เอกสารทางวิชาการ

แผนพัฒนาการปฏิบัติการ ด้านไซเบอร์ กองทัพไทย

- นักศึกษาวิทยาลัยเสนาธิการทหาร รุ่นที่ ๖๓
- นักศึกษาวิทยาลัยการทัพบก ชุดที่ ๖๗
- นักศึกษาวิทยาลัยการทัพเรือ รุ่นที่ ๕๔
- นักศึกษาวิทยาลัยการทัพอากาศ รุ่นที่ ๕๖

ชื่อเรื่อง : แผนพัฒนาการปฏิบัติการด้านไซเบอร์ กองทัพไทย
ISBN : 978-616-8035-84-9

คณะผู้จัดทำ

บรรณาธิการบริหาร

พล.ท. ศุภรัช นรินทรภักดี พล.ร.ต. สิทธิชัย ต่างใจ ร.น.

ที่ปรึกษาบรรณาธิการ

พล.ต. บรรพต สังข์มาลา พล.ต. วิชาติ เอี่ยมไพจิตร์

พล.ร.ต. พิเศษ ขันแข็ง ร.น. พล.อ.ต. วชิระ เริงฤทธิ์

บรรณาธิการ

พ.อ. วิทวัส เอกฉันท์ น.อ. วาริท รามโกมุท

พ.อ. เอกพงศ์ แพ่งกุล น.อ. ภาณุวัฒน์ สมัคงาน

กองบรรณาธิการ

น.อ. ภาสกร ไชยกำเนิด น.อ. ทรงวุฒิ ขยันหา ร.น.

พ.อ. ธนัท กำแหงฤทธิรงค์ พ.อ พงศภัค ลิมปิยนันท์

พ.อ. เปี่ยมศักดิ์ ภักดีพินิจ พ.อ. พีรพัฒน์ ราชพิบูลย์

พ.อ. จารุวัตร สิริสังกาส พ.อ. วันชัย ปรีวัน

นาง สุทิษา รังคเสนี นาย สมภพ เพ็ชรเกลี้ยง

พ.อ. ยิ่งโรจน์ สันติวุฒน์ พ.อ. อรุณ แก้วเศษ

น.อ. บรรเจิด ทองชิว ร.น. นาย เอก มุติตาภรณ์

ออกแบบรูปเล่ม

นาย สมภพ เพ็ชรเกลี้ยง พ.อ. สิริวัฒน์ ทัศนานุตริยกุล

เรียบเรียงข้อมูล

นักศึกษาวิทยาลัยเสนาธิการทหาร รุ่นที่ ๖๓

นักศึกษาวิทยาลัยการทัพบก ชุดที่ ๖๗

นักศึกษาวิทยาลัยการทัพเรือ รุ่นที่ ๕๔

นักศึกษาวิทยาลัยการทัพอากาศ รุ่นที่ ๕๖

จัดทำโดย

วิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ

๗๘ วิทยาลัยเสนาธิการทหาร ถนนวิภาวดี-รังสิต แขวงรัชดาภิเษก

เขตดินแดง กรุงเทพฯ ๑๐๔๐๐

โทรศัพท์ แผนกธุรการ กองอำนวยการ ๐-๒๒๗๗-๓๖๗๓

Website: https://jwc.rtarf.mi.th

พิมพ์ครั้งที่ ๑ : กันยายน ๒๕๖๕

คำนำ

เอกสารทางวิชาการ **“แผนพัฒนาการปฏิบัติการด้านไซเบอร์ กองทัพไทย”** ฉบับนี้ เป็นส่วนหนึ่งของการศึกษาและเป็นผลงานทางวิชาการของนักศึกษาวิทยาลัยเสนาธิการทหาร รุ่นที่ ๖๓ วิทยาลัยการทัพบก ชุดที่ ๖๗ วิทยาลัยการทัพเรือ รุ่นที่ ๕๔ และวิทยาลัยการทัพอากาศ รุ่นที่ ๕๖ ประจำปีการศึกษา ๒๕๖๕ และเป็นไปตามหลักสูตรการศึกษาและนโยบายของสถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย เพื่อนำเสนอแนวความคิดในการพัฒนากองทัพ อำนาจกำลังรบและขีดความสามารถทางทหาร ซึ่งเป็นหนึ่งในพลังอำนาจของชาติ (National Power) ที่สามารถนำมาใช้เป็นเครื่องมือของรัฐควบคู่กับการใช้เครื่องมือประเภทอื่น เช่น การทูต (Diplomacy) ข้อมูลข่าวสาร (Information) เศรษฐกิจ (Economy) ให้เหมาะสมกับเวลาและสถานการณ์ ซึ่งนักศึกษาทั้ง ๔ สถาบัน มีความเห็นสอดคล้องกันว่า แนวโน้มของภัยคุกคามสำคัญที่จะส่งผลกระทบต่อความมั่นคงของชาติในอนาคตอันใกล้ คือ การถูกโจมตีทางไซเบอร์ต่อระบบโครงสร้างพื้นฐานของประเทศ ซึ่งหน่วยงานภาครัฐ เอกชน และประชาชนทั่วไป มีความเสี่ยงเท่าเทียมกัน เนื่องจากพฤติกรรมของหน่วยงาน องค์กร และประชาชน มีการพึ่งพาเทคโนโลยีสารสนเทศในชีวิตประจำวันที่เพิ่มสูงขึ้นโดยเฉพาะในช่วงสถานการณ์การแพร่ระบาดของ COVID-19 ในห้วงที่ผ่านมา อีกทั้งปัจจุบันไทยกำลังเผชิญกับสถานการณ์สำคัญระดับโลก กรณีสงครามยูเครน ในระดับภูมิภาค กรณีเหตุการณ์ความไม่สงบในเมียนมาและปัญหาการก่อความไม่สงบภายในประเทศ ที่เกิดจากการแทรกแซงจากต่างชาติ ทำให้การดำเนินนโยบายด้านการต่างประเทศของไทยมีความเปราะบางเป็นอย่างมาก ซึ่งหากเกิดข้อผิดพลาดในการตัดสินใจอย่างใดอย่างหนึ่ง ไทยอาจเป็นเป้าหมายในการถูกโจมตีทางไซเบอร์จากชาติมหาอำนาจที่มีศักยภาพสูง ทั้งจากสหรัฐฯ รัสเซีย หรือ จีน ในขณะที่ระบบป้องกันและตอบโต้การปฏิบัติการดังกล่าวของกองทัพยังไม่ได้รับการพัฒนาอย่างเหมาะสม ทั้งในด้านการป้องกันตนเองภายในกองทัพหรือการสนับสนุนหน่วยงานภาครัฐ เอกชน และประชาชนเมื่อถูกโจมตีทางไซเบอร์ในยุทธบริเวณ ดังนั้น วิทยาลัยเสนาธิการทหาร วิทยาลัยกองทัพบก วิทยาลัยกองทัพเรือ และวิทยาลัยกองทัพอากาศ จึงได้ร่วมกันศึกษาและจัดทำ **“เอกสารวิชาการ แผนพัฒนาการปฏิบัติการด้านไซเบอร์ กองทัพไทย”** ซึ่งสอดคล้องกับ (ร่าง) แผนปฏิบัติการด้านการปกป้องอธิปไตยและรักษาผลประโยชน์ของชาติ พ.ศ.๒๕๖๖ - ๒๕๗๐ เพื่อเป็นกรอบแนวความคิดและแนวทางการพัฒนาขีดความสามารถของกองทัพไทย ให้สอดคล้องกับสถานการณ์ความมั่นคงของโลกในยุคปัจจุบัน พร้อมทั้งสามารถบูรณาการการปฏิบัติระหว่างหน่วยงานทหารและหน่วยงานภายนอกได้อย่างเหมาะสม มีความพร้อมในการรับมือกับภัยคุกคามรูปแบบต่างๆ เพื่อรักษาผลประโยชน์ของชาติในภาพรวมต่อไป

- **นักศึกษาวิทยาลัยเสนาธิการทหาร รุ่นที่ ๖๓**
- **นักศึกษาวิทยาลัยการทัพบก ชุดที่ ๖๗**
- **นักศึกษาวิทยาลัยการทัพเรือ รุ่นที่ ๕๔**
- **นักศึกษาวิทยาลัยการทัพอากาศ รุ่นที่ ๕๖**

สารบัญ

บทสรุปผู้บริหาร

โลกในยุคปัจจุบันทุกภาคส่วนต้องพึ่งพาเทคโนโลยีสารสนเทศโดยมีแนวโน้มเพิ่มสูงขึ้น ซึ่งสอดคล้องกับความเจริญก้าวหน้าทางด้านการเมือง เศรษฐกิจ สังคมจิตวิทยา และการทหาร ดังนั้น จึงเกิดเป็นช่องว่างที่ภัยคุกคามทางไซเบอร์จะก้าวเข้ามาเป็นประเด็นสำคัญที่จะทำให้เกิดผลกระทบต่อความมั่นคงของชาติในอนาคตอันใกล้นี้ และเป็นภัยคุกคามที่สามารถเกิดขึ้นได้ในทุกย่านของความขัดแย้ง กล่าวคือ สามารถเกิดขึ้นได้ตั้งแต่ยามสงบ ยามขัดแย้ง และยามสงคราม ทำให้ขอบเขตการปฏิบัติการด้านไซเบอร์เป็นความท้าทายต่อการพัฒนากองทัพไทยในอีก ๒๐ ปีข้างหน้า เพื่อเป็นกองทัพอเนกประสงค์ที่สามารถตอบสนองต่อภัยคุกคามได้ในทุกมิติ มีการพัฒนาไปสู่การพึ่งพาตนเองด้วยการใช้นวัตกรรมและเทคโนโลยีเพื่อสร้างความเปลี่ยนแปลง ซึ่งเป็นวิสัยทัศน์ กองทัพไทยในปี ๒๕๗๙ “กองทัพชั้นนำในภูมิภาค ตอบสนองภัยคุกคามได้ในทุกมิติ มีกำลังรบทันสมัย พึ่งพาตนเองได้ และใช้นวัตกรรม”

โดยวัตถุประสงค์ในการพัฒนางานด้านไซเบอร์ของกองทัพนั้น ได้กำหนดจุดหมายปลายทางหรือเป้าหมาย (End) ไว้ที่การนำหลักการปฏิบัติการร่วมที่มีเครือข่ายเป็นศูนย์กลาง (Network Centric Operation : NCO) มาใช้เป็นแนวทางในการพัฒนาเพื่อนำไปสู่การปฏิบัติหลายมิติ (Multi Domain Operation : MDO) ซึ่งการดำเนินการนั้นต้องมีความสัมพันธ์และสอดคล้องกับการพัฒนาของทุกเหล่าทัพ โดยกองทัพต้องมีขีดความสามารถในการป้องกันและปรามปรามภัยคุกคามด้านไซเบอร์ภายในเหล่าทัพของตนเอง จากนั้นจึงพัฒนาไปสู่ขีดความสามารถในการป้องปรามและตอบโต้ด้านไซเบอร์ในกรอบของ MDO และสุดท้ายสามารถสนับสนุนและปฏิบัติการด้านไซเบอร์ร่วมกับภาคส่วนต่างๆ ได้อย่างมีประสิทธิภาพตั้งแต่ยามปกติ โดยมีแนวความคิดในการดำเนินการ (Concept of Operations : CONOPs) หรือวิธีการ (Ways) ที่จะนำไปสู่ความสำเร็จ ได้แก่ การกำหนดเป็นประเด็นการพัฒนาตั้งแต่ การสร้างการรับรู้ สร้างภูมิคุ้มกันและป้องกันความเสี่ยง จนสามารถก้าวไปสู่การพัฒนาด้านการข่าวกรองไซเบอร์ การป้องกันและป้องปรามทางไซเบอร์ และแสวงหาความร่วมมือทางไซเบอร์ ซึ่งเครื่องมือ (Means) ที่สำคัญ คือ การนำเทคโนโลยีที่ทันสมัยเข้ามาเพิ่มประสิทธิภาพในการอำนวยการปฏิบัติการร่วม โดยมีแผนงานต่างๆ เป็นส่วนขับเคลื่อน ได้แก่ การพัฒนาโครงสร้างพื้นฐานด้านไซเบอร์ (Cyber Infrastructure) การพัฒนาระบบค้นหาและเฝ้าตรวจ (Sensor System) การพัฒนาระบบการเชื่อมต่อข้อมูล (Data Link) การพัฒนาระบบการวิเคราะห์และจำลองทางเลือก (Analysis and Simulation System) และการพัฒนาระบบควบคุมหน่วยปฏิบัติการ (Shooter System) ซึ่งแนวคิดการพัฒนาดังกล่าวเกิดจากข้อจำกัดของกองทัพที่สำคัญ คือ การพัฒนาการปฏิบัติการด้านไซเบอร์ของกองทัพที่ดำเนินการมาตามลำดับยังขาดการบูรณาการและระบบควบคุมบังคับบัญชาที่มีประสิทธิภาพ โดยศูนย์บัญชาการทางทหาร(ศบท.) ยังไม่สามารถแสดงบทบาทนำหรือแสดงออกถึงขีดความสามารถทางการบังคับบัญชาในภาพรวม เพื่อแก้ปัญหาและตอบโต้ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของชาติตั้งแต่ยามปกติในทุกมิติได้อย่างมีประสิทธิภาพ

ผลที่คาดว่าจะได้รับจากการพัฒนาด้านไซเบอร์ของกองทัพไทยทั้งระบบ คือ ศูนย์บัญชาการทางทหาร (ศบท.) ต้องสามารถอำนวยการในการปฏิบัติการได้ตั้งแต่ยามปกติและต้องบูรณาการร่วมกับเหล่าทัพ (ทบ. ทร. ทอ.) รวมถึงทุกภาคส่วนได้อย่างมีประสิทธิภาพ ด้วยการนำเทคโนโลยีเข้ามาช่วยเหลือในการจัดเก็บ คัดกรอง และประมวลผลข้อมูล ซึ่งครอบคลุมการทำงานตั้งแต่การเชื่อมต่อระบบการเฝ้าตรวจและค้นหา (Sensor System) ของทุกขอบเขตพื้นที่ (Domain) การจัดระบบการเก็บข้อมูล (Data Governance) การวิเคราะห์และประมวลผล (Analysis) เพื่อให้ได้ข้อพิจารณาเกี่ยวกับระดับของภัยคุกคาม (Threat) เกณฑ์เสี่ยง (Risk) และแนวทางการแก้ปัญหา (Recommendation) สำหรับจัดทำเป็นแผนปฏิบัติการ (Operation Plan) ซึ่งจะทำให้ผู้บังคับบัญชาสามารถตกลงใจและเลือกใช้เครื่องมือที่เป็น Soft Power หรือ Hard Power ได้อย่างถูกต้อง รวดเร็ว และทันเวลา เหมาะสมและสอดคล้องกับภัยคุกคามในแต่ละระดับ

ปัจจัยแห่งความสำเร็จในการขับเคลื่อนการพัฒนาด้านไซเบอร์ของกองทัพไทย จำเป็นต้องมีเปลี่ยนแปลง ปรับปรุงด้านต่างๆ ให้เหมาะสมและสอดคล้องกับรูปแบบการปฏิบัติงานที่ต้องการความรวดเร็ว ยืดหยุ่น และแม่นยำในการตัดสินใจ โดยเริ่มตั้งแต่การปรับเปลี่ยนระบบการควบคุมบังคับบัญชาและวัฒนธรรมองค์กร เพื่อสร้างระบบการทำงานที่ต้องการความอ่อนตัวสามารถปรับเปลี่ยนตามสถานการณ์ที่เกิดขึ้นได้ทันเวลา และต้องการความรวดเร็วในการตกลงใจเลือกหนทางปฏิบัติในการแก้ปัญหา รวมทั้งต้องมีการจัดสรรงบประมาณให้สอดคล้องกับการปฏิบัติงานและสถานการณ์ที่เกิดขึ้น โดยขั้นต้นควรพัฒนาศูนย์ไซเบอร์ กองบัญชาการกองทัพไทย เป็นศูนย์ความร่วมมือด้านการรักษาความปลอดภัยทางไซเบอร์(จำลอง) เพื่อศึกษา จัดหา เสริมสร้างขีดความสามารถของกำลังพลและพัฒนาโครงสร้างพื้นฐาน รวมทั้งฝึกการทำงานร่วมกับเทคโนโลยี ในการควบคุม อำนวยการ และสั่งการให้เกิดความชำนาญและเข้าใจกระบวนการทำงานก่อนที่จะจัดตั้งเป็นศูนย์ความร่วมมือแบบถาวร เพื่อเป็นก้าวแรกของการเป็นผู้นำด้านความปลอดภัยทางไซเบอร์ในภูมิภาค และเตรียมการพัฒนาเป็นศูนย์ยุทธศาสตร์ทหารอัจฉริยะในห้วงต่อไป จนกระทั่งสามารถขยายความร่วมมือไปยังองค์กรชั้นนำด้านความมั่นคงทั้งภายในและภายนอกประเทศได้อย่างมีประสิทธิภาพ ขณะเดียวกันต้องเร่งดำเนินการพัฒนาและจัดหากำลังพลที่มีคุณสมบัติเหมาะสมในการทำงาน โดยแบ่งเป็น ๑) กลุ่มที่เข้าใจกระบวนการทำงานขององค์กรในระดับเชี่ยวชาญ ๒) กลุ่มที่มีขีดความสามารถทางไซเบอร์ และ ๓) กลุ่มที่ทำหน้าที่ประสานงานระหว่าง ๑) และ ๒) อีกทั้งควรปรับเปลี่ยนกระบวนการทำงาน และโครงสร้างองค์กรให้เหมาะสมต่อการทำงาน รวมทั้งพัฒนาปรับปรุงกฎหมายด้านความมั่นคงให้สอดคล้องกับการปฏิบัติการด้านไซเบอร์ โดยไม่ส่งผลกระทบต่อความรู้สึกของภาคเอกชน รวมถึงประชาชนทั่วไป

สุดท้าย เพื่อให้กองทัพไทย เป็นผู้นำด้านความปลอดภัยทางไซเบอร์แห่งแรกในภูมิภาค ต้องพยายามแก้ไขอุปสรรคสำคัญของระบบการปฏิบัติการร่วม คือ การแลกเปลี่ยนและกระจายข้อมูลที่เป็นชั้นความลับของแต่ละองค์กรทุกระดับให้มีความเหมาะสมและต้องมีความปลอดภัย แต่สิ่งที่มีความสำคัญที่สุดของระบบการทำงาน คือ ขีดความสามารถของกำลังพลที่ต้องได้รับการพัฒนาให้สามารถทำงานร่วมกับเทคโนโลยีที่ทันสมัยได้อย่างลงตัว พร้อมทั้งต้องได้รับการสนับสนุนงบประมาณที่สอดคล้องกับสถานการณ์ในแต่ละช่วงของการพัฒนาอย่างเหมาะสม และเพื่อให้ง่ายในการจดจำ เห็นควรกำหนดเป็นสัญลักษณ์ชื่อ “ALPHA” ซึ่งประกอบด้วย A. Agile Operation, L : Leadership Supervision, P : Performance Excellence, H : Hyper Intelligence, A : Action Empowerment

บทที่ ๑
บทนำ

บทที่ ๑ | บทนำ

(ร่าง) แผนปฏิบัติการด้านการปกป้องอธิปไตยและรักษาผลประโยชน์ของชาติในภาพรวม พ.ศ. ๒๕๖๖ - ๒๕๗๐ ประกอบด้วยหลักสำคัญด้านการป้องกันประเทศ ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทย และยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ซึ่งกำหนดวิสัยทัศน์ **"ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง"**

การทบทวนสภาวะแวดล้อมต่อบริบทความมั่นคง ได้ทำการวิเคราะห์ถึงสภาวะแวดล้อมด้านความมั่นคงของโลก ภูมิภาคเอเชียตะวันออกเฉียงใต้ และภายในประเทศ รวมทั้งภัยคุกคามและความท้าทายให้ห้วง ๑๐ ปีข้างหน้า พร้อมกับ**กำหนดวิสัยทัศน์กองทัพไทย** คือ **"เป็นกองทัพชั้นนำในภูมิภาค บูรณาการการปฏิบัติการร่วมในทุกมิติ และพร้อมสนับสนุนรัฐบาลในการช่วยเหลือประชาชน"** โดยกำหนดวัตถุประสงค์มูลฐานด้านความมั่นคงของประเทศ จำนวน ๔ ประเด็น ได้แก่ ๑) การอยู่ร่วมกันอย่างสันติสุข การมีเกียรติและศักดิ์ศรีของชาติในประชาคมระหว่างประเทศ ๒) สถาบันหลักของชาติ และการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขดำรงอยู่อย่างมั่นคง ๓) สถานการณ์ภายในประเทศมีความสงบเรียบร้อยประชาชนอยู่ร่วมกันได้อย่างสันติสุข และ ๔) ประเทศมีความมั่นคงปลอดภัยจากภัยคุกคามทางทหาร และยึดถือแนวความคิดทางยุทธศาสตร์ด้านการป้องกันประเทศและด้านความมั่นคงที่เกี่ยวข้องกับกระทรวงกลาโหม ซึ่งได้กำหนดไว้ ๓ แนวคิดทางยุทธศาสตร์ ได้แก่ ๑) การสร้างความร่วมมือด้านความมั่นคง (Secuity Cooperation) ๒) การผนึกกำลังป้องกันประเทศ (United Defence) และ ๓) การป้องกันเชิงรุก (Active Defence) พร้อมทั้งกำหนดเป็นประเด็น การพัฒนารองรับ จำนวน ๗ ประเด็น ซึ่งสอดคล้องกับแผนปฏิบัติราชการของกระทรวงกลาโหม ดังนี้

ยุทธศาสตร์ด้านการป้องกันประเทศและด้านความมั่นคง

ประเด็นการพัฒนาที่ ๑

การพิทักษ์รักษา และเทิดทูนสถาบันพระมหากษัตริย์ กองทัพไทยต้องปกป้องและเทิดทูน สถาบันพระมหากษัตริย์ ถวายความปลอดภัย ถวายพระเกียรติและพระมหากษัตริย์ พระราชินี พระรัชทายาท พระบรมวงศานุวงศ์ ผู้สำเร็จราชการแทนพระองค์ ผู้แทนพระองค์ และพระราชอาคันตุกะ อย่างเข้มแข็งและสง่างาม รวมทั้งสนับสนุนโครงการพระราชดำริต่าง ๆ

ประเด็นการพัฒนาที่ ๒

การปฏิบัติการทางทหารเพื่อรักษาอธิปไตยและผลประโยชน์แห่งชาติกองทัพไทยต้องเตรียมกำลังเพื่อการป้องปราม และใช้กำลังเพื่อการป้องกันประเทศในลักษณะปฏิบัติการร่วมเชิงรุก โดยใช้หลักการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) เพื่อให้เกื้อกูลต่อฝ่ายเรา และให้ได้มาซึ่งการได้เปรียบทางทหาร มีความพร้อมในการปฏิบัติการทางทหารในขนาดกำลังที่เหมาะสม สามารถเข้าแก้ปัญหาเพื่อยุติความขัดแย้งได้อย่างเด็ดขาดและรวดเร็ว โดยมุ่งความพยายามให้พื้นที่การรบแตกหักอยู่บริเวณพื้นที่ระวังป้องกัน สามารถควบคุมทะเลได้ตามความต้องการ อีกทั้งสามารถครองความได้เปรียบทางอากาศ ตลอดจนมีกำลังที่พร้อมปฏิบัติการรุกอย่างจำกัด โดยมีผลลัพธ์สุดท้าย คือ ฝ่ายเราเป็นฝ่ายได้เปรียบนอกจากนี้ยังต้องเป็นกองทัพอเนกประสงค์ มีขีดความสามารถในการปฏิบัติการได้หลายบทบาทในเวลาเดียวกัน โดยสามารถทำการรบได้อย่างเต็มขีดความสามารถ ในขณะเดียวกันก็สามารถปฏิบัติงานด้านความมั่นคงอื่น ๆ จึงต้องพัฒนาขีดความสามารถเพื่อให้สามารถบรรลุภารกิจที่กำหนด อาทิ สามารถปฏิบัติการข่าวกรองในทุกระดับอย่างต่อเนื่องและกว้างขวาง พัฒนาการบริหารจัดการด้านการสนับสนุนการรบ การสนับสนุนการช่วยรบ และการระดมสรรพกำลังให้มีประสิทธิภาพมีความต่อเนื่อง และสามารถปฏิบัติได้จริง พัฒนาการปฏิบัติการสงครามสารสนเทศ สงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์ เป็นต้น ซึ่งการเตรียมกำลังให้มีความพร้อมรบต้องพัฒนาระบบการฝึกร่วม กองทัพไทยให้มีความทันสมัยมีประสิทธิภาพ และสอดคล้องกับการเปลี่ยนแปลงของสภาวะแวดล้อมด้านความมั่นคง รวมถึงรองรับภัยคุกคามรูปแบบต่าง ๆ

ประเด็นการพัฒนาที่ ๓

“การรักษาความมั่นคงของรัฐ กองทัพไทยต้องสนับสนุนรัฐบาลในการแก้ไขปัญหาของประเทศอันเกิดจากภัยคุกคามรูปแบบต่าง ๆ รวมทั้งต้องมีส่วนร่วมสำคัญในการปลูกฝังอุดมการณ์ความรักชาติ ศาสนา และพระมหากษัตริย์ ตลอดจนสร้างความปรองดองให้กับคนในชาติ นอกจากนี้ยังต้องแสดงบทบาทในการผนึกพลังอำนาจของชาติ เพื่อสนับสนุนกิจการของกองทัพ ด้านการเตรียมกำลัง และใช้กำลัง ทั้งในยามสงบและยามสงคราม

