THE APPLICATION OF AI TECHNOLOGY IN MILITARY: A STUDY OF AI IMPACTS ON CYBERSECURITY

ภูมิพัทธ ธัญยนพพร

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ

2566

ผลกระทบจากการใช้ปัญญาประดิษฐ์ทางทหารต่อความมั่นคงทางไซเบอร์

ภูมิพัทธ ธัญยนพพร

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
รัฐศาสตรมหาบัณฑิต สาขาวิชาการทูตและความสัมพันธ์ระหว่างประเทศ
คณะสังคมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
ปีการศึกษา 2566

THE APPLICATION OF AI TECHNOLOGY IN MILITARY:
A STUDY OF AI IMPACTS ON CYBERSECURITY

PHUMIPATH THUNYANOPPORN

A Master's Project Submitted in Partial Fulfillment of the Requirements

for the Degree of MASTER OF POLITICAL SCIENCE

(Diplomacy and International Relations)

Faculty of Social Sciences, Srinakharinwirot University

2023

สารนิพนธ์

เรื่อง

ผลกระทบจากการใช้ปัญญาประดิษฐ์ทางทหารต่อความมั่นคงทางไซเบอร์

ของ

ภูมิพัทธ ธัญยนพพร

ได้รับอนุมัติจากบัณฑิตวิทยาลัยให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญารัฐศาสตรมหาบัณฑิต สาขาวิชาการทูตและความสัมพันธ์ระหว่างประเทศ
ของมหาวิทยาลัยศรีนครินทรวิโรฒ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
คณบดีบัณฑิตวิทยาลัย

คณะกรรมการสอบปากเปล่าสารนิพนธ์

..... ที่ปรึกษาหลัก
(รองศาสตราจารย์ ดร.ศิพิมพ์ ศรบัลลังก์)

..... ประธาน
(อาจารย์ ดร.ศิบดี นพประเสริฐ)

..... กรรมการ
(อาจารย์ ดร.กุลนันทน์ คันธิก)

ชื่อเรื่อง	ผลกระทบจากการใช้ปัญญาประดิษฐ์ทางทหารต่อความมั่นคงทางไซเบอร์
ผู้วิจัย	ภูมิพัทธ ธัญยนพพร
ปริญญา	รัฐศาสตรมหาบัณฑิต
ปีการศึกษา	2566
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร. ศิพิมพ์ ศรบัลลังก์

การวิจัยนี้มุ่งศึกษาผลกระทบจากการพัฒนาและการใช้ปัญญาประดิษฐ์ ทางการทหารต่อความมั่นคงทางไซเบอร์ โดยการวิเคราะห์ว่าการนำปัญญาประดิษฐ์มาใช้ในการปฏิบัติการทางการทหารส่งผลกระทบอย่างไรต่อความมั่นคงทางไซเบอร์ ทั้งในเชิงบวกและเชิงลบ ผลการวิจัยพบว่าปัญญาประดิษฐ์ สามารถเพิ่มประสิทธิภาพในการตรวจจับและตอบโต้ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ซึ่งช่วยเสริมสร้างความมั่นคงของระบบไซเบอร์ ในทางกลับกันปัญญาประดิษฐ์ ก็สามารถเป็นเครื่องมือในการโจมตีทางไซเบอร์ที่มีความซับซ้อนและมีประสิทธิภาพมากขึ้น การศึกษานี้เน้นให้ความสำคัญกับการวิเคราะห์ผลกระทบต่อความมั่นคงทางไซเบอร์ที่เกิดขึ้นจากการใช้ปัญญาประดิษฐ์ ในทางการทหาร รวมถึงการเสนอแนะให้รัฐพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ให้พร้อมรับมือกับภัยคุกคามที่อาจเกิดขึ้นจากการใช้ AI เพื่อเสริมสร้างความมั่นคงของประเทศในทุกมิติ

คำสำคัญ : ปัญญาประดิษฐ์ทางการทหาร, ความมั่นคงทางไซเบอร์, การโจมตีทางไซเบอร์

Title	THE APPLICATION OF AI TECHNOLOGY IN MILITARY: A STUDY OF AI IMPACTS ON CYBERSECURITY
Author	PHUMIPATH THUNYANOPPORN
Degree	MASTER OF POLITICAL SCIENCE
Academic Year	2023
Thesis Advisor	Assoc. Prof. Dr. Sipim Sornbanlang

This research aims to study the impact of the development and use of artificial intelligence (AI) in military operations in term of cybersecurity. The analysis focuses on how the implementation of AI in military operations affects cybersecurity with both positive and negative aspects. The findings reveal that AI significantly enhanced the efficiency of detecting and countering cyber threats, thereby strengthening the security of cyber systems. Conversely, AI can also serve as a highly effective tool for conducting sophisticated cyberattacks. This study emphasizes the importance of analyzing the cybersecurity implications arising from the military use of AI and provides recommendations for states to develop a robust cyber infrastructure to cope with potential threats posed by the use of AI in military contexts, thereby enhancing national security across all dimensions.

Keyword : Cybersecurity, Cyber Attacks, Military AI

กิตติกรรมประกาศ

ข้าพเจ้าขอแสดงความขอบคุณอย่างยิ่งต่อทุกท่านที่มีส่วนร่วมและสนับสนุนการวิจัยครั้งนี้จนสำเร็จลุล่วง งานวิจัยชิ้นนี้จะไม่สามารถสำเร็จลุล่วงไปได้ หากปราศจากคำแนะนำอันทรงคุณค่าจากท่านอาจารย์ที่ปรึกษา รศ.ดร.ศิพิมพ์ ศรบัลลังก์ ที่ให้การสนับสนุนอย่างไม่ลดละ และกำลังใจตลอดระยะเวลาการทำวิจัย คำแนะนำและความเชี่ยวชาญของท่านได้ช่วยทำให้ข้าพเจ้าสามารถแก้ไขปัญหาและก้าวผ่านอุปสรรคต่าง ๆ ในการทำวิจัยครั้งนี้ได้อย่างราบรื่น

ขอขอบคุณ คณาจารย์ทุกท่านจาก ภาควิชารัฐศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ที่ให้การสนับสนุนและอบรมความรู้ นับตั้งแต่วันแรกที่ข้าพเจ้าเข้ามาศึกษา คณาจารย์ทุกท่านมีความสำคัญอย่างยิ่งในการทำให้การวิจัยนี้สามารถดำเนินไปได้อย่างสมบูรณ์

ขอขอบคุณ คุณอภิสรา ที่ได้ให้กำลังใจอย่างเต็มที่ตลอดระยะเวลาการทำวิจัย ขอบคุณมายด์มิ้งค์ สำหรับการแลกเปลี่ยนความคิดเห็นและความช่วยเหลือในการศึกษานับตั้งแต่ระดับปริญญาตรี และกำลังใจจากทุกท่านที่ไม่ได้เอ่ยถึง เป็นแรงผลักดันที่สำคัญและช่วยให้ข้าพเจ้ามีความมุ่งมั่นในการทำวิจัยครั้งนี้

ขอขอบคุณ คุณจิระเดช คุณจุฑามาศ และคุณไตรรัตน์ ครอบครัวของข้าพเจ้าที่ให้การสนับสนุนและความเข้าใจตลอดช่วงเวลาการทำวิจัย ความรักและกำลังใจจากท่านทำให้ข้าพเจ้ามีกำลังใจและความสามารถที่จะผ่านพ้นช่วงเวลาที่ยากลำบากมาได้

สุดท้ายนี้ ข้าพเจ้าขอขอบคุณตัวเองที่มีความมุ่งมั่นและพยายามอย่างไม่ลดละในการทำวิจัยครั้งนี้ การทำงานอย่างหนักและการยึดมั่นในเป้าหมายทำให้ข้าพเจ้าสามารถก้าวผ่านอุปสรรคและความท้าทายต่าง ๆ มาได้จนสำเร็จลุล่วง ขอบคุณตัวเองที่ไม่ยอมแพ้และมีความเชื่อมั่นในความสามารถของตนเอง ข้าพเจ้าหวังว่างานวิจัยฉบับนี้จะเป็นประโยชน์สำหรับหน่วยงานที่เกี่ยวข้องและผู้ที่สนใจศึกษาต่อไปในอนาคต

ภูมิพัทธ ธัญยนพพร

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

ปัจจุบันเทคโนโลยีสิ่งที่ขาดไม่ได้ทางการทหาร ที่มีการใช้งานมาอย่างยาวนานนับตั้งแต่สงครามได้เกิดขึ้น ทุกประเทศต่างพัฒนานวัตกรรมต่าง ๆ เพื่อนำมาใช้ในการรบและนำมาซึ่งชัยชนะ อย่างการพัฒนาอินเทอร์เน็ตที่ได้เกิดขึ้นจากโครงการทางทหาร กลายเป็นสายใยเชื่อมต่อผู้คนบนโลกให้เข้าถึงกันในยุคโลกาภิวัตน์ ผู้คนต่างสามารถเชื่อมต่อกันได้เพียงปลายนิ้วมือ เทคโนโลยีต่าง ๆ ได้รับการวิจัยและพัฒนาอย่างต่อเนื่อง ทั้งระบบประมวลผลการคำนวณทางคณิตศาสตร์ หรือการประมวลผลวิเคราะห์ข้อมูลต่าง ๆ ส่งผลให้เกิดการขยายตัวทางเทคโนโลยีจนแพร่หลายอย่างในปัจจุบัน เทคโนโลยีได้กลายมาเป็นส่วนหนึ่งในชีวิตประจำวัน ปริมาณข้อมูลการใช้งานที่มากขึ้น ได้ถูกนำไปต่อยอดและพัฒนาอย่างต่อเนื่อง หนึ่งในนั้นคือการนำไปพัฒนาเทคโนโลยีปัญญาประดิษฐ์ ที่ได้ก้าวเข้ามามีบทบาทมากยิ่งขึ้นเรื่อย ๆ โดยกลายมาเป็นเทคโนโลยีสำคัญในการประมวลผลข้อมูลต่าง ๆ ช่วยในการวิเคราะห์ข้อมูลได้อย่างรวดเร็ว จากความสามารถในการเข้าใจภาพ เสียง เนื้อหาข้อความและภาษามนุษย์ รวมไปถึงคลังความรู้ขนาดใหญ่ เปรียบเสมือนผู้เชี่ยวชาญในทุกด้านทั้งศาสตร์และศิลป์ จนกลายมาเป็นส่วนหนึ่งในเทคโนโลยีที่ได้ใช้ในตั้งแต่ในชีวิตประจำวัน ไปจนถึงการประมวลผลคำนวณขั้นสูง เบื้องหน้าที่เปรียบเสมือนผู้ช่วยที่มีความสามารถนั้น แต่ในอีกด้านหนึ่ง ปัญญาประดิษฐ์ได้ถูกนำไปใช้ในทางการทหาร ไม่ว่าจะเป็นทั้งในด้านหน่วยข่าวกรอง หรือการนำไปพัฒนาอาวุธเพื่อใช้สมรภูมิรบ และหนึ่งในนั้นคือการนำมาเป็นอาวุธไซเบอร์ จากภาพสมรภูมิรบที่คร่าชีวิตกันจากใบมีดดาบ ได้แปรเปลี่ยนเป็นการรบผ่านโครงข่ายทางไซเบอร์ ที่เป็นดั่งโครงสร้างพื้นฐานของประเทศที่เชื่อมโยงผู้คนภายในประเทศไปสู่ภายนอก ปัญญาประดิษฐ์ได้กลายเป็นเครื่องมือในการสร้างไวรัสการโจมตีที่มีความซับซ้อนและมีความอันตรายมากยิ่งขึ้นจากการประมวลผลขั้นสูง ข้อมูลต่าง ๆ ที่เป็นความลับและเกี่ยวข้องกับความมั่นคงของประเทศได้ถูกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต ไม่เพียงแค่หน่วยงานของรัฐบาลเท่านั้น ทั้งองค์กรที่ไม่เกี่ยวข้องกับรัฐ อุตสาหกรรมต่าง ๆ สถาบันการศึกษา หรือกลุ่มนักกิจกรรมเคลื่อนไหวทางการเมือง ต่างสามารถถูกโจมตีทางไซเบอร์ที่สร้างขึ้นโดยปัญญาประดิษฐ์และเข้าถึงฐานข้อมูลได้ภายในระยะเวลาเพียงเสี้ยววินาทีเท่านั้น

ดังนั้น ความมั่นคงทางไซเบอร์จึงกลายมาเป็นอีกหนึ่งในความมั่นคงระหว่างประเทศสมัยใหม่ ที่รัฐต้องหันมาให้ความสำคัญและให้การสนับสนุนการวิจัยและพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ เนื่องจากการป้องกันระบบไซเบอร์จากการโจมตีแบบดั้งเดิมนั้นไม่ปลอดภัยอีกต่อไป

ดังเช่นประเทศมหาอำนาจต่าง ๆ ที่มีการวางรากฐานและนโยบายทางปัญญาประดิษฐ์มาใช้ในการป้องกันความมั่นคงทางไซเบอร์นี้จากภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้ในอนาคต

1.2 **คำถามวิจัย**

จากการพัฒนาเทคโนโลยีปัญญาประดิษฐ์ทางการทหารส่งผลกระทบต่อความมั่นคงทางไซเบอร์อย่างไร

1.3 **สมมติฐานการวิจัย**

การพัฒนาและการนำเทคโนโลยีปัญญาประดิษฐ์ทางการทหารมาใช้ส่งผลกระทบต่อความมั่นคงทางไซเบอร์ทั้งในเชิงบวกและเชิงลบ รัฐต่าง ๆ จึงควรที่จะต้องหันมาให้ความสำคัญต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากผลพวงของการพัฒนาเทคโนโลยีปัญญาประดิษฐ์ที่ใช้ในทางการทหาร และนำปัญญาประดิษฐ์มาใช้ให้เกิดประโยชน์สูงสุดต่อความมั่นคงของรัฐ

1.4 **ทบทวนวรรณกรรม**

การทบทวนวรรณกรรมเกี่ยวกับการใช้เทคโนโลยีปัญญาประดิษฐ์ในความมั่นคงทางไซเบอร์สามารถแบ่งออกได้เป็นสามส่วนหลัก ได้แก่ พัฒนาการของการใช้ปัญญาประดิษฐ์ การประยุกต์ใช้ปัญญาประดิษฐ์ในภาคอุตสาหกรรมและการทหาร และผลกระทบจากการใช้ปัญญาประดิษฐ์ทางการทหาร ในส่วนสุดท้ายจะเพิ่มเติมมุมมองและการวิจัยอื่น ๆ เพื่อหาช่องว่างและเติมเต็มการศึกษาในอนาคต

ในด้านพัฒนาการของการใช้ปัญญาประดิษฐ์ การพัฒนาปัญญาประดิษฐ์เริ่มต้นขึ้นในปี 1950 โดยนักคณิตศาสตร์ อลัน ทัวริ่ง (Alan Turing) ที่เสนอคำถามเกี่ยวกับความสามารถในการคิดของเครื่องจักร การทดสอบทัวริ่ง (Turing Test) ที่ทัวริ่งเสนอเป็นการทดสอบให้เครื่องจักรพิมพ์ตอบโต้สนทนากับมนุษย์ และให้ผู้ทดสอบพยายามแยกว่าเป็นเครื่องจักรหรือมนุษย์ ถ้าไม่สามารถแยกแยะได้หมายความว่าเครื่องจักรนั้นผ่านการทดสอบแล้ว ตั้งแต่นั้นมา ปัญญาประดิษฐ์ได้รับการพัฒนาอย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งในส่วนของการเรียนรู้ของเครื่องจักร (Machine Learning: ML) ซึ่งช่วยให้เครื่องจักรสามารถทำการคำนวณและตัดสินใจในระดับที่สูงขึ้น ตัวอย่างเช่น การที่ปัญญาประดิษฐ์สามารถเอาชนะ Garry Kasparov แชมป์หมากรุกโลกในปี 1997 เป็นการแสดงให้เห็นถึงความก้าวหน้าของปัญญาประดิษฐ์ ก่อนที่จะมีการเรียนรู้ภาษาและนำมาใช้ในภาคอุตสาหกรรม

