ยุทธศาสตร์ความมั่นคงไทยในพลวัตเทคโนโลยีอุบัติใหม่ จากทฤษฎีสู่บทปฏิบัติการแห่งอนาคต (พ.ศ. 2569–2573)

โดย สุนันทา พาเมล่า วอร์ด [1]

1 การเปลี่ยนผ่านเชิงโครงสร้างของความมั่นคงในศตวรรษที่ 21

ในช่วงสองทศวรรษที่ผ่านมา แนวคิดเรื่อง “ความมั่นคงของชาติ” ได้เกิดการเปลี่ยนผ่านเชิงโครงสร้างอย่างมีนัยสำคัญ จากกรอบความมั่นคงแบบดั้งเดิม (Traditional Security) ที่มุ่งเน้นการป้องกันอธิปไตยทางกายภาพ การสะสมแสนยานุภาพ และการใช้กำลังทางทหาร ไปสู่กรอบความมั่นคงสมัยใหม่ที่ต้องเผชิญกับภัยคุกคามรูปแบบใหม่ (Non-traditional Security) ซึ่งมิได้จำกัดอยู่เพียงมิติทางกายภาพ หากแต่แฝงตัวอยู่ในมิติของข้อมูล เทคโนโลยี อัลกอริทึม ข้อมูลมหาศาล และรหัสพันธุกรรม ท่ามกลางกระแสการเปลี่ยนแปลงของโลกในยุค Hyper-connectivity แนวคิดเรื่องความมั่นคงของชาติได้ข้ามพ้นขอบเขตของเส้นเขตแดนทางภูมิศาสตร์ไปสู่โลกเสมือนที่ไร้พรมแดน ส่งผลให้รัฐต้องเผชิญกับความท้าทายด้านความมั่นคงในมิติใหม่ที่ซับซ้อน เชื่อมโยง และไม่อาจรับมือได้ด้วยเครื่องมือทางทหารแบบเดิมเพียงอย่างเดียว

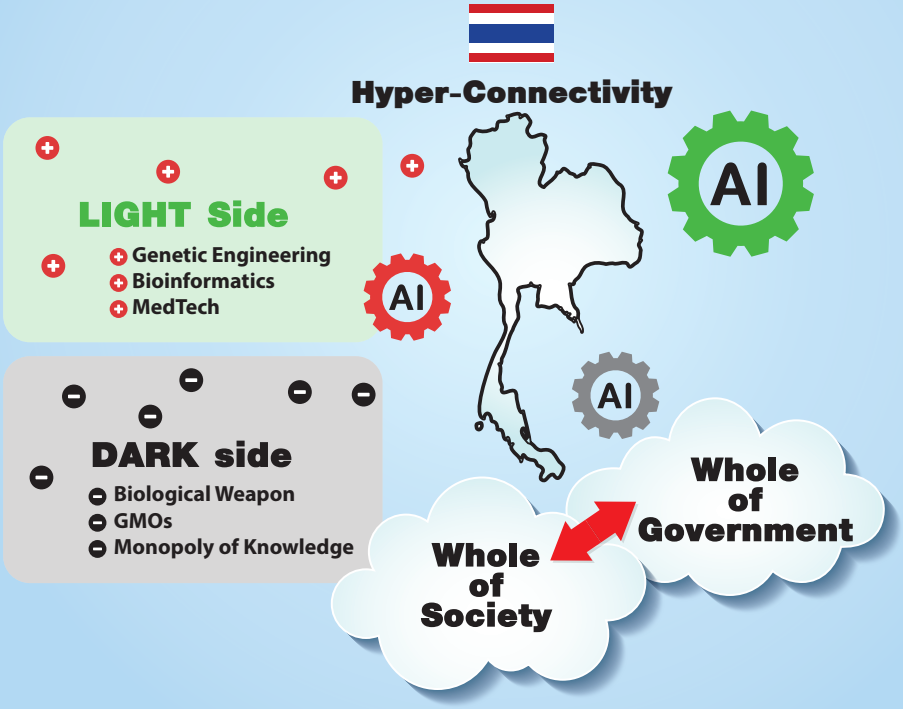
เทคโนโลยีอุบัติใหม่ โดยเฉพาะปัญญาประดิษฐ์ (Artifficial Intelligence AI) ความมั่นคงไซเบอร์ และเทคโนโลยีชีวภาพ มิได้มีบทบาทเพียงในฐานะเครื่องมือที่ช่วยเพิ่มประสิทธิภาพในการบริหารราชการแผ่นดินหรือการพัฒนาทางเศรษฐกิจและสังคมเท่านั้น หากแต่ได้ยกระดับขึ้นเป็น “สนามรบรูปแบบใหม่” (New Battlefield) และ “ตัวแปรเชิงโครงสร้าง” (Structural Variables) ที่ส่งผลกระทบต่ออธิปไตย ความมั่นคง และเสถียรภาพของประเทศในระดับรากฐาน เทคโนโลยีเหล่านี้จึงมีศักยภาพในการเปลี่ยนแปลงสมดุลอำนาจระหว่างรัฐ และสร้างทั้งโอกาสและความเสี่ยงในเวลาเดียวกัน โดยเฉพาะในบริบทที่การแข่งขันเชิงเทคโนโลยีระหว่างรัฐมหาอำนาจทวีความเข้มข้นขึ้นอย่างต่อเนื่อง

[1] นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กองความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ

ในมิติด้านปัญญาประดิษฐ์ AI ไม่เพียงทำหน้าที่เป็นเครื่องมือวิเคราะห์ข้อมูลหรือสนับสนุนการตัดสินใจเชิงนโยบาย แต่ยังสามารถถูกนำไปใช้เป็นอาวุธเชิงยุทธศาสตร์ ทั้งในรูปแบบของการปฏิบัติการไซเบอร์อัตโนมัติ การบิดเบือนข้อมูลข่าวสาร การปฏิบัติการทางจิตวิทยา และการควบคุมการรับรู้ของมวลชน ขณะที่ความมั่นคงไซเบอร์ได้กลายเป็นเสาหลักของความมั่นคงแห่งชาติ เนื่องจากระบบดิจิทัลและโครงสร้างพื้นฐานสำคัญของรัฐและสังคมล้วนพึ่งพาเครือข่ายไซเบอร์เป็นหลัก ฉะนั้นการถูกเจาะระบบหรือแทรกแซงเพียงครั้งเดียวอาจก่อให้เกิดผลกระทบเป็นลูกโซ่ต่อเศรษฐกิจ การเมือง และความเชื่อมั่นของประชาชน

