ISSN: 2774-0080

จุลสารด้านความมั่นคง
Security Pamphlet

ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ

ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก
ฉบับที่ ๒ ประจำปีงบประมาณ ๒๕๖๘

ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ

พิมพ์เมื่อ : พ.ศ. ๒๕๖๘

จัดพิมพ์โดย : กรมยุทธศึกษาทหารบก ๔๑ ถนนเทอดดำริ แขวงถนนนครไชยศรี เขตดุสิต กรุงเทพฯ ๑๐๓๐๐

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก

จุลสารด้านความมั่นคง : ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ

กองทัพบก กระทรวงกลาโหม, ๒๕๖๘

ISSN 2774 - 0080

พิมพ์ที่ : บริษัท ธนอรุณการพิมพ์ จำกัด

๔๕๗/๖ - ๗ ถนนพระสุเมรุ แขวงบวรนิเวศ เขตพระนคร กรุงเทพฯ ๑๐๒๐๐

โทร. ๐ - ๒๒๘๒ - ๖๐๓๓ - ๔ โทรสาร ๐ - ๒๒๘๐ - ๒๑๘๗ - ๘

E-mail: thanaaroon19@gmail.com

คำนำ

ภัยคุกคามจากเทคโนโลยีถือเป็นภัยคุกคามรูปแบบใหม่ที่ส่งผลต่อความมั่นคงของชาติ ซึ่งเป็นประเด็นที่สอดคล้องกับยุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ - ๒๕๘๐), ร่างยุทธศาสตร์กองทัพบก และนโยบายการปฏิบัติงานของกองทัพในด้านการเตรียมความพร้อมเพื่อรับมือกับสถานการณ์ด้านความมั่นคง ปัจจุบันโลกมีการเปลี่ยนแปลงเทคโนโลยีอย่างรวดเร็ว โดยเฉพาะเทคโนโลยีปัญญาประดิษฐ์ (AI) ที่กำลังมีผลกระทบไปทั่วโลก กลายเป็นความท้าทายต่อการป้องกันภัยคุกคามที่ส่งผลกระทบต่อทุกองค์กร ทั้งภาครัฐและเอกชน เทคโนโลยีปัญญาประดิษฐ์ถูกนำมาใช้ในการสงครามมากขึ้น รวมถึงถูกนำมาใช้ในชีวิตประจำวัน เนื่องจากปัญญาประดิษฐ์เป็นเครื่องมือทางเลือกที่สามารถยกระดับการทำงานและสามารถสนับสนุนการตัดสินใจได้อย่างมีประสิทธิภาพ

ดังนั้น ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก จึงได้จัดทำจุลสารด้านความมั่นคง ฉบับที่ ๒ ประจำปีงบประมาณ ๒๕๖๘ เรื่อง “ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ” โดยรวบรวมข้อมูลจากแหล่งข้อมูลทางวิชาการ และข้อมูลจากสรุปผลการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหารในประเด็นที่เกี่ยวข้อง (โดยพิจารณาจากกรอบสถานการณ์

ที่ผ่านมาจนถึงห้วงเดือน มิถุนายน พ.ศ. ๒๕๖๘) เพื่อสร้างความรู้ ความเข้าใจเกี่ยวกับปัญญาประดิษฐ์ ที่มีผลต่อภัยคุกคามด้านความมั่นคงของชาติ รวมถึงการสร้างความตระหนักรู้ให้กับกำลังพลของกองทัพบกถึงภัยคุกคามจากปัญญาประดิษฐ์ ซึ่งเป็นหนึ่งในรูปแบบใหม่ของภัยคุกคาม เพื่อให้กำลังพลของกองทัพบกสามารถปรับตัวและปฏิบัติงานให้สอดคล้องกับสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงไป

กรมยุทธศึกษาทหารบกหวังเป็นอย่างยิ่งว่า จุลสารด้านความมั่นคงฉบับนี้จะเป็นประโยชน์ต่อกำลังพลทุกระดับ และหน่วยงานของกองทัพบกในการปฏิบัติภารกิจของหน่วย เพื่อตอบสนองกิจสำคัญระดับยุทธการวัตถุประสงค์และนโยบายของกองทัพบกต่อไป

พลโท

(ธิติพันธ์ ฐานะจาโร)

เจ้ากรมยุทธศึกษาทหารบก

สารบัญ

เรื่อง “ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ”

๑. กล่าวนำ

ภาพที่ ๑ *เทคโนโลยีปัญญาประดิษฐ์ (AI) ที่มีผลกระทบไปทั่วโลก*

ปัจจุบันปัญญาประดิษฐ์ (AI) นอกจากจะเป็นเทคโนโลยีที่มีคุณประโยชน์แล้วยังเป็นเทคโนโลยีที่ถือเป็นภัยคุกคามด้านความมั่นคงของชาติได้ด้วยเช่นกัน เทคโนโลยีปัญญาประดิษฐ์ มีการพัฒนาก้าวหน้าอย่างรวดเร็ว ในรูปแบบคอมพิวเตอร์ที่ใช้เทคโนโลยีก้าวหน้าสมัยใหม่ที่ถูกสร้างขึ้นมาเพื่อบริหารจัดการกับข้อมูลที่มีความซับซ้อนเกินขีดความสามารถของมนุษย์ที่จะจัดการได้ โดยมีความสามารถในการวิเคราะห์และประมวลผลสามารถตรวจจับช่องโหว่ของระบบ รวมถึงสร้างกลยุทธ์การโจมตีได้โดยอัตโนมัติ ทำให้อาชญากรทางไซเบอร์สามารถวิเคราะห์เป้าหมายการโจมตี วางแผน และดำเนินการสร้างความเสียหายให้กับองค์กร ไม่ว่าจะเป็นองค์กรของรัฐ หรือที่มีใช้กันในภาคส่วนต่าง ๆ ส่งผลทำให้ภัยคุกคามปัญญาประดิษฐ์เป็นภัยต่อความมั่นคงของชาติ ซึ่งแนวโน้มปัญญาประดิษฐ์ ในปี พ.ศ. ๒๕๖๘ มีการคาดการณ์ว่าสงครามทางไซเบอร์จะเข้ามามีบทบาทสำคัญอย่างมากในการขับเคลื่อนยุทธศาสตร์ทางทหารของหลายประเทศ อย่างเช่น สหรัฐอเมริกา, รัสเซีย, จีน, อังกฤษ และอิสราเอล เป็นต้น เทคโนโลยี AI เป็นอาวุธในการทำสงครามไซเบอร์ รวมถึงประเทศไทยจะต้องตระหนักถึงภัยคุกคามของปัญญาประดิษฐ์ ซึ่งภัยคุกคามทางเทคโนโลยีนี้สามารถทำลายระบบสำคัญของศัตรูได้โดยไม่ต้องใช้การสู้รบแบบดั้งเดิม เนื่องจากเทคโนโลยี AI สามารถทำให้เกิดการโจมตีอย่างรวดเร็วและแม่นยำ ดังนั้นการเตรียมพร้อมรับมือภัยคุกคามปัญญาประดิษฐ์ ซึ่งถือเป็นภัยคุกคามรูปแบบใหม่ จึงเป็นสิ่งสำคัญในการปฏิบัติภารกิจที่หน่วยงานด้านความมั่นคง รวมทั้งกองทัพบกจะต้องนำไปพิจารณาดำเนินการ

๒. คำจำกัดความของปัญญาประดิษฐ์ (AI)

๒.๑ ปัญญาประดิษฐ์คืออะไร

ปัญญาประดิษฐ์ หรือ AI (Artificial Intelligence) คือ โปรแกรมเทคโนโลยีคอมพิวเตอร์ ที่มีประสิทธิภาพสูงในการประมวลผลข้อมูล สามารถเรียนรู้และวิเคราะห์ข้อมูลได้อย่างแม่นยำและรวดเร็ว ทำให้ปัจจุบันปัญญาประดิษฐ์ ได้เข้ามามีบทบาทสำคัญในเทคโนโลยีต่าง ๆ ที่นำมาปรับใช้ในชีวิตประจำวัน โดยสามารถใช้เป็นเครื่องมือหรือตัวช่วยด้านการประมวลผลเพื่ออำนวยความสะดวกช่วยให้มนุษย์ใช้ข้อมูลมาประกอบการตัดสินใจได้ง่ายมากยิ่งขึ้น โดยปัญญาประดิษฐ์สามารถวิเคราะห์และสรุปผลให้มนุษย์ได้ภายในเวลาอันรวดเร็ว อีกทั้งยังช่วยลดความผิดพลาดของมนุษย์ (Human Error) ในการคิดคำนวณ นอกจากนี้ประโยชน์ของปัญญาประดิษฐ์ยังช่วยลดทรัพยากรและประหยัดเวลาในการทำงาน รวมทั้งลดความเสี่ยงต่อชีวิตและทรัพย์สินในการทำงาน ยกตัวอย่างเช่น กรณีเกิดเหตุการณ์ตึกถล่ม สามารถเลือกใช้หุ่นยนต์ค้นหาในการปฏิบัติภารกิจได้ ปัญญาประดิษฐ์มีระบบประมวลผลและยังมีฟังก์ชันที่สามารถทำงานได้เสมือนกับมนุษย์ และสามารถเลียนแบบการทำกิจกรรมของมนุษย์ได้ ได้แก่ การเรียนรู้ การวางแผน และการแก้ไขปัญหาต่าง ๆ ซึ่งจะเน้นไปในเรื่องของการประมวลผลและวิเคราะห์ข้อมูลต่าง ๆ สามารถทำงานได้รวดเร็วกว่าสมองของมนุษย์ และมีการคาดการณ์ว่า AI จะมีบทบาทเข้ามาทำหน้าที่แทนมนุษย์ในตำแหน่งบทบาทหน้าที่ต่าง ๆ ในอนาคตอีกด้วย

นอกจากนี้ความสามารถของปัญญาประดิษฐ์ ยังสามารถเข้าใจเนื้อหาสาระ รวมทั้งสามารถแปลและสื่อความหมายด้านภาษา, เรียบเรียงเนื้อหา, สามารถวิเคราะห์ภาพและวีดิโอ และเรียนรู้จากข้อมูลที่หลากหลายเพื่อหาความเชื่อมโยงที่มนุษย์มองข้ามไปหรือคาดไม่ถึง ซึ่ง AI มีผลกระทบทางเศรษฐกิจ กล่าวคือ ประเทศที่เชี่ยวชาญด้านปัญญาประดิษฐ์สามารถสร้างธุรกิจและตำแหน่งงานใหม่ ทำให้ภาคอุตสาหกรรมมีประสิทธิภาพมากยิ่งขึ้น

๒.๒ ระบบการทำงานของปัญญาประดิษฐ์ (AI)

เป็นปฏิบัติการทำงานโดยการรับข้อมูล วิเคราะห์ข้อมูล และประมวลผลโดยผ่านการใช้คำพูด ข้อความ หรือการกระทำต่าง ๆ และนำผลลัพธ์นั้นมาใช้ประโยชน์ให้ตรงกับจุดประสงค์ที่ผู้ใช้ต้องการ อีกทั้งยังสามารถใช้รูปแบบการทำงานนี้ เพื่อคาดการณ์สถานการณ์ที่จะเกิดขึ้นในอนาคตได้ ซึ่งการทำงานของระบบทั้งหมดนั้นต้องถูกเขียนโปรแกรมขึ้นมา โดยการเขียนโปรแกรมของ AI นั้นจะเน้นไปที่ทักษะการรับรู้ต่าง ๆ ดังนี้

