหนดโดยให้กองบัญชาการกองทัพไทยรับผิดชอบการฝึกและศึกษาในระดับยุทธศาสตร์ ทั้งในการปฏิบัติการร่วมของกองทัพไทยและการปฏิบัติการของกองบัญชาการกองทัพไทย ขณะที่กองทัพบก กองทัพเรือ และกองทัพอากาศรับผิดชอบการฝึกและการศึกษาในระดับยุทธการและยุทธวิธี

๖) มาตรา ๓๑ กำหนดให้กองบัญชาการกองทัพไทยวางแผน พัฒนาและดำเนินการเกี่ยวกับระบบควบคุมบังคับบัญชากองทัพไทย เพื่อให้สามารถติดต่อเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ ทั้งในระดับรัฐบาล ระดับกระทรวง และหน่วยงานในกระทรวงกลาโหมตลอดจนการแบ่งมอบความรับผิดชอบการดำเนินการดังกล่าวให้กับเหล่าทัพและส่วนราชการที่เกี่ยวข้องตามความเหมาะสม

๗) มาตรา ๓๙ บัญญัติให้กองทัพไทยจัดตั้งศูนย์บัญชาการทางทหารในแต่ละระดับขึ้นตั้งแต่ยามปกติเพื่อใช้ในการ

ติดตามสถานการณ์และทำหน้าที่เป็นศูนย์ควบคุม อำนวยการ และสั่งการการปฏิบัติการทางทหาร โดยศูนย์บัญชาการทางทหารของกองบัญชาการกองทัพไทย มีหน้าที่ควบคุม อำนวยการและสั่งการศูนย์บัญชาการทางทหาร ในแต่ละระดับดังกล่าว หรือควบคุมกองกำลังเฉพาะกิจร่วมที่จัดตั้งขึ้นตามแผนป้องกันประเทศ แล้วแต่กรณี

๒.๑.๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ซึ่งเป็นกฎหมายหลักด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ กฎหมายฉบับนี้กำหนดว่าการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมุ่งสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของประเทศ มีประเด็นที่เกี่ยวข้องดังนี้

๑) คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ถูกจัดตั้งขึ้นเพื่อกำหนดนโยบายและแผนทางด้านไซเบอร์ของประเทศ โดยมีรัฐมนตรีว่าการกระทรวงกลาโหม เป็นกรรมการโดยตำแหน่ง

๒) สำนักงานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ยังได้รับมอบหมายให้กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสารสนเทศสำคัญของประเทศ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ไม่ให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อบภายในประเทศ

๓) มาตรา ๙ พระราชบัญญัติฉบับนี้กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีนายกรัฐมนตรีเป็นประธาน มีหน้าที่จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เสนอต่อคณะรัฐมนตรีเพื่อใช้เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในสถานการณ์ยามปกติและในสภาวะที่มีภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติตลอดจนกรอบนโยบายและแผนแม่บทด้านความมั่นคงที่เกี่ยวข้องของสภาความมั่นคงแห่งชาติ

๔) มาตรา ๑๒ ได้จัดตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) โดยให้ผู้บัญชาการทหารสูงสุดเป็นคณะกรรมการโดยตำแหน่ง

๕) มาตรา ๑๔ ได้วางกรอบความร่วมมือในการสนับสนุน สำนักงานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ในการแก้ไขปัญหา และรับมือกับภัยคุกคามทางไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ

๖) จัดตั้งคณะกรรมการรับมือภัยคุกคามในระดับร้ายแรง (ครร.) โดยมีผู้บัญชาการทหารสูงสุด เป็นกรรมการโดยตำแหน่ง

๒.๑.๓ นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕-๒๕๗๐)

เป็นแผนระดับ ๓ เพื่อใช้ในการขับเคลื่อนภารกิจในด้านการรักษาความมั่นคงปลอดภัยของประเทศ ซึ่งเป็นแผนระดับชาติ ทั้งนี้ ได้กำหนดบทบาทให้กองบัญชาการกองทัพไทยและ

หน่วยงานโครงสร้างพื้นฐานสำคัญต่างๆ ต้องดำเนินภารกิจ ตามนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- กลยุทธ์ ๑.๑ การเพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์

- กลยุทธ์ ๑.๒ การสร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรและประชาชน

- กลยุทธ์ ๑.๓ การส่งเสริมการวิจัยและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

- กลยุทธ์ ๔.๑ การเพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒.๑.๔ ประกาศ/ระเบียบของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) คณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ (กกม.) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

อ้างอิงประมวลแนวทางและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๔ และแผนรับมือเหตุการณ์ทางไซเบอร์เพื่อใช้เป็นแนวทางและมาตรฐานในการดำเนินงานอย่างเป็นระบบ

๒.๒ หลักการสำคัญต่าง ๆ ที่เกี่ยวข้อง

๑) แผนการพัฒนาทางไซเบอร์เพื่อความมั่นคงกระทรวงกลาโหม (พ.ศ. ๒๕๖๖-๒๕๗๐) กำหนดแนวทางการพัฒนา

ศักยภาพด้านไซเบอร์และการปฏิบัติการทางไซเบอร์ เพื่อเสริมสร้างความแข็งแกร่งในการรักษาความปลอดภัยทางไซเบอร์จากภัยคุกคามทั้งภายในและภายนอกประเทศ ตลอดจนสร้างความเชื่อมั่นการใช้เทคโนโลยีดิจิทัลให้มีประสิทธิภาพและเหมาะสมกับการปฏิบัติภารกิจ อีกทั้งยังให้ความสำคัญกับการบริหารจัดการปัจจัยแวดล้อมที่เอื้ออำนวยต่อการใช้ไซเบอร์อย่างมีประสิทธิภาพ โดยมุ่งลดจุดอ่อนหรือจุดล่อแหลมที่อาจส่งผลต่อการปฏิบัติภารกิจ พร้อมทั้งเสริมสร้างเอกภาพ ในการเตรียมกำลังและใช้ศักยภาพทางไซเบอร์ผ่านกำกับดูแลที่เป็นระบบและการแบ่งแยกขอบเขตการปฏิบัติที่ชัดเจน

๒) ยุทธศาสตร์ทหารด้านสงครามไซเบอร์ กองบัญชาการกองทัพไทย (พ.ศ. ๒๕๕๘) และ หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ กองบัญชาการกองทัพไทย (พ.ศ. ๒๕๖๑) กำหนดแนวทางการปฏิบัติการทาง ไซเบอร์ที่ครอบคลุมการดำเนินงานใน ๓ ลักษณะ ได้แก่ การปฏิบัติการทางไซเบอร์เชิงรับ (Defensive Cyber Operations: DCO) การปฏิบัติการทางไซเบอร์เชิงป้องปราม (Offensive Cyber Operations: OCO) การปฏิบัติการสารสนเทศและเครือข่าย (Information and Network Operations: INO)

๓) นโยบายของรัฐมนตรีว่าการกระทรวงกลาโหม (รมว.กห.) ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ มุ่งเน้นการพัฒนากองทัพให้ทันสมัยและมีศักยภาพ เป็นกลไกหลักด้านความมั่นคงของรัฐในศตวรรษที่ ๒๑ โดยต้องสามารถตอบโต้ภัยคุกคามได้ทุกรูปแบบ และเป็นที่พึ่งของประชาชนในทุกสถานการณ์ ทั้งในด้าน

ความมั่นคงและการช่วยเหลือประชาชน รวมถึงสนับสนุนการพัฒนาประเทศเพื่อความมั่นคงอย่างยั่งยืน

๒.๓ แนวทางการเตรียมการทางไซเบอร์ของกองบัญชาการกองทัพไทย

๒.๓.๑ การเตรียมกำลังและการใช้กำลังทางไซเบอร์ของกองบัญชาการกองทัพไทย

๑) การเตรียมกำลัง ได้มีการดำเนินการปรับโครงสร้างหน่วยงานทางไซเบอร์ พัฒนาบุคลากรทางไซเบอร์ กระบวนการปฏิบัติงาน และพัฒนาเครื่องมือเทคโนโลยีให้มีประสิทธิภาพอย่างต่อเนื่อง