ในด้านการประยุกต์ใช้ปัญญาประดิษฐ์ในภาคอุตสาหกรรมและการทหาร ปัญญาประดิษฐ์ถูกนำมาใช้ในหลายด้าน ตั้งแต่หุ่นยนต์ประกอบรถยนต์ หุ่นยนต์ทำความสะอาดบ้าน ไปจนถึงหุ่นยนต์ที่สามารถมีอารมณ์นึกคิดใกล้เคียงกับมนุษย์ การพัฒนาปัญญาประดิษฐ์ควบคู่ไปกับเทคโนโลยีเซมิคอนดักเตอร์ ทำให้ความสามารถในการประมวลผลข้อมูลได้รับการพัฒนาเช่นกัน นอกจากนี้ การเรียนรู้การประมวลผลภาษาธรรมชาติ (Natural Language Processing: NLP) ช่วยให้ปัญญาประดิษฐ์สามารถเข้าใจและตอบสนองภาษาของมนุษย์ได้อย่างมีประสิทธิภาพ จนเกิดเป็นโมเดลภาษาขนาดใหญ่ (Large Language Model: LLM) ซึ่งหมายถึงปัญญาประดิษฐ์ที่ถูกพัฒนาให้เข้าใจและสร้างภาษามนุษย์ได้ในระดับสูง โดยใช้เทคโนโลยีการเรียนรู้เชิงลึก (Deep Learning) โมเดลเหล่านี้ถูกฝึกฝนด้วยข้อมูลข้อความขนาดมหาศาลจากแหล่งข้อมูลต่าง ๆ เช่น หนังสือ บทความ เว็บไซต์ และอื่น ๆ ส่งผลให้การสื่อสารระหว่างมนุษย์และเครื่องจักรเป็นไปอย่างราบรื่น และความสามารถในการเรียนรู้เชิงลึกช่วยให้ปัญญาประดิษฐ์สามารถวิเคราะห์ข้อมูลมหาศาลและสื่อสารกับมนุษย์ได้อย่างมีประสิทธิภาพ

ในด้านผลกระทบจากการใช้ปัญญาประดิษฐ์ทางการทหาร ได้แบ่งออกเป็นสามส่วนหลัก ได้แก่ ผลกระทบต่อความมั่นคงของชาติ ผลกระทบต่อรูปแบบของสงคราม และผลกระทบต่อความมั่นคงทางไซเบอร์ ในด้านความมั่นคงของชาติ ปัญญาประดิษฐ์สามารถใช้ในการพัฒนาระบบป้องกันประเทศ เช่น ระบบตรวจจับขีปนาวุธ อย่างไรก็ตาม มันยังสามารถถูกใช้ในการโจมตีโครงสร้างพื้นฐานดิจิทัลของประเทศ ส่งผลให้เกิดความเสียหายอย่างมาก ในส่วนของรูปแบบสงคราม การรบแบบเดิมที่ใช้กำลังพลได้ถูกแทนที่ด้วยการรบผ่านระบบไซเบอร์ เช่น การเผยแพร่ข่าวปลอม การเจาะระบบฐานข้อมูล และการโจมตีผ่านโครงสร้างพื้นฐานดิจิทัล ซึ่งส่งผลกระทบโดยตรงต่อความมั่นคงทางไซเบอร์ และอาจบานปลายไปยังด้านอื่น ๆ อีกด้วย

หลังจากทบทวนงานวิจัยหลายฉบับที่เกี่ยวกับผลกระทบต่อทางไซเบอร์นั้น พบว่า ถึงแม้จะมีการวิจัยเกี่ยวกับผลกระทบของปัญญาประดิษฐ์ต่อความมั่นคงทางไซเบอร์อย่างกว้างขวางในระดับสากล แต่ในบริบทของประเทศไทยนั้นกลับมีการศึกษาที่เกี่ยวข้องน้อยมาก เมื่อเทียบกับจำนวนงานวิจัยในต่างประเทศ การศึกษาในประเด็นนี้ยังคงเป็นเรื่องใหม่และมีข้อมูลที่จำกัด ทำให้ยังไม่มีความเข้าใจที่ชัดเจนเกี่ยวกับการประยุกต์ใช้ปัญญาประดิษฐ์ในการทหารและผลกระทบที่เกิดขึ้นจากการใช้งานปัญญาประดิษฐ์ในการทหารในประเด็นของความมั่นคงทางไซเบอร์

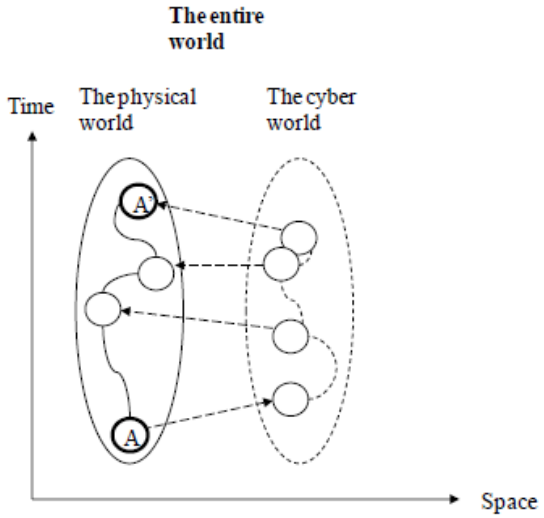
การวิจัยนี้จึงมุ่งเน้นไปที่การเติมเต็มช่องว่างดังกล่าว โดยศึกษาผลกระทบของการใช้ปัญญาประดิษฐ์ในการทหารต่อความมั่นคงทางไซเบอร์ในระดับสากล ผ่านตัวอย่างการใช้งานเพื่อโจมตีและเพื่อป้องกันทางไซเบอร์ ด้วยวิธีนี้งานวิจัยนี้จะช่วยเพิ่มความเข้าใจเกี่ยวกับผลกระทบ

ของปัญญาประดิษฐ์ในการทหาร และเสนอแนวทางในการพัฒนาความมั่นคงทางไซเบอร์ในประเทศไทยให้มีประสิทธิภาพมากยิ่งขึ้น

1.5 กรอบแนวคิดและทฤษฎี

ทฤษฎีความมั่นคงทางไซเบอร์

คำว่า "ไซเบอร์" (cyber) มาจากภาษากรีก “kybereo” ซึ่งแปลว่า "นำ", "ควบคุม", "กำกับ" ในช่วงปลายทศวรรษ 1940 นักคณิตศาสตร์ชาวอเมริกัน Norbert Wiener ได้เริ่มใช้คำว่า "ไซเบอร์เนติกส์" (cybernetics) เพื่ออธิบายระบบควบคุมโดยคอมพิวเตอร์ ใช้การสื่อสารและข้อมูลป้อนกลับเพื่อควบคุมระบบต่าง ๆ ทั้งเครื่องจักรและสิ่งมีชีวิต นักวิทยาศาสตร์นิยมใช้คำว่า "ไซเบอร์" ร่วมกับคำที่เกี่ยวข้องกับคอมพิวเตอร์และหุ่นยนต์ นักเขียนนวนิยายวิทยาศาสตร์ William Gibson ได้สร้างคำว่า "ไซเบอร์สเปซ" (cyberspace) ในนวนิยายเรื่อง Neuromancer โดยไซเบอร์สเปซถูกมองว่าเป็นโครงข่ายข้อมูลคอมพิวเตอร์ระดับโลกที่มีการเข้ารหัสในรูปแบบสามมิติ (Lehto, 2015) คำนิยามของ "ไซเบอร์" ในความหมายกว้าง ไม่เพียงแค่ครอบคลุมในส่วนของคอมพิวเตอร์และเครือข่าย แต่ยังรวมถึงระบบที่ครอบคลุมการดำรงอยู่และกิจกรรมของมนุษย์ที่ได้รับการสนับสนุนจากเทคโนโลยีสารสนเทศและเครือข่ายอีกด้วย



ภาพประกอบ 1 แสดงการเปรียบเทียบปฏิสัมพันธ์ระหว่างโลกกายภาพกับโลกไซเบอร์

ที่มา: Kuusisto, R., & Kuusisto, T. (2013). Strategic Communication for Cyber-security Leadership. Journal of Information Warfare, 12(3), 41-48. https://www.jstor.org/stable/26486840

ในปัจจุบันความมั่นคงปลอดภัยไซเบอร์ ได้นำมาใช้ในบริบทของมาตรการในการป้องกันระบบคอมพิวเตอร์และเครือข่ายจากการเข้าถึงหรือการโจมตีที่ไม่ได้รับอนุญาต และยังเกี่ยวข้องกับการจัดการความเสี่ยง การอุดช่องโหว่ และการปรับปรุงความทนทานของระบบ ที่ใช้เทคนิคในการตรวจจับพฤติกรรมที่ผิดปกติของเครือข่ายและมัลแวร์ ดังนั้น ผลกระทบเมื่อเกิดขึ้นโลกไซเบอร์จะส่งผลกระทบต่อชีวิตประจำวันด้วยเช่นกัน จากปฏิสัมพันธ์ที่เกิดขึ้นของผู้ใช้งานในทุกช่วงเวลา ดังภาพประกอบ 1 ซึ่ง Kuusisto ได้เสนอว่า แนวคิดโลกไซเบอร์ในความหมายกว้างนี้ทำให้สามารถพิจารณาปรากฏการณ์ทางสังคมและเทคโนโลยีใหม่ ๆ เช่น พฤติกรรมทางสังคมของมนุษย์ที่ได้รับการสนับสนุนจากเทคโนโลยีสารสนเทศ โดยมองว่าเทคโนโลยีคือสิ่งสนับสนุน มิใช่ครอบงำกิจกรรมของมนุษย์ (Sipola et al., 2023)

การเข้าใจประเภทต่างๆ ของความมั่นคงทางไซเบอร์เป็นสิ่งสำคัญสำหรับการรับรองความปลอดภัยโดยรวม โดย ได้อธิบายประเภทของความมั่นคงทางไซเบอร์เพื่อความเข้าใจที่ดียิ่งขึ้นในแนวคิดนี้ ดังที่แสดงในรูปที่ 1 ดังต่อไปนี้

1. ความมั่นคงของเครือข่าย (Network Security): ประกอบด้วยมาตรการที่มุ่งป้องกันการแทรกแซง เช่น ไวรัสหรือการโจมตีจากแฮกเกอร์ ความมั่นคงเครือข่ายเป็นชุดของโซลูชั่นที่ช่วยให้องค์กรสามารถรักษาเครือข่ายคอมพิวเตอร์ให้อยู่ห่างจากแฮกเกอร์ ผู้โจมตีที่มีการจัดการ และซอฟต์แวร์ที่เป็นอันตราย

2. ความมั่นคงของแอปพลิเคชัน (Security of Applications): การใช้เครื่องมือฮาร์ดแวร์และซอฟต์แวร์ (เช่น แอนตี้ไวรัส การเข้ารหัส และไฟร์วอลล์) เพื่อปกป้องระบบจากภัยคุกคามภายนอกที่อาจส่งผลต่อการพัฒนาแอปพลิเคชัน

3. ความมั่นคงของข้อมูล (Information Security): การปกป้องข้อมูลทั้งทางกายภาพและดิจิตอลจากการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การใช้งานที่ไม่ถูกต้อง การแก้ไขโดยมิชอบ และการลบ

4.ความมั่นคงเชิงปฏิบัติการ (Operational Security): กระบวนการและการตัดสินใจที่มุ่งควบคุมและปกป้องข้อมูล เช่น การตั้งค่าการอนุญาตให้ผู้ใช้เข้าถึงเครือข่าย หรือการจัดตั้งขั้นตอนที่กำหนดว่าเมื่อใดและที่ใดที่ข้อมูลสามารถถูกเก็บไว้ได้

5. ความมั่นคงบนคลาวด์ (Cloud Security): การปกป้องข้อมูลบนคลาวด์ (พื้นฐานซอฟต์แวร์) และการตรวจสอบเพื่อลดความเสี่ยงจากการโจมตี

6. การฝึกอบรมผู้ใช้ (User Training): มุ่งเน้นไปที่แง่มุมของความมั่นคงทางไซเบอร์ที่อาจไม่คาดคิดและเกี่ยวข้องกับการกระทำของผู้คน ซึ่งหมายถึงการฝึกอบรมผู้ใช้เกี่ยวกับความ

ตระหนักถึงภัยคุกคามที่อาจเกิดขึ้นและการกระทำเพื่อรับรองความปลอดภัยออนไลน์ เช่น การสอนผู้ใช้วิธีลบสิ่งที่แนบมากับอีเมลที่น่าสงสัยและหลีกเลี่ยงการเชื่อมต่ออุปกรณ์ USB ที่ไม่รู้จักและอุปกรณ์อื่นๆ ควรเป็นส่วนหนึ่งของแผนความมั่นคงขององค์กร

ภาพประกอบ 2 ภาพแสดงประเภทของความมั่นคงทางไซเบอร์

ที่ ม า : Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. Multidisciplinary Science Journal, 6, 2024ss0219. https://doi.org/10.31893/multiscience.2024ss0219

กรอบแนวคิด

คำถามสำคัญของการวิจัยครั้งนี้คือ “การพัฒนาเทคโนโลยีปัญญาประดิษฐ์ทางการทหารส่งผลกระทบต่อความมั่นคงทางไซเบอร์อย่างไร” ข้อเสนอของการศึกษาครั้งนี้ คือ การพัฒนาและการนำเทคโนโลยีปัญญาประดิษฐ์ทางการทหารมาใช้ส่งผลกระทบต่อความมั่นคงทางไซเบอร์ในเชิงลบ เนื่องจากเทคโนโลยีปัญญาประดิษฐ์จะมีความสามารถในการสร้างภัยคุกคามต่างๆ ที่มีประสิทธิภาพมากขึ้น จากข้อเสนอข้างต้นทำให้กรอบแนวคิดคือ การจำแนกประเภทและระดับของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากการใช้ปัญญาประดิษฐ์ทางการทหาร

การโจมตีทางไซเบอร์แบบปกติกับการโจมตีโดยใช้ปัญญาประดิษฐ์นั้น มีจุดสำคัญที่แตกต่างกัน คือ การโจมตีทางไซเบอร์แบบทั่วไป มักจะเน้นไปที่การปลอมแปลง การแก้ไข การปฏิเสธ การเปิดเผยข้อมูล การปฏิเสธการให้บริการ และการยกระดับสิทธิ์ในการเข้าถึงข้อมูลนั้น ๆ ผ่านวิธีต่าง ๆ โดยที่ผู้ใช้งานนั้นไม่ได้ให้ความยินยอม ในขณะที่การโจมตีโดยใช้ปัญญาประดิษฐ์จัดกลุ่มเป็นการจำแนกข้อมูลผิดพลาด การสร้างข้อมูลสังเคราะห์ และการวิเคราะห์ข้อมูล การโจมตีต่าง ๆ จะสอดคล้องกับผลกระทบต่อความปลอดภัยทางไซเบอร์(Kravchenko et al., 2024)

	Attack Paradigm	Attack Type	Attack Impact
Cyber Attack	Classical	Spoofing Identity	Authentication
		Tempering with data	Integrity
		Repudiation	Nor-Repudiation
		Information Disclosure	Confidentiality
		Denial of service	Availability
		Elevation of privilege	Authorization
	AI Powered	Data misclassification	False positive results by AI algorithms
		Synthetic data generation	Fake information for user manipulation
		Data analysis	AI assisted classical attack generation

ภาพประกอบ 3 ภาพแสดงการเปรียบเทียบระหว่างการโจมตีทางไซเบอร์แบบดั้งเดิมกับการโจมตีทางไซเบอร์แบบปัญญาประดิษฐ์

ที่มา: ดัดแปลมาจาก Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. Journal of Information Security and Applications, 57, 102722. https://doi.org/10.1016/j.jisa.2020.102722

ดังเช่นภาพประกอบ 3 ที่ได้มีการจำแนกประเภทการโจมตีแบบดั้งเดิมโดยใช้แนวคิด STRIDE แบบจำลองภัยคุกคามหรือ Threat Model รูปแบบหนึ่งที่ไมโครซอฟท์เป็นผู้นำเสนอ (Microsoft, 2022) โดยนำภัยคุกคามด้านซอฟต์แวร์ทั้งหมดทั้งที่เกิดจากซอฟต์แวร์หรือพฤติกรรมมนุษย์ มาวิเคราะห์แล้วจัดแบ่งประเภทตามลักษณะการทำงานของภัยคุกคามนั้นได้เป็น 6 กลุ่ม ได้แก่