ประเด็นการพัฒนาที่ ๔

การสร้างความร่วมมือด้านความมั่นคงกับมิตรประเทศกองทัพไทยต้องเสริมสร้างความสัมพันธ์ด้านความมั่นคงร่วมกับประเทศเพื่อนบ้าน มิตรประเทศ และประเทศมหาอำนาจในภูมิภาคต่างๆ เพื่อสร้างความไว้เนื้อเชื่อใจ ลดความหวาดระแวง การได้รับผลประโยชน์ร่วมกัน และหลักการต่างตอบแทนในการเจรจา รวมทั้งรักษาสมดุลในการพัฒนาความสัมพันธ์ และความร่วมมือด้านความมั่นคงกับประเทศมหาอำนาจ และประเทศที่มีบทบาทสำคัญในภูมิภาค โดยเน้นประเทศเพื่อนบ้าน และประเทศในกลุ่มอาเซียน พัฒนาความร่วมมือทางทหารกับกองทัพประเทศเพื่อนบ้าน มิตรประเทศ และประเทศมหาอำนาจในภูมิภาคต่าง ๆ รวมทั้งองค์การระหว่างประเทศ ในการคุ้มครองและรักษาผลประโยชน์แห่งชาติร่วมกัน รวมทั้งมีขีดความสามารถในการสนับสนุนกำลังสำหรับปฏิบัติภารกิจเพื่อสันติภาพภายใต้กรอบสหประชาชาติ กรอบความร่วมมือต่างๆ ในระดับภูมิภาคบนพื้นฐานของผลประโยชน์แห่งชาติ

ประเด็นการพัฒนาที่ ๕

การพัฒนาประเทศและช่วยเหลือประชาชน กองทัพไทยต้องสนับสนุนรัฐบาลในการพัฒนาประเทศและช่วยเหลือประชาชน เพื่อลดความเหลื่อมล้ำ เสริมสร้างความเป็นปึกแผ่นภายในชาติ ตลอดจนดำรงไว้ซึ่งความสงบสุข และเสถียรภาพของสังคมไทย

ประเด็นการพัฒนาที่ ๖

การพัฒนาขีดความสามารถของกำลังพล และเทคโนโลยีทางทหาร กองทัพไทยต้องสามารถพึ่งพาตนเอง โดยเฉพาะการวิจัยและพัฒนาทางทหาร สนับสนุนอุตสาหกรรมทางด้านเทคโนโลยีป้องกันประเทศตามกรอบแนวทางของกระทรวงกลาโหมสอดคล้องกับสถานการณ์ด้านวิทยาศาสตร์และเทคโนโลยี ซึ่งมีการพัฒนาเทคโนโลยีและนวัตกรรมแบบก้าวกระโดด (Disruptive Technology) เพื่อให้สามารถทวีกำลังรบและตอบสนองต่อการเตรียมกำลังรบในอนาคต โดยพิจารณาถึงความเหมาะสมและคุ้มค่า สามารถทำการผลิตยุทโธปกรณ์ ที่ทันสมัย อาทิ ยานพาหนะทางทหาร อากาศยานตรวจการณ์ไร้คนขับ อาวุธและกระสุน เป็นต้น นอกจากนี้ยังต้องพัฒนาขีดความสามารถของกำลังพลทุกระดับให้สามารถรองรับการเปลี่ยนแปลงของเทคโนโลยีและนวัตกรรม

ประเด็นการพัฒนาที่ ๗

การเตรียมกำลังเพื่อสนับสนุนรัฐบาลในการแก้ไขปัญหาที่สำคัญของชาติ ปัจจุบันมีความจำเป็นที่ทหารจะต้องเข้าไปมีส่วนร่วมในการปฏิบัติ และแก้ไขปัญหาของชาติในภาพรวมแทบทุกภารกิจ อาทิ ปัญหายาเสพติด ปัญหาสิ่งแวดล้อม ปัญหาการคอร์รัปชั่น ปัญหาความรุนแรงทั้งในครอบครัวและสังคม รวมไปถึงปัญหาภัยพิบัติทางธรรมชาติ เพราะในการดำเนินภารกิจเหล่านั้น มีความยากลำบาก และต้องใช้พละกำลังทั้งร่างกายที่มีความอดทนและจิตใจที่เข้มแข็ง รวมถึงขีดความสามารถของยุทธปกรณ์ที่ต้องสอดรับกับภารกิจ ดังนั้น ทหารจึงต้องให้การสนับสนุนรัฐบาล ทั้งในยามปกติและเมื่อเกิดสถานการณ์ฉุกเฉินและเร่งด่วนจากภัยทางธรรมชาติหรือภัยคุกคามทางด้านเทคโนโลยีและสิ่งแวดล้อม โดยเข้าร่วมปฏิบัติและให้การสนับสนุนอย่างทันเหตุการณ์ รวมทั้งให้การสนับสนุนยุทโธปกรณ์หรือเครื่องมือ เมื่อได้รับการร้องขอเพื่อเป็นการบรรเทาความเดือดร้อนของประชาชน ทั้งทางตรงและทางอ้อม นอกจากนั้นทหารจะต้องมีการปรับปรุงโครงสร้างหน่วยเพื่อให้รองรับกับภารกิจที่หลากหลายยิ่งขึ้น โดยให้มีกลไกในการแลกเปลี่ยนข่าวสารและติดต่อประสานงานและมีการ บูรณาการระหว่างหน่วยงานทางทหารและหน่วยงานภาคพลเรือนในทุกระดับ

ทั้งนี้ ได้กำหนดเป้าหมายในการพัฒนาเสริมสร้างกำลังกองทัพเป็น ๒ ระยะ ๆ ละ ๕ ปี ซึ่งสอดคล้องตามกรอบของยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๑ - ๒๕๘๐) กล่าวคือ

ระยะที่ ๑ (ปี ๒๕๖๔-๒๕๖๕) มีเป้าหมายสำคัญ ได้แก่ เสริมสร้างความพร้อมมุ่งไปสู่การปฏิบัติการ ร่วมแสดงบทบาทนำอย่างสร้างสรรค์ในกรอบอาเซียน โดยมุ่งเน้นการให้ความช่วยเหลือด้านมนุษยธรรมและการบรรเทาภัยพิบัติ และการปฏิบัติการเพื่อสันติภาพ รวมทั้งพัฒนาขีดความสามารถด้านกิจการไซเบอร์และกิจการอวกาศเพื่อความมั่นคง

ระยะที่ ๒ (ปี ๒๕๖๖-๒๕๗๐) มีเป้าหมายสำคัญ ได้แก่ การพัฒนากองทัพไปสู่การมีโครงสร้างกองทัพที่มีความกะทัดรัด จำนวนกำลังพลที่เหมาะสม ยุทโธปกรณ์และเทคโนโลยีที่ทันสมัย เป็นกองทัพอเนกประสงค์ สามารถปฏิบัติภารกิจได้อย่างหลากหลาย

สำหรับปัจจัยแห่งความสำเร็จของการดำเนินการปกป้องอธิปไตยและรักษาผลประโยชน์ของชาติในภาพรวมให้บรรลุตามเป้าหมายที่กำหนดไว้ ได้แก่ การจัดทำแผนการจัดเตรียมกำลังและแผนการใช้กำลังที่เกี่ยวข้อง อาทิ แผนแม่บทการปฏิรูปการบริหารจัดการและการปรับปรุงโครงสร้างกระทรวงกลาโหม แผนพัฒนาขีดความสามารถกระทรวงกลาโหม และยุทธศาสตร์เฉพาะเรื่องตลอดจนใช้เป็นพื้นฐานในการจัดทำโครงการและความต้องการงบประมาณประจำปีให้มีความสอดคล้อง และสนับสนุนการบรรลุเป้าหมายตามแผนปฏิบัติการด้านการปกป้องอธิปไตย และรักษาผลประโยชน์ของชาติในภาพรวม พ.ศ. ๒๕๖๖-๒๕๗๐ รวมทั้งให้มีการประเมินผลสัมฤทธิ์และปัญหาข้อขัดข้องของแผนปฏิบัติการ ที่จัดทำรองรับอย่างต่อเนื่องตลอดจนกำหนดให้มีการทบทวนและปรับปรุงแผนปฏิบัติการด้านการปกป้องอธิปไตยและรักษาผลประโยชน์ของชาติในภาพรวมทุก ๆ ๒ ปี หรือเมื่อสถานการณ์ด้านความมั่นคง มีการเปลี่ยนแปลงไปอย่างรวดเร็ว ทั้งนี้ กระทรวงกลาโหมมีความจำเป็นที่จะต้องได้รับการสนับสนุนงบประมาณจากรัฐบาลอย่างต่อเนื่อง ในแต่ละปีงบประมาณไม่ต่ำกว่าร้อยละ ๒ ของผลิตภัณฑ์มวลรวมในประเทศ (Gross Domestic Product : GDP) และได้รับการสนับสนุนงบประมาณเพิ่มเติมในระดับที่เหมาะสมกับสถานการณ์ด้านความมั่นคงที่เปลี่ยนแปลงไป

บทที่ ๒

วิเคราะห์สภาวะแวดล้อมด้านความมั่นคง ที่ส่งผลกระทบต่อมิติความมั่นคงทางทหาร ในปี ๒๕๖๖ - ๒๕๗๐

บทที่ ๒ วิเคราะห์สภาวะแวดล้อมด้านความมั่นคงที่ส่งผลกระทบต่อมิติความมั่นคงทางทหาร ในปี ๒๕๖๖ - ๒๕๗๐

ทิศทางโลก

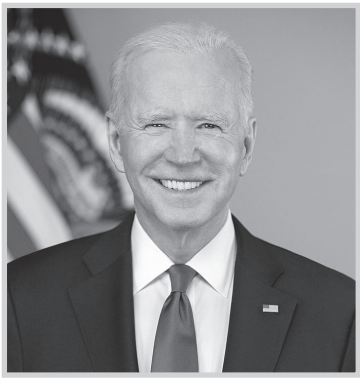
หลังจากการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID-19) โลกจะเผชิญภัยคุกคาม ในรูปแบบผสมผสาน (Hybrid Threats) ระหว่างภัยคุกคามแบบดั้งเดิมและภัยคุกคามรูปแบบใหม่ อาทิ การเปลี่ยน แปลงสภาพภูมิอากาศ การแพร่ระบาดของโรคอุบัติใหม่ การโจมตีโดยการใช้เทคโนโลยี และการโจมตีทางไซเบอร์ เป็นต้น ซึ่งจะสร้างความเสียหายต่อระบบการเมือง เศรษฐกิจ สังคม ความมั่นคง และความสัมพันธ์ระหว่างประเทศ อีกทั้งประเด็นต่างๆ เหล่านี้ หน่วยงานความมั่นคงส่วนใหญ่ ยังขาดความ เชี่ยวชาญ และต้องใช้งบประมาณในการ รับมือในระดับสูง ดังนั้นจึงต้องมีการบูรณาการระหว่างหน่วยงาน ภาครัฐและเอกชนในการแก้ปัญหาแบบองค์รวม มากขึ้น และจากวิกฤต COVID-19 ทั่วโลกต้องปรับตัวครั้งใหญ่ ทำให้เป็นตัวเร่งให้เกิดการพัฒนาเทคโนโลยีและการเปลี่ยนแปลงในทุกๆ ด้านอย่างรวดเร็ว

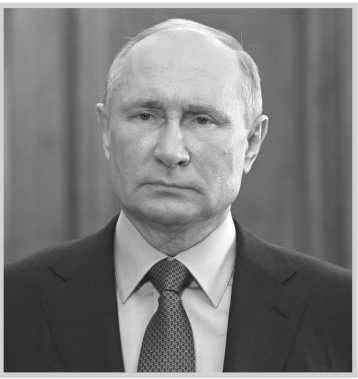
นอกจากนี้สถานการณ์ความขัดแย้งระหว่างรัสเซีย-ยูเครน ที่ยังไม่มีแนวโน้มว่าจะยุติในเวลาอันสั้นได้ส่ง ผลกระทบโดยรวมทั้งด้านเศรษฐกิจ พลังงาน และอาหารทั่วโลก จากเหตุการณ์การสู้รบระหว่างรัสเซียกับยูเครน พบว่าการปฏิบัติการทางทหารแบบดั้งเดิมได้พัฒนาไปอย่างมาก มีการนำอาวุธที่มีเทคโนโลยีสูงมาใช้งานอย่างกว้างขวาง เช่น ขีปนาวุธไฮเปอร์โซนิก ระบบป้องกันภัยทางอากาศที่ทันสมัย เป็นต้น นอกจากนี้ยังพบว่ามีการนำเครื่องมือทางด้าน Soft Power มาใช้สนับสนุนการปฏิบัติทางทหารอย่างกว้างขวาง โดยเฉพาะการปฏิบัติการข่าวสาร และ การปฏิบัติการด้านไซเบอร์โดยการปฏิบัติการข่าวสารนั้น มีการดำเนินการทั้งแบบเปิดเผยและ ปิดลับ ด้วยการพยายามแทรกแซง ครอบงำกลุ่ม/องค์กรที่เป็นประโยชน์ต่อการปล่อยข่าว ทั้งสื่อมวลชน องค์กรที่ไม่แสวงหาผลกำไร (NGOs) สถาบันคลังสมอง (Think Tank) รวมทั้งพรรคการเมืองในประเทศต่างๆ เพื่อลดทอน ความน่าเชื่อถือ สร้างความหวาดกลัวและความเกลียดชัง ตลอดจนบิดเบือนข้อมูล (Disinformation) และสร้างความจริงใหม่ เพื่อโน้มน้าวและชักจูงประชาคมโลกให้เชื่อและคิดไปในทางเดียวกัน ส่วนการปฏิบัติการด้านไซเบอร์ การโจมตีส่วนใหญ่มุ่งเป้าไปที่โครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา โทรคมนาคม การโจมตีหน่วยงานต่างๆ เช่น กระทรวงมหาดไทย กลาโหมต่างประเทศ สาธารณสุข ยุติธรรม สารสนเทศศึกษา รวมทั้งภาคธนาคาร สื่อสารมวลชนของรัฐ โดยเฉพาะรัสเซียเป็นมหาอำนาจทางไซเบอร์ที่มีทั้งเครื่องมือและแฮกเกอร์ที่มีความสามารถ และในระยะหลังรัสเซียประกาศรายชื่อประเทศไม่เป็นมิตร ส่งผลให้ประเทศที่ร่วมประณามและคว่ำบาตรรัสเซียต้องเผชิญกับการโจมตีทางไซเบอร์มากขึ้นอย่างมีนัยสำคัญ

การตรวจสอบสภาวะแวดล้อมสถานการณ์โลก

ในห้วงที่ผ่านมามีการแข่งขันระหว่างประเทศมหาอำนาจ และขั้วอำนาจต่าง ๆ ของโลกอย่างเข้มข้น โดยเฉพาะการแข่งขันของประเทศมหาอำนาจอย่างสหรัฐอเมริกาเพื่อสกัดกั้นอิทธิพลของจีน และในห้วงต่อไป โลกจะเผชิญภาวะการแข่งขันของ ๓ ขั้วอำนาจ ระหว่างสหรัฐฯ กับจีนและรัสเซีย ทำให้แนวโน้มของสภาวะการณ์ในปัจจุบัน ความขัดแย้งหรือวิกฤตการณ์การสู้รบของประเทศมหาอำนาจหนึ่งที่มีต่ออีกประเทศหนึ่ง ย่อมมีสัญญาณบ่งชี้ว่าผลกระทบจะขยายออกไปสู่วงกว้างในระดับโลก ทั้งในเรื่องของการแสดงท่าทีและการดำเนินความสัมพันธ์ระหว่างประเทศ รวมทั้งการดำเนินนโยบายรองรับการเปลี่ยนแปลงห่วงโซ่อุปทานโลก นอกจากนี้แนวโน้มการรวมกลุ่ม ของขั้วอำนาจต่างๆ ที่มีการต่อรองผลประโยชน์ร่วมกัน เริ่มมีการเร่งรัดกระบวนการแยกตัว (decoupling) ของระบบการเมือง การทหาร เศรษฐกิจ และเทคโนโลยีระหว่างกลุ่มประเทศต่างๆ ที่ชัดเจนและรวดเร็วยิ่งขึ้น แต่อย่างไรก็ตาม การรวมกลุ่มกันในประเด็นผลประโยชน์ที่มีความเชื่อมโยงทับซ้อน กันระหว่างประเทศในแต่ละขั้วอำนาจ มีแนวโน้มว่าไม่ได้แยกออกจากกันโดยสิ้นเชิง ในห้วงต่อไปการแข่งขันเพื่อขยายอิทธิพลที่สำคัญ คือ ๑) การสะสมอาวุธและการแพร่ขยายอาวุธ และ ๒) การแสวงประโยชน์จากความก้าวหน้าทางเทคโนโลยีและนวัตกรรม

การแพร่ระบาดของ COVID-19 ตลอดห้วงที่ผ่านมา ส่งผลให้การเคลื่อนไหวของกลุ่มก่อการร้ายต่างๆ ลดน้อยลง และมีการปรับเปลี่ยนรูปแบบการก่อเหตุเป็นลักษณะของการปฏิบัติการโดยลำพัง (Lone Actor) รวมถึงมุ่งเน้นการเผยแพร่/บ่มเพาะแนวคิดสุดโต่งที่นิยมความรุนแรงมากขึ้น อีกทั้งการก่อการร้ายยังเกี่ยวข้องกับ อาชญากรรมอื่นๆ โดยเฉพาะการขยายตัวของอาชญกรรมทางเศรษฐกิจ การเปลี่ยนแปลงทางเทคโนโลยีอย่างฉับพลัน เป็นปัจจัยเร่งให้วิถีชีวิตของประชาชนต้องพึ่งพิงระบบเทคโนโลยีสารสนเทศมากขึ้น จึงมีความเสี่ยงที่จะโดยภัยคุกคามทางไซเบอร์ทั้งจากรัฐ (State) และตัวแสดงที่ไม่ใช่รัฐ (Non-State Actors) ในการนำข้อมูลไปใช้ สำหรับการก่อการร้ายและอาชญากรรมทางไซเบอร์ รวมถึงการโจมตีโครงสร้างพื้นฐานสำคัญ (Critical Infrastructures-CI) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructures-CII)



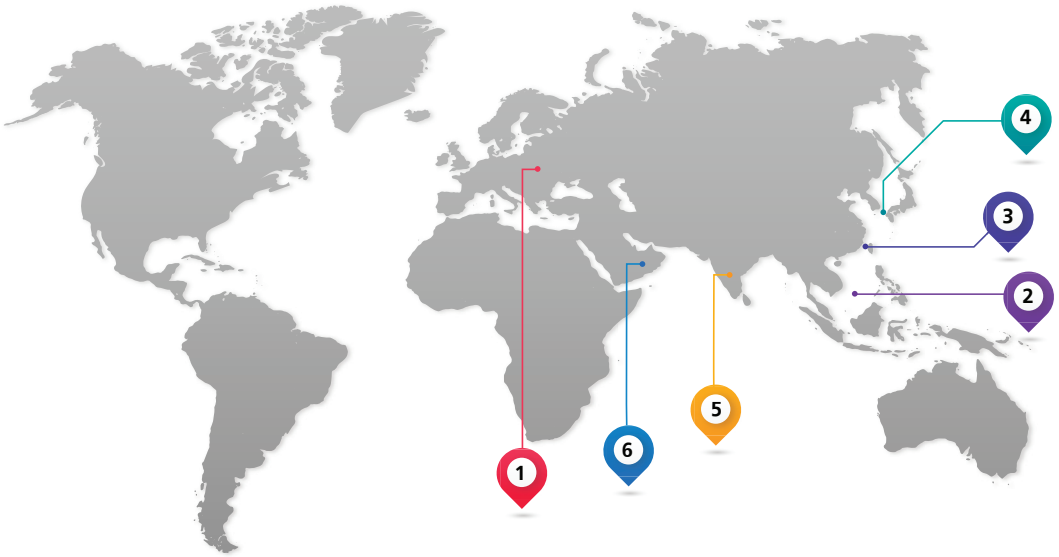


ปัจจัยทางชีวภาพของเชื้อโรคที่มีวิวัฒนาการอย่างสม่ำเสมอ การดื้อยาต้านจุลชีพ พฤติกรรมของมนุษย์ที่ ไม่ถูกสุขลักษณะ และปัจจัยด้านการเปลี่ยนแปลงของสภาพภูมิอากาศที่เกิดขึ้นอย่างต่อเนื่อง ส่งผลให้โรคติดต่อ อุบัติใหม่และภัยสุขภาพต่าง ๆ เพิ่มมากขึ้น โดยเฉพาะโรคติดต่ออุบัติใหม่มีแนวโน้มยกระดับเป็นโรคระบาดที่เป็น โรคติดต่อหรือโรคที่ยังไม่ทราบสาเหตุของการเกิดโรคแน่ชัด ส่งผลกระทบต่อความมั่นคงทางอาหารและความมั่นคงทางสุขภาพต่อสุขภาวะของคนในชาติ

ผลกระทบจากการเปลี่ยนแปลงสภาพภูมิอากาศและภาวะโลกร้อน มีความเกี่ยวข้องกับมิติความมั่นคง หลายประการและเป็นปัจจัยที่เพิ่มความเปราะบางของปัญหาที่มีอยู่เดิม ได้แก่ ๑) ปัญหาระดับน้ำทะเลที่สูงขึ้น ส่งผลกระทบต่อการกัดเซาะบริเวณชายฝั่งทำให้เส้นฐาน (Baseline) ที่ใช้ในการกำหนดเขตพื้นที่ดังกล่าวถอยร่นตามแนวน้ำที่สูงขึ้นจากตำแหน่งเดิม ๒) ปัญหาการขาดแคลนและแย่งชิงทรัพยากรน้ำ ๓) ปัญหาการโยกย้ายถิ่นฐาน ๔) ปัญหาความมั่นคงทางอาหารและน้ำ และ ๕) ปัญหาความมั่นคงทางพลังงาน

นอกจากนี้ ปัญหาการเข้าสู่สังคมสูงอายุอย่างสมบูรณ์ในประเทศกำลังพัฒนา จะนำมาซึ่งความท้าทายต่อความมั่นคงของประเทศ ทั้งในเรื่องปัญหาการขาดแคลนแรงงาน ปัญหาการค้ามนุษย์อันเป็นผลมาจากความ ต้องการด้านแรงงานที่เพิ่มขึ้น การขาดระบบสวัสดิการที่เพียงพอ ปัญหาสุขภาพจิตใจของผู้สูงวัยจากการถูกแยก ออกจากภาคเศรษฐกิจและสังคม รวมถึงปัญหาช่องว่างระหว่างวัยที่นำไปสู่การปะทะกันทางความคิดและความแตกแยกในสังคม

จุดขัดแย้ง (Hot Spot) ที่สำคัญของโลกในยุคปัจจุบัน



1. สถานการณ์ความขัดแย้งระหว่างรัสเซีย-ยูเครน
2. ทะเลจีนใต้
3. สถานการณ์ในช่องแคบไต้หวัน
4. สถานการณ์คาบสมุทรเกาหลี
5. เอเชียใต้
6. ตะวันออกกลาง

๑ สถานการณ์ความขัดแย้งระหว่างรัสเซีย-ยูเครน

เป็นสถานการณ์ที่ส่งผลกระทบต่อทั้งโลกเป็นวงกว้าง ในหลายประเด็น หลายฝ่ายประเมินสอดคล้องกันว่า อาจเกิดวิกฤติความมั่นคงทางอาหาร ซึ่งเป็นความท้าทาย ครั้งใหญ่ของโลกนับตั้งแต่ยุคสงครามโลกครั้งที่ ๒ รวมทั้งเกิดวิกฤติด้านมนุษยธรรม ความเสี่ยงด้านสงคราม นิวเคลียร์ รวมถึงกลุ่มก่อการร้ายและกลุ่มแนวคิดสุดโต่งอาจแสวงประโยชน์จากการสู้รบ เนื่องจากกลุ่มก่อการร้าย ส่วนใหญ่มีท่าทีเห็นด้วยกับการปฏิบัติการทางทหารของรัสเซีย และมีแนวโน้มว่าองค์การระหว่างประเทศอาจถูก ประเทศตะวันตกใช้เป็นกลไกในการกดดันรัสเซีย เพื่อกีดกันและโดดเดี่ยวรัสเซียออกจากประชาคมหรือองค์การ ระหว่างประเทศ ปัจจุบันสถานการณ์ดังกล่าวยังไม่มีแนวโน้มจะยุติในเวลาอันสั้น และส่งผลกระทบโดยรวมทั้งใน ด้านเศรษฐกิจ พลังงาน และอาหารทั่วโลก

๒ ทะเลจีนใต้

เป็นพื้นที่สุ่มเสี่ยงที่สุดที่จะเกิดการปะทะทางทหารระหว่างสหรัฐอเมริกากับจีน หากมีการประเมินสถานการณ์ที่ผิดพลาด ปัจจุบันการจัดทำประมวลปฏิบัติในทะเลจีนใต้ (Code of Conduct-CoC) ยังไม่มีความคืบหน้า ทั้งในด้านการแก้ไขข้อพิพาทหมู่เกาะพาราเซลอย่างเป็นรูปธรรม การเพิ่มบทบาทของสหรัฐฯ โดยเฉพาะการปฏิบัติการของเสรีภาพในการเดินเรือในทะเลจีนใต้ รวมถึงการโจมตีจีนในการละเมิดอนุสัญญาสหประชาชาติว่าด้วยกฎหมายทะเล ค.ศ. 1982 (United Nations Convention on the Law of the Sea-UNCLOS)

๓ สถานการณ์ในช่องแคบไต้หวัน

จีนยังคงเพิ่มการข่มขู่ไต้หวันทั้งด้านการทหาร การเมือง เศรษฐกิจ และการเมืองระหว่างประเทศ ขณะที่ไต้หวันตอบโต้ด้วยการกระชับความสัมพันธ์กับพันธมิตรโดยเฉพาะอย่างยิ่งสหรัฐอเมริกา รวมทั้งการสร้างบทบาทในเวทีโลกและการขยายความร่วมมือทางเศรษฐกิจ

