

ความมั่นคงแห่งชาติในยุคปัญญาประดิษฐ์ การเปลี่ยนผ่านเชิงยุทธศาสตร์ และฉากทัศน์อนาคตของประเทศไทย (ค.ศ. 2025-2030)

โดย สุณันทา พามล่า วอร์ด¹

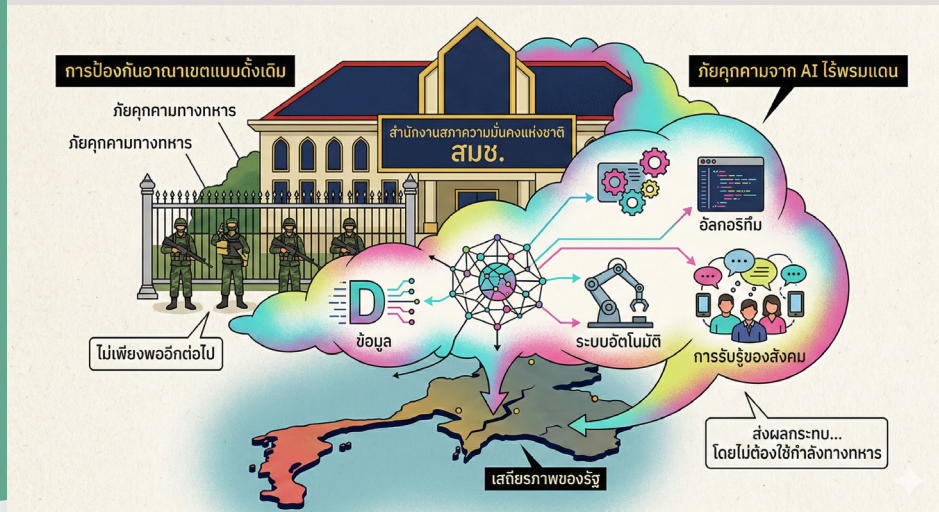
1 บทนำ ความท้าทายใหม่ในโลกที่คาดการณ์ไม่ได้

นับตั้งแต่ทศวรรษที่ 2020 เป็นต้นมา โลกได้ก้าวเข้าสู่สภาวะที่เรียกว่า VUCA อย่างเต็มรูปแบบ อันประกอบด้วยความผันผวน (Volatility) ความไม่แน่นอน (Uncertainty) ความซับซ้อน (Complexity) และความคลุมเครือ (Ambiguity) ซึ่งได้กลายเป็น “ความปกติใหม่” (New Normal) ที่ท้าทายกรอบความคิด และทฤษฎีความมั่นคงแบบดั้งเดิมของรัฐอย่างรากฐาน ปัจจัยสำคัญที่เร่งให้เปลี่ยนแปลงดังกล่าว เกิดขึ้นอย่างรวดเร็วและลึกซึ้งที่สุด คือเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence AI) ซึ่งได้พัฒนาจากการเป็นเพียงเครื่องมืออำนวยความสะดวกทางเทคโนโลยี ไปสู่การเป็น “ตัวเปลี่ยนเกม” (Game Changer) และ “อำนาจเชิงโครงสร้าง” (Structural Power) ที่แทรกซึมอยู่ในทุกมิติของรัฐ และสังคม

ในบริบทโลกปัจจุบันและอนาคตอันใกล้ ช่วงปี ค.ศ. 2025-2030 (พ.ศ. 2568-2573) AI มิได้ทำหน้าที่เพียงสนับสนุนประสิทธิภาพทางเศรษฐกิจหรือการบริหารจัดการภาครัฐเท่านั้น หากแต่ได้กลายเป็นโครงสร้างพื้นฐานใหม่ของอำนาจรัฐ อธิปไตยดิจิทัล และดุลอำนาจระหว่างประเทศ ตั้งแต่ระบบเศรษฐกิจ การสื่อสารสาธารณะ การกำหนดนโยบาย ไปจนถึงการตัดสินใจทางการทหาร และความมั่นคง AI จึงมีไม่เพียงเทคโนโลยี แต่เป็นปัจจัยกำหนดทิศทางความปลอดภัยและความอยู่รอดของรัฐในศตวรรษที่ 21



¹ นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กองความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ



สำหรับประเทศไทย ภายใต้บทบาทและความรับผิดชอบของสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) การนิยามความมั่นคงแบบดั้งเดิมที่มุ่งเน้นการป้องกันอาณาเขตทางกายภาพหรือการรับมือภัยคุกคามทางทหารเพียงอย่างเดียว ไม่เพียงพออีกต่อไป ภัยคุกคามจาก AI มีลักษณะไร้พรมแดนแฝงตัวอยู่ในมิติของข้อมูล อัลกอริทึม ระบบอัตโนมัติ และการรับรู้ของสังคม ซึ่งสามารถส่งผลกระทบต่อเสถียรภาพของรัฐได้โดยไม่ต้องใช้กำลังทางทหารแม้แต่หน่วย

บทความนี้จึงมุ่งนำเสนอการสังเคราะห์และเรียบเรียงกรอบแนวคิดต่าง ๆ เพื่อใช้เป็นรากฐานทางทฤษฎีในการวิเคราะห์ความมั่นคงสมัยใหม่ในบริบทของ AI โดยมุ่งอธิบายว่าทฤษฎีความมั่นคงร่วมสมัยจะสามารถนำมาประยุกต์ใช้เพื่อรับมือกับความท้าทายจาก AI ได้อย่างไร การวิเคราะห์ครอบคลุมตั้งแต่พื้นฐานเชิงทฤษฎี การพิจารณาผลกระทบของ AI ต่อประเทศไทย ใน 7 มิติหลัก ไปจนถึงการวิพากษ์ผ่านฉากทัศน์ทางเลือกของอนาคต (Future Scenarios) เพื่อประเมินแนวทางการบริหารจัดการความเสี่ยงเชิงรุกและการกำหนดยุทธศาสตร์ที่เหมาะสม

สรุป

โดยสรุป บทนำนี้ตั้งอยู่บนสมมติฐานสำคัญว่า ความมั่นคงในยุค AI มิใช่การพยายามควบคุมเทคโนโลยีเพียงอย่างเดียว

