

ปัญญาประดิษฐ์ (Artificial Intelligence: AI) กับจุดเปลี่ยนของสงครามในอนาคต Artificial Intelligence (AI): A Culmination of Future Warfare

บทความวิชาการ

อัครชัย หนูนกดี¹ และ ศิวาลัย สิริโรจน์บริรักษ์²

Tamrongchai Noonpugdee and Siwalee Sirojborirak

กองภูมิภาคศึกษา ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ กรุงเทพฯ ประเทศไทย 10400

Strategic Studies Center, National Defence Studies Institute, Bangkok, Thailand 10400

E-mail: xtazee_4253@hotmail.com¹ and E-mail: rsd.ssc@gmail.com²

บทคัดย่อ

บทความเรื่อง “ปัญญาประดิษฐ์ (Artificial Intelligence: AI) กับจุดเปลี่ยนของสงครามในอนาคต” มีวัตถุประสงค์เพื่อศึกษาระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทย และเพื่อเสนอแนะแนวทางการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทย เพื่อรองรับสงครามในอนาคต

ผลการศึกษา พบว่า ตัวแบบระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทย เพื่อรองรับสงครามในอนาคตนั้น กระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ควรผลักดันให้เกิดระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ใน 5 ประการ ได้แก่ 1) การสนับสนุนเชิงนโยบายจากภาครัฐ 2) การจัดการบุคลากร ให้มีความชำนาญและองค์ความรู้ 3) การวิจัยและพัฒนาด้าน AI 4) ความร่วมมือภาครัฐและภาคเอกชน และ 5) โครงสร้างหรือหน่วยงานจัดการด้านข้อมูลและการรักษาความปลอดภัยทางไซเบอร์ ที่ช่วยสนับสนุนกิจกรรมด้าน AI ของกองทัพไทย ซึ่งระบบนิเวศของปัญญาประดิษฐ์ดังกล่าวจะช่วยสนับสนุนงานด้านปัญญาประดิษฐ์ (AI) ระบบคลาวด์ (CLOUD) ระบบบัญชาการควบคุมและการสื่อสาร (Command Control Communication: C3) และความปลอดภัยด้านไซเบอร์ ซึ่งเป็นองค์ประกอบของ “การปฏิบัติการด้านดิจิทัล (Digital Operations)” ที่ประสานสอดคล้องกัน เพื่อให้กองทัพไทยสามารถปฏิบัติการได้ตลอดย่านความขัดแย้ง (Military Spectrum of Conflict)

บทความนี้เป็นส่วนหนึ่งของเอกสารศึกษาเฉพาะกรณี (Case Study) เรื่อง “ปัญญาประดิษฐ์ (Artificial Intelligence: AI) กับจุดเปลี่ยนของสงครามในอนาคต” ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ

วันที่รับบทความ: 27 พ.ค.64

วันที่แก้ไขบทความ: 13 ส.ค.64

วันที่ต้องรับบทความ: 18 ส.ค.64

บทส่งท้าย ยังได้นำเสนอถึงควอนตัมเทคโนโลยี (Quantum Technology) กับสงครามในอนาคต เนื่องจากเทคโนโลยีควอนตัมเป็นกุญแจสำคัญในการขยายศักยภาพของปัญญาประดิษฐ์ (AI) ในการเรียนรู้เพื่อนำไปสู่การแก้ไขปัญหาที่เกี่ยวข้องกับการปฏิบัติงานด้านความมั่นคงที่ซับซ้อนมากขึ้น ซึ่งอาจส่งผลกระทบต่อความมั่นคงของชาติ เช่น การสูญเสียความลับ การสูญเสียทางการข่าว (Loss of Intelligence) และการโจมตีทางควอนตัม (Quantum Attack) เป็นต้น ซึ่งกองทัพไทยและหน่วยงานที่เกี่ยวข้อง ควรเตรียมพร้อมรับความท้าทายที่จะเกิดขึ้นจากเทคโนโลยีดังกล่าว

คำสำคัญ: ปัญญาประดิษฐ์, สงครามในอนาคต, ระบบนิเวศของปัญญาประดิษฐ์, ควอนตัมคอมพิวเตอร์

Abstract

This article aims to examine the AI ecosystem for the advancement of the Royal Thai Armed Forces' affairs and to recommend appropriate AI ecosystem development approaches to prepare for dealing with future warfare.

The findings show that in advancing the Royal Thai Armed Forces' operations to deal with future warfare, the Ministry of Defence, the Royal Thai Armed Forces Headquarters, and the military branches should strive for five aspects of such an AI ecosystem as follows: (1) government policies support; (2) personnel management to enhance their expertise and knowledge; (3) AI research and development; (4) government and private sectors cooperation; and (5) information management and cybersecurity structure or agency to maintain the Royal Thai Armed Forces' AI operations.

The establishment of such an AI ecosystem will support the Royal Thai Armed Forces' AI operations, CLOUD system, Command Control Communication (C3) system, and Cybersecurity, which are vital elements of a synchronized "digital operation" that will enable the Royal Thai Armed Forces to effectively operate across the full military spectrum of conflict.

Finally, the epilogue presents the relationship between Quantum Technology (QT) and future warfare. Since QT is a key to an increase in AI capabilities for learning and solving more complex defence and security problems, which may have an impact on national security issues such as loss of confidentiality, loss of intelligence, and quantum attacks, the Royal Thai Armed Forces and related agencies should be well prepared to deal with such QT challenges.

Keywords: Artificial Intelligence (AI), Future warfare, AI ecosystem, Quantum Technology (QT)

บทนำ

จากความก้าวหน้าทางเทคโนโลยีในปัจจุบัน โดยเฉพาะ "การพัฒนาคอมพิวเตอร์เชิงควอนตัม" (Quantum Computer) ถือเป็นการปฏิวัติวงการคอมพิวเตอร์ในปัจจุบันที่กำลังจะเปลี่ยนแปลงเทคโนโลยีในอนาคต (มหาวิทยาลัยมหิดล สถาบันนวัตกรรมการเรียนรู้, 2561) เนื่องจากเป็นเทคโนโลยีคอมพิวเตอร์รูปแบบใหม่ที่มีการประมวลผลข้อมูลที่เร็วกว่าคอมพิวเตอร์ทั่วไปอย่างมหาศาล จากรายงานของสถาบัน RAND (The RAND Corporation, 2020) ซึ่งเป็นหน่วยงานคลังสมอง (Think Tank) ของสหรัฐฯ

กล่าวว่าในปี พ.ศ.2566 (ค.ศ.2023) บริษัทยักษ์ใหญ่ของโลก จะนำควอนตัมคอมพิวเตอร์มาใช้ในเชิงพาณิชย์อย่างสมบูรณ์ ซึ่งเมื่อถึงเวลานั้น โลกต้องเผชิญกับการโจมตีทางไซเบอร์ จากควอนตัมคอมพิวเตอร์ในปี พ.ศ.2576 (ค.ศ.2033) ทั้งนี้ เป้าหมายสำคัญในการพัฒนาควอนตัมคอมพิวเตอร์ ประการหนึ่งคือ การนำมาใช้ด้าน “Advance Machine Learning” ซึ่งเป็นส่วนการเรียนรู้ของเครื่องจักร หรือ เปรียบเสมือนเป็นสมองของปัญญาประดิษฐ์ (AI) ดังนั้น จึงหมายความว่า ในอนาคตอันใกล้ บรรดาเทคโนโลยี ที่ใช้ระบบการเรียนรู้ของเครื่องจักร โดยเฉพาะเทคโนโลยี ปัญญาประดิษฐ์ จะมีขีดความสามารถอย่างก้าวกระโดด จนไม่อาจจินตนาการถึงขีดจำกัดได้ และความก้าวหน้าของ เทคโนโลยีปัญญาประดิษฐ์ดังกล่าวข้างต้น ถือเป็นจุดเปลี่ยน สำคัญของรูปแบบสงครามในอนาคต