1. Spoofing Identity เป็นการเข้าถึงและใช้ข้อมูลการรับรองความถูกต้องของผู้ใช้รายอื่นโดยไม่ได้รับอนุญาต เช่น ชื่อผู้ใช้และรหัสผ่าน

2. Tempering with data เป็นการแก้ไขข้อมูลโดยมีเจตนาร้าย ตัวอย่างเช่น การเปลี่ยนแปลงข้อมูลถาวรโดยไม่ได้รับอนุญาต เช่น ในฐานข้อมูล หรือการเปลี่ยนแปลงข้อมูลระหว่างการส่งผ่านเครือข่ายเปิด เช่น อินเทอร์เน็ต

3. Repudiation เกี่ยวข้องกับผู้ใช้ที่ปฏิเสธการกระทำบางอย่างโดยที่ผู้อื่นไม่สามารถพิสูจน์ได้ เช่น ผู้ใช้ทำการกระทำผิดกฎหมายในระบบที่ไม่สามารถติดตามได้ non-repudiation คือความสามารถในการตอบโต้การปฏิเสธการกระทำนั้น เช่น ผู้ใช้ที่ซื้อสินค้าอาจต้องลงลายมือชื่อเมื่อรับของ ผู้ขายสามารถใช้หลักฐานนั้นแสดงว่าผู้ใช้ได้รับสินค้าจริง

4. Information Disclosure เป็นการเปิดเผยข้อมูลให้กับบุคคลที่ไม่ได้รับอนุญาต เช่น ผู้ใช้สามารถอ่านไฟล์ที่ไม่ได้รับสิทธิ์ หรือผู้บุกรุกสามารถอ่านข้อมูลระหว่างการส่งผ่านระหว่างเครื่องคอมพิวเตอร์

5. Denial of service เป็นการปฏิเสธการให้บริการแก่ผู้ใช้ที่ถูกต้อง เช่น ทำให้เว็บเซิร์ฟเวอร์ชั่วคราวใช้งานไม่ได้ ต้องป้องกันประเภทนี้เพื่อเพิ่มความพร้อมใช้งานและเสถียรภาพของระบบ

6. Elevation of privilege ผู้ใช้ที่ไม่มีสิทธิพิเศษสามารถเข้าถึงสิทธิพิเศษ ซึ่งทำให้สามารถคุกคามหรือทำลายระบบทั้งหมดได้ อันตรายมากถ้าผู้บุกรุกสามารถเอาชนะการป้องกันระบบและเป็นส่วนหนึ่งของระบบที่เชื่อถือได้

การโจมตีทางไซเบอร์ด้วยเทคโนโลยีปัญญาประดิษฐ์ (Yamin et al., 2021) ได้มีการเสนอไว้ 3 ประเภท คือ

1. Data misclassification การจัดการแบ่งแยกข้อมูลผิดประเภท ทำให้เกิดข้อผิดพลาดในระบบการใช้งาน โดยมุ่งเน้นการโจมตีไปที่อัลกอริทึมของปัญญาประดิษฐ์

2. Synthetic data generation ข้อมูลสังเคราะห์ที่เกิดเทคโนโลยีปัญญาประดิษฐ์ ซึ่งนำไปใช้โดยการสังเคราะห์ข้อมูลที่เป็นเท็จไปเพื่อการหลอกลวงต่อผู้ใช้งาน

3. Data analysis การวิเคราะห์ข้อมูลและประมวลผลโดยปัญญาประดิษฐ์เพื่อนำไปใช้ในการโจมตีทางไซเบอร์แบบดั้งเดิม ผ่านการเขียนโปรแกรมไวรัสต่าง ๆ

เมื่อถูกนำไปใช้ในทางการทหารนั้น ปัญญาประดิษฐ์ได้มีการยกระดับให้มีความรุนแรงมากยิ่งขึ้น สอดคล้องกับกรอบแนวคิดต่อมาคือการแบ่งระดับความรุนแรงของภัยคุกคาม โดย Lehto, M. (2015) ได้มีการแบ่งระดับของภัยคุกคามตามแรงจูงใจ (Motivation-based Threat Classification) ทั้งหมดเป็น 5 ระดับด้วยกัน ได้แก่

1. การกระทำผิดในไซเบอร์เพื่อสิทธิและเสรีภาพ (Cyber Activism) การทำลายข้อมูล การเจาะระบบ และกลุ่มแฮกเกอร์

2. อาชญากรรมไซเบอร์ (Cybercrime) การคุกคามทางอิเล็กทรอนิกส์ การเผยแพร่เนื้อหาผิดกฎหมาย และการโจมตีระบบเครือข่าย

3. การสอดแนมทางไซเบอร์ (Cyber Espionage) เพื่อขโมยข้อมูลลับเชิงพาณิชย์หรือทางการทหาร

4. การก่อการร้ายทางไซเบอร์ (Cyber Terrorism) การโจมตีระบบสารสนเทศสำคัญเพื่อทำให้เกิดความเสียหายและสร้างความหวาดกลัว เป็นเครื่องมือบีบบังคับทางการเมือง

5. สงครามไซเบอร์ (Cyber Warfare) การดำเนินการทางไซเบอร์ในระหว่างสงครามระหว่างประเทศ ทั้งระดับยุทธศาสตร์ ปฏิบัติการรบ และสงครามระดับต่าง ๆ(Lehto, 2015)

1.6 วัตถุประสงค์วิจัย

1. ศึกษาพัฒนาเทคโนโลยีปัญญาประดิษฐ์ทางการทหารที่ใช้ในความมั่นคงทางไซเบอร์
2. ศึกษาการโจมตีทางไซเบอร์โดยเทคโนโลยีปัญญาประดิษฐ์ทางการทหาร
3. ศึกษาผลกระทบความมั่นคงทางไซเบอร์ที่เกิดจากการใช้เทคโนโลยีปัญญาประดิษฐ์

1.7 ขอบเขตการวิจัย

งานวิจัยชิ้นนี้ศึกษาการนำปัญญาประดิษฐ์มาใช้ในทางการทหาร นับตั้งแต่ปี 2018 ถึง 2024 ซึ่งเป็นช่วงเวลาที่การพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างเป็นรูปธรรมมากขึ้นและศึกษาการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการโจมตีในระดับสากลที่ตรวจจับ โดยนำมาวิเคราะห์ว่า การนำปัญญาประดิษฐ์มาใช้ในทางการทหารนั้นส่งผลกระทบอย่างไรต่อความมั่นคงทางไซเบอร์ โดยอาศัยกรอบแนวคิดการจำแนกประเภทและระดับของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากการใช้ปัญญาประดิษฐ์ทางการทหาร และคาดการณ์ผลกระทบที่มีต่อประเทศไทย

1.8 วิธีวิจัย

การวิจัยนี้จะใช้การวิจัยเอกสาร (documentary research) เป็นหลักจากเอกสารในระดับต่าง ๆ ประกอบไปด้วย

1. ระดับปฐมภูมิ (Primary Sources) เอกสารจากเว็บไซต์ของหน่วยงานรัฐทั้งในประเทศและต่างประเทศ ที่เกี่ยวข้องกับการพัฒนาการเทคโนโลยีปัญญาประดิษฐ์ เช่น กระทรวงการต่างประเทศ กระทรวงกลาโหม หน่วยงานความมั่นคงไซเบอร์ กระทรวงความมั่นคงแห่ง

มาตุภูมิสหรัฐ และรายงานจากเว็บไซต์องค์กรอิสระ และองค์กรระหว่างประเทศที่เกี่ยวข้องกับการใช้ปัญญาประดิษฐ์ในทางด้านทหาร ทั้งในรูปแบบสิ่งพิมพ์และสื่ออิเล็กทรอนิกส์

2. ระดับทุติยภูมิ (Secondary Sources) ได้แก่ หนังสือ วิทยานิพนธ์ งานวิจัย วารสาร บทความวิชาการ ข่าวสารต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาการเทคโนโลยีปัญญาประดิษฐ์ การโจมตีทางไซเบอร์จากเทคโนโลยีปัญญาประดิษฐ์ ทั้งภาษาไทย ภาษาอังกฤษ และภาษาจีน

ข้อมูลที่ได้จากการวิจัยเอกสารทั้งสองระดับจะถูกนำมาวิเคราะห์โดยใช้วิธีการวิเคราะห์เนื้อหา (content analysis) เพื่อหาความสัมพันธ์และแนวโน้มในการพัฒนาการเทคโนโลยีปัญญาประดิษฐ์และการใช้ในด้านการทหารและความมั่นคงเพื่อศึกษาหาผลกระทบ โดยข้อมูลปฐมภูมิจะช่วยให้เข้าใจถึงการดำเนินงานของหน่วยงานต่าง ๆ ส่วนข้อมูลทุติยภูมิจะช่วยเสริมสร้างความเข้าใจในภาพรวมและให้บริบททางวิชาการเพิ่มเติม เพื่อนำไปวิเคราะห์หาผลกระทบที่มีต่อความมั่นคงทางไซเบอร์

1.9 นิยามปฏิบัติการ

ปัญญาประดิษฐ์ทางการทหาร

หมายถึง การประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในกิจกรรมและระบบต่าง ๆ ที่เกี่ยวข้องกับการทหาร และความมั่นคงแห่งชาติ โดยได้รับการสนับสนุนจากรัฐบาล ตั้งแต่การรวบรวมและวิเคราะห์ข้อมูลข่าวกรอง การวางแผนยุทธศาสตร์ การพัฒนาและควบคุมอาวุธ ระบบป้องกันภัย การฝึกทหาร และการตัดสินใจในสถานการณ์วิกฤต

บทที่ 2
การพัฒนาเทคโนโลยีทางทหารต่อความมั่นคงทางไซเบอร์

บทนี้จะเริ่มต้นด้วยการให้ภาพรวมเกี่ยวกับประวัติและพัฒนาการของปัญญาประดิษฐ์ ตามด้วยการสำรวจการประยุกต์ใช้ปัญญาประดิษฐ์ในภาคการทหารโดยเฉพาะ และสุดท้ายจะเน้นไปที่การประยุกต์ใช้ปัญญาประดิษฐ์ในการเสริมสร้างความมั่นคงทางไซเบอร์ บทนี้จะช่วยให้เข้าใจถึงการเปลี่ยนแปลงและการพัฒนาของปัญญาประดิษฐ์ในทางการทหารและความมั่นคงทางไซเบอร์ที่เกิดจากการประยุกต์ใช้ปัญญาประดิษฐ์ในยุคปัจจุบัน

2.1 พัฒนาการของการใช้ปัญญาประดิษฐ์

แนวคิดเรื่อง “ปัญญาประดิษฐ์” ได้เกิดขึ้นในปี 1950 จากนักคณิตศาสตร์ที่มีชื่อว่า อลันทัวริ่ง (Alan Turing) ที่ได้มีการตีพิมพ์บทความเรื่อง Computing Machinery and Intelligence ภายใต้การตั้งคำถามว่า เครื่องจักรนั้นสามารถมีความคิดได้หรือไม่ การทดสอบครั้งนี้ เขาได้มีการตั้งชื่อว่า “การทดสอบทัวริ่ง (Turing Test)” ด้วยการนำเครื่องจักรมาพิมพ์ตอบโต้สนทนากับมนุษย์และให้แยกว่า คู่สนทนานั้นเป็นเครื่องจักรหรือมนุษย์ หากไม่สามารถแยกแยะได้หมายความว่าเครื่องจักรได้ผ่านการทดสอบ (Turing, 1950) แม้ว่าการทดสอบนี้จะผ่านการวิจารณ์อย่างหนักตั้งแต่เวลาที่เผยแพร่ แต่ก็ยังคงเป็นส่วนสำคัญของประวัติศาสตร์ของปัญญาประดิษฐ์และเป็นแนวคิดที่ต่อเนื่องในด้านปรัชญาเนื่องจากมันใช้ไอเดียเกี่ยวกับภาษาวิทยา

ต่อมา ในปี 1956 นักวิทยาศาสตร์คอมพิวเตอร์ John McCarthy ได้ให้กำเนิดคำว่าปัญญาประดิษฐ์ (AI) และได้รับการบัญญัติศัพท์ขึ้นในงานตีพิมพ์ว่า “ปัญญาประดิษฐ์ คือวิทยาศาสตร์และเทคโนโลยี ที่ทำให้เครื่องจักรและคอมพิวเตอร์มีความฉลาด” ในการประชุม Dartmouth Conference ซึ่งได้รวบรวมกลุ่มนักวิจัยเพื่อสำรวจความเป็นไปได้ในการสร้างเครื่องจักรอัจฉริยะ เหตุการณ์นี้มักถูกมองว่าเป็นจุดกำเนิดของปัญญาประดิษฐ์เป็นสาขาการศึกษาที่แตกต่างกัน ปีต่อมา อัลเลน นิวเอลล์ (Allen Newell)และเฮอร์เบิร์ต ไซมอน (Herbert Simon) สร้างโปรแกรมปัญญาประดิษฐ์แรกที่ทำงานได้ ชื่อ โปรแกรมนักทฤษฎีตรรกศาสตร์ (Logic Theorist) เป็นโปรแกรมหาเหตุผลและพิสูจน์ทฤษฎีตรรกศาสตร์ ตามมาด้วย วอร์เรน แมคคัลลอช์ (Warren McCullough)และวอลเธอร์ พิทซ์ (Walter Pitts) ที่ร่วมกันสร้างแบบจำลองหน่วยประสาทเดี่ยว (neurons) และได้กลายมาเป็นพื้นฐานของการทำงานของปัญญาประดิษฐ์ (AI) ในการจำลองกระบวนการคิดของสมองมนุษย์ในปัจจุบัน มีการใช้ความรู้เกี่ยวกับหน้าที่ของสมองใน

เชิงกายภาพ ตรรกศาสตร์ และทฤษฎีการคำนวณ โดยการฝึกฝนให้ระบบสามารถเลียนแบบทักษะการแก้ปัญหาของมนุษย์ได้ (Anyoha, 2017)

ต่อมาในปี 1997 สตูอาร์ต รัสเซล และปีเตอร์ นอร์วิก เขียนหนังสือ " Artificial Intelligence: A Modern Approach" โดยมีการรวบรวมความก้าวหน้าของปัญญาประดิษฐ์ทั้งในเชิงตรรกะ ความน่าจะเป็นทางคณิตศาสตร์ ต่อเนื่องถึงการรับรู้ การคิด การเรียนรู้และการกระทำต่าง ๆ ตั้งแต่ไมโครอิเล็กทรอนิกส์ (microelectronic) ไปจนถึง หุ่นยนต์สำรวจดาวเคราะห์ (Russell & Norvig, 2016) และกลายเป็นหนังสือเรียนหลักในการศึกษาเกี่ยวกับปัญญาประดิษฐ์ในปัจจุบัน

ปัญญาประดิษฐ์ในช่วงต้นนั้นได้มีการนำมาประยุกต์ผ่านการทำงานกับมนุษย์ โดยการให้ให้มีเรียนรู้ผ่านการเรียนรู้ของเครื่องจักร (Machine Learning: M) เป็นสาขาหนึ่งของปัญญาประดิษฐ์ (AI) และวิทยาการคอมพิวเตอร์ที่มุ่งเน้นการใช้ข้อมูลและอัลกอริทึมเพื่อให้ปัญญาประดิษฐ์สามารถเลียนแบบวิธีการเรียนรู้ของมนุษย์ได้ โดยจะค่อย ๆ ปรับปรุงความแม่นยำให้ดีขึ้นเรื่อย ๆ (IBM, 2024b) ซึ่งส่วนมากเป็นการนำมาใช้กับอุตสาหกรรมการคำนวณเท่านั้น

ตัวอย่างเช่น การนำมาใช้ในการพัฒนาเกมหมากรุก ในปี 1997 สมองกลที่ชื่อ ดีพบลู (Deep Blue) ได้ท้าทายความชาญฉลาดของมนุษย์ โดย แกรี่ กาสปาโรฟ แชมป์หมากรุกโลกชาวรัสเซีย ต้องเสียชัยชนะให้กับดีพบลู ซึ่งใช้หลักการค้นหาลึกและฟังก์ชันที่ซับซ้อน บนเครื่องคอมพิวเตอร์สมรรถนะสูง พัฒนาโดยมหาวิทยาลัยคาร์เนกีเมลลอน (Carnegie Mellon Universit) และบริษัทไอบีเอ็ม สมองกลรุ่นใหม่นี้ทำให้หุ่นยนต์ทำงานได้รวดเร็วมากขึ้น โดยสามารถวิเคราะห์ข้อมูลและตัดสินใจได้เอง โดยไม่ต้องอาศัยการตัดสินใจจากมนุษย์