หากแต่คือการปรับกรอบความคิดของรัฐให้สามารถเข้าใจเปลี่ยนแปลง และอยู่ร่วมกับความไม่แน่นอนอย่างเป็นระบบ การสร้างขีดความสามารถในการคาดการณ์ การปรับตัว และการบริหารความเสี่ยงเชิงยุทธศาสตร์

จะเป็นปัจจัยชี้ขาดว่าประเทศไทยจะสามารถรักษาอธิปไตย เสถียรภาพ และความปลอดภัยของชาติได้อย่างยั่งยืนในโลกที่ไม่อาจคาดเดาได้เพียงใด

2

กรอบแนวคิด ทฤษฎี และรากฐานการวิเคราะห์

การกำหนดนโยบายความมั่นคงของรัฐท่ามกลาง “พายุทางเทคโนโลยี” และความไม่แน่นอนเชิงโครงสร้างในโลกยุค VUCA จำเป็นต้องอาศัย “เข็มทิศ” ทางทฤษฎีที่มีความแม่นยำและยืดหยุ่นเพียงพอ การพึ่งพาประสบการณ์ในอดีตหรือการตอบสนองต่อปัญหาแบบรับมือตามสถานการณ์ (Reactive) ไม่สามารถรองรับภัยคุกคามที่มีลักษณะไม่เป็นเส้นตรง มีความเร็วสูง และเชื่อมโยงกันหลายมิติอย่างปัญญาประดิษฐ์ (AI) ได้อีกต่อไป ด้วยเหตุนี้ บทความนี้จึงได้รวบรวมและสังเคราะห์กรอบแนวคิดและทฤษฎีฐานรากจำนวน 6 ประการ ซึ่งทำหน้าที่เป็นรากฐานในการวิเคราะห์อนาคตและการขับเคลื่อนยุทธศาสตร์ความมั่นคงของชาติในยุคใหม่ โดยเฉพาะในบริบทของประเทศไทยและบทบาทของสำนักงานสภาความมั่นคงแห่งชาติ (สมช.)

2.1 Strategic Foresight การมองอนาคตเชิงยุทธศาสตร์

ภายใต้บริบทโลกที่ภัยคุกคามมีลักษณะไม่เป็นเชิงเส้น (Non-linear) และยากต่อการคาดการณ์ การรอให้ปัญหาเกิดขึ้นก่อนแล้วจึงแก้ไข ถือเป็นความเสี่ยงเชิงยุทธศาสตร์อย่างยิ่ง แนวคิด Strategic Foresight จึงถูกนำมาใช้ในฐานะเครื่องมือเชิงรุก เพื่อช่วยให้รัฐสามารถ “มองการณ์ไกล” และ “คิดล่วงหน้า” อย่างเป็นระบบ

Strategic Foresight มุ่งเน้นการระบุแรงขับเคลื่อนหลักของการเปลี่ยนแปลง (Drivers of Change) โดยการตรวจจับสัญญาณอ่อน (Weak Signals) และการพัฒนาฉากทัศน์อนาคต (Scenario Planning) เพื่อเตรียมความพร้อมต่อสถานการณ์ที่อาจเกิดขึ้นได้ในหลายรูปแบบ แนวคิดนี้ช่วยให้การตัดสินใจเชิงนโยบายของ สมช. มีความยืดหยุ่น สามารถปรับตัวได้ทันทั่วทั้งที่และลดความเสี่ยงจากความไม่แน่นอนที่เกิดจากการพัฒนาอย่างรวดเร็วของ AI และเทคโนโลยีดิจิทัล

2.2 ทฤษฎีความมั่นคงแบบองค์รวม (Comprehensive Security Theory)

ทฤษฎีความมั่นคงแบบองค์รวม ซึ่งมีรากฐานสำคัญจากงานของ Barry Buzan ได้ขยายขอบเขตความมั่นคงออกจากการมุ่งเน้นมิติการทหารเพียงอย่างเดียว ไปสู่มิติเศรษฐกิจ สังคม การเมือง สิ่งแวดล้อม และมนุษย์ โดยมองว่าภัยคุกคามในโลกสมัยใหม่มีความเชื่อมโยงกันเชิงระบบ (Interconnected Threats)

ในบริบทของประเทศไทย แนวคิดนี้มีความสำคัญอย่างยิ่งต่อการรับมือภัยคุกคามข้ามพรมแดนและภัยคุกคามที่มีไซเบอร์ (Non-traditional Security) เช่น ภัยไซเบอร์ การบิดเบือนข้อมูล หรือความล้มเหลวของโครงสร้างพื้นฐานดิจิทัล ซึ่ง AI ทำหน้าที่เป็น “ตัวกลาง” ที่เชื่อมโยงมิติเหล่านี้เข้าด้วยกันอย่างแยกไม่ออก ความมั่นคงจึงไม่อาจแยกส่วนได้อีกต่อไป แต่ต้องพิจารณาในลักษณะองค์รวมและบูรณาการ

สรุปภาพรวม

กรอบแนวคิดทั้งหกประการนี้ทำหน้าที่เป็นรากฐานสำคัญในการวิเคราะห์ความมั่นคงในยุค AI โดยช่วยให้รัฐสามารถเข้าใจธรรมชาติของภัยคุกคามที่ซับซ้อน คาดการณ์อนาคตอย่างเป็นระบบ และออกแบบนโยบายที่ยืดหยุ่นทันต่อการเปลี่ยนแปลง และสอดคล้องกับบริบทของประเทศไทย ซึ่งจะนำไปสู่การวิเคราะห์ผลกระทบเชิงลึกและฉพาะด้านในอนาคตในส่วนถัดไปของบทความ

3 วิเคราะห์ประเด็นความมั่นคงจากการเปลี่ยนแปลงเทคโนโลยี AI ในประเทศไทย (พ.ศ. 2568–2573)