๒) การใช้กำลังทางไซเบอร์ ได้มีการจัดตั้ง ศูนย์ปฏิบัติการร่วมทางไซเบอร์ ภายใต้ศูนย์บัญชาการทางทหาร (ศรช.ศบท. หรือ Joint Cyberspace Operations Center : JCOC) เพื่อบูรณาการการปฏิบัติการร่วมทางไซเบอร์ร่วมกับเหล่าทัพ และหน่วยงานที่เกี่ยวข้องในระดับประเทศ โดยดำเนินการติดตามเฝ้าระวัง และบริหารจัดการเหตุการณ์ภัยคุกคามทางไซเบอร์ทั้งยามปกติและยามวิกฤติหรือยามสงคราม ตลอดจนการปฏิบัติการด้านข่าวกรองทางไซเบอร์ ทั้งในระดับกองบัญชาการกองทัพไทย เหล่าทัพ และระดับประเทศ

๒.๓.๒ เหตุผลและความจำเป็นในการจัดตั้งหน่วยบัญชาการไซเบอร์ทหาร

๑) เพื่อปรับปรุงโครงสร้างหน่วยงานทางไซเบอร์ของกองทัพให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ตามนโยบายรัฐมนตรีว่าการกระทรวงกลาโหม ที่มุ่งปฏิรูปกองทัพให้มี

ความทันสมัย ลดขนาดกำลังพลหลัก มุ่งเน้นการพัฒนาเทคโนโลยีในด้านการป้องกันประเทศ

๒) เพื่อปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการสนับสนุน สกมช. ในการแก้ไขปัญหาและรับมือกับภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (CII) ซึ่งครอบคลุม ๗+๑ ด้าน ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงิน การธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่นๆตามที่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติ (ศรบ.) ประกาศกำหนดเพิ่มเติม ทั้งนี้ เป็นไปตาม มาตรา ๑๔ ของพระราชบัญญัติดังกล่าวที่กำหนดให้หน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ต้องทำงานร่วมกับหน่วยงานอื่น ๆ ในระดับประเทศ

๓) เพื่อการปฏิบัติการร่วม (Joint Warfighting Functions) โดยมี ศูนย์ปฏิบัติการร่วมทางไซเบอร์ ศูนย์บัญชาการทางทหาร (ศรซ.ศบท.) เป็นศูนย์กลางในการปฏิบัติการทางไซเบอร์ร่วมกับเหล่าทัพตามแนวคิด “การปฏิบัติการไซเบอร์ภายใต้การปฏิบัติการหลายมิติ” เพื่อเพิ่มขีดความสามารถทางไซเบอร์ทั้งในเชิงรับเชิงป้องปราม และการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ นอกจากนี้ยังมีการจัดเตรียมชุดเคลื่อนที่เร็วเพื่อสนับสนุนการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ได้แก่ ชุดปฏิบัติการป้องกันทางไซเบอร์ (Cyber Protection Team: CPT) ชุดปฏิบัติการเชิงรุกทางไซเบอร์

(Cyber Combat Mission Team: CCMT) และชุดปฏิบัติการด้านโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Cyber National Mission Team: CNMT) โดยชุดปฏิบัติการเหล่านี้จะอยู่ภายใต้การควบคุมทางยุทธการกับ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ ศูนย์บัญชาการทางทหาร (ศรซ.ศบท.) เตรียมพร้อมในการปฏิบัติเพื่อสนับสนุนการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ในระดับกองทัพไทย และระดับประเทศ

๓. กรอบยุทธศาสตร์สำหรับความมั่นคงปลอดภัยทางไซเบอร์

๓.๑ กรอบความคิด

๓.๑.๑ วิสัยทัศน์ หน่วยบัญชาการไซเบอร์ทหาร มีความสามารถในการปฏิบัติการทางไซเบอร์ และการปฏิบัติการร่วมทางไซเบอร์ ซึ่งเป็นหนึ่งในห้ามิติการรบในการปฏิบัติการหลายมิติ และประสานสอดคล้องกับการปฏิบัติการคลื่นแม่เหล็กไฟฟ้า และการปฏิบัติการรบด้านอื่น ๆ ทั้งในและนอกการปฏิบัติการหลายมิติของกองทัพไทย อีกทั้งยังมีความสามารถในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศตลอดจนแก้ปัญหาทางไซเบอร์กับหน่วยงานที่เกี่ยวข้องให้เกื้อกูลกับการรักษาผลประโยชน์ของชาติ และความมั่นคงของประเทศ รวมถึงมีขีดความสามารถในการปฏิบัติการร่วม-ผสมทางไซเบอร์ที่เพียงพอกับหน่วยงานทางไซเบอร์ของกองทัพนานาชาติ

๓.๑,๒ ภารกิจ วางแผน กำกับดูแล ประสานงาน ประสานสอดคล้องกับการปฏิบัติการทางไซเบอร์และการปฏิบัติการร่วมทางไซเบอร์ ทั้งในและผ่านมิติทางไซเบอร์ ให้เกิดเสรีในการเตรียมกำลังและใช้กำลังในทุกมิติ ตลอดจนประสานสอดคล้องกับการ

ปฏิบัติการคลื่นแม่เหล็กไฟฟ้า และปฏิบัติการรบด้านอื่น ๆ ของกองทัพไทย นำไปสู่การตัดสินใจที่เหนือกว่าฝ่ายตรงข้าม รวมทั้งการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ดำรงไว้ซึ่งสภาวะที่เกื้อกูลต่อการปฏิบัติการทางทหาร และพร้อมเข้าสู่สงครามที่มีมิติไซเบอร์เป็นมิติการรบในการปฏิบัติการหลายมิติ เพื่อรักษาผลประโยชน์ของชาติและความมั่นคงของประเทศ

๓.๑.๓ แนวความคิดในการปฏิบัติการทางไซเบอร์

ป้องกันมิติไซเบอร์ในความรับผิดชอบ ทั้งในระดับยุทธการและยุทธศาสตร์ ตั้งแต่ยามปกติ ประกอบด้วย การปฏิบัติการทางไซเบอร์เชิงป้องปราม (Offensive Cyberspace Operations: OCO) การปฏิบัติการทางไซเบอร์เชิงรับ (Defensive Cyberspace Operations: DCO) และการปฏิบัติการสารสนเทศและเครือข่าย (Information Network Operations: INO) เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์จากการโจมตีของฝ่ายตรงข้าม สามารถป้องกันไม่ให้ฝ่ายตรงข้ามเข้ามาในมิติทางไซเบอร์ของฝ่ายเรา ขณะเดียวกันสนับสนุนให้ฝ่ายเราสามารถเข้าไปในมิติทางไซเบอร์ของฝ่ายตรงข้าม สอดคล้องตามขั้นตอนการปฏิบัติ ตลอดห้วงเวลาการปฏิบัติการ และมีความพร้อมในการใช้การปฏิบัติการทางไซเบอร์ได้ทันที เมื่อความขัดแย้งระหว่างกำลังฝ่ายเรากับฝ่ายตรงข้ามไม่สามารถยุติได้ การปฏิบัติการดังกล่าวครอบคลุมการป้องกันระบบเครือข่ายสารสนเทศของกองบัญชาการกองทัพไทย การบูรณาการให้เกิดการปฏิบัติการร่วมในมิติไซเบอร์ในระดับกองทัพไทย และเป็นหน่วยงานหลักในการแก้ไข

ปัญหาเหตุการณ์ทางไซเบอร์ในระดับประเทศ ผ่านสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๓.๒ **เป้าหมาย: Ends**

ในการขับเคลื่อนการเสริมสร้างความมั่นคงปลอดภัยและปกป้องผลประโยชน์ของประเทศอย่างยั่งยืน จำต้องมุ่งเน้นการเสริมสร้างขีดความสามารถในด้านการปฏิบัติการทางไซเบอร์ การปกป้องโครงสร้างพื้นฐานสำคัญ ตลอดจนการสนับสนุนความร่วมมือในระดับชาติและนานาชาติ ได้กำหนดเป้าหมายสำคัญไว้ดังนี้