๑.) การเรียนรู้ (Learning) โดยจะเน้นไปที่การรับข้อมูล และสร้างกฎสำหรับการเปลี่ยนเป็นข้อมูลที่นำไปใช้ได้จริง ซึ่งกฎนั้นเรียกว่า อัลกอริทึม (Algorithms) คือ กระบวนการแก้ปัญหาที่อธิบายเป็นขั้นตอนไว้อย่างชัดเจน หรือชุดของขั้นตอนที่ชัดเจน

๒.) การใช้เหตุผล (Reasoning) เน้นการตัดสินใจเลือกอัลกอริทึมที่เหมาะสมเพื่อให้ได้ผลลัพธ์ที่ต้องการ

๓.) การแก้ไขข้อผิดพลาด (Self-Correction) มีการออกแบบเพื่อปรับแต่งอัลกอริทึมให้วิเคราะห์ได้อย่างละเอียด เพื่อให้ได้ผลลัพธ์ที่แม่นยำที่สุด

๔.) การมีความคิดสร้างสรรค์ (Creativity) เป็นส่วนที่ใช้เครือข่ายประสาทเทียม (Artificial Neural Network) คือ แบบจำลองทางคณิตศาสตร์ที่ออกแบบมาเพื่อเลียนแบบการทำงานของเครือข่ายเซลล์ประสาทในสมองของมนุษย์ โดยอิงตามกฎ วิธีทางสถิติ และเทคนิคอื่น ๆ เพื่อให้สามารถสร้างภาพใหม่หรือแนวคิดใหม่ได้

๒.๓ แนวความคิดกับปัญญาประดิษฐ์

จุดเปลี่ยนครั้งสำคัญของ AI ในยุคนี้ เริ่มในปี ค.ศ. ๒๐๑๒ (พ.ศ. ๒๕๕๕) ซึ่งถือว่าเป็นการค้นพบที่เป็นความคืบหน้าครั้งสำคัญของ AI ที่เรียกว่า การเรียนรู้เชิงลึก (Deep Learning) ทั้งนี้โลกรู้จัก AI มาตั้งแต่ช่วงกลางทศวรรษ ๑๙๕๐ แต่มีข้อจำกัดหลายอย่างที่ทำให้ไม่สามารถพัฒนาได้เร็วเท่าที่ควร แนวความคิดการพัฒนาเทคโนโลยี AI ในยุคแรกแบ่งออกเป็น ๒ แนวทาง คือ Rule-Based และ Neural Networks ในสมัยก่อน AI ตามแนวทาง Rule-Based เป็นที่ยอมรับมากกว่า กล่าวคือ เป็นการสอนให้ AI เรียนรู้ถึงหลักการ, ทฤษฎี และหาคำตอบโดยยึดหลักการที่ถูกป้อนข้อมูล แต่มีข้อจำกัดที่ไม่สามารถทำงานที่ซับซ้อนได้มากนัก ส่วนแนวทางแบบ Neural Networks เปรียบเทียบได้กับการเรียนรู้ของเครื่องจักรที่ได้จากประสบการณ์ ยิ่งมีการป้อนข้อมูลให้มากเท่าไร ก็จะมีความถูกต้องแม่นยำมากขึ้นเท่านั้น จึงเป็นที่มาของแนวทางการพัฒนา AI ในปัจจุบันโดยมีชื่อใหม่ที่รู้จักในวงกว้างว่า Deep Learning ซึ่งจัดเป็นส่วนหนึ่งของ Machine Learning หรือ การเรียนรู้ของเครื่องจักร มีวิธีการทำงานที่แตกต่างแบบตรงกันข้ามกับการปฏิบัติการในรูปแบบโปรแกรมคอมพิวเตอร์แบบดั้งเดิม

ปัญญาประดิษฐ์ถูกพัฒนาขึ้นอย่างต่อเนื่องในปี ค.ศ. ๒๐๑๕ (พ.ศ. ๒๕๕๘) เทคโนโลยีปัญญาประดิษฐ์เป็นที่น่าสนใจอยู่ในกระแสการเปลี่ยนแปลงเทคโนโลยีของโลก เนื่องจากเทคโนโลยี AI เป็นความพยายามของมนุษย์ในการพัฒนาสิ่งที่ไม่มีชีวิตให้มีระบบประมวลผลหรือเสมือนการใช้สติปัญญาทัดเทียมมนุษย์ นักวิทยาศาสตร์จึงได้มีการศึกษาแนวคิดด้านความฉลาดของมนุษย์ควบคู่ไปกับเทคโนโลยี ตามทฤษฎีการจัดการความรู้ของมนุษย์ ที่แบ่งความรู้ออกเป็น ๒ ประเภท คือ ๑.) ความรู้ชัดแจ้ง (Explicit Knowledge) ที่เป็นรูปธรรมและสามารถถ่ายทอดความรู้ให้ผู้อื่นได้ และ ๒.) ความรู้ที่ซ่อนอยู่ในตัวปัจเจกบุคคล (Tacit Knowledge) ยากต่อการถ่ายทอด ในด้านการพัฒนา AI มีแนวคิดในการสร้างความฉลาดให้แก่ AI เช่นกัน โดยเป็นการถ่ายทอดความรู้ให้แก่ AI โดยเฉพาะความรู้ที่เป็นแบบชัดแจ้ง (Explicit Knowledge) เท่านั้น ซึ่งการสร้างความฉลาดให้แก่ AI มี ๒ รูปแบบ คือ ๑.) ความฉลาดจากฐานความรู้ (Knowledge – Based System) เป็นการใช้ความรู้ที่เกิดจากการเรียนรู้และประสบการณ์ ซึ่งเป็นความรู้ที่สามารถถ่ายทอดได้ การสร้างความฉลาดเชิงความรู้ให้ AI มุ่งเน้นการสร้างคลังความรู้และคลังเครื่องมือในการแก้ปัญหา และ ๒.) ความฉลาดเชิงคำนวณ (Computational Intelligence) เป็นการสร้างรูปแบบในการประเมินคำตอบที่มีความแม่นยำ เพื่อแก้ปัญหาที่ไม่สามารถนำความแน่นอนทางตรรกะมาใช้ได้ ที่มีขั้นตอนการปรับปรุงแก้ไขปัญหาที่เป็นอัตโนมัติ นอกจากนี้สภาพเศรษฐกิจโลก (World Economic Forum) ได้คาดการณ์ไว้ว่า เทคโนโลยีปัญญาประดิษฐ์ และ Big Data Analytic จะมีขีดความสามารถอันทรงพลังในช่วงปี พ.ศ. ๒๕๖๘ - พ.ศ. ๒๕๗๓

ประเภทของปัญญาประดิษฐ์ (AI) แบ่งออกได้เป็น ๓ ประเภท คือ ๑.) ปัญญาประดิษฐ์เฉพาะทาง (Narrow AI) มีความสามารถในการทำงานเฉพาะทางได้ดีกว่ามนุษย์ เช่น AI ที่ช่วยในการผ่าตัด เป็นต้น ๒.) ปัญญาประดิษฐ์ทั่วไป (General AI) มีความสามารถในการทำงานและการใช้ความคิดเทียบเท่ากับมนุษย์ ๓.) ปัญญาประดิษฐ์ที่แข็งแรง (Strong AI) มีความสามารถทำงานได้ดีกว่ามนุษย์ ปัญญาประดิษฐ์เป็นเครื่องมือที่ก่อให้เกิดรายได้และสามารถใช้ได้หลากหลายในด้านอุตสาหกรรม

๒.๔ การใช้ปัญญาประดิษฐ์ (AI) ในมิติด้านความมั่นคง

ประเทศมหาอำนาจต่างมีแนวโน้มในการพัฒนาปัญญาประดิษฐ์เพื่อใช้ในการทำสงคราม เนื่องจากมีความพร้อมหลายด้าน โดยเฉพาะประเทศสหรัฐอเมริกากับประเทศจีนต่างแข่งขันการเป็นมหาอำนาจทาง AI สหรัฐฯ ต้องการเป็นมหาอำนาจทางปัญญาประดิษฐ์ ขณะที่จีนต้องการเป็นผู้นำแห่งโลกปัญญาประดิษฐ์ ภายในปี พ.ศ. ๒๕๗๓ กองทัพในหลายประเทศได้มีการประยุกต์ใช้ปัญญาประดิษฐ์ในภารกิจทางทหารในทุกพื้นที่ปฏิบัติการ ทำให้ปัญญาประดิษฐ์เข้ามามีส่วนช่วยในการสนับสนุนการรบ โดยการใช้การเรียนรู้ของเครื่องจักร (Machine Learning) เช่น ระบบควบคุมบังคับบัญชา ระบบเฝ้าระวังภัยและการตระหนักรู้ถึงสถานการณ์ และการส่งกำลังบำรุง เป็นต้น นอกจากนี้ปัญญาประดิษฐ์ สามารถช่วยในภารกิจอื่นที่ต้องอาศัยทรัพยากรทางทหาร ทั้งยุทโธปกรณ์และกำลังพล ได้แก่ ภารกิจในการช่วยเหลือด้านมนุษยธรรมและการบรรเทาภัยพิบัติ ซึ่งสามารถใช้ AI ในการสร้างแผนที่บริเวณที่ประสบภัยพิบัติได้อย่างรวดเร็ว และสามารถประเมินความเร่งด่วนของผู้ประสบภัยได้อีกด้วย

ปัญญาประดิษฐ์ หรือ AI เข้ามามีบทบาทอย่างมากในชีวิตประจำวันอย่างหลีกเลี่ยงไม่ได้ ทุกองค์กรมีความจำเป็นที่จะต้องปรับตัวให้สามารถนำปัญญาประดิษฐ์มาเพิ่มประสิทธิภาพให้กับองค์กร โดยจะต้องมีการปรับทัศนคติของคนในองค์กรให้เปิดใจยอมรับการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ ดังนั้น การนำปัญญาประดิษฐ์มาพัฒนาและปรับใช้ต้องขึ้นอยู่กับจริยธรรมของผู้สร้างปัญญาประดิษฐ์ ทั้งนี้การนำปัญญาประดิษฐ์มาใช้จะมีทั้งประโยชน์และมีความเสี่ยง โดยจะต้องมีการควบคุมและกำกับดูแลโดยหน่วยงานด้านความมั่นคงที่เกี่ยวข้อง

๓. แนวโน้มและทิศทางการใช้ปัญญาประดิษฐ์ (AI)

ภาพที่ ๒ *ปัจจุบันมีการกำหนดเกณฑ์การใช้คลาวน์ (Cloud) ในไทย*

การคาดการณ์แนวโน้มการใช้งาน AI ในปี พ.ศ. ๒๕๖๘ นักวิชาการได้คาดการณ์ทิศทางการพัฒนาของ AI ที่สำคัญ ได้แก่ การปรับแต่งเฉพาะบุคคลขั้นสูง AI จะมีการปรับแต่งที่ซับซ้อนมากขึ้น โดยระบบมีความสามารถในการสร้างเนื้อหาและประสบการณ์ที่ปรับแต่งเฉพาะบุคคล โดยอิงจากการวิเคราะห์ข้อมูลแบบเรียลไทม์ (Real Time) ซึ่งอาจมีการบูรณาการ AI เข้ากับเทคโนโลยีที่ผสมผสานระหว่างโลกเสมือนและโลกแห่งความเป็นจริง (Augmented Reality) และเทคโนโลยีความจริงเสมือน (Virtual Reality) เพื่อเสริมประสบการณ์เฉพาะบุคคล ในเรื่องการรักษาความปลอดภัยของแอปพลิเคชันจะถูกยกระดับมากขึ้น AI สามารถนำไปใช้ เพื่อปรับปรุงมาตรการด้านความปลอดภัยของแอปพลิเคชัน หรือการจำลองภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เพื่อเป็นการเตรียมความพร้อมและรองรับภัยคุกคามในรูปแบบใหม่