ในช่วงระยะเวลา 5 ปีข้างหน้า การพัฒนาอย่างก้าวกระโดดของปัญญาประดิษฐ์ (AI) จะไม่เพียงเปลี่ยนรูปแบบเศรษฐกิจหรือการบริหารรัฐเท่านั้น หากแต่จะส่งผลกระทบต่อ “ความมั่นคงของชาติ” ในทุกมิติอย่างหลีกเลี่ยงไม่ได้ AI ได้กลายเป็นตัวเร่ง (Accelerator) ที่ทำให้ความเสี่ยงเดิมทวีความรุนแรงขึ้น และก่อให้เกิดภัยคุกคามรูปแบบใหม่ที่รัฐไทยไม่เคยเผชิญมาก่อน

การวิเคราะห์นี้จึงแบ่งผลกระทบของ AI ต่อประเทศไทยออกเป็น 7 มิติหลัก ซึ่งมีความเชื่อมโยงกันเชิงระบบ และไม่สามารถรับมือโดยแยกส่วนได้

3.1 มิติสังคมและจิตวิทยา วิกฤตศรัทธา ความจริง และความเหลื่อมล้ำทางปัญญา

ภัยคุกคามที่รุนแรงที่สุดในมิตินี้คือการบั่นทอน “ความไว้วางใจ” (Trust) ซึ่งเป็นรากฐานของสังคมประชาธิปไตย AI โดยเฉพาะเทคโนโลยี Deepfake และ Generative AI ที่ทำให้การผลิตข่าวปลอม ภาพ เสียง และวิดีโอที่สมจริงจนมนุษย์แยกไม่ออกกลายเป็นเรื่องง่าย ต้นทุนต่ำ และแพร่กระจายได้อย่างรวดเร็ว ส่งผลให้สังคมเข้าสู่ภาวะสับสนว่า “อะไรคือความจริง?”

สถานการณ์ดังกล่าวอาจนำไปสู่การแบ่งขั้วทางสังคม (Social Polarization) อย่างรุนแรง และเปิดช่องให้เกิดการปลุกปั่นความเกลียดชัง (Hate Speech) ในวงกว้าง ขณะเดียวกัน ปัญหาความเหลื่อมล้ำทางดิจิทัลและ “ความเหลื่อมล้ำทางปัญญา” (Cognitive Inequality) จะทวีความชัดเจนขึ้น เนื่องจากการเข้าถึง AI คุณภาพสูงยังกระจุกตัวอยู่ในกลุ่มทุนและประชากรเมือง ขณะที่ชนบทและกลุ่มเปราะบางขาดทรัพยากรและทักษะที่จำเป็น นอกจากนี้ ยังมีปัญหา echo-chambers ที่เกิดจากอัลกอริทึมตามแพลตฟอร์มต่าง ๆ ที่ปรับเนื้อหาเสนอเข้ากับค่านิยมส่วนบุคคลมากเกินไปจนถูกตัดขาดจากสังคมที่แตกต่างและเห็นต่างจากตัวเอง ซึ่งนำไปสู่การรวมกลุ่มทางความคิดในวงปิดและเป็นปฏิปักษ์กับกลุ่มแนวคิดอื่น ๆ



ยิ่งไปกว่านั้น อคติของอัลกอริทึม (AI Bias) ยังเกิดจากข้อมูลฝึกสอนซึ่งไม่สะท้อนความหลากหลายของสังคมไทย อาจนำไปสู่การเลือกปฏิบัติต่อกลุ่มชาติพันธุ์ คนชายขอบ หรือผู้มีรายได้น้อยโดยไม่ตั้งใจ และในระยะยาว การพึ่งพา AI มากเกินไปในหมู่เยาวชน อาจบั่นทอนทักษะการคิดวิเคราะห์และการตัดสินใจด้วยตนเอง ส่งผลต่อศักยภาพแรงงานในอนาคต

3.2 มิติเทคโนโลยี ธิปไตยดิจิทัลภายใต้ร่มเงาหาอำนาจ

ประเทศไทยยังคงอยู่ในสถานะ “ผู้บริโภคนวัตกรรม” มากกว่าผู้พัฒนา โครงสร้างพื้นฐานสำคัญของ AI ตั้งแต่ระบบ Cloud, Data Center ไปจนถึงชิปประมวลผล (Semiconductors) ล้วนพึ่งพาต่างชาติเกือบทั้งหมด ความเปราะบางนี้ส่งผลโดยตรงต่ออธิปไตยดิจิทัล (Digital Sovereignty) ของประเทศ

การขาดแคลน “AI สัญชาติไทย” (Sovereign AI) ทำให้ข้อมูลสำคัญของรัฐและประชาชนเสี่ยงต่อการเข้าถึงหรือแทรกแซงผ่านกฎหมายของประเทศผู้ให้บริการ เช่น กฎหมาย Cloud Act ของสหรัฐฯ นอกจากนี้ ปัญหา Black Box AI ซึ่งระบบมีความซับซ้อนจนไม่สามารถอธิบายกระบวนการตัดสินใจได้อย่างโปร่งใส ถือเป็นความเสี่ยงอย่างยิ่งหากนำไปใช้ในระบบราชการ ระบบยุติธรรม หรือโครงสร้างพื้นฐานระดับชาติ เพราะเมื่อเกิดข้อผิดพลาด จะไม่สามารถตรวจสอบหรือระบุผู้รับผิดชอบได้อย่างชัดเจน

3.3 มิติเศรษฐกิจ การผูกขาดเชิงเทคโนโลยีและวิกฤตแรงงาน

ในมิติเศรษฐกิจ AI จะสร้างความได้เปรียบแบบก้าวกระโดดให้แก่องค์กรขนาดใหญ่ที่มีทุนและข้อมูลมหาศาล (Enterprise Advantage) ขณะที่ธุรกิจขนาดกลางและขนาดย่อม (SMEs) มีความเสี่ยงสูงที่จะถูกบดขยี้จากช่องว่างด้านประสิทธิภาพและต้นทุน ในตลาดแรงงาน AI จะเข้ามาแทนที่งานประจำและงานซ้ำซ้อน (Routine Jobs) ในภาคบริการ ธุรกิจ และอุตสาหกรรมบางประเภท ส่งผลให้เกิดการว่างงานเชิงโครงสร้างในวงกว้าง หากรัฐไม่สามารถจัดเก็บภาษีจากแพลตฟอร์มดิจิทัลข้ามชาติ (Digital Tax) ได้อย่างเป็นธรรม ประเทศจะขาดงบประมาณสำหรับการ Re-skilling และ Up-skilling แรงงานนับล้านคน ซึ่งจะนำไปสู่ปัญหาความไม่มั่นคงทางสังคมในระยะยาว