- **เป้าหมายที่ ๑** มีขีดความสามารถปฏิบัติการทางไซเบอร์และการปฏิบัติการร่วมทางไซเบอร์ ซึ่งเป็นหนึ่งใน ๕ มิติการรบในการปฏิบัติการหลายมิติ และประสานสอดคล้องกับการปฏิบัติการต่างๆ ทั้งในและนอกการปฏิบัติการรบหลายมิติ เช่น การปฏิบัติการคลื่นแม่เหล็กไฟฟ้า
- **เป้าหมายที่ ๒** มีขีดความสามารถปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ตลอดจนแก้ปัญหาทางไซเบอร์กับหน่วยงานที่เกี่ยวข้องให้เกื้อกูลกับความมั่นคงของประเทศและปกป้องผลประโยชน์ของชาติ
- **เป้าหมายที่ ๓** มีขีดความสามารถปฏิบัติการร่วม-ผสมทางไซเบอร์ที่เพียงพอกับหน่วยงานทางไซเบอร์ของกองทัพนานาชาติ
- **เป้าหมายที่ ๔** มีขีดความสามารถในการลดขีดความสามารถ ขัดขวาง ทำลาย และควบคุมฝ่ายตรงข้าม

๓.๓ วิธีการ: Ways

เพื่อให้การเดินทางไปสู่เป้าหมายต่าง ๆ ได้อย่างถูกต้องและมีทิศทาง โดยใช้การพิจารณา 3 เสาหลัก ได้แก่ ทรัพยากรบุคคล กระบวนการ และเทคโนโลยี (**People-Process-Technology**) ดังนี้

- **เป้าหมายที่ ๑**

People ➔ ทรัพยากรบุคคล ประกอบด้วย ผู้บังคับบัญชา ฝ่ายอำนวยการ ชุดปฏิบัติการทางไซเบอร์ (CPT), ชุดปฏิบัติการทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CNMT) ดูหัวข้อ ๔) ทีมสนับสนุนและช่วยสนับสนุนการปฏิบัติการทางไซเบอร์ ได้แก่ ข่าวกรองภัยคุกคามทางไซเบอร์ (CTI), ทีมสนับสนุนวิเคราะห์ทางไซเบอร์ (AST), ทีมประเมินภัยคุกคามทางไซเบอร (CAT), ทีมสนับสนุนภารกิจทางไซเบอร์ (MST) ดูหัวข้อ ๔) แนวร่วมนักรบอาสาทางไซเบอร์ พันธมิตรในการปฏิบัติการร่วม พนักงานราชการเชี่ยวชาญพิเศษ **มีการพัฒนาบุคลากร** โดยโรงเรียนไซเบอร์ทหารที่มีหลักสูตรทางไซเบอร์ขั้นพื้นฐาน ขั้นกลาง ขั้นสูง และด้านฝ่ายอำนวยการ **มีศูนย์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อความเป็นเลิศ** ในการสร้างเครือข่ายบุคลากรไซเบอร์ งานวิจัยทางไซเบอร์ งานประชาสัมพันธ์สร้างความตระหนักรู้ทางไซเบอร์ งานวิชาการทางไซเบอร์ รวมถึงการพัฒนาบุคลากรผ่านหลักสูตรภายนอกโดยสถาบันรับรองที่มีมาตรฐาน และสถาบันการศึกษาทั้งในและต่างประเทศ **มีการฝึกฝนความชำนาญให้กับบุคลากร** ผ่านการฝึกร่วมของกองทัพไทย การฝึกเป็นหน่วย การฝึกตามหน้าที่ การจัดการฝึกบริหารวิกฤตการณ์ระดับชาติ การฝึกกับศูนย์ปฏิบัติการ

ต่อต้านการก่อการร้ายสากล การแข่งขันทักษะทางไซเบอร์ครอบคลุมทุกระดับการศึกษา การจัด Cyber Bootcamp ระดับมัธยมศึกษา **มีระบบ Recruit and Talent Management**

Process ➔ กรอบแนวคิด ยุทธศาสตร์ (White Paper) หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐมนตรีว่าการกระทรวงกลาโหม และผู้บัญชาการทหารสูงสุด แผนรับมือภัยคุกคามทางไซเบอร์กองบัญชาการกองทัพไทย สนับสนุนสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แผนปฏิบัติการทางไซเบอร์ (ผนวก ซ) ประกอบแผนป้องกันประเทศ กฎหมาย พระราชบัญญัติ กฎกระทรวง กฎการใช้กำลัง ที่เกี่ยวข้อง และมาตรฐานขั้นตอนการทำงาน การดำเนินการต่าง ๆ ได้แก่ การประเมินความเสี่ยง การตรวจประเมินทางไซเบอร์ที่เป็นมาตรฐาน การปฏิบัติการด้านการข่าวกรองทางไซเบอร์ที่มีประสิทธิภาพ การสร้างความร่วมมือด้านข้อมูลข่าวสารกับหน่วยงานทั้งในและนอกประเทศ รวมทั้งการดำเนินงานภายใต้กรอบความร่วมมือประชาคมไซเบอร์กองทัพไทย

Technology ➔ เทคโนโลยี ประกอบด้วย **โรงเรียนไซเบอร์ทหาร** มี Online Course System, Cyber Range & Simulation, Training Center, Training Labs, Operational Technology (OT) Labs **ศูนย์ปฏิบัติการร่วมทางไซเบอร์** มี Joint Cyber Operation Center (JCOC), Cyber-C2 Technology, Protect & Detect Response, Cyber Threat Intelligence, Cloud

& Edge Computing, Post-Quantum Cryptography (PQC) Technology, Zero Trusted Architecture Technology, Internet of Things (IOT), Industrial Internet of Things (IIOT) **มีเทคโนโลยีในการสนับสนุนทีมปฏิบัติการ** Cyber Deployment Platform Technologies, Forensics, Big DATA, Artificial Intelligence (AI), Geographic Information System

เป้าหมายที่ ๒

People ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เน้น** ชุดปฏิบัติการทางไซเบอร์สองชุด คือ ชุดปฏิบัติการทางไซเบอร์ (CPT), ชุดปฏิบัติการทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CNMT) และ **เพิ่มเติมการฝึก** รับมือเหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) กับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

Process ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เน้น**แผนรับมือภัยคุกคามทางไซเบอร์ กองทัพไทย(ทท.) สนับสนุน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และ**เพิ่มเติมการดำเนินการ** สร้างความร่วมมือด้านข่าวสารข้อมูลกับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

Technology ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เน้น** ห้องปฏิบัติการเทคโนโลยีปฏิบัติการ (OT Labs) และ**เพิ่มเติมห้องปฏิบัติการ** ห้องจำลองการฝึกเฝ้าระวังเหตุการณ์ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งครอบคลุม ๗+๑ **เป้าหมายที่ ๓**

People ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เพิ่มเติมการฝึก** การฝึกร่วม/ผสม กับเหล่าทัพและกองกำลังต่างชาติ ประกอบด้วย กลุ่ม Bilateral เช่น US, UK, AUS, Singapore, Malaysia, Indonesia เป็นต้น และกลุ่ม Multilateral เช่น Cobra Gold, Cyber Flag, Cyber Marvel, Talisman Sabre เป็นต้น รวมถึง การฝึกปฏิบัติการร่วมทางไซเบอร์ขั้นสูง เชิญหน่วยงานต่างประเทศ เข้าร่วมการแข่งขันทักษะทางไซเบอร์

Process ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เพิ่มเติมการดำเนินการ** การประสานความร่วมมือกับต่างประเทศ ได้แก่ Cyber Defense Working Group (CDWG), Significant Security Cooperation Initiative (SSCI), ASEAN Defense Ministers' Meeting (ADMM) ด้าน Cyber และ**การปฏิบัติการ** Joint Cyberspace Operations Task Force Deployment, Cyber Threat Intelligence (CTI) Sharing เป็นต้น