๔ สถานการณ์คาบสมุทรเกาหลี

การรื้อฟื้นการเจรจาระหว่างสหรัฐอเมริกากับเกาหลีเหนือ เพื่อปลด อาวุธนิวเคลียร์มีความไม่แน่นอน ขณะที่ปัญหาเศรษฐกิจและการแข่งขันอิทธิพลของมหาอำนาจอาจส่งผลให้ การแก้ไขปัญหาซับซ้อนยิ่งขึ้น

๕ เอเชียใต้

การกลับมามีอำนาจของตาลิบันยังคงส่งผลกระทบต่อความมั่นคงและการเมืองระหว่างประเทศที่ยังไม่มีการรับรองสถานะของรัฐบาลประกอบกับนโยบายลดความสัมพันธ์กับกลุ่มก่อการร้ายที่เป็นพันธมิตร อาจทำให้อัฟกานิสถานเป็นแหล่งบ่มเพาะการก่อการร้ายสากลอีกครั้ง

๖ ตะวันออกกลาง

คู่ขัดแย้งระหว่างอิหร่านและซาอุดีอาระเบียอาจยกระดับเป็นสงครามเย็นในภูมิภาค อิหร่านกับสหรัฐอเมริกาและประเทศตะวันตกอาจเกิดการทำสงครามตัวแทน สงครามกลางเมืองที่ยืดเยื้อในเยเมนและสถานการณ์ความมั่นคงในอิรักยังคงมีความไม่แน่นอนเนื่องจากยังคงเชื่อมโยงกับกลุ่ม IS

การตรวจสอบสภาวะแวดล้อมในภูมิภาคเอเชียตะวันออกเฉียงใต้

ที่ตั้งของภูมิภาคเอเชียตะวันออกเฉียงใต้เป็นเส้นทางคมนาคมและแหล่งทรัพยากรพลังงานที่สำคัญ ทำให้เกิดการแข่งขันและขยายอิทธิพลเชิงยุทธศาสตร์ของประเทศมหาอำนาจและขั้วอำนาจต่างๆ ในภูมิภาคแห่งนี้ โดยเฉพาะ ๒ พื้นที่สำคัญ ได้แก่ ๑) พื้นที่พิพาทในทะเลจีนใต้ ซึ่งเป็นเส้นทางการเดินเรือพาณิชย์ และ ๒) พื้นที่ อนุภูมิภาคลุ่มน้ำโขง เนื่องจากเป็นพื้นที่ใช้ทรัพยากรธรรมชาติและสิ่งแวดล้อมร่วมกัน ซึ่งการแข่งขันอิทธิพลจีน - สหรัฐฯ จะครอบงำบรรยากาศการเมืองระหว่างประเทศ โดยสหรัฐฯ จะสกัดกั้นอิทธิพลของจีนในภูมิภาค อินโด - แปซิฟิก ผ่านการสานต่อการดำเนินยุทธศาสตร์อินโด - แปซิฟิก ที่เน้นนโยบายเพิ่มความเกี่ยวพัน และส่งเสริม ความร่วมมือกับประเทศในภูมิภาคนี้ในทุกมิติ ตลอดจนส่งเสริมบทบาทของประเทศมหาอำนาจ และหุ้นส่วน ในยุโรป อาทิ สหราชอาณาจักร เยอรมนี ให้ร่วมมีบทบาทด้านความมั่นคงในภูมิภาค ที่สำคัญคือ เพิ่มความร่วมมือเพื่อค้ำประกันเสรีภาพการเดินเรือในทะเลจีนใต้ ส่งเสริมบทบาทของกลุ่ม AUKUS (ออสเตรเลีย สหราชอาณาจักร สหรัฐฯ) และพันธมิตรความมั่นคงสี่ฝ่าย (Quadrilateral Security Dialogue - QUAD) (สหรัฐฯ อินเดีย ญี่ปุ่น ออสเตรเลีย) ประกอบกับสหรัฐฯ จะเพิ่มความร่วมมือด้านการทหารกับไต้หวัน ซึ่งการดำเนินการของสหรัฐฯ ดังกล่าวอาจเพิ่มความท้าทายต่อความมั่นคงของภูมิภาค เพราะจะยิ่งกระตุ้นให้บรรยากาศ ความร่วมมือของประเทศในภูมิภาคกับสหรัฐฯ และจีน ดำเนินไปท่ามกลางการแข่งขันอิทธิพลของ ทั้งสองประเทศ

แนวโน้มสถานการณ์ในเมียนมาจะยังคงเป็นปัจจัยเสี่ยงสำคัญที่สุดต่อเสถียรภาพและความมั่นคงของ ภูมิภาคเอเชียตะวันออกเฉียงใต้โดยเฉพาะไทย

เมียนมาต้องเผชิญกับการเคลื่อนไหวของกองกำลังป้องกันชายแดน (People's Defence Force -PDF) รวมทั้งการช่วงชิงความเป็นรัฐบาลที่ชอบธรรมระหว่างสภาบริหารแห่งรัฐ (State Administration Council - SAC) กับรัฐบาลเอกภาพแห่งชาติ (National Unity Goverment - NUG) ซึ่งจะส่งผลให้ไทยเผชิญแรงกดดันมากขึ้นจากประเทศต่างๆ ที่ต้องการให้ไทยโน้มน้าว SAC ให้เร่งแก้วิกฤติด้วยแนวทางเจรจา นอกจากนี้ไทยอาจถูกใช้เป็นพื้นที่เคลื่อนไหวต่อต้าน SAC หรือกลุ่มอื่นๆ ที่พยายามแทรกแซง สถานการณ์ในเมียนมา อีกทั้งไทยต้องเผชิญกับการลักลอบเข้าเมืองโดยผิดกฎหมายและการอพยพของผู้หนีภัย จากการสู้รบชาวเมียนมา

นอกจากนี้ ความแตกต่างด้านค่านิยม วัฒนธรรม ระดับการพัฒนา ระบบการปกครอง เป็นความท้าทายของอาเซียนในการมีกฎเกณฑ์และค่านิยมร่วมกันที่อาจส่งผลต่อปัญหาและความท้าทายที่สำคัญ ไม่ว่าจะเป็นการป้องกันและแก้ไขภัยคุกคามระหว่างประเทศสมาชิกอาเซียน ความมีเอกภาพ ความเป็นแกนกลาง และมุมมองของ อาเซียนต่อแนวคิดอินโด - แปซิฟิก (ASEAN Outlook on Indo - Pacific: AOIP) ซึ่งอาเซียนต้องทบทวนบทบาท เกี่ยวกับการคงสถานะความเป็นกลางที่จะไม่แทรกแซงกิจการภายในของประเทศสมาชิก

ประเด็นประเทศมหาอำนาจโดยเฉพาะการแข่งขันอิทธิพลระหว่างสหรัฐฯ และจีน จะมีบทบาทต่อสถานการณ์ความมั่นคงในภูมิภาคนี้ ทั้งในมิติด้านการเมือง เศรษฐกิจ สังคม และการแทรกแซงการเมือง โดยไทยจะได้รับผลกระทบโดยตรงจากสถานการณ์ตึงเครียดตามแนวชายแดนในการเป็นพื้นที่รองรับหรือการใช้ไทยเป็นทางผ่านไปยังประเทศอื่น รวมถึงความพยายามที่จะให้ไทยเข้าไปมีส่วนร่วมในประเด็นความขัดแย้งตลอดจนผลกระทบทางเศรษฐกิจและการค้าชายแดนของไทย

สถานการณ์ความมั่นคงชายแดนมีความแตกต่างกันไปตามบริบทของพื้นที่ และความสัมพันธ์เชื่อมโยงกับมิติต่างๆ ที่ส่งผลกระทบต่อความมั่นคงของประเทศโดยรวม โดยปัญหาที่สำคัญ คือ อาชญากรรมข้ามชาติ แรงงานผิดกฎหมาย การลักลอบเข้าเมืองผิดกฎหมาย ความไม่ชัดเจนของเส้นเขตแดน และปัญหาโรคระบาด รวมถึงการเฝ้าระวังการแย่งชิงผลประโยชน์และการแข่งขันทางทะเล

นอกจากนี้แนวโน้มความมั่นคงทางไซเบอร์ อากาศ และอวกาศ จะเป็นสนามการแข่งขันที่สำคัญผ่าน การพัฒนานวัตกรรม และเทคโนโลยีต่างๆ การพัฒนาท่าอากาศยาน การบริการด้านการบินพลเรือน ตลอดจน การจัดหาอาวุธยุทโธปกรณ์เพื่อเสริมสร้างศักยภาพทางการทหารและปกป้องผลประโยชน์ของประเทศ นอกเหนือ จากการแข่งขันการพัฒนาขีดความสามารถของกำลังทางอากาศแล้ว มีแนวโน้มที่ประเทศต่างๆ จะให้ความสำคัญ กับบริบทความมั่นคงทางอวกาศ (Space Security) มากยิ่งขึ้นด้วย โดยประเทศมหาอำนาจมีแนวทาง ดำเนินนโยบายเพื่อช่วงชิง การเป็นผู้นำทางอวกาศและการป้องกันประเทศ การลงทุนและการให้บริการ อินเทอร์เน็ตความเร็วสูง ตลอดจนการสร้างความร่วมมือกับมิตรประเทศต่างๆ ในอาเซียน ซึ่งเป็นพื้นที่เป้าหมาย สำคัญเชิงยุทธศาสตร์ที่อยู่ตรงกลางของภูมิภาคอินโด - แปซิฟิก โดยมีการสนับสนุนการแลกเปลี่ยนและถ่ายทอด องค์ความรู้ด้านนวัตกรรม และเทคโนโลยีทางอวกาศให้แก่ประเทศดังกล่าว ทำให้ส่งผลต่อการช่วงชิงพื้นที่ทางยุทธศาสตร์ต่อบริบทความมั่นคง โดยไทยสามารถแสวงหาโอกาสจากความร่วมมือ การเตรียมพร้อมทรัพยากร การพัฒนาองค์ความรู้และทักษะ ตลอดจนการส่งเสริมและแลกเปลี่ยนงานวิจัยและนวัตกรรมทั้งภายในประเทศ และสถาบันหรือองค์การระหว่างประเทศ

ปัญหาอาชญากรรมข้ามชาติ ยังเป็นปัญหาความมั่นคงที่สำคัญและมีความซับซ้อน เชื่อมโยงระหว่างประเทศมากขึ้น โดยมีประเด็นสำคัญที่ควรเฝ้าระวัง ทั้งในเรื่องการลักลอบค้ายาเสพติด การปลอมแปลงเอกสาร และหลักฐานเกี่ยวกับตัวบุคคล การลักลอบเข้าเมืองและการค้ามนุษย์ รวมถึงการฟอกเงิน ด้วยเหตุนี้ประเทศไทย จึงมีแนวโน้มได้รับผลกระทบและเผชิญกับประเด็นท้าทายด้านการก่ออาชญากรรมข้ามชาติ เนื่องจากที่ตั้งเป็นศูนย์กลางด้านการคมนาคมและการสัญจรระหว่างประเทศที่สำคัญของภูมิภาค รวมทั้งเป็นแหล่งพักพิงและพื้นที่ ปฏิบัติการของเครือข่ายอาชญากรรมข้ามชาติ นอกจากนี้ กลุ่มผู้ก่อเหตุยังใช้พื้นที่ชายแดนในการกระทำความผิด ในการก่อปัญหาอาชญากรรมทางไซเบอร์ มิจฉาชีพคอลเซ็นเตอร์ (Call Center) การฟอกเงิน และการพนันออนไลน์ ซึ่งส่งผลกระทบต่อประชาชนภายในประเทศ จึงจำเป็นต้องแก้ไขปัญหาอาชญากรรมข้ามชาติในพื้นที่ชายแดน ผ่านกลไกความร่วมมือทวิภาคีในระดับพื้นที่ โดยเฉพาะด้านการข่าวและการปฏิบัติการทางด้านความมั่นคงร่วมกัน เพื่อป้องกันไม่ให้อาชญากรรมข้ามชาติในพื้นที่ชายแดนส่งผลเข้ามายังพื้นที่ชั้นในของประเทศ

ปัญหาการก่อการร้ายและปัญหาจากการบ่มเพาะแนวคิดสุดโต่งที่นิยมความรุนแรงยังเป็นอีกหนึ่งปัญหาที่สำคัญของภูมิภาค โดยเฉพาะการแสวงหาแนวร่วมผ่านการใช้สื่อสังคมออนไลน์ ในขณะที่สถานการณ์ความขัดแย้งทางการเมืองภายในภูมิภาคตะวันออกกลางและในอัฟกานิสถานยังไม่แน่นอน มีสัญญาณและแนวโน้มที่คาดว่าจะเกิดการเคลื่อนย้ายนักรบก่อการร้ายต่างชาติ (Foreign Terrorist Fighters) และการก่อเหตุของผู้ปฏิบัติการโดยลำพัง อีกทั้งทำเลที่ตั้งของไทยซึ่งเป็นศูนย์กลางการเดินทางระหว่างประเทศที่สำคัญในภูมิภาคอาจถูกใช้เป็น ทางผ่าน แหล่งพักพิงและแหล่งจัดหาวัสดุอุปกรณ์ และมักจะก่อเหตุในพื้นที่เปราะบาง

การตรวจสอบสภาวะแวดล้อมภายในประเทศ

การประเมินภัยคุกคามภายในประเทศที่จะกระทบต่อความมั่นคงของชาติ มีประเด็นที่น่าสนใจดังนี้.-

๑ การบ่อนทำลายสถาบัน

มีแนวโน้มรุนแรงและขยายวงกว้าง โดยเฉพาะในกลุ่มเยาวชนที่กล้าแสดง ออกผ่านกิจกรรมที่หลากหลายมากขึ้นทั้งในพื้นที่สาธารณะและการใช้สื่อสังคมออนไลน์ โดยมักเผยแพร่ความคิด ของกลุ่มนักวิชาการหรือผู้มีอิทธิพลทางความคิด (Influencer) ทั้งที่อยู่ในไทยและต่างประเทศผ่านการแสดงความคิดเห็น หรือเผยแพร่เนื้อหา (Content) ในรูปแบบต่างๆ ทางออนไลน์ รวมทั้งพยายามดึงต่างชาติเข้ามากดดันการปฏิรูปสถาบัน ซึ่งจะทำให้การจัดการกับปัญหาดังกล่าวยากลำบากมากขึ้น

๒ ความขัดแย้งทางการเมือง

ซึ่งมีตัวละครที่สำคัญประกอบด้วย ฝ่ายรัฐบาล ฝ่ายค้าน กลุ่มการเมือง นอกสภาผู้แทนราษฎร กลุ่มพลังต่างๆ และผู้ได้รับความเดือดร้อนทางเศรษฐกิจ ตลอดจนการได้รับอิทธิพลจากการเผยแพร่ค่านิยมประชาธิปไตย และสิทธิมนุษยชนจากต่างชาติ ทำให้การเมืองไทยเกิดความแตกแยกทางความคิด และอุดมการณ์ทางการเมือง ส่งผลกระทบต่อความพยายามในการแก้ไขปัญหาอื่นๆ

๓ ภาวะเศรษฐกิจตกต่ำ

มีสาเหตุหลักมาจากวิกฤติ COVID-19 และระบบเศรษฐกิจโลกที่มีความไม่แน่นอนและผันผวนสูง เป็นปัจจัยหนึ่งที่ส่งผลให้ไทยต้องเผชิญกับภาวะการชะลอตัวทางเศรษฐกิจ อย่างไรก็ตาม กลุ่มทุนขนาดใหญ่จะยังคงถือครองกำไรส่วนใหญ่และมีอำนาจในการกำหนดราคาสินค้าและบริการ ส่งผลให้ภาควิสาหกิจขนาดกลางและขนาดย่อม รวมทั้งผู้ประกอบการรายย่อยเกิดความไม่คล่องตัวในการบริหารจัดการ นอกจากนี้การเข้าสู่ยุคดิจิทัลได้ปรับเปลี่ยนลักษณะการดำเนินกิจกรรมทางเศรษฐกิจที่มุ่งไปใช้ประโยชน์จากแพลตฟอร์มออนไลน์มากขึ้น อีกทั้งพฤติกรรมการบริโภคที่เปลี่ยนแปลงไปได้กลายเป็นปัจจัยเสี่ยงต่อการก่ออาชญากรรมทางเศรษฐกิจที่ขยายตัวมากขึ้น อาทิ การลักลอบค้าสินค้าละเมิดทรัพย์สินทางปัญญา การค้าน้ำมันเถื่อน การโจรกรรม และการพนันออนไลน์ รวมถึงภัยคุกคามทางไซเบอร์ต่อสถาบันการเงิน

๔ ความไม่สงบในจังหวัดชายแดนภาคใต้

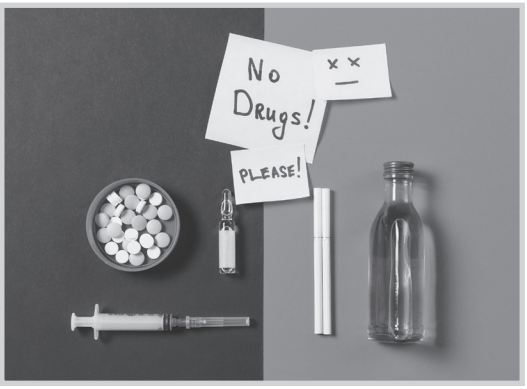
มีความเสี่ยงสูงที่จะเกิดการก่อเหตุในรูปแบบต่างๆ มากขึ้น ขณะที่การพูดคุยสันติสุขระหว่างรัฐบาลกับกลุ่มแนวร่วมปฏิวัติแห่งชาติมลายูปาตานี (Barisan Revolusi Nasional - BRN) ยังไม่อาจเป็นหลักประกันได้ว่าการก่อความไม่สงบจะลดลง ส่วนบทบาทขององค์กรพัฒนา เอกชน (Non-Governmental Organizations - NGOs) และภาคประชาสังคม ในพื้นที่ทางการมาเลเซีย ตลอดจนประเทศและองค์กรอื่นๆ ทั้งในและต่างประเทศ เป็นประเด็นที่ต้องติดตามและอาจมีผลต่อสถานการณ์ใน จชต. ทั้งทางบวกและลบ เช่น เดียวกับความพยายามเชื่อมโยงปัญหา จชต.กับการเมืองส่วนกลาง นอกจากนี้ ปัญหาภัย แทรกซ้อน ปัญหาทางด้านเศรษฐกิจและสังคม ปัญหาความหวาดระแวงและความเข้าใจระหว่างกันยังคงเป็นปัญหาที่เชื่อมโยงและส่งผลกระทบในพื้นที่อย่างมีนัยสำคัญ ขณะเดียวกันสถานการณ์การแพร่ระบาดของ COVID-19 ยังส่งผลให้ปัญหาเศรษฐกิจมีความรุนแรง และมีความเหลื่อมล้ำมากยิ่งขึ้น

๕ ความมั่นคงตามแนวชายแดนทางบกและทางน้ำ

การสู้รบตามแนวชายแดนไทย - เมียนมา ระหว่าง กองทัพเมียนมากับกองกำลังฝ่ายต่อต้านและกลุ่มชาติพันธุ์ จะเป็นปัญหาความมั่นคงหลักตามแนวชายแดนทางบก ซึ่งจะทำให้ไทยได้รับผลกระทบจากการสู้รบและปัญหาจากผู้ประสบภัยจากการสู้รบ ผู้ได้รับความเดือดร้อน ทางเศรษฐกิจ การกระทำผิดกฎหมาย การแพร่ระบาดของโรคติดต่อ และสุ่มเสี่ยงที่จะประสบปัญหาความสัมพันธ์ระหว่างประเทศ ส่วนปัญหาความมั่นคงตามแนวชายแดนอื่น ๆ ที่สำคัญได้แก่ ปัญหาพิพาทเขตแดนทางบกและทางน้ำกับเมียนมา ลาว กัมพูชา และมาเลเซีย และการกระทำผิดกฎหมายข้ามแดนทางบก แม่น้ำโขง และทะเล อาณาเขต เช่น การรุกล้ำน่านน้ำ ของเรือประมงต่างชาติ และการโยกย้ายถิ่นฐานไม่ปกติในมหาสมุทรอินเดีย

๖ ปัญหายาเสพติด

การเปลี่ยนแปลงรูปแบบการผลิตเป็นอุตสาหกรรมขนาดใหญ่ที่ดำเนินการโดย องค์กรอาชญากรรมข้ามชาติ ทำให้การผลิตยาเสพติดในพื้นที่สามเหลี่ยมทองคำขยายตัวมากขึ้น ประกอบกับสถานการณ์ความไม่สงบภายในประเทศเพื่อนบ้าน



เป็นช่องโหว่ให้ผู้ค้ายาเสพติดฉกฉวยโอกาสในการเร่งผลิตและลักลอบขนส่งยาเสพติดเข้าสู่ประเทศไทย ตลอดจนการใช้ประเทศไทยเป็นทางผ่านเพื่อส่งต่อยาเสพติดไปยัง ประเทศที่สาม ทั้งนี้ การแพร่กระจายของยาเสพติดยังมีต่อเนื่องการแสวงหาโอกาสจากรูปแบบการส่งยาเสพติดทางพัสดุไปรษณีย์ การค้ายาเสพติดผ่านช่องทางออนไลน์ โฆษณา และขยายโครงข่ายการค้ายาเสพติดให้เข้าถึงกลุ่มผู้เสพ มีความหลากหลายรูปแบบและในพื้นที่ห่างไกลเพิ่มมากขึ้น ในขณะเดียวกันแนวโน้มการขยายตัวของ อาชญากรรมทางไซเบอร์มีความเกี่ยวเนื่องกับปัญหาการค้ายาเสพติดที่ใช้ช่องทางบล็อกเชน (Blockchain) ในการซื้อและขายมากขึ้น โดยเฉพาะในรูปแบบสกุลเงินดิจิทัล (Cryptocurrency) ทำให้การติดตามตรวจสอบ เพื่อระบุตัวตนดำเนินการได้ยากขึ้น ด้วยเหตุนี้ ปัญหายาเสพติดจึงเป็นตัวการสำคัญที่ก่อให้เกิดปัญหาสังคมอื่นๆ ตามมาหลายประการ เช่น ปัญหาครอบครัว ปัญหาความอ่อนแอทั้งร่างกายและจิตใจของประชาชน ปัญหาอาชญากรรมและการกระทำผิดกฎหมาย เป็นต้น ซึ่งส่งผลต่อความสงบเรียบร้อยและความมั่นคงของประชาชน และของชาติโดยรวม

๗ การก่อการร้ายและอาชญากรรมข้ามชาติ

มีความเป็นไปได้ที่กลุ่มก่อการร้ายจะกลับมาก่อเหตุมากขึ้น หลังสถานการณ์ COVID-19 คลี่คลาย โดยกลุ่ม Islamic State (IS) กลุ่มอัลกออิดะฮ์ และกลุ่มก่อการร้าย ที่ได้รับการสนับสนุนจากอิหร่าน เป็นกลุ่มหลักที่ต้องให้ความสนใจ ขณะที่การเผยแพร่และปลูกฝังแนวคิดผ่านระบบ ออนไลน์เป็นสิ่งที่ต้องเฝ้าระวัง รวมทั้งจำเป็นต้องมีการประเมินภัยก่อการร้ายและร่วมมือกับประชาคมระหว่างประเทศ สำหรับอาชญากรรมข้ามชาติจะมีการใช้ระบบออนไลน์ในการก่อเหตุเพิ่มขึ้น ส่วนการทำบัตรเครดิต และเอกสารปลอมจะเป็นปัญหามากขึ้นหลังการผ่อนคลายมาตรการปิดประเทศ

๘ การขยายอิทธิพลของต่างชาติ

ปรากฏในหลายรูปแบบและหลากหลายประเทศ นอกเหนือจากความขัดแย้งและการแข่งขันทางภูมิรัฐศาสตร์ระหว่างจีนกับสหรัฐฯ เช่น การเผยแพร่ค่านิยมทางการเมือง และสิทธิมนุษยชนของประเทศตะวันตกผ่านนักการทูตและเจ้าหน้าที่องค์กรระหว่างประเทศที่อยู่ในไทย ซึ่งจะมีผลต่อแนวคิดทางการเมือง ของประชาชนกลุ่มต่างๆ รวมถึงสถานการณ์ใน จชต. และต่อเนื่องถึงกระแสการสนับสนุน หรือต่อต้านรัฐบาล การเคลื่อนไหวของ NGOs บางองค์กรมีผลกระทบต่อการผลักดันโครงการของรัฐ การเข้ามา ของชาวต่างชาติในระดับบุคคลอาจสร้างปัญหา โดยอ้อมทั้งการแย่งอาชีพหรือเปิดกิจการแข่งกับคนไทย หรือกรณี ที่กลุ่มต่อต้านรัฐบาลทหารเมียนมามีความเชื่อมโยงกับ NGOs ด้านแรงงานของไทย เนื่องจากมีแรงงานเมียนมา ในไทยเป็นจำนวนมาก อาจทำให้มีการจัดกิจกรรมที่สุ่มเสี่ยงจะกระทบต่อความสัมพันธ์ไทย-เมียนมา

๙ การเปลี่ยนแปลงสภาพภูมิอากาศ

เป็นภัยต่อความมั่นคงของมนุษย์ที่สำคัญไม่ต่างจากภัยจากโรคติดต่อ เนื่องจากจะส่งผลกระทบต่อประชาชนและประเทศต่างๆ ซึ่งต้องใช้เวลานานในการแก้ไขปัญหา ในส่วนของไทยภัยแล้งและอุทกภัยจะเป็นปัญหาสำคัญของทุกภูมิภาค รวมถึงปัญหาหมอกควัน ไฟป่า และฝุ่น PM 2.5 ทั้งที่มีต้นเหตุจากในประเทศและจากประเทศเพื่อนบ้าน