3.4 มิติการทหารและความมั่นคง สงครามที่ไร้มนุษย์ควบคุม

การเข้าสู่ยุคของระบบอาวุธสังหารอัตโนมัติ (Lethal Autonomous Weapons Systems LAWS) กำลังเปลี่ยนธรรมชาติของสงครามอย่างสิ้นเชิง การแข่งขันด้านอาวุธ AI (AI Arms Race) ในภูมิภาคเอเชียตะวันออกเฉียงใต้มีแนวโน้มทวีความเข้มข้น และเพิ่มความเสี่ยงของความขัดแย้งที่มนุษย์ไม่สามารถควบคุมได้อย่างแท้จริง นอกจากภัยคุกคามระดับรัฐแล้ว กลุ่มอาชญากรไซเบอร์และกลุ่มก่อการร้ายยังสามารถใช้ AI ในการโจมตีโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) การจัดหาเงินทุนผิดกฎหมาย และการบิดเบือนข้อมูลเพื่อบ่อนทำลายรัฐจากภายใน ทำให้เส้นแบ่งระหว่าง “สงคราม” และ “อาชญากรรม” เลือนรางลงอย่างมาก

3.5 มิติการเมือง เผด็จการดิจิทัลและการบ่อนทำลายประชาธิปไตย

AI อาจถูกใช้เป็นเครื่องมือของ Digital Authoritarianism ทั้งโดยรัฐหรือกลุ่มอำนาจผ่านการสอดแนม การเซนเซอร์ข้อมูล และการใช้ระบบวิเคราะห์พฤติกรรมเพื่อควบคุมหรือชี้นำความคิดของประชาชน โดยอาจใช้ AI วิเคราะห์จุดอ่อนทางจิตวิทยาของเยาวชนหรือกลุ่มเปราะบาง เพื่อนำมาพาดพิงทางการเมืองหรือการเลือกตั้ง ถือเป็นภัยคุกคามโดยตรงต่อกระบวนการประชาธิปไตย และอาจทำให้ความชอบธรรมของรัฐถูกตั้งคำถามอย่างรุนแรง

3.6 มิติกฎหมาย ช่องว่างของความรับผิดชอบและความยุติธรรม

กฎหมายไทยในปัจจุบันยังไม่สามารถรองรับความซับซ้อนของ AI ได้อย่างเพียงพอ โดยเฉพาะประเด็นความรับผิดชอบทางกฎหมาย (AI Liability) เมื่อ AI ก่อความเสียหาย ใครควรเป็นผู้รับผิดชอบ ระหว่างผู้พัฒนา ผู้ใช้งาน หรือองค์กรรัฐ นอกจากนี้ ยังมีความคลุมเครือด้านทรัพย์สินทางปัญญาของผลงานที่ AI สร้างขึ้น และความท้าทายในการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในยุคที่ AI ต้องพึ่งพาข้อมูลมหาศาลเพื่อการเรียนรู้ หากไม่เร่งอุดช่องว่างเหล่านี้ ระบบยุติธรรมอาจสูญเสียความน่าเชื่อถือในสายตาประชาชน

3.7 มิติทรัพยากรธรรมชาติและสิ่งแวดล้อม ต้นทุนที่ซ่อนอยู่ของความฉลาด

การพัฒนา AI โดยเฉพาะโมเดลขนาดใหญ่ ต้องอาศัย Data Center ที่ใช้พลังงานไฟฟ้าปริมาณมหาศาล และก่อให้เกิดการปล่อยก๊าซเรือนกระจกในระดับสูง และยังมีปัญหาขยะอิเล็กทรอนิกส์จากฮาร์ดแวร์ที่汰กรุ่นอย่างรวดเร็ว ซึ่งเป็นภาระด้านสิ่งแวดล้อมที่ไทยยังขาดแผนรับมืออย่างเป็นระบบ ด้วยเหตุนี้ ความมั่นคงทางพลังงานและสิ่งแวดล้อมจึงไม่อาจแยกออกจากความมั่นคงทาง AI ได้อีกต่อไป



สรุปภาพรวม

การเปลี่ยนแปลงของ AI ในช่วง พ.ศ. 2568–2573 จะสร้างผลกระทบเชิงโครงสร้างต่อความมั่นคงของประเทศไทยในทุกมิติ ตั้งแต่ระดับปัจเจกสังคม เศรษฐกิจ ไปจนถึงอธิปไตยของรัฐ การรับมือภัยคุกคามเหล่านี้จึงไม่อาจอาศัยมาตรการเชิงเทคนิคเพียงอย่างเดียว แต่ต้องอาศัยการบูรณาการเชิงยุทธศาสตร์ ซึ่งจะนำไปสู่การอภิปรายวาททัศน์อนาคตและข้อถกเถียงเชิงนโยบายในเนื้อเรื่องส่วนถัดไป

4

การวิเคราะห์เชิงลึกและข้อถกเถียงผ่านฉากทัศน์อนาคต

สมช. ได้มีการวิเคราะห์เชิงลึกและข้อถกเถียงผ่าน **ฉากทัศน์อนาคต (Alternative Futures Scenarios)** ของประเทศไทยในบริบทของการพัฒนาและผลกระทบจาก **ปัญญาประดิษฐ์ (AI)** โดยเฉพาะในปี **2030** โดยการวิเคราะห์ใช้ **แกน 2 มิติหลัก** คือ

แกน X คือเสถียรภาพทางสังคม (Social Stability) — วัดจากระดับความสามัคคี ความไว้วางใจในสถาบัน ความเท่าเทียม และการรับมือกับข้อมูลบิดเบือนหรือการแบ่งขั้วในสังคม