๓.๑ แนวโน้มของปัญญาประดิษฐ์ในภาคพลเรือน

ในภาคพลเรือน มีรายงานผลการวิจัยพบว่า AI ช่วยในการอ่านผล X-ray ที่มีประสิทธิภาพมากยิ่งขึ้น มีการใช้ในการจัดลำดับคิวในการรักษาพยาบาล ช่วยในการวิเคราะห์ การจำแนกโรคและการพบแพทย์ที่เชี่ยวชาญในโรคนั้น ๆ ซึ่งเห็นได้ว่า AI มีความใกล้ตัวมากยิ่งขึ้น ส่วนในด้านอุตสาหกรรมป้องกันประเทศ AI ถูกนำมาใช้ในการบริหารจัดการเพิ่มมากขึ้น ยกตัวอย่างเช่น บริษัทที่เป็นผู้ผลิตอุปกรณ์ไฟฟ้านำ AI มาใช้ในการประมวลผล ช่วยในเรื่องการคำนวณต้นทุนในการจัดซื้ออุปกรณ์ และในอุตสาหกรรมเหล็กกล้ามีการนำ AI มาใช้ในกระบวนการผลิต จึงสามารถสรุปได้ว่าปัจจุบันมีการใช้ AI ที่มีความเชี่ยวชาญเฉพาะทางมากยิ่งขึ้น

แนวโน้มของปัญญาประดิษฐ์ในภาคพลเรือน (ข้อมูลจาก นวพร เหมือนประสาท ในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร) รูปแบบของปัญญาประดิษฐ์ (AI) ที่ใกล้ตัวมากที่สุด คือ การใช้โทรศัพท์มือถือ เมื่อต้องการค้นหาข้อมูลในเว็บไซต์หรือแอปพลิเคชันต่าง ๆ จะขึ้นข้อมูลในสิ่งที่ผู้ใช้สนใจ หรือได้พูดผ่านโทรศัพท์มือถือ ซึ่งถือได้ว่าเป็นรูปแบบของ AI ที่ใกล้ตัวมากที่สุด ตัวอย่างที่เห็นได้ชัดเจน คือ การทำงานของมิจฉาชีพ มิจฉาชีพมีการใช้ AI ในการหลอกลวง โดยการนำเสียงของผู้ใช้ไปดัดแปลงเพื่อที่จะไปหลอกลวงบุคคลใกล้ตัวของผู้ใช้ ดังนั้นในภาคพลเรือนจึงควรมีการเรียนรู้การใช้ AI ในเรื่องการเพิ่มศักยภาพในการทำงาน ในภาคพลเรือนจึงจำเป็นต้องมีความกระตือรือร้นที่ต้องศึกษาในเรื่องที่สำคัญ ไม่ว่าจะเป็นการทำคอนเทนต์ (Content) การคิดวิเคราะห์และการศึกษา AI เมื่อมีการศึกษา AI จะทำให้เกิดความเข้าใจและสามารถนำข้อมูลมาวิเคราะห์และประยุกต์ใช้ในการปฏิบัติงานได้อย่างเหมาะสมต่อไป

แนวโน้มการใช้ปัญญาประดิษฐ์ในปัจจุบันเริ่มมีการใช้แชตบอต (Chatbot) ในหน่วยงานต่าง ๆ มากขึ้น ซึ่งเป็นรูปแบบหนึ่งของปัญญาประดิษฐ์ เป็นรูปแบบแอปพลิเคชันที่เลียนแบบการสนทนาของมนุษย์ โดยระบบแชตบอตสามารถประมวลผลในรูปแบบภาษาไทยแล้วตอบโต้กับมนุษย์ได้ ที่เห็นได้ชัดเจน คือ ในหลายหน่วยงานนำแชตบอตมาใช้เพื่อแทนที่พนักงานคอลเซนเตอร์ในการตอบคำถามลูกค้า จะเห็นได้ว่าเทคโนโลยี AI ได้ก้าวสู่อุตสาหกรรมด้านต่าง ๆ โดยเข้ามาแทนที่มนุษย์และส่งผลกระทบต่อการจ้างงานในบางประเภท ดังนั้น การเรียนรู้เท่าทันเทคโนโลยีเป็นสิ่งสำคัญยิ่ง เพื่อเป็นการเตรียมความพร้อมในการปรับตัวให้สามารถรองรับการเปลี่ยนแปลงเทคโนโลยีที่ทันสมัย ก้าวล้ำในอนาคต

๓.๒ แนวโน้มปัญญาประดิษฐ์ด้านการทหาร

แนวโน้มการใช้ปัญญาประดิษฐ์ (ข้อมูลจาก น.ท. กนก บุนนาค ในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร) ยุโรปมองว่าสงครามในอนาคต สิ่งที่มีบทบาทที่สำคัญคือ เทคโนโลยีดิจิทัลมีผลกระทบต่อสงครามในอนาคต แนวโน้มเทคโนโลยีปัญญาประดิษฐ์ (AI) ทางการทหารในระยะเวลา ๕ ปี มีผลต่อการเพิ่มศักยภาพ ในเรื่องการเพิ่มความเร็วอัตโนมัติ การใช้งานในเชิงของอุปกรณ์ต่าง ๆ การใช้งานเชิงการตัดสินใจ, การควบคุมบังคับบัญชา, การติดต่อสื่อสาร, เพิ่มความรวดเร็วแบบ Real Time (การประมวลผลหรือการแสดงผลข้อมูลที่เกิดขึ้นทันที) ประเทศสหรัฐอเมริกาเริ่มใช้ปัญญาประดิษฐ์ช่วยในการตัดสินใจของผู้บังคับบัญชาแล้ว โดยมีการพัฒนาโปรแกรมและทดสอบการใช้งาน จะเห็นได้ว่าปัญญาประดิษฐ์เป็นการปฏิสัมพันธ์ระหว่างมนุษย์กับเครื่องจักรซึ่งจะมีเพิ่มมากขึ้น สำหรับแนวโน้มการใช้ปัญญาประดิษฐ์ในปัจจุบัน ยังคงมีคนเข้ามามีส่วนร่วมในการดำเนินการ โดยเฉพาะในการตัดสินใจขั้นสุดท้าย ปัจจุบันเริ่มมีการนำ AI มาใช้ในงานความมั่นคงด้านการทหารในบริบทของสงครามสมัยใหม่ AI สามารถช่วยในการให้ข้อเสนอแนะและนำข้อมูลมาประมวลผล วิเคราะห์สถานการณ์ต่าง ๆ ได้

กรณีศึกษาที่เห็นได้ชัดเจน ได้แก่ สงครามรัสเซียกับยูเครน, ความขัดแย้งระหว่างอิสราเอลกับกลุ่มฮามาส โดย AI มีบทบาทใช้ในการรวบรวมข้อมูล, วิเคราะห์ข้อมูล และประมวลผลข้อมูล เพื่อช่วยให้ข้อเสนอแนะในการตัดสินใจของผู้บังคับบัญชา นอกจากนี้ยังมีการใช้ปัญญาประดิษฐ์ในเรื่องปฏิบัติการไซเบอร์ การใช้ AI ในเชิงจิตวิทยา รวมถึงการใช้ AI ในลักษณะที่เป็นระบบ

อัตโนมัติ กล่าวคือ ในปัจจุบันยุทโธปกรณ์มีการติดตั้ง AI ให้สามารถประมวลผล สามารถเชื่อมโยงระหว่างการปฏิบัติการของยุทโธปกรณ์กับระบบประมวลผลข้อมูลเพื่อช่วยให้เป็นข้อเสนอแนะในการตัดสินใจของผู้บังคับบัญชา

ภาพที่ ๓ *โดรน S-70 Okhotnik-B ของรัสเซีย และ Iron Dome ของอิสราเอล*

ในการปฏิบัติการทางทหาร มีการนำเทคโนโลยีโดรนมาใช้ในการปฏิบัติการ นอกจากการนำเทคโนโลยี AI มาใช้ในสงครามรัสเซียกับยูเครน รัสเซียมีการใช้โดรนล่องหน S-70 “Okhotnik-B” ซึ่งเป็นตัวอย่างเทคโนโลยีอากาศยานไร้คนขับขนาดใหญ่ที่รัสเซียพัฒนาขึ้น เพื่อใช้ร่วมกับเครื่องบินขับไล่ โดรนรุ่นนี้มีขนาดใหญ่และพิสัยการรบไกล ถูกออกแบบให้ทำหน้าที่เป็น “เพื่อนร่วมรบ” (Loyal Wingman) เป็นอากาศยานไร้คนขับ โดยมีนักบินช่วยเปิดทางหรือโจมตีเป้าหมายที่มีความเสี่ยงแทนนักบินมนุษย์ กรณีสงครามอิสราเอลกับกลุ่มฮามาส เทคโนโลยีโดรนที่เห็นได้ชัดเจนคือ Iron Dome ของอิสราเอล ซึ่งใช้โดรนในการคำนวณ การวิเคราะห์เป้าหมาย ช่วยเรื่องการตัดสินใจในการยิง แนวโน้มการใช้โดรนของอิสราเอล ปัจจุบันมีการใช้เป็นตัวล่อเป้า ใช้โจมตีเป้าที่เป็นเรดาห์ เพื่อรบกวนการทำงานของเรดาห์ และตามด้วยมีการยิงมิสไซล์เข้าโจมตีเป้าหมายอีกทั้งยุทโธปกรณ์สมัยใหม่จะมี AI เป็นเซนเซอร์ (Sensor) ใช้ตรวจจับและวัดระยะทางอีกด้วย

จะเห็นได้ว่าสงครามและความขัดแย้งในยุคปัจจุบันได้มีการนำเทคโนโลยีปัญญาประดิษฐ์มาทดสอบและประยุกต์ใช้งานในสนามรบ โดยมีตัวอย่างที่เห็นได้ชัด จากสงครามรัสเซีย-ยูเครน และความขัดแย้งระหว่างอิสราเอล-กลุ่มฮามาส ที่มีการประยุกต์ใช้ปัญญาประดิษฐ์ในการสู้รบ เพื่อการช่วงชิงความได้เปรียบในการปฏิบัติการทางทหาร และเพื่อลดความแตกต่างของศักย์สงครามระหว่างคู่กรณี

แนวโน้มการใช้ปัญญาประดิษฐ์ (AI) ของกองทัพบก (ข้อมูลจาก พ.อ. อภิชา ศรีจิระภาส ในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร) เริ่มแรกกองทัพบกมีการสร้างปัญญาประดิษฐ์ในกลุ่มเล็ก ๆ ก่อนในลักษณะของการจำลองสนามรบเพื่อใช้ในการฝึก การนำปัญญาประดิษฐ์มาใช้ในกองทัพบกต้องอาศัยปัจจัย ดังนี้ ๑.) มีความเข้าใจในเทคโนโลยี ๒.) มีข้อมูลที่ถูกต้อง และ ๓.) คอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอ จะเห็นได้ว่าปัจจุบันกองทัพกำลังเผชิญสมรภูมิการรบที่มีรูปแบบเปลี่ยนแปลงไป จากเดิมเป็นศัตรูที่อยู่ตรงหน้า แต่ปัจจุบันศัตรูได้เปลี่ยนแปลงไป ไม่ใช่แค่มิติทางบก ทางเรือ ทางอากาศ แต่ในปัจจุบันเป็นมิติทางดิจิทัลหรือทางข้อมูล ซึ่งถือได้ว่าเป็นมิติใหม่ กองทัพบกจะต้องเตรียมความพร้อม จะต้องเรียนรู้ปัญญาประดิษฐ์เพื่อสร้างความเข้าใจ เพราะในปัจจุบันเป็นสิ่งที่ใกล้ตัวมาก และต้องมีความเข้าใจบริบทของสงครามในปัจจุบัน เข้าใจในสงครามรูปแบบใหม่ ซึ่งหน่วยงานที่เกี่ยวข้องของกองทัพบกกำลังสร้างและทำความเข้าใจ บทบาทด้านการทหารของปัญญาประดิษฐ์ (AI) ช่วยพัฒนาให้การทหารมีความทันสมัยมากขึ้น สามารถวิเคราะห์ภัยคุกคามและตัดสินใจได้อย่างรวดเร็ว และยังมีการนำปัญญาประดิษฐ์มาใช้ในการฝึกร่วม