นโยบายผู้บัญชาการทหารสูงสุด ประจำปีงบประมาณ พ.ศ.2563 ได้กำหนดวิสัยทัศน์ของกองบัญชาการกองทัพไทย ประจำปีงบประมาณ พ.ศ.2563 ได้แก่ “เป็น *DIGITAL Headquarters* ภายใน พ.ศ.2565 และมุ่งสู่การเป็น *SMART Headquarters* ภายใน พ.ศ.2580” โดย ได้กำหนดเป้าหมายการเป็น *DIGITAL Headquarters* ภายใน พ.ศ.2565 ไว้ 7 ประการ โดยประการที่ 5 ได้แก่ *Technology 4.0* ใช้เทคโนโลยีที่มีความฉลาด (AI) ทำงาน แทนคน และกำหนดวิสัยทัศน์ในการมุ่งสู่การเป็น *SMART Headquarters* ภายใน พ.ศ.2580 ไว้ 5 ประการ โดย ประการที่ 3 ได้แก่ “*AI C2 (Artificial Intelligence for Command and Control) มีความพร้อมในการควบคุม บังคับบัญชาที่ทันสมัย ถูกต้อง แม่นยำ ทันเวลา*” ดังนั้น จะเห็นได้ว่า การจะบรรลุวิสัยทัศน์ดังกล่าว กองทัพไทย จำเป็นต้องเตรียมความพร้อม “ระบบนิเวศของปัญญา ประดิษฐ์ (AI Ecosystem)” (Center for Strategic and International Studies, 2018) เพื่อรองรับจุดเปลี่ยน ของสงครามในอนาคตดังกล่าว

การศึกษาตัวแบบระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทย

การศึกษาตัวแบบระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทย ประกอบด้วย 3 ส่วนคือ 1) การศึกษาตัวแบบระบบนิเวศ ปัญญาประดิษฐ์จากสถาบันคลังสมองระดับโลก 2) การศึกษาตัวอย่างของประเทศที่ประสบความสำเร็จ ด้านการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ และ 3) การศึกษาตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของ กองทัพแต่ละประเทศ ดังนี้

1. การศึกษาตัวแบบระบบนิเวศปัญญาประดิษฐ์ จากสถาบันคลังสมอง (Think Tank) ระดับโลก

จากการศึกษาเอกสาร และรายงานจากสถาบัน ที่เกี่ยวข้องกับการพัฒนาระบบนิเวศปัญญาประดิษฐ์ ได้แก่ 1) สถาบัน Center for Strategic and International Studies (Sheppard, Karlen, Hunter, and Balieiro, 2018) ซึ่งเป็นสถาบันคลังสมองด้านความมั่นคงของสหรัฐฯ 2) สถาบัน McKinsey Global Institute (MGI) (2018) ซึ่งเป็นสถาบันวิจัยด้านเศรษฐกิจจากภาคเอกชน 3) ศูนย์วิจัย Oxford Insights and the International Development Research Centre (2019) และ 4) Tortoise Intelligence (2019) ซึ่งเป็นสื่อสารมวลชนด้านเทคโนโลยีทำให้สามารถ กำหนดตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของบทความ ฉบับนี้ ได้แก่ 1) การสนับสนุนเงินนโยบายจากภาครัฐ 2) การจัดการบุคลากรให้มีความชำนาญและองค์ความรู้ 3) การวิจัยและพัฒนาด้าน AI 4) ความร่วมมือภาครัฐ และเอกชน 5) โครงสร้างหรือหน่วยงานจัดการด้านข้อมูล และการรักษาความปลอดภัยทางไซเบอร์ ดังตารางที่ 1

ตารางที่ 1 การศึกษาองค์ประกอบระบบนิเวศปัญญาประดิษฐ์ จากสถาบันคลังสมอง (Think Tank) ระดับโลก เพื่อกำหนด
ตัวแบบระบบนิเวศของปัญญาประดิษฐ์ในการส่งเสริมกิจการของกองทัพไทย

| สถาบัน/ หน่วยงาน | องค์ประกอบระบบนิเวศปัญญาประดิษฐ์ (AI Ecosystem) | | | | | | | |
|---|---|--|---|---|--|-------------------------------|-----------------------|---|
| Center for Strategic and International Studies (CSIS) | การจัดการบุคลากรที่มี ความชำนาญ และองค์ความรู้ | ขีดความสามารถ ด้านดิจิทัล สำหรับ การตรวจสอบ การจัดการ และ การใช้ข้อมูล | การสถาปนา ความเชื่อมั่น ความปลอดภัย และความไว้วางใจ ทางเทคนิค | สภาพแวดล้อม ด้านการลงทุน และกรอบ นโยบายที่ สนับสนุนการ เจริญเติบโต ของ AI | | | | |
| McKinsey Global Institute (MGI) | การลงทุน | การวิจัย | ผลิตภัณฑ์ที่เกิดจาก AI | การใช้งาน เทคโนโลยี | การสร้าง นวัตกรรม ที่รวมถึงทุน การวิจัย และพัฒนา และการ สร้างตัวแบบ ธุรกิจ | ทรัพยากร มนุษย์ | การเข้าถึง เทคโนโลยี | โครงสร้าง ตลาด แรงงาน ที่เกี่ยวข้องกับ AI |
| Oxford Insights and the International Development Research Centre | ธรรมาภิบาล ของรัฐ | โครงสร้างพื้นฐาน และข้อมูล | ทักษะ และการศึกษา | การบริการ ภาครัฐ และ สาธารณะ | | | | |
| Tortoise Intelligence | การส่งเสริม ความสามารถ ของบุคลากร ในการใช้ AI | โครงสร้างพื้นฐาน | สภาพแวดล้อม ที่ส่งเสริม การปฏิบัติงาน | การวิจัย ด้านนวัตกรรม | การพัฒนา ด้านนวัตกรรม | ยุทธศาสตร์ การลงทุน จากภาครัฐ | การลงทุน จากภาค เอกชน | |

2. การศึกษาตัวอย่างของประเทศที่ประสบความสำเร็จด้านการพัฒนาระบบนิเวศของปัญญาประดิษฐ์

การศึกษาตัวอย่างของประเทศที่ประสบความสำเร็จด้านการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ ได้แก่ สหรัฐอเมริกา สาธารณรัฐประชาชนจีน และสาธารณรัฐสิงคโปร์

จากสถาบัน McKinsey Global Institute (2018) ศูนย์วิจัย Oxford Insights and the International Development Research Centre (2019) และ Tortoise Intelligence (2019) สรุปได้ดังตารางที่ 2