แกน Y คือระดับภัยคุกคามไซเบอร์ (Cyber Threat Level) — วัดจากความแข็งแกร่งของระบบป้องกันไซเบอร์ การพึ่งพาเทคโนโลยีต่างชาติ ความสามารถในการรับมือการโจมตีจากภายนอกหรือภายใน และการใช้ AI เป็นเครื่องมือโจมตี

การตัดกันของ 2 แกนนี้ สร้าง **4 ฉากทัศน์อนาคต** ที่เป็นไปได้สำหรับประเทศไทย โดยแต่ละฉากทัศน์มาพร้อมลักษณะเด่นและข้อถกเถียงเชิงวิพากษ์ ที่ชี้ให้เห็นความท้าทายเชิงนโยบาย จริยธรรม และความเป็นจริงทางการเมืองและเศรษฐกิจของไทย ได้ดังนี้

4.1 ฉากทัศน์ที่ 1 สังคมมั่นคงปลอดภัยไซเบอร์ (Safe and Cohesive Society)

ลักษณะหลัก สังคมไทยมีความเท่าทันต่อ AI (AI Literacy) สูง ประชาชนเข้าใจและใช้ AI อย่างมีสติ รัฐบาลประสบความสำเร็จในการลดความเหลื่อมล้ำ สร้างความไว้วางใจ และพัฒนาระบบป้องกันไซเบอร์ที่แข็งแกร่ง เชิงรุก มี Sovereign Cloud และโครงสร้างพื้นฐานดิจิทัลของตนเองสูง AI ถูกใช้เพื่อเสริมสร้างความเป็นธรรมและนวัตกรรมอย่างสมดุล

ข้อถกเถียงสำคัญ ประเทศไทยมีความพร้อมและเจตจำนงทางการเมืองเพียงพอหรือไม่ในการลงทุนมหาศาลระยะยาวทั้งด้านทรัพยากรมนุษย์ เช่น การสร้าง AI Talent กว่า 30,000 คน ตามแผน NAIS หรือโครงสร้างพื้นฐาน เช่น Sovereign AI และ National AI Platform ในการลดการพึ่งพาเทคโนโลยีต่างชาติ? การเมืองไทยมักมีการเปลี่ยนแปลงบ่อย ดังนั้นการจัดสรรงบประมาณระยะยาวอาจถูกขัดขวางโดยความไม่ต่อเนื่องทางการเมือง นอกจากนี้ หากรัฐต้อง “เสียสละอำนาจการควบคุมบางส่วน” เพื่อเปิดพื้นที่นวัตกรรม ซึ่งอาจขัดแย้งกับวัฒนธรรมการปกครองดั้งเดิมแบบรวมศูนย์ของไทย

4.2 ฉากทัศน์ที่ 2 สังคมมั่นคง แต่ถูกคุกคามไซเบอร์ (Cohesive but Threatened / Cohesive Society Under Cyber Threats)

ลักษณะหลัก สังคมไทยยังคงมีความสามัคคี ไว้วางใจรัฐสูง และมี AI Literacy ดี แต่โครงสร้างพื้นฐานดิจิทัล เช่น ระบบธนาคาร ไฟฟ้า การเงิน ต้องพึ่งพาเทคโนโลยีต่างชาติสูง ทำให้ตกเป็นเป้าหมายของการโจมตีไซเบอร์จากมหาอำนาจหรือแฮกเกอร์ระดับโลกได้ง่าย เช่น AI-driven attacks, ransomware, deepfake scams ที่พุ่งสูงในปี 2025

ข้อถกเถียงสำคัญ ความสามัคคีทางสังคมจะยืนยาวได้แค่ไหน หากภัยคุกคามไซเบอร์ทำให้โครงสร้างพื้นฐานล่มสลายบ่อยครั้ง? นอกจากนี้ ยังมีคำถามว่าในบริบทของประเทศกำลังพัฒนา อธิปไตยทางเทคโนโลยี (Sovereign AI) เป็นไปได้จริงหรือไม่ เมื่อการลงทุนใน Sovereign Cloud หรือ AI ท้องถิ่นต้องแข่งกับยักษ์ใหญ่ต่างชาติที่ถูกกว่าและเร็วกว่า? หากระบบเศรษฐกิจดิจิทัลถูกโจมตีซ้ำ ความไว้วางใจในรัฐอาจสั่นคลอน นำไปสู่ความไม่มั่นคงทางสังคมในที่สุด

4.3 จากทัศน์ที่ 3 สังคมแตกแยก และถูกคุกคามไซเบอร์ (Fragmented and Threatened) — จากทัศน์เลวร้ายที่สุด

ลักษณะหลัก สังคมแบ่งขั้วรุนแรง ข้อมูลบิดเบือนจาก AI (เช่น deepfake, misinformation campaigns) ทำงานได้ผล การว่างงานจาก automation พุ่งสูง ระบบป้องกันไซเบอร์อ่อนแอ AI ถูกใช้เป็นอาวุธบ่อนทำลายภายในชาติ เช่น การโจมตีข้อมูลส่วนบุคคล การปลูกปั่นความขัดแย้ง ซึ่งนำไปสู่ “สงครามกลางเมืองข้อมูลข่าวสาร” หรือรัฐล้มเหลวในยุคดิจิทัล

ข้อถกเถียงสำคัญ หาก สมช. หรือหน่วยงานที่เกี่ยวข้องไม่สามารถสร้างธรรมาภิบาล AI ที่เป็นธรรมและครอบคลุมได้ ประเทศไทยอาจเข้าสู่วงจรอุบาทว์ที่ AI เร่งความแตกแยกทางสังคม ขณะที่ภัยไซเบอร์จากทั้งภายในและภายนอกทำให้รัฐสูญเสียการควบคุม การฟื้นฟูจากจุดนี้ยากยิ่ง เพราะขาดทั้งความไว้วางใจและทรัพยากรพื้นฐาน