ในส่วนของเทคโนโลยีชีวภาพ ความก้าวหน้าในด้านพันธุวิศวกรรม ชีวสารสนเทศ และเทคโนโลยีทางการแพทย์ขั้นสูง ได้เปิดโอกาสใหม่ในการพัฒนาคุณภาพชีวิตของประชาชน แต่ในขณะเดียวกันก็สร้างความเสี่ยงด้านความมั่นคงในรูปแบบใหม่ เช่น ความเป็นไปได้ของอาวุธชีวภาพ การดัดแปลงพันธุกรรมเพื่อวัตถุประสงค์ที่ไม่พึงประสงค์ หรือการผูกขาดองค์ความรู้และทรัพยากรชีวภาพ ซึ่งอาจกระทบต่อความมั่นคงด้านสาธารณสุขและอธิปไตยทางชีวภาพของประเทศ

ภายใต้บริบทที่เทคโนโลยีพัฒนาอย่างรวดเร็วจนกฎหมาย กลไกกำกับดูแล และกรอบจริยธรรมของมนุษย์ไม่สามารถปรับตัวได้ทัน การศึกษานี้จึงมุ่งเน้นการสังเคราะห์ข้อมูลและองค์ความรู้เพื่อค้นหาคำตอบเชิงยุทธศาสตร์ว่า ประเทศไทยจะสามารถดำรงไว้ซึ่งเสถียรภาพ ความปลอดภัย และอธิปไตยของรัฐได้อย่างไรในยุคแห่งความไม่แน่นอนดังกล่าว โดยให้ความสำคัญกับการบริหารจัดการภาครัฐแบบบูรณาการ (Whole-of-Government) ที่เชื่อมโยงหน่วยงานด้านความมั่นคง เศรษฐกิจ เทคโนโลยี และสังคมเข้าด้วยกัน ควบคู่กับการมีส่วนร่วมของทุกภาคส่วนในสังคม (Whole-of-Society) เพื่อสร้างภูมิคุ้มกันเชิงโครงสร้าง เสริมสร้างความตระหนักรู้ และพัฒนาขีดความสามารถของประเทศในการรับมือกับความท้าทายด้านความมั่นคงในศตวรรษที่ 21 อย่างยั่งยืน



2 มิติผลกระทบและพลวัตของเทคโนโลยีต่อความมั่นคง

2.1 ภูมิรัฐศาสตร์ด้านไซเบอร์และการยกระดับสู่โดเมนที่ 5 ของความมั่นคง

ในปัจจุบันไซเบอร์ได้ยกระดับจากการเป็นเพียงเครื่องมือสนับสนุนทางเทคโนโลยี จนกลายเป็น “โดเมนที่ 5” ของความมั่นคง ต่อจากโดเมนทางบก ทางน้ำ ทางอากาศ และอวกาศ โดยได้รับการยอมรับอย่างเป็นทางการในมิติทางยุทธศาสตร์ว่าเป็นพื้นที่แห่งการแข่งขันระหว่างรัฐมหาอำนาจ ซึ่งสามารถใช้เป็นเครื่องมือในการบ่อนทำลายฝ่ายตรงข้ามได้โดยไม่จำเป็นต้องใช้กำลังทางทหารโดยตรงความสำคัญของโดเมนไซเบอร์อยู่ที่ความสามารถในการเข้าถึงเป้าหมายจากระยะไกล ด้วยต้นทุนที่ต่ำ แต่สามารถสร้างผลกระทบในวงกว้างและรุนแรงในระดับโครงสร้างรัฐและสังคม

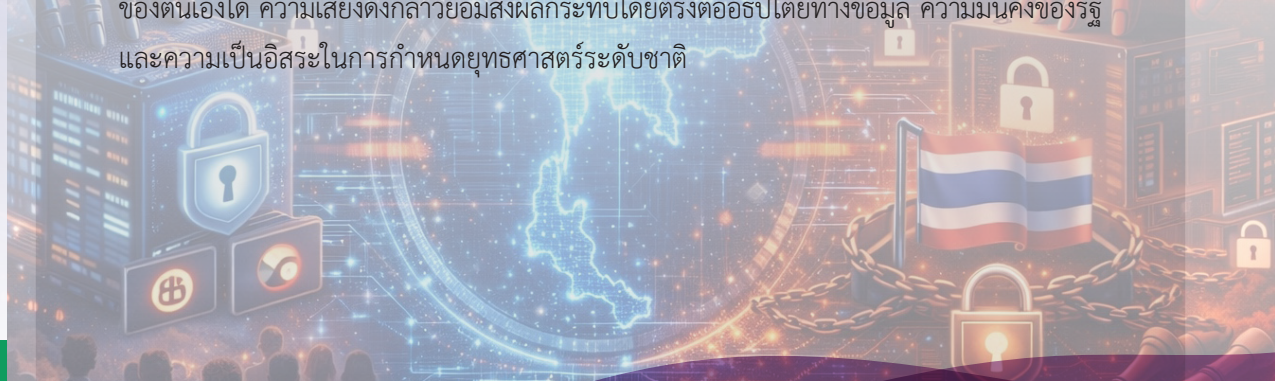
ภัยคุกคามในโดเมนไซเบอร์มิได้จำกัดอยู่เพียงการโจมตีโครงสร้างพื้นฐานที่สำคัญของชาติ (Critical Infrastructure) เช่น ระบบพลังงาน การสื่อสาร การเงิน หรือระบบสาธารณสุขเท่านั้น หากแต่ได้ขยายตัวไปสู่มิติของสงครามข้อมูลข่าวสาร (Information Warfare) และการปฏิบัติการในเชิงจิตวิทยาอย่างเป็นระบบ โดยอาศัยเทคโนโลยีดิจิทัล บอทอัตโนมัติ และปัญญาประดิษฐ์ (AI) เป็นเครื่องมือหลักในการบิดเบือนข้อมูล การควบคุมวาทกรรม และการชี้นำการรับรู้ของสังคม