๑๐ ปัญหาการทุจริตคอรัปชัน

แม้ว่าภาครัฐมีความพยายามแก้ไขปัญหาอย่างจริงจังผ่านการบริหาร จัดการบ้านเมืองที่ดีตามหลักธรรมาภิบาล (Good Governance) แต่การจัดอันดับความโปร่งใสของไทยและอันดับการรับรู้การทุจริตของประเทศพบว่า สถานการณ์การทุจริตคอรัปชันในภาครัฐ การทุจริตต่อหน้าที่ หรือการแสวงหาประโยชน์โดยมิชอบของเจ้าหน้าที่รัฐได้เกี่ยวพันกับการป้องกันและแก้ไขปัญหาภัยคุกคามอื่นๆ อาทิ ยาเสพติด ผู้หลบหนีเข้าเมือง กลุ่มผู้มีอิทธิพลในพื้นที่ที่ประกอบธุรกิจผิดกฎหมาย และการฟอกเงิน ส่งผลให้ปัญหาทวีความรุนแรงและซับซ้อนมากยิ่งขึ้น อีกทั้งยังเป็นอุปสรรคสำคัญในการพัฒนาประเทศตลอดจนส่งผลต่อความเชื่อมั่นต่อรัฐบาล ภาครัฐ และระบอบประชาธิปไตย ตามลำดับ

๑๑ ปัญหาข่าวปลอม (Fake News)

เป็นภัยที่มีผลต่อการแก้ไขปัญหาความมั่นคงแบบองค์รวม และเป็น ปัจจัยที่สร้างความยากลำบากในการจัดการกับปัญหาการบ่อนทำลายสถาบัน ความขัดแย้งทางการเมือง และการแบ่งแยกทางความคิด ซึ่งในยุคที่เทคโนโลยีมีการพัฒนาอย่างก้าวกระโดดและมีการเชื่อมต่อกันทุกภาคส่วน ทำให้การติดตามและแก้ไขปัญหาอย่างเป็นรูปธรรม รวมทั้งการรู้เท่าทันภัยจากข่าวปลอม จึงเป็นสิ่งสำคัญที่ต้องมีการปรับเปลี่ยนให้ทันกับสถานการณ์ทั้งระดับบุคคล องค์กร และประเทศ

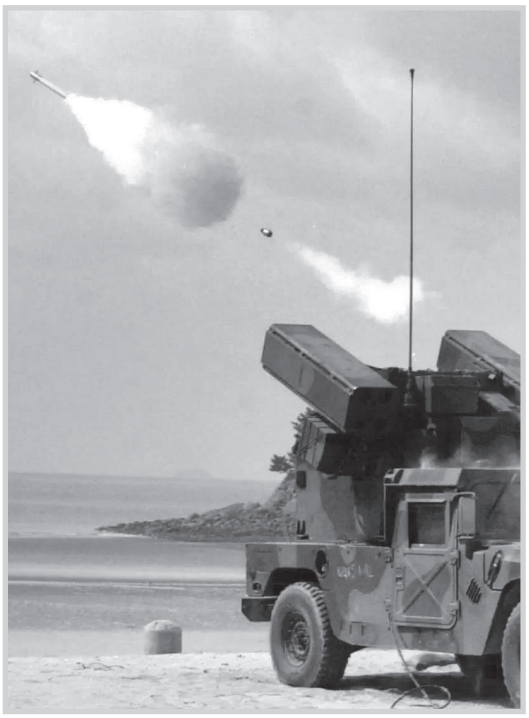
๑๒ ปัญหาจากเทคโนโลยีและภัยคุกคามทางไซเบอร์

ที่สำคัญ ได้แก่ การใช้เทคโนโลยีไซเบอร์เพื่อดำเนินกิจกรรมที่เป็นภัยต่อความมั่นคงทางการเมือง สถาบัน และ จชต. รวมถึงการก่ออาชญากรรมทางเศรษฐกิจ มีแนวโน้มจะขยายตัว ส่วนปัญหาจากเทคโนโลยีไซเบอร์ที่ต้องจับตามอง ได้แก่ มัลแวร์เรียกค่าไถ่ (Ransomware) การลงทุนเพื่อเก็งกำไรในสินทรัพย์ดิจิทัล โดยเฉพาะสกุลเงินดิจิทัล (Cryptocurrency) และความเสี่ยงต่อ ความมั่นคงปลอดภัยของข้อมูล ทั้งนี้ เทคโนโลยีไซเบอร์เป็นสิ่งใหม่ ที่ภาครัฐไม่มีมาตรการกำกับดูแลมาก่อน การกำหนดแนวทางจัดการปัญหาตามบริบทของไทยเป็นสิ่งจำเป็นที่ต้องเร่งดำเนินการให้ทันกับสถานการณ์ พร้อมกับศึกษาแนวทางการจัดการกับอาชญากรรมทางไซเบอร์ของต่างประเทศ เนื่องจากจะมีผลต่อแนวทางการดำเนินการของไทย

ภัยคุกคามด้านไซเบอร์ในอนาคต

“สงครามไซเบอร์” หรือ Cyber Warfare หมายถึง การใช้เทคโนโลยีเพื่อโจมตีประเทศใดประเทศหนึ่ง รัฐบาลหรือแม้แต่ประชาชน ซึ่งก่อให้เกิดความเสียหายได้เทียบเคียงกับสงครามจริงที่มีการใช้อาวุธในการสู้รบ จนถึงปัจจุบันยังไม่เคยมีการเปิดเผยถึง **“สงครามไซเบอร์”** กับคู่กรณีอย่างตรงไปตรงมา มีเหตุการณ์หลายกรณีที่ เกิดการหยุดชะงักอย่างรุนแรงของโครงสร้างพื้นฐานของประเทศ ซึ่งถูกสงสัยว่าเป็นการดำเนินการโดยประเทศอื่นที่เป็นศัตรูกัน สำหรับคำอธิบายในพจนานุกรม Oxford English อธิบายเกี่ยวกับสงครามไซเบอร์ว่า **“การใช้เทคโน โลยีคอมพิวเตอร์เพื่อขัดขวางกิจกรรมของรัฐหรือองค์กร โดยเฉพาะอย่างยิ่งการโจมตีที่มีเจตนา เกี่ยวกับระบบ สารสนเทศเพื่อวัตถุประสงค์เชิงกลยุทธ์หรือการทหาร”** ดังนั้น ปัญหาเกี่ยวกับสงครามไซเบอร์นั้นยากมากในการที่จะหาว่าใครจะเป็นผู้โจมตีในตอนแรก ซึ่งในหลายๆ กรณี ยังไม่มีใครออกมาอ้างความรับผิดชอบเกี่ยวกับการโจมตี แต่เหตุการณ์ส่วนใหญ่มักเป็นที่น่าสงสัยว่าการโจมตีนั้น น่าจะมีหน่วยงานของรัฐเข้ามาเกี่ยวข้อง หรือเป็นการโจมตีประเภท “State-sponsored Attack” เป็นเพราะความเชื่อมโยงโดยตรงกับรัฐที่ฝ่ายตรงข้าม นั้นพิสูจน์ได้ยาก

สถานการณ์ความขัดแย้งรัสเซีย-ยูเครน เป็นสงครามที่สะท้อนรูปแบบสงครามในอนาคต ซึ่งการปฏิบัติการทางทหารรูปแบบปกติ (Kinetic Warfare) มีการใช้อาวุธทำลายล้างสูงที่มีเทคโนโลยีใหม่ เช่น อากาศยานไร้คนขับ หรือ ขีปนาวุธไฮเปอร์โซนิค โดยที่การปฏิบัติการทางสงครามไซเบอร์ ไม่ค่อยเป็นข่าวมากนัก แต่ในทางกลับกัน พบว่า การที่ประชาชนในประเทศคู่ขัดแย้งเกิดความเดือดร้อนเป็นวงกว้าง ทำให้ทำลายขวัญกำลังใจฝ่ายตรงข้าม อย่างมี



ประสิทธิภาพ เนื่องจากประชาชนพบกับปัญหาระบบไฟฟ้า-ประปาขัดข้อง บัญชีธนาคารต่างๆ ไม่สามารถทำธุรกรรมได้ การเดินทางสาธารณะมีปัญหาจากระบบตั๋วโดยสารขัดข้อง รวมทั้งการสร้างข่าวปลอม ข้อมูลเท็จ ที่มีปรากฏมากมายในสื่อสังคมออนไลน์ ซึ่งสร้างความสับสนโกลาหลในประเทศคู่ขัดแย้ง ซึ่งการโจมตีครั้งนี้ รัสเซียถูกมองว่าเป็นตัวการสำคัญ แต่ก็ไม่อาจปฏิเสธได้ว่าอาจมีการโจมตีจากชาติอื่นๆ เช่น เกาหลีเหนือ อิหร่าน หรือจีน ที่เป็นไปเพื่อการทดสอบอาวุธทางไซเบอร์ที่ตนครอบครองอยู่ ด้วยเหตุนี้ทำให้เห็นความเป็นไปได้ในการใช้สงครามไซเบอร์เป็นสงครามแห่งอนาคต

ปัจจุบันความตึงเครียดทางด้านภูมิศาสตร์กำลังทวีความรุนแรงมากขึ้นในด้านเทคโนโลยีและมิติไซเบอร์ (Cyber Space) พบว่าการโจมตีทางไซเบอร์มีความรุนแรงเพิ่มมากขึ้น สาเหตุมาจากการปรับเปลี่ยนรูปแบบการ ทำงานที่นำเทคโนโลยีสารสนเทศเข้ามามีส่วนช่วยขับเคลื่อนธุรกิจมากขึ้น โดยแนวโน้มสถานการณ์โลก การปฏิบัติการทางไซเบอร์ระหว่าง สหรัฐฯ รัสเซีย และจีน จะเพิ่มขึ้น ซึ่งสหรัฐฯ มองว่า กลุ่มแฮกเกอร์รัสเซีย เป็นภัยคุกคามที่สร้างผลกระทบต่อการเมืองสหรัฐฯ และสร้างความแตกแยกทางสังคม ส่วนจีน ถือเป็นภัยคุกคามในระยะยาวที่ อันตรายกว่า เนื่องจากอำนาจทางเศรษฐกิจของรัสเซียยังไม่สามารถเทียบเท่าจีน อีกทั้งการก่อการร้ายทางไซเบอร์ (Cyber Terrorism) มีแนวโน้มเพิ่มขึ้น กลุ่มแฮกเกอร์ที่ดำเนินการโดยรัฐและไม่ใช่รัฐมีขีดความสามารถและการพัฒนาเทคนิคต่างๆ ในการโจมตีทางไซเบอร์เพิ่มมากขึ้น ถือเป็นภัยคุกคามต่อความมั่นคงของโลกและเศรษฐกิจ ความเสียหายที่เพิ่มขึ้นทางมิติไซเบอร์อาจเป็นสิ่งกระตุ้นให้เกิดความขัดแย้งในโลกภายนอกได้

แนวโน้มการโจมตีทางไซเบอร์

มหาวิทยาลัย Surrey ของสหราชอาณาจักร เผยแพร่งานวิจัยที่มีชื่อว่า Nation States, Cyberconflict and the Web of Profit ซึ่งได้วิเคราะห์ว่าการโจมตีทางไซเบอร์ของรัฐมีความหลากหลายเปิดกว้าง และมีความถี่มากขึ้นอย่างมีนัยสำคัญ จนเข้าใกล้ระดับที่เรียกว่า **“Advanced Cyberconflict”** และงานวิจัยได้กำหนดระดับของความขัดแย้งทางไซเบอร์ระหว่างรัฐไว้ ๓ ระดับ ได้แก่

ระดับที่ ๑ : Cyber-Competition

หมายถึง ระดับที่รัฐใช้มิติทางไซเบอร์อย่างจริงจัง เพื่อทำให้ ได้เปรียบทางเศรษฐกิจ

ระดับที่ ๒ : Cyberconflict

หมายถึง ระดับที่รัฐมีวัตถุประสงค์เชิงกลยุทธ์ นอกเหนือจากความได้เปรียบทางเศรษฐกิจ กรอบข้อตกลงที่ร่วมกันไม่มีผลอีกต่อไป เป็นความขัดแย้งกันที่ตอบโต้กันอย่างไม่เปิดเผย อาทิ การโจมตีทางไซเบอร์ การจารกรรมข้อมูลคู่แข่ง เป็นต้น

ระดับที่ ๓ : Advanced Cyberconflict

หมายถึง ระดับที่รัฐต่างๆ เริ่มมีส่วนร่วมในการโจมตีและ ตอบโต้ทางไซเบอร์ เช่น การโจมตีทางไซเบอร์ที่มีเป้าหมายเพื่อบุกรุกเครือข่ายและทำให้สูญเสียความควบคุม และการโจมตีต่อทรัพย์สินทางกายภาพมากขึ้น อาทิ ระบบไฟฟ้า-ประปา เป็นต้น รวมถึงการใช้อาวุธยุทโธปกรณ์ปกติ (Conventional Weapon) เพื่อตอบโต้การโจมตีทางไซเบอร์

ประชาคมข่าวกรองสหรัฐฯ เผยแพร่รายงานการประเมินแนวโน้มสถานการณ์โลกว่า ใน ๒๐ ปีข้างหน้า ทั่วโลกจะต้องเผชิญหน้ากับการปฏิบัติการทางไซเบอร์เชิงรุก(Offensive Cyber Operation) และการเผยแพร่ ข่าวเท็จที่เพิ่มมากขึ้น ประเทศต่างๆ จะใช้ตัวแทน(Proxies) ในการปฏิบัติการทางไซเบอร์ อาทิ กลุ่มแฮกเกอร์ หรือ บริษัทที่ได้รับจ้างจากกองทัพ ซึ่งการดำเนินการดังกล่าวมาจากความผันผวนของสภาพความมั่นคงของโลกทำให้แต่ละประเทศมีการเผชิญหน้ากันมากขึ้น และโดยส่วนใหญ่การปฏิบัติการทางไซเบอร์เชิงรุกจะถูกนำมาใช้ก่อนการ ปฏิบัติการทางทหาร และมีเป้าหมายไปที่โครงสร้างพื้นฐานสำคัญในส่วนของพลเรือนและทหาร

วัตถุประสงค์ในการโจมตีทางไซเบอร์ พบว่ารัฐให้ความสำคัญกับการสอดแนมมากกว่าการจารกรรมข้อมูล เพื่อป้องกันการถูกตรวจพบและต้องการแทรกซึมอยู่ในระบบของเป้าหมายให้นานขึ้น ซึ่งข้อพิจารณาดังกล่าวได้มาจากข้อมูลเชิงสถิติที่ชี้ให้เห็นว่า ร้อยละ ๕๐ ใช้เพื่อการเฝ้าระวังทางไซเบอร์ ร้อยละ ๑๕ ใช้แทรกซึมเข้าสู่ระบบเครือข่ายและการระบุตำแหน่ง ร้อยละ ๑๔ ใช้สร้างความเสียหายและทำลาย ร้อยละ ๘ ใช้สำหรับการจารกรรมข้อมูล

ประเมินสถานการณ์ภัยคุกคามทางไซเบอร์ของประเทศไทย

ประเทศไทยเริ่มเผชิญเหตุโจมตีทางไซเบอร์ที่สร้างความเสียหายรุนแรงคล้ายคลึงกับในต่างประเทศ เนื่องจากโลกไซเบอร์ไร้พรมแดน ดังนั้น เหตุโจมตีทางไซเบอร์ที่เคยเกิดขึ้นในต่างประเทศจึงมีโอกาสเกิดขึ้นในไทยได้เช่นกัน เช่น กรณีการไฟฟ้าส่วนภูมิภาค (กฟภ.) ถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่ เมื่อ ๑๓ มิ.ย. ๖๓ ทำให้ระบบให้บริการของ กฟภ. ต้องปิดให้บริการหลายวัน และต้องร้องขอให้ศูนย์ไซเบอร์แห่งชาติเข้ามาให้ความช่วยเหลือ อีกทั้งแฮกเกอร์ที่โจมตียังได้นำข้อมูลภายใน กฟภ. ออกเผยแพร่เพื่อข่มขู่เรียกร้องเงินค่าไถ่ (ไม่มีการเปิดเผยข้อมูล) หรือกรณีโรงพยาบาลสระบุรี ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ เมื่อ ๖ ก.ย. ๖๓ ส่งผลกระทบต่อการบริการประชาชนและเสี่ยงต่อชีวิตคนไข้ ดังนั้น ระบบสารสนเทศของหน่วยงานภาครัฐ ส่วนใหญ่จึงมี ความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ ซึ่งอาจทำให้ข้อมูลสำคัญเกี่ยวกับ เศรษฐกิจ ความมั่นคง การทหาร รวมถึงข้อมูลส่วนบุคคลของประชาชน ซึ่งเก็บไว้โดยหน่วยงานภาครัฐมีความเสี่ยงที่จะรั่วไหล สร้างความเสียหาย ทั้งในแง่ของการหยุดให้บริการความเสียหายต่อโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ ต้นทุนการฟื้นฟูระบบ ทำให้เสียโอกาสในการสร้างนวัตกรรมใหม่เพื่อเพิ่มมูลค่าการให้บริการของระบบ โดยสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ได้ประมวลและวิเคราะห์ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่สำคัญ ได้แก่

๑. ภัยคุกคามทางไซเบอร์ที่เกิดจาก มัลแวร์เรียกค่าไถ่ หรือ "Ransomware"

ปัจจุบัน Ransomware เป็นรูปแบบการโจมตีทางไซเบอร์ที่ได้รับความนิยมสูงสุด เพราะมีค่าใช้จ่าย ในการลงทุนที่ต่ำ ทั้งยังมีโอกาสได้รับค่าตอบแทนสูงเมื่อเทียบกับการโจมตีรูปแบบอื่น การเกิดขึ้นของ **"บริการมัลแวร์เรียกค่าไถ่"** (ransomware-as-a-service) ยังเปิดโอกาสให้แฮกเกอร์มือใหม่สามารถเข้าถึงเครื่องมือชนิดนี้ได้ง่าย ทั้งนี้ ในช่วงสองปีที่ผ่านมา พบจำนวนและระดับความเสียหายจากการโจมตีด้วย Ransomware เพิ่มมากขึ้นเรื่อยๆ ทั้งยังมีแนวโน้มที่จะมุ่งเน้นการโจมตีไปยังโครงสร้างพื้นฐานของรัฐมากขึ้น เพราะหน่วยงานเหล่านี้มักยอมจ่ายค่าไถ่อย่างง่ายดาย ในบางกรณีอาจส่งผลถึงชีวิตของผู้คน และอาจนำไปสู่ สถานการณ์ในระดับวิกฤตได้ ปัจจุบันไทยเป็นหนึ่งในประเทศที่ตกเป็นเป้าหมายการโจมตีด้วยมัลแวร์เรียกค่าไถ่ โดยในปี ๒๕๖๔ มีรายงานองค์กรที่ถูกโจมตีจำนวน ๑๙ องค์กร (ในจำนวนนี้ เป็นการโจมตีโดย Lockbit Ransomware รวม ๑๐ องค์กร) ทั้งนี้ มีการประเมินว่า ระดับภัยคุกคามจากมัลแวร์เรียกค่าไถ่ในไทย อยู่ในระดับใกล้เคียงกับประเทศอาเซียนอื่นๆ เมื่อคำนึงถึงระดับพัฒนาการของเศรษฐกิจดิจิทัลที่ใกล้เคียงกันและภูมิทัศน์ด้านความมั่นคงในภูมิภาค

๒. ภัยคุกคามทางไซเบอร์ที่เกี่ยวกับความมั่นคงปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security)

เป็นภัยคุกคาม จากการต้องพึ่งพาเทคโนโลยีต่างชาติ ทำให้รัฐขาดศักยภาพในการบริหาร จัดการไซเบอร์ภายในประเทศด้วยตนเองและเสี่ยงได้รับผลกระทบจากช่องโหว่ที่ถูกพบในอุปกรณ์ หรือระบบสารสนเทศของต่างชาติ รวมถึงการถูกสอดแนมจากประเทศผู้ผลิตเทคโนโลยีเสียเอง ภัยคุกคามลักษณะนี้กำลังเป็นที่สนใจของต่างชาติ ไม่ว่าจะเป็น สหรัฐอเมริกา สหราชอาณาจักร ออสเตรเลีย และเกาหลีใต้ ซึ่งทุกประเทศเห็นความจำเป็นของการจัดตั้งมาตรฐานหรือระเบียบข้อบังคับต่าง ๆ เพื่อรับประกันว่า เทคโนโลยี เครื่องมือดิจิทัล และบริการจากผู้ค้าระหว่างประเทศมีความปลอดภัยที่จะนำมาใช้ภายในประเทศ รวมถึงการสร้างสมดุล ในการเลือกนำเข้าอุปกรณ์สารสนเทศมาใช้ภายในประเทศ ซึ่งไทยเป็นประเทศ ที่มีความเปราะบาง (vulnerable) ของห่วงโซ่อุปทานด้านเทคโนโลยีสูง เพราะไทยยังขาดการคิดค้นหรือประดิษฐ์เทคโนโลยีเพื่อใช้เอง (lack of home ground technology) มากนัก และต้องพึ่งพาเทคโนโลยีจากต่างชาติ (tech dependency) จำนวนมาก ไทยจึงมีความเสี่ยงที่จะถูกโจมตีผ่านเทคโนโลยีต่างชาติที่ไม่มีมาตรฐานความปลอดภัย

๓. สถานการณ์ความขัดแย้งรัสเซีย-ยูเครน

ในสถานการณ์ดังกล่าว พบการใช้เครื่องมือทางไซเบอร์ในการสนับสนุน ปฏิบัติการทางการทหารของทั้งสองฝ่ายในลักษณะ **“สงครามแบบผสม”** (hybrid warfare) ปรากฏการณ์ที่เกิดขึ้นสะท้อนให้เห็นถึงความสำคัญของพื้นที่ทางไซเบอร์ในฐานะพื้นที่ทางยุทธศาสตร์ด้านความมั่นคงแห่งชาติ และยังเป็นตัวแบบสำคัญในการจินตนาการถึงสงครามทางไซเบอร์ที่อาจเกิดขึ้นจริงในอนาคต สำหรับไทยแม้ว่าจะไม่ได้มีส่วนร่วมกับประเทศคู่ ขัดแย้งโดยตรง แต่ก็อาจได้รับผลกระทบในลักษณะของการโดนลูกหลง (spill-over) หากปฏิบัติการทางไซเบอร์ขยายวงกว้างมากขึ้น

บทที่ ๓

หลักการสำคัญ
ด้านการป้องกันประเทศ

บทที่ ๓ หลักการสำคัญด้านการป้องกันประเทศ

๑. รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ ได้บัญญัติหลักการสำคัญที่เกี่ยวข้องกับบทบาท ภารกิจ และหน้าที่ของกระทรวงกลาโหม ดังนี้

มาตรา ๑ ประเทศไทยเป็นราชอาณาจักรอันหนึ่งอันเดียวจะแบ่งแยกมิได้

มาตรา ๒ ประเทศไทยมีการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

มาตรา ๖ องค์พระมหากษัตริย์ทรงดำรงอยู่ในฐานะอันเป็นที่เคารพสักการะ ผู้ใดจะละเมิดมิได้ ผู้ใดจะกล่าวหาหรือฟ้องร้องพระมหากษัตริย์ในทางใดๆ มิได้

มาตรา ๘ พระมหากษัตริย์ทรงดำรงตำแหน่งจอมทัพไทย

มาตรา ๕๒ รัฐต้องพิทักษ์รักษาไว้ซึ่งสถาบันพระมหากษัตริย์ เอกราช อธิปไตย บูรณภาพแห่งอาณาเขตและเขตที่ประเทศไทยมีสิทธิอธิปไตย เกียรติภูมิและผลประโยชน์ของชาติ ความมั่นคงของรัฐ และความสงบเรียบร้อยของประชาชน เพื่อประโยชน์แห่งการนี้ รัฐต้องจัดให้มีการทหาร การทูต และการข่าวกรองที่มีประสิทธิภาพ กำลังทหารให้ใช้เพื่อประโยชน์ในการพัฒนาประเทศด้วย

๒. ยุทธศาสตร์ชาติด้านความมั่นคง

ยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๑ - ๒๕๘๐) เป็นแนวทางสำคัญที่รัฐบาลใช้เป็นเครื่องมือในการพัฒนาประเทศอย่างต่อเนื่องให้บรรลุวิสัยทัศน์ **“ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง”** เพื่อให้ประเทศมีขีดความสามารถในการแข่งขัน มีรายได้สูงอยู่ในกลุ่มประเทศพัฒนาแล้ว คนไทยมีความสุข อยู่ดี กินดี สังคมมีความมั่นคง เสมอภาคและเป็นธรรม โดยเน้นการพัฒนา ๖ ด้าน ได้แก่ ความมั่นคง การสร้างความสามารถในการแข่งขัน การพัฒนาและเสริมสร้างศักยภาพคน การสร้างโอกาสความเสมอภาคและเท่าเทียมกันทางสังคม การสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม และการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

พระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๐ มาตรา ๑๐ กำหนดว่าเมื่อมีพระบรมราชโองการประกาศใช้ยุทธศาสตร์ชาติแล้ว ให้คณะกรรมการจัดทำยุทธศาสตร์ชาติแต่ละด้านจัดทำแผนแม่บทเพื่อบรรลุเป้าหมายตามที่กำหนดไว้ในยุทธศาสตร์ชาติ ซึ่งคณะรัฐมนตรีได้พิจารณาให้ความเห็นชอบแผนแม่บทภายใต้ยุทธศาสตร์ชาติ จำนวน ๒๓ แผนแม่บท และได้ประกาศให้ใช้แผนแม่บทฯ ตั้งแต่ ๒๔ เมษายน ๒๕๖๒ และถือเป็นแผนระดับที่ ๒ ตามมติคณะรัฐมนตรีเมื่อ ๕ ธันวาคม ๒๕๖๐

"แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง"

ถือเป็นกรอบแนวทางการดำเนินการหลักที่จะนำไปสู่จุดหมายปลายทางในภาพรวมที่เป็นรูปธรรมชัดเจนในระยะ ๒๐ ปี ตามที่ยุทธศาสตร์ชาติด้านความมั่นคงได้กำหนดเอาไว้ซึ่งก็คือ **"ประเทศชาติมั่นคง ประชาชนมีความสุข"** โดยมีเป้าหมายสำคัญ ประกอบด้วย

๑. ประชาชนอยู่ดีกินดีและมีความสุข

๒. บ้านเมืองมีความมั่นคงในทุกมิติและทุกระดับ

๓. กองทัพ หน่วยงานด้านความมั่นคง ภาครัฐ ภาคเอกชน และภาคประชาชน มีความพร้อมในการป้องกันและแก้ไขปัญหาความมั่นคง

๔. ประเทศไทยมีบทบาทด้านความมั่นคงเป็นที่ชื่นชมและได้รับการยอมรับโดยประชาคมระหว่างประเทศ

๕. การบริหารจัดการความมั่นคงมีผลสำเร็จที่เป็นรูปธรรมอย่างมีประสิทธิภาพ เพื่อให้บรรลุเป้าหมายดังกล่าวข้างต้น โดยสาระสำคัญประกอบไปด้วยแผนย่อยจำนวนทั้งสิ้น ๕ แผนย่อย ได้แก่

๑) การรักษาความสงบภายในประเทศ
๒) การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง
๓) การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคง
๔) การบูรณาการความร่วมมือด้านความมั่นคงกับอาเซียนและนานาชาติ รวมทั้งองค์กรของชาติ ภาครัฐและมิใช่ภาครัฐ
๕) การพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม

๓. วัตถุประสงค์มูลฐานด้านความมั่นคงของประเทศ

จากรัฐธรรมนูญแห่งราชอาณาจักรไทย ผลประโยชน์แห่งชาติ และยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๑ - ๒๕๘๐) เมื่อวิเคราะห์เฉพาะด้านความมั่นคงของประเทศในส่วนที่เกี่ยวข้องกับกองทัพไทย สามารถกำหนดเป็นวัตถุประสงค์มูลฐานด้านความมั่นคงของประเทศได้ ดังนี้

๑) การอยู่ร่วมกันอย่างสันติสุข การมีเกียรติและศักดิ์ศรีของชาติ ในประชาคมระหว่างประเทศ

๒) สถาบันหลักของชาติและการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขดำรงอยู่อย่างมั่นคง

๓) สถานการณ์ภายในประเทศมีความสงบเรียบร้อย ประชาชนอยู่ร่วมกันได้อย่างสันติสุข

๔) ประเทศมีความมั่นคงปลอดภัยจากภัยคุกคามทางทหาร

๔. แผนปฏิบัติการด้านการพัฒนาศักยภาพของประเทศด้านความมั่นคงระยะที่ ๑ (พ.ศ.๒๕๖๓ - ๒๕๖๕) กระทรวงกลาโหม

เป็นกรอบในการบริหารจัดการงานด้านความมั่นคง ตามบทบาทอำนาจหน้าที่ของกระทรวงกลาโหมซึ่งได้ทบทวนให้มีความสอดคล้องกับยุทธศาสตร์ชาติ และสภาวะแวดล้อมด้านความมั่นคงที่เปลี่ยนแปลงไป โดยยังคงยึดถือแนวคิดทางยุทธศาสตร์ ๓ ประการ ประกอบด้วย

๑) การสร้างความร่วมมือด้านความมั่นคง (Security Cooperation)

หมายถึง การพิจารณาใช้ทรัพยากรทางทหารในการสนับสนุนรัฐบาลโดยสร้างความร่วมมือกับประเทศเพื่อนบ้าน มิตรประเทศ และประเทศมหาอำนาจต่างๆ ทั้งในระดับทวิภาคีและพหุภาคี เพื่อสร้างบรรยากาศความเป็นมิตร รักษาความเป็นกลาง ลดเงื่อนไขและลดโอกาสที่จะนำไปสู่ความขัดแย้ง รวมทั้งป้องกันมิให้ความขัดแย้งขยายขอบเขตออกไปนอกเหนือการควบคุม โดยยึดมั่นในหลักการแนวความคิดเชิงป้องกัน (Preventive) ซึ่งเป็นการแก้ปัญหาในเชิงรุกก่อนที่ความขัดแย้งจะเกิดขึ้น และหากความขัดแย้งเกิดขึ้นแล้วจะต้องสามารถควบคุมได้ทันเวลา โดยมาตรการดังกล่าวจะต้องอยู่บนพื้นฐานของความมีเกียรติและศักดิ์ศรีในเวทีการเมืองระหว่างประเทศ รวมทั้งผลประโยชน์ที่ประเทศพึงจะได้รับ

๒) การผนึกกำลังป้องกันประเทศ (United Defense)

หมายถึง การนำทรัพยากรที่เป็นพลังอำนาจของชาติทุกประเภท ในทุกมิติทั้งด้านการทหารการเมือง เศรษฐกิจ สังคมจิตวิทยา วิทยาศาสตร์และเทคโนโลยี มาบูรณาการอย่างมีระเบียบแบบแผนและเป็นระบบตั้งแต่ยามปกติ เพื่อแก้ไขข้อจำกัดของชาติ รวมทั้งชดเชยอำนาจกำลังรบของกองทัพที่มีอยู่อย่างจำกัด เพื่อให้สามารถปฏิบัติหน้าที่ในการป้องกันประเทศได้อย่างมีประสิทธิภาพ โดยจะต้องมีการเตรียมการและกระทำอย่างต่อเนื่องทั้งในยามปกติและยามสงคราม

๓) การป้องกันเชิงรุก (Active Defense)

หมายถึง การจัดเตรียมกำลัง เสริมสร้าง พัฒนา และบริหารจัดการทรัพยากรทางทหารทั้งมวลให้กองทัพสามารถพึ่งตนเองได้และมีความพร้อมในการใช้กำลังเพื่อการป้องปราม การแก้ไขและยุติความขัดแย้งโดยที่ฝ่ายเราเป็นฝ่ายได้เปรียบ โดยมุ่งเน้นมาตรการด้านการข่าวอย่างต่อเนื่องและเชิงลึกในทุกสถานการณ์มีระบบแจ้งเตือนและเฝ้าตรวจที่มีประสิทธิภาพ พร้อมรับสถานการณ์ทั้งในยามปกติและยามสงคราม สามารถปฏิบัติ การรบได้หนึ่งด้านและป้องกันอีกหนึ่งด้านในเวลาในเดียวกัน การปฏิบัติการทางทหารต้องใช้การปฏิบัติในลักษณะของการรบร่วมเป็นหลัก โดยยึดมั่นในหลักการ การมีกำลังรบเพื่อป้องกันตนเอง และมุ่งความพยายามให้พื้นที่การรบแตกหักอยู่บริเวณแนวชายแดน และใช้หน่วยที่มีคล่องแคล่วในการเคลื่อนที่ที่จัดเตรียมไว้เข้าคลี่คลายสถานการณ์ในขั้นต้น พร้อมขยายกำลังได้ตามสถานการณ์ที่เปลี่ยนแปลง

โดยแบ่งการดำเนินงาน ออกเป็น ๒ แนวทาง ได้แก่

แนวทางที่ ๑ การเสริมสร้างความสัมพันธ์ และความร่วมมือกับประเทศเพื่อนบ้าน มิตรประเทศ และองค์การนานาชาติ

แนวทางที่ ๒ การพัฒนาศักยภาพของประเทศด้านความมั่นคง ซึ่ง **“แผนพัฒนาการปฏิบัติการด้านไซเบอร์ กองทัพไทย”** สอดคล้องกับแนวทางที่ ๒ การพัฒนาศักยภาพของประเทศด้านความมั่นคง ใน**ประเด็นการปฏิบัติการทางทหารเพื่อรักษาอธิปไตยและผลประโยชน์แห่งชาติ** ด้วยการพัฒนาขีดความสามารถทางทหาร เพื่อการป้องปราม แก้ไข และยุติความขัดแย้งด้วยการปฏิบัติการร่วมเป็นหลัก ซึ่งมีกลยุทธ์ทั้งสิ้น ๘ กลยุทธ์ ได้แก่

๑ พัฒนาขีดความสามารถทางหทารด้วยการปฏิบัติการร่วม

๒ พัฒนาขีดความสามารถด้านไซเบอร์เพื่อความมั่นคง

๓ พัฒนาเทคโนโลยีอวกาศ

๔ พัฒนาระบบข่าวกรองเพื่อการแจ้งเตือนภัยคุกคามทางทหาร

๕ พัฒนาระบบควบคุมบังคับบัญชาและระบบสารสนเทศ

๖ พัฒนางานการกำลังสำรอง

๗ พัฒนาระบบการส่งกำลังบำรุงร่วม และ

๘ ส่งเสริมการวิจัยพัฒนาวิทยาศาสตร์และเทคโนโลยีป้องกันประเทศ

๕. อำนาจหน้าที่ของกระทรวงกลาโหม

พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.๒๕๔๕ มาตรา ๘ กำหนดให้กระทรวงกลาโหม มีอำนาจหน้าที่เกี่ยวกับการป้องกันและรักษาความมั่นคงของราชอาณาจักรจากภัยคุกคามทั้งภายนอกและภายในประเทศ การรักษาผลประโยชน์แห่งชาติ สนับสนุนการพัฒนาประเทศและราชการอื่นตามที่มีกฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกระทรวงกลาโหม หรือส่วนราชการที่สังกัดกระทรวงกลาโหม

นอกจากนี้ พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.๒๕๕๑ ได้กำหนดอำนาจ หน้าที่ของกระทรวงกลาโหม ดังนี้

---

๑) พิทักษ์รักษาเอกราชและความมั่นคงแห่งราชอาณาจักร จากภัยคุกคามทั้งภายนอกและภายในราชอาณาจักร ปราบปรามการกบฏและการจลาจล โดยจัดให้มีและใช้กำลังทหารตามที่รัฐธรรมนูญแห่งราชอาณาจักรไทยหรือตามที่มีกฎหมายกำหนด

---

๒) พิทักษ์รักษาปกป้องสถาบันพระมหากษัตริย์ตลอดจนสนับสนุนภารกิจของสถาบันพระมหากษัตริย์

---

๓) ปกป้องพิทักษ์รักษาผลประโยชน์แห่งชาติและการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข พัฒนาประเทศเพื่อความมั่นคงตลอดจนสนับสนุนภารกิจอื่นของรัฐในการพัฒนาประเทศการป้องกันและแก้ไขปัญหาจากภัยพิบัติและการช่วยเหลือประชาชน

---

๔) ศึกษาวิจัยพัฒนา และดำเนินการด้านอุตสาหกรรมป้องกันประเทศและพลังงานทหารด้านวิทยาศาสตร์และเทคโนโลยีป้องกันประเทศ และด้านกิจการอวกาศเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ เพื่อสนับสนุนภารกิจของกระทรวงกลาโหมและความมั่นคงของประเทศ

---

๕) ปฏิบัติการอื่นที่เป็นการปฏิบัติการทางทหารนอกเหนือจากสงครามเพื่อความมั่นคงแห่งราชอาณาจักรหรือปฏิบัติการอื่นใด ทั้งนี้ตามที่มีกฎหมายกำหนดหรือตามมติคณะรัฐมนตรี

---

๖. (ร่าง) แผนปฏิบัติการด้านการปกป้องอธิปไตยและผลประโยชน์ของชาติในภาพรวม ระยะที่ ๒ (พ.ศ. ๒๕๖๖ - ๒๕๗๐)

กองบัญชาการกองทัพไทย ได้จัดทำแผนปฏิบัติการด้านการปกป้องอธิปไตยและผลประโยชน์แห่งชาติ ในภาพรวม ยึดถือตามแนวทางการพัฒนาของแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง แผนย่อย การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง ส่วนที่ ๒ การปกป้องอธิปไตยและผลประโยชน์ของชาติ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.๒๕๖๖ - ๒๕๗๐) และแนวความคิดทางยุทธศาสตร์ของกระทรวงกลาโหม ๓ แนวความคิด ได้แก่ การสร้างความร่วมมือด้านความมั่นคง การผนึกกำลังป้องกันประเทศ และการป้องกันเชิงรุก ซึ่งจะสามารถตอบสนองเป้าหมายของแผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง ซึ่งระบุไว้ว่า “ปัญหาความมั่นคงที่มีอยู่ในปัจจุบันได้รับการแก้ไขจนไม่ส่งผลกระทบต่อการบริหารและพัฒนาประเทศ” โดยแผนปฏิบัติการฯ นี้ได้แบ่งออกเป็น ๗ ประเด็นการพัฒนา และแนวทางการพัฒนาทั้งสิ้นจำนวน ๒๒ แนวทางการพัฒนา ซึ่งเอกสารฉบับนี้ให้ความสำคัญกับประเด็นการพัฒนาที่สอดคล้องกับภัยคุกคามที่เกิดจากการปฏิบัติการด้านไซเบอร์ ได้แก่ ประเด็นการพัฒนาการเสริมสร้างขีดความสามารถด้านการปฏิบัติการร่วม การพัฒนาระบบการควบคุมบังคับบัญชา และการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ซึ่งประกอบด้วย ๔ แนวทางการพัฒนา ได้แก่ (๑) การพัฒนาและปรับปรุงระบบควบคุมบังคับบัญชา และการประสานสอดคล้องกับเหล่าทัพ และกลไกความร่วมมือกับหน่วยงานอื่นๆ ที่เกี่ยวข้องกับการป้องกันประเทศ (๒) การบูรณาการระบบงานข่าวกรองเชื่อมต่อแลกเปลี่ยนข้อมูลระหว่างเหล่าทัพและประชาคมข่าวกรอง (๓) การปรับปรุงระบบส่งกำลังบำรุงและการบริหารทรัพยากรร่วมกัน และ (๔) การพัฒนาและปรับปรุงระบบสื่อสาร เทคโนโลยีสารสนเทศ และไซเบอร์เพื่อการป้องกันประเทศ และ ประเด็นการพัฒนาแนวทางการใช้กำลังในการปฏิบัติภารกิจป้องกันประเทศ ซึ่งประกอบด้วย ๓ แนวทางการพัฒนา ได้แก่ (๑) การเฝ้าระวังและตรวจการณ์ทุกมิติอย่างมีประสิทธิภาพ (๒) การรักษาความมั่นคงและแก้ไขปัญหาสถานการณ์ตามแนวชายแดน และ (๓) การปฏิบัติการด้วยกำลังเฉพาะกิจทางบก ทางเรือ และตามลำน้ำ

ความสอดคล้องระหว่างแผนปฏิบัติการด้านการปกป้องอธิปไตยและผลประโยชน์ของชาติในภาพรวม ระยะที่ ๒ (๒๕๖๖ - ๒๕๗๐) กับแผน ๓ ระดับ ตามนัยของมติคณะรัฐมนตรี เมื่อวันที่ ๔ ธันวาคม ๒๕๖๐ ที่เกี่ยวข้องกับ "แผนพัฒนาการปฏิบัติการด้านไซเบอร์ กองทัพไทย" คือ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง ใน ๒ แผนย่อย ประกอบด้วย

๑. แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

โดยมีแนวคิดในการดำเนินการที่สำคัญ ได้แก่

๑	การจัดการกับภัยคุกคามด้านความมั่นคงในภาพรวม ด้วยแนวคิดเชิงป้องกันและป้องปราม
๒	การเฝ้าระวัง และตรวจการณ์ทุกมิติอย่างมีประสิทธิภาพ
๓	การแก้ไขปัญหาเขตแดนทั้งทางบก ทางทะเล และทางอากาศ กับประเทศเพื่อนบ้านอย่างสันติวิธี
๔	การสร้างความสัมพันธ์และความร่วมมือระหว่างกองทัพไทยกับกองทัพของประเทศเพื่อนบ้าน มิตรประเทศ และมหาอำนาจ
๕	การแสวงหาและใช้ประโยชน์จากความร่วมมือระหว่างประเทศในการรับมือกับภัยคุกคามความมั่นคงอย่างมีประสิทธิภาพ
๖	การบังคับใช้กฎหมายอย่างเคร่งครัดให้สอดคล้องกับกฎหมายและพันธกรณีระหว่างประเทศและ
๗	การรณรงค์ให้ความรู้ การศึกษา และการประชาสัมพันธ์กับประชาชนและผู้มีส่วนได้ส่วนเสีย รวมทั้งเปิดโอกาสให้เข้ามามีส่วนร่วมในการปกป้องและรักษาความมั่นคงและผลประโยชน์ของชาติ และ

๒. แผนย่อยการพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ

โดยมีแนวทางการดำเนินการที่สำคัญ ได้แก่

๑	การเตรียมกำลังและใช้กำลังเพื่อการป้องปราม แก้ไข และยุติความขัดแย้งด้วยการปฏิบัติการร่วมเป็นหลัก
๒	พัฒนาปฏิบัติการไซเบอร์เพื่อความมั่นคง และพัฒนาเทคโนโลยีอวกาศ เพื่อการใช้งานดาวเทียมสื่อสาร ดาวเทียมถ่ายภาพด้านความมั่นคง และการสังเกตการณ์ทางอวกาศด้วยความร่วมมือจากทุกภาคส่วนทั้งในประเทศและต่างประเทศ
๓	พัฒนาระบบข่าวกรองเพื่อการแจ้งเตือนภัยคุกคามทางทหาร โดยจัดให้มีระบบฐานข้อมูลข่าวกรองร่วม ด้วยความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง หน่วยงานภาครัฐ และหน่วยงานข่าวกรองต่างประเทศ และพัฒนาระบบข่าวกรองทางยุทธศาสตร์ทั้งในระดับนโยบาย ระดับอำนวยการข่าว และระดับปฏิบัติการข่าว
๔	พัฒนาเสริมสร้างกำลังประชาชน ทหารกองหนุน ทหารนอกประจำการ ทหารผ่านศึกทุกประเภท เพื่อมุ่งไปสู่การออมกำลังและชดเชยอำนาจกำลังรบของกองทัพที่มีอยู่อย่างจำกัดในยามสงคราม รวมทั้งการแจ้งเตือนด้านการข่าว ด้วยการเสริมสร้างจิตสำนึกในการมีส่วนร่วมป้องกันประเทศ รวมทั้งจัดทำฐานข้อมูลอย่างเป็นระบบ
๕	พัฒนาการผนึกกำลังและทรัพยากรจากทุกภาคส่วน เพื่อเตรียมพร้อมช่วยเหลือและบรรเทาผลกระทบจากภัยคุกคามทุกรูปแบบ
๖	พัฒนาเสริมสร้างความสัมพันธ์และความร่วมมือทางทหารกับประเทศเพื่อนบ้าน ประเทศสมาชิกอาเซียน มิตรประเทศประเทศมหาอำนาจ และองค์การระหว่างประเทศ
๗	ในยามสงบใช้กำลังกองทัพในการพัฒนาประเทศ และช่วยเหลือประชาชน (ตามที่กำหนดไว้ในรัฐธรรมนูญ)

อีกทั้ง (ร่าง) นโยบายและแผนระดับชาติว่าด้วย ความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๖ - ๒๕๗๐) ในนโยบายและแผนความมั่นคงที่ ๒ การปกป้องอธิปไตยและผลประโยชน์ของชาติ และการพัฒนาศักยภาพการป้องกันประเทศ ได้กำหนดเป้าหมายในการปกป้อง รักษา และแก้ไขปัญหาที่กระทบต่ออธิปไตยของชาติและผลประโยชน์แห่งชาติ รวมทั้งการพัฒนาขีดความสามารถเชิงยุทธศาสตร์ของกองทัพเพื่อการป้องกันประเทศในอนาคตไว้ ๒ เป้าหมาย โดยเป้าหมายที่ ๑ คือ การปกป้อง รักษา และแก้ไขปัญหาที่กระทบต่ออธิปไตยของชาติและผลประโยชน์ของชาติ มีตัวชี้วัดที่สำคัญได้แก่ ความพร้อมของกองทัพในการปฏิบัติการตามแผนป้องกันประเทศ ด้วยระบบปฏิบัติการร่วม โดยหน่วยทหารตามแผนป้องกันประเทศผ่านเกณฑ์มาตรฐานการฝึกร่วมกองทัพไทยภายในปี ๒๕๗๐ และ เป้าหมายที่ ๒ คือ การพัฒนาขีดความสามารถเชิงยุทธศาสตร์ของกองทัพเพื่อการป้องกันประเทศในอนาคต มีตัวชี้วัดที่สำคัญ ได้แก่ การพัฒนากองทัพไปสู่ความมทันสมัย ด้านการประยุกต์ใช้เทคโนโลยีดิจิทัลในการเชื่อมโยงระบบงานทั้งภายในและภายนอกกองทัพ ตลอดจนเสริมสร้างความพร้อมเพื่อให้สามารถรองรับการปฏิบัติการทางไซเบอร์และอวกาศได้ ภายในปี ๒๕๗๐

๗. อำนาจหน้าที่ของกองทัพไทย

พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. ๒๕๕๑ ได้กำหนดอำนาจหน้าที่ของกองทัพไทย ดังนี้

มาตรา ๑๕ กองทัพไทยมีหน้าที่เตรียมกำลังกองทัพไทย การป้องกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังทหารตามอำนาจหน้าที่ของกระทรวงกลาโหม มีผู้บัญชาการทหารสูงสุดเป็นผู้บังคับบัญชารับผิดชอบ

มาตรา ๑๖ กองทัพไทยอาจตั้งคณะกรรมการ คณะอนุกรรมการ หรือบุคคลใด เพื่อพิจารณาเรื่องใดๆ ที่เกี่ยวกับแผนเพื่อรักษาเอกราชและผลประโยชน์แห่งชาติ รวมทั้งการปฏิบัติการทางทหารของทุกส่วนราชการ ตามมาตรา ๑๗ ร่วมกันได้

มาตรา ๑๗ กองทัพไทยมีส่วนราชการ ได้แก่ กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ กองทัพอากาศ และส่วนราชการอื่นตามที่กำหนดโดยพระราชกฤษฎีกา

มาตรา ๑๘ กองบัญชาการกองทัพไทย มีหน้าที่ ควบคุม อำนวยการ สั่งการและกำกับดูแลการดำเนินงานของส่วนราชการในกองทัพไทยในการเตรียมกำลัง การป้องกันราชอาณาจักร และการดำเนินการเกี่ยวกับการใช้กำลังทหารตามอำนาจหน้าที่ของกระทรวงกลาโหมให้เกิดประสิทธิภาพสูงสุด มีผู้บัญชาการทหารสูงสุด เป็นผู้บังคับบัญชารับผิดชอบ

มาตรา ๑๙ กองทัพบก มีหน้าที่ เตรียมกำลังกองทัพบก การป้องกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังกองทัพบกตามอำนาจหน้าที่ของกระทรวงกลาโหม มีผู้บัญชาการทหารบก เป็นผู้บังคับบัญชารับผิดชอบ

มาตรา ๒๐ กองทัพเรือ มีหน้าที่ เตรียมกำลังกองทัพเรือ การป้องกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังกองทัพเรือตามอำนาจหน้าที่ของกระทรวงกลาโหม มีผู้บัญชาการทหารเรือ เป็นผู้บังคับบัญชารับผิดชอบ

มาตรา ๒๑ กองทัพอากาศ มีหน้าที่ เตรียมกำลังกองทัพอากาศ การป้องกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังกองทัพอากาศตามอำนาจหน้าที่ของกระทรวงกลาโหม มีผู้บัญชาการทหารอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

มาตรา ๒๙ โครงสร้างองค์กรการฝึกและการศึกษาของทหารและข้าราชการพลเรือนกลาโหม ให้เป็นไปตามนโยบายที่กระทรวงกลาโหมกำหนด โดยให้กองบัญชาการกองทัพไทยรับผิดชอบการฝึก และศึกษาในระดับยุทธศาสตร์ การปฏิบัติการร่วมของกองทัพไทยและการปฏิบัติการของกองบัญชาการกองทัพไทย และให้กองทัพบก กองทัพเรือ และกองทัพอากาศ รับผิดชอบในระดับปฏิบัติการและระดับยุทธวิธี

มาตรา ๓๑ ให้กองบัญชาการกองทัพไทย รับผิดชอบ การวางแผนพัฒนาและดำเนินการเกี่ยวกับระบบควบคุมบังคับบัญชากองทัพไทย ให้สามารถติดต่อเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่าง ๆ ทั้งในระดับรัฐบาล ระดับกระทรวง และหน่วยงานในกระทรวงกลาโหม ตลอดจนการแบ่งมอบความรับผิดชอบในการดำเนินการให้กับกองทัพและส่วนราชการที่เกี่ยวข้อง

มาตรา ๓๙ ให้กองทัพไทย จัดตั้งศูนย์บัญชาการทางทหาร ในแต่ละระดับขึ้น ตั้งแต่ยามปกติ เพื่อใช้ในการติดตามสถานการณ์ และเป็นศูนย์ควบคุม อำนวยการ และสั่งการการปฏิบัติ ให้ศูนย์บัญชาการทางทหารในกองบัญชาการกองทัพไทย มีหน้าที่ควบคุม อำนวยการและสั่งการศูนย์บัญชาการทางทหารในแต่ละระดับตามวรรคหนึ่งหรือกองกำลังเฉพาะกิจร่วมที่จัดตั้งขึ้นตามแผนป้องกันประเทศ แล้วแต่กรณี

๘. แผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคงกระทรวงกลาโหม พ.ศ.๒๕๖๖ - ๒๕๗๐