ตารางที่ 2 การศึกษาตัวอย่างของประเทศที่ประสบความสำเร็จด้านการพัฒนาระบบนิเวศของปัญญาประดิษฐ์

| สถาบัน/หน่วยงาน | สหรัฐอเมริกา | สาธารณรัฐประชาชนจีน | สาธารณรัฐสิงคโปร์ |
|--|---|--|--|
| McKinsey Global Institute (MGI) ได้จัดทำดัชนีความพร้อมของประเทศด้านปัญญาประดิษฐ์ | สหรัฐฯ มีความพร้อมอยู่เหนือค่ามาตรฐานเฉลี่ยโลก (Threshold) ด้านปัญญาประดิษฐ์ในการวัดผลรวม รวมถึงการวัดผลย่อย ยกเว้น ด้านโครงสร้างตลาดแรงงาน | จีน แม้จะมีความพร้อมอยู่เหนือค่ามาตรฐานเฉลี่ยโลก (Threshold) ด้านปัญญาประดิษฐ์ในการวัดผลรวม เพียงด้านการลงทุน การพัฒนา และการเข้าถึงเทคโนโลยี แต่ MGI ยังคงจัดให้จีนเป็นหนึ่งในสองประเทศ ร่วมกับสหรัฐฯ ในการเป็นผู้นำระดับโลก (Active global Leaders) ที่ขับเคลื่อนประเทศด้วยปัญญาประดิษฐ์ | สิงคโปร์ มีความพร้อมอยู่เหนือค่ามาตรฐานเฉลี่ยโลก (Threshold) ด้านปัญญาประดิษฐ์ในการวัดผลรวม โดยมีประเด็นย่อยที่อยู่เหนือค่ามาตรฐานเฉลี่ยดังกล่าว ประกอบด้วย ผลผลิตที่เกิดจากปัญญาประดิษฐ์ การสร้างนวัตกรรม ที่รวมถึงทุนการวิจัยและพัฒนา และการเข้าถึงเทคโนโลยี |
| Oxford Insights and the International Development Research Centre ได้จัดทำดัชนีความพร้อมของภาครัฐด้านปัญญาประดิษฐ์ ปี ค.ศ.2019 | สหรัฐฯ ได้คะแนนเฉลี่ยจาก 4 กลุ่มตัวชี้วัดอยู่ที่ 8.804 เป็นลำดับที่ 4 จาก 194 ประเทศ อันมาจากการใช้และพัฒนายุทธศาสตร์ชาติด้านปัญญาประดิษฐ์ที่เน้นในการสร้างระบบนิเวศที่สนับสนุนปัญญาประดิษฐ์มาตั้งแต่ปี ค.ศ.2016 โดยเฉพาะการวิจัยและพัฒนา | จีน ได้คะแนนเฉลี่ยจาก 4 กลุ่มตัวชี้วัดอยู่ที่ 7.370 เป็นลำดับที่ 20 จาก 194 ประเทศทั่วโลก แต่อย่างไรก็ตาม ศูนย์วิจัยดังกล่าวยังคงคาดการณ์ถึงสาธารณรัฐจีนว่า จะสามารถทำอันดับได้สูงขึ้นอีกในปีถัดไป เนื่องจากความโดดเด่นด้านการลงทุนในขีดความสามารถและบุคลากรด้านปัญญาประดิษฐ์ | สิงคโปร์ ได้คะแนนเฉลี่ยจาก 4 กลุ่มตัวชี้วัดอยู่ที่ 9.186 เป็นลำดับที่ 1 จาก 194 ประเทศ ด้วยความโดดเด่นในการดำเนินยุทธศาสตร์การพัฒนาปัญญาประดิษฐ์ที่เกิดจากความร่วมมือจากทุกภาคส่วน และเป็นหนึ่งในไม่กี่ประเทศที่จัดตั้งสภาที่ปรึกษาด้านศีลธรรมปัญญาประดิษฐ์ |
| Tortoise Intelligence ได้จัดทำดัชนี Global AI Index | สหรัฐฯ ได้คะแนนรวมลำดับที่ 1 จาก 54 ประเทศทั่วโลก โดยได้ลำดับที่ 1 ในประเด็นย่อยในดัชนีดังกล่าว ในด้านการส่งเสริมความสามารถบุคคลากร โครงสร้างพื้นฐาน การวิจัย การพัฒนา และการลงทุนจากภาคเอกชน | จีน ได้คะแนนรวมลำดับที่ 2 จาก 54 ประเทศทั่วโลก โดยได้ลำดับที่ 1 ในประเด็นย่อยในดัชนีดังกล่าว ในด้านการพัฒนา และยุทธศาสตร์การลงทุนจากภาครัฐ | สิงคโปร์ ได้คะแนนรวมลำดับที่ 7 จาก 54 ประเทศทั่วโลก โดยประเด็นย่อยในดัชนีดังกล่าว สิงคโปร์ได้ลำดับที่ 2 ด้านการส่งเสริมความสามารถของบุคคลากร ลำดับที่ 4 ด้านโครงสร้างพื้นฐาน และลำดับที่ 6 ด้านการลงทุนจากภาคเอกชน |

3. การศึกษาตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของกองทัพแต่ละประเทศ

การศึกษาตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของกองทัพแต่ละประเทศ ได้แก่ กระทรวงกลาโหม

สหรัฐอเมริกา (Department of Defense, 2019) กระทรวงกลาโหมสาธารณรัฐประชาชนจีน (Allen, 2019) กระทรวงกลาโหมสาธารณรัฐสิงคโปร์ (Ministry of Defence, 2019) สรุปได้ดังตารางที่ 3

ตารางที่ 3 การเปรียบเทียบตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของกองทัพแต่ละประเทศ

| ระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ของกองทัพแต่ละประเทศ | | | |
|---|---|---|--|
| ตัวแบบระบบนิเวศปัญญาประดิษฐ์ | สหรัฐอเมริกา | สาธารณรัฐประชาชนจีน | สาธารณรัฐสิงคโปร์ |
| 1. การสนับสนุนเชิงนโยบายจากภาครัฐ | <ul style="list-style-type: none"> - ปี ค.ศ.2014 กระทรวงกลาโหมสหรัฐฯ ได้ประกาศยุทธศาสตร์ย่อยที่สาม (Third Offset Strategy) เพื่อพัฒนาขีดความสามารถของเหล่าทัพในการรับมือกับสงครามอนาคตที่มี AI เป็นเทคโนโลยีส่วนหนึ่งของการปฏิบัติงาน - ปี ค.ศ.2018 กระทรวงกลาโหมสหรัฐฯ ได้ประกาศ “ยุทธศาสตร์ปัญญาประดิษฐ์” โดยกำหนดวิสัยทัศน์ ได้แก่ “การใช้ AI ในการสร้างความมั่นคงและผาสุกของประเทศ (Harnessing AI to Advance Our Security and Prosperity)” - จัดตั้งศูนย์ปัญญาประดิษฐ์ร่วม (Joint Artificial Intelligence Center) - ปี ค.ศ.2018 กระทรวงกลาโหมสหรัฐฯ ออก “ยุทธศาสตร์สร้างความทันสมัยด้านดิจิทัล (Digital Modernization Strategy)” เพื่อสร้างสถาปัตยกรรมเทคโนโลยีสารสนเทศ | <ul style="list-style-type: none"> - ปี ค.ศ.2017 จีนประกาศ “แผนพัฒนาปัญญาประดิษฐ์รุ่นใหม่ (New Generation Artificial Intelligence Development Plan: AIDP)” แสดงให้เห็นถึงการให้ความสำคัญกับ AI ในการสร้างความได้เปรียบเชิงการแข่งขันและการรักษาความมั่นคงแห่งชาติ - จีนกล่าวถึงการสร้างความฉลาด “Intelligentized” (智能化) ให้กับเทคโนโลยีทางทหารซึ่งจะเป็นพื้นฐานของสงครามอนาคต ทั้งนี้การใช้คำว่า “การสร้างฉลาด” เป็นสัญญาณว่า การพัฒนาเทคโนโลยีทางทหารของกองทัพจีนได้ก้าวข้ามคำว่า เทคโนโลยีสารสนเทศไปสู่ AI เป็นที่เรียบร้อยแล้ว - จีนมุ่งหมายเพื่อใช้ AI ในการสร้างความได้เปรียบในการแสวงหาประโยชน์จากข่าวกรอง และเร่งความเร็วกระบวนการตัดสินใจในสนามรบ - จีนสนับสนุนทุกกิจกรรมที่เกี่ยวข้องกับเทคโนโลยี AI ให้เข้ามาเป็นส่วนหนึ่งของการป้องกันประเทศ | <ul style="list-style-type: none"> - ปี ค.ศ.2017 รัฐบาลสิงคโปร์ได้ประกาศแผนยุทธศาสตร์ของประเทศด้านปัญญาประดิษฐ์ หรือ “National Artificial Intelligence Strategy” - ปี ค.ศ.2017 รัฐบาลสิงคโปร์เปิดตัวหน่วยงาน “AI Singapore” เพื่อเป็นการกระตุ้นและพัฒนาความสามารถด้าน AI ของสิงคโปร์ - ปี ค.ศ.2017 AI เข้ามาเป็นส่วนหนึ่งของการปฏิบัติการด้านไซเบอร์ (Cyber Operation) โดยกระทรวงกลาโหมสิงคโปร์ได้จัดตั้ง “องค์กรป้องกันทางไซเบอร์ (Defence Cyber Organisation: DCO)” เพื่อสนับสนุนกองทัพและรัฐบาล (Singapore’s whole-of-government: WoG) ในการส่งเสริมความมั่นคงทางไซเบอร์ - ปี ค.ศ.2019 กระทรวงกลาโหมสิงคโปร์ ได้เปิดตัวพันธกิจใหม่ในมิติที่หก “การเป็นกลาโหมดิจิทัล (Digital Defense)” ภายใต้ยุทธศาสตร์ Total Defence |
| 2. การจัดการบุคลากรให้มีความชำนาญและองค์ความรู้ | <ul style="list-style-type: none"> - การสร้างและเพิ่มพูนขีดความสามารถด้าน AI ให้กับบุคลากรของกองทัพ - การพัฒนาองค์ความรู้ และสร้างทักษะเฉพาะทางด้าน AI จากพันธมิตร - การรับสมัครบุคลากรที่มีความเป็นเลิศด้าน AI เข้าประจำการในกองทัพ - การรับสมัครบุคลากรที่เชี่ยวชาญ และการเพิ่มพูนขีดความสามารถบุคลากรของกองทัพผ่านการฝึก/ ศึกษา | <ul style="list-style-type: none"> - จีนประสบปัญหาการขาดแคลนบุคลากรผู้เชี่ยวชาญด้าน AI ทั้งวิศวกร นักวิจัย และนักข้อมูลวิทยา - บุคลากรผู้เชี่ยวชาญดังกล่าวในจีนมีประสบการณ์ไม่ถึง 5 ปี - จีนได้ทุ่มความพยายามท่ามกลางความขาดแคลนบุคลากรผู้เชี่ยวชาญด้าน AI โดยใช้บุคลากรดังกล่าวไปในการพัฒนา AI ในกิจการทหาร | <ul style="list-style-type: none"> - ปี ค.ศ.2017 ลงนามความร่วมมือด้าน AI กับศูนย์ประสานงานขับเคลื่อนยุทธศาสตร์ปัญญาประดิษฐ์ (Joint Artificial Intelligence Center: JAIC) ของกระทรวงกลาโหมสหรัฐฯ - จัดตั้งหลักสูตร Cyber Specialist Cadet Course (CSCC) เพื่อสร้างบุคลากรทางทหารที่เชี่ยวชาญด้าน AI - มีความร่วมมือกับสถาบันการศึกษาในสาขาปัญญาประดิษฐ์ |

ตารางที่ 3 การเปรียบเทียบตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของกองทัพแต่ละประเทศ (ต่อ)

| ระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ของกองทัพแต่ละประเทศ | | | |
|---|---|---|---|
| ตัวแบบระบบนิเวศปัญญาประดิษฐ์ | สหรัฐอเมริกา | สาธารณรัฐประชาชนจีน | สาธารณรัฐสิงคโปร์ |
| 3. การวิจัยและพัฒนา ด้าน AI | <ul style="list-style-type: none"> - ปี ค.ศ.2018 กองทัพสหรัฐฯ ให้ความสำคัญกับการวิจัยและพัฒนาด้าน AI โดยให้องค์การโครงการวิจัยขั้นสูงด้านความมั่นคง (Defense Advanced Research Projects Agency: DARPA) ของกองทัพทำการวิจัยและค้นหาค้นลูกต่อไปของเทคโนโลยี AI - บริการระบบคลาวด์และเอเดจ เพื่อกระจายศูนย์ (Decentralize) รวมทั้งการพัฒนาและทดลองให้ขยายวงกว้างออกไปสู่ภาคส่วนที่เกี่ยวข้อง | <ul style="list-style-type: none"> - กองทัพจีนมีหน่วยงานของกองทัพที่ดำเนินการด้านการวิจัยและพัฒนา ด้าน AI เช่น สถาบัน Institute for Intelligent Sciences ภายใต้ PLA National University of Defense Technology และสถาบัน National Innovation Institute of Defense Technology (NIIDT) ที่ประกอบด้วย ศูนย์วิจัย Artificial Intelligence Research Center (AIRC) - การจัดตั้งหลักสูตรการศึกษาเกี่ยวกับ AI ทางทหารขึ้นเป็นหลักสูตรแรกในโลก | <ul style="list-style-type: none"> - จัดตั้งสำนักงานวิทยาศาสตร์และเทคโนโลยีการป้องกันประเทศ (The Defence Science and Technology Agency: DSTA) ซึ่งมีการฝึกในการออกแบบและพัฒนาเทคโนโลยี AI ในกิจการด้านไซเบอร์ของกองทัพสิงคโปร์ - จัดตั้งองค์การวิทยาศาสตร์กลาโหม(The Defence Science Organisation) ซึ่งเป็นองค์กรวิจัยและพัฒนาด้านการป้องกันประเทศที่ใหญ่ที่สุดของสิงคโปร์ - จัดสรรงบประมาณ 45 ล้าน ดอลลาร์สหรัฐฯ ทุกปี ให้ห้องปฏิบัติการด้าน Artificial Intelligence and Robotics |
| 4. ความร่วมมือภาครัฐ และเอกชน | <ul style="list-style-type: none"> - กระทรวงกลาโหมสหรัฐฯ ได้ทุ่มงบประมาณในสัดส่วนที่มากที่สุดไปในระบบ AI โดยเฉพาะการพัฒนาระบบการเรียนรู้และปัญญา (Learning and Intelligence) ร่วมกับบริษัทเอกชน สำหรับการพัฒนาระบบ AI - ภายใต้ยุทธศาสตร์ปัญญาประดิษฐ์ กระทรวงกลาโหมสหรัฐฯ มีแนวทางในการร่วมมือกับภาคเอกชน การศึกษา ประเทศพันธมิตร และคู่สัญญา | <ul style="list-style-type: none"> - การลงทุนด้าน AI ในกิจการด้านความมั่นคงของจีนดำเนินการตามเส้นทาง Military-civil Fusion-style Innovation ที่เป็นการผนวกรวมนวัตกรรมทางทหารเข้ากับระบบนวัตกรรมแห่งชาติกับภาคส่วนที่เกี่ยวข้อง - กระทรวงกลาโหมจีนทุ่มเทความพยายามในการวิจัยและพัฒนา AI ผ่านความร่วมมือระหว่างพลเรือนและทหาร เช่น โครงการ New AI/ Machine Learning ภายใต้ห้องทดลอง Military Intelligence และ Military Civil Fusion National Defense Peak Technologies Laboratory เพื่อพัฒนาเทคโนโลยีอุบัติใหม่ | <ul style="list-style-type: none"> - จัดตั้ง “ชุมชนเทคโนโลยีป้องกันประเทศ(Defence Technology Community)” เพื่อเป็นแหล่งรวบรวมหน่วยงานที่มีหน้าที่รับผิดชอบในการวางแผน การวิจัย และการพัฒนาด้านเทคโนโลยี AI - กระทรวงกลาโหมสิงคโปร์ได้เข้ามามีส่วนร่วมสนับสนุนรัฐบาลในการทำงานอย่างใกล้ชิดกับภาคส่วนต่างๆ ในการสร้างความเชี่ยวชาญ และสนับสนุนทรัพยากรในการตอบสนอง และการดำเนินการกู้คืนระบบหากเกิดเหตุการณ์วิกฤตภายในประเทศ |