Technology ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เพิ่มเติมในส่วนโรงเรียนฯ** ให้สามารถสนับสนุนระบบ Integrated Multinational Cyber Information sharing and Training Environment (IMCITE) จาก CDWG ซึ่งเป็นหลักสูตรทางไซเบอร์แบบออนไลน์ เป็นต้น

● เป้าหมายที่ ๔

People ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เพิ่มเติมผู้เชี่ยวชาญ**ด้าน Network, Website, Mobile, Malware **เพิ่มเติมหลักสูตร** การพัฒนาช่องโหว่ (Exploit) การพัฒนา Malware และ

เพิ่มเติมการฝึก การฝึกร่วมผสมทางไซเบอร์ระดับ กองบัญชาการกองทัพไทย, กองทัพไทย, และนานาชาติ

Process ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เพิ่มเติมกรอบแนวคิด** National Institute of Standards and Technology (NIST) 800-115, SANS' Red Team Framework and Methodology (RTFM) และ Open Web Application Security Project (OWASP) ในยุทธศาสตร์ หลักนิยมฯ และ**การดำเนินการ** ตามคู่มือการปฏิบัติการแบบ Red Team

Technology ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ **เพิ่มเติมในส่วนโรงเรียนฯ** ระบบฝึกทักษะป้องปรามทางไซเบอร์ **เพิ่มส่วนสนับสนุนการปฏิบัติการ** การเตรียม Platform เชิงป้องปรามที่เกี่ยวข้อง

๓.๔ ทรัพยากร: Means

การขับเคลื่อนสู่เป้าหมายทั้ง ๔ ต้องอาศัยทรัพยากรที่หลากหลาย ประกอบด้วย

๑) หน่วยงาน ประกอบด้วยทั้งภาครัฐและเอกชนที่จะสนับสนุนหนทางปฏิบัติ

- ภาครัฐ ได้แก่ กระทรวงกลาโหม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงศึกษาธิการกองทัพไทย กองบัญชาการกองทัพไทย หน่วยบัญชาการไซเบอร์ทหาร ศูนย์ปฏิบัติการร่วมทางไซเบอร์ โรงเรียน ไซเบอร์ทหาร ศูนย์ไซเบอร์ของเหล่าทัพ และสำนักงานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- ภาคเอกชน ได้แก่ บริษัทด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT) บริษัทด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในและต่างประเทศ สถาบันการศึกษาของเอกชน สถาบันการศึกษาของต่างประเทศ สถาบันฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์

๑) ทรัพยากรบุคลากร เป็นหัวใจสำคัญ เช่น ผู้บังคับบัญชาระดับต่าง ๆ ที่มีความเข้าใจและตระหนักถึงความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ ข้าราชการทหารทุกระดับใน กองทัพไทย (ทท.), กองบัญชาการกองทัพไทย (บก.ทท.) และเหล่าทัพที่เป็นเจ้าหน้าที่ปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในส่วนต่าง ๆ พันธกิจของหน่วยบัญชาการไซเบอร์ ที่ปรึกษาจากเอกชนที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์

๒) ทรัพยากรด้านเทคโนโลยี ได้แก่ระบบต่าง ๆ ที่มีความจำเป็นในการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ เช่น ระบบตรวจจับภัยคุกคามขั้นสูง (Intrusion Detection Systems และ SIEM) ซอฟต์แวร์ป้องกันมัลแวร์ ระบบวิเคราะห์ข้อมูลข่าวกรอง และเครื่องมือสำหรับการเจาะระบบและจำลองสถานการณ์ (Penetration Testing Tools) เป็นต้น

๓) งบประมาณและการลงทุน ในการพัฒนาโครงสร้างพื้นฐาน เช่น ศูนย์ข่าวกรองไซเบอร์ ศูนย์ฝึกซ้อม (Cyber Range) และห้องสมุดดิจิทัล เป็นสิ่งสำคัญสำหรับสร้างความมั่นคงระยะยาว

๔) ความร่วมมือระหว่างประเทศและองค์กรในประเทศ เช่น หน่วยงานภาครัฐ ภาคเอกชน และพันธมิตรระหว่างประเทศที่ช่วยเสริมการแบ่งปันข้อมูลและพัฒนามาตรฐานร่วมกัน

๕) นโยบายและกฎหมาย ที่สนับสนุนการทำงาน เช่น การคุ้มครองข้อมูลและความปลอดภัยในระบบไซเบอร์ เพื่อช่วยเพิ่มความน่าเชื่อถือในการปฏิบัติการ

๖) โครงสร้างพื้นฐานดิจิทัลที่ปลอดภัย เช่น เครือข่ายสื่อสารที่เข้ารหัสและการจัดเก็บข้อมูลสำรองเพื่อป้องกันเหตุการณ์ฉุกเฉิน รวมถึงการสร้างความตระหนักรู้แก่ประชาชนและบุคลากรในทุกระดับ เพื่อเสริมสร้างภูมิคุ้มกันทางไซเบอร์ที่ยั่งยืน

๔. ขีดความสามารถที่ต้องการทางไซเบอร์ตามกรอบยุทธศาสตร์

การเสริมสร้างขีดความสามารถทางไซเบอร์เป็นสิ่งจำเป็นอย่างยิ่งและเป็นหัวใจสำคัญในการบรรลุเป้าหมาย (Ends) ของกองทัพไทย ขีดความสามารถทางไซเบอร์ที่ต้องการประกอบด้วยส่วนต่าง ๆ ดังนี้

๔.๑ ทรัพยากรบุคคล (People)

๔.๑.๑ บุคลากร

๑) ผู้บังคับบัญชา และฝ่ายอำนวยการ: สามารถบริหารงาน วางแผนปฏิบัติการทางไซเบอร์ มีความเข้าใจในยุทธศาสตร์ หลักนิยม และเทคโนโลยีเกี่ยวกับการปฏิบัติการทางไซเบอร์ เพื่อให้การสั่งการหรือการให้แนวทางปฏิบัติมีประสิทธิภาพ

๒) ชุดปฏิบัติการป้องกันทางไซเบอร์ (Cyber Protection Team: CPT) สามารถปกป้องเครือข่ายข้อมูล โครงสร้าง

สารสนเทศของกองทัพไทย หน่วยงานราชการ และเอกชน รวมถึงการสนับสนุนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

๓) ชุดปฏิบัติการทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CNMT) มีขีดความสามารถเช่นเดียวกับ ชุดปฏิบัติการป้องกันทางไซเบอร์ (CPT) และมุ่งเน้นการป้องกันระบบเทคโนโลยีปฏิบัติการ (Operational Technology: OT) ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของประเทศ

๔) ชุดปฏิบัติการข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence: CTI) สามารถรวบรวมข้อมูล วิเคราะห์แหล่งที่มา ติดตาม คาดการณ์ภัยคุกคามในอนาคต ประเมินความเสี่ยง และผลกระทบ รวมถึงการสร้างกลยุทธ์ในการป้องกันภัยคุกคามทางไซเบอร์เชิงป้องปราม

๕) ชุดปฏิบัติการด้านการวิเคราะห์ทางไซเบอร์ (Analyst Support Team: AST) สามารถรวบรวมข้อมูลภัยคุกคามและมัลแวร์ วิเคราะห์พฤติกรรม ช่องโหว่ในระบบ ข้อมูลย้อนกลับการแพร่กระจายของมัลแวร์ และประเมินผลกระทบจากการโจมตีเพื่อวางแผนการป้องกันอย่างมีประสิทธิภาพ

๖) ชุดตรวจประเมินทางไซเบอร์ (Cyber Audit Team: CAT) สามารถประเมินความเสี่ยงทางไซเบอร์ ตรวจสอบและวิเคราะห์ข้อมูลในเครือข่าย ประเมินความปลอดภัยของแอปพลิเคชัน ตรวจสอบระบบควบคุมการเข้าถึง ตรวจสอบการตั้งค่าความปลอดภัยของระบบปฏิบัติการ การประเมินผลกระทบของเหตุการณ์