๑) วัตถุประสงค์

(๑) เพื่อเสริมสร้างความแข็งแกร่งในการรักษาความปลอดภัยทางไซเบอร์จากทั้งภัยภายในประเทศและภัยภายนอกประเทศ และสร้างความเชื่อมั่นการใช้เทคโนโลยีดิจิทัลให้มีประสิทธิภาพเหมาะสมกับการปฏิบัติภารกิจ การจัดการปัจจัยแวดล้อมที่เอื้ออำนวยต่อการใช้ไซเบอร์อย่างได้เปรียบ ไม่ให้เป็นจุดอ่อนหรือจุดล่อแหลมต่อการปฏิบัติภารกิจ มีเอกภาพในการเตรียมและใช้ศักยภาพด้านไซเบอร์โดยรวม การควบคุมแยกการปฏิบัติ

(๒) เพื่อป้องปรามภัยคุกคามทางไซเบอร์ที่จะกระทำต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกระทรวงกลาโหม

(๓) เพื่อยกระดับขีดความสามารถและทักษะด้านไซเบอร์ให้กับบุคลากรของกระทรวงกลาโหม และส่งเสริมการเผยแพร่ความรู้ให้แก่กำลังพลของกระทรวงให้สามารถใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้ในทุกระดับ อย่างเหมาะสมเพียงพอ ทั้งเชิงคุณภาพ และเชิงปริมาณ

(๔) เพื่อการบูรณาการและยกระดับประสิทธิภาพ การสร้างความร่วมมือสนับสนุนการ

ใช้ศักยภาพ ไซเบอร์ระดับชาติมีความพร้อมเป็นหน่วยงานนำในการจัดการภัยคุกคามทางไซเบอร์ระดับชาติ เมื่อได้รับมอบหมายจากรัฐบาลและเมื่อถึงเงื่อนไขที่กำหนด แสวงประโยชน์จากความร่วมมือระดับนานาชาติ และรักษาสมดุลของความสัมพันธ์ได้อย่างบังเกิดผลเป็นรูปธรรม

(๕) เพื่อเตรียมความพร้อมตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการปกป้องระบบคอมพิวเตอร์และโครงข่ายเพื่อให้สามารถให้บริการได้เป็นปกติและหน่วยงานสามารถรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

๒) แนวทางการดำเนินการ/พัฒนา

(๑) การพัฒนาศักยภาพไซเบอร์ มีกรอบการดำเนินงาน ดังนี้

- การยกระดับความพร้อมหรือขีดความสามารถของหน่วยตามมาตรฐานสากล
- การพัฒนาหลักนิยมทางไซเบอร์
- การสนับสนุนบุคลากรที่ปฏิบัติการทางด้านไซเบอร์ให้มีความรู้ความสามารถที่สูงขึ้น
- การสนับสนุนการพัฒนาเครื่องมือและอุปกรณ์ในการปฏิบัติการทางไซเบอร์

(๒) การปฏิบัติการไซเบอร์ของกระทรวงกลาโหม มีกรอบการดำเนินงาน ดังนี้

- การดำเนินการในกรอบของกฎหมายของกระทรวงกลาโหม
- การข่าวกรองในมิติไซเบอร์เพื่อสนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหม
- การตอบสนองต่อสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยไซเบอร์

(๓) ความร่วมมือด้านความมั่นคงไซเบอร์ มีกรอบการดำเนินงาน ดังนี้

- ระดับนโยบาย ได้แก่ การดำเนินการความร่วมมือด้านการป้องกันไซเบอร์กับต่างประเทศ โดยการกำหนดเป้าหมายและจัดลำดับความเป็นไปได้ในการใช้ความสัมพันธ์ให้เกิดประโยชน์ ประกอบด้วย ความร่วมมือด้านไซเบอร์ในกรอบการประชุมรัฐมนตรีกลาโหมอาเซียน การแสวงความร่วมมือด้านไซเบอร์กับกระทรวงกลาโหมมิตรประเทศ และความร่วมมือด้านไซเบอร์กับหน่วยงานที่เกี่ยวข้องกับกระทรวงกลาโหม ซึ่งต้องมีงบประมาณสนับสนุนเพียงพอสำหรับการดำรงรักษาและพัฒนาความสัมพันธ์ ซึ่งมีส่วนสำคัญต่อการรักษาภาพลักษณ์อันน่าเชื่อถือ และศักยภาพด้านไซเบอร์ของกระทรวงกลาโหม รวมทั้งต้องมีการรักษาความลับอย่างเข้มงวดเมื่อต้องมีการแลกเปลี่ยนข้อมูลข่าวสารหรือ

- ระดับปฏิบัติ ได้แก่ การฝึก/แข่งขันในระดับกองบัญชาการกองทัพไทย เหล่าทัพกับมิตรประเทศ รวมถึงกิจกรรมการประชุม และความร่วมมือในประเทศกับหน่วยงานความมั่นคงปลอดภัยไซเบอร์และหน่วยงานโครงสร้างพื้นฐานเพื่อการบูรณาการรักษาความปลอดภัยไซเบอร์และการฝึกการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ

๙. กฎหมาย ข้อบังคับ และนโยบายด้านไซเบอร์ที่สำคัญ

๑) กฎหมาย

(๑) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๒) พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒) ข้อบังคับที่เกี่ยวข้อง

(๑) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้งหน้าที่และอำนาจของ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔

(๒) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะ หน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการ ควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔

(๓) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

(๔) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

(๕) ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔

๓) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์

(๒) (ร่าง) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ - ๒๕๗๐

(๓) (ร่าง) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ - ๒๕๗๐

(๔) (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑๐. นโยบายเร่งด่วนด้านการป้องกันประเทศของผู้บัญชาการทหารสูงสุด (๑ ต.ค. ๖๔)

๑) นโยบายทั่วไป

(๑) มีขีดความสามารถและความพร้อมในการป้องกันประเทศและรักษาผลประโยชน์ของชาติทั้งมิติทางบก มิติทางน้ำ มิติทางอากาศ มิติทางอวกาศ และมิติทางไซเบอร์

(๒) ปฏิบัติการร่วมภายใต้การอำนวยการของ บก.ทท. โดยมุ่งไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง และนำระบบฐานข้อมูลร่วมมาใช้ประโยชน์ รวมทั้งผนึกกำลังร่วมกับหน่วยงานทุกภาคส่วนอย่างเป็นปึกแผ่นในการสนับสนุนการปฏิบัติภารกิจทางทหาร

(๓) พัฒนาเสริมสร้างกองทัพให้เข้มแข็ง และทันสมัย มีความคล่องแคล่วและอำนาจกำลังรบสูง ดำรงความริเริ่มในการนำขีดความสามารถทางเทคโนโลยีสมัยใหม่มาเพิ่มศักยภาพในการปฏิบัติงานของกองทัพ เพื่อให้สอดคล้องกับการรักษาสมดุลของพลังอำนาจทางทหารในภูมิภาค

๒) นโยบายเฉพาะ

(๑) จัดและวางกำลังในการป้องกันชายแดนตามระดับภัยคุกคาม ให้สอดคล้องกับการบริหารจัดการชายแดนทั้งทางบกและทางทะเล การจัดตั้งเขตพัฒนาเศรษฐกิจพิเศษ การพัฒนาการค้าชายแดน การใช้ประโยชน์พื้นที่ที่มีปัญหาร่วมกับประเทศเพื่อนบ้าน และการรักษาผลประโยชน์ของชาติทางทะเล

(๒) สนับสนุนการพัฒนาขีดความสามารถของศูนย์บัญชาการทางทหารเพื่อเพิ่มประสิทธิภาพในการบูรณาการข้อมูลที่จำเป็นในการวางแผน และการอำนวยการปฏิบัติการร่วมกับ ศปก. เหล่าทัพ และส่วนราชการที่เกี่ยวข้องทั้งข้อมูลในเครือข่ายที่มีชั้นความลับ (C4I) และเครือข่ายสำหรับการบริหารงาน (MIS)

(๓) พัฒนาและบูรณาการระบบงานข่าวกรองของกองทัพไทยให้มีประสิทธิภาพ โดยมุ่งเน้นระบบฐานข้อมูลร่วมด้านการข่าวของกองทัพไทย

(๔) ปลูกฝังจิตสำนึกการเป็นเจ้าหน้าที่รวบรวมข่าวสารให้กับกำลังพลทุกนาย เพื่อรายงานข่าวที่มีผลกระทบต่อความมั่นคงได้รวดเร็ว ถูกต้อง ทันเวลา รวมทั้งพัฒนาขีดความสามารถของนักวิเคราะห์ข่าว ให้สามารถแจ้งเตือนแนวโน้มภัยคุกคามได้อย่างมีประสิทธิภาพ มีความถูกต้อง แม่นยำ

(๕) บูรณาการการฝึกของกองทัพไทยทุกระดับ ให้สอดคล้องกับการเตรียมกำลังและใช้กำลังตามแผนป้องกันประเทศ และนำการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางมาใช้ในการฝึก รวมทั้งปรับแผนและรูปแบบการฝึกให้สอดคล้องกับฐานวิถีชีวิตใหม่ ทั้งการฝึกกับมิตรประเทศ และการฝึกภายในของกองทัพไทย

(๖) สนับสนุนการขยายเครือข่ายการติดต่อสื่อสาร ระบบควบคุมบังคับบัญชา C4I และสนับสนุนการปฏิบัติภารกิจของตำรวจตระเวนชายแดน เพื่อให้สามารถปฏิบัติการร่วมกับกองทัพไทยได้อย่างมีประสิทธิภาพ

(๗) พัฒนาขีดความสามารถเทคโนโลยีทางการทหาร การส่งเสริมการวิจัยและพัฒนาทางทหาร เพื่อนำไปสู่การพึ่งพาตนเองที่ตอบสนองต่อการเตรียมกำลังรบ และขยายผลเพื่อการพาณิชย์

(๘) พัฒนาขีดความสามารถด้านไซเบอร์ของกองทัพไทย ทั้งในด้านกำลังพล เครื่องมือ องค์ความรู้ และระบบบริหารจัดการ รวมทั้งบูรณาการความร่วมมือกับทุกภาคส่วนทั้งภายในและต่างประเทศให้สอดคล้องกับการปฏิบัติการทางทหารในมิติอื่นๆ ได้อย่างมีประสิทธิภาพ

(๙) บูรณาการการพัฒนาขีดความสามารถและการใช้ประโยชน์กิจการอวกาศ ทั้งดาวเทียมสื่อสารดาวเทียมถ่ายภาพ และการเฝ้าระวังทางอวกาศ เพื่อสนับสนุนภารกิจด้านความมั่นคงของ บก.ทท. และเหล่าทัพให้เกิดประสิทธิภาพสูงสุด

(๑๐) ดำรงความต่อเนื่องการบูรณาการการใช้แผนที่กลางของกองทัพไทย เพื่อสนับสนุนการปฏิบัติการร่วมของกองทัพไทยภายใต้การอำนวยการยุทธ์ร่วมของ บก.ทท.

(๑๑) บูรณาการการพัฒนาขีดความสามารถและการใช้งานยุทโธปกรณ์ที่มีใช้ร่วมกันทุกเหล่าทัพ เพื่อสนับสนุนภารกิจการป้องกันประเทศ โดยการจัดทำ/พัฒนาหลักนิยมร่วม การวิจัย/พัฒนา ตลอดจนพัฒนาขีดความสามารถของกำลังพลเพื่อรองรับเทคโนโลยีที่ทันสมัย อาทิ อากาศยานไร้คนขับ (โดรน) ปัญญาประดิษฐ์ (AI) ระบบตรวจจับ (Sensor) ขีดความสามารถด้านไซเบอร์ ขีดความสามารถด้านสงครามอิเล็กทรอนิกส์ เป็นต้น

(๑๒) การจัดหายุทโธปกรณ์ใหม่ให้กระทำเท่าที่จำเป็น มุ่งเน้นการซ่อมแซมยุทโธปกรณ์ที่มีอยู่ให้มีสภาพพร้อมใช้งาน โดยยึดหลักความสอดคล้องกับสถานการณ์ ความสมดุลพลังอำนาจทางทหาร และ ขีดความสามารถด้านงบประมาณของประเทศ

(๑๓) พัฒนาระบบงานส่งกำลังบำรุงร่วมให้มีความพร้อมและใช้ประโยชน์จากงานมาตรฐานยุทโธปกรณ์ทางทหาร ได้แก่ ระบบวงรอบการส่งกำลัง ระบบจัดทำบัญชีความต้องการทางทหารด้านการระดมสรรพกำลัง และระบบรายงานสถานภาพความพร้อมรบด้านการส่งกำลังบำรุง

(๑๔) ขยายความร่วมมือกับมิตรประเทศด้านการสนับสนุนยุทธปัจจัย ในภาวะวิกฤติระหว่างกัน

(๑๕) ให้มีความพร้อมของกิจการกำลังพลสำรองทางด้านบัญชีการบรรจุ การระดมพล รวมถึงความพร้อมในการระดมสรรพกำลังเพื่อการทหาร

(๑๖) สร้างเครือข่ายภาครัฐ ภาคเอกชน และภาคประชาชน เพื่อให้การสนับสนุนการปฏิบัติภารกิจของกองทัพด้านการป้องกันประเทศ และภารกิจเพื่อความมั่นคง

บทที่ ๔

แนวทางการพัฒนาการปฏิบัติการด้านไซเบอร์ของกองทัพไทย

บทที่ ๔ แนวทางการพัฒนาการปฏิบัติการด้านไซเบอร์ของกองทัพไทย

ความท้าทายของกองทัพไทย

ปัจจุบันสภาวะแวดล้อมของโลกมีการเปลี่ยนแปลงและมีการพัฒนาการของเทคโนโลยีและนวัตกรรมอย่างรวดเร็ว ควบคู่กับการเกิดเหตุการณ์การแพร่ระบาดของเชื้อไวรัสโคโรน่า (COVID-19) ที่ส่งผลกระทบต่อการใช้ชีวิตประจำวันของประชาชนทั่วโลกซึ่งทำให้เกิดพฤติกรรมการใช้งานระบบอินเตอร์เนตเพิ่มสูงขึ้น จากสถานการณ์ดังกล่าวทำให้เกิดพัฒนาการของภัยคุกคามโดยผสมผสานระหว่างภัยคุกคามแบบดั้งเดิมและรูปแบบใหม่กลายเป็นภัยคุกคามแบบผสมผสาน (Hybrid Threat) ที่กำลังพัฒนาการไปสู่การทำสงครามที่รัฐหรือตัวแสดงที่ไม่ใช่รัฐจะใช้เครื่องมือทุกรูปแบบในการทำสงคราม (Surrogate Warfare) ซึ่งสงครามที่เกิดขึ้นนั้นทุกประเทศจะมีความเชื่อมโยงกันแต่ได้รับความเสียหายแตกต่างกันขึ้นอยู่การเตรียมพร้อมรองรับสถานการณ์ของแต่ละประเทศ

แผนภาพที่ ๔-๑ แสดงมิติของภัยคุกคามในอนาคต

จากการเปลี่ยนแปลงของสภาพแวดล้อมในข้างต้นผู้บัญชาการทหารสูงสุด กองทัพไทยได้เล็งเห็นถึงความสำคัญของปัญหาจึงได้กำหนดนโยบายเร่งด่วน โดยมีประเด็นที่สำคัญต่อการป้องกันประเทศที่ต้องเร่งรัดในการดำเนินการ คือ การพัฒนาระบบควบคุมบังคับบัญชาไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางและนำระบบฐานข้อมูลร่วมมาใช้ประโยชน์ และพัฒนาการระบบปฏิบัติการร่วมไปสู่การผนึกกำลังร่วมกับหน่วยงานทุกภาคส่วนอย่างบูรณาการ รวมทั้งพัฒนาการปฏิบัติการด้านไซเบอร์ทั้งในด้านกำลังพล เครื่องมือ องค์ความรู้ และระบบบริหารจัดการ รวมทั้งบูรณาการความร่วมมือกับทุกภาคส่วนทั้งภายในและต่างประเทศให้สอดคล้องกับการปฏิบัติการทางทหารในมิติอื่นๆ ได้อย่างมีประสิทธิภาพ

แนวความคิดในการพัฒนากองทัพเพื่อความมั่นคงด้านไซเบอร์ (Cyber Security) กองทัพไทย

ประมาณการภัยคุกคามด้านไซเบอร์ในอนาคต

ข้อมูลจาก Global Trend 2040 ซึ่งจัดทำโดย The National Intelligence Council สหรัฐฯ เผยแพร่เมื่อ มี.ค. ๖๔ ชี้ว่า ทั่วโลกจะต้องเผชิญหน้ากับการปฏิบัติการทางไซเบอร์เชิงรุก (Offensive Cyber Operation) ต้องเผชิญกับการเผยแพร่ข่าวเท็จเพิ่มมากขึ้น และการปฏิบัติการไซเบอร์เชิงรุกจะถูกนำมาใช้ก่อนการปฏิบัติการทางทหารโดยมีเป้าหมายที่ระบบโครงสร้างพื้นฐานที่สำคัญทั้งในส่วนของพลเรือนและทหาร รวมทั้งประเทศต่างๆ จะใช้ตัวแทน (Proxies) ในการปฏิบัติการทางไซเบอร์ เช่น กลุ่มแฮกเกอร์ หรือบริษัทที่ได้รับการว่าจ้างจากกองทัพเพิ่มมากขึ้นตามลำดับ และข้อมูลจาก International Strategic Analysis, The Ten Leading Geopolitical Risk in 2021 ชี้ว่าภัยคุกคามจากการก่อการร้ายทางไซเบอร์จะเพิ่มขึ้นอย่างต่อเนื่อง โดยกลุ่มแฮกเกอร์ที่ดำเนินการโดยรัฐและไม่ใช่รัฐมีขีดความสามารถและการพัฒนาเทคนิคต่างๆ ในการโจมตีทางไซเบอร์เพิ่มมากขึ้น สำหรับความเสียหายที่เพิ่มขึ้นจากการโจมตีทางไซเบอร์อาจเป็นสิ่งที่กระตุ้นให้เกิดความขัดแย้งภายนอก

แผนพัฒนาขีดความสามารถด้านไซเบอร์กองบัญชาการกองทัพไทย

จากสภาวะแวดล้อมของโลกที่กำลังเปลี่ยนแปลงไปอย่างรวดเร็วในยุคปัจจุบัน กองบัญชาการกองทัพไทย ต้องมีระบบควบคุมบังคับบัญชาที่ทันสมัย เพื่อก่อให้เกิดความพยายามร่วม (Joint Effort) ของเหล่าทัพ ในลักษณะของการอำนวยการและการบริหารทรัพยากร (Conduct and Management) ในการปฏิบัติการร่วมมากกว่าการบังคับบัญชาเพื่อให้เกิดความรวดเร็วในการวางแผน การปฏิบัติตามขั้นตอน และการปฏิบัติตามจังหวะการรบในทางยุทธวิธี ให้เป็นไปตามเจตนารมณ์ของผู้บัญชาการร่วม มีความคิดริเริ่มและเสรีในการปฏิบัติเพื่อป้องกันและตอบโต้ภัยคุกคามที่สำคัญในอนาคตคือ การปฏิบัติการด้านไซเบอร์ ซึ่งเกิดจากความก้าวหน้าทางเทคโนโลยีที่ทันสมัยรวดเร็ว ส่งผลให้พฤติกรรมการใช้ชีวิตของคนเกิดการเปลี่ยนแปลงโดยพึ่งพาเทคโนโลยีเพิ่มมากขึ้น ทั้งในด้านการเมืองการปกครอง เศรษฐกิจ และสังคมจิตวิทยา รวมทั้งการทหาร ทำให้เกิดพื้นที่ต่อสู้และแย่งชิงผลประโยชน์ ในขอบเขตของไซเบอร์ (Cyber Domain) เพิ่มขึ้น

ดังนั้นแนวทางการใช้กำลังของกองทัพไทยในอนาคต ต้องสามารถรองรับบทบาททางทหารทั้งเพื่อการรบและบทบาทที่มิใช่การรบ โดยบูรณาการและพัฒนาการปฏิบัติการร่วมในลักษณะการปฏิบัติการหลายมิติ (Multi Domains Operations : MDO) ให้มีประสิทธิภาพและปรับปรุงระบบควบคุมบังคับบัญชาการไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง(Network Centric Operation : NCO) สามารถสั่งการทรัพยากรทางทหารเพื่อตอบสนองภารกิจด้านความมั่นคงได้ทุกรูปแบบทุกสภาวะทั้งภารกิจของกองทัพและภารกิจที่ต้องสนับสนุนอื่นๆ ที่เกี่ยวข้อง สามารถทำงานร่วมกับภาคส่วนต่างๆ ทั้งส่วนราชการพลเรือน ภาคเอกชน รวมถึงภาคประชาชน โดยเฉพาะการมีส่วนร่วมในการแก้ปัญหาภัยคุกคามรูปแบบใหม่

กรอบแนวคิดในการพัฒนาการปฏิบัติการด้านไซเบอร์ ของศูนย์บัญชาการทางทหาร (ศบท.)

เพื่อทำให้กรอบในการปฏิบัติการด้านไซเบอร์มีความชัดเจนและมีทิศทางในการพัฒนา ซึ่งจะทำให้เหล่าทัพต่างๆ สามารถนำไปวางแผนและกำหนดรูปแบบการปฏิบัติการได้อย่างมีประสิทธิภาพและนำไปสู่การปฏิบัติการร่วมที่ใช้เครือข่ายเป็นศูนย์กลาง(Network Centric Operation : NCO) รวมทั้งพัฒนาจนสามารถปฏิบัติการหลายมิติได้(Multi Domains Operation : MDO) เพื่อตอบสนองการปฏิบัติการตามแผนป้องกันประเทศได้อย่างมีประสิทธิภาพตั้งแต่ยามปกติ ทำให้เกิดความท้าทายต่อกองทัพไทย ที่ต้องเตรียมความพร้อมในการใช้กำลังตั้งแต่ยามปกติ เพื่อป้องกัน ป้องปราม และตอบโต้ภัยคุกคามที่เกิดจากรัฐหรือตัวแสดงที่ไม่ใช่รัฐจะใช้ความเจริญก้าวหน้าทางเทคโนโลยีที่รวดเร็วในการแย่งชิงและแข่งขันเพื่อผลประโยชน์ของชาติตน ก่อให้เกิดเป็นความซับซ้อนของปัญหา จนอาจนำไปสู่การใช้เครื่องมือทุกรูปแบบในการทำสงคราม ซึ่งเหตุการณ์ดังกล่าวย่อมส่งผลกระทบต่อความมั่นคงของชาติในหลายมิติ โดยมีจุดเริ่มต้นในการดำเนินการตั้งแต่ยามปกติและสามารถก้าวเข้าสู่สภาวะทางสงครามอย่างรวดเร็ว ทำให้ผู้บัญชาการทหารสูงสุดได้กำหนดนโยบายเร่งด่วนที่สำคัญต่อการป้องกันประเทศ ได้แก่ การพัฒนาระบบควบคุมบังคับบัญชา การพัฒนาระบบปฏิบัติการร่วม และการพัฒนาการปฏิบัติการด้านไซเบอร์ เพื่อให้เกิดความพร้อมสำหรับรองรับภัยคุกคามตามที่กล่าวมาข้างต้น

แผนภาพที่ ๔-๒ แสดงกรอบแนวคิดความท้าทายของกองทัพไทย

ดังนั้นจึงได้กำหนด**ผลลัพธ์ที่ต้องการ (Ends)** สำหรับการพัฒนาด้านไซเบอร์ของศูนย์บัญชาการกองทัพไทย (ทท.) เป็นลักษณะของขอบเขตการปฏิบัติการด้านไซเบอร์ โดยแบ่งออกเป็น ๓ ขอบเขต ดังนี้

ขอบเขตที่ ๑ : ศูนย์บัญชาการทางทหาร (ศบท.) และเหล่าทัพ (ทบ., ทร., ทอ.) มีขีดความสามารถในการป้องกันและป้องปรามการปฏิบัติการด้านไซเบอร์ภายในกองบัญชาการและหน่วยขึ้นตรงได้อย่างมีประสิทธิภาพ

ขอบเขตที่ ๒ : ศูนย์บัญชาการทางทหาร (ศบท.) และเหล่าทัพ (ทบ., ทร., ทอ.) มีขีดความสามารถในการสนับสนุนการป้องปรามและตอบโต้ภัยคุกคามทางไซเบอร์ ในลักษณะการปฏิบัติการหลายมิติ (Multi Domains Operations) รวมทั้งสามารถพิจารณาใช้เครื่องมือ Soft Power และ Hard Power ในการตอบโต้ได้อย่างเหมาะสมกับระดับต่างๆ ของภัยคุกคามที่เกิดขึ้น

ขอบเขตที่ ๓ : กองทัพไทยมีขีดความสามารถในการสนับสนุนการป้องปรามและตอบโต้ภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติร่วมกับภาคส่วนต่างๆ ได้อย่างมีประสิทธิภาพ

สำหรับแนวความคิดในการดำเนินการ (Concept of Operations : CONOPS) นักศึกษาทั้ง ๔ สถาบัน ได้ทำการศึกษาและทบทวนแล้ว พบว่า ความท้าทายของ กองบัญชาการกองทัพไทย และเหล่าทัพ มาจากภัยคุกคามในอนาคตที่มีความซับซ้อนมากขึ้น ซึ่งผู้บัญชาการทหารสูงสุดได้มอบนโยบายเพื่อพัฒนากองทัพ สำหรับเตรียมความพร้อมในการรองรับสถานการณ์ดังกล่าว โดยนโยบายที่สำคัญด้านป้องกันประเทศ คือ การพัฒนาระบบควบคุมบังคับบัญชา การพัฒนาระบบปฏิบัติการร่วม และการพัฒนาการปฏิบัติการซึ่งจากการศึกษาพบว่าข้อจำกัดในปัจจุบันของกองทัพในภาพรวม คือ ทุกส่วนมีการพัฒนาการปฏิบัติการทางไซเบอร์ของตนเองมาตามลำดับแล้ว แต่ยังขาดการบูรณาการ และระบบการควบคุมบังคับบัญชา เพื่อสร้างเอกภาพในการบังคับบัญชาและความประสานสอดคล้องระหว่างกองทัพกับภาคส่วนอื่นๆ รวมถึงแนวทางการปฏิบัติการร่วมด้านไซเบอร์ เพื่อนำไปสู่การปฏิบัติการหลายมิติ เพื่อให้การดำเนินการสามารถปฏิบัติได้อย่างเป็นรูปธรรมและสอดคล้องกับผลลัพธ์ที่ต้องการ (Ends) โดยมุ่งเน้นในการเตรียมการตั้งแต่ขั้นปกติของแผนป้องกันประเทศ เพื่อสกัดกั้นและลดศักยภาพของภัยคุกคามตั้งแต่เริ่มต้น รวมทั้งสร้างความได้เปรียบเมื่อเข้าสู่ภาวะความขัดแย้งและสงครามตามลำดับ จึงกำหนดกลยุทธ์ในการดำเนินการ (Ways) เป็นประเด็นการพัฒนา จำนวน ๕ ประเด็น ดังนี้.-