ภาพที่ ๔ *เทคโนโลยีชีวภาพกับเทคโนโลยีควอนตัม*

นอกเหนือจากการเริ่มต้นนำเทคโนโลยีดิจิทัลมาใช้ในการจำลองสนามรบโลกในปัจจุบันมีการแข่งขันด้านเทคโนโลยีที่มีความรุนแรงมากยิ่งขึ้น ระบบ AI ถูกนำมาใช้ในการโจมตี โดยปัญญาประดิษฐ์มีความสามารถในการตรวจจับและหยุดขีปนาวุธหรือโดรนได้อย่างรวดเร็วและมีประสิทธิภาพ สนามรบปัจจุบันมีเทคโนโลยีสำคัญที่ถูกนำมาใช้ ได้แก่ ปัญญาประดิษฐ์ (AI), เซมิคอนดักเตอร์ (Semiconductor), ควอนตัมคอมพิวติ้ง (Quantum Computing) และเทคโนโลยีชีวภาพ (Biotechnology) ซึ่งการแข่งขันทางเทคโนโลยีอาจนำไปสู่สงครามเย็นรูปแบบใหม่ในอนาคตได้

๔. ภัยคุกคามของปัญญาประดิษฐ์ (AI) กับผลกระทบด้านความมั่นคง

๔.๑ ผลกระทบด้านความมั่นคงและการรับมือกับภัยคุกคามของปัญญาประดิษฐ์ (AI)

ภัยคุกคามด้านปัญญาประดิษฐ์ มีการพัฒนาด้านเทคนิคเพื่อใช้ในการหลอกลวงต่าง ๆ ที่เห็นได้ชัดเจน คือ กระบวนการทำงานของแก๊งคอลเซนเตอร์ (Call Center) และในปัจจุบันมีสื่อโซเชียลมีเดียทำให้การควบคุม AI เป็นไปได้ยากขึ้นและมีความเสี่ยง ดังนั้นจึงต้องมีกฎหมายควบคุม AI จึงมีพระราชบัญญัติ AI ได้กำหนดสิ่งต้องห้าม มีสาระสำคัญ ได้แก่ การใช้เทคนิคการหลอกลวงข้อมูลทำให้การตัดสินใจเสียหาย จนก่อให้เกิดอันตรายร้ายแรง ห้ามแสวงหาผลประโยชน์จากจุดอ่อนที่เกี่ยวข้องกับอายุหรือสถานการณ์ทางเศรษฐกิจและสังคม รวมทั้งห้ามใช้ AI เพื่อประมวลผลข้อมูลที่อ่อนไหว

ในเรื่องการใช้ AI ในสงครามจิตวิทยา (ข้อมูลจาก พ.อ. อภิชา ศรีจิระภาส) ต้องมีการวิเคราะห์ แยกแยะ ประเด็นของข่าวสาร ว่าเป็นข่าวจริงหรือข่าวปลอม ลำดับแรกหน่วยงานด้านความมั่นคง ไม่ว่าจะเป็นทหารหรือตำรวจจะต้องทำการแยกแยะข่าวจริงกับข่าวปลอม ก่อนที่จะมีการส่งข่าวต่อ หลังจากนั้นภาคพลเรือนควรมีสติในการรับรู้ข่าวสารก่อนที่จะมีการแชร์หรือเผยแพร่ข้อมูลออกไป และที่สำคัญคือจะต้องมีหน่วยงานกลางที่เข้าไปตรวจสอบความถูกต้องของข่าว ดังนั้น ขั้นตอนแรกของการแก้ไขปัญหา คือ หน่วยทหารจะต้องตรวจสอบข้อเท็จจริงของข่าวสารให้ได้ และระดับสุดท้าย คือ ระดับรัฐบาลควรจัดตั้งหน่วยงานต่อต้านข่าวปลอม

ในปัจจุบันเริ่มมีการเผชิญกับการต่อสู้ในลักษณะของชิป (Chip) ซึ่งเป็นรากฐานของเทคโนโลยีสมัยใหม่ ชิปเป็นชิ้นส่วนสำคัญในอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ยกตัวอย่าง ยูเครนใช้โดรนในสนามรบ ใช้ควบคุม ตรวจสอบ และตอบโต้ภัยคุกคาม ยูเครนมีชิป สหรัฐอเมริกาได้ส่งชิปให้ยูเครน มีการใช้โดรนโดยใช้ชิปในการควบคุมทั้งแบบออนไลน์และออฟไลน์

ในการรับมือกับภัยคุกคามของปัญญาประดิษฐ์ เริ่มแรกจะต้องมีการเรียนรู้ให้เกิดความรู้ ความเข้าใจถึงการใช้งาน แนวโน้ม รวมถึงผลกระทบด้านความมั่นคง การใช้ปัญญาประดิษฐ์เข้ามาเป็นส่วนหนึ่งในสงครามจิตวิทยาทำให้กระทรวงกลาโหมได้ตระหนักถึงภัยด้านความมั่นคงของปัญญาประดิษฐ์ในมุมมองด้านความมั่นคง (ข้อมูลจาก พ.อ. จารุกฤษณ์ เรืองสุวรรณ ในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร) กระทรวงกลาโหมได้มีการรับรู้และตระหนักถึงภัยคุกคามของปัญญาประดิษฐ์ (AI) เพื่อเตรียมตัวรับมือ ซึ่งการใช้ AI ต้องควบคู่ไปกับเรื่องจริยธรรมด้วย จะเห็นได้ว่าปัญญาประดิษฐ์ถูกนำมาใช้ในการบิดเบือนข้อมูลข่าวสาร เช่น การใช้ AI ตัดต่อภาพทหาร

ซึ่งทำให้เกิดความเข้าใจผิด เป็นต้น ส่งผลทำให้หน่วยงานด้านความมั่นคงของไทยต้องพิจารณาแนวทางการกำกับควบคุมดูแลเกี่ยวกับการนำปัญญาประดิษฐ์มาใช้ โดยพิจารณานำแนวทางการปฏิบัติด้านนโยบายเกี่ยวกับปัญญาประดิษฐ์ (OECD AI Principles) ซึ่งเป็นหลักสากลทั่วไป มีแนวปฏิบัติที่สำคัญ ได้แก่ ๑.) ปัญญาประดิษฐ์ควรมีประโยชน์ต่อคนและโลก ๒.) ปัญญาประดิษฐ์ควรออกแบบให้เคารพหลักนิติธรรม สิทธิมนุษยชน ค่านิยม และประชาธิปไตย และมีการป้องกัน ๓.) ปัญญาประดิษฐ์ควรมีความโปร่งใสและเปิดเผยข้อมูล

๔.๒ ท่าทีของประเทศมหาอำนาจกับการรับมือภัยคุกคามปัญญาประดิษฐ์

องค์การสนธิสัญญาแอตแลนติกเหนือ (NATO) ประกาศเพิ่มงบประมาณด้านการป้องกันประเทศ สำนักข่าวต่างประเทศ รายงานว่า บรรดาผู้นำของชาติสมาชิกนาโต ประกาศสนับสนุนการเพิ่มงบประมาณด้านการป้องกันประเทศเป็นร้อยละ ๕ ของผลิตภัณฑ์มวลรวมในประเทศ หรือ จีดีพี (GDP) สำหรับค่าใช้จ่ายด้านการป้องกันประเทศ ตามข้อเสนอของประธานาธิบดี โดนัลด์ ทรัมป์ ของสหรัฐอเมริกา ระหว่างการประชุมสุดยอดนาโต (NATO) ที่ กรุงเฮก ประเทศเนเธอร์แลนด์ เมื่อวันที่ ๒๕ มิถุนายน พ.ศ. ๒๕๖๘ ทั้งนี้ สมาชิกนาโต ๓๒ ประเทศยังยืนยันความมุ่งมั่นอันแน่วแน่ต่อการป้องกันประเทศร่วมกัน ตามบทบัญญัติที่ ๕ ของสนธิสัญญานาโต ที่ระบุไว้ว่า “การโจมตีสมาชิกนาโต ประเทศใดประเทศหนึ่ง เท่ากับเป็นการโจมตีสมาชิกนาโตทั้งหมด” ซึ่งผู้นำของสหรัฐฯ ต้องการเพิ่มงบประมาณด้านการป้องกันประเทศของสมาชิกนาโต ถือเป็นชัยชนะที่ยิ่งใหญ่และมุ่งหวังว่างบประมาณที่เพิ่มขึ้นจะถูกนำไปซื้ออาวุธยุทโธปกรณ์ที่ผลิตในสหรัฐฯ เพื่อรับมือกับสงครามที่นำปัญญาประดิษฐ์มาใช้มากขึ้น

๔.๓ ผลกระทบปัญญาประดิษฐ์ (AI) ต่อความปลอดภัยไซเบอร์ (Cyber Security)

ในยุคที่ปัญญาประดิษฐ์กำลังเปลี่ยนแปลงอุตสาหกรรมต่าง ๆ อย่างรวดเร็ว ทั้งแฮ็กเกอร์ (Hacker) ที่มีความซับซ้อนมากขึ้น รูปแบบการโจมตีที่หลากหลาย การโจมตีโครงสร้างพื้นฐานที่เพิ่มขึ้น ถึงแม้ว่าเทคโนโลยี AI จะมีคุณสมบัติและประโยชน์ที่เป็นระบบอัตโนมัติ และมีความสามารถในการวิเคราะห์เชิงคาดการณ์ อย่างไรก็ตาม AI ยังมีช่องว่างหรือเป็นเครื่องมือของอาชญากรไซเบอร์สามารถใช้ประโยชน์ที่ส่งผลกระทบต่อด้านความมั่นคง ทำให้ระบบความปลอดภัยทางไซเบอร์เผชิญกับความท้าทายมากยิ่งขึ้น

ภาพที่ ๕ *ปัญญาประดิษฐ์ (AI) กับผลกระทบต่อความปลอดภัยไซเบอร์ (Cyber Security)*

การโจมตีทางไซเบอร์ที่ขับเคลื่อนด้วย AI อาชญากรไซเบอร์สามารถใช้ AI เพื่อทำให้การโจมตีเป็นอัตโนมัติ และหลบเลี่ยงการป้องกันด้านความปลอดภัย เนื่องจากระบบ AI ต้องใช้ชุดข้อมูลขนาดใหญ่เพื่อทำงานได้อย่างมีประสิทธิภาพ ทำให้เกิดข้อกังวลเกี่ยวกับความเป็นส่วนตัวของผู้ใช้และการปกป้องข้อมูล ดังนั้น องค์กรจึงต้องมีกลยุทธ์ในการเพิ่มความมั่นคงปลอดภัยทางไซเบอร์ เพื่อบรรเทาความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่ขับเคลื่อนด้วย AI กลยุทธ์ที่สำคัญ ได้แก่ ๑.) ใช้เครื่องมือที่ขับเคลื่อนด้วย AI เพื่อตรวจจับภัยคุกคาม การประเมินความเสี่ยง และการตอบสนองต่อเหตุการณ์ ๒.) เสริมสร้างมาตรการการเข้าถึงข้อมูลหรือปกป้องข้อมูล และปฏิบัติตามกฎระเบียบด้านความเป็นส่วนตัวของข้อมูล ๓.) ส่งเสริมความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ให้กับบุคลากรในหน่วยงานและผู้ใช้เกี่ยวกับภัยคุกคามที่เกี่ยวข้องกับ AI และแนวทางการปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัย ๔.) พัฒนานโยบาย AI ที่มีจริยธรรม และ ๕.) กำหนดแนวทางในการใช้งาน AI อย่างมีความรับผิดชอบและปลอดภัย