ทางไซเบอร์ ตลอดจนการตรวจสอบความพร้อมของแผนรับมือเหตุการณ์ฉุกเฉิน

๗) ชุดสนับสนุนการช่วยปฏิบัติการทางไซเบอร์ (Mission Support Team: MST) สามารถแก้ไขปัญหาซอฟต์แวร์ ฮาร์ดแวร์ อุปกรณ์เครือข่าย เซิร์ฟเวอร์และระบบคลาวด์ ตรวจสอบแก้ไขปัญหาการเชื่อมต่อเครือข่าย และโครงสร้างสายสัญญาณ

๔.๑.๒ การพัฒนาบุคลากร โรงเรียนไซเบอร์ทหารสามารถออกแบบหลักสูตรทางไซเบอร์ขั้นพื้นฐาน ขั้นกลาง ขั้นสูง และด้านฝ่ายอำนวยการ เพื่อผลิตบุคลากรในข้อ ๔.๑.๑ รวมถึงสามารถประเมินผลหลักสูตร ตามแนวทางการประกันคุณภาพการศึกษาที่ กองบัญชาการกองทัพไทย (บก.ทท.) กำหนด

๔.๑.๓ ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อความเป็นเลิศ เป็นแกนนำในการสร้างเครือข่ายบุคลากรทางไซเบอร์ ดำเนินกิจกรรมทางวิชาการและงานวิจัยทางไซเบอร์ ประชาสัมพันธ์สร้างความตระหนักรู้ทางไซเบอร์ รวมถึงพัฒนาบุคลากรผ่านหลักสูตรที่มีสถาบันรับรองมาตรฐานทั้งในและต่างประเทศ

๔.๑.๔ การฝึกฝนความชำนาญให้กับบุคลากร หน่วยบัญชาการไซเบอร์ทหาร (นซบ.ทหาร) สามารถนำบุคลากรทางไซเบอร์ในกลุ่มงานต่าง ๆ เข้ารับการฝึกร่วมของกองทัพไทย การฝึกเป็นหน่วย การฝึกตามหน้าที่ การจัดการฝึกบริหารวิกฤตการณ์ระดับชาติ (National Crisis Management Exercise: C-MEX) ร่วมกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) การฝึกรับมือเหตุการณ์ทาง ไซเบอร์ที่

เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) การฝึกกับศูนย์ปฏิบัติการต่อต้านการก่อการร้ายสากล การฝึกร่วม/ผสม กับเหล่าทัพและกองกำลังต่างชาติทั้งแบบ Bilateral; US UK AUS Singapore Malaysia, Indonesia และ Multilateral; Cobra Gold, Cyber Flag, Cyber Marvel, Talisman Sabre รวมถึงการฝึกปฏิบัติการร่วมทางไซเบอร์ขั้นสูง

๔.๑.๕ มีระบบ Recruit and Talent Management สามารถคัดเลือกบุคลากรที่มีประสิทธิภาพเข้าประจำการ และบริหารจัดการกลุ่มคนเหล่านั้นได้อย่างเหมาะสม ผ่านการจัดการแข่งขันทักษะทางไซเบอร์ (ระดับกองทัพไทย หน่วยงานรัฐ เอกชน และหน่วยงานต่างประเทศ ระดับโรงเรียนทหาร-ตำรวจ ระดับนักเรียนทหาร และมัธยมศึกษา) จัดกิจกรรม Cyber Bootcamp ระดับมัธยมศึกษา เพื่อประชาสัมพันธ์และสร้างฐานข้อมูลบุคลากรที่มีความสามารถทางไซเบอร์เพื่อเลือกใช้งาน รวมถึงสามารถคัดเลือกแนวร่วมนักรบอาสาทางไซเบอร์ พันธมิตรในการปฏิบัติการร่วม พนักงานราชการเชี่ยวชาญพิเศษ รวมถึงผู้เชี่ยวชาญด้าน Network, Website, Mobile, Malware มาเสริมกำลังทั้งการป้องกัน โจมตี ป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และงานด้านการสนับสนุนการปฏิบัติการ ฯ

๔.๒ กระบวนการ (Process)

๔.๒.๑ กรอบแนวคิด สามารถพัฒนายุทธศาสตร์ (White Paper) หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ที่สนับสนุนแนวคิด Multi-Domain Operations (MDO), National Institute of

Standards and Technology (NIST 800-115), SANS' Red Team Framework and Methodology (RTFM) และ Open Web Application Security Project (OWASP) รวมถึงการพัฒนานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ รัฐมนตรีกระทรวงกลาโหม (รมว.กห.) และ ผู้บัญชาการทหารสูงสุด (ผบ.ทสส.) แผนรับมือภัยคุกคามทางไซเบอร์ กองทัพไทย (ทท.) สนับสนุน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ผนวก ซ การปฏิบัติการทางไซเบอร์ ประกอบแผนป้องกันประเทศ กฎหมาย, พระราชบัญญัติ, กฎกระทรวง กฎการใช้กำลัง (Rules of Engagement: ROE) ที่เกี่ยวข้อง และมาตรฐานขั้นตอนการทำงาน (Standard Operating Procedure: SOP) ในบริบทที่สัมพันธ์กันกับยุทธศาสตร์และหลักนิยม ฯ

๔.๒.๒ การดำเนินการต่าง ๆ สามารถดำเนินการประเมินความเสี่ยง ตรวจประเมินทางไซเบอร์ที่เป็นมาตรฐาน ปฏิบัติการด้านการข่าวไซเบอร์ที่มีประสิทธิภาพ สร้างความร่วมมือด้านข่าวสารข้อมูลกับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน่วยงานอื่นทั้งในและนอกประเทศ ดำเนินงานประชาคมไซเบอร์กองทัพไทย ประสานความร่วมมือกับต่างประเทศ ได้แก่ CDWG SSCI ADMM (Cyber) ปฏิบัติตามคู่มือการปฏิบัติการแบบ Red Team รวมถึงการปฏิบัติการ Joint Cyberspace Operations Task Force Deployment และ CTI Sharing

๔.๓ เทคโนโลยี (Technology)

๔.๓.๑ โรงเรียนไซเบอร์ทหาร มีห้องปฏิบัติการคอมพิวเตอร์สำหรับการเรียนและฝึกฝนอย่างพอเพียง มีระบบ Online Course ที่สามารถสนับสนุนการศึกษาด้วยตนเองสำหรับบุคลากรในข้อ ๔.๑.๑ รวมถึงระบบ Online Course ที่ได้รับการสนับสนุนจากต่างประเทศเช่น ระบบ IMCITE เป็นต้น มีระบบ Cyber Range & Simulation, Training Center, Training Labs ทางไซเบอร์ที่ต้องการอย่างครบถ้วน มี ห้องปฏิบัติการเทคโนโลยีปฏิบัติการ (Operational Technology Lab: OT Lab) ที่เป็นห้องจำลองการฝึกเฝ้าระวังเหตุการณ์ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

๔.๓.๒ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ มีเครื่องมือที่จำเป็นในการปฏิบัติงานได้แก่ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ (Joint Cyber Operations Center: JCOC) และ เทคโนโลยีการบังคับบัญชาและควบคุมทางไซเบอร์ (Cyber Command and Control Technology: Cyber-C2 Technology) ใช้วางแผน ควบคุม และประสานงาน Protect & Detect Response ใช้ป้องกันและตอบสนองต่อภัยคุกคาม Cyber Threat Intelligence ใช้วิเคราะห์ภัยคุกคามและให้ข้อมูลเชิงลึก Cloud & Edge Computing รองรับการจัดเก็บและประมวลผลข้อมูลจำนวนมาก Post Quantum Cryptography Technology ใช้การเข้ารหัสที่ป้องกันการโจมตีจากคอมพิวเตอร์ควอนตัมในอนาคต Zero Trusted Architecture

Technology ปฏิบัติการบนหลักการ “ไม่เชื่อถือใคร” โดยตรวจสอบทุกการเข้าถึง

๔.๓.๓ เทคโนโลยีในการสนับสนุนทีมปฏิบัติการ มีเครื่องมือที่จำเป็นสำหรับการสนับสนุนการปฏิบัติงานได้แก่ Cyber Deployment Platform Technologies, Forensic, Big DATA, AI, GIS และการเตรียม Platform อื่น ๆ ที่จำเป็นสำหรับการปฏิบัติการ