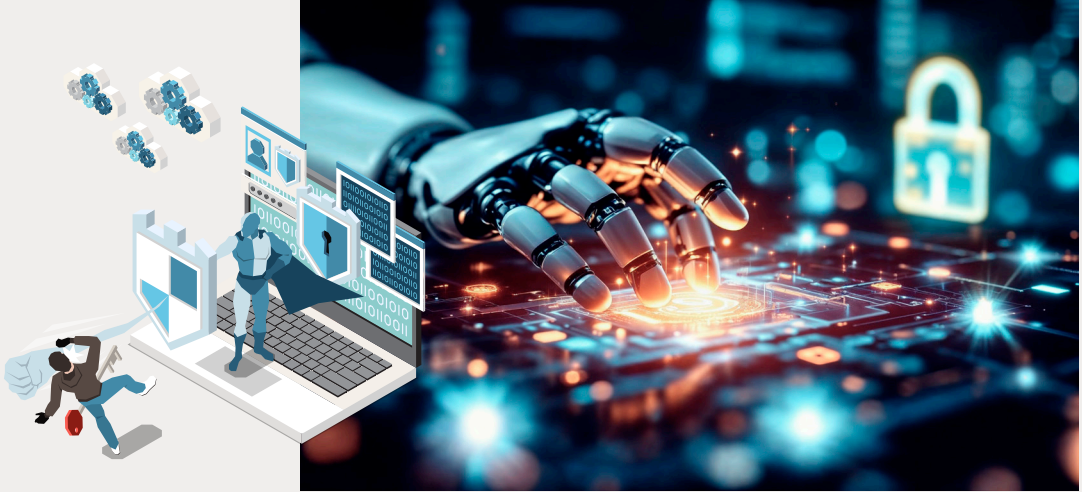
4.4 จากทัศน์ที่ 4 สังคมแตกแยก แต่มีความมั่นคงทางไซเบอร์ (Fragmented but Cyber-Safe / Fragmented with Strong Cybersecurity)

ลักษณะหลัก รัฐสร้างระบบป้องกันไซเบอร์เข้มงวดมาก โดยอาจใช้ AI ในการสอดส่องและเฝ้าระวัง ทำให้ภัยคุกคามจากภายนอกต่ำ แต่สังคมภายในมีความขัดแย้งสูง เกิดความไม่ไว้วางใจรัฐและภายในสังคมเดียวกันเอง ความมั่นคงทางไซเบอร์จึงกลายเป็นเครื่องมือรักษาอำนาจมากกว่าปกป้องประชาชน

ข้อถกเถียงสำคัญ ระบบป้องกันที่แข็งแกร่งจะมีความหมายอย่างไร หากโครงสร้างทางสังคมพังทลายจากภายใน? ความมั่นคงที่เน้นแต่ “เปลือกนอก” (technical cybersecurity) แต่ละเลยความเชื่อมั่นและความสามัคคีของประชาชน อาจนำไปสู่รัฐอำนาจนิยมดิจิทัล ซึ่งในระยะยาวอาจกลายเป็นจุดอ่อนให้ต่างชาติแทรกแซง เช่น การใช้ความไม่พอใจภายในประเทศเป็นช่องทางปฏิบัติการแทรกแซงทางความคิดเพื่อสร้างความแตกแยกในลักษณะ hybrid warfare เพราะความมั่นคงที่แท้จริงต้องมาจากทั้งปัจจัยทางเทคนิคที่มีความแข็งแกร่งและปัจจัยทางสังคมที่มีความสมานฉันท์

สรุปภาพรวมและความสัมพันธ์เชิงระบบ (Cross-Impact)

ทั้ง 4 ฉากทัศน์นี้ไม่ใช่แค่การคาดการณ์แบบแยกส่วน แต่มีความสัมพันธ์เชื่อมโยงกัน หากรัฐล้มเหลวในการสร้าง AI Literacy และลดความเหลื่อมล้ำ อาจนำไปสู่ฉากทัศน์ที่ 3 หรือ 4 ได้ง่าย แต่หากลงทุนด้านความมั่นคงไซเบอร์ แต่ละเลยการพัฒนาสังคมอาจตกไปสู่ฉากทัศน์ที่ 4 ดังนั้นการบรรลุฉากทัศน์ที่ 1 ซึ่งเป็นเป้าหมายสูงสุด ต้องอาศัยการบูรณาการนโยบายทั้งหมด จากแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. 2565 - 2570) หรือ NAIS 2022-2027 ที่เน้น 5 ยุทธศาสตร์ ได้แก่ 1) การเตรียมความพร้อมของประเทศในด้านสังคม จริยธรรม กฎหมาย และกฎระเบียบสำหรับการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance) 2) การพัฒนาโครงสร้างพื้นฐานและระบบสนับสนุนด้านปัญญาประดิษฐ์เพื่อการพัฒนาอย่างยั่งยืน (Infrastructure) 3) การเพิ่มศักยภาพบุคลากรและการพัฒนาการศึกษาด้านปัญญาประดิษฐ์ (Human Resource) 4) การพัฒนาเทคโนโลยีและนวัตกรรมเพื่อสนับสนุน เทคโนโลยีปัญญาประดิษฐ์ (Innovation) และ 5) การส่งเสริมให้การใช้เทคโนโลยี และระบบปัญญาประดิษฐ์ในภาครัฐและภาคเอกชน (Application) ซึ่งรวมถึงการสร้าง ecosystem อย่างต่อเนื่องหลังปี 2027 รวมถึงการพัฒนาอาชีพโดย AI และการยกระดับการตระหนักรู้ด้าน AI ให้ครอบคลุม 10 ล้านคนตามเป้าหมายล่าสุด ตลอดจนการรับมือภัยไซเบอร์ที่เพิ่มขึ้นอย่างรวดเร็วที่เกิดจากการโจมตีจาก AI ในปี 2025-2026





! โดยสรุป

โดยสรุปแล้วข้อตกเตียงหลักทั้งหมดชี้ไปที่ประเด็นเดียวกัน ได้แก่ ประเทศไทย จะเลือก “ความมั่นคงทางเทคนิคแต่แตกแยก” หรือ “ความสมดุลระหว่างสังคม และเทคโนโลยี” โดยการตัดสินใจในช่วง 2026-2030 จะกำหนดว่าไทยจะเป็น “รัฐที่มั่นคงในยุค AI” หรือตกเป็นเหยื่อของความขัดแย้งดิจิทัลที่ไม่มีวันสิ้นสุด