ประเด็นการพัฒนาที่ ๑ : การสร้างการรับรู้ สร้างภูมิคุ้มกัน และป้องกันความเสี่ยง

ประเด็นการพัฒนาที่ ๒ : การข่าวกรองไซเบอร์

ประเด็นการพัฒนาที่ ๓ : การป้องกันทางไซเบอร์(เชิงรับ)

ประเด็นการพัฒนาที่ ๔ : การป้องปรามทางไซเบอร์(เชิงรุก)

ประเด็นการพัฒนาที่ ๕ : การแสวงหาความร่วมมือทางไซเบอร์

ดังนั้นเพื่อให้การดำเนินการเกิดเป็นรูปธรรม จึงได้กำหนดแผนงานและโครงการ (Means) ที่จะทำไปสู่ผลลัพธ์ที่ต้องการ จำนวน ๕ แผนงาน และ ๑๐ โครงการ ดังนี้.-

แผนงานที่ ๑ : การพัฒนาโครงสร้างพื้นฐานด้านไซเบอร์

ประกอบด้วย ๒ โครงการ ได้แก่

๑) โครงการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ กองทัพบก กองทัพเรือ กองทัพอากาศ

๒) โครงการส่งเสริมความตระหนักรู้ทางไซเบอร์

แผนงานที่ ๒ : การพัฒนาระบบค้นหาและเฝ้าตรวจ (Sensor System)

ประกอบด้วย ๑ โครงการ ได้แก่ โครงการพัฒนาระบบค้นหาและเฝ้าตรวจ ศูนย์บัญชาการกองทัพไทย กองทัพบก กองทัพเรือ กองทัพอากาศ

แผนงานที่ ๓ : การพัฒนาระบบการเชื่อมต่อข้อมูล (Data Link)

ประกอบด้วย ๑ โครงการ ได้แก่ โครงการพัฒนาระบบการเชื่อมต่อข้อมูลศูนย์บัญชาการทางทหาร กองทัพบก กองทัพเรือ กองทัพอากาศ

แผนงานที่ ๔ : การพัฒนาระบบการวิเคราะห์และจำลองทางเลือก (Analysis and Simulation System)

๑) โครงการพัฒนาระบบวิเคราะห์และจำลองทางเลือก Phase 1 (ป้องกัน) ศูนย์บัญชาการทางทหาร

๒) โครงการปฏิบัติการทางไซเบอร์เพื่อการป้องกัน กองทัพบก กองทัพเรือ กองทัพอากาศ

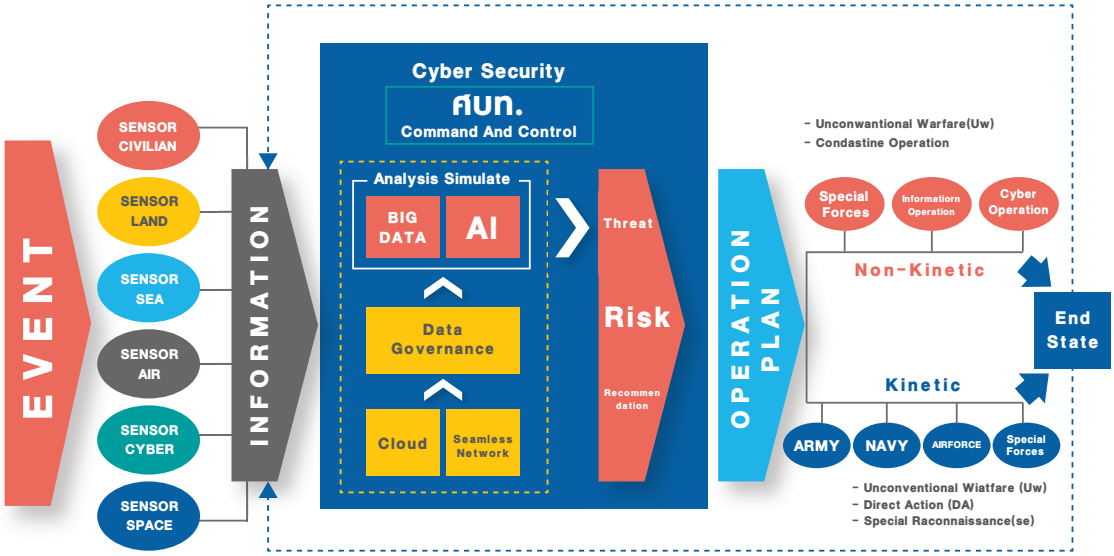
๓) โครงการพัฒนาระบบวิเคราะห์และจำลองทางเลือก Phase 2 (ป้องปราม) ศูนย์บัญชาการทางทหาร

๔) โครงการปฏิบัติการทางไซเบอร์เพื่อการป้องปราม กองทัพบก กองทัพเรือ กองทัพอากาศ

แผนงานที่ ๕ : การพัฒนาระบบควบคุมหน่วยปฏิบัติการ (Shooter System)

๑) โครงการพัฒนาระบบบัญชาการและควบคุมหน่วยปฏิบัติการ ศูนย์บัญชาการทางทหาร

๒) โครงการสร้างความร่วมมือด้านไซเบอร์ ศูนย์บัญชาการทางทหาร กองทัพบก กองทัพเรือ กองทัพอากาศ



แผนภาพที่ ๔ - ๓ แสดงกลไกการทำงานของศูนย์บัญชาการกองทัพไทยเมื่อได้รับการพัฒนา

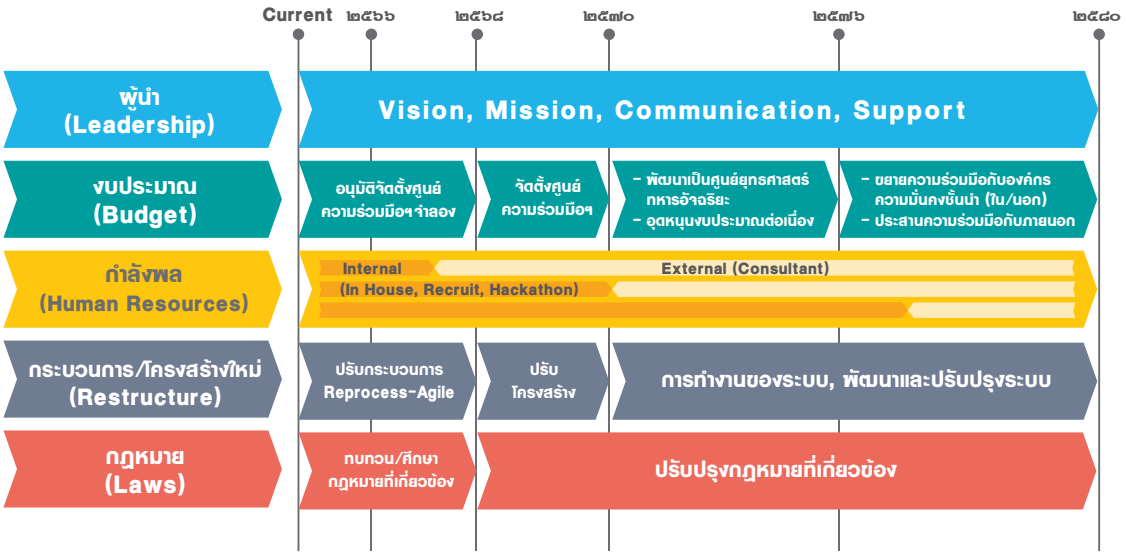
ปัจจัยแห่งความสำเร็จในการพัฒนาการปฏิบัติการด้านไซเบอร์ของกองทัพไทย

การปฏิบัติการด้านไซเบอร์นั้นจำเป็นต้องมีเปลี่ยนแปลง ปรับปรุงในด้านต่างๆ ให้เหมาะสมและสอดคล้องกับรูปแบบการปฏิบัติงานที่ต้องการความรวดเร็ว ยืดหยุ่น และแม่นยำในการตัดสินใจ ซึ่งต้องการองค์ประกอบที่สำคัญต่างๆ ดังนี้.-

๑. การปรับเปลี่ยนระบบการควบคุมบังคับบัญชาและวัฒนธรรมองค์กร เพื่อสร้างระบบการทำงานที่ต้องการความอ่อนตัวในการปรับเปลี่ยนตามสถานการณ์ที่เกิดขึ้นได้ทันเวลา และต้องการความรวดเร็วในการตกลงใจเลือกหนทางปฏิบัติในการแก้ปัญหา

๒. การจัดสรรงบประมาณให้สอดคล้องกับการปฏิบัติงานและสถานการณ์ที่เกิดขึ้น โดยขั้นต้นควรจัดตั้งศูนย์ความร่วมมือด้านการรักษาความปลอดภัยทางไซเบอร์จำลองก่อน เพื่อศึกษา จัดหา เสริมสร้างขีดความสามารถของกำลังพลและพัฒนาโครงสร้างพื้นฐาน รวมทั้งฝึกการทำงานร่วมกับเทคโนโลยี ทั้งในการควบคุม อำนวยการ และสั่งการ ให้เกิดความชำนาญและเข้าใจกระบวนการทำงาน ก่อนที่จะจัดตั้งเป็นศูนย์ความร่วมมือแบบถาวร เพื่อเป็นก้าวแรกของการเป็นผู้นำด้านความปลอดภัยทางไซเบอร์ในภูมิภาค และเตรียมการพัฒนาเป็นศูนย์ยุทธศาสตร์ทหารอัจฉริยะในห้วงต่อไป จนกระทั่งสามารถขยายความร่วมมือไปยังองค์กรชั้นนำด้านความมั่นคงทั้งภายในและภายนอกประเทศต่อไป

๓.	การพัฒนาและจัดหากำลังพลที่มีคุณสมบัติเหมาะสมในการทำงาน เป็นปัจจัยหลัก โดยมีข้อพิจารณาที่สำคัญ คือ การคัดเลือกคนที่มีทักษะที่จำเป็นในการปฏิบัติการด้านไซเบอร์ ซึ่งอาจจำแนกได้ ๓ กลุ่มที่สำคัญ ได้แก่ กลุ่มที่ ๑ กลุ่มที่มีความรู้ความเข้าใจและประสบการณ์ในการทำงานเกี่ยวกับกระบวนการทำงานขององค์กรในระดับเชี่ยวชาญ กลุ่มที่ ๒ กลุ่มที่มีทักษะการทำงานเฉพาะทางด้านไซเบอร์ ซึ่งอาจมีการคัดเลือกจากบุคคลภายนอก โดยมีวิธีการคัดเลือกที่เหมาะสม และ กลุ่มที่ ๓ กลุ่มที่ทำหน้าที่ในการวิเคราะห์กระบวนการทำงานตามระบบและปรับเปลี่ยนเป็นคำสั่งการปฏิบัติการทางไซเบอร์ (ทำหน้าที่ประสานการปฏิบัติระหว่างกลุ่มที่ ๑ และ ๒)
๔.	การปรับเปลี่ยนกระบวนการทำงาน และโครงสร้างองค์กรให้เหมาะสมต่อการทำงาน ซึ่งสืบเนื่องมาจากการปรับเปลี่ยนแนวทางการปฏิบัติงานในข้อ ๑. - ๓.
๔.	การพัฒนาปรับปรุงกฎหมายด้านความมั่นคงให้สอดคล้องกับการปฏิบัติการด้านไซเบอร์ทั้งในด้านการป้องกันและการป้องปรามอย่างเหมาะสม โดยไม่ส่งผลต่อความรู้สึกของภาคเอกชน รวมถึงประชาชนทั่วไป



แผนภาพที่ ๔ - ๔ แสดงรูปแบบการพัฒนาการปฏิบัติการด้านไซเบอร์

ระยะเวลาการเสริมสร้างขีดความสามารถการปฏิบัติการด้านไซเบอร์ของศูนย์บัญชาการทางทหาร

ระยะที่ ๑ (๒๕๖๖ - ๒๕๗๐) จัดตั้งศูนย์ความร่วมมือด้านการรักษาความปลอดภัยทางไซเบอร์ (Joint Cyber Security Collaboration Center) ของกองทัพไทย เพื่อเป็นก้าวแรกของการเป็นผู้นำด้านความปลอดภัยทางไซเบอร์ในภูมิภาค โดยจัดตั้งศูนย์ความร่วมมือจำลองสำหรับทดลองการทำงานของระบบเพื่อศึกษาความเป็นไปได้ในการปฏิบัติการในช่วงแรกของการเริ่มต้นโครงการ

ระยะที่ ๒ (๒๕๗๑ - ๒๕๗๕) พัฒนาศูนย์ความร่วมมือด้านการรักษาความปลอดภัยทางไซเบอร์เป็นศูนย์ยุทธศาสตร์ทหารร่วมอัจฉริยะ (Joint Intelligent Military Strategic Center)

ระยะที่ ๓ (๒๕๗๖ - ๒๕๘๐) ขยายความร่วมมือด้านการรักษาความปลอดภัยทางไซเบอร์ไปสู่องค์กรชั้นนำด้านความมั่นคงทั้งภายในและภายนอกประเทศ (Collaboration Expansion with Others) แผนพัฒนาขีดความสามารถด้านไซเบอร์กองทัพบก

แผนพัฒนาขีดความสามารถด้านไซเบอร์กองทัพบก

แนวทางการพัฒนาด้านไซเบอร์ของกองทัพบกภายในห้วงระยะเวลา ๓ - ๕ ปี นับจากนี้ กำหนดขึ้นโดยสอดคล้องตามกรอบยุทธศาสตร์ของกองทัพบกด้านการเตรียมกำลังและการใช้กำลัง เพื่อให้มีขีดความสามารถในการบรรลุพันธกิจหลักด้านไซเบอร์ในอนาคต ประกอบด้วย การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ การข่าวกรอง การปฏิบัติการไซเบอร์เพื่อการป้องกัน การปฏิบัติการไซเบอร์เพื่อการป้องปรามและการเสริมสร้างความร่วมมือด้านไซเบอร์กับหน่วยงานภายนอกกระทรวงกลาโหม ตั้งแต่ยามปกติ ภายใต้ขอบเขตการปฏิบัติการ ๓ ขอบเขต ได้แก่ ขอบเขตตามภารกิจของกองทัพบก ขอบเขตในการสนับสนุนการปฏิบัติการยุทธ์หลายมิติของกองบัญชาการกองทัพไทย และขอบเขตในการสนับสนุนด้านไซเบอร์ให้กับส่วนราชการอื่นตามที่ได้รับอนุมัติ โดยแนวทางการพัฒนาด้านไซเบอร์ของกองทัพบก มีดังนี้

๑. ด้านการเตรียมกำลัง

๑) โครงสร้างการจัดหน่วย งานด้านไซเบอร์จะต้องสามารถตอบสนองต่อการใช้ขีดความสามารถด้านไซเบอร์ได้อย่างมีประสิทธิภาพ ได้แก่ การจัดตั้งสำนักงานการปฏิบัติการด้านไซเบอร์ ซึ่งเป็นหน่วยยขึ้นตรงของกองทัพบก มีหน้าที่ในการวางแผน อำนวยการ ปฏิบัติการ ประสานงาน กำกับดูแล ให้ข้อเสนอแนะ และประเมินผลการดำเนินการด้านไซเบอร์ในภาพรวมของกองทัพบก และดำเนินการแลกเปลี่ยนข้อมูล บูรณาการ การวางแผนร่วมและการปฏิบัติการร่วมกับกองบัญชาการกองทัพไทยและเหล่าทัพต่างๆ รวมถึงหน่วยงานอื่นๆ ตามที่ได้รับอนุมัติ ซึ่งสำนักงานดังกล่าวอาจจัดตั้งตามอัตราเฉพาะกิจ มีกำลังพลที่มีขีดความสามารถเฉพาะด้านตามอัตรา และได้รับการสนับสนุนเครื่องมือสิ่งอำนวยความสะดวก และงบประมาณที่จำเป็น

๒) ความพร้อมรบด้านไซเบอร์ ประกอบด้วย ความพร้อมรบด้านกำลังพล ด้านสิ่งอุปกรณ์ด้านการฝึกศึกษา ด้านแผนปฏิบัติการ และด้านข้อบังคับ/ระเบียบงาน ที่มีลักษณะเฉพาะในการปฏิบัติการด้านไซเบอร์ รวมทั้งการกำหนดหลักเกณฑ์หรือมาตรฐานที่เกี่ยวข้องกับงานด้านไซเบอร์ในการได้มาซึ่งสิ่งอุปกรณ์ การเช่าใช้หรือดำเนินการร่วมกับหน่วยงานนอกกระทรวงกลาโหมหรือภาคเอกชน

๓) ความต่อเนื่องในการปฏิบัติการด้านไซเบอร์ เช่น การพัฒนากำลังพลทดแทนด้านไซเบอร์ การส่งกำลังบำรุงสิ่งอุปกรณ์ด้านไซเบอร์ การพัฒนา ประเมินผล และปรับปรุงระบบงานด้านไซเบอร์ เป็นต้น

๔) ความทันสมัยด้านไซเบอร์ หมายถึง ความทันสมัยของหลักนิยมทางทหารด้านไซเบอร์ สิ่งอุปกรณ์ด้านไซเบอร์ เทคโนโลยีสารสนเทศ เครือข่ายคอมพิวเตอร์การสื่อสาร การโทรคมนาคม และอิเล็กทรอนิกส์ เป็นต้น

๒. ด้านการใช้กำลัง

๑) การใช้ขีดความสามารถด้านไซเบอร์ของกองทัพบก เพื่อการป้องกันประเทศ เป็นการยับยั้งการปฏิบัติการที่จะขัดขวาง และ/หรือ เป็นการสร้างสภาวะที่เกื้อกูลต่อการปฏิบัติการทางทหารใน ๓ ระดับ/ขั้นความรุนแรงของสถานการณ์ ได้แก่ ขั้นปกติ ขั้นตอบโต้ และขั้นป้องกันประเทศ ทั้งเป้าหมายภายในมิติไซเบอร์ และเป้าหมายภายนอกที่กระทำผ่านมิติไซเบอร์

๒) การใช้ขีดความสามารถด้านไซเบอร์ของกองทัพบก ในการปฏิบัติการทางทหารเพื่อความมั่นคงด้านอื่นๆ เป็นการปฏิบัติการไซเบอร์ในเชิงบังคับเพื่อป้องปราม ป้องกัน และแก้ไขปัญหาที่เกิดขึ้น เพื่อปฏิบัติภารกิจในรูปแบบการให้การช่วยเหลือ ส่งเสริม และสนับสนุนการบริหารราชการแผ่นดินของรัฐ และการปฏิบัติภารกิจหลักของส่วนราชการอื่น ๆ ตามที่ได้รับอนุมัติ

ขีดความสามารถด้านการปฏิบัติการไซเบอร์นั้น จะต้องได้รับการพัฒนาอย่างต่อเนื่องและเท่าทัน ซึ่งต้องสามารถป้องกันภัยคุกคามทางไซเบอร์ รวมทั้งพัฒนาและใช้ประโยชน์จากขีดความสามารถดังกล่าว เพื่อเพิ่มมิติและขยายขีดความสามารถการปฏิบัติการทางทหารตอบสนองต่อยุทธศาสตร์/แผนการปฏิบัติการร่วมของกองบัญชาการกองทัพไทย เหล่าทัพ และหน่วยงานอื่น เพื่อให้ผู้บังคับบัญชาสามารถมองเห็นภาพการปฏิบัติการเป็นภาพเดียวกัน ทั้งยามปกติและยามสงคราม ทั้งทางด้านการข่าว ยุทธการ การวิจัยและพัฒนายุทธวิธี และเทคโนโลยีไซเบอร์ สามารถทำให้กองทัพบกมีความพร้อมในการปฏิบัติการทางทหารผ่านมิติไซเบอร์ในลักษณะNon-kinetic Soft Power ในเชิงจิตวิทยาและพฤติกรรมทั้งต่อฝ่ายตรงข้าม ฝ่ายเป็นกลาง และฝ่ายเรา ส่งผลด้านการป้องปราม การสร้างความเชื่อมั่นและความร่วมมือในการสนับสนุนการปฏิบัติของกองทัพบก รวมทั้งดำเนินการร่วมมือกับหน่วยงานภายในประเทศ เพื่อการผนึกกำลังการป้องกันภัยคุกคามด้านไซเบอร์ในระดับหน่วยเหนือขึ้นไป แสวงและพัฒนาความร่วมมือกับนานาชาติ รวมทั้งรักษาสมดุลของความสัมพันธ์ด้านไซเบอร์กับประเทศทั้งในและนอกภูมิภาครวมถึงชาติมหาอำนาจ เพื่อการมีบทบาทในการป้องกันภัยคุกคามด้านไซเบอร์เป็นที่ประจักษ์ และเป็นโอกาสในการนำเสนอภาพลักษณ์เชิงบวกต่อการดำเนินการด้านไซเบอร์ในภาพรวมของกองทัพแก่ประชาชนและประชาคมโลก

แผนพัฒนาขีดความสามารถด้านไซเบอร์กองทัพเรือ

กองทัพเรือ กำหนดประเด็นยุทธศาสตร์การพัฒนาขีดความสามารถด้านไซเบอร์แบ่งเป็น ๓ ประเด็นหลัก ได้แก่ เชิงป้องกัน (defensive) เชิงป้องปราม (offensive) และการเสริมสร้างความร่วมมือ โดยเริ่มดำเนินการจากเชิงป้องกันเป็นลำดับแรก ซึ่งจะดำเนินการควบคู่กับการแสวงหาความร่วมมือด้านไซเบอร์กับหน่วยงานภาครัฐและเอกชนภายในประเทศและการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ เมื่อได้ผลลัพธ์ตามที่กำหนดไว้แล้ว จะดำเนินการเสริมสร้างขีดความสามารถด้านอื่นๆ ต่อไปตามลำดับ

ความเชื่อมโยงกับยุทธศาสตร์ชาติและทิศทางการพัฒนาไซเบอร์

ยุทธศาสตร์ชาติ (พ.ศ.๒๕๖๑ - ๒๕๘๐) ได้ระบุในแผนแม่บทภายใต้ยุทธศาสตร์ชาติด้านความมั่นคงซึ่งเป็นแผนระดับ ๒ กำหนดการยกระดับขีดความสามารถของกองทัพในแผนย่อยที่ ๓ ให้กองทัพและหน่วยงานด้านความมั่นคงมีความพร้อมสูงขึ้นที่จะเผชิญภัยคุกคามทุกรูปแบบทุกมิติและทุกระดับความรุนแรง จึงเป็นกรอบการปฏิบัติที่ใช้ในการพัฒนาด้านไซเบอร์โดยตรง ทั้งนี้ กองทัพเรือในฐานะหน่วยงานภาครัฐที่ต้องดำเนินตามนโยบายได้เห็นความสำคัญด้านไซเบอร์ที่อาจส่งผลกระทบต่อการปฏิบัติงาน จึงได้อนุมัติโครงสร้างเจ้าหน้าที่และจัดตั้งห้องปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) โดยใช้ระบบเฝ้าระวังภัยคุกคามไซเบอร์ผ่านโปรแกรมระบบ Security Information and Event Manager : SIEM มีวัตถุประสงค์ให้เป็นศูนย์เฝ้าระวังภัยคุกคามไซเบอร์และศูนย์รับแจ้งเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นทั้งภายในและภายนอกกองทัพเรือ เพื่อให้สอดคล้องกับนโยบายด้านไซเบอร์ โดยให้ศูนย์ไซเบอร์ กรมสื่อสารและเทคโนโลยีสารสนเทศ กองทัพเรือ (สสท.ทร.) เป็นหน่วยรับผิดชอบหลัก มีภารกิจเกี่ยวกับการปฏิบัติการสงครามไซเบอร์เชิงรับเป็นหลัก ได้แก่ การรักษาความมั่นคงปลอดภัยไซเบอร์ การตอบสนองภัยคุกคามไซเบอร์ การเฝ้าระวังและการแจ้งเตือนเหตุภัยคุกคามไซเบอร์ รวมถึงการแก้ไขปัญหาด้านไซเบอร์ที่เกิดขึ้นบนระบบเครือข่ายสารสนเทศกองทัพเรือ ตลอด ๒๔ ชั่วโมง ๗ วันต่อสัปดาห์ พร้อมทั้งกองทัพเรือได้ดำเนินการประเด็นยุทธศาสตร์การพัฒนาขีดความสามารถด้านไซเบอร์ใน ๓ โครงการ คือ โครงการพัฒนาขีดความสามารถเชิงป้องกัน โครงการพัฒนาขีดความสามารถเชิงป้องปราม และโครงการพัฒนาขีดความสามารถเสริมสร้างความร่วมมือ โดยทิศทางการพัฒนาจะเริ่มจากเชิงป้องกันเป็นลำดับแรก