๕. แผนพัฒนาขีดความสามารถทางไซเบอร์

๕.๑ การพัฒนาทรัพยากรบุคคลทางไซเบอร์ (People)

๕.๑.๑ การขับเคลื่อนการพัฒนาองค์ความรู้ทางไซเบอร์

๑) พัฒนาองค์ความรู้ผ่านการเปิดหลักสูตรทางไซเบอร์ เพื่อผลิตบุคลากรทางไซเบอร์ให้กับกองทัพและหน่วยงานภาครัฐที่ดูแลระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (CII) โดยแบ่งออกเป็น ๕ กลุ่มหลักสูตร ดังนี้

- <u>หลักสูตรพื้นฐาน</u> ได้แก่ หลักสูตรปรับพื้นฐานบุคลากรทางไซเบอร์ หลักสูตรนายทหารรักษาความมั่นคงปลอดภัยทางไซเบอร์ฯ และหลักสูตรเพิ่มพูนความรู้ทางทางไซเบอร์ให้ ผู้บริหารระดับสูง ผู้บริหารระดับกลาง และผู้ใช้งาน

- <u>หลักสูตรระดับกลาง</u> ได้แก่ หลักสูตรการปฏิบัติการทางไซเบอร์ (CPT) หลักสูตรการปฏิบัติการไซเบอร์เชิงป้องปราม (CCMT) และหลักสูตรการปฏิบัติการทางไซเบอร์ด้านโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CNMT)

- หลักสูตรขั้นสูง สำหรับผู้เชี่ยวชาญทางไซเบอร์ขั้นสูง ในการผลิต คิดค้น วิเคราะห์ ออกแบบ เผยแพร่ สอนหลักสูตรพื้นฐานและระดับกลาง เช่น ศูนย์ปฏิบัติการทางไซเบอร์ (Security Operations Center: SOC) ขั้นสูง

- หลักสูตรเฉพาะทาง ได้แก่ หลักสูตรการรวบรวมข่าวกรองทางไซเบอร์ หลักสูตรการตรวจประเมินทางไซเบอร์ หลักสูตรการวิเคราะห์ภัยคุกคามทางไซเบอร์และมัลแวร์ หลักสูตรการประเมินความเสี่ยงทางไซเบอร์ เป็นต้น

- หลักสูตรบริหารงานไซเบอร์ เป็นหลักสูตรที่มุ่งเน้นการวางแผนของฝ่ายอำนวยการสำหรับสนับสนุนงานในมิติทางไซเบอร์และการบริหารศูนย์ปฏิบัติการทางไซเบอร์

๕.๑.๒ การขับเคลื่อนการพัฒนาขีดความสามารถและการตระหนักรู้ทางไซเบอร์

๑) โครงการ Train the Trainers เป็นโครงการพัฒนาอาจารย์ทางไซเบอร์ และรับรองความสามารถในการสอนโดยสถาบันด้านความมั่นคงปลอดภัยทางไซเบอร์ระดับสากล

๒) โครงการจัดแข่งขันทักษะทางทางไซเบอร์ เพื่อพัฒนาขีดความสามารถและการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ข้าราชการ ภาคเอกชน นักศึกษาระดับอุดมศึกษา และนักเรียนมัธยม

๓) โครงการสร้างเครือข่ายของบุคลากรทางไซเบอร์ อาจารย์ นักวิจัย และผู้ปฏิบัติงานทางไซเบอร์ ทั้งภาครัฐ เอกชน และพันธมิตรต่างประเทศ ผ่านประชาคมไซเบอร์กองทัพไทย โดยสร้าง

เว็บไซต์เป็นตัวกลางในการเชื่อมโยง การแลกเปลี่ยนข้อมูล การรวบรวมและเผยแพร่ข่าว แบ่งปันข้อมูล งานวิจัย และองค์ความรู้

๔) โครงการ Cyber Bootcamp เพื่อพัฒนาขีดความสามารถให้กับเยาวชนระดับมัธยมที่สนใจงานด้านความมั่นคงปลอดภัยทางไซเบอร์ และเพิ่มจำนวนผู้ที่มีความตระหนักรู้ทางไซเบอร์ให้มากขึ้น เป็นส่วนหนึ่งในการเตรียมฐานข้อมูลของบุคลากรทางไซเบอร์ในระบบ Recruit and Talent Management

๕) การจัดทำบันทึกข้อตกลงความร่วมมือ (MOU) ดังนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่องการรักษาความปลอดภัยทางไซเบอร์ กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย และนวัตกรรม เรื่องทุนการศึกษาต่างประเทศในทางไซเบอร์ และมหาวิทยาลัยธรรมศาสตร์ เพื่อเปิดอบรมหลักสูตรการพัฒนาศักยภาพบุคลากรทางไซเบอร์ แลกเปลี่ยนอาจารย์ผู้สอน จัดหาทุนทางไซเบอร์ และรับนักศึกษาฝึกงานทุกปี

๕.๑.๓ การขับเคลื่อนการพัฒนาขีดความสามารถของนักรบไซเบอร์

๑) เตรียมความพร้อมของกำลังพลสำหรับชุดปฏิบัติการทางไซเบอร์ จำนวน ๑๒ นาย/ชุด

๒) เตรียมความพร้อมของกำลังพลสำหรับชุดปฏิบัติการทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ จำนวน ๑๒ นาย/ชุด

๓) เตรียมความพร้อมของกำลังพลสำหรับงานวิเคราะห์ภัยคุกคามและมัลแวร์

๔) เตรียมความพร้อมของกำลังพลสำหรับงานข่าวกรองทางไซเบอร์

๕) เตรียมความพร้อมของกำลังพลสำหรับงานตรวจและประเมินทางไซเบอร์

๖) เตรียมความพร้อมของกำลังพลสำหรับงานสนับสนุนการช่วยปฏิบัติการทางไซเบอร์

๗) เตรียมความพร้อมของบุคลากรในการสนับสนุนการปฏิบัติการไซเบอร์ใน Multi-Domain Operations

๘) การดำเนินโครงการ Up-Skill และ Re-Skill สำหรับเจ้าหน้าที่ในข้อ ๑–๕

๙) เข้าร่วมการฝึกของกองทัพไทย การฝึกเป็นหน่วย การฝึกตามหน้าที่ การจัดการฝึกบริหารวิกฤตการณ์ระดับชาติ (C-MEX) ร่วมกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) การฝึกรับมือเหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) การฝึกกับศูนย์ปฏิบัติการต่อต้านการก่อการร้ายสากล

๑๐) เข้าร่วมการฝึกร่วม/ผสม กับเหล่าทัพและกองกำลังต่างชาติทั้งแบบ Bilateral; US UK AUS Singapore Malaysia, Indonesia และ Multilateral; Cobra Gold, Cyber Flag, Cyber Marvel, Talisman Sabre การฝึกปฏิบัติการร่วมทางไซเบอร์ขั้นสูง

๕.๒ การพัฒนากระบวนการทางไซเบอร์ (Process)

ประกอบด้วย

๕.๒.๑ การปรับปรุงกรอบแนวคิดด้านการปฏิบัติการทางไซเบอร์

เป็นการปรับปรุงเนื้อหาสำหรับหน่วยบัญชาการไซเบอร์ทหารที่ตั้งขึ้นใหม่ในปีงบประมาณ พ.ศ. ๒๕๖๘ ประกอบด้วย

๑) ร่างหลักนิยมการปฏิบัติการร่วมทางไซเบอร์ พ.ศ. ๒๕๖๘ จัดทำขึ้นเพื่อเป็นแนวทางการทำความเข้าใจ ตีความ และอธิบาย การดำเนินการในมิติทางไซเบอร์ของกองทัพไทย ให้สอดคล้องกับข้อกำหนดต่าง ๆ ที่ประกาศกำหนดใช้ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และหลักการปฏิบัติการทางทหารที่เกี่ยวข้อง