หุ่นยนต์ได้ถูกพัฒนาความสามารถทางกายภาพและความคิดอย่างต่อเนื่อง บทบาทของหุ่นยนต์ได้เปลี่ยนจากเครื่องจักรกลที่ทำงานอย่างแม่นยำในโรงงานอุตสาหกรรม เป็นหุ่นยนต์ที่มีอารมณ์และความรู้สึก ในปี ค.ศ.1999 หุ่นยนต์สุนัข ไอโบ้ (Aibo) ซึ่งพัฒนาโดยบริษัทโซนี่ (Sony) ประเทศญี่ปุ่น ถูกสร้างขึ้นให้มีลักษณะเหมือนสัตว์เลี้ยง มีความรู้สึกตอบสนอง เพื่อให้สามารถเป็นเพื่อนกับมนุษย์ได้ อีกตัวอย่างหนึ่งคือ ROOMBA หุ่นยนต์ดูดฝุ่นที่สามารถเคลื่อนที่และทำความสะอาดบ้านได้เอง ซึ่งเป็นการผลิตเชิงอุตสาหกรรมจำนวนมากครั้งแรก

ต่อมาได้มีการพัฒนาการสื่อสารระหว่างมนุษย์และปัญญาประดิษฐ์ให้มีความเข้าใจง่ายมากยิ่งขึ้นผ่านการประมวลผลภาษาธรรมชาติ (NLP) ซึ่งเป็นศาสตร์สำคัญทางด้าน Machine Learning ที่ประกอบด้วยองค์ความรู้จากหลากหลายแขนง เช่น ภาษาศาสตร์ (Linguistics), วิทยาการคอมพิวเตอร์ (Computer Science), ปัญญาประดิษฐ์ (Artificial Intelligence: AI), และ

สถิติ (Statistics) จากการพัฒนาเหล่านี้เกิดเป็น LLM หรือ "Large Language Model" (โมเดลภาษาขนาดใหญ่) ซึ่งหมายถึงปัญญาประดิษฐ์ที่ถูกพัฒนาให้เข้าใจและสร้างภาษามนุษย์ได้ในระดับสูง โดยมีจุดมุ่งหมายเพื่อให้คอมพิวเตอร์สามารถทำความ “เข้าใจ” ข้อมูลที่มีลักษณะเป็นข้อความหรือคำพูดได้เช่นเดียวกับมนุษย์ ซึ่งไม่ใช่เพียงแค่เข้าใจความหมายโดยตรงของข้อความแต่ยังรวมถึงการรับรู้ถึงความหมายโดยนัย ความรู้สึกของผู้เขียน ความแตกต่างทางบริบทของภาษา และสามารถทำการวิเคราะห์ในรูปแบบต่าง ๆ ได้อีกด้วย ตัวอย่างเช่น การใช้ LLM ในการตอบคำถามของลูกค้าในแชทบอท ช่วยให้การตอบสนองมีความเป็นธรรมชาติและแม่นยำมากขึ้น หรือการใช้ NLP ในการวิเคราะห์ความคิดเห็นจากสื่อสังคมออนไลน์เพื่อทำความเข้าใจความรู้สึกและทัศนคติของผู้คนเกี่ยวกับผลิตภัณฑ์หรือบริการต่าง ๆ(Artit Sagoolmuang et al., 2023)

ในปี 2011 Apple เปิดตัว Siri พร้อมกับ iPhone 4s ซึ่งเป็นระบบผู้ช่วยเสมือนที่สามารถโต้ตอบกับผู้ใช้ผ่านการสนทนา แม้ว่าจะมีคำวิจารณ์ในช่วงแรกเกี่ยวกับการทำงานที่ไม่สมบูรณ์ในบางประเทศ แต่ Apple ก็ได้มุ่งมั่นพัฒนาและปรับปรุง Siri อย่างต่อเนื่องเพื่อให้สามารถตอบสนองความต้องการของผู้ใช้ได้ดียิ่งขึ้น

ในปี 2014 มีการพัฒนา chatbot ชื่อ Eugene Goostman ซึ่งสามารถทำให้ผู้พิพากษาหลายคนเชื่อว่าเป็นมนุษย์ โดยผ่านการทดสอบที่ใช้ในการประเมินว่าปัญญาประดิษฐ์สามารถแสดงพฤติกรรมหรือความคิดที่คล้ายมนุษย์ได้หรือไม่

ในปี 2016 Microsoft เปิดตัว AI ชื่อว่า Tay ซึ่งออกแบบมาเพื่อสนทนากับผู้คนบนแพลตฟอร์มออนไลน์ Tay สามารถพูดคุยด้วยภาษาสแลงและมุกตลกได้อย่างเป็นธรรมชาติ โดยเรียนรู้จากการโต้ตอบกับผู้ใช้ อย่างไรก็ตาม หลังจากเปิดตัวไม่นาน Tay ก็ถูกปิดการใช้งานเนื่องจากการตอบสนองที่ไม่เหมาะสม (ไทยพีบีเอส, 2561)

ในปี 2017 AlphaGo ของ Google ได้สร้างประวัติศาสตร์ใหม่ในโลกของปัญญาประดิษฐ์ โดยสามารถเอาชนะนักเล่นโกะมืออันดับหนึ่งของโลกจากจีนในเกมการแข่งขันที่สำคัญ(ธนาคารกรุงเทพ, 2566)

เหตุการณ์เหล่านี้แสดงถึงความก้าวหน้าอย่างต่อเนื่องในด้านปัญญาประดิษฐ์และความสามารถในการเรียนรู้และตอบสนองต่อสภาพแวดล้อมของเทคโนโลยี AI

ปัจจุบัน พลังการคำนวณของคอมพิวเตอร์ได้มีการพัฒนาอย่างต่อเนื่อง ทำให้สามารถเรียนรู้และประมวลผลข้อมูลจำนวนมหาศาลจากผู้ใช้ได้อย่างมีประสิทธิภาพ เทคโนโลยีการเรียนรู้เชิงลึก (Deep Learning) ได้รับความนิยมอย่างมากและถูกนำมาใช้งานแทนที่ Machine Learning แบบดั้งเดิม ซึ่งพึ่งพาความรู้ทางสถิติ การเรียนรู้เชิงลึกถูกนำมาใช้งานในหลากหลาย

ด้าน รวมถึงการประมวลผลภาษาธรรมชาติ (NLP) เช่น การสร้างแบบจำลองทางภาษา (Language Model) และการวิเคราะห์โครงสร้างข้อความ (Parsing)

ความสำคัญของ NLP ได้รับความสนใจอย่างต่อเนื่อง เนื่องจากความต้องการในการประมวลผลข้อมูลข้อความที่เพิ่มขึ้นในหลายภาคส่วน เช่น การศึกษา ธุรกิจ และเทคโนโลยีการสื่อสาร ซึ่งแต่ละปีมีข้อมูลในลักษณะนี้เข้าสู่ระบบดิจิทัลเป็นจำนวนมหาศาล ความสามารถในการจัดการและวิเคราะห์ข้อความจึงมีบทบาทสำคัญในการพัฒนาและปรับปรุงประสิทธิภาพของระบบต่างๆ (Artit Sagoolmuang et al., 2023) ตัวอย่างเช่น

ChatGPT เปิดตัวครั้งแรกในเดือนพฤศจิกายน ปี 2022 ชื่อ ChatGPT ย่อมาจากคำว่า "Chat" และ "Generative Pre-training Transformer" ซึ่งเป็นโมเดลภาษาที่พัฒนาโดย OpenAI การใช้งานในรูปแบบของแชตบอทอัจฉริยะทำให้มีศักยภาพที่ทรงพลัง เทคโนโลยีนี้ถูกพัฒนาให้สามารถจดจำข้อมูลจากอินเทอร์เน็ต และนำมาตอบคำถาม ให้ข้อมูล และตอบกลับอย่างเป็นธรรมชาติในระยะเวลาอันรวดเร็ว คล้ายกับการสนทนาของมนุษย์

นอกจากการตอบคำถามทั่วไปแล้ว ChatGPT ยังสามารถทำงานได้หลากหลายรูปแบบ เช่น ให้ข้อมูล, คำนวณเลข, แนะนำไอเดียในการสร้างคอนเทนต์, เขียนโปรแกรม, วางแผนทริปท่องเที่ยว, แต่งเพลง, คิดแคปชั่น, คำโฆษณา, และเขียนบทความในรูปแบบต่างๆ อีกด้วย (Thairath, 2024)

Claude AI เป็นบอทแชท AI อัจฉริยะจากบริษัท Anthropic ซึ่งได้รับการพัฒนาด้วยเทคโนโลยีการประมวลผลภาษาธรรมชาติ (NLP) ขั้นสูง ทำให้ผู้ใช้สามารถสนทนากับ Claude ได้อย่างเป็นธรรมชาติและมีประสิทธิภาพ Claude ถูกออกแบบมาให้สามารถใช้งานได้หลากหลายวัตถุประสงค์ เช่น การตอบคำถาม การให้คำแนะนำ และการช่วยงานต่าง ๆ โดยมีคุณสมบัติใกล้เคียงกับ ChatGPT ของ OpenAI (Piasak, 2023)

2.2 การประยุกต์ใช้ปัญญาประดิษฐ์ในทางการทหาร

อาวุธที่ใช้ปัญญาประดิษฐ์ (AI) มีประวัติยาวนานตั้งแต่ทศวรรษ 1950 เมื่อมีการพัฒนาตอร์ปิโดนำวิถีด้วยคลื่นเสียง ต่อมาหน่วยงานวิจัยทางการทหารอย่าง DARPA ได้ผลักดันการวิจัยและพัฒนาอาวุธปัญญาประดิษฐ์ อย่างต่อเนื่อง มีการทดลองควบคุมการวางแผนทางการทหารด้วยปัญญาประดิษฐ์ในโครงการ "Survival Adaptive Planning Experiment" ในปี 1991 (Yamin et al., 2021) และมีการพัฒนาต่อมาเรื่อย ๆ จนถึงปัจจุบันตามยุคสมัย ตั้งแต่การสร้างองค์ความรู้ใหม่ ยุคแห่งการใช้การเรียนรู้ของเครื่อง (Machine Learning) และยุค AI Next ในปัจจุบัน โดย

ล่าสุด OpenAI ได้มีการเริ่มเปิดให้กระทรวงกลาโหมสหรัฐเข้ามามีส่วนร่วมในการพัฒนาเครื่องมือปัญญาประดิษฐ์ รวมถึงเครื่องมือความมั่นคงปลอดภัยทางไซเบอร์แบบเปิดแหล่งที่มา การเปลี่ยนแปลงนโยบายครั้งนี้อาจส่งผลกระทบต่อการนำเทคโนโลยีปัญญาประดิษฐ์ไปใช้ในภาคส่วนกลาโหมและความมั่นคง ซึ่งเป็นประเด็นที่มีข้อถกเถียงทางจริยธรรมอยู่มาก อย่างไรก็ตาม OpenAI ยังคงระบุในนโยบายว่าผู้ใช้ไม่ควร "ใช้บริการของเราในทางที่เป็นอันตรายต่อตนเองหรือผู้อื่น" รวมถึง "การพัฒนาหรือใช้อาวุธ" (Field, 2024) ถึงแม้ว่าจะขัดแย้งกับการกระทำของบริษัทก็ตาม

ตารางที่ 1 โครงการระบบข่าวกรองอัจฉริยะของอเมริกา

โครงการ	ปี	สถาบันวิจัย	เนื้อหาหลัก	เทคโนโลยีหลัก
CREATE	2016	IARPA	พัฒนาเครื่องมือที่ช่วยนักวิเคราะห์ข่าวกรองในการทำความเข้าใจและประเมินข้อมูลได้ดีขึ้น	การเรียนรู้ของเครื่อง, การวิเคราะห์ข้อมูล
MEADE	2016	U.S. Air Force	สร้างระบบตอบคำถามข่าวกรอง เพื่อช่วยนักวิเคราะห์ประมวลผลข้อมูลซับซ้อน	การประมวลผลภาษาธรรมชาติ
Maven	2017	U.S. Department of Defense	ช่วยนักวิเคราะห์ประมวลผลข้อมูลจากโดรนในสนามรบ	การเรียนรู้เชิงลึก, การจดจำภาพ
MARS	2018	DIA	สร้างระบบการจัดการข้อมูลบนคลาวด์สำหรับการวิเคราะห์ข่าวกรองทหาร	การประมวลผลข้อมูลขนาดใหญ่, การใช้คลาวด์
KAIROS	2019	DARPA	ใช้ปัญญาประดิษฐ์วิเคราะห์ข้อมูลขนาดใหญ่เพื่อเพิ่มความสามารถในการประเมินสถานการณ์สนามรบในการเข้าใจและมองเห็นสถานการณ์	การประมวลผลภาษาธรรมชาติ, การเรียนรู้เชิงลึก
IP2	2021	DARPA	เพิ่มความแม่นยำในการลาดตระเวนด้วยข้อมูลภาพและวิดีโอ เพื่อช่วยวิเคราะห์ข้อมูลข่าวกรอง	เครือข่ายประสาทเทียม, การมองเห็นด้วยคอมพิวเตอร์

ที่ ม า : Zhao Yaping, H. Y., Li Hong, Meng Jie. (2023). The Application and Development of Artificial Intelligence Technology in the Field of Military Intelligence (in Chinese) [Article]. Command Control & Simulation / Zhihui Kongzhi yu Fangzhen, 45(4), 36-43. https://doi.org/10.3969/j.issn.1673-3819.2023.04.006

ในปัจจุบันมีการประยุกต์ใช้ปัญญาประดิษฐ์หลายรูปแบบ ไม่ว่าจะเป็นแชทบอท วงการอากาศยานไร้คนขับ การจดจำใบหน้า ผู้ช่วยเสมือนจริง ระบบอัตโนมัติทางปัญญา การตรวจจับการฉ้อโกง ยานพาหนะไร้คนขับ และแอปพลิเคชันสำหรับการวิเคราะห์เชิงพยากรณ์ อย่างไรก็ตาม ไม่ว่าปัญญาประดิษฐ์จะถูกนำไปประยุกต์ใช้อย่างไร แอปพลิเคชันเหล่านี้ล้วนมีสิ่งที่เหมือนกันร่วมกัน แม้จะมีการประยุกต์ใช้ที่หลากหลาย แต่ผู้สร้างโครงการต่างๆ ที่เกี่ยวกับปัญญาประดิษฐ์จะสร้างโครงการที่เกี่ยวข้องภายใต้ 7 รูปแบบ และทั้งหมดนี้ได้สร้างการปฏิวัติให้กับปฏิบัติการทางทหารในช่วงไม่กี่ปีที่ผ่านมา คือ

1. Hyper-Personalization คือ การนำเอา Big Data หรือข้อมูลขนาดใหญ่มาวิเคราะห์พฤติกรรมต่าง ๆ ร่วมกับการเรียนรู้ของเครื่อง (Machine Learning) เพื่อสร้างโปรไฟล์รายบุคคล และจากนั้นโปรไฟล์นั้นจะเรียนรู้และปรับตัวเองตามระยะเวลา สำหรับวัตถุประสงค์ต่างๆ ในการประมวลผล เช่น การแสดงเนื้อหาที่เกี่ยวข้อง การแนะนำผลิตภัณฑ์ที่เหมาะสม และการให้คำแนะนำเฉพาะบุคคล ในบริบททางการทหาร รูปแบบนี้สามารถนำมาใช้ได้หลายด้าน เช่น วิเคราะห์ข้อมูลจากโดรนหรืออากาศยานไร้คนขับ แล้วแนะนำกลยุทธ์หรือเป้าหมายที่เหมาะสมกับสถานการณ์ วิเคราะห์ข้อมูลจากยานพาหนะทหาร แล้วเลือกเส้นทางหรือวิธีการที่เหมาะสมที่สุด สร้างระบบฝึกอบรมนักรบที่ปรับตามศักยภาพและจุดบกพร่องของแต่ละคน และวิเคราะห์ข้อมูลจากเซนเซอร์และกล้องเพื่อตรวจจับเป้าหมายได้อย่างแม่นยำ