โครงการพัฒนาขีดความสามารถเชิงป้องกัน, ป้องปราม และเสริมสร้างความร่วมมือ

ในปีงบประมาณ พ.ศ. ๒๕๖๖ - ๒๕๗๐ กองทัพเรือ กำหนดความต้องการโครงการ/งาน/กิจกรรมที่สำคัญด้านไซเบอร์ จำนวน ๔๑ โครงการ โดยมีเป้าหมายสำคัญในด้าน ๑) ความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญ ๒) ความพร้อมของเทคโนโลยีระบบการรักษาความมั่นคงปลอดภัยไซเบอร์และ ๓) ความพร้อมของกำลังพลที่ปฏิบัติการด้านไซเบอร์ซึ่งจะดำเนินการควบคู่กับการแสวงหาความร่วมมือด้านไซเบอร์กับหน่วยงานภาครัฐและเอกชนภายในประเทศและการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้บรรลุเป้าหมายและตัวชี้วัดตามที่กำหนดไว้ต่อไป

แผนพัฒนาขีดความสามารถด้านไซเบอร์กองทัพอากาศ

กองทัพอากาศ มุ่งพัฒนาขีดความสามารถในมิติไซเบอร์รองรับการปฏิบัติการหลายมิติ (Multi - Domain Operations : MDO) ทั้งการพัฒนาหลักนิยมปฏิบัติการ การปรับปรุงโครงสร้างหน่วยงาน และการเสริมสร้างขีดความสามารถกำลังพลและนักรบไซเบอร์ เพื่อให้มีขีดความสามารถที่เพียงพอเหมาะสม และมีความพร้อมในการป้องกันประเทศและปกป้องอธิปไตยและผลประโยชน์แห่งชาติได้อย่างมีประสิทธิภาพ โดยกำหนดแนวทางการพัฒนา จำนวน ๕ แนวทาง ตามแนวความคิดการปฏิบัติการในมิติไซเบอร์ของกองทัพอากาศ

แนวทางที่ ๑ การสร้างความตระหนักรู้ทางไซเบอร์ (Cyber Awareness)

กลยุทธ์

๑. เสริมสร้างความตระหนักรู้เกี่ยวกับการปฏิบัติการและความสำคัญของมิติไซเบอร์

๒. สร้างความรู้ความเข้าใจ และจิตสำนึกด้านการรักษาความปลอดภัยทางไซเบอร์ รวมทั้งส่งเสริมวัฒนธรรมการรักษาความปลอดภัยทางไซเบอร์ในการปฏิบัติงานให้แก่กำลังพลของกองทัพอากาศทุกระดับ

โครงการ

- โครงการส่งเสริมความตระหนักรู้ทางไซเบอร์

แนวทางดำเนินการที่ ๒ การป้องกันทางไซเบอร์

กลยุทธ์

๑. พัฒนาระบบเครือข่ายและการเชื่อมต่อ รวมทั้งระบบการบริหารจัดการรองรับการป้องกันทางไซเบอร์

๒. เสริมสร้างขีดความสามารถระบบเฝ้าระวังและตรวจจับภัยคุกคามด้านไซเบอร์

๓. บูรณาการเครื่องมือทางไซเบอร์หรือซอฟแวร์ระบบการตรวจจับ การตอบสนอง และการฟื้นฟูให้สามารถใช้งานร่วมกันหรือผนึกกำลังร่วมกันได้

โครงการ

๑. โครงการพัฒนาขีดความสามารถการป้องกันทางไซเบอร์

๒. โครงการพัฒนาโครงสร้างพื้นฐานการป้องกันทางไซเบอร์

แนวทางดำเนินการที่ ๓ การข่าวกรองไซเบอร์ (Cyber Intelligence)

กลยุทธ์

๑. พัฒนาขีดความสามารถการข่าวกรองทางไซเบอร์ (Cyber Intelligence) เพื่อสนับสนุนข้อมูลข่าวกรองสำหรับการปฏิบัติงานด้านยุทธการ

๒. พัฒนาขีดความสามารถการข่าวกรองไซเบอร์เพื่อรองรับการป้องกันและการป้องปรามทางไซเบอร์

โครงการ

- โครงการพัฒนาขีดความสามารถการข่าวกรองไซเบอร์

แนวทางดำเนินการที่ ๔ การป้องปรามทางไซเบอร์ (Cyber Offense)

กลยุทธ์

๑. พัฒนาเครื่องมือ ฐานข้อมูล และรูปแบบในการฝึกจำลองยุทธ์ และรวบรวมข้อมูลสำหรับการป้องปรามทางไซเบอร์อย่างต่อเนื่อง

๒. เสริมสร้างขีดความสามารถและความพร้อมของชุดปฏิบัติการป้องปรามทางไซเบอร์รองรับการปฏิบัติภารกิจที่ได้รับมอบหมาย

โครงการ

- โครงการพัฒนาขีดความสามารถการป้องปรามทางไซเบอร์

แนวทางดำเนินการที่ ๕ ความร่วมมือทางไซเบอร์

กลยุทธ์

๑. สร้างความร่วมมือด้านไซเบอร์กับหน่วยงานภาครัฐ ภาคเอกชน สถาบันการศึกษาและสถาบันวิจัยที่มีศักยภาพทั้งในประเทศและต่างประเทศ

๒. ส่งเสริมการบูรณาการการฝึกปฏิบัติการทางไซเบอร์เข้ากับการปฏิบัติการในมิติทางอากาศ และมิติอวกาศ ในการฝึกการใช้กำลังกองทัพอากาศ การฝึกร่วม และการฝึกร่วมผสม

โครงการ

๑. โครงการความร่วมมือด้านการป้องกันทางไซเบอร์

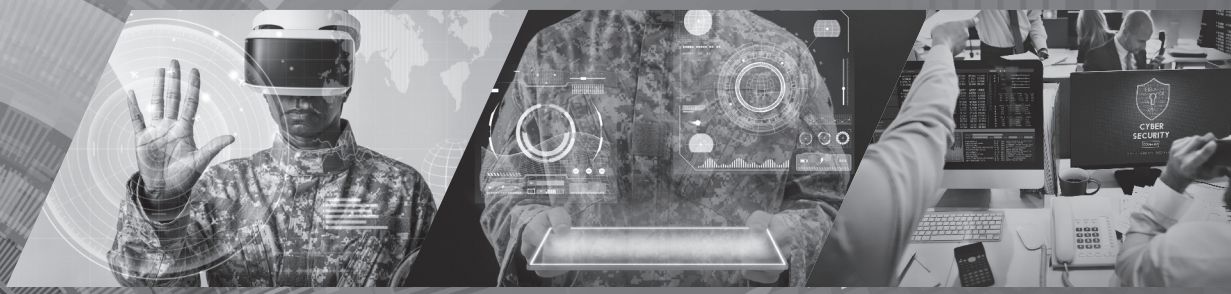
๒. โครงการความร่วมมือด้านการข่าวกรองไซเบอร์

๓. โครงการความร่วมมือด้านการป้องปรามทางไซเบอร์

๔. การแสวงหาความร่วมมือและแลกเปลี่ยนความรู้กับหน่วยงานภายนอก

บทที่ ๕

ปัจจัยสำคัญที่จะนำไปสู่ความสำเร็จ

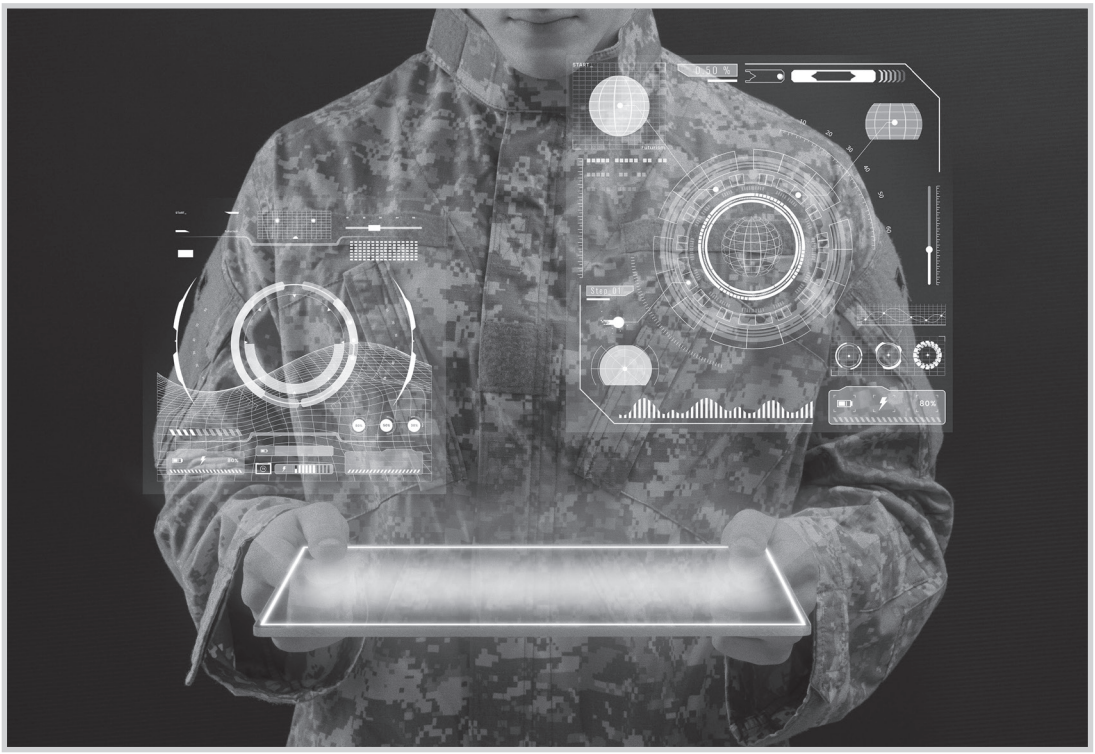


บทที่ ๕ ปัจจัยสำคัญที่จะนำไปสู่ความสำเร็จ

การจัดทำเอกสาร **แผนพัฒนาการปฏิบัติการด้านไซเบอร์ กองทัพไทย** เป็นผลงานทางวิชาการที่มีความมุ่งหมายเพื่อใช้เป็นแนวทางในการขับเคลื่อนการปฏิบัติการด้านไซเบอร์ของกองทัพไทย สำหรับป้องกันและตอบโต้ภัยคุกคามด้านไซเบอร์ที่มีแนวโน้มเพิ่มสูงขึ้นในอนาคต ซึ่งเป็นภัยคุกคามที่สามารถเกิดขึ้นได้ทุกเวลาตั้งแต่ยามปกติและส่งผลกระทบต่อความมั่นคงในทุกมิติ โดยเฉพาะผลกระทบต่อระบบโครงสร้างพื้นฐานของประเทศทั้งในด้านเศรษฐกิจ ด้านการเมืองการปกครอง ด้านสังคมจิตวิทยา และด้านการทหาร ดังนั้นกำลังทหารหรือกองทัพ ซึ่งเป็นเครื่องมือสำคัญของรัฐด้านความมั่นคง ต้องเตรียมความพร้อมเพื่อรับมือกับภัยคุกคามที่จะเกิดขึ้นได้ทุกรูปแบบ

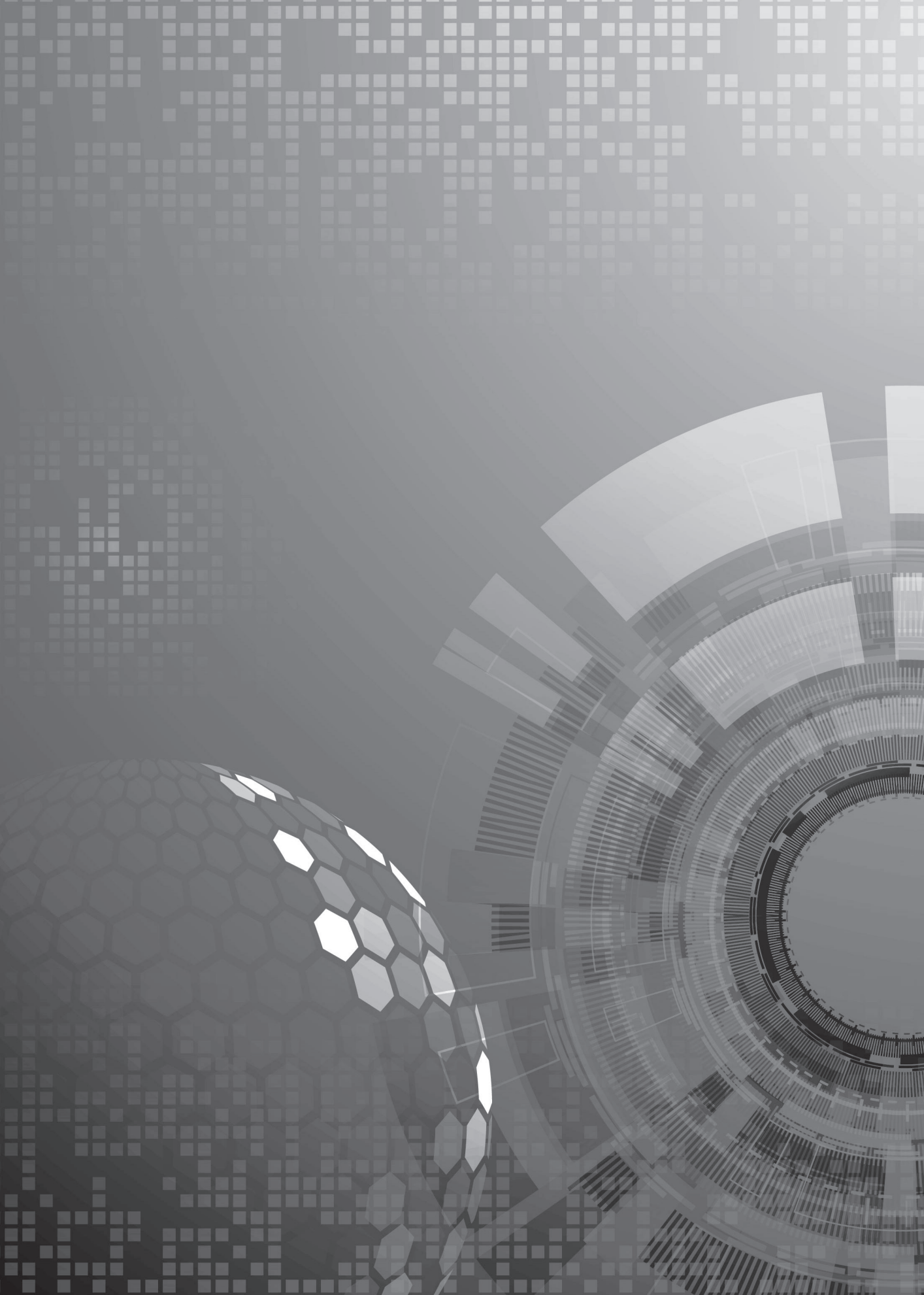
แต่อย่างไรก็ตามปัจจัยสำคัญที่จะนำไปสู่ความสำเร็จของแผนพัฒนาการปฏิบัติการด้านไซเบอร์นั้น มีประเด็นที่สำคัญ จำนวน ๕ ประเด็น ได้แก่

๑	ผู้บังคับบัญชาทางทหารต้องเป็นผู้นำแห่งการเปลี่ยนแปลงสร้างความท้าทายด้วยแนวคิดใหม่ ยอมรับความริเริ่ม เพิ่มเติมโอกาส ไม่พลาดการเรียนรู้
๒	ให้ความสำคัญกับการเสริมสร้างขีดความสามารถให้กับกำลังพลที่ต้องรับผิดชอบการปฏิบัติการไซเบอร์ทั้งระบบ เพื่อให้สามารถใช้งานเทคโนโลยีที่ทันสมัยได้เต็มประสิทธิภาพ
๓	การปรับโครงสร้างองค์กรให้มีความเหมาะสมกับระบบปฏิบัติการทางไซเบอร์ โดยใช้เทคโนโลยีมาช่วยเหลือในการประมวลผลเกี่ยวกับข้อมูลจำนวนมาก และปรับเปลี่ยนกระบวนการทำงานโดยใช้คนทำหน้าที่ในการตัดสินใจหรือตกลงใจหรือสั่งการในส่วนที่เกี่ยวข้องจากผลของการวิเคราะห์ข้อมูลที่มีความซับซ้อนซึ่งได้รับการตรวจสอบจากระบบการจำลองการวิเคราะห์เรียบร้อยแล้ว
๔	ต้องได้รับการสนับสนุนงบประมาณจากรัฐบาลอย่างต่อเนื่องในแต่ละปีงบประมาณ และสามารถเพิ่มเติมงบประมาณได้ในระดับที่เหมาะสม เพื่อรองรับการดำรงขีดความสามารถและพัฒนาระบบให้สอดคล้องกับสถานการณ์ภัยคุกคามด้านความมั่นคงที่เปลี่ยนแปลงอย่างรวดเร็ว
๕	การพัฒนากฎหมายด้านความมั่นคงให้สอดคล้องกับการปฏิบัติการด้านไซเบอร์ เนื่องจากการปฏิบัติการด้านไซเบอร์โดยกองทัพมีความล่อแหลมและละเอียดอ่อนต่อความรู้สึกของประชาชนและภาคเอกชนในด้านการละเมิดสิทธิส่วนบุคคล ดังนั้นจึงควรมีมาตรการควบคุมและข้อบังคับในการดำเนินการที่เข้มงวด แต่ต้องมีความยืดหยุ่นเพียงพอสำหรับการรักษาความมั่นคงของชาติและการป้องกันประเทศ



สรุปได้ว่า กองทัพต้องให้ความสำคัญในการเตรียมความพร้อมทั้งในด้านกำลังพลและยุทโธปกรณ์สำหรับป้องกันและตอบโต้ภัยคุกคามทั้งแบบดั้งเดิมและรูปแบบใหม่ที่มีความซับซ้อนตั้งแต่ยามปกติ เพื่อลดศักยภาพของภัยคุกคามไม่ให้ขยายตัวไปสู่ความขัดแย้งและเข้าสู่ภาวะสงคราม แต่หากหลีกเลี่ยงไม่ได้ต้องมีความได้เปรียบเมื่อต้องใช้การปฏิบัติการทางทหารเต็มรูปแบบในการป้องกันประเทศ โดยต้องเปิดรับการนำเทคโนโลยีที่ทันสมัยให้เข้ามามีบทบาทในการเสริมสร้างขีดความสามารถทางทหาร และเสริมสร้างกำลังพลให้มีขีดความสามารถในการใช้เทคโนโลยีในการแก้ไขปัญหาที่มีความซับซ้อนในระดับสูงได้อย่างมีประสิทธิภาพ รวมทั้งต้องมีการบูรณาการความร่วมมือกับทุกภาคส่วน ทั้งส่วนราชการพลเรือน เอกชน และประชาชน ตั้งแต่การเตรียมกำลังและแนวทางการใช้กำลังให้สอดคล้องกับแนวคิดทางยุทธศาสตร์ด้านการผนึกกำลังป้องกันประเทศ เพื่อส่งมอบผลผลิตด้านความมั่นคงให้กับประเทศชาติและประชาชนให้ได้อย่างมีประสิทธิภาพสูงสุด **ภายใต้วิสัยทัศน์ของกองทัพไทย พ.ศ. ๒๕๗๙ “กองทัพชั้นนำในภูมิภาค ตอบสนองต่อภัยคุกคามได้ในทุกมิติ มีกำลังรบที่ทันสมัย พึ่งพาตนเองได้ และใช้นวัตกรรม” ต่อไป** และเพื่อให้ง่ายในการจดจำ เห็นควรกำหนดเป็นสัญลักษณ์ชื่อ “ALPHA” ซึ่งจะประกอบด้วย

A : Agile Operation
L : Leadership Supervision
P : Performance Excellence
H : Hyper Intelligence
A : Action Empowerment



คณะทำงานจัดทำผลงานวิชาการ ยุทธศาสตร์ทหารร่วม ๔ สถาบัน

วิทยาลัยเสนาธิการทหาร

อาจารย์ควบคุม

๑. พล.ท. ศุภธัช นรินทรภักดี
๒. พล.ร.ต. สิทธิชัย ต่างใจ ร.น.
๓. พล.ต. บรรพต สังข์มาลา
๔. น.อ. ธานี สวัสดี
๕. น.อ. ยุทธนพงษ์ นพกุลสถิตย์ ร.น.
๖. พ.อ. ธีรพล อมราพิทักษ์
๗. น.อ. อภิชาติ นาถนิติธาดา

นักศึกษาวิทยาลัยเสนาธิการทหาร รุ่นที่ ๖๓

๑. พ.อ. วิทวัส เอกฉันท์
๒. น.อ. ภาสกร ไชยกำเนิด
๓. น.อ. ทรงวุฒิ ขยันหา ร.น.
๔. พ.อ. ธนัท กำแหงฤทธิรงค์
๕. พ.อ. พงศภัค ลิมปิยนันท์
๖. พ.อ. เปี่ยมศักดิ์ ภักดีพินิจ
๗. พ.อ. พีรพัฒน์ ราชพิบูลย์
๘. พ.อ. จารุวัตร สิริสังกาส
๙. พ.อ. วันชัย ปรีวัน
๑๐. นาง สุทิษา รังคเสนี
๑๑. นาย สมภพ เพ็ชรเกลี้ยง
๑๒. พ.อ. ยิ่งโรจน์ สันติวุฒน์
๑๓. พ.อ. อรุณ แก้วเศษ
๑๔. น.อ. บรรเจิด ทองชิว ร.น.
๑๕. นาย เอก มุติตาภรณ์

วิทยาลัยการทัพบก

อาจารย์ที่ปรึกษา

๑. พล.ต. วิชาติ เอี่ยมไพจิตร์
๒. พ.อ. ฉกาจ ขันตี
๓. พ.อ. ชนะชัย พลเตชา
๔. พ.อ. สินสมุทร์ จันทรเนตร
๕. พ.อ. ปริญญา ฉายะพงษ์

นักศึกษาวิทยาลัยการทัพบก ชุดที่ ๖๗

๑. พ.อ. เอกพงศ์ แพ่งกุล
๒. พ.อ. ชัยธัช ยิ้มทิม
๓. พ.อ. ณัฏฐานันธ์ ปรีชาภัฏสกุล
๔. พ.อ. เธียรทรรศน์ ภาม่วงเลี่ยม
๕. พ.อ. ทัพหพงศ์ บำเรอราช
๖. พ.อ.หญิง ธนิตา วงษ์จินดา
๗. พ.อ.หญิง ธมลวรรณ ตั้งวงษ์เจริญ
๘. พ.อ.หญิง นภาพิศ เอี่ยมสอาด
๙. น.อ. สันติ เกศศรีพงษ์ศา ร.น.
๑๐. น.อ. ศุภวัจน์ จิตรมนตรี
๑๑. นาย สุพพัต หีบโอสถ
๑๒. นาย ฐิติพงศ์ สมัครพงศ์

วิทยาลัยการทัพเรือ

อาจารย์ที่ปรึกษา

๑. พล.ร.ต. พิเศษ ขันแข็ง
๒. น.อ. กิติพงศ์ ทิพย์เสถียร ร.น.
๓. น.อ. พีระพล ใบกว้าง

นักศึกษาวิทยาลัยการทัพเรือ รุ่นที่ ๕๔

๑. น.อ. ภาณุวัฒน์ สมัคงาน
๒. น.อ. วรินทร คำโฮง
๓. น.อ. พิสุทธิ์ แดงเผือก
๔. น.อ. เดช สิทธิไชย
๕. น.อ. ไวพจน์ วีระประเสริฐศักดิ์
๖. น.อ. ชัยอนันต์ พลเสน
๗. น.อ. ปณต มีมอญ
๘. น.อ. ณัฐพงษ์ พัฒนจงรักษ์
๙. น.อ. สาธุ สุวรรณรักษ์
๑๐. น.อ. ศรัณย์ ดาราวิโรจน์

วิทยาลัยการทัพอากาศ

คณะอาจารย์ควบคุม

๑. น.อ. อัมพร เพ็ชราช
๒. น.อ. ประภาส ศรีประเสริฐ
๓. น.อ. เอก ศรลัมภ์
๔. น.อ. โอฐศิลป์ นิลุบล
๕. น.อ.หญิง วชิราภรณ์ เชาวน์ศิริ
๖. น.อ.หญิง ธนินี พึ่งเจียม
๗. น.อ. เทอดศักดิ์ รอดรี
๘. น.อ. เอกประสิทธิ์ พรมทัณ

นักศึกษาวิทยาลัยการทัพอากาศ รุ่นที่ ๕๖

๑. น.อ. วาริท รามโกมุท
๒. น.อ. ทรงศักดิ์ ธรรมสาร
๓. น.อ. ธีระยุทธ เกื้อสกุล
๔. น.อ. พูลสินธุ์ แจ่มใส
๕. น.อ. กฤษฎา เขียวเจริญ
๖. น.อ. ณัฏฐ์ภัทร์ สอนสืบ
๗. น.อ. ธนิต มาลีแก้ว
๘. น.อ.หญิง ชนิตรานันท์ ไวทยกุล
๙. นาย เถลิงศักดิ์ ผาทอง
๑๐. น.อ. พีระพงษ์ เปรินกุล
๑๑. น.อ. อัษฎายุธณ์ แก้วไทรย้อย
๑๒. น.อ. ภูยส โพพี
๑๓. น.อ. ณัฐจักร์ ชำนาญศรีสินเพชร
๑๔. น.อ. นัฐพล สาครเย็น
๑๕. น.อ. ณรงค์ชัย ภู่เจริญยศ ร.น.
๑๖. พ.อ. มลชัย ยิ้มอยู่
๑๗. น.อ. หม่อมหลวง กฤษณพงษ์ ศุขสวัสดิ
๑๘. น.อ. ฉัตรรัตน์ นันทะศิริ
๑๙. น.อ. กฤษณะ ดอนไพรคำ
๒๐. น.อ. นุกูล สุขประการ
๒๑. น.อ.หญิง ณัฐพรทิรา ผลากรกุล
๒๒. น.อ. ปกภณ ฉัตรภัทรไชย