๒) ร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ รัฐมนตรีว่าการกระทรวงกลาโหม และผู้บัญชาการทหารสูงสุด พ.ศ. ๒๕๖๘

๓) ร่างแผนรับมือภัยคุกคามทางไซเบอร์ กองบัญชาการกองทัพไทยสนับสนุนสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) พ.ศ. ๒๕๖๘

๕.๒.๒ การกำหนดนโยบายการใช้งาน

การกำหนดนโยบายต่างๆ เพื่อบังคับใช้ร่วมกัน เช่น การกำหนดนโยบาย Join AD เพื่อควบคุมผู้ใช้งานจากส่วนกลาง การพัฒนากรอบแนวทางนโยบาย และแนวปฏิบัติการรักษาความมั่นคง

ปลอดภัยทางไซเบอร์ เพื่อเป็นกรอบแนวทางเดียวกันทั้งกองทัพไทย ทำให้เกิดความมั่นคงปลอดภัยทางไซเบอร์ และได้กรอบแนวทางสนับสนุน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๕.๒.๓ การสร้างความร่วมมือภายในประเทศ

การสร้างความร่วมมือระหว่างหน่วยงานภายในกองทัพไทย รวมถึงการประสานงานกับหน่วยงานภายนอกและองค์กรที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) เป็นแนวทางสำคัญในการพัฒนาและยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพไทย (บก.ทท.) เพื่อให้สามารถป้องกัน รับมือ และตอบโต้ภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของประเทศได้อย่างมีประสิทธิภาพ นอกจากนี้ การบูรณาการความร่วมมือระหว่าง บก.ทท. และเหล่าทัพ จะช่วยเสริมสร้างการปฏิบัติการร่วมทางไซเบอร์ เพื่อสนับสนุนการปฏิบัติการของกองทัพไทยในทุกมิติ รวมถึงการบริหารจัดการภัยคุกคามทางไซเบอร์ในระดับยุทธศาสตร์ ความร่วมมือกับหน่วยงานที่รับผิดชอบ CII จะช่วยเพิ่มขีดความสามารถในการบริหารจัดการวิกฤตการณ์ทางไซเบอร์ ตั้งแต่ระดับปกติไปจนถึงระดับวิกฤต แนวทางดังกล่าวสอดคล้องกับ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยเน้นการประสานงานระหว่างกองทัพไทยและหน่วยงานพลเรือน เพื่อให้สามารถรับมือกับ

ภัยคุกคามทางไซเบอร์ได้อย่างเป็นระบบ และสนับสนุนการรักษาความมั่นคงปลอดภัยของประเทศในมิติไซเบอร์อย่างมีประสิทธิภาพ

๕.๒.๔ **การสร้างความร่วมมือกับต่างประเทศ**

เป็นแนวทางสำคัญในการพัฒนาขีดความสามารถทางไซเบอร์ ให้กับ กองบัญชาการกองทัพไทย (บก.ทท.) และเหล่าทัพ โดยมีแนวทางดำเนินการ ดังนี้

- การออกแบบและพัฒนาระบบ Cloud โดย Massachusetts Institute of Technology Research and Engineering (MITRE)

- การปรับปรุงหลักสูตรการศึกษาทางไซเบอร์ของหน่วยงาน Institute for Security Governance: ISG หน่วยงาน USCYBERCOM, USINDOPACOM (J6) ของ กห.สหรัฐอเมริกา และหน่วยงาน SIBAT (International Defense Cooperation Directorate of the Israel Ministry of Defense) ของ กห.อิสราเอล

- ประสานความร่วมมือกับต่างประเทศ ได้แก่ CDWG SSCI ADMM (ด้าน Cyber)

- การอบรมแลกเปลี่ยนข้อมูลหลักสูตรและเทคโนโลยีเชิญร่วมฝึกอบรม/สัมมนาทางไซเบอร์กับประเทศออสเตรเลีย และอังกฤษ

- การแลกเปลี่ยนเยี่ยมชมและศึกษาดูงานหน่วยงานด้านไซเบอร์ของประเทศในประเทศพันธมิตร เช่น มาเลเซียและอิสราเอล

๕.๓ การพัฒนาเทคโนโลยีทางไซเบอร์ (Technology)

๕.๓.๑ ด้านการพัฒนาบุคลากร

๑) Computer Lab ห้องเรียนคอมพิวเตอร์ ๔ ห้อง รองรับผู้เรียน ๑๒๐ คนพร้อมกัน

๒) Online Courses รองรับการเรียนแบบ On Demand ทั้งในห้องเรียน และด้วยตนเอง รองรับหลักสูตรทั้งหมดของโรงเรียนไซเบอร์ทหาร และรองรับระบบ IMCITE ที่ได้รับการสนับสนุนจากต่างประเทศ

๓) Network Laboratory ระบบฝึกปฏิบัติการทางเครือข่าย เพื่อการจำลองการสร้างเครือข่ายที่ปลอดภัยและมีประสิทธิภาพ

๔) Cyber Exercise ระบบจำลองการฝึกเพื่อให้กองทัพไทยมีระบบจำลองเครือข่ายสำหรับการฝึกทางไซเบอร์ที่มีประสิทธิภาพ เพื่อพัฒนาขีดความสามารถทางไซเบอร์ทั้งเชิงรับและป้องปราม

๕) Operational Technology Laboratory: OT Lab ห้องปฏิบัติการสำหรับการเฝ้าระวังและป้องกันเหตุการณ์ในโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (CII) ซึ่งครอบคลุม ๗+๑

๖) Training Center ศูนย์ฝึกทางไซเบอร์เพื่อยกระดับการผลิตนักรับไซเบอร์เพื่อรองรับสงครามไซเบอร์และภัยคุกคามในอนาคตในหลายมิติทั้งทางบก ทางทะเล ทางอากาศ และทางอวกาศ

๗) Cyber Offensive Training สำหรับการฝึกปฏิบัติการป้องปราม เช่น การวิเคราะห์ช่องโหว่ และการป้องกันหลังการโจมตี การทดสอบการเจาะระบบ (Penetration Testing) และการสร้างระบบจำลอง (Simulation Environment)

๘) Cyber Range & Simulation ระบบพัฒนาทักษะทางไซเบอร์เพื่อพัฒนาขีดความสามารถทักษะทางไซเบอร์ ที่สามารถปฏิบัติงานสนับสนุนภารกิจงานทางไซเบอร์

๕.๓.๒ ด้านการปฏิบัติการ

๑) Cyber-C2 Technology (Command and Control) สำหรับการวางแผน การควบคุม และการประสานงานในภารกิจไซเบอร์

๒) Protect & Detect Response เพื่อการป้องกันและตอบสนองต่อภัยคุกคามแบบเรียลไทม์

๓) Cloud Server & Edge Computing รองรับการจัดเก็บและประมวลผลข้อมูลจำนวนมาก

๔) Post Quantum Cryptography เป็นเทคโนโลยีการเข้ารหัสที่ป้องกันการโจมตีจากคอมพิวเตอร์ควอนตัมในอนาคต

๕) Zero Trust Architecture Technology เป็นเทคโนโลยีตามหลักการ “ไม่เชื่อถือใคร” โดยตรวจสอบทุกการเข้าถึงระบบ

๖) Security Information and Event Management: SIEM เพื่อการตรวจสอบและวิเคราะห์ข้อมูลภัยคุกคามในองค์กร

๗) Cyber threat intelligence ระบบงานข่าวกรองและการทำบัญชีเป้าหมาย ทำให้รับข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ได้ล่วงหน้าและทันเวลา สามารถนำข้อมูลการวิเคราะห์ และนำไปขยายผลสำหรับการปฏิบัติภารกิจทางทหาร พลเรือน หรือภารกิจร่วม ทั้งยามปกติ และยามสงคราม

๘) Cyber Deployment Platform Technologies ระบบสนับสนุนชุดเคลื่อนที่เร็ว เพื่อให้ชุดเครื่องที่เร็ว CPT CCT CNMT สามารถปฏิบัติงานสนับสนุนการรับมือ แก้ไขปัญหางานทางไซเบอร์