ในระยะหลัง ภัยคุกคามดังกล่าวได้พัฒนาไปสู่รูปแบบที่ลึกซึ้งยิ่งขึ้น คือ “สงครามพุทธิปัญญา” (Cognitive Warfare) ซึ่งมุ่งโจมตีไม่ใช่เพียงระบบคอมพิวเตอร์หรือเครือข่ายข้อมูล หากแต่เป็นการโจมตีโดยตรงต่อความคิด ความเชื่อ และการตัดสินใจของประชาชน ผ่านการสร้างข้อมูลเท็จ การปลุกปั่นอารมณ์ การขยายกระแสความเกลียดชัง หรือการแบ่งขั้วทางสังคม การใช้ AI และบอทจำนวนมหาศาลในการปฏิบัติการดังกล่าว ทำให้การบิดเบือนการรับรู้ (Information Manipulation) เกิดขึ้นอย่างแนบเนียน รวดเร็ว และยากต่อการตรวจจับ

ผลกระทบของภัยคุกคามในโดเมนไซเบอร์จึงมิได้จำกัดอยู่เพียงความเสียหายทางเทคนิคหรือเศรษฐกิจ แต่ส่งผลโดยตรงต่อเสถียรภาพทางการเมือง ความไว้วางใจของประชาชนต่อสถาบันรัฐ และความมั่นคงทางจิตวิทยาของมวลชน ในบริบทนี้ พื้นที่ไซเบอร์จึงกลายเป็นสมรภูมิที่รัฐสามารถสั่นคลอนหรือควบคุมฝ่ายตรงข้ามได้โดยไม่ต้องยิงกระสุนแม้แต่นัดเดียว ซึ่งสะท้อนให้เห็นถึงการเปลี่ยนแปลงเชิงโครงสร้างของลักษณะสงครามและความมั่นคงในศตวรรษที่ 21 อย่างชัดเจน

2.2 อธิปไตยทางเทคโนโลยีและดิจิทัล (Digital Sovereignty) หนึ่งในความเปราะบางเชิงโครงสร้างที่สำคัญที่สุดของประเทศไทยในยุคดิจิทัล คือการพึ่งพาเทคโนโลยีและโครงสร้างพื้นฐานจากต่างชาติอย่างเข้มข้น โดยเฉพาะในด้านระบบคลาวด์ (Cloud Computing) ชิปประมวลผลหรือเซมิคอนดักเตอร์ (Semiconductors) และโมเดลภาษาขนาดใหญ่ (Large Language Models LLMs) ซึ่งล้วนเป็นหัวใจของระบบดิจิทัล เศรษฐกิจ และความมั่นคงสมัยใหม่ การพึ่งพาเทคโนโลยีเหล่านี้จากต่างประเทศ แม้จะช่วยเพิ่มประสิทธิภาพและลดต้นทุนในระยะสั้น แต่กลับสร้างความเสี่ยงเชิงยุทธศาสตร์ในระยะยาว เนื่องจากประเทศไทยอาจตกอยู่ในสถานะที่ไม่สามารถควบคุมห่วงโซ่อุปทาน การเข้าถึงข้อมูล และการทำงานของระบบสำคัญได้อย่างแท้จริง

ในบริบทของการแข่งขันเชิงภูมิรัฐศาสตร์ระหว่างมหาอำนาจ เทคโนโลยีได้กลายเป็นเครื่องมือในการกดดัน แทรกแซง หรือจำกัดอธิปไตยของรัฐคู่ขัดแย้ง การควบคุมระบบคลาวด์ โครงสร้างพื้นฐานด้านเซมิคอนดักเตอร์ หรือแพลตฟอร์ม AI อาจถูกใช้เป็นกลไกในการปิดกั้นการเข้าถึงเทคโนโลยี ชะลอการพัฒนา หรือแม้แต่แทรกแซงการตัดสินใจเชิงนโยบายของรัฐในยามวิกฤต หากประเทศไทยไม่สามารถสร้างและรักษา “อธิปไตยทางเทคโนโลยี” (Technological Sovereignty) ของตนเองได้ ความเสี่ยงดังกล่าวย่อมส่งผลกระทบโดยตรงต่ออธิปไตยทางข้อมูล ความมั่นคงของรัฐ และความเป็นอิสระในการกำหนดยุทธศาสตร์ระดับชาติ



ในมิติปัญญาประดิษฐ์ การพัฒนา AI สัญชาติไทย โดยเฉพาะโมเดลภาษาขนาดใหญ่ที่เข้าใจบริบทภาษาไทย วัฒนธรรม สังคม และระบบกฎหมายของประเทศอย่างลึกซึ้ง มิใช่เป็นเพียงประเด็นด้านความสะดวกสบายหรือประสิทธิภาพเชิงเทคนิคเท่านั้น หากแต่เป็นเครื่องมือสำคัญในการรักษาอำนาจในการตัดสินใจของรัฐให้เป็นอิสระจากอิทธิพลภายนอก เนื่องจาก AI ที่พึ่งพาโมเดลต่างชาติอาจแฝงด้วยอคติ (Bias) ชุดคุณค่า หรือข้อจำกัดที่ไม่สอดคล้องกับบริบทของประเทศไทย ซึ่งอาจส่งผลต่อการกำหนดนโยบาย การบังคับใช้กฎหมาย และการสื่อสารกับประชาชนในระยะยาว

นอกจากนี้ ความเสี่ยงเชิงยุทธศาสตร์ยังขยายไปสู่การพึ่งพาโครงสร้างพื้นฐานต่างชาติในระบบ เช่น ศูนย์ข้อมูลและระบบคลาวด์ข้ามพรมแดน ซึ่งอาจถูกใช้เป็นเครื่องมือในการกดดันหรือแทรกแซงในยามวิกฤต ทั้งในรูปแบบของการจำกัดการให้บริการ การควบคุมข้อมูล หรือการเข้าถึงระบบสำคัญของรัฐและภาคเอกชน ด้วยเหตุนี้ การมุ่งสู่ “การพึ่งพาตนเองด้านนวัตกรรม” จึงกลายเป็นภารกิจเชิงยุทธศาสตร์ของประเทศ