5 บทสรุป ยุทธศาสตร์นำการเปลี่ยนผ่าน

บทสรุปนี้เป็นจุดจบที่สมบูรณ์แบบของการวิเคราะห์ทั้งหมด โดยรวบรวมประเด็นเชิงยุทธศาสตร์หลัก จากฉากทัศน์อนาคตทั้ง 4 รูปแบบ และชี้ให้เห็นทิศทางที่ประเทศไทยควรเดิน เพื่อหลีกเลี่ยงวิกฤต และมุ่งสู่ฉากทัศน์ที่ 1 สังคมมั่นคงและความมั่นคงปลอดภัยไซเบอร์ ในปี 2030 ต่อไปนี้จะเป็นการเชื่อมโยง ระหว่างความมั่นคงแห่งชาติ กับ AI ในฐานะปัจจัยชี้ขาดโดยยึดแนวคิดการกำกับดูแลแบบคาดการณ์ล่วงหน้า เป็นหลักคิด ซึ่งวิเคราะห์ได้ดังนี้

5.1 ยุทธศาสตร์นำการเปลี่ยนผ่านจากเครื่องมือเทคนิคสู่ปัจจัยเชิงยุทธศาสตร์ของรัฐ

ปัญญาประดิษฐ์ (AI) ในยุคปัจจุบัน (ปี 2026) ไม่ใช่แค่เทคโนโลยี แต่กลายเป็น **โครงสร้างอำนาจใหม่** ที่กำหนดเสถียรภาพของประเทศไทย ความมั่นคงที่แท้จริงไม่ได้วัดจากว่าไทยมีโมเดล AI ที่ล้ำสมัยที่สุด เช่น LLM ขนาดใหญ่ แต่วัดจากความสมดุลสองด้าน ได้แก่ ด้านเทคนิค และด้านสังคม

- **ด้านเทคนิค** การพัฒนาขีดความสามารถทางไซเบอร์ (cyber resilience) รวมถึงระบบป้องกันภัยคุกคามจาก AI, อธิปไตยของระบบคลาวด์ และโครงสร้างพื้นฐานที่ควบคุมได้เอง

- **ด้านสังคม** การสร้างภูมิคุ้มกันทางสังคม ผ่านความตระหนักรู้ด้าน AI ที่ครอบคลุม การลดความเหลื่อมล้ำดิจิทัล และการป้องกันการใช้อำนาจ AI เป็นเครื่องมือแบ่งขั้วหรือบ่อนทำลายสังคม

หากขาดสมดุลนี้ ไทยอาจตกอยู่ใน ฉากทัศน์ที่ 3 ที่สังคมแตกแยกและถูกคุกคามโดยไซเบอร์ ซึ่งอาจนำไปสู่การเป็นรัฐล้มเหลวในยุคดิจิทัลที่ AI เร่งความขัดแย้งภายใน ขณะที่ภัยไซเบอร์จากภายนอก เช่น การโจมตีโครงสร้างพื้นฐานจากมหาอำนาจอาจทำให้รัฐสูญเสียการควบคุม สมช. จึงต้องเปลี่ยนบทบาทจาก “ผู้กำกับดูแล” (regulator) มาเป็น “ผู้อำนวยการอำนวยความสะดวกเชิงยุทธศาสตร์” (strategic facilitator) ที่ใช้ Anticipatory Governance เพื่อคาดการณ์ความเสี่ยงล่วงหน้า ปรับนโยบายแบบยืดหยุ่น และสร้างธรรมาภิบาล AI ที่มีมนุษย์เป็นศูนย์กลาง (Human-Centric AI)

5.2 ข้อเสนอแนะหลัก 3 ประเด็นเร่งด่วนที่ สมช. และหน่วยงานที่เกี่ยวข้องต้องขับเคลื่อน

5.2.1 การเร่งสร้างอธิปไตยทางข้อมูลและเทคโนโลยี (Sovereign AI)

ไทยต้องลดการพึ่งพาโครงสร้างพื้นฐาน AI จากต่างชาติอย่างเร่งด่วน เช่น cloud providers รายใหญ่จากสหรัฐฯ หรือจีน ซึ่งเป็นจุดอ่อนในยามวิกฤตภูมิรัฐศาสตร์ ในปี 2025-2026 คณะกรรมการขับเคลื่อนแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (National AI Committee) ได้อนุมัติงบประมาณกว่า 25 พันล้านบาท สำหรับขับเคลื่อนภาคีเครือข่าย และสร้างศูนย์ความเชี่ยวชาญด้าน AI เพื่อการพัฒนาประเทศไทย เพื่อเร่งรัดการพัฒนาและบูรณาการการทำงานอย่างมีประสิทธิภาพเบื้องต้น จำนวน 9 แห่ง ได้แก่

- ศูนย์นวัตกรรมปัญญาประดิษฐ์ด้านการศึกษา
- ศูนย์นวัตกรรมอุตสาหกรรมสร้างสรรค์ด้วยปัญญาประดิษฐ์
- ศูนย์นวัตกรรมปัญญาประดิษฐ์ด้านการเกษตร
- ศูนย์ความเป็นเลิศด้านปัญญาประดิษฐ์เพื่อการท่องเที่ยว
- ศูนย์ความเป็นเลิศด้านปัญญาประดิษฐ์เพื่อสุขภาพและสุขภาวะ
- ศูนย์ความเป็นเลิศด้านปัญญาประดิษฐ์เพื่อการผลิต
- กลุ่มภาคีเครือข่ายด้านโมเดลภาษาขนาดใหญ่ภาษาไทย
- ศูนย์การประมวลผลปัญญาประดิษฐ์ภาครัฐ
- ศูนย์สอบเทียบสมรรถนะและทดสอบมาตรฐานผลิตภัณฑ์ปัญญาประดิษฐ์ รวมถึงการตั้ง **Thai Large Language Model Network Group, Government AI Processing Center** และ **AI Centers of Excellence (CoEs)** เพื่อพัฒนาโมเดลภาษาไทย โครงสร้างพื้นฐานเปิด (open-source AI platforms) และ Sovereign AI ที่ควบคุมข้อมูลสำคัญของชาติได้เอง หากไม่เร่งเรื่องนี้ ไทยจะตกอยู่ใน **ฉากทัศน์ที่ 2** ที่สังคมสามัคคี แต่ถูกคุกคามไซเบอร์ได้ง่าย