2. Pattern Recognition หรือการจดจำรูปแบบ เป็นวิธีการทางคอมพิวเตอร์ที่มีประสิทธิภาพสำหรับประเมินข้อมูลภาพ โดยแบ่งออกเป็นการเรียนรู้แบบมีการควบคุม (supervised) และไม่มีการควบคุม (unsupervised) การเรียนรู้แบบไม่มีการควบคุมจะแบ่งกลุ่มข้อมูลตามเกณฑ์ที่กำหนด เพื่อค้นหารูปแบบใหม่ๆ โดยไม่ต้องอิงตัวอย่างการฝึกอบรมก่อนหน้า ในขณะที่การจดจำรูปแบบมีข้อได้เปรียบหลายประการ เช่น สามารถวิเคราะห์ภาพทั้งหมดเพื่อระบุพื้นที่สนใจได้โดยไม่ต้องแยกส่วนภาพก่อน สามารถใช้ร่วมกับอัลกอริทึมการแบ่งภาพย่อย และให้ผลการวิเคราะห์ที่ดีกว่าและมีประสิทธิภาพมากกว่า ซึ่งในบริบทของกองทัพนั้น ได้มีการใช้กระบวนการจดจำรูปแบบในการสั่งการรบอย่างมีประสิทธิภาพ เนื่องจากต้องแปลความหมายสัญลักษณ์บนแผนที่และภาพซ้อนทับได้อย่างรวดเร็ว ที่ผ่านมาความสามารถในการจดจำรูปแบบสำคัญเป็นสัญญาณของผู้เชี่ยวชาญ ทั้งจากผู้เขียนโปรแกรมมืออาชีพ นักหมากรุกระดับมาสเตอร์ ผู้เชี่ยวชาญสถาปัตย์ วิศวกรวงจรไฟฟ้า และแพทย์ผู้อ่านภาพรังสี ดังนั้นจึงเป็นที่น่าสนใจว่าความสามารถในการจดจำรูปแบบสำคัญบนสนามรบอาจเป็นหนึ่งในองค์ประกอบของความเชี่ยวชาญในการสั่งการรบ

3. Conversational Pattern หรือ รูปแบบการสนทนา เป็นการสร้างปฏิสัมพันธ์และการสื่อสารระหว่างมนุษย์กับเครื่องจักรในลักษณะการสนทนา ทั้งแบบเสียง ข้อความ หรือรูปภาพ โดยมีจุดมุ่งหมายคือทำให้เครื่องจักรสามารถโต้ตอบกับมนุษย์ได้เช่นเดียวกับที่มนุษย์พูดคุยกัน หนึ่งในความก้าวหน้าที่สำคัญคือการพัฒนาโปรแกรมสนทนาหรือแชทบอท (chatbot) บนรูปแบบการสนทนา รูปแบบการสนทนากำลังเป็นที่สนใจในวงการทหาร เนื่องจากแชทบอทสามารถให้ข้อมูลและคำแนะนำแก่ทหารระหว่างปฏิบัติภารกิจในพื้นที่ที่ไม่คุ้นเคย หลายประเทศกำลังพัฒนาระบบสนทนาสำหรับสถานการณ์ทางทหารบนพื้นฐานของรูปแบบการสนทนา การนำแชทบอททางทหารมาใช้ จะช่วยให้ทหารได้รับคำตอบทันท่วงทีและเกิดประสิทธิภาพมากขึ้นสำหรับงานประจำ

4. Predictive Analytics หรือ การวิเคราะห์เชิงพยากรณ์ กำลังได้รับความสนใจเป็นอย่างมากในภาคธุรกิจเนื่องจากประโยชน์ในการวิเคราะห์พฤติกรรมผู้บริโภคและการตลาดเจาะจง (Niche Marketing) ในบริบทของปัญญาประดิษฐ์ การวิเคราะห์เชิงคาดการณ์จะใช้ประโยชน์จากอัลกอริทึมและแบบจำลองข้อมูลเพื่อคาดการณ์ผลลัพธ์ตามรูปแบบข้อมูลมันมีบทบาทในการปรับปรุงกระบวนการตัดสินใจระบุความเสี่ยงและการใช้โอกาส โดยอินเทอร์เน็ตของสรรพสิ่ง (IoT) เป็นหนึ่งในเทคโนโลยีการวิเคราะห์เชิงพยากรณ์ที่มีแนวโน้มจะนำมาประยุกต์ใช้ในภาคทหารมากขึ้น ยกตัวอย่างการใช้ IoT ทางทหารหลายด้าน เช่น เก็บข้อมูลสนามรบ ตรวจจับข้าศึก การบำรุงรักษา ติดตามสุขภาพของทหาร การจัดการอุปกรณ์และยานพาหนะ เป็นต้น จากหน้าที่หลักของการวิเคราะห์เชิงพยากรณ์คือการคาดการณ์ในอนาคตจากข้อมูลในอดีต ซึ่งอาจใช้หรือไม่ใช้เทคนิคการเรียนรู้ของเครื่อง ยกตัวอย่างการใช้การวิเคราะห์เชิงพยากรณ์ทางทหาร เช่น คาดการณ์ประสิทธิภาพของทหารในสนามรบจริงจากการฝึกสมมุติ การบำรุงรักษายานพาหนะทางทหารล่วงหน้า การคาดการณ์ความต้องการ การฝึกและสวัสดิการของทหาร และหลายประเทศได้มีการลงทุนงบประมาณจำนวนมากในการนำการวิเคราะห์เชิงพยากรณ์มาปรับปรุงขีดความสามารถทางทหาร

5. Goal-Driven Systems มีจุดมุ่งหมายในการค้นหาคำตอบที่ดีที่สุดสำหรับปัญหาต่างๆ เช่น การนำทางผ่านเขาวงกต การจัดการห่วงโซ่อุปทาน การลดเวลาว่างและเส้นทางการเดินทาง เป็นแนวคิดของปัญญาประดิษฐ์ที่ให้อำนาจความเป็นอิสระแก่ตัวแทนอัตโนมัติในการค้นหาปัญหาภายใต้เป้าหมายและวัตถุประสงค์ปัจจุบันของตน ในวงการทหาร มีการใช้ระบบที่มุ่งหวังเป้าหมายเช่นนี้เป็นหลัก ระบบนี้จะทำให้ง่ายขึ้นสำหรับกองทัพในการปฏิบัติการของตน เพื่อให้คำชี้แจงที่ชัดเจนในกระบวนการวางแผนเพื่อให้การดำเนินงานเป็นไปตามเป้าหมายที่กำหนดไว้ วิธี KAOS ที่เรียกว่า "knowledge acquisition in automated specification" หรือ "keep all

objectives satisfied" เป็นหนึ่งในตัวอย่างที่โดดเด่นของรูปแบบระบบที่มุ่งหวังในปัจจุบันของปัญญาประดิษฐ์ในโลกสมัยใหม่ มันช่วยในการอธิบายกระบวนการที่ต้องการจากเป้าหมายระดับสูงที่ระบบรวมต้องบรรลุไปจนถึงการกระทำ วัตถุประสงค์ และ ข้อจำกัดของส่วนซอฟต์แวร์ มันเป็นวิธีสำหรับการวิศวกรรมความต้องการที่เน้นไปที่การจับตามเป้าหมายของซอฟต์แวร์ ระบบรวมเป็นโปรแกรมที่ตั้งใจและสภาพแวดล้อมของมันในบริบทนี้ ซึ่งช่วยในการเข้าใจสภาพแวดล้อมบนสนามรบหรือเข้าใจพื้นที่ของผู้โจมตี วิธีการนี้ช่วยในการจับตามการเข้ามาของศัตรูได้ดีกว่าโปรแกรมปกติในการทหาร และ ยังสามารถแบ่งปันข้อมูลระหว่างทีมได้ นอกจากนี้ ยังมีการใช้เทคโนโลยีที่เป็นกระบวนการที่มุ่งหวังเป้าหมายในการพัฒนาและการใช้ระบบในสายที่ต่างกันเช่น Distributed Artificial Intelligence (DAI) ซึ่งได้รับการนำมาใช้ในการเก็บข้อมูล สำรวจ การวิเคราะห์และการแสดงผลข้อมูลเชิงพื้นที่เพื่อเพิ่มประสิทธิภาพในการตัดสินใจจากมุมมองของเป้าหมายบนสนามรบ

6. Autonomous Systems Pattern เป็นรูปแบบของปัญญาประดิษฐ์ที่ซับซ้อนที่สุด โดยมีการอัตโนมัติกระบวนการต่างๆ เพื่อให้เกิดระบบที่สามารถทำงานได้อย่างอิสระจากการควบคุมของมนุษย์ มีการนำไปใช้งานในระบบยานพาหนะไร้คนขับ (unmanned autonomous systems) อย่างแพร่หลาย ทั้งยานพาหนะบนบก อากาศ หรือใต้น้ำ โดยใช้อัลกอริทึมปัญญาประดิษฐ์ในการวางแผนเส้นทาง ระบุสัญญาณ และระบบวิสัยทัศน์ นอกจากยานไร้คนขับแล้ว ยังมีการนำมาใช้ในหุ่นยนต์ร่วมงาน (cobots) ที่สามารถทำงานร่วมกับมนุษย์ได้อย่างใกล้ชิด เป็นรูปแบบที่ท้าทายที่สุดในการพัฒนา เนื่องจากต้องการความน่าเชื่อถือและประสิทธิภาพสูงในการทำงานอย่างอัตโนมัติ มีหลักการทำงานหลักคือ วงจรควบคุมที่ประกอบด้วย การติดตาม วิเคราะห์ วางแผน และปฏิบัติการ (MAPE) โดยสรุปแล้ว Autonomous Systems Pattern เป็นรูปแบบที่มีบทบาทสำคัญมากในภาคทหารสมัยใหม่ในการพัฒนาระบบต่างๆ ให้สามารถทำงานได้อย่างอัตโนมัติและมีประสิทธิภาพสูง แม้จะมีความท้าทายในการพัฒนา

7. Patterns and Anomalies เป็นหนึ่งในแนวคิดหลักของปัญญาประดิษฐ์ที่ใช้ในหลายอุตสาหกรรม รวมถึงทหารด้วย การใช้เทคโนโลยีปัญญาประดิษฐ์เพื่อตรวจจับความผิดปกติของเครื่องบินทหารและการเรียนรู้ของเครื่องมักเป็นที่นิยม เครื่องมักมีความสามารถในการวิเคราะห์ข้อมูลจำนวนมากเพื่อตรวจจับรูปแบบ ความผิดปกติ หรือข้อมูลที่ผิดปกติ ซึ่งมีการประยุกต์ใช้ในหลายด้าน เช่น การตรวจจับการฉ้อโกงและความเสี่ยง หรือการช่วยลดข้อผิดพลาดจากมนุษย์ การทำนายข้อความก็เป็นตัวอย่างหนึ่ง การนำแนวคิดนี้มาใช้ช่วยให้กองทัพมีความเข้าใจดีขึ้นเกี่ยวกับสภาพแวดล้อมในสนามรบและสภาพแวดล้อมที่สำคัญ การตรวจจับรูปแบบและความผิดปกติยัง

ช่วยให้มีการวิเคราะห์ข้อมูลเชิงลึกและการพยากรณ์ในหลายด้านอื่นๆ อย่างไรก็ตาม การใช้ข้อมูลที่ไม่เป็นมิตรอาจส่งผลกระทบต่อการตรวจจับรูปแบบและความผิดปกติของปัญญาประดิษฐ์เช่น การแนวทางการฝึกฝนในทหารหากใช้ข้อมูลที่มีลักษณะเฉพาะที่ไม่เท่าเทียมกันได้สร้างความไม่เสมอภาคในการตรวจจับรูปแบบและความผิดปกติ (Szabadföldi, 2021)

เมื่อย้อนกลับมาดูภาพรวมใหญ่แล้ว ปัญญาประดิษฐ์ทางการทหารสามารถแบ่งออกตามการใช้งานได้เป็น 3 ระดับ คือ

1. Enterprise AI หรือปัญญาประดิษฐ์สำหรับงานธุรการและสนับสนุน เป็นการนำปัญญาประดิษฐ์มาใช้ในงานสนับสนุนหรืองานด้านการบริหารจัดการขององค์กรทหาร เช่น ระบบบริหารการเงิน การจัดการทรัพยากรบุคคล การวางแผนและจัดการด้านการปฏิบัติงานสนับสนุน เนื่องจากเป็นงานที่ไม่เกี่ยวข้องกับการปฏิบัติการรบโดยตรง จึงมีความเสี่ยงต่ำหากระบบปัญญาประดิษฐ์มีข้อผิดพลาด

2. Mission Support AI เป็นการใช้ปัญญาประดิษฐ์เพื่อสนับสนุนภารกิจและการปฏิบัติการทางทหาร เช่น ระบบประมวลผลและวิเคราะห์ข้อมูลข่าวกรองขนาดใหญ่ ระบบสนับสนุนการตัดสินใจของผู้บังคับบัญชา ระบบควบคุมและสั่งการยานไร้คนขับ เป็นต้น มีความเสี่ยงปานกลาง เนื่องจากเกี่ยวข้องกับภารกิจและการปฏิบัติการโดยตรง แต่ยังมีการควบคุมดูแลจากมนุษย์

3. Operational AI เป็นการนำปัญญาประดิษฐ์มาใช้ในพื้นที่ปฏิบัติการหรือสนามรบโดยตรง เช่น ระบบอาวุธนำวิถีอัตโนมัติ หุ่นยนต์ทหารอัตโนมัติ ระบบป้องกันขีปนาวุธ เป็นต้น ถือเป็นการใช้งานปัญญาประดิษฐ์ที่มีความเสี่ยงสูงสุด เนื่องจากสภาพแวดล้อมไม่แน่นอนและหากระบบปัญญาประดิษฐ์ทำงานผิดพลาด อาจทำให้เกิดความสูญเสียต่อชีวิตและทรัพย์สินได้ (Ertan, 2022)

2.3 การประยุกต์ใช้ปัญญาประดิษฐ์กับความมั่นคงทางไซเบอร์

แนวคิดเรื่องการนำปัญญาประดิษฐ์มาใช้ในความมั่นคงทางไซเบอร์นั้น เริ่มขึ้นนับตั้งแต่การเกิดขึ้นของระบบผู้เชี่ยวชาญ (Expert Systems) ซึ่งถูกออกแบบมาเพื่อเลียนแบบความสามารถในการตัดสินใจของผู้เชี่ยวชาญมนุษย์ในหลายสาขา รวมถึงด้านความมั่นคงปลอดภัยไซเบอร์ โดยพื้นฐานของระบบผู้เชี่ยวชาญ ได้แก่ ฐานความรู้ (Knowledge Base) ซึ่งเป็นแหล่งรวบรวมข้อมูลเฉพาะด้าน เครื่องมือการคิดเหตุผล (Inference Engine) ที่ประยุกต์ใช้กฎเกณฑ์ตรรกะเพื่อนำข้อมูลมาสรุปหรือตัดสินใจ สำหรับบทบาทในความมั่นคงปลอดภัยไซเบอร์