การพัฒนา AI สัญชาติไทย (Thai LLM) ควบคู่กับการออกแบบระบบ AI แบบ Edge หรือ Offline ที่สามารถทำงานได้โดยไม่ต้องพึ่งพาเซิร์ฟเวอร์หรือโครงสร้างพื้นฐานจากต่างประเทศ จึงเป็นแนวทางสำคัญในการเสริมสร้างอธิปไตยทางข้อมูล (Data Sovereignty) และอธิปไตยดิจิทัล (Digital Sovereignty) ของประเทศไทย แนวทางดังกล่าวไม่เพียงช่วยลดความเสี่ยงจากการพึ่งพาภายนอก แต่ยังเอื้อต่อการสร้างระบบนิเวศนวัตกรรมภายในประเทศ การพัฒนาทักษะบุคลากร และการเสริมสร้างความสามารถในการแข่งขันของไทยในเวทีโลกอย่างยั่งยืน

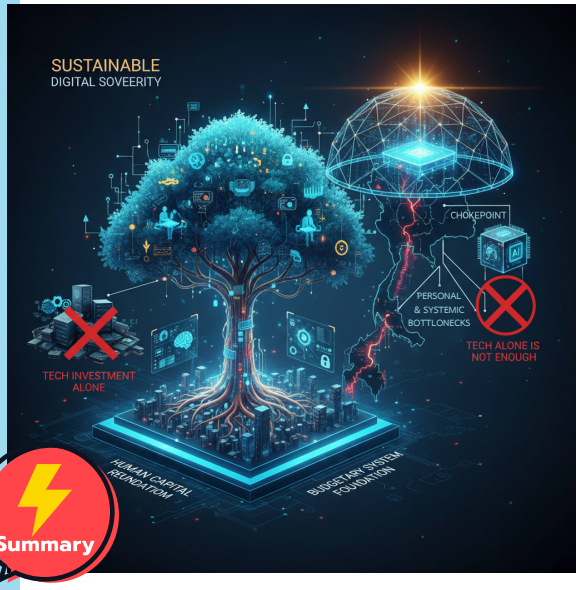
2.3 ทุนมนุษย์และโครงสร้างงบประมาณเชิงยุทธศาสตร์ หนึ่งในข้อจำกัดเชิงโครงสร้างที่สำคัญที่สุดของการเสริมสร้างความมั่นคงในยุคเทคโนโลยีขั้นสูงคือปัญหาการขาดแคลนบุคลากรที่มีความเชี่ยวชาญด้านปัญญาประดิษฐ์ (AI) และความมั่นคงไซเบอร์ซึ่งสามารถพิจารณาได้ว่าเป็น “คอขวด” (Structural Bottleneck) ที่ส่งผลโดยตรงต่อขีดความสามารถของรัฐในการรับมือกับภัยคุกคามรูปแบบใหม่ แม้ว่าประเทศไทยจะมีความต้องการใช้เทคโนโลยีขั้นสูงในภาครัฐเพิ่มขึ้นอย่างต่อเนื่อง แต่จำนวนผู้เชี่ยวชาญที่มีทักษะเชิงลึกและสามารถปฏิบัติงานในระดับยุทธศาสตร์กลับมีอยู่อย่างจำกัด อีกทั้งการแข่งขันดึงดูดบุคลากรจากภาคเอกชนและต่างประเทศยิ่งทำให้ภาครัฐเผชิญกับความเสียเปรียบในด้านค่าตอบแทน ความก้าวหน้าในอาชีพ และสภาพแวดล้อมการทำงาน

ในบริบทดังกล่าว การรักษาความมั่นคงของรัฐในศตวรรษที่ 21 จึงมิได้ขึ้นอยู่กับเพียงการลงทุนในเทคโนโลยีหรือโครงสร้างพื้นฐานเท่านั้น หากแต่ขึ้นอยู่กับความสามารถของภาครัฐในการออกแบบกลไกเพื่อดึงดูด รักษา และพัฒนาทุนมนุษย์ที่มีความเชี่ยวชาญเฉพาะด้านเข้าสู่ระบบราชการและหน่วยงานด้านความมั่นคงอย่างยั่งยืน ซึ่งอาจรวมถึงการปรับรูปแบบการจ้างงานให้มีความยืดหยุ่น การเปิดช่องทางการจ้างผู้เชี่ยวชาญเฉพาะกิจ (Specialist / Mission-based Employment) หรือการสร้างระบบนิเวศความร่วมมือระหว่างภาครัฐ ภาคเอกชน และสถาบันการศึกษา

ขณะเดียวกัน โครงสร้างงบประมาณและกระบวนการจัดซื้อจัดจ้างแบบดั้งเดิมของระบบราชการ ซึ่งมุ่งเน้นความถูกต้องตามระเบียบและความโปร่งใสในเชิงเอกสารเป็นหลัก กลับกลายเป็นอุปสรรคต่อการพัฒนาเทคโนโลยีที่ต้องอาศัยความรวดเร็ว ความยืดหยุ่น และการปรับตัวอย่างต่อเนื่อง วงจรการจัดทำงบประมาณประจำปีและกระบวนการจัดซื้อจัดจ้างที่ใช้ระยะเวลายาวนานมักไม่สอดคล้องกับธรรมชาติของเทคโนโลยี AI และไซเบอร์ ซึ่งมีการเปลี่ยนแปลงอย่างรวดเร็วและต้องการการลงทุนแบบต่อเนื่องในระยะยาว