5.2.2 การปฏิรูปกฎหมาย AI แบบยืดหยุ่นและเป็นผลลัพธ์ แทนที่จะออกกฎหมาย

เข้มงวดแบบตายตัว ที่อาจทำลายการสร้างนวัตกรรม ควรเน้นระบบความรับผิดชอบและกำกับดูแลบนพื้นฐานของผลลัพธ์ (outcome-based regulation) เช่น การใช้กรอบจริยธรรมจาก UNESCO ที่ไทยร่วมเป็นเจ้าภาพในงาน Global Forum on the Ethics of AI ณ กรุงเทพฯ ในปี 2025 รวมถึงแนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Securities Guideline) ที่ออกโดยสำนักงานคณะกรรมการการรักษามั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ช่วงตุลาคม 2025 ที่ผนวกมาตรฐานสากลอย่าง ISO/IEC 42001:2023 เข้ากับกฎหมาย PDPA และพระราชบัญญัติการรักษามั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ปัจจุบัน ETDA กำลังปรับร่าง “ร่างหลักการกฎหมาย AI (Draft Principles of the AI Law)” ที่รวมร่างกฎหมายเดิมสองฉบับของ ETDA และ ONDE ให้เป็นฉบับเดียวเพื่อสมดุลระหว่างนวัตกรรมและความเสี่ยง โดยมี ศูนย์กลางธรรมาภิบาล AI เป็นหน่วยงานช่วยให้คำปรึกษาและทำ sandbox เพื่อช่วยป้องกันไม่ให้ AI กลายเป็นเครื่องมือบ่อนทำลายสังคมในฉากทัศน์ที่ 3

5.2.3 การยกระดับความฉลาดทางดิจิทัลของมวลชน (AI Literacy & Social Resilience)

การศึกษาต้องเป็นด่านหน้าในการสร้างภูมิคุ้มกันต่อ deepfake, misinformation และอคติจาก AI โดยเป้าหมายจากคณะกรรมการขับเคลื่อนแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติ เพื่อการพัฒนาประเทศไทย (National AI Committee) คือยกระดับความตระหนักรู้ด้าน AI ให้ประชากร 10 ล้านคน ภายใน 2 ปี พร้อมฝึกอบรมผู้เชี่ยวชาญ 90,000 คน และนักพัฒนา 50,000 คน ผ่านแพลตฟอร์มอย่าง THAI Academy ร่วมกับ Microsoft และโครงการ AI for All หากทำสำเร็จจะเป็นเกราะป้องกันไม่ให้อิทธิพลจากข้อมูลบิดเบือน และช่วยให้ไทยหลุดพ้นจาก**ฉากทัศน์ที่ 4** ที่รัฐมีความมั่นคงทางไซเบอร์ที่แข็งแกร่งแต่ประชาชนไม่ไว้วางใจกันเอง



การใช้ AI เพื่อความมั่นคงของครอบครัวและความยั่งยืน

นอกจากป้องกันภัย ไทยควรใช้ AI เป็นเครื่องมือเชิงรุกในการบริหารจัดการทรัพยากร เช่น การคาดการณ์แนวโน้มการใช้พลังงาน การจัดการน้ำท่วม การเกษตรแม่นยำ และการดูแลสุขภาพ เพื่อสร้างความมั่งคั่งและความยั่งยืนในระยะยาว ซึ่งสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี และเป้าหมายเป็น AI Hub ในอาเซียนปี 2027



ข้อสรุปของความมั่นคงที่แท้จริงในยุค AI

ในโลกที่ AI เปลี่ยนแปลงทุกอย่างได้อย่างรวดเร็ว ความมั่นคงไม่ได้อยู่ที่ “ใครมีเครื่องจักรที่ฉลาดที่สุด” แต่อยู่ที่ใครใช้เครื่องจักรในการรับใช้สังคม ความเป็นธรรม และความเป็นมนุษย์ ได้ดีที่สุดในประเทศไทยในปี 2026 อยู่ที่จุดตัดว่าจะเลือกเป็นชาติที่ AI เป็นภัยคุกคามนำไปสู่ความแตกแยกและรัฐล้มเหลว หรือจะใช้การกำกับดูแลและวางยุทธศาสตร์เพื่อเปลี่ยน AI ให้เป็นโอกาสในการสร้างสังคมที่มั่นคง เท่าเทียม และยั่งยืน

หาก สมช. และหน่วยงานระดับชาติเร่งดำเนินการตาม 3 ประเด็นหลักข้างต้น พร้อมมีการสนับสนุนด้านงบประมาณอย่างต่อเนื่อง พร้อมทั้งสร้างความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชนได้อย่างเหมาะสม นอกจากไทยจะรอดพ้นจากภัยคุกคามแห่งยุคดิจิทัลแล้ว จะก้าวขึ้นเป็นแบบอย่างของประเทศกำลังพัฒนาที่ใช้ AI เพื่อเสริมสร้างความมั่นคงแห่งชาติอย่างแท้จริง นั่นคือจะสามารถสร้างความมั่นคงที่มาจากภายใน ทั้งในทางเทคโนโลยี และในทางสังคมอีกด้วย

เอกสารอ้างอิง

AI Thailand. (n.d.). แผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. 2565–2570). <https://www.ai.in.th>

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2025, July 30). บอร์ด AI แห่งชาติ ประกาศลงทุนภาครัฐ ขั้นต่ำ 25,000 ล้านบาท ขับเคลื่อนภาคีเครือข่าย - ศูนย์ความเชี่ยวชาญด้าน AI [Facebook post].