อย่างไรก็ตาม ในเรื่องการสงครามปัญญาประดิษฐ์ยังไม่สามารถมาแทนที่มนุษย์ได้ เนื่องจาก AI ไม่มีหัวใจเป็นนักรบและไม่มีความเป็นผู้นำ ปัญญาประดิษฐ์ตัดสินใจจากข้อมูลที่มี เป็นเพียงเครื่องมือที่นำมาใช้ในสนามรบ ดังนั้น มนุษย์จึงมีหน้าที่ควบคุมการตัดสินใจของปัญญาประดิษฐ์ การนำปัญญาประดิษฐ์มานำและตกลงใจแทนมนุษย์ในการทำสงคราม จึงยังคงอีกนานที่จะกระทำได้ ขณะเดียวกันเทคโนโลยี AI ยังคงพัฒนาไปข้างหน้าอย่างต่อเนื่อง มาตรการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพจะเป็นสิ่งสำคัญที่ทุกองค์กรจะต้องมีเพื่อรับมือกับภัยคุกคามปัญญาประดิษฐ์

๔. การประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ในมิติด้านความมั่นคง

การประยุกต์ใช้งานปัญญาประดิษฐ์ของประเทศไทยจาก (ข้อมูลของศูนย์ธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance Center หรือ AIGC) ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)) ที่ได้เผยผลสำรวจความพร้อมในการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์สำหรับบริการดิจิทัลประจำปี พ.ศ. ๒๕๖๗ ระบุว่า สัดส่วนขององค์กรไทยที่ประยุกต์ใช้งาน AI เพิ่มขึ้น ๑๗.๘% จากปี พ.ศ. ๒๕๖๖ และยังมีองค์กรที่จะเตรียมใช้งาน AI ในอนาคตสูงถึง ๗๓.๓%

การประยุกต์ใช้ปัญญาประดิษฐ์ (AI) กรณีศึกษาการใช้เทคโนโลยี AI ของสหรัฐอเมริกา ซึ่งสหรัฐฯ ถือได้ว่าเป็นชาติแรก ๆ ที่มีการประยุกต์ใช้ปัญญาประดิษฐ์ด้านความมั่นคง เนื่องจากสหรัฐฯ เป็นประเทศที่มีต้นทุน มีทรัพยากร และมีเงินทุนด้านการวิจัยและพัฒนาค่อนข้างมาก รวมทั้งสหรัฐฯ ได้มีการกำหนดยุทธศาสตร์การประยุกต์ใช้ข้อมูลวิเคราะห์ AI เมื่อปี ค.ศ. ๒๐๒๓ (พ.ศ. ๒๕๖๖) โดยเริ่มใช้งานเชิงธุรกิจก่อน เพื่อช่วยในการประมวลผลการทำงาน นอกจากนี้สหรัฐฯ ยังได้จัดตั้งหน่วยงานที่ทำงานด้านปัญญาประดิษฐ์ขึ้นโดยเฉพาะภายใต้กระทรวงกลาโหมของสหรัฐฯ แนวคิดของสหรัฐฯ คือ ต้องการใช้ระบบ AI เป็นโครงสร้างพื้นฐานสำคัญ และมีแนวทางการใช้ AI อย่างเป็นระบบ และสหรัฐฯ มีการจัดตั้งกองกำลังเฉพาะกิจเพื่อศึกษาเรียนรู้การประยุกต์ใช้ รวมทั้งสหรัฐฯ ได้มีการทดลองใช้ปัญญาประดิษฐ์ที่ใช้ในการฝึกทางการทหารในปี พ.ศ. ๒๕๖๖ เป็นต้นมา

การประยุกต์ใช้ปัญญาประดิษฐ์ในด้านความมั่นคง (ข้อมูลจาก พ.อ. จารุกฤษณ์ เรืองสุวรรณ) ต้องมีการพิจารณาประเด็นสำคัญดังนี้ ๑.) ความเสี่ยง จะต้องมีการประเมินความเสี่ยงในการใช้งานและจะต้องพิจารณาว่าเป็นการใช้ AI ในลักษณะใดที่มีความเสี่ยงสูง ๒.) ความโปร่งใสที่สามารถชี้แจงฐานข้อมูลในการประมวลผล และ ๓.) ต้องมีคำแนะนำในการปฏิบัติ

นโยบายของโลก ในปี ค.ศ. ๒๐๑๙ (พ.ศ. ๒๕๖๒) เป็นหลักการกว้าง ๆ เกี่ยวกับการประยุกต์ใช้ปัญญาประดิษฐ์ มีสาระสำคัญ คือ ๑.) ควรมีประโยชน์ต่อมนุษย์และโลก ๒.) ปัญญาประดิษฐ์ควรออกแบบให้เคารพต่อหลักนิติธรรม สิทธิมนุษยชน ค่านิยมประชาธิปไตยและมีการป้องกัน ๓.) ปัญญาประดิษฐ์ควรมีความโปร่งใสและเปิดเผยข้อมูล ๔.) ต้องทำงานได้แข็งแกร่งและปลอดภัย มีการประเมินและการจัดการความเสี่ยง และ ๕.) องค์กรหรือบุคคลที่พัฒนาติดตั้ง หรือดำเนินการ AI ต้องรับผิดชอบต่อ AI ที่เกิดขึ้น

ทั้งนี้หลักการที่เกิดขึ้น ๕ ประการ ได้นำไปสู่การพูดคุยในเวทีต่าง ๆ สหรัฐฯ มีหน่วยงานกลางชื่อว่า NIST (National Institute of Standards and Technology) เป็นหน่วยงานที่ออกมาตรฐานการจัดการความเสี่ยงของ AI ว่าควรจะใช้ AI ได้อย่างปลอดภัยอย่างไรบ้าง โดยได้ให้คำจำกัดความ AI ว่าเป็นเครื่องมือที่เป็นลักษณะทางสังคมและเทคนิคร่วมกัน โดยการดำเนินการต้องรับผิดชอบต่อสังคม ดังนั้น การดำเนินการต้องยึดมนุษย์เป็นศูนย์กลาง มีความรับผิดชอบต่อสังคม และมีความยั่งยืนในการใช้งาน หลักการของ NIST ประกอบด้วย ๑.) การกำกับดูแล ๒.) ต้องมีการทำความเข้าใจระบบ ๓.) การประเมินผล และ ๔.) การจัดการ ขณะเดียวกันในปี พ.ศ. ๒๕๖๖ หน่วยงาน ISO (International Organization for Standardization) ซึ่งเป็นหน่วยงานมาตรฐานด้านอุตสาหกรรมได้ออกมาตรฐาน AI ชื่อว่า “AI Management System” ให้การใช้ AI เป็นไปอย่างมีมาตรฐาน ซึ่งเป็นแนวทางการบริหารจัดการ AI

ภาพที่ ๖ *กฎหมายด้านปัญญาประดิษฐ์ของสหภาพยุโรป (EU AI ACT)*

กฎหมายด้านปัญญาประดิษฐ์ของสหภาพยุโรป (EU AI ACT) เป็นกฎหมายด้านปัญญาประดิษฐ์ที่เป็นที่รู้จักอย่างกว้างขวางเป็นที่นิยมและมีการบังคับใช้ทั้งสหภาพยุโรป จึงบีบบังคับให้ประเทศที่ค้าขายกับสหภาพยุโรปต้องดำเนินการตามกฎหมายฉบับนี้ สาระสำคัญ ได้แก่ ๑.) ต้องจำแนกลักษณะการใช้งาน AI โดยจำแนกว่าลักษณะการใช้งานใดที่มีความเสี่ยงสูง ความเสี่ยงปานกลางและความเสี่ยงต่ำ ซึ่งหากมีความเสี่ยงสูงจะไม่นำ AI มาใช้ จะไม่นำไปใช้ในทางที่ผิดจริยธรรมหรือใช้ในทางที่ผิดต่อหลักการสิทธิมนุษยชน ๒.) ความโปร่งใสและความรับผิดชอบของผู้พัฒนา ๓.) การดำเนินการต้องมีคำแนะนำ และคำเตือน มีลิขสิทธิ์ และ ๔.) การประเมินความเสี่ยง

การดำเนินการในระดับรัฐบาล โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งเป็นหน่วยงานของสภาความมั่นคงแห่งชาติ (สมช.) ที่บริหารงานด้านไซเบอร์ มีกฎหมายที่ออกมาบังคับใช้แล้ว คือ หลักเกณฑ์การใช้คลาวด์ในประเทศไทย ทั้งนี้ทางรัฐบาลกำลังพิจารณาแนวทางการใช้ AI ที่ดี เพื่อเป็นกรอบให้ทุกหน่วยงานดำเนินการ ส่วนรัฐบาลมีแนวทางในการขับเคลื่อน AI เพื่อสร้างความพร้อมของประเทศไทยในการรับมือภัยคุกคามปัญญาประดิษฐ์ ในการประชุมคณะกรรมการขับเคลื่อนแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อพัฒนาประเทศไทย ครั้งที่ ๑ ปี พ.ศ. ๒๕๖๘ ได้มีการกำหนดแนวทางการขับเคลื่อนเพื่อให้ประเทศไทยมีระบบนิเวศที่จะสามารถผลักดันให้ประเทศไทยเป็นศูนย์กลางการขับเคลื่อนปัญญาประดิษฐ์ของภูมิภาค และสร้างการเติบโตด้านเศรษฐกิจของประเทศ ช่วงที่ผ่านมาประเทศไทยต้องเผชิญความท้าทาย ซึ่งการที่มีปัญญาประดิษฐ์หรือเทคโนโลยี AI เข้ามามีส่วนช่วยทำให้เศรษฐกิจของไทยดีขึ้น รัฐบาลจึงได้เล็งเห็นว่าเรื่องดังกล่าว เป็นสิ่งที่สำคัญและจำเป็นต้องมีการพัฒนาต่อเนื่อง เพื่อให้ประเทศไทยมีศักยภาพในการแข่งขันกับทั่วโลกได้ โดยมีการแต่งตั้งคณะกรรมการขับเคลื่อนแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติ เพื่อการพัฒนาประเทศไทย (National AI Committee) เพื่อกำหนดแนวทางในการเตรียมความพร้อมในด้านต่าง ๆ ของประเทศไทย โดยเฉพาะอย่างยิ่งการพัฒนากำลังคนด้านปัญญาประดิษฐ์ให้มีจำนวนที่เพียงพอ ซึ่งเป็นปัจจัยพื้นฐาน นอกจากนี้จะมีการส่งเสริมการลงทุนเพื่อพัฒนาโครงสร้างพื้นฐาน ได้แก่ ระบบคลาวด์ ดาต้าเซนเตอร์ และการพัฒนาแพลตฟอร์มปัญญาประดิษฐ์เปิด (Open Source AI Platform) ให้เพียงพอ เพื่อส่งเสริมการขยายตัวของ