ด้วยเหตุนี้ รัฐจึงมีความจำเป็นต้องปรับปรุงโครงสร้างงบประมาณและกระบวนการจัดซื้อจัดจ้างให้มีลักษณะเชิงยุทธศาสตร์มากขึ้น โดยเปลี่ยนจากการจัดสรรงบประมาณแบบโครงการระยะสั้นไปสู่การลงทุนระยะยาวที่มุ่งสร้างขีดความสามารถ (Capability-based Budgeting) และผลลัพธ์เชิงยุทธศาสตร์ (Outcome-oriented Budgeting) ควบคู่กับการออกแบบกลไกจัดซื้อจัดจ้างที่มีความยืดหยุ่น สามารถรองรับนวัตกรรม การทดลองเชิงนโยบาย (Policy Sandbox) และการพัฒนาเทคโนโลยีแบบต่อยอดอย่างต่อเนื่อง

โดยสรุป การเสริมสร้างความมั่นคงในยุคดิจิทัลจึงต้องอาศัยการปฏิรูปเชิงโครงสร้าง ทั้งในมิติของทุนมนุษย์และระบบงบประมาณควบคู่กัน หากภาครัฐไม่สามารถแก้ไข “คอขวด” ด้านบุคลากรและข้อจำกัดเชิงระบบเหล่านี้ได้ การลงทุนด้านเทคโนโลยีเพียงอย่างเดียวจะไม่สามารถแปรเปลี่ยนเป็นขีดความสามารถด้านความมั่นคงที่แท้จริงและยั่งยืนได้



3 การสร้างความสมดุลระหว่างประสิทธิภาพ จริยธรรม การควบคุม และสิทธิมนุษยชน

การนำเทคโนโลยีอุบัติใหม่ โดยเฉพาะปัญญาประดิษฐ์ (AI) มาใช้ในภาครัฐและภาคความมั่นคง มิใช่เพียงประเด็นด้านเทคนิคหรือประสิทธิภาพเชิงการบริหารเท่านั้น หากแต่เป็นกระบวนการที่เกี่ยวข้องโดยตรงกับหลักนิติรัฐ จริยธรรม สิทธิมนุษยชน และความชอบธรรมของอำนาจรัฐ การออกแบบนโยบายด้าน AI จึงต้องเผชิญกับข้อถกเถียงเชิงโครงสร้างที่รัฐไม่อาจหลีกเลี่ยง และจำเป็นต้องพิจารณาอย่างรอบด้านในหลายมิติ ดังนี้

1 ประการแรก **ประสิทธิภาพกับสิทธิเสรีภาพของประชาชน** การใช้ AI ในการสอดส่อง เฝ้าระวัง และคัดกรองพฤติกรรม (Surveillance) สามารถเพิ่มประสิทธิภาพในการป้องกันอาชญากรรม การก่อการร้าย หรือภัยคุกคามต่อความมั่นคงได้อย่างมีนัยสำคัญ อย่างไรก็ตาม การขยายอำนาจของรัฐในการเก็บ วิเคราะห์ และเชื่อมโยงข้อมูลส่วนบุคคลจำนวนมหาศาล ย่อมนำมาซึ่งความเสี่ยงต่อการละเมิดสิทธิในความเป็นส่วนตัว การใช้กฎหมายเป็นเครื่องมือทางการเมือง หรือการเลือกปฏิบัติต่อกลุ่มใดกลุ่มหนึ่ง หากขาดกลไกถ่วงดุลและการกำกับดูแลที่เหมาะสม

2 ประการที่สอง **ความเป็นอัตโนมัติกับการควบคุมโดยมนุษย์ (Meaningful Human Control)** โดยเฉพาะในมิติการทหารและความมั่นคง การพัฒนาระบบอาวุธสังหารอัตโนมัติ (Lethal Autonomous Weapon Systems LAWS) ได้ก่อให้เกิดข้อถกเถียงระดับนานาชาติว่า การปล่อยให้ AI มีอำนาจตัดสินใจในการใช้กำลังถึงขั้นคร่าชีวิตมนุษย์นั้นขัดต่อหลักจริยธรรมและกฎหมายมนุษยธรรมหรือไม่

3 ประการที่สาม **การกำกับดูแลกับการส่งเสริมนวัตกรรม** การออกกฎหมายหรือกรอบกำกับดูแล AI ในระดับชาติ (เช่น National AI Act) หากมีความเข้มงวดมากเกินไป อาจกลายเป็นอุปสรรคต่อการวิจัย การพัฒนา และการเติบโตของผู้ประกอบการ โดยเฉพาะวิสาหกิจขนาดกลางและขนาดย่อม (MSMEs) และสตาร์ตอัพด้านเทคโนโลยี ในทางกลับกัน หากกฎหมายมีความหละหลวมเกินไป รัฐอาจไม่สามารถป้องกันความเสี่ยงจากอคติในอัลกอริทึม การใช้ AI อย่างไม่รับผิดชอบ หรือภัยจากเทคโนโลยีบิดเบือนข้อมูล เช่น Deepfake ได้อย่างทันท่วงที

4 ประการที่สี่ **การเฝ้าระวังกับความเป็นส่วนตัว** การใช้ระบบ AI วิเคราะห์พฤติกรรม การติดตามข้อมูลขนาดใหญ่ หรือการจดจำใบหน้า (Facial Recognition) ในพื้นที่สาธารณะ อาจช่วยลดเหตุร้ายและเพิ่มความปลอดภัยของสังคม แต่ในขณะเดียวกันก็สร้างความกังวลว่ารัฐอาจก้าวเข้าสู่สภาวะของ “รัฐสอดแนม” (Surveillance State) ซึ่งประชาชนถูกติดตาม ตรวจสอบ และประเมินพฤติกรรมอย่างต่อเนื่อง ส่งผลกระทบต่อเสรีภาพในการแสดงออกและความไว้วางใจต่อสถาบันรัฐในระยะยาว

5 ประการที่ห้า **ความรับผิดชอบของเครื่องจักรและระบบอัลกอริทึม** เมื่อ AI ถูกนำมาใช้ในกระบวนการที่มีผลผูกพันทางกฎหมายหรือชีวิตมนุษย์ เช่น งานนิติวิทยาศาสตร์ การคัดกรองผู้ต้องสงสัย หรือการตัดสินใจทางทหาร (LAWS) คำถามสำคัญคือ ใครควรเป็นผู้รับผิดชอบเมื่อเกิดความผิดพลาด ระหว่างโปรแกรมเมอร์ ผู้ใช้งาน ผู้บังคับบัญชา หรือรัฐในฐานะเจ้าของระบบ เนื่องจากระบบกฎหมายปัจจุบันยังคงตั้งอยู่บนฐานของความรับผิดชอบของมนุษย์ ไม่ใช่ของอัลกอริทึม