ระบบผู้เชี่ยวชาญทำหน้าที่เป็นระบบรักษาความปลอดภัยดิจิทัลในยุคแรก ๆ เพื่อติดตามการตรวจสอบการรับส่งข้อมูลเครือข่าย กิจกรรมของระบบ และพฤติกรรมผู้ใช้ เปรียบเทียบกับลายเซ็นของภัยคุกคามที่รู้จัก ตรวจจับความผิดปกติหรือการเบี่ยงเบนที่อาจระบุถึงการถูกโจมตีหรือจุดอ่อน แต่การทำงานในช่วงเริ่มต้นนั้นยังคงมีจุดอ่อนอยู่ คือ ประสิทธิภาพขึ้นอยู่กับความครอบคลุมและความถูกต้องของฐานความรู้ เนื่องจากหากเป็นภัยคุกคามใหม่ที่ไม่มีในฐานข้อมูลระบบผู้เชี่ยวชาญอาจไม่สามารถตรวจจับได้ ดังนั้นจึงเป็นวิธีตอบสนองเชิงรับที่ต้องพึ่งพารูปแบบภัยคุกคามที่รู้จักมาก่อน ชี้ให้เห็นความจำเป็นในการมีแนวทางที่ปรับตัวได้และเชิงรุกมากขึ้นในอนาคต ซึ่งเริ่มเกิดขึ้นในยุคต่อมาหลังจากที่มีการพัฒนาการเรียนรู้ของเครื่อง (Machine Learning) สำเร็จ เนื่องจากระบบรักษาความปลอดภัยแบบดั้งเดิมพึ่งพากฎเกณฑ์และลายเซ็นภัยคุกคามที่ทราบมาก่อน แต่อัลกอริทึมการเรียนรู้ของเครื่องนั้นเติบโตจากข้อมูล และปรับปรุงตัวเองตลอดเวลา โดยวิเคราะห์ชุดข้อมูลขนาดใหญ่ เพื่อสร้างข้อมูลอ้างอิงของพฤติกรรมปกติในระบบหรือเครือข่าย ดังนั้นจึงสามารถตรวจจับความเบี่ยงเบนหรือความผิดปกติที่อาจบ่งบอกถึงภัยคุกคามถึงแม้จะไม่ได้รู้จักกันมาก่อนก็ตาม อีกหนึ่งสิ่งที่เข้ามายกระดับการพัฒนาความมั่นคงทางไซเบอร์นั้น คือการที่ปัญญาประดิษฐ์สามารถเข้าใจถึงภาษาของมนุษย์ การเข้ามาของการประมวลผลภาษาธรรมชาติถือเป็นจุดเปลี่ยนสำคัญ ที่ทำให้ระบบรักษาความปลอดภัยไม่จำกัดอยู่เพียงการวิเคราะห์รหัสหรือข้อมูลการรับส่งข้อมูลเครือข่าย แต่สามารถประมวลผลและเข้าใจข้อความปริมาณมากได้อีกด้วย

ต่อมาการเข้ามาของเทคนิคการเรียนรู้เชิงลึกและเครือข่ายประสาทเทียมนับเป็นก้าวกระโดดสำคัญของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ โดยมีรายละเอียด คือ เครือข่ายประสาทเทียมคอนโวลูชันนัล (Convolutional Neural Networks - CNNs) เป็นประเภทของเครือข่ายประสาทเทียมเชิงลึกที่มีความสามารถโดดเด่นในการรับรู้รูปภาพและรูปแบบ รวมถึงการวิเคราะห์โครงสร้างอีเมลที่ซับซ้อน สามารถแยกแยะอีเมลปลอมหรือการฉ้อโกงจากอีเมลปกติ เพิ่มการป้องกันภัยคุกคามที่พบบ่อยอย่างการฉ้อโกง และ เครือข่ายประสาทเทียมรีเคอร์เรนต์ (Recurrent Neural Networks - RNNs) ถูกออกแบบมาเพื่อรับรู้รูปแบบลำดับในข้อมูล จึงเหมาะสำหรับงานวิเคราะห์ข้อมูลแบบลำดับ ในด้านรักษาความปลอดภัย RNNs ถูกใช้ติดตามพฤติกรรมผู้ใช้งาน เพื่อวิเคราะห์ลำดับการกระทำของผู้ใช้เพื่อสร้างรูปแบบพฤติกรรมปกติ และระบุพฤติกรรมเบี่ยงเบนที่น่าสงสัย ทำให้สามารถตรวจจับภัยคุกคามได้ในเวลาจริง รวมไปถึงกลไกการตอบสนองอัตโนมัติ ระบบรักษาความปลอดภัยแบบดั้งเดิมมักแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบภัยคุกคาม แต่กับการโจมตีไซเบอร์ในปัจจุบันที่รวดเร็วและมีขนาดใหญ่ การรอการตอบสนอง

จากมนุษย์อาจสร้างความเสียหายรุนแรง โมเดลการเรียนรู้เชิงลึกที่มีกลไกตอบสนองอัตโนมัติสามารถดำเนินมาตรการป้องกันได้ทันที เช่น ตัดการเชื่อมต่อจุดที่ถูกคุกคาม หรือกักกันสิ่งที่เป็นภัยคุกคาม เพื่อลดความเสียหาย (VC3, 2023)

จากเนื้อหาทั้งหมดในบทนี้ ทำให้เห็นพัฒนาการที่สำคัญของปัญญาประดิษฐ์ ตั้งแต่ยุคเริ่มแรกจนถึงปัจจุบัน การประยุกต์ใช้ปัญญาประดิษฐ์ในทางการทหารได้มีบทบาทสำคัญต่อการเสริมสร้างความมั่นคงทางไซเบอร์ และได้พิจารณาการนำปัญญาประดิษฐ์มาใช้ในรูปแบบต่าง ๆ เพื่อเพิ่มประสิทธิภาพในการป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม การนำปัญญาประดิษฐ์มาใช้ก็ยังมีความเสี่ยงที่ต้องพิจารณา เนื่องจากปัญญาประดิษฐ์เองก็สามารถเป็นเครื่องมือที่มีประสิทธิภาพในการโจมตีทางไซเบอร์ได้เช่นกัน

บทที่ 3
การประยุกต์ใช้ปัญญาประดิษฐ์ทางการทหารกับความมั่นคงทางไซเบอร์

ในบทนี้จะเจาะลึกถึงการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในทางการทหารและความมั่นคงทางไซเบอร์ โดยจะเน้นไปที่การวิเคราะห์รูปแบบของการโจมตีและการป้องกันที่ใช้เทคโนโลยีปัญญาประดิษฐ์ซึ่งการศึกษาในส่วนนี้มีความสำคัญอย่างยิ่งเนื่องจากปัญญาประดิษฐ์ไม่เพียงแต่เพิ่มประสิทธิภาพในการตรวจจับและตอบโต้ภัยคุกคาม แต่ยังสามารถเป็นเครื่องมือที่ทรงพลังในการโจมตีทางไซเบอร์ได้ด้วย

3.1 การโจมตีทางไซเบอร์โดยเทคโนโลยีปัญญาประดิษฐ์ทางการทหาร

การแข่งขันในสมรภูมิรบไซเบอร์นั้นมีความตึงเครียดมากยิ่งขึ้น โดยมีการโจมตีทางไซเบอร์ในด้านต่าง ๆ ไม่ว่าจะเป็นการสร้างข่าวปลอมเผยแพร่ข้อมูลเท็จ การเจาะระบบฐานข้อมูลขององค์กรเพื่อเข้าถึงข้อมูลบัญชีผู้ใช้ส่วนตัว โดยกองทัพไซเบอร์ ที่ได้รับการสนับสนุนจากรัฐบาลโดยอาจจะมีวัตถุประสงค์เพื่อช่วงชิงผลประโยชน์ทางเศรษฐกิจหรือการเมือง การสอดแนมทางเศรษฐกิจหรือการเก็บรวบรวมข่าวสารจากรัฐคู่อริ เนื่องจากปัญญาประดิษฐ์ (AI) มีศักยภาพมากพอที่จะส่งผลกระทบต่อรูปแบบของสงครามที่เปลี่ยนแปลงไปและมีความรุนแรงและอันตรายมากยิ่งขึ้น โดยพื้นที่ไซเบอร์ได้กลายมาเป็นอีกสมรภูมิรบอีกแห่งหนึ่ง ด้วยการโจมตีผ่านทางไซเบอร์หรือที่เรียกว่า สงครามไซเบอร์ (Cyber Warfare) หมายถึงการโจมตีทางไซเบอร์หรือชุดของการโจมตีที่มีเป้าหมายเป็นประเทศหนึ่ง มีศักยภาพในการสร้างความเสียหายต่อโครงสร้างพื้นฐานทั้งภาครัฐและพลเรือน รวมถึงระบบสำคัญต่าง ๆ อาจนำไปสู่ความเสียหายต่อรัฐและสูญเสียชีวิตได้

โดยไมโครซอฟท์ได้มีการตั้งชื่อกลุ่มผู้คุกคามผ่านธีมที่เกี่ยวกับสภาพอากาศ ดังเช่นในภาพประกอบ 4 เพื่อให้เกิดความชัดเจนมากขึ้นสำหรับลูกค้าและนักวิจัยด้านความปลอดภัย ระบบการตั้งชื่อใหม่นี้มีความเป็นระเบียบ เข้าใจง่าย และช่วยให้องค์กรสามารถจัดลำดับความสำคัญและป้องกันตัวเองได้ดีขึ้น รวมทั้งช่วยให้นักวิจัยด้านความปลอดภัยที่ต้องรับมือกับข้อมูลข่าวกรองภัยคุกคามที่มีมากมายได้ง่ายขึ้นด้วย

ภาพประกอบ 4 การตั้งชื่อและแหล่งที่มาของมัลแวร์โดยไมโครซอฟต์

ที่มา: Microsoft Defender. (2024, April 29). How Microsoft names threat actors. Microsoft. https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming

ตัวอย่างการตรวจพบการโจมตีทางไซเบอร์ กลุ่มแฮกเกอร์ต่าง ๆ มักจะมีการเน้นใช้ปัญญาประดิษฐ์ในส่วนของ Large Language Models ในการสร้างไฟล์ไวรัสต่าง ๆ หรือการพัฒนาการเขียนโค้ดไวรัส เพื่อทำการทำโจมตีทางไซเบอร์ จากการร่วมมือและแบ่งปันข้อมูลระหว่าง OpenAI กับ Microsoft ได้มีการยับยั้งนักโจมตีที่เป็นกลุ่มอันตรายที่เกี่ยวข้องกับรัฐจำนวนห้ากลุ่ม ได้แก่

Crimson Sandstorm จากอิหร่าน ได้มีการใช้บริการในการช่วยเขียนสคริปต์ที่เกี่ยวข้องกับการพัฒนาแอปและเว็บ สร้างเนื้อหาที่น่าจะใช้ในการโจมตีแบบ spear-phishing ซึ่งเป็นการโจมตีทางไซเบอร์ที่มีการปรับแต่งข้อความให้เฉพาะเจาะจงกับเป้าหมาย โดยนักโจมตีจะใช้ข้อมูลที่หามาได้จากแหล่งข้อมูลสาธารณะหรือออนไลน์ เพื่อสร้างอีเมลหรือข้อความที่ดูเหมือนมาจากแหล่งที่เชื่อถือได้ เช่น หัวหน้า เพื่อนร่วมงาน หรือองค์กรที่รู้จัก และศึกษาวิธีหลบซ่อนการจากตรวจจับของระบบ โดยถูกสังเกตเห็นว่าใช้เครือข่ายของบัญชีโซเชียลมีเดียปลอมเพื่อสร้างความไว้วางใจกับเป้าหมายและส่งมัลแวร์เพื่อขโมยข้อมูล นอกจากนี้ ในปี 2021 Crimson Sandstorm ได้ดำเนินการโจมตีแบบ spear-phishing โดยมุ่งเป้าไปที่บริษัทที่ให้บริการด้าน IT และวิศวกรรมสำหรับหน่วยงานป้องกันประเทศและหน่วยข่าวกรองของสหรัฐฯ ซึ่งน่าจะเป็นส่วนหนึ่งของปฏิบัติการห่วงโซ่อุปทานเพื่อเข้าถึงลูกค้าของพวกเขารวมไปถึงรัฐบาลในตะวันออกกลางอีกด้วย (Microsoft, 2024a)

Emerald Sleet จากเกาหลีเหนือ ใช้บริการในการระบุตัวผู้เชี่ยวชาญและองค์กรที่มุ่งเน้นประเด็นการป้องกันในภูมิภาคเอเชียแปซิฟิก ทำความเข้าใจช่องโหว่ที่เปิดเผยต่อสาธารณะ ช่วยเหลือในการเขียนโปรแกรมเบื้องต้น และร่างเนื้อหาที่สามารถใช้ในการโจมตีฟิชชิ่ง โดยเป็นกลุ่มแฮกเกอร์ที่มีความเคลื่อนไหวมากที่สุดของเกาหลีเหนือที่ Microsoft ติดตามในปีที่ผ่านมา กลุ่มนี้ยังคงส่งอีเมล spear-phishing ไปยังผู้เชี่ยวชาญเรื่องคาบสมุทรเกาหลีทั่วโลกเพื่อรวบรวมข่าวกรอง โดยมุ่งเป้าไปยังผู้เชี่ยวชาญด้านเกาหลีเหนือที่มีอิทธิพลในสหรัฐอเมริกาและประเทศพันธมิตร แทนที่จะส่งไฟล์หรือลิงก์ที่เป็นอันตราย กลุ่มนี้ใช้เทคนิคเฉพาะโดยการแอบอ้างเป็นสถาบันการศึกษาที่มีชื่อเสียงและองค์กร NGOs เพื่อหลอกล่อเหยื่อให้ตอบกลับด้วยความคิดเห็นและข้อมูลเชิงลึกเกี่ยวกับนโยบายต่างประเทศที่เกี่ยวข้องกับเกาหลีเหนือ (Microsoft, 2024b)

Forest Blizzard จากรัสเซีย ใช้บริการของเราในการค้นหาข้อมูลจากแหล่งเปิดเกี่ยวกับวิธีการสื่อสารผ่านดาวเทียมและเทคโนโลยีการถ่ายภาพด้วยเรดาร์ รวมถึงการช่วยในการเขียนโปรแกรมเบื้องต้น(OpenAI, 2024) โจมตีใช้เทคนิคการเข้าถึงแรกเริ่มที่หลากหลาย รวมถึงการเจาะช่องโหว่ในแอปพลิเคชันที่เปิดให้ใช้งานผ่านเว็บ และการขโมยข้อมูลประจำตัวผ่านการโจมตีแบบ spear phishing รวมถึงการใช้เครื่องมือการเดารหัสผ่านอัตโนมัติ มุ่งเน้นไปยังหน่วยงานรัฐบาล องค์กรการทูตและการป้องกันประเทศ คลังสมอง องค์กรที่ไม่ใช่รัฐบาล สถาบันการศึกษา บริการซอฟต์แวร์และ IT บริษัทที่เกี่ยวข้องการค้าอาวุธ ประเทศที่ตกเป็นเป้าหมาย ได้แก่ ออสเตรเลีย แคนาดา อินเดีย อิสราเอล ญี่ปุ่น ยูเครนและสหรัฐอเมริกา (Microsoft, 2024c)

Charcoal Typhoon จากจีน ได้มีการใช้บริการต่าง ๆ เพื่อศึกษาบริษัทและเครื่องมือด้านความปลอดภัยทางไซเบอร์ โดยเฉพาะการแก้ไขข้อผิดพลาดของโค้ดและการสร้างสคริปต์เพื่อใช้ในการโจมตี นอกจากนี้ยังสร้างเนื้อหาที่น่าจะใช้ในการโจมตีฟิชชิ่ง ซึ่งเป็นการสร้างข้อความหรืออีเมลที่ดูเหมือนมาจากแหล่งที่น่าเชื่อถือเพื่อหลอกลวงผู้รับให้เปิดเผยข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับ การกระทำดังกล่าวทำให้ Charcoal Typhoon สามารถแทรกซึมและเจาะระบบของเป้าหมายได้อย่างมีประสิทธิภาพมากขึ้น

Salmon Typhoon จากจีน ใช้บริการที่หลากหลายในการแปลเอกสารทางเทคนิคและดึงข้อมูลที่เปิดเผยต่อสาธารณะเกี่ยวกับหน่วยงานข่าวกรองและกลุ่มแฮกเกอร์ในภูมิภาคอื่น ๆ การใช้ข้อมูลนี้ช่วยให้ Salmon Typhoon สามารถวิเคราะห์และเข้าใจถึงกลยุทธ์และเครื่องมือที่คู่แข่งใช้ นอกจากนี้ยังใช้ปัญญาประดิษฐ์ ในการช่วยเขียนโค้ดและศึกษาวิธีการหลบซ่อนจากการตรวจจับของระบบความปลอดภัย ปัญญาประดิษฐ์ ที่ใช้ช่วยในการสร้างโค้ดที่มีความซับซ้อนและการปรับเปลี่ยนโค้ดเพื่อหลีกเลี่ยงการตรวจจับจากโปรแกรมป้องกันไวรัสและระบบตรวจจับการโจมตี