ตารางที่ 3 การเปรียบเทียบตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของกองทัพแต่ละประเทศ (ต่อ)

| ระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ของกองทัพแต่ละประเทศ | | | |
|--|--|---------------------|--|
| ตัวแบบระบบนิเวศปัญญาประดิษฐ์ | สหรัฐอเมริกา | สาธารณรัฐประชาชนจีน | สาธารณรัฐสิงคโปร์ |
| 5. โครงสร้างหรือหน่วยงานจัดการด้านข้อมูลและการรักษาความปลอดภัยทางไซเบอร์ | <ul style="list-style-type: none"> - มีผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกระทรวงกลาโหม (DoD Chief Information Officer: DoD CIO) ในการขับเคลื่อนยุทธศาสตร์ดิจิทัล - จัดตั้งคณะกรรมการ JIE (JIE Executive Committee: JIE EXCOM) ประกอบด้วย ผู้แทนจาก DoD CIO กองบัญชาการไซเบอร์สหรัฐฯ (U.S. Cyber Command) และเสนาธิการร่วมด้านการสื่อสาร (Joint Staff 6) ทำหน้าที่สร้างการประสานสอดคล้องของหน่วยงานที่เกี่ยวข้อง | - | <ul style="list-style-type: none"> - มีการจัดตั้ง Defence Cyber Group โดยขึ้นตรงกับสำนักผู้บังคับบัญชา (Defence Cyber Chief) มีหน้าที่รับผิดชอบ ได้แก่ 1) ดูแลความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ตลอด 24 ชั่วโมง 2) กำกับดูแลการพัฒนาความสามารถในการป้องกันโลกไซเบอร์โดยรวม และ 3) การประเมินความเสี่ยงและการเพิ่มความแข็งแกร่งให้กับการป้องกันทางไซเบอร์ของกระทรวงกลาโหม |

แนวทางการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทยเพื่อรองรับสงครามในอนาคต

จากการศึกษาข้างต้น จึงนำมาสู่แนวทางการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทยเพื่อรองรับสงครามในอนาคต ดังนี้

1. การสนับสนุนเชิงนโยบายจากภาครัฐ

กระทรวงกลาโหมควรมี “แผนปฏิบัติการปัญญาประดิษฐ์” หรือ “แผนปฏิบัติการสร้างความทันสมัยด้านดิจิทัล (Digital Modernization Plan)” เพื่อกำหนดเป็นแผนปฏิบัติการที่มุ่งเน้นการส่งเสริมระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ทั้งระบบในลักษณะ “การปฏิบัติการด้านดิจิทัล (Digital Operations)” ที่ประกอบด้วย ปัญญาประดิษฐ์ (AI) ระบบคลาวด์ (CLOUD) ระบบบัญชาการ

ควบคุมและการสื่อสาร (Command Control Communication: C3) และความปลอดภัยด้านไซเบอร์ (Cyber) บน “สภาพแวดล้อมด้านสารสนเทศร่วม (Joint Information Environment: JIE)” ของกระทรวงกลาโหม ตลอดจนความขัดแย้ง (Military Spectrum of Conflict)

สำหรับกองบัญชาการกองทัพไทย ควรมีแผนปฏิบัติการหรือแผนปฏิบัติราชการ ในการเสริมสร้างระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) อย่างเป็นรูปธรรมตาม “แผนปฏิบัติการปัญญาประดิษฐ์” หรือ “แผนปฏิบัติการสร้างความทันสมัยด้านดิจิทัล (Digital Modernization Plan)” ตามแนวทางของกระทรวงกลาโหม เพื่อกำหนดแผนปฏิบัติการ หรือแผนปฏิบัติราชการที่มุ่งเน้นการส่งเสริมระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ของกองบัญชาการกองทัพไทย

2. การจัดการบุคลากรให้มีความชำนาญและองค์ความรู้

กองบัญชาการกองทัพไทย ควรมีการจัดตั้ง “ศูนย์เพื่อความเป็นเลิศด้าน AI” (Center for Excellence) ของกองบัญชาการกองทัพไทย เพื่อเป็นหน่วยงานสำคัญในการสร้าง พัฒนา และเพิ่มพูนขีดความสามารถของบุคลากรด้าน AI ของกองบัญชาการกองทัพไทยในมิติต่าง ๆ เช่น 1) การสร้างทักษะเฉพาะทาง และการพัฒนาองค์ความรู้ด้าน AI 2) การเพิ่มพูนขีดความสามารถบุคลากรของกองบัญชาการกองทัพไทยผ่านการฝึก/ศึกษา และ 3) มีการจัดตั้งหลักสูตรด้าน AI ร่วมกันระหว่างกองบัญชาการกองทัพไทยกับสถาบันการศึกษา เป็นต้น

3. การวิจัยและพัฒนาด้าน AI

กระทรวงกลาโหม ควรจัดตั้ง “ศูนย์ปัญญาประดิษฐ์ร่วม (Joint Artificial Intelligence Center: JAIC)” เพื่อสร้างวัฒนธรรมการทำงานร่วมกันของเหล่าทัพ และหน่วยงานความมั่นคง ให้สามารถนำเทคโนโลยีปัญญาประดิษฐ์เข้ามาเป็นส่วนหนึ่งของการปฏิบัติงานอย่างไร้รอยต่อ ควบคู่กับการเป็นผู้นำในด้านจริยธรรมทางทหารและความปลอดภัย AI และให้ “ศูนย์ปัญญาประดิษฐ์ร่วม (Joint Artificial Intelligence Center: JAIC)” เป็นองค์กรสำคัญในการวิจัยและพัฒนาด้าน AI ของกองบัญชาการกองทัพไทย เช่น 1) การเป็นแหล่งรวบรวม แบ่งปันข้อมูล และเครื่องมือด้าน AI ร่วมกับภาคส่วนอื่น 2) การให้บริการระบบคลาวด์ และเอเดจ์เพื่อกระจายศูนย์ (Decentralize) การพัฒนา และทดลองให้ขยายวงกว้างออกไปสู่ภาคส่วนที่เกี่ยวข้อง 3) มีการจัดทำงานวิจัยด้าน AI (Joint AI Research) ร่วมกับสถาบันการศึกษาทั้งในประเทศและต่างประเทศ และ 4) มีฐานข้อมูลกลาง เพื่อการแบ่งปันข้อมูลในการรักษาความมั่นคงปลอดภัยไซเบอร์ (ภายใต้การมีชั้นความลับ) ของกองบัญชาการกองทัพไทย เป็นต้น