6 ประการที่หก **อคติในอัลกอริทึมและความเป็นธรรมทางสังคม** การใช้ AI ในกระบวนการยุติธรรม การคัดกรองบุคคล การให้สินเชื่อ หรือการประเมินความเสี่ยง อาจนำไปสู่การเลือกปฏิบัติโดยไม่ตั้งใจ หากข้อมูลที่ใช้ฝึกฝน (Training Data) มีอคติแฝงอยู่ตามโครงสร้างทางสังคม เศรษฐกิจ หรือชาติพันธุ์ ซึ่งอาจส่งผลให้ AI ตอกย้ำความเหลื่อมล้ำเดิมแทนที่จะลดทอนความไม่เป็นธรรม

Summary

โดยสรุป ข้อถกเถียงเกี่ยวกับการใช้ AI และเทคโนโลยีขั้นสูงมิใช่เป็นเพียงการเลือกระหว่าง “ความมั่นคง” หรือ “สิทธิมนุษยชน” หากแต่เป็นโจทย์เชิงสมดุลที่รัฐต้องออกแบบนโยบายและกลไกกำกับดูแลอย่างรอบคอบ เพื่อให้สามารถใช้ประโยชน์จากเทคโนโลยีในการเสริมสร้างความมั่นคงและประสิทธิภาพของรัฐ ควบคู่ไปกับการคุ้มครองสิทธิเสรีภาพ ความเป็นธรรม และศักดิ์ศรีความเป็นมนุษย์ในระยะยาว

4 ข้อสรุปและข้อเสนอแนะเชิงนโยบาย

การศึกษานี้สะท้อนให้เห็นว่าความมั่นคงในยุคดิจิทัลและยุคปัญญาประดิษฐ์มิได้ขึ้นอยู่กับการจัดหาเทคโนโลยีที่ทันสมัยเพียงอย่างเดียว หากแต่เป็นการสร้าง “ระบบนิเวศแห่งความมั่นคง” (Security Ecosystem) ที่บูรณาการมิติด้านเทคโนโลยี ทุนมนุษย์ กฎหมาย โครงสร้างรัฐ และภาคสังคมเข้าด้วยกันอย่างเป็นองค์รวม ภายใต้บริบทที่ภัยคุกคามมีความซับซ้อน ไร้พรมแดนและพัฒนาเร็วกว่ากลไกการกำกับดูแลแบบเดิมของรัฐ

การขับเคลื่อนนโยบายด้านความมั่นคงจึงต้องเปลี่ยนจากแนวคิดเชิงรับ (Reactive) ไปสู่แนวคิดเชิงรุก (Proactive) และจากการทำงานแบบแยกส่วนไปสู่การบริหารจัดการแบบบูรณาการทั้งภาครัฐและสังคม (Whole-of-Government และ Whole-of-Society) โดยสามารถสังเคราะห์เป็นข้อเสนอเชิงนโยบายหลัก 4 ประการ และขยายเป็นมาตรการเชิงยุทธศาสตร์ ดังต่อไปนี้

4.1 มาตรการด้านที่ 1 การปฏิรูปทุนมนุษย์และภูมิคุ้มกันทางสังคม *(Human Capital & Social Resilience)*

หัวใจของความมั่นคงในยุคเทคโนโลยีมิใช่เครื่องจักรหรืออัลกอริทึม หากแต่คือ “คน” ทั้งในระดับผู้เชี่ยวชาญ ข้าราชการ และประชาชนทั่วไป การพัฒนา AI และระบบความมั่นคงจะไม่อาจเกิดผลได้ หากขาดทุนมนุษย์ที่มีความรู้ ความเข้าใจ และจริยธรรมรองรับ

ในระดับผู้เชี่ยวชาญ (Elite Talent) รัฐควรจัดตั้งสถาบันฝึกอบรมขั้นสูงด้าน AI และความมั่นคงไซเบอร์ร่วมกับมหาวิทยาลัยชั้นนำ เพื่อผลิตบุคลากรระดับ “ไซเบอร์-นักรบ” และนักวิเคราะห์ภัยคุกคามที่ใช้ AI เป็นเครื่องมือหลักพร้อมทั้งออกแบบมาตรการจูงใจด้านค่าตอบแทนและเส้นทางอาชีพให้สามารถแข่งขันกับภาคเอกชน เพื่อลดปัญหาการสมองไหล (Brain Drain)

ในระดับข้าราชการและบุคลากรภาครัฐ ควรยกระดับสมรรถนะผ่านโครงการ “AI for Intelligence” โดยฝึกอบรมการใช้เครื่องมือ OSINT และระบบวิเคราะห์ข้อมูลขั้นสูงที่ขับเคลื่อนด้วย AI เพื่อเพิ่มขีดความสามารถในการติดตามอาชญากรรมไซเบอร์ เครือข่ายอาชญากรรมข้ามชาติ และภัยคุกคามใน Dark Web