ตารางที่ 2 แสดงการโจมตีทางไซเบอร์ที่ใช้เทคโนโลยีปัญญาประดิษฐ์ทางการทหาร

ชื่อ	ประเทศที่สนับสนุน	เทคโนโลยีที่ใช้	เป้าหมายการโจมตี
Forest Blizzard	รัสเซีย	LLMs, การวิจัยเทคโนโลยีดาวเทียมและเรดาร์	หน่วยงานรัฐบาล, องค์กรการทูตและการป้องกันประเทศ, คลังสมอง, สถาบันการศึกษา, บริษัทที่เกี่ยวข้องการค้าอาวุธ
Emerald Sleet	เกาหลีเหนือ	LLMs, การปลอมแปลงสถาบันวิชาการและ NGO	ผู้เชี่ยวชาญเรื่องคาบสมุทรเกาหลี, สถาบันการศึกษาที่มีชื่อเสียง, องค์กร NGOs
Crimson Sandstorm	อิหร่าน	LLMs, การพัฒนา .NET, การวิจัยกลยุทธ์การหลบเลี่ยง	บริษัท IT และวิศวกรรม, หน่วยงานป้องกันประเทศและหน่วยข่าวกรองของสหรัฐฯ, รัฐบาลในตะวันออกกลาง
Charcoal Typhoon	จีน	LLMs, การวิจัยเทคโนโลยีและแพลตฟอร์มต่าง ๆ	บริษัทด้านความปลอดภัยทางไซเบอร์, การโจมตีฟิชชิ่ง
Salmon Typhoon	จีน	LLMs, การประเมินข้อมูลที่ละเอียดอ่อน	หน่วยงานข่าวกรอง, กลุ่มแฮกเกอร์ในภูมิภาคอื่น ๆ

ที่มา: Microsoft Threat Intelligence. (2024, February 14). Staying ahead of threat actors in the age of AI. Microsoft. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

กลุ่มแฮกเกอร์จากจีนยังได้มีการมุ่งเป้าไปที่กวม ขณะที่สหรัฐฯ กำลังสร้างฐานทัพหลักของกองทัพเมรีน โดยแบ่งออกเป็น 3 กลุ่มหลัก ได้แก่ Circle Typhoon (DEV-0322), Volt Typhoon (DEV-0391), และ Mulberry Typhoon (MANGANESE) ได้เพิ่มการโจมตีอุตสาหกรรมอุตสาหกรรมป้องกันของสหรัฐฯ โดย Circle Typhoon ดำเนินกิจกรรมไซเบอร์อย่างกว้างขวาง รวมถึงการพัฒนาทรัพยากร การรวบรวมข้อมูล การเข้าถึงเบื้องต้น และการเข้าถึงข้อมูลประจำตัว มักใช้อุปกรณ์ VPN เป็นช่องทางในขณะที่ Volt Typhoon ยังทำการสำรวจ บริษัทอุตสาหกรรมป้องกันของสหรัฐฯ หลายแห่ง โดยมักจะเจาะระบบเครื่องเราเตอร์ขนาดเล็ก และ Mulberry Typhoon ยังมุ่งเป้าโจมตีอุตสาหกรรมป้องกันของสหรัฐฯ โดยใช้ช่องโหว่ "zero-day" หรือที่เรียกว่า zero-day exploit หมายถึงการโจมตีทางไซเบอร์ที่เกิดขึ้นเมื่อผู้ไม่หวังดีหรือแฮกเกอร์ค้นพบช่องโหว่ในซอฟต์แวร์และใช้ประโยชน์จากช่องโหว่นั้นก่อนที่ผู้พัฒนาโปรแกรมจะทราบและมีการแก้ไขช่องโหว่นี้เรียกว่า "zero-day" เนื่องจากผู้พัฒนาโปรแกรมมีเวลา "ศูนย์วัน" ในการแก้ไขช่องโหว่และก่อนที่จะมีการโจมตีเกิดขึ้นการเพิ่มการโจมตีกวมนั้นมีความหมายสำคัญ เนื่องจากกวมเป็น

ดินแดนของสหรัฐฯ ที่ใกล้เอเชียตะวันออกมากที่สุด และมีความสำคัญต่อยุทธศาสตร์ของสหรัฐในภูมิภาค (Department of Justice, 2024)

นอกจากนี้ยังมีการสร้างรูปภาพจาก Generative AI ซึ่งเป็นเทคโนโลยีปัญญาประดิษฐ์ที่สามารถสร้างข้อมูลใหม่ที่ไม่เคยมีมาก่อนบนพื้นฐานของข้อมูลที่มีอยู่ เทคโนโลยีนี้สามารถสร้างเนื้อหาต่าง ๆ เช่น ข้อความ รูปภาพ วิดีโอ หรือเสียง โดยใช้โมเดลการเรียนรู้เชิงลึก (deep learning) ที่ได้รับการฝึกฝนด้วยข้อมูลจำนวนมากเพื่อสร้างรูปภาพ และโพสต์ผ่านสื่อบัญชีสังคมออนไลน์ที่ควบคุมโดยพรรคคอมมิวนิสต์จีน หรือที่เรียกว่า “AI Deepfakes” และมีจำนวนมากยิ่งขึ้นเรื่อย ๆ รับหน้าที่โดยกองทัพ IO ก่อนการเลือกตั้งสหรัฐฯ ปี 2022 ซึ่งศูนย์วิเคราะห์ภัยคุกคามของ Microsoft (MTAC) ได้เฝ้าระวังแฮกเกอร์ในจีนที่โพสต์เผยแพร่ข้อมูลปลอมไปยังพลเรือนอเมริกันบนโซเชียลมีเดีย ได้พบเจอว่า ได้มีสร้างเนื้อหาปลอมโดยใช้ปัญญาประดิษฐ์เพื่อพยายามแทรกแซงการเลือกตั้งประธานาธิบดีไต้หวันที่มีขึ้นในเดือนมกราคมที่ผ่านมา ซึ่งเป็นครั้งแรกที่มีกลุ่มที่มีรัฐชาติหนุนหลังใช้เนื้อหาที่ปัญญาประดิษฐ์สร้างขึ้นในการไปพยายามบิดเบือนผลการเลือกตั้งของรัฐอื่น การเผยแพร่ข้อมูลเท็จผ่านโลกโซเชียลเพื่อพยายามส่งอิทธิพลต่อการเลือกตั้งทั่วโลกจะส่งผลน้อยในยุคปัจจุบัน แต่จีนก็จะพยายามทดลองพัฒนาเนื้อหาด้วยการเพิ่มมีม คลิปวิดีโอ และใส่เสียงต่อไป ซึ่งอาจส่งผลเป็นรูปธรรมในอนาคต โดยใช้ปัญญาประดิษฐ์สร้างขึ้น รวมไปถึงบางโพสต์พยายามเผยแพร่ทฤษฎีสมคบคิดเกี่ยวกับเหตุการณ์ใหญ่อีกด้วย (Johnson, 2024) ทำให้อังกฤษได้รับความกังวลจากผู้เชี่ยวชาญทางด้านความปลอดภัยทางไซเบอร์ว่า อาจจะมีการนำเทคโนโลยี Generative AI มาใช้แทรกแซงการเลือกตั้งที่กำลังจะเกิดขึ้นหลายวิธี โดยเฉพาะการเผยแพร่ข้อมูลเท็จที่ได้รับการสนับสนุนจากปัญญาประดิษฐ์ โดยมีการคาดการณ์ว่าการโจมตีที่ได้รับการสนับสนุนจากรัฐจะเพิ่มมากขึ้นก่อนการเลือกตั้ง และวิเคราะห์ว่าประเทศจีน รัสเซีย และอิหร่านอาจจะดำเนินการปฏิบัติการข้อมูลเท็จต่อการเลือกตั้งทั่วโลกด้วยความช่วยเหลือจากเครื่องมือปัญญาประดิษฐ์ (Browne, 2024)

3.2 การป้องกันทางไซเบอร์โดยเทคโนโลยีปัญญาประดิษฐ์ทางการทหาร

ปัญญาประดิษฐ์ได้เข้ามามีบทบาทในการสร้างเกราะคุ้มกันต่อภัยคุกคามทางไซเบอร์ที่เข้ามาโจมตีด้วยวิธีต่าง ๆ ในทางทหาร และทำงานร่วมกันหน่วยงานรัฐบาลเพื่อตรวจสอบตรวจหา และตรวจจับภัยคุกคามที่ได้รับการสนับสนุนจากรัฐ (state-sponsored cyberattack) เพื่อโจมตีโครงสร้างพื้นฐาน ตัวอย่างเช่นในสหรัฐอเมริกา ได้มีการนำเอาเทคโนโลยีปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง มาใช้ในการช่วยเหลือสำนักงานความมั่นคงแห่งชาติ ที่

เป็นหน่วยงานข่าวกรองระดับชาติของกระทรวงกลาโหมสหรัฐ และหน่วยงานอื่น ๆ ในสหรัฐอเมริกา ในการตรวจจับมัลแวร์และกิจกรรมทางไซเบอร์ที่เป็นอันตรายของจีนได้ และได้มีการรายงานหลังจากการประชุมร่วมกับศูนย์ความร่วมมือด้านความปลอดภัยทางไซเบอร์ว่า จีนกำลังเจาะโครงสร้างพื้นฐานที่สำคัญและรอ เวลาที่ดีที่สุดในการใช้ประโยชน์จากเครือข่ายเหล่านี้(Vicens, 2024)

ตารางที่ 3 เทคโนโลยีปัญญาประดิษฐ์ที่มีการใช้งานในสำนักความมั่นคงโครงสร้างพื้นฐานและการรักษาความมั่นคงปลอดภัยไซเบอร์

ชื่อเทคโนโลยี	เนื้อหาหลัก	เทคโนโลยีปัญญาประดิษฐ์ที่ใช้	ระยะของการพัฒนาระบบ
AIS Automated Scoring & Feedback (AS&F)	อัลกอริทึมที่ช่วยเพิ่มความแม่นยำในการประเมินและให้คะแนนข้อมูลไซเบอร์	Descriptive Analysis, Machine Learning, Natural Language Processing (NLP)	ดำเนินงานอยู่
Automated Indicator Sharing (AIS) Automated PII Detection	การตรวจจับข้อมูลส่วนบุคคลอัตโนมัติผ่านการวิเคราะห์และการตรวจทานของมนุษย์	Natural Language Processing (NLP)	ดำเนินงานอยู่
Advanced Analytic Enabled Forensic Investigation	การใช้ปัญญาประดิษฐ์เพื่อช่วยนักวิเคราะห์ในการตรวจสอบเหตุการณ์ไซเบอร์	Machine Learning	เริ่มต้นพัฒนา
Advanced Network Anomaly Alerting	แจ้งเตือนความผิดปกติของเครือข่ายโดยใช้ปัญญาประดิษฐ์ค้นหาการโจมตี	Machine Learning	เริ่มต้นพัฒนา
AI Security and Robustness	กระบวนการและเครื่องมือในการทดสอบและประเมินปัญญาประดิษฐ์เพื่อความปลอดภัยและความน่าเชื่อถือ	Machine Learning, Natural Language Processing (NLP)	เริ่มต้นพัฒนา
Cyber Incident Reporting	การรวบรวมและการเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์โดยใช้ AI	Machine Learning, Natural Language Processing (NLP)	เริ่มต้นพัฒนา
Cyber Threat Intelligence Feed Correlation	การเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์จากหลายแหล่งด้วย AI	Machine Learning, Natural Language Processing (NLP)	เริ่มต้นพัฒนา
Cyber Vulnerability Reporting	การรายงานช่องโหว่ไซเบอร์โดยใช้ปัญญาประดิษฐ์เพื่อเพิ่มความแม่นยำและความเกี่ยวข้องของข้อมูล	Natural Language Processing (NLP), Visualization	เริ่มต้นพัฒนา

ตารางที่ 3 (ต่อ)

ชื่อเทคโนโลยี	เนื้อหาหลัก	เทคโนโลยีปัญญาประดิษฐ์ที่ใช้	ระยะของการพัฒนาระบบ
Malware Reverse Engineering	การย้อนรอยและวิเคราะห์มัลแวร์เพื่อปรับปรุงการรับมือภัยคุกคาม	Machine Learning	เริ่มต้นพัฒนา
Security Information and Event Management (SIEM) Alerting Models	แจ้งเตือนความผิดปกติใน Log ด้วยปัญญาประดิษฐ์เพื่อค้นหาการโจมตีไซเบอร์	Machine Learning	เริ่มต้นพัฒนา

ที่มา: Cybersecurity and Infrastructure Security Agency. (2024). CISA Artificial Intelligence Use Cases. https://www.cisa.gov/ai/cisa-use-cases

ตัวอย่างการนำเอาเทคโนโลยีมาใช้ในการรักษาความมั่นคงทางไซเบอร์ โดยสำนักความมั่นคงโครงสร้างพื้นฐานและการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity and Infrastructure Security Agency- CISA) ของสหรัฐอเมริกา ที่ได้นำมาประยุกต์ใช้ในการป้องกันภัยคุกคามทางไซเบอร์ ดังเช่นในตารางที่ 3 ที่ ถึงแม้ว่าบางเทคโนโลยีจะอยู่ในช่วงของการเริ่มต้นในการพัฒนา แต่ก็ถือว่าเป็นหมุดหมายสำคัญที่ดีสำหรับรักษาความมั่นคงทางไซเบอร์ที่อาจลุกลามไปยังส่วนอื่น ๆ ของโครงสร้างพื้นฐานของชาติได้

ไม่เพียงแค่ในสหรัฐอเมริกาเท่านั้นที่ให้ความสำคัญกับการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์กับความมั่นคงทางไซเบอร์ สหราชอาณาจักรก็ได้มีการจัดตั้งศูนย์ปัญญาประดิษฐ์ด้านการป้องกัน (Defence Artificial Intelligence Centre - DAIC) สนับสนุนกรณีการใช้งานปัญญาประดิษฐ์ทางทหารโดยทำงานร่วมกับพันธมิตรระหว่างประเทศทั้งในรัฐบาล สถาบันการศึกษา และอุตสาหกรรม โดยมีเป้าหมายคือ การพัฒนาเครือข่ายปัญญาประดิษฐ์ด้านการป้องกันและความมั่นคงแห่งชาติเพื่อส่งเสริมการแลกเปลี่ยนความสามารถและการสร้างร่วมกัน เครือข่ายนี้จะส่งเสริมการลงทุนจากภาคพลเรือนในงานวิจัยและพัฒนาปัญญาประดิษฐ์ที่เกี่ยวข้องกับการป้องกัน เพื่อให้ง่ายต่อการเข้าถึงข้อมูลและทรัพยากรการป้องกัน ขณะเดียวกันยังเป็นพื้นที่ในการแบ่งปันข้อกำหนดและพัฒนาวิธีปฏิบัติที่ดีที่สุดในกิจกรรมต่าง ๆ ตั้งแต่นโยบายและเทคนิคไปจนถึงการค้าขายและการจัดซื้อจัดจ้าง(Government Digital Service, 2024)

ดังนั้นจึงเห็นได้ว่า การนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการป้องกันทางไซเบอร์ในทางการทหารเป็นวิธีการที่มีประสิทธิภาพสูง โดยสามารถตรวจจับและตอบสนองต่อภัยคุกคาม

ได้อย่างรวดเร็วและแม่นยำ ทั้งยังช่วยเสริมสร้างความมั่นคงปลอดภัยให้กับเครือข่ายและข้อมูลสำคัญ การวิเคราะห์ข้อมูลแบบเรียลไทม์และการตรวจจับพฤติกรรมที่ผิดปกติในเครือข่ายเป็นเครื่องมือสำคัญในการป้องกันการโจมตีทางไซเบอร์ที่ซับซ้อนและไม่เคยเกิดขึ้นมาก่อน การใช้ปัญญาประดิษฐ์ในการป้องกันทางไซเบอร์จึงเป็นการพัฒนาและยกระดับมาตรการป้องกันให้ทันสมัยและมีประสิทธิภาพมากยิ่งขึ้น ซึ่งมีความสำคัญอย่างยิ่งในการรักษาความมั่นคงปลอดภัยในสภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างรวดเร็วและเต็มไปด้วยความท้าทายทางไซเบอร์ในปัจจุบัน

บทที่ 4
ผลกระทบจากการใช้ปัญญาประดิษฐ์ทางการทหารต่อความมั่นคงทางไซเบอร์

บทนี้จะนำเสนอการวิเคราะห์เกี่ยวกับผลกระทบที่เกิดขึ้นจากการใช้ปัญญาประดิษฐ์ในทางการทหารต่อความมั่นคงทางไซเบอร์ วัตถุประสงค์ของบทนี้คือเพื่อวิเคราะห์และอธิบายถึงผลกระทบทั้งด้านบวกและด้านลบของการนำปัญญาประดิษฐ์มาใช้ในทางการทหารต่อความมั่นคงทางไซเบอร์ ซึ่งเป็นจุดเริ่มต้นของการวางนโยบายของรัฐต่าง ๆ อีกด้วย ดังต่อไปนี้