๘) Deterrence System ระบบป้องปรามเชิงป้องกันสำหรับชุด Cyber Combat Mission Team (CCMT) โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

๙) Cyber Joint Big Data Analytics ระบบวิเคราะห์ฐานข้อมูลขนาดใหญ่ทางไซเบอร์เพื่อให้ บก.ทท. ทท. และระดับประเทศ มีระบบวิเคราะห์ที่มีประสิทธิภาพในการตรวจจับการละเมิดทางไซเบอร์

๑๐) Advanced Detection System: ADS ระบบเฝ้าตรวจภัยคุกคามทางไซเบอร์เพื่อให้มีความพร้อมในการรับมือ และแก้ไขภัยคุกคามที่จะเกิดขึ้นได้ทันเวลา

๑๑) Automated Penetration Testing เป็นเครื่องมือการทดสอบเจาะระบบ ซึ่งมีขีดความสามารถในการค้นหาวิเคราะห์ช่องโหว่ของระบบโดยใช้ปัญญาประดิษฐ์ (AI) ซึ่งสามารถ

บันทึกและสืบค้นข้อมูลผลการทดสอบเจาะระบบ และแจ้งเตือนช่องโหว่ได้อัตโนมัติ

๑๒) Automated Forensic เป็นเครื่องมือที่สามารถใช้ในการสนับสนุนการตรวจพิสูจน์หลักฐานทางไซเบอร์ภายในกองบัญชาการกองทัพไทย, กองทัพไทย และระดับประเทศ

๖. สรุป

ท่ามกลางการเปลี่ยนแปลงอย่างรวดเร็วของโลกดิจิทัล ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ยังคงพัฒนาไปอย่างต่อเนื่องในลักษณะที่ซับซ้อนและไม่สามารถคาดการณ์ได้ ด้วยเหตุนี้ความมั่นคงปลอดภัยทางไซเบอร์จึงไม่ใช่เพียงการป้องกันและรับมือกับการโจมตีทางไซเบอร์เท่านั้น หากแต่เป็นองค์ประกอบเชิงยุทธศาสตร์ที่ต้องอาศัยการวางแผนระยะยาวเพื่อเสริมสร้างขีดความสามารถของประเทศในทุกมิติ ตั้งแต่การพัฒนากำลังพล การเสริมสร้างโครงสร้างพื้นฐานด้านไซเบอร์ ตลอดจนการกำหนดนโยบายและกฎหมายที่สามารถรองรับสถานการณ์ที่เปลี่ยนแปลงไปอย่างต่อเนื่อง

ในอนาคต การพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยจำเป็นต้องมีการพัฒนาอย่างเป็นระบบและต่อเนื่อง โดยเฉพาะอย่างยิ่งการสร้างบุคลากรที่มีทักษะสูงผ่านหลักสูตรเฉพาะทางที่สามารถตอบสนองต่อภัยคุกคามที่มีความซับซ้อนมากขึ้น โรงเรียนไซเบอร์ทหารจะมีบทบาทสำคัญในการจัดทำหลักสูตรที่ทันสมัยและสอดคล้องกับสถานการณ์จริง ทั้งนี้ การส่งเสริมความร่วมมือด้านการศึกษาและฝึกอบรมกับหน่วยงานพันธมิตรในระดับสากลจะช่วยให้เป็นปัจจัย

สำคัญที่ช่วยให้บุคลากรมีโอกาสพัฒนาทักษะและสามารถปฏิบัติการร่วมทางไซเบอร์ได้อย่างมีประสิทธิภาพ

นอกจากนี้ การพัฒนาโครงสร้างพื้นฐานด้านไซเบอร์ถือเป็นหัวใจสำคัญในการรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต ศูนย์ปฏิบัติการร่วมทางไซเบอร์ ศูนย์บัญชาการทางทหาร (ศรช.ศบท.) จะต้องได้รับการยกระดับให้มีขีดความสามารถสูงขึ้นในทุกด้าน โดยเฉพาะในส่วนของการตรวจจับ วิเคราะห์ และตอบโต้การโจมตีทางไซเบอร์แบบเรียลไทม์ ซึ่งจำเป็นต้องอาศัยเทคโนโลยีขั้นสูง เช่น การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) และปัญญาประดิษฐ์ (Artificial Intelligence: AI) รวมถึงการออกแบบโครงสร้างพื้นฐานให้เป็นไปตามแนวคิด สถาปัตยกรรม Zero Trust Architecture เพื่อให้สามารถป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพในทุกระดับ

ในขณะเดียวกัน ในยุคที่ภัยคุกคามทางไซเบอร์ไม่สามารถถูกจำกัดอยู่เพียงภายในพรมแดนของประเทศ ความร่วมมือระหว่างประเทศจึงมีความสำคัญอย่างยิ่งต่อการเสริมสร้างศักยภาพในการป้องกันและตอบโต้การโจมตีทางไซเบอร์ของกองทัพไทย การเข้าร่วมเป็นส่วนหนึ่งของกลุ่มความร่วมมือทางไซเบอร์ระหว่างประเทศ เช่น Cyber Defense Working Group จะช่วยให้สามารถแลกเปลี่ยนข้อมูลภัยคุกคามกับพันธมิตรต่างประเทศ ได้อย่างรวดเร็วและมีประสิทธิภาพ อีกทั้งยังช่วยให้สามารถพัฒนามาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ให้ทัดเทียมกับมาตรฐานสากล นอกจากนี้ การเข้าร่วมการฝึกซ้อมทางไซเบอร์ระดับนานาชาติ เช่น

Cyber Flag, Cyber Marvel และ Talisman Sabre จะช่วยให้กองทัพไทยสามารถปรับตัวให้เข้ากับแนวทางการป้องกันภัยคุกคามที่ทันสมัย และสามารถพัฒนาแนวทางการปฏิบัติการทางไซเบอร์ให้สอดคล้องกับมาตรฐานของนานาประเทศ

นอกเหนือจากการพัฒนากำลังพลและโครงสร้างพื้นฐานด้านไซเบอร์แล้ว การสร้างความมั่นคงปลอดภัยทางไซเบอร์ในระยะยาวยังต้องอาศัยกฎหมายและนโยบายที่สามารถรองรับภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จะต้องได้รับการปรับปรุงให้สามารถรองรับภัยคุกคามที่เกิดขึ้นจากเทคโนโลยีใหม่ๆ ได้อย่างมีประสิทธิภาพ อีกทั้ง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) จะต้องมีบทบาทสำคัญในการกำหนดแนวทางปฏิบัติที่สามารถนำไปใช้ได้จริงในหน่วยงานภาครัฐและเอกชน เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศมีความเป็นเอกภาพ และสามารถรับมือกับภัยคุกคามที่เกิดขึ้นได้อย่างทันท่วงที

อนาคตของความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยในอนาคตขึ้นอยู่กับความสามารถในการปรับตัวให้ทันกับภัยคุกคามที่มีความซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลา การพัฒนากำลังพลที่มีทักษะสูง การเสริมสร้างโครงสร้างพื้นฐานด้านเทคโนโลยี การสร้างความร่วมมือกับพันธมิตรระหว่างประเทศ และการกำหนดนโยบายและกฎหมายที่ทันสมัย ล้วนเป็นปัจจัยสำคัญที่ส่งผลต่อความสามารถของประเทศไทยในการรักษาเสถียรภาพและความมั่นคงปลอดภัยทางไซเบอร์ในระยะยาว ดังนั้น กองทัพไทยจะต้องมีบทบาท

สำคัญในฐานะกำลังหลักในการป้องกันประเทศจากภัยคุกคามทางไซเบอร์ โดยต้องอาศัยเทคโนโลยีขั้นสูง ควบคู่กับการดำเนินกลยุทธ์ที่สอดคล้องกับมาตรฐานสากล เพื่อสร้างความเชื่อมั่นให้กับประชาชนและพันธมิตรระหว่างประเทศว่า ประเทศไทยมีศักยภาพในการรับมือกับความท้าทายทางไซเบอร์ในศตวรรษที่ ๒๑ ได้อย่างมั่นคงและยั่งยืน