การประยุกต์ใช้เทคโนโลยีในราคาที่เหมาะสม รวมไปถึงการจัดตั้งศูนย์ข้อมูลที่จะรวมข้อมูลที่เป็นประโยชน์ต่อการพัฒนาปัญญาประดิษฐ์ในสาขาต่าง ๆ โดยมีนโยบายส่งเสริมให้หน่วยงานของรัฐปรับตัวให้เป็นระบบดิจิทัลทั้งหมดภายในปี พ.ศ. ๒๕๖๙

การประยุกต์ใช้ปัญญาประดิษฐ์ของประเทศไทย (ข้อมูลจาก นวพร เหมือนประสาท) ในเรื่องการสร้าง Cloud First Policy หรือ การขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก ไทยยังอยู่ในระยะเริ่มแรก ดังนั้น ไม่ว่าจะเป็นข้าราชการและประชาชนควรเตรียมความพร้อม โดยเริ่มจากสิ่งใกล้ตัวที่ใช้ได้ง่ายและรวดเร็ว สามารถจับต้องได้ ยกตัวอย่าง การใช้โทรศัพท์มือถือสมาร์ทโฟนและคอมพิวเตอร์ในชีวิตประจำวันโดยใช้งานให้เกิดความเข้าใจ ซึ่งสิ่งสำคัญที่ควรตระหนัก คือ ไม่นำข้อมูลที่เป็นส่วนบุคคล หรือข้อมูลที่เป็นชั้นความลับใส่เข้าไปในแอปพลิเคชันต่าง ๆ

การใช้ปัญญาประดิษฐ์ โลกของการสื่อสารได้เปลี่ยนแปลงไป การรับรู้ข่าวสารจึงเป็นสิ่งที่สำคัญต่อการรับรู้ของบุคคล ข่าวใดที่ถูกใจ ข่าวนั้นเป็นสิ่งที่ถูกต้อง จะเห็นได้ว่าข่าวปลอมจะเร็วกว่าข่าวจริงเสมอ ซึ่งถือว่าเป็นความน่ากลัวของความเร็วของข่าว ซึ่งได้สร้างผลกระทบในวงกว้าง AI ควรถูกป้อนข้อมูลที่เป็นจริงโดยมีการแยกแยะข่าวจริงและข่าวปลอม (Fake News) ดังนั้นควรจะใช้อย่างมีทักษะ ซึ่งมีจุดที่สังเกตได้ว่าสิ่งใดจริงหรือไม่จริง สิ่งที่ควรตระหนัก คือ ๑.) เมื่อพบเห็น ๓ ข้อนี้ได้แก่ “ด่วน, ช็อก, เปิดโปง” ผู้ใช้ต้องตั้งสติและพิจารณาตรวจสอบก่อน ๒.) ข้อมูลออกมาเป็นข้อความโดด ๆ ไม่มีฐานข้อมูลอ้างอิง เช่น ไม่มีชื่อบุคคล เป็นต้น หากไม่มีชื่ออ้างอิง ให้พิจารณาได้ว่าน่าจะเป็นข่าวปลอม โดยพื้นฐานผู้ใช้ไม่สามารถที่จะป้องกันหรือตั้งรับได้เพราะไม่ได้เป็นเจ้าของ

ข้อมูล ซึ่งผู้ที่เป็นเจ้าของข้อมูลในด้านความมั่นคง คือหน่วยงานด้านความมั่นคง หรือกองทัพมีข้อมูลมากที่สุดและสามารถประยุกต์ข้อมูลที่สามารถเปิดเผยกับประชาชนได้ เพื่อไม่ให้เกิดความกลัวและตื่นตระหนก ซึ่งสิ่งเหล่านี้เป็นสิ่งที่ประชาชนต้องการ อย่างไรก็ตาม จะเห็นได้ว่าการใช้ AI นั้นตรวจสอบได้ยากและไม่มีจริยธรรม แต่อย่างน้อยผู้ใช้ต้องตรวจสอบวิเคราะห์ข้อมูลในเบื้องต้น และในภาคเอกชนควรหาแนวทางร่วมกันในเรื่องการส่งต่อข้อมูล

การดำเนินการของกระทรวงกลาโหม หลักการในการควบคุมการใช้ปัญญาประดิษฐ์ที่กล่าวมาข้างต้น จะเป็นกรอบให้กระทรวงกลาโหมนำไปพิจารณาว่าควรดำเนินการเรื่องปัญญาประดิษฐ์อย่างไร กระทรวงกลาโหมได้ตระหนักถึงความสำคัญในการดำเนินการรับมือกับภัยคุกคามของ AI ทั้งนี้ เมื่อปี พ.ศ. ๒๕๖๗ ได้ออกเอกสารสมุดปกขาว (White Paper) มีใจความสำคัญว่าเทคโนโลยีปัญญาประดิษฐ์ (AI) จะเป็นเทคโนโลยีหนึ่งที่จะเข้ามาเปลี่ยนกองทัพร่วมกับคลาวด์ (Cloud) และควอนตัม (Quantum Technology) ซึ่ง ๓ เทคโนโลยีนี้ จะเป็นเทคโนโลยีเป้าหมายสำคัญของกระทรวงกลาโหมที่จะมุ่งเน้นไปในอีก ๒๐ ปีข้างหน้า ดังนั้นแนวทางการดำเนินการของหน่วยงานด้านความมั่นคง จะต้องเป็นแนวทางที่สอดคล้องกับสมุดปกขาว คือ หน่วยงานด้านความมั่นคงที่ใช้ AI เพื่อเพิ่มประสิทธิภาพในการดำเนินการตามภารกิจที่ได้รับมอบหมาย ต้องทำให้ AI สอดคล้องกับหลักการที่มีความรับผิดชอบ ข้อมูลที่ป้อนเข้าไปต้องเป็นข้อมูลที่ยินยอมให้ AI นำไปประมวลผล ดังนั้นข้อมูลที่มีความอ่อนไหว หรือข้อมูลที่เป็นความลับและข้อมูลที่เป็นข้อมูลส่วนตัวจึงไม่เหมาะกับ AI รวมทั้งกระทรวงกลาโหมจะต้องพิจารณาเลือกโมเดลที่เหมาะสมและมีความปลอดภัยที่ได้รับการยืนยันกับทางผู้เชี่ยวชาญว่าโมเดลมีความปลอดภัยและได้รับการยืนยันจากผู้ใช้งาน ซึ่งได้แก่ เหล่าทัพต่าง ๆ ว่า

โมเดลที่นำมาใช้มีความปลอดภัยและเหมาะสม นอกจากนี้หน่วยงานด้านไซเบอร์ถือว่ามีความสำคัญ เนื่องจากต้องใช้ปัญญาประดิษฐ์ผ่านระบบเทคโนโลยี ดังนั้นจึงหลีกเลี่ยงไม่ได้ที่จะต้องมีการเรียนรู้ด้านไซเบอร์ ระบบที่ใช้ AI ต้องมีความปลอดภัยทางไซเบอร์ (Cyber Security) ซึ่งความปลอดภัยไซเบอร์มี ๓ หลักการ คือ ความลับ ความถูกต้องและความพร้อมใช้งาน ควบคู่ไปกับการใช้งาน AI

แนวทางการกำกับดูแล AI ของกระทรวงกลาโหม ที่สำคัญ มีดังนี้

๑.) ห้ามใช้ข้อมูลที่มีชั้นความลับ ข้อมูลทางการทหาร และข้อมูลด้านความมั่นคง ห้ามใช้สร้างความเกลียดชัง หรือใช้ในทางที่ผิดกฎหมาย เพื่อประมวลผลโดยไม่ได้รับอนุญาตโดยเด็ดขาด

๒.) การใช้งานปัญญาประดิษฐ์ (AI) ควรตรวจสอบข้อมูล โดยใช้เครื่องมือที่ได้รับอนุญาต และอ้างอิงแหล่งที่มาเพื่อรักษาความถูกต้องและความโปร่งใส และหลีกเลี่ยงการสร้างเนื้อหาที่มีอคติหรือผิดกฎหมาย ได้แก่ ข้อมูลเท็จที่ไม่ได้ตั้งใจให้เกิดความเข้าใจผิด (Misinformation) และข้อมูลเท็จที่จงใจให้เกิดความเข้าใจผิด (Disinformation)

๓.) หลีกเลี่ยงการใช้งาน AI ฟรีหรือที่ไม่เสียค่าใช้จ่าย หรือจากแพลตฟอร์มที่ไม่มีมาตรฐาน เพราะอาจเสี่ยงต่อการรั่วไหลของข้อมูลหรือการนำข้อมูลไปฝึกโมเดลโดยไม่ได้รับอนุญาต

๔.) องค์กรควรมีการจัดฝึกอบรมเรื่องปัญญาประดิษฐ์ (AI) ให้บุคลากรอย่างน้อยปีละ ๑ ครั้ง เพื่อให้เกิดความเข้าใจถึงความเสี่ยงของ AI และแนวทางปฏิบัติ

ดังนั้นทั้งภาครัฐและภาคเอกชนต้องตระหนักถึงความเสี่ยงที่เกิดจากการใช้งาน AI เพื่อสร้างความไว้วางใจให้กับผู้บริโภคและผู้มีส่วนได้ส่วนเสีย ซึ่งควรคำนึงถึงแนวทางปฏิบัติด้าน AI อย่างมีความรับผิดชอบ และนำไปประยุกต์ใช้กับลูกค้าในกลุ่มอุตสาหกรรมต่าง ๆ รวมทั้งคำนึงถึงความปลอดภัยของข้อมูลส่วนบุคคลเป็นสิ่งสำคัญที่ทุกองค์กรจะต้องมี และควรปฏิบัติตามกฎระเบียบการปกป้องข้อมูลที่เกี่ยวข้องและนำแนวทางจัดการข้อมูลที่ปลอดภัยมาใช้ มีการกำกับดูแลปัญญาประดิษฐ์อย่างมีความรับผิดชอบ ถือเป็นประเด็นสำคัญที่ทุกองค์กรจำเป็นต้องมี เพื่อสร้างความไว้วางใจและจัดการความเสี่ยงได้อย่างเป็นระบบ โดยการกำกับดูแลที่แข็งแกร่งโดยทีมตรวจสอบภายในที่มีทักษะสูงหรือผู้เชี่ยวชาญจากภายนอก จะมีความสำคัญอย่างยิ่งต่อการควบคุมการใช้งาน AI และจะสามารถดึงศักยภาพของ AI มาใช้ให้เกิดประโยชน์สูงสุดในการเปลี่ยนแปลงไปสู่องค์กรดิจิทัล สำหรับหน่วยงานด้านความมั่นคงของไทยควรมีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาเพิ่มประสิทธิภาพในการดำเนินการตามภารกิจที่ได้รับมอบหมาย โดยเป็นแนวทางที่สามารถนำไปประยุกต์ใช้ และจะต้องมีการบริหารจัดการความเสี่ยงอย่างรัดกุมและเหมาะสมตามลักษณะการใช้งาน รวมถึงมีการรักษาความปลอดภัยจากการใช้งาน

๖. แนวทางการเตรียมความพร้อมด้านการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ของกองทัพบก