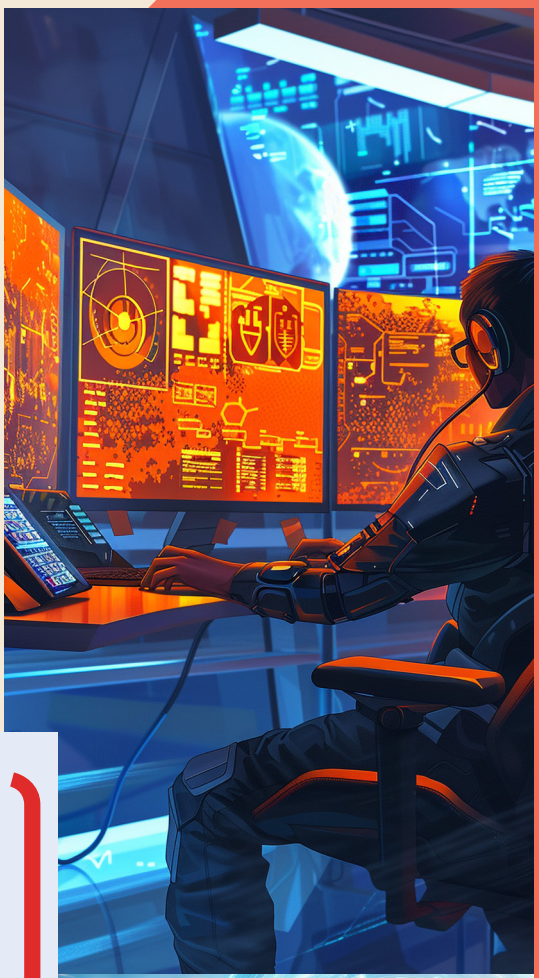
ในระดับประชาชน (Civil Resilience) การสร้างภูมิคุ้มกันทางสังคมเป็นแนวป้องกันด่านแรกของประเทศ รัฐควรบรรจุ AI Literacy และ Media Literacy เป็นส่วนหนึ่งของการศึกษาภาคบังคับ เพื่อให้ประชาชนสามารถแยกแยะข่าวปลอม Deepfake และปฏิบัติการข้อมูลข่าวสารได้อย่างมีวิจารณญาณ ควบคู่กับการสนับสนุนเครือข่ายภาคประชาสังคมในบทบาท Watchdog เพื่อเสริมสร้างความโปร่งใสและความไว้วางใจระหว่างรัฐกับประชาชน

4.2 มาตรการด้านที่ 2 การสร้างอธิปไตยทางเทคโนโลยีและระบบป้องกันเชิงรุก

(Technological Sovereignty & Proactive Defense)

ความมั่นคงของชาติไม่อาจเกิดขึ้นได้ หากประเทศยังต้องใช้โครงสร้างพื้นฐานและ “เทคโนโลยีหลัก” ของผู้อื่น การพึ่งพาต่างชาติในระบบ Cloud, Semiconductor และ AI Core Technology คือความเสี่ยงเชิงยุทธศาสตร์ที่ต้องได้รับการแก้ไขในระยะยาว

รัฐควรลงทุนพัฒนา Sovereign Cloud และ Data Center ที่เป็นกรรมสิทธิ์ของไทยอย่างสมบูรณ์ เพื่อคุ้มครองข้อมูลด้านความมั่นคงและข้อมูลอ่อนไหวจากการแทรกแซงภายนอก ควบคู่กับการพัฒนา Thai LLM สำหรับงานด้านความมั่นคง การข่าว และการสืบสวนสอบสวน โดยไม่ต้องส่งข้อมูลออกไปประมวลผลในต่างประเทศ



ในมิติการป้องกันเชิงรุก ควรยกระดับศูนย์ปฏิบัติการที่เกี่ยวข้องกับความมั่นคงไซเบอร์ ให้ปฏิบัติงานด้วยปัญญาประดิษฐ์ (AI-driven) โดยสามารถตรวจจับและตอบโต้ภัยคุกคามแบบเรียลไทม์ รวมถึงสนับสนุนอุตสาหกรรมป้องกันประเทศในการพัฒนาโดรนและหุ่นยนต์ยุทโธปกรณ์ที่มีซอฟต์แวร์ของไทยเอง เพื่อลดความเสี่ยงการควบคุมจากภายนอก หรือ (Backdoor)

4.3 มาตรการด้านที่ 3 การปฏิรูปกฎหมายและธรรมาภิบาลดิจิทัล *(Legal Reform & AI Governance)*

กฎหมายในยุค AI ต้องทำหน้าที่ทั้งเป็น “เบรก” เพื่อคุ้มครองสิทธิประชาชน และเป็น “คันเร่ง” ที่เอื้อต่อการพัฒนานวัตกรรมอย่างปลอดภัย รัฐควรเร่งผลักดัน National AI Act ที่กำหนดความรับผิดชอบทางกฎหมายอย่างชัดเจนเมื่อมีการใช้ AI ในงานของรัฐ พร้อมยึดหลัก AI ที่ยึดมนุษย์เป็นศูนย์กลาง (Human-centric AI) และมีมนุษย์เป็นผู้ควบคุมในการตัดสินใจที่สำคัญ

ในด้านการรับมือ Deepfake และสงครามข้อมูลข่าวสาร ควรออกกฎหมายเฉพาะที่กำหนดให้เนื้อหาจาก AI ต้องมีการติดฉลากหรือฝังลายน้ำดิจิทัลที่ไม่สามารถลบได้ เพื่อปกป้องประชาชนจากการบิดเบือนข้อมูล พร้อมทั้งจัดตั้ง “สนามทดลอง” ภายใต้การกำกับดูแลของหน่วยงานรัฐ (Regulatory Sandbox) สำหรับเทคโนโลยีความมั่นคง เพื่อให้รัฐสามารถทดลองนวัตกรรมใหม่ได้โดยไม่ติดกับดักกฎหมายเดิม

นอกจากนี้ ความมั่นคงไซเบอร์เป็นประเด็นข้ามพรมแดน ประเทศไทยควรมีบทบาทเชิงรุกในการผลักดันความร่วมมือระดับอาเซียน เพื่อสร้างมาตรฐานร่วมด้านการแลกเปลี่ยนข้อมูลภัยคุกคามและการจัดการอาชญากรรมไซเบอร์ข้ามชาติ

4.4 มาตรการด้านที่ 4 การปฏิรูปโครงสร้างรัฐและงบประมาณยุทธศาสตร์ *(Structural Reform & Strategic Budgeting)*

โครงสร้างการบริหารและงบประมาณแบบเดิมไม่สอดคล้องกับธรรมชาติของเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว รัฐจึงจำเป็นต้องปรับระบบจัดซื้อจัดจ้างให้มีความคล่องตัว เช่น การจัดซื้อแบบ Subscription (การเช่าใช้บริการโดยจ่ายค่าสมาชิกต่อเนื่องตามรอบรายเดือนหรือรายปี) หรือ Pay-per-use (การจ่ายตามการใช้งานจริง) และการจัดตั้งกองทุนพิเศษด้านความมั่นคงไซเบอร์ที่สามารถอนุมัติงบได้อย่างรวดเร็วในภาวะวิกฤต