4. ความร่วมมือภาครัฐและเอกชน

กองบัญชาการกองทัพไทย ควรมีการดำเนินการความร่วมมือกับภาครัฐและเอกชน ในลักษณะ “Military-civil Fusion-style innovation” เพื่อสร้างความเชี่ยวชาญด้าน AI และควรขยายความร่วมมือด้าน AI ในมิติต่าง ๆ เช่น การลงทุนในการพัฒนาขีดความสามารถทางวิทยาศาสตร์ และนวัตกรรมใหม่ ๆ และการนำ AI มาใช้ในการรองรับการเติบโตของอุตสาหกรรมป้องกันประเทศ เป็นต้น พร้อมทั้งจัดตั้ง “ชุมชนปัญญาประดิษฐ์” (AI Community) เพื่อเป็นแหล่งรวบรวมหน่วยงานที่มีหน้าที่รับผิดชอบในการวางแผน การวิจัย และการพัฒนาด้านเทคโนโลยี AI ของทุกภาคส่วนเข้าด้วยกัน

5. โครงสร้างหรือหน่วยงานจัดการด้านข้อมูล และการรักษาความปลอดภัยทางไซเบอร์

สำหรับโครงสร้างหรือหน่วยงานจัดการด้านข้อมูล ภายใต้ “แผนปฏิบัติการปัญญาประดิษฐ์” หรือ “แผนปฏิบัติการสร้างความทันสมัยด้านดิจิทัล (Digital Modernization Plan)” ของกระทรวงกลาโหม นั้นกองบัญชาการกองทัพไทย ควรมีกิจกรรมในการสนับสนุนการปฏิบัติงานในลักษณะ “การปฏิบัติการด้านดิจิทัล (Digital Operations)” พร้อมทั้งควรทำหน้าที่ในการสนับสนุนให้เกิดโครงสร้างหรือหน่วยงานจัดการด้านข้อมูลและการรักษาความปลอดภัยทางไซเบอร์ในลักษณะสภาพแวดล้อมด้านสารสนเทศร่วม (Joint Information Environment: JIE) ที่สนับสนุนการดำเนินงานของ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกระทรวงกลาโหม (MoD Chief Information Officer: MoD CIO)

สรุปได้ว่า แนวทางการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทยเพื่อรองรับสงครามในอนาคต ประกอบด้วย 5 ประการที่สำคัญ ดังกล่าวข้างต้น อันจะช่วยสนับสนุนองค์ประกอบของระบบ “การปฏิบัติการด้านดิจิทัล (Digital Operations)” ที่ประกอบด้วย ปัญญาประดิษฐ์

(AI) ระบบคลาวด์ (CLOUD) ระบบบัญชาการควบคุมและการสื่อสาร (Command Control Communication: C3) และความปลอดภัยด้านไซเบอร์ (Cyber) เพื่อให้กองทัพ

สามารถปฏิบัติการได้ตลอดย่านความขัดแย้ง (Military Spectrum of Conflict) (European Union Military Staff, 2014) ดังตัวแบบตามภาพด้านล่าง



ภาพ ตัวแบบระบบนิเวศของปัญญาประดิษฐ์ในการส่งเสริมกิจการของกองทัพไทย

บทสรุป

การศึกษา “**ตัวแบบระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทย**” ประกอบด้วย 3 ส่วนคือ **ส่วนที่หนึ่ง** การศึกษาตัวแบบระบบนิเวศปัญญาประดิษฐ์จากสถาบันคลังสมอง (Think Tank) ระดับโลก ได้แก่ 1) สถาบัน Center for Strategic and International Studies ซึ่งเป็นสถาบันคลังสมองด้านความมั่นคงของสหรัฐฯ 2) สถาบัน McKinsey Global Institute (MGI) ซึ่งเป็นสถาบันวิจัยด้านเศรษฐกิจจากภาคเอกชน 3) ศูนย์วิจัย Oxford Insights and the International Development Research Centre และ 4) Tortoise Intelligence ซึ่งเป็นสื่อสารมวลชนด้านเทคโนโลยี ทำให้สามารถกำหนดตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของบทความฉบับนี้ได้ 5 ประเด็น ได้แก่ 1) การสนับสนุนเชิงนโยบายจากภาครัฐ 2) การจัดการ

บุคลากรให้มีความชำนาญและองค์ความรู้ 3) การวิจัยและพัฒนาด้าน AI 4) ความร่วมมือภาครัฐและเอกชน และ 5) โครงสร้างหรือหน่วยงานจัดการด้านข้อมูลและการรักษาความปลอดภัยทางไซเบอร์ **ส่วนที่สอง** การศึกษาตัวอย่างของประเทศที่ประสบความสำเร็จด้านการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ ได้แก่ 1) สหรัฐอเมริกา 2) สาธารณรัฐประชาชนจีน และ 3) สาธารณรัฐสิงคโปร์ จากสถาบัน McKinsey Global Institute ศูนย์วิจัย Oxford Insights and the International Development Research Centre และ Tortoise Intelligence **ส่วนที่สาม** การศึกษาตัวแบบระบบนิเวศของปัญญาประดิษฐ์ของกองทัพแต่ละประเทศ ได้แก่ 1) กระทรวงกลาโหมสหรัฐฯ 2) กระทรวงกลาโหมสาธารณรัฐประชาชนจีน และ 3) กระทรวงกลาโหมสาธารณรัฐสิงคโปร์ จนนำมาสู่แนวทางการพัฒนาระบบนิเวศของปัญญาประดิษฐ์

(AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทย เพื่อรองรับสงครามในอนาคต

โดย “**แนวทางการพัฒนาระบบนิเวศของปัญญาประดิษฐ์ (AI Ecosystem) ในการส่งเสริมกิจการของกองทัพไทยเพื่อรองรับสงครามในอนาคต**” ได้แก่

- 1) การสนับสนุนเชิงนโยบายจากภาครัฐ ควรมี “แผนปฏิบัติการปัญญาประดิษฐ์” หรือ “แผนปฏิบัติการสร้างความทันสมัยด้านดิจิทัล (Digital Modernization Plan)” เพื่อกำหนดเป็นแผนปฏิบัติการที่มุ่งเน้นการส่งเสริมระบบนิเวศของ AI
- 2) การจัดการบุคลากรให้มีความชำนาญและองค์ความรู้ ควรมีการจัดตั้ง “ศูนย์เพื่อความเป็นเลิศด้าน AI” (Center for Excellence) เพื่อเป็นหน่วยงานสำคัญในการสร้าง พัฒนา และเพิ่มพูนขีดความสามารถของบุคลากรด้าน AI
- 3) การวิจัยและพัฒนาด้าน AI ควรจัดตั้ง “ศูนย์ปัญญาประดิษฐ์ร่วม (Joint Artificial Intelligence Center: JAIC)” เพื่อสร้างวัฒนธรรมการทำงานร่วมกันของเหล่าทัพ และหน่วยงานความมั่นคงอย่างไร้รอยต่อ ควบคู่กับการเป็นผู้นำในด้านจริยธรรมทางทหารและความปลอดภัย AI
- 4) ความร่วมมือภาครัฐและเอกชน ควรมีการดำเนินความร่วมมือกับภาครัฐและเอกชน ในลักษณะ “Military-civil Fusion-style innovation” เพื่อสร้างความเชี่ยวชาญ และขยายความร่วมมือด้าน AI ในมิติต่าง ๆ และ
- 5) โครงสร้างหรือหน่วยงานจัดการด้านข้อมูล และการรักษาความปลอดภัยทางไซเบอร์ ควรมีการรักษาความปลอดภัยทางไซเบอร์ในลักษณะสภาพแวดล้อมด้านสารสนเทศร่วม (Joint Information Environment: JIE) ที่สนับสนุนการดำเนินงานของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกระทรวงกลาโหม (MoD Chief Information Officer: MoD CIO) อันจะช่วยสนับสนุนองค์ประกอบของระบบ “การปฏิบัติการด้านดิจิทัล (Digital Operations)” เพื่อให้กองทัพสามารถปฏิบัติการได้ตลอดย่านความขัดแย้ง (Military Spectrum of Conflict)