ภัยคุกคามด้านปัญญาประดิษฐ์มีผลกระทบด้านความมั่นคง ดังนั้น กองทัพบกจะต้องมีการปรับตัวและรับมือดำเนินการให้สอดคล้องกับสถานการณ์ โดยทุกหน่วยจะต้องมีการตระหนักรู้และเข้าใจเกี่ยวกับปัญญาประดิษฐ์และนำมาปรับใช้ในการปฏิบัติภารกิจ ทั้งนี้ศูนย์ไซเบอร์ของกองทัพบกเป็นหน่วยดำเนินการหลักในเรื่องการประยุกต์ใช้ปัญญาประดิษฐ์ ซึ่งการดำเนินการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ใช้คณะทำงานหรือทีมงานของกองทัพบก โดยศูนย์ไซเบอร์กองทัพบกดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) และมีหน้าที่ดูแลระบบให้กับ สกมช. ซึ่งถือได้ว่าเป็นขีดความสามารถด้านปัญญาประดิษฐ์ (AI) ของกองทัพบก

ในมุมมองของภาคเอกชน มองว่าการประยุกต์ใช้ปัญญาประดิษฐ์ของกองทัพ ต้องพิจารณาในเรื่องที่มีชั้นความลับเป็นหลัก เพราะปัญญาประดิษฐ์เป็นภัยด้านความมั่นคง และต้องพิจารณาถึงข่าวปลอม (Fake News) กองทัพบกเป็นหน่วยงานด้านความมั่นคงต้องพิจารณาและตรวจสอบข่าวปลอม และเป็นหน้าที่ความรับผิดชอบของทุกภาคส่วนในการตรวจสอบข่าวปลอมและการร่วมมือรับมือภัยคุกคาม รวมถึงประชาชนต้องเรียนรู้และระมัดระวังการใช้ปัญญาประดิษฐ์ที่เข้ามามีบทบาทในชีวิตประจำวัน

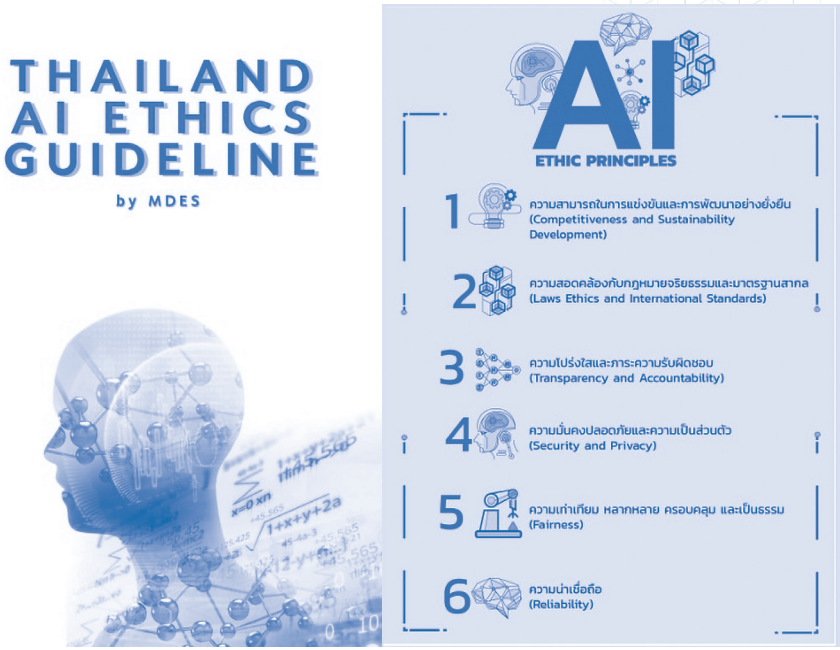
การประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ของกองทัพ มีหลักการสำคัญ คือ ต้องการผู้ใช้ที่มีทักษะและเลือกโมเดลที่เหมาะสม และ AI ต้องการข้อมูลที่ถูกต้อง ในโลกมีบริษัทที่สามารถทำ AI ได้ คือ บริษัท NVIDIA เป็นบริษัทของไต้หวันที่ใช้เทคโนโลยีของสหรัฐอเมริกา และเป็นผู้นำด้านการออกแบบและผลิตเทคโนโลยีปัญญาประดิษฐ์ (AI) โดยบริษัท NVIDIA เป็นผู้ออกแบบชิปที่เป็นอุปกรณ์อิเล็กทรอนิกส์ขนาดเล็ก ในปัจจุบันสหรัฐฯ ได้ออกประกาศ การห้ามขายชิปให้กับประเทศจีน ในภูมิภาคเอเชียตะวันออกเฉียงใต้ มีไทย สิงคโปร์ อินโดนีเซีย และมาเลเซีย ที่สามารถซื้อชิปที่ใช้เทคโนโลยีของสหรัฐอเมริกาได้ ถึงแม้ว่าประเทศไทยจะพัฒนาให้มีข้อมูลที่สมบูรณ์แต่ก็ยังทำ AI ไม่ได้ เนื่องจากยังคงขาด Data Center ที่สมบูรณ์ ซึ่ง Data Center ก็คือ ศูนย์จัดเก็บข้อมูล ที่นอกจากจะเป็นศูนย์กลางโดยเป็นที่อยู่ของข้อมูลแล้ว ยังเป็นศูนย์รวมของอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบที่เกี่ยวข้องในการจัดเก็บข้อมูลอีกด้วย

สรุปการประยุกต์ใช้ปัญญาประดิษฐ์ของกองทัพบกในขั้นต้น ประเทศไทยจะต้องมี Data Center และ AI เป็นของตนเอง โดยจะต้องมีชิป (Chip) และต้องมีฐานข้อมูลที่เป็นดิจิทัล ซึ่งชิปเปรียบเสมือนระเบิดนิวเคลียร์ยุคใหม่ที่สามารถซื้อขายได้ ซึ่งไทยสามารถซื้อชิปจากสหรัฐฯ ได้ สำหรับกองทัพบก ศูนย์ไซเบอร์กำลังดำเนินการทำชิปให้กับกองทัพบก และจัดซื้อ Data Center เพื่อที่จะทำปัญญาประดิษฐ์ให้กับกองทัพบก

๗. จริยธรรมการใช้ปัญญาประดิษฐ์ (AI)

ปัจจุบันมีแอปพลิเคชันด้าน AI ที่ถูกสร้างขึ้นมาและให้มีการใช้งานได้ฟรี โดยไม่เสียค่าใช้จ่าย สาเหตุก็คือการที่สร้าง AI ขึ้นมา เริ่มต้นจากความคิดที่ไม่คำนึงถึงจริยธรรม ซึ่งสิ่งที่สำคัญ คือ จะต้องเข้าใจว่าผู้ใช้มีจริยธรรม แต่ในความเป็นจริง AI ถูกใช้ในทางที่ผิดจริยธรรม และถูกมองว่าเป็นอาวุธไม่ใช่จริยธรรม ดังนั้น จะต้องมีการปลูกฝังผู้ใช้ให้มีจริยธรรมและต้องรู้กลไก การทำงานของปัญญาประดิษฐ์ เพื่อให้สามารถยับยั้งการทำงานของปัญญาประดิษฐ์ได้ หากไม่มีจริยธรรม การใช้ปัญญาประดิษฐ์อย่างมีจริยธรรม (AI Ethics) ข้อมูลจากผลสำรวจพบว่า ความพร้อมในการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์สำหรับบริการดิจิทัลประจำปี พ.ศ. ๒๕๖๗ ของศูนย์ธรรมาภิบาลปัญญาประดิษฐ์ (AIGC) ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ระบุว่า มีเพียง ๑๖.๕% ขององค์กรไทยที่นำจริยธรรมปัญญาประดิษฐ์มาประยุกต์ใช้ภายในองค์กรแล้ว ในขณะที่ ๔๓.๗% กำลังเริ่มวางแนวคิดในการนำหลักจริยธรรมมาปรับใช้ในองค์กร ซึ่งจะมีการกำหนดกรอบจริยธรรมและระเบียบข้อบังคับการใช้ AI อย่างกว้างขวาง เพื่อนำไปสู่แนวปฏิบัติด้านจริยธรรมที่เข้มงวดมากยิ่งขึ้น โดยเน้นถึงความเป็นส่วนตัว ความปลอดภัย และการลดอคติ เพื่อให้การใช้ปัญญาประดิษฐ์มีการใช้งานอย่างมีความรับผิดชอบ

การใช้ปัญญาประดิษฐ์ต้องมีการใช้อย่างมีจริยธรรม เนื่องจากโลกมีประชากรในหลายช่วงอายุ (Generations) Gen Y กับ Gen Z ทำให้เกิดช่องว่างระหว่างช่วงอายุ ทำให้การเข้าถึง AI มีความแตกต่างกัน จะเห็นได้ว่า Gen Z จะเรียนรู้การใช้ AI ได้เร็วกว่า ในเรื่องของจริยธรรมการใช้ AI ที่ใกล้ตัวที่สุด ตัวอย่างเช่น การนำภาพบุคคลที่ไม่ได้รับอนุญาต นำไปใช้ในเชิงการค้า หรือนำไปใช้ในทางทุจริต การใช้ AI อาจเป็นเรื่องผิดกฎหมายได้ ดังนั้นการใช้ปัญญาประดิษฐ์ต้องระมัดระวังถึงความเสี่ยงที่จะผิดจริยธรรม จะเห็นได้ว่ามิจฉาชีพออนไลน์มุ่งเป้าไปที่ผู้สูงอายุ เพราะเข้าถึงได้มากที่สุดและไม่รู้จักการปกป้องข้อมูลส่วนบุคคล ส่วนในยุควัยกลางคนจะใช้ AI ในลักษณะการทำงานเพื่อเพิ่มประสิทธิภาพและความรวดเร็ว สุดท้าย Gen ที่เป็นความหวังคือ Gen ในวัยเด็ก โดยมีการเรียนรู้ตั้งแต่ระดับปฐมวัย โดยจะมีการปลูกฝังในเรื่องของจริยธรรมการใช้งาน ดังนั้นปัจจุบันจะเห็นได้ว่ามีอยู่ 2 Gen คือ ผู้สูงอายุกับวัยกลางคนหรือวัยทำงาน ซึ่งจะใช้งานในระดับเริ่มใช้กับไม่เปิดใจ การไม่เปิดใจเนื่องจากเชื่อว่าปัญญาประดิษฐ์มีความน่ากลัว เพราะไม่มีจริยธรรมจึงทำให้ไม่เปิดใจที่จะลองใช้ ดังนั้นควรมีการเปิดใจ ถึงจะเริ่มป้อนข้อมูลที่มีความถูกต้อง ซึ่งถือได้เป็นวิธีที่ดีที่สุดในการใช้ปัญญาประดิษฐ์อย่างมีจริยธรรม



ภาพที่ ๗ *หลักการใช้ปัญญาประดิษฐ์อย่างมีจริยธรรมของ*
สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

แนวทางการใช้ปัญญาประดิษฐ์อย่างมีจริยธรรม ตามข้อมูลเอกสารแนวปฏิบัติจริยธรรมปัญญาประดิษฐ์ (Thailand AI Ethics Guideline) ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้กำหนดแนวทางจริยธรรมปัญญาประดิษฐ์เพื่อใช้เป็นแนวทางสำหรับการกำกับการดำเนินงานเกี่ยวกับปัญญาประดิษฐ์ของหน่วยงานภาครัฐทั้งระดับประเทศและระดับองค์กร โดยได้กำหนดหลักการจริยธรรมปัญญาประดิษฐ์ ๖ ข้อ ดังนี้

๑.) ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน (Competitiveness and Sustainability Development) ปัญญาประดิษฐ์ควรถูกสร้างและใช้งานเพื่อสร้างประโยชน์ให้แก่มนุษย์ สังคม เศรษฐกิจและสิ่งแวดล้อมอย่างยั่งยืน AI ควรได้รับการวิจัยและพัฒนาอย่างต่อเนื่อง เพื่อให้มนุษย์เกิดการสร้างสรรค์นวัตกรรมและอุตสาหกรรมใหม่