ในเชิงโครงสร้าง ควรจัดตั้ง หน่วยงานหรือศูนย์ปฏิบัติการโดยปัญญาประดิษฐ์ที่ทำหน้าที่รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลข่าวสารจากหลายแหล่ง (AI-driven Fusion Center) เพื่อบูรณาการฐานข้อมูลความมั่นคงของหน่วยงานต่าง ๆ เพื่อลดปัญหา “ไซโลข้อมูล” หรือการที่ข้อมูลถูกเก็บแยกส่วนกันในแต่ละแผนก ระบบ หรือทีมภายในองค์กร (Data Silos) และเพิ่มประสิทธิภาพการวิเคราะห์ภัยคุกคามเชิงระบบ ขณะเดียวกัน นโยบายด้านเทคโนโลยีของรัฐควรคำนึงถึงความยั่งยืน โดยกำหนดแนวทางการพัฒนาและใช้งานปัญญาประดิษฐ์ที่มุ่งเน้นความยั่งยืนเป็นมิตรต่อสิ่งแวดล้อม (Green AI) และการใช้พลังงานสะอาดใน Data Center ของรัฐ

5 บทสรุปเชิงยุทธศาสตร์

การขับเคลื่อนตามแนวทางทั้งสี่ด้านนี้ จะช่วยให้ประเทศไทยสามารถเปลี่ยนผ่านสู่โลกยุค AI ได้อย่างมั่นคง ไม่เพียงใช้เทคโนโลยีเพื่อเพิ่มขีดความสามารถทางเศรษฐกิจและการบริหารรัฐเท่านั้น แต่ยังสามารถรักษาอธิปไตย ความมั่นคง และความปลอดภัยของประชาชนในทุกมิติได้อย่างแท้จริงและยั่งยืน ในมิติดังนี้

5.1 การเปลี่ยนผ่านเศรษฐกิจและยกระดับการบริหาร (Economic & Public Transformation) จะช่วยเพิ่มจีดีพีด้วยเทคโนโลยีโดยการนำ AI มาใช้ในภาคอุตสาหกรรมและเกษตรกรรมจะช่วยลดต้นทุนและเพิ่มผลผลิตมหาศาล ตามเป้าหมายของแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติ (สวทช.) และสร้างรัฐบาลดิจิทัล โดยใช้ AI ในงานบริการภาครัฐจะช่วยลดขั้นตอนที่ซับซ้อน ทำให้การอนุมัติโครงการต่าง ๆ รวดเร็วและโปร่งใสขึ้น ซึ่งสามารถตรวจสอบแนวทางการพัฒนาได้ที่สำนักงานพัฒนารัฐบาลดิจิทัล (DGA)

5.2 อธิปไตยและความมั่นคงทางข้อมูล (Sovereignty & Security) การมีอธิปไตยไซเบอร์ช่วยลดการพึ่งพาเทคโนโลยีต่างชาติเพียงอย่างเดียวซึ่งมีความเสี่ยงสูง ฉะนั้นการพัฒนา “Thai Large Language Model” หรือโครงสร้างพื้นฐานของตัวเองจะช่วยให้เราไม่ต้องส่งข้อมูลที่มีชั้นความลับของประเทศไปประมวลผลบนเซิร์ฟเวอร์ต่างแดน นอกจากนี้ ความมั่นคงปลอดภัย AI จะเป็นโล่ป้องกันภัยไซเบอร์ที่สามารถตรวจจับความผิดปกติและรับมือกับการโจมตีได้แบบทันเหตุการณ์ตามภารกิจหลักของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

5.3 ความปลอดภัยของประชาชนในทุกมิติ (Public Safety & Ethics) จะช่วยลดความเหลื่อมล้ำโดยการวางโครงสร้างพื้นฐานที่ดีจะทำให้คนทุกกลุ่มเข้าถึง AI ได้โดยไม่ใช่แค่คนในเมืองใหญ่ นอกจากนี้ ธรรมาภิบาล AI หรือการขับเคลื่อนต้องมาคู่กับ “จริยธรรม” เพื่อป้องกันการละเมิดสิทธิส่วนบุคคลและการใช้ AI ในทางที่ผิด ตามแนวทางของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

กล่าวคือหากไทยสามารถปฏิบัติตามยุทธศาสตร์ครบทั้งหมด 4 ด้าน ประเทศไทยจะไม่เป็นเพียง “ผู้ซื้อ” เทคโนโลยี แต่จะเป็น “ผู้คุมเกม” ที่ใช้ AI สร้างความมั่งคั่งพร้อมกับปกป้องผลประโยชน์ของคนในชาติได้อย่างยั่งยืน

6 รายการอ้างอิง (References)

เอกสารและกฎหมายไทย:

สำนักงานสภาความมั่นคงแห่งชาติ (สมช.). (2566). *นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 - 2570).* กรุงเทพฯ: สำนักนายกรัฐมนตรี.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.). (2568). *รายงานผลการประเมินความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปี พ.ศ. 2568*. สืบค้นเมื่อ 15 มกราคม 2569, จาก https://www.ncsa.or.th

คณะกรรมการปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติ. (2565). *แผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. 2565 - 2570).* กรุงเทพฯ: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (2569). *ร่างพระราชบัญญัติปัญญาประดิษฐ์แห่งชาติ ฉบับรับฟังความคิดเห็น*.

บทความวิชาการและรายงานสากล:

Oxford Insights. (2025). *Government AI Readiness Index 2025: Global Trends and Comparisons*. London: Oxford Insights.

UNESCO. (2024). *Thailand's Readiness for Ethical and Inclusive Artificial Intelligence: A Whole-of-Society Approach*. Bangkok: UNESCO Office.

TDRI (Thailand Development Research Institute). (2025). *Strategizing Thailand in the Global AI Race: Challenges and Opportunities*.

GIGA Hamburg. (2025). *From Global Governance to Nationalism: The Future of AI Strategy*. GIGA Focus Global.