บทส่งท้าย: ควอนตัมเทคโนโลยีกับสงครามในอนาคต

ขณะที่เรากำลังรับรู้ถึงการปฏิวัติอุตสาหกรรมครั้งที่ 4 ซึ่งเกิดจากความก้าวหน้าทาง “เทคโนโลยีอย่างก้าวกระโดด (Exponential Technology)” หนึ่งในนั้นคือ “ปัญญาประดิษฐ์ (Artificial Intelligence: AI)” ซึ่งเราได้เห็นศักยภาพของ AI ในการเข้ามามีส่วนร่วมในการปฏิบัติงานและการใช้ชีวิตในปัจจุบันและอนาคตอย่างที่เราอาจคาดไม่ถึง และเรายังคงพัฒนา AI ให้มีขีดความสามารถที่ตอบสนองได้ดียิ่งขึ้นไปอีก ตลอดหลายปีที่ผ่านมาเรายังได้เห็นการเจริญเติบโตอย่างแข็งแกร่งในนวัตกรรมคอมพิวเตอร์ทั้งพลังและความเร็วในการคำนวณ ซึ่งขีดจำกัดของคอมพิวเตอร์ที่ใช้ในการประมวลผลอาจเป็นขีดจำกัดต่อการขยายศักยภาพใน “การเรียนรู้ของเครื่องจักร (Machine learning)” ของ AI ด้วย เนื่องจาก “วิธีการคำนวณของคอมพิวเตอร์” ในปัจจุบัน ที่ใช้ “การคำนวณแบบเลขฐานสอง (Binary Calculation)” โดยคอมพิวเตอร์ จะดำเนินการคำนวณได้คราวละ 1 คู่ ซึ่งประเด็นดังกล่าวเป็นอุปสรรคต่อการขยายศักยภาพของ AI หากเราต้องการให้ AI ทำงานที่ซับซ้อน เช่น การวิเคราะห์ การตัดสินใจ หรือการบริหารจัดการอย่างมีประสิทธิภาพอย่างเป็นอัตโนมัติ และตอบสนองอย่างรวดเร็ว ย่อมต้องอาศัยข้อมูลจำนวนมากและการคำนวณที่ซับซ้อนมากยิ่งขึ้น

ดังนั้น “การคำนวณควอนตัม (Quantum Computing)” ที่มีขีดความสามารถในการรองรับสถานะการคำนวณได้ 4 คู่ ในคราวเดียวกัน ทำให้การคำนวณควอนตัมสามารถรองรับปริมาณข้อมูลสำหรับการคำนวณได้มากกว่า เมื่อเทียบกับการคำนวณแบบเดิม ซึ่งหมายถึงความเร็วของการประมวลผลที่เพิ่มมากขึ้นอย่างมาก และนำไปสู่การสร้างการทำงานของ AI ที่ซับซ้อนมากยิ่งขึ้นตลอดจนเทคโนโลยีอื่นที่ต้องอาศัย การคำนวณที่ซับซ้อนอย่างมากในที่สุด เช่น 1) การเข้ารหัส (Encryption) ในการรองรับการเข้ารหัสขั้นสูง (High-level Cryptography)

2) ความมั่นคง ในการปรับปรุงขีดความสามารถด้านการป้องกันประเทศ 3) โทรคมนาคม ในการจัดการกับข้อมูลและความปลอดภัยทางการสื่อสารอย่างเหมาะสม 4) พลังงาน ในการจัดการกับการใช้พลังงานและการค้นหาแหล่งพลังงานใหม่ 5) ธุรกิจและการเงิน ในการเพิ่มประสิทธิภาพการดำเนินงานและการใช้ทรัพยากร และ 6) สุขภาพ ในการคิดค้นสูตรยา วัคซีน ตลอดจนการรักษาผู้ป่วย เป็นต้น เช่นเดียวกับเครื่องจักรไอน้ำและไมโครโปรเซสเซอร์ที่ครั้งหนึ่งเคยเปลี่ยนโฉมหน้าของอุตสาหกรรมทั้งหมดไปอย่างสิ้นเชิง ดังนั้น “เทคโนโลยีควอนตัม (Quantum Technology)” หรือเทคโนโลยีที่เกิดจากการคำนวณควอนตัมจะสามารถสร้างสรรค์ธุรกิจประเภทใหม่ ตลอดจนกำหนดกรอบสำหรับการพัฒนาในอนาคตซึ่งรวมถึง AI (Haddad, Schinasi-Halet, Moutaouakil, Saf and Belhouchat, 2019)

สำหรับงานด้านความมั่นคง เทคโนโลยีควอนตัมได้ถูกนำมาประยุกต์ใช้เพื่อเสริมประสิทธิภาพของเทคโนโลยีด้านความมั่นคงที่ใช้อยู่ในปัจจุบัน และกำลังเปลี่ยนโฉมหน้าของสงครามในอนาคต เช่น 1) การตรวจจับและมาตรวิทยาควอนตัม (Quantum Sensing and Metrology) เช่น Light Detection and Ranging (LiDAR) Quantum ที่มีประสิทธิภาพตรวจจับที่ดีกว่า ขณะที่ใช้พลังงานที่ต่ำกว่า เรดาร์ หรือ LiDAR แบบเดิม 2) การเข้ารหัสและการสื่อสารควอนตัม (Quantum Cryptography and Communication) ทำให้การสื่อสารมีความปลอดภัยมากขึ้นผ่าน “การเข้ารหัสเชิงควอนตัม (Quantum Key distribution: QKD)” ซึ่งช่วยรักษาความปลอดภัยทางการสื่อสารที่มีความอ่อนไหวสูง และ 3) การคำนวณควอนตัม (Quantum Computing) เป็นกุญแจสำคัญในการสร้างประสิทธิภาพการทำงานของ การตรวจจับ และมาตรวิทยาควอนตัม การเข้ารหัสและการสื่อสารควอนตัมและเพิ่มขีดความสามารถการเรียนรู้ของ AI เพื่อนำไปสู่การปฏิบัติงาน

ความมั่นคงที่ซับซ้อน เช่น การอำนวยความสะดวกและการส่งกำลังบำรุงที่พอเหมาะต่อ “เขตปฏิบัติการสงคราม (Theater of War)” และการวางแผนการใช้ทรัพยากรที่เหมาะสมในแต่ละย่านการปฏิบัติการ (Spectrum of operation) (Wolf et al., 2019)