๒.) ความสอดคล้องกับกฎหมายจริยธรรมและมาตรฐานสากล (Laws Ethics and International Standards) ปัญญาประดิษฐ์ควรได้รับการวิจัย ออกแบบ พัฒนาให้ใช้งาน โดยสอดคล้องกับกฎหมาย จริยธรรม และมาตรฐานสากล AI ควรใช้หลักการมนุษย์เป็นศูนย์กลางและเป็นผู้ตัดสินใจ ไม่ควรถูกใช้ในการกำหนดชะตาชีวิตของมนุษย์

๓.) ความโปร่งใสและความรับผิดชอบ (Transparency and Accountability) ปัญญาประดิษฐ์ควรได้รับการวิจัย ออกแบบ พัฒนาให้ใช้งานด้วยความโปร่งใส ผู้วิจัยหรือผู้ออกแบบ AI ควรมีความรับผิดชอบ (Accountability) ต่อผลกระทบที่เกิดขึ้นจากปัญญาประดิษฐ์ตามภาระหน้าที่ของตน

๔.) ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy) ปัญญาประดิษฐ์ควรถูกสร้างเพื่อบริการ แต่ไม่ควรถูกใช้เพื่อหลอกลวง ต่อต้านและคุกคามมนุษย์ AI ควรใช้หลักป้องกันความเสี่ยง เพื่อป้องกันการโจมตีจากภัยคุกคาม เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล รวมถึงหน่วยงานภาครัฐควรวางแผนกำกับดูแลและให้ความร่วมมือกับนานาชาติในการหลีกเลี่ยงการแข่งขันสร้างอาวุธอัตโนมัติจาก AI ที่ร้ายแรง

๕.) ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness) การออกแบบและพัฒนาปัญญาประดิษฐ์ควรคำนึงถึงความหลากหลาย หลีกเลี่ยงการผูกขาด เพื่อก่อให้เกิดประโยชน์ต่อผู้คนจำนวนมาก และควรสามารถพิสูจน์ถึงความเป็นธรรมได้

๖.) ความน่าเชื่อถือ (Reliability) ปัญญาประดิษฐ์ควรให้มีความน่าเชื่อถือในการใช้งานต่อสาธารณะ โดยสามารถคาดการณ์ ตัดสินใจ และให้คำแนะนำได้อย่างแม่นยำถูกต้อง (Accuracy) สร้างผลลัพธ์ที่สามารถเชื่อถือได้ (Reliability) และสามารถสร้างใหม่ได้เมื่อต้องการ (Reproducibility)

พื้นฐานเบื้องต้นของจริยธรรมในหน่วยงานด้านความมั่นคง ซึ่งสอดคล้องกับหลักการการใช้ปัญญาประดิษฐ์ของโลก คือ ๑.) ห้ามนำข้อมูลเท็จ (Disinformation) มาใช้ในปัญญาประดิษฐ์ ๒.) ห้ามนำข้อมูลส่วนบุคคล และข้อมูลที่อ่อนไหว (Sensitive Data) ไปประมวลผล ๓.) ห้ามใช้ปัญญาประดิษฐ์ไปตัดสินผู้อื่น นอกจากนี้ในหน่วยงานด้านความมั่นคงต้องใช้ช่องทางที่มีความปลอดภัย เพื่อที่จะประมวลผลไม่ให้ข้อมูลนั้นรั่วไหล ซึ่งเป็นสิ่งที่จะต้องหารือกันในเรื่องการไปสู่กองทัพดิจิทัล ซึ่งเป็นเรื่องค่อนข้างยาก สิ่งที่ควรทำ คือ เริ่มแรกจะต้องทำการจัดหมวดหมู่ข้อมูล (Data Classification) ข้อมูลที่ป้อนเข้าไปในปัญญาประดิษฐ์ควรจะเป็นข้อมูลที่ถูกคัดแยก รวมถึงมีการกำหนดจริยธรรมการใช้ปัญญาประดิษฐ์ และการกำหนดเกณฑ์การใช้คลาวด์ (Cloud) หน่วยงานด้านความมั่นคงควรมีแนวทางการใช้ปัญญาประดิษฐ์ที่สำคัญ คือ ห้ามนำข้อมูลส่วนบุคคลและข้อมูลที่เป็นความลับไปประมวลผล และกำลังพลทุกนายควรเรียนรู้และมีความเข้าใจเกี่ยวกับปัญญาประดิษฐ์ และเรียนรู้ถึงคุณและโทษของเทคโนโลยีสมัยใหม่ต่าง ๆ เพื่อป้องกันความเสี่ยงในการใช้งาน

๘. สรุป

แนวโน้มการใช้ปัญญาประดิษฐ์ (AI) ถูกนำมาใช้ทั้งทางภาคพลเรือนและด้านการทหารมากขึ้น ที่เห็นได้ชัดเจน คือ ถูกนำมาใช้ในการบิดเบือนข้อมูลข่าวสาร ซึ่งมีผลกระทบต่อความมั่นคงของชาติ จะเห็นได้ว่าศัตรูในปัจจุบันได้เปลี่ยนแปลงไป ไม่ใช่แค่มิติทางบก ทางเรือ ทางอากาศ แต่เป็นมิติทางดิจิทัลหรือทางข้อมูล อย่างไรก็ตาม ปัญญาประดิษฐ์ยังไม่สามารถมาแทนที่มนุษย์ได้ ยังคงเป็นเพียงเครื่องมือที่นำมาใช้ในสนามรบ มนุษย์จึงมีหน้าที่ควบคุมการตัดสินใจของปัญญาประดิษฐ์ รวมถึงมีการรักษาความปลอดภัยจากการใช้งานปัญญาประดิษฐ์จะต้องมีเรื่องของจริยธรรมเข้ามาเกี่ยวข้อง ที่สำคัญ คือ AI ไม่ควรถูกใช้เพื่อหลอกลวง ควรใช้หลักป้องกันความเสี่ยง เพื่อป้องกันการโจมตีจากภัยคุกคามเพื่อรักษาความมั่นคงปลอดภัยของข้อมูล รวมถึงหน่วยงานภาครัฐควรวางแผนกำกับดูแลและให้ความร่วมมือกับนานาชาติในการหลีกเลี่ยงการแข่งขันสร้างอาวุธอัตโนมัติจาก AI ที่ร้ายแรง การประยุกต์ใช้ปัญญาประดิษฐ์ของกองทัพบกต้องพิจารณาในเรื่องที่มีชั้นความลับเป็นหลัก เพราะปัญญาประดิษฐ์เป็นภัยด้านความมั่นคง และต้องพิจารณาถึงข่าวปลอม ดังนั้น หน่วยงานด้านความมั่นคงรวมถึงกองทัพบกควรมีการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้เพื่อเพิ่มประสิทธิภาพในการดำเนินการตามภารกิจที่ได้รับมอบหมาย และจะต้องมีการบริหารจัดการความเสี่ยงอย่างรัดกุม รวมถึงมีการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมต่อไป

๙. เอกสารอ้างอิง

น.ท. กนก บุนนาค. ปัญญาประดิษฐ์ในบริบทของสงครามสมัยใหม่. เอกสารการบรรยายในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร.

พ.อ. จารุกฤษณ์ เรืองสุวรรณ. ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ. เอกสารการบรรยายในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร.

นวพร เหมือนประสาท. แนวโน้มปัญญาประดิษฐ์. เอกสารการบรรยายในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร.

พ.อ. อภิชา ศรีจิระภาส. เทคโนโลยีปัญญาประดิษฐ์. เอกสารการบรรยายในการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร.

อัญชลี จวงจันทร์. เทคโนโลยีปัญญาประดิษฐ์ (AI) กับการบริหารงานภาครัฐ. วิจัยปริทัศน์ของสำนักงานเลขาธิการสภาผู้แทนราษฎร. ฉบับที่ ๔๐ เดือนพฤศจิกายน ๒๕๖๖.

สรุปผลการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร เรื่อง “ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ”. ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก. วันที่ ๒๘ พฤษภาคม พ.ศ. ๒๕๖๘ ณ โรงแรมบ้านไทย บูทิก กรุงเทพฯ.

รศ.ดร. ธนชาติ นุ่มนนท์. “Generative AI เทคโนโลยีเปลี่ยนชีวิต”. สำนักพิมพ์แสงดาว : กรุงเทพฯ. พ.ศ. ๒๕๖๗.

สุทธิชัย ทักษนันต์. “AI เปลี่ยนอนาคต”. สำนักพิมพ์บ้านพระอาทิตย์ : กรุงเทพฯ. พ.ศ. ๒๕๖๓.

เอกสารศึกษาเฉพาะกรณี. เรื่องปัญญาประดิษฐ์กับจุดเปลี่ยนของสงครามในอนาคต. ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย.

เอกสารแนวปฏิบัติจริยธรรมปัญญาประดิษฐ์. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

แนวทางขับเคลื่อน AI สร้างความพร้อมประเทศไทย. สำนักข่าวอินโฟเควสท์. ๑ พฤษภาคม ๒๕๖๘.

บทความหลักการทำงานของ AI และการใช้ในอุตสาหกรรม. https://www.dia.co.th/article/what-is-artificial-intelligence/.

บทความปัญญาประดิษฐ์กับการรักษาความปลอดภัยไซเบอร์. https://www.thailand.intel.com/content/www/th/th/learn/ai-in-cybersecurity.html.

ข่าวนาโต (NATO) เพิ่มงบประมาณด้าน AI. https://thainews.prd.go.th/.

ภาพกิจกรรม
การเสวนาด้านความมั่นคงและยุทธศาสตร์ทหาร

ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก จัดการเสวนาด้านความมั่นคงและยุทธศาสตร์ทหารของ ทบ. ครั้งที่ ๒ ประจำปีงบประมาณ ๒๕๖๘ ในหัวข้อ **"ปัญญาประดิษฐ์ (AI) กับภัยความมั่นคงของชาติ"** เมื่อวันที่ ๒๘ พฤษภาคม ๒๕๖๘ โดยมี พล.ต. วุทธยา จันทมาศ รอง จก.ยศ.ทบ. เป็นประธานพิธีเปิดการเสวนาฯ ณ โรงแรมบ้านไทย บูทิก กรุงเทพฯ









วัตถุประสงค์ของการเสวนาฯ

๑. เพื่อให้ผู้เข้าร่วมเสวนามีความรู้ความเข้าใจ เกี่ยวกับปัญญาประดิษฐ์ (AI) และเทคโนโลยีสมัยใหม่
๒. เพื่อให้ทราบว่าปัญญาประดิษฐ์ (AI) มีผลกระทบต่อภัยคุกคามความมั่นคงอย่างไร
๓. แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ด้านความมั่นคงอย่างมีจริยธรรม เพื่อความมั่นคงยั่งยืน

ผลการดำเนินงาน

ผู้เข้าร่วมเสวนา ได้รับความรู้ความเข้าใจ แนวคิดใหม่ ๆ เกี่ยวกับปัญญาประดิษฐ์ (AI) ที่มีผลต่อความมั่นคงในหลากหลายมิติ และสามารถใช้ประโยชน์จากศักยภาพปัญญาประดิษฐ์ (AI) ในการเสริมสร้างความมั่นคงของชาติ ได้อย่างมีประสิทธิภาพควบคู่ไปกับการป้องกันและผลกระทบจากภัยคุกคามที่อาจจะเกิดขึ้นในอนาคต

ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์
กรมยุทธศึกษาทหารบก