จากศักยภาพของเทคโนโลยีควอนตัม ทำให้หลายประเทศต่างลงทุนอย่างมหาศาลในด้านการวิจัยควอนตัม เพื่อสร้างความได้เปรียบเชิงเศรษฐกิจและทางทหาร เช่น สาธารณรัฐประชาชนจีนกับการบรรลุความสำเร็จในเทคโนโลยีควอนตัมในปี ค.ศ.2030 สหรัฐอเมริกาลงทุนอย่างมหาศาลในเทคโนโลยี “ควอนตัมคอมพิวเตอร์” และ “การสื่อสารบนพื้นฐานควอนตัม (Quantum-based Communications)” สหภาพยุโรปสนับสนุนงบประมาณระยะยาว 10 ปี ในโครงการ “European Commission’s quantum-technologies Flagship Programme” และรัสเซีย ได้ลงทุนในการคำนวณควอนตัมผ่าน “ศูนย์ควอนตัมแห่งรัสเซีย (Russian Quantum Center)” เป็นต้น

นอกจากนี้ เทคโนโลยีควอนตัมยังส่งผลกระทบต่อความมั่นคงของชาติ เช่น 1) การสูญเสียความลับโดยการเข้ารหัส (Cryptograh) เป็นหนทางหนึ่งในการรักษาความปลอดภัยทางข้อมูล ซึ่ง “ควอนตัมคอมพิวเตอร์” สามารถถอดรหัส RSA (Rivest-Shamir-Adleman) ขนาด 2048 บิต ที่สร้างขึ้นโดยคอมพิวเตอร์ในปัจจุบันได้ในเวลาไม่กี่ชั่วโมง เราจึงได้เห็นหลายประเทศต่างกำลังพัฒนา “อัลกอริทึมสำหรับต่อต้านการถอดรหัสโดยควอนตัม (Quantum-resistant Algorithms)” สำหรับระบบ เช่น โทรคมนาคม 2) การสูญเสียทางการข่าว (Loss of Intelligence) ซึ่งการสื่อสารควอนตัม เป็นหนทางหนึ่งในการลดการสูญเสียดังกล่าวได้ผ่านเทคนิค เช่น การเข้ารหัสเชิงควอนตัม (Quantum Key Distribu-tion: QKD) และ LiDAR Quantum และ 3) การโจมตีทางควอนตัม

(Quantum Attack) ยิ่งทำให้การโจมตีต่อคอมพิวเตอร์ทำได้รวดเร็วและมีประสิทธิภาพมากขึ้น จึงจำเป็นต้องมีการพัฒนารูปแบบใหม่ของการเข้ารหัสในการป้องกันการโจมตีทางควอนตัมที่เรียกว่า “Post-Quantum Cryptography (PQC)” โดยกลุ่มผู้เชี่ยวชาญด้านควอนตัมจาก Google และเจ้าหน้าที่ด้านความปลอดภัยสารสนเทศจากภาคการบริการด้านการเงินคาดการณ์ว่า ในปี ค.ศ.2023 จะมีการนำมาตรฐานรักษาความปลอดภัยควอนตัมที่รวมถึง PQC มาใช้เพื่อป้องกันการโจมตีควอนตัม และปี ค.ศ.2033 จะเป็นปีที่ควอนตัมคอมพิวเตอร์จะสามารถถอด “รหัสกุญแจสาธารณะ (Public-key Cryptography)” หรือ RSA (Rivest-Shamir-Adleman) ได้ (Norris, 2020)

ขณะที่โลกกำลังเรียนรู้ที่จะใช้ประโยชน์จากเทคโนโลยีควอนตัม ซึ่งอาจสร้างคุณประโยชน์ หรือผลเสียให้เกิดขึ้นกับผู้มีส่วนได้ส่วนเสียในแต่ละบริบท เช่นเดียวกับบริบทด้านความมั่นคง เทคโนโลยีควอนตัมเป็นสิ่งขับเคลื่อนหนึ่งที่สำคัญที่มีผลต่อวิวัฒนาการของแนวคิด การวางแผน การปฏิบัติการ ตลอดจนการพัฒนาและใช้ AI ในสงครามอนาคต ซึ่งกองทัพและหน่วยงานที่เกี่ยวข้องควรเตรียมพร้อมในการพัฒนาและใช้ประโยชน์จากเทคโนโลยีควอนตัมได้อย่างมีประสิทธิภาพ ตลอดจนเตรียมพร้อมรับความท้าทายที่เกิดจากเทคโนโลยีดังกล่าวเช่นกัน

เอกสารอ้างอิง

- จรัสชัย หนูนักดี. (2562). ปัญหาประติษฐ์กับความมั่นคงแห่งชาติ. *เอกสารประกอบการประชุม Xiangshan Forum ครั้งที่ 9, 20-22 ตุลาคม 2562 ณ เมืองปักกิ่ง สาธารณรัฐประชาชนจีน*. กรุงเทพฯ: ศูนย์ศึกษายุทธศาสตร์สถาบันวิชาการป้องกันประเทศ.
- สถาบันนวัตกรรมและการเรียนรู้ มหาวิทยาลัยมหิดล. (2561). รู้จัก “Quantum Computing” เทคโนโลยีที่จะมาเปลี่ยนแปลงโลก. สืบค้นเมื่อ 8 เมษายน 2563, จาก <https://il.mahidol.ac.th/th/i-Learning-Clinic/computer-articles/รู้จัก-quantum-computing-เทคโนโลยีที่/>
- Allen, G. C. (2019). *Understanding China's AI Strategy*. Retrieved June, 23 2020, from <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>
- Department of Defense. (2019). *DoD Digital Modernization Strategy*. Retrieved June, 28 2020, from <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>
- European Union Military Staff. (2014). *EU Operations in a 'Wicked' World (Military adaptation to the Comprehensive Approach)*. Retrieved July, 14 2020, from <https://bit.ly/2QqoG8K>
- Haddad, M., Schinasi-Halet, G., Moutaouakil, A.E., Saf, J., & Belhouchat, S. (2019). *PwC point of view-Quantum Computing: A technology of the future already present*. Retrieved July, 14 2020, from <https://www.pwc.fr/fr/assets/files/pdf/2019/11/en-france-pwc-point-of-view-quantum-computing-2019.pdf>

- McKinsey Global Institute. (2018). *NOTES FROM THE AI FRONTIER: MODELING THE IMPACT OF AI ON THE WORLD ECONOMY*. Retrieved June, 24 2020 from <https://mck.co/3wRV9Wt>
- Ministry of Defence. (2019). *CYBER DEFENCE: DEFENCE CYBER ORGANISATION*. Retrieved June, 31 2020 from <https://bit.ly/3dgOcpU>
- Norris, M. (2020). *Quantum Computers Will Break the Internet, but Only If We Let Them*. Retrieved July, 14 2020 from <https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html>
- Oxford Insights and the International Development Research Centre. (2019). *Government Artificial Intelligence Readiness Index 2019*. Retrieved June, 24 2020 from <https://www.oxfordinsights.com/ai-readiness2019>
- Sheppard, L.R., Karlen, R., Hunter, A.P., and Balieiro, L., (2018). *ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY THE IMPORTANCE OF THE AI ECOSYSTEM*. Retrieved June, 24 2020 from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181102_AI_interior.pdf?6jofglR0rJ2qFc3.TCg8jQ8p.Mpc81X
- The RAND Corporation. (2020). *Quantum Computers Will Break the Internet, but Only If We Let Them*. Retrieved April, 17 2020 from <https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html>
- Tortoise Intelligence. (2019). *Global AI Index*. Retrieved June, 24 2020 from <https://members.tortoisemedia.com/2019/12/03/global-ai-index/content.html>
- Wolf, S.A., Joneckis, L.G., Waruhiu, S., Biddie, J.C., Sun, O.S., & Buckley, L. J. (2019). *Overview of the Status of Quantum Science and Technology and Recommendations for the DoD*. Retrieved July, 14 2020 from <https://bit.ly/3dhLb8Q>