4.1 ผลกระทบต่อความมั่นคงทางเครือข่าย

การนำปัญญาประดิษฐ์มาใช้ในภาคการทหารเพื่อเพิ่มความมั่นคงทางเครือข่าย มีทั้งผลกระทบที่เป็นประโยชน์และผลกระทบที่มีความเสี่ยงระดับสูง การวิเคราะห์ผลกระทบที่เกิดขึ้นต่อระบบเครือข่ายสามารถแบ่งออกได้ดังต่อไปนี้

1. การเพิ่มประสิทธิภาพในการป้องกันและตรวจจับภัยคุกคาม

การใช้ปัญญาประดิษฐ์ในระบบไฟร์วอลล์และระบบป้องกันการบุกรุก (IPS) ช่วยให้สามารถตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้น ระบบเหล่านี้สามารถวิเคราะห์ข้อมูลขนาดใหญ่และซับซ้อนได้อย่างรวดเร็ว ทำให้สามารถระบุและตอบสนองต่อภัยคุกคามใหม่ๆ ได้ทันที เช่น ไฟร์วอลล์รุ่นใหม่ที่เรียกว่า Next-Generation Firewall (Fortinet, 2024) ที่ใช้ปัญญาประดิษฐ์สามารถตรวจสอบข้อมูลอย่างละเอียดและตรวจจับภัยคุกคามที่ซับซ้อนได้ดียิ่งขึ้น ทำให้เครือข่ายปลอดภัยมากขึ้นจากการโจมตีทางไซเบอร์ต่างๆ ไม่ว่าจะเป็นการโจมตีแบบที่รู้จักแล้วหรือการโจมตีใหม่ๆ ที่เกิดขึ้นในอนาคต

2. การปรับตัวและพัฒนาระบบความปลอดภัยอย่างต่อเนื่อง

ปัญญาประดิษฐ์มีความสามารถในการเรียนรู้จากข้อมูลใหม่ๆ และปรับตัวตามสถานการณ์ ซึ่งทำให้ระบบความปลอดภัยสามารถพัฒนาและปรับปรุงเพื่อตอบสนองต่อภัยคุกคามที่เปลี่ยนแปลงตลอดเวลาได้อย่างมีประสิทธิภาพ การทำงานนี้ช่วยลดความเสี่ยงจากการถูกโจมตีและเพิ่มความมั่นคงให้กับเครือข่าย

ตัวอย่างเช่น ระบบปัญญาประดิษฐ์สามารถวิเคราะห์และทำนายรูปแบบการโจมตีใหม่ๆ ที่อาจเกิดขึ้นในอนาคต ทำให้สามารถเตรียมการป้องกันล่วงหน้าได้ ซึ่งหมายความว่าระบบสามารถปรับปรุงตัวเองเพื่อรับมือกับการโจมตีที่อาจเกิดขึ้นได้ตลอดเวลา และยังสามารถตอบสนองต่อภัยคุกคามใหม่ๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ

3. ความเสี่ยงจากการโจมตีที่ซับซ้อนมากขึ้น

ในขณะที่ปัญญาประดิษฐ์ช่วยในการป้องกันภัยคุกคาม การโจมตีที่ใช้ปัญญาประดิษฐ์ก็มีแนวโน้มที่จะซับซ้อนและมีประสิทธิภาพมากขึ้นเช่นกัน ผู้โจมตีสามารถใช้ปัญญาประดิษฐ์ในการวิเคราะห์ช่องโหว่และดำเนินการโจมตีที่ซับซ้อนขึ้น ทำให้การป้องกันทางไซเบอร์ต้องพัฒนาอย่างต่อเนื่องเพื่อรับมือกับการโจมตีที่ใช้ AIการโจมตีระบบไฟร์วอลล์ของ Cisco (Winder, 2024) ที่ใช้ช่องโหว่ zero-day แสดงให้เห็นถึงความซับซ้อนและความรุนแรงของการโจมตีที่สามารถเข้าถึงข้อมูลสำคัญได้ ถูกติดตามโดย Cisco Talos ในชื่อ UAT4356 และโดย Microsoft ในชื่อ STORM-1849 ซึ่งกลุ่ม STORM-1849 มีความเชื่อมโยงกับประเทศจีน ซึ่งเป็นหนึ่งในประเทศที่มีการสนับสนุนการโจมตีทางไซเบอร์ในหลากหลายเหตุการณ์ที่เกิดขึ้นในปัจจุบัน

4. ความจำเป็นในการเฝ้าระวังและการตอบสนองที่รวดเร็ว

การใช้ปัญญาประดิษฐ์ในการตรวจจับและป้องกันการโจมตีเครือข่ายทำให้สามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและแม่นยำยิ่งขึ้น การเฝ้าระวังที่มีประสิทธิภาพและการตอบสนองที่ทันท่วงทีช่วยลดความเสียหายที่อาจเกิดขึ้นจากการโจมตี ตัวอย่างเช่น ปัญญาประดิษฐ์สามารถตรวจสอบพฤติกรรมที่ผิดปกติและตอบสนองต่อการโจมตีในเวลาที่รวดเร็ว ช่วยป้องกันการเข้าถึงข้อมูลที่สำคัญและการล้มเหลวของระบบ

จะเห็นได้ว่า การใช้ปัญญาประดิษฐ์ในการเพิ่มความมั่นคงทางเครือข่ายในภาคการทหารและองค์กรต่าง ๆ ในขณะเดียวกันก็ต้องระมัดระวังและเตรียมพร้อมรับมือกับความท้าทายใหม่ ๆ ที่อาจเกิดขึ้นจากการใช้เทคโนโลยีปัญญาประดิษฐ์ในการโจมตีทางไซเบอร์เช่นกัน

4.2 ผลกระทบต่อความมั่นคงทางแอปพลิเคชัน

การใช้ปัญญาประดิษฐ์มีบทบาทสำคัญในการเพิ่มความมั่นคงทางแอปพลิเคชันในยุคดิจิทัล ซึ่งต้องเผชิญกับภัยคุกคามหลากหลายรูปแบบ การใช้ฮาร์ดแวร์และซอฟต์แวร์ที่มีปัญญาประดิษฐ์เป็นส่วนประกอบ เช่น แอนตี้ไวรัส การเข้ารหัส และไฟร์วอลล์ ช่วยเสริมสร้างการป้องกันที่แข็งแกร่งขึ้น การรักษาความมั่นคงของแอปพลิเคชัน (Application Security) มุ่งเน้นการป้องกันข้อมูลหรือโค้ดภายในแอปพลิเคชันไม่ให้ถูกขโมยหรือโจมตี รวมถึงการพิจารณาด้านความปลอดภัยตั้งแต่การพัฒนาและออกแบบไปจนถึงการป้องกันหลังการใช้งาน มาตรการเหล่านี้อาจรวมถึงฮาร์ดแวร์ ซอฟต์แวร์ และขั้นตอนต่าง ๆ เพื่อระบุหรือลดช่องโหว่ทางด้านความปลอดภัย

มาตรการความปลอดภัยของแอปพลิเคชัน

Authentication: เพื่อให้แน่ใจว่าเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงแอปพลิเคชันได้

Authorization: ตรวจสอบว่าผู้ใช้มีสิทธิ์ในการใช้งานแอปพลิเคชันหรือไม่

Encryption: ป้องกันข้อมูลที่สำคัญไม่ให้ถูกมองเห็นหรือใช้โดยผู้ไม่ประสงค์ดี

Logging: บันทึกกิจกรรมเพื่อสามารถตรวจสอบการละเมิดความปลอดภัยได้

Application Security Testing: การทดสอบเพื่อให้แน่ใจว่าการควบคุมความปลอดภัยทั้งหมดทำงานอย่างถูกต้อง (Vmware, 2024)

การรักษาความปลอดภัยของแอปพลิเคชันในคลาวด์มีความท้าทายมากยิ่งขึ้น เนื่องจากสิ่งแวดล้อมคลาวด์มีการแชร์ทรัพยากรและข้อมูลที่มีความสำคัญ มีความเสี่ยงต่อการถูกโจมตีมากขึ้น ในขณะที่ความปลอดภัยของแอปพลิเคชันบนมือถือจะเน้นไปที่การป้องกันข้อมูลที่ส่งผ่านอินเทอร์เน็ตและการใช้งาน VPN เพื่อเพิ่มความปลอดภัยในการเชื่อมต่อระยะไกล ตัวอย่างเช่น การโจมตีระบบความปลอดภัยของแอปพลิเคชันของ Pegasus Spyware

Pegasus เป็นสปายแวร์ที่พัฒนาโดย NSO Group ของอิสราเอล เพื่อการสอดแนมผู้ใช้งานอุปกรณ์เคลื่อนที่ มันสามารถติดตั้งโดยไม่ต้องมีการกระทำใด ๆ จากผู้ใช้และสามารถเข้าถึงข้อมูลที่สำคัญในอุปกรณ์ของผู้ใช้ได้ เช่น ข้อความ อีเมล การโทร และตำแหน่ง โดยสามารถติดตั้งผ่านช่องโหว่แบบ zero-click exploits ซึ่งผู้ใช้ไม่จำเป็นต้องคลิกลิงก์หรือทำการใด ๆ ตัวสปายแวร์จะสามารถอ่านข้อความและอีเมล เข้าถึงไมโครโฟนและกล้อง ฟังการสนทนาโทรศัพท์ บันทึกรหัสผ่าน ติดตามตำแหน่งและการใช้งานแอป ข้อมูลที่ถูกเก็บรวบรวมจะถูกส่งไปยังเซิร์ฟเวอร์ของ NSO Group เพื่อการวิเคราะห์ (Apportugal, 2024)

ผลกระทบต่อความมั่นคงทางแอปพลิเคชัน

1. การเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคาม ปัญญาประดิษฐ์ช่วยในการตรวจจับและป้องกันภัยคุกคามที่ซับซ้อนได้อย่างมีประสิทธิภาพมากขึ้น เช่น การใช้ปัญญาประดิษฐ์ในการพัฒนาแอนตี้ไวรัสและไฟร์วอลล์

2. การปรับปรุงกระบวนการ Authentication และ Authorization ปัญญาประดิษฐ์ช่วยในการพัฒนาระบบการตรวจสอบและยืนยันตัวตนที่มีความปลอดภัยและแม่นยำมากขึ้น เช่น การวิเคราะห์พฤติกรรมของผู้ใช้เพื่อยืนยันตัวตน

3. การเพิ่มประสิทธิภาพในการเข้ารหัสและการจัดการข้อมูล ปัญญาประดิษฐ์ ช่วยเพิ่มความสามารถในการเข้ารหัสข้อมูลและการจัดการข้อมูลที่มีความสำคัญ ทำให้ป้องกันข้อมูลไม่ให้ถูกเข้าถึงหรือถูกขโมยได้

4. การเฝ้าระวังและการตอบสนองต่อภัยคุกคามแบบเรียลไทม์ ปัญญาประดิษฐ์สามารถช่วยในการเฝ้าระวังและตอบสนองต่อภัยคุกคามที่เกิดขึ้นแบบเรียลไทม์ ทำให้สามารถลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้นได้

การใช้ปัญญาประดิษฐ์เพื่อเสริมสร้างความมั่นคงทางแอปพลิเคชันมีประโยชน์ในด้านการเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคาม การปรับปรุงกระบวนการ Authentication และ Authorization การเพิ่มประสิทธิภาพในการเข้ารหัสและการจัดการข้อมูล และการเฝ้าระวังและตอบสนองต่อภัยคุกคามแบบเรียลไทม์ อย่างไรก็ตาม การใช้ปัญญาประดิษฐ์ยังมีความเสี่ยงที่ต้องระมัดระวัง เช่น การโจมตีที่ซับซ้อนมากขึ้นและการใช้ปัญญาประดิษฐ์ ในการโจมตี ดังนั้นการพัฒนาและใช้งานปัญญาประดิษฐ์ ต้องมีการควบคุมและตรวจสอบอย่างต่อเนื่องเพื่อให้สามารถรับมือกับความท้าทายที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

4.3 ผลกระทบต่อความมั่นคงทางข้อมูล

การใช้ปัญญาประดิษฐ์ในภาคการทหารไม่เพียงแต่เพิ่มความมั่นคงทางเครือข่ายและแอปพลิเคชัน แต่ยังส่งผลสำคัญต่อความมั่นคงทางข้อมูลด้วย ความมั่นคงทางข้อมูลนั้นครอบคลุมถึงการรักษาความลับ (Confidentiality), ความถูกต้อง (Integrity), และ ความพร้อมใช้งาน (Availability) ซึ่งเรียกรวมกันว่า "CIA Triad"

องค์ประกอบของความมั่นคงทางข้อมูล (CIA Triad)

1. การรักษาความลับ (Confidentiality) การป้องกันไม่ให้ข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลยังคงเป็นความลับและเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์หรือจำเป็นต้องใช้เพื่อปฏิบัติหน้าที่

2. ความถูกต้อง (Integrity) การป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งรวมถึงการเพิ่มเติม การลบ หรือการแก้ไขข้อมูล เพื่อให้ข้อมูลมีความแม่นยำและเชื่อถือได้ และไม่ถูกแก้ไขโดยไม่ถูกต้องไม่ว่าจะโดยตั้งใจหรือโดยไม่ตั้งใจ

3. ความพร้อมใช้งาน (Availability) การมุ่งเน้นให้ข้อมูลสามารถเข้าถึงและใช้งานได้ตลอดเวลาเมื่อจำเป็น เพื่อสนับสนุนการดำเนินงานอย่างต่อเนื่องขององค์กร

ในทางการทหารสามารถเสริมสร้างความมั่นคงทางข้อมูลได้อย่างมาก เช่น การเสริมสร้างการรักษาความลับปัญญาประดิษฐ์ ช่วยในการวิเคราะห์และตรวจจับกิจกรรมที่ผิดปกติบนเครือข่าย ทำให้สามารถป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตได้ดีขึ้น เช่น การใช้ปัญญาประดิษฐ์ในบริการวิเคราะห์การจำลองการป้องกันของ IBM ร่วมกับแพลตฟอร์มผู้ให้บริการระบบความปลอดภัยไซเบอร์ของกระทรวงกลาโหมของสหราชอาณาจักร ที่มีการจำลองระบบ

นิเวศไซเบอร์ขึ้น เพื่อทดสอบความปลอดภัยและตั้งค่าระบบโครงสร้างการจัดเก็บข้อมูลให้มีความปลอดภัย (Leendert van Bochoven, 2022)

การรักษาความถูกต้องของข้อมูลปัญญาประดิษฐ์ ช่วยในการตรวจสอบและป้องกันการเปลี่ยนแปลงข้อมูลที่ไม่พึงประสงค์ เช่น การใช้ปัญญาประดิษฐ์ ในการตรวจสอบความถูกต้องของข้อมูลที่ถูกส่งผ่านเครือข่าย และการแจ้งเตือนเมื่อมีการพยายามแก้ไขข้อมูลโดยไม่ได้รับอนุญาต การเพิ่มความพร้อมใช้งาน ปัญญาประดิษฐ์ ช่วยในการตรวจสอบและป้องกันการโจมตีที่อาจทำให้ระบบไม่สามารถใช้งานได้ เช่น การใช้ปัญญาประดิษฐ์ ในการตรวจจับและป้องกันการโจมตีแบบ DDoS (Distributed Denial of Service) ที่อาจทำให้ระบบไม่สามารถให้บริการได้ ตัวอย่างเช่น กรณีความขัดแย้งระหว่างรัสเซียกับยูเครน ทำให้เกิดการโจมตีทางไซเบอร์และการโจมตีทางทหารระหว่างทั้งสองฝ่าย ในช่วงวันที่ 22-25 กุมภาพันธ์ 2565 มีการโจมตีทางไซเบอร์ในรูปแบบ DDoS ที่มุ่งเป้าไปยังเว็บไซต์ของหน่วยงานสำคัญระดับประเทศของยูเครน เช่น กระทรวงการต่างประเทศ กระทรวงสาธารณสุข และภาคธนาคาร การโจมตีเหล่านี้ทำให้หลายเว็บไซต์ไม่สามารถเข้าใช้งานได้ ส่งผลให้ระบบเครือข่ายอินเทอร์เน็ตล่ม (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2565)

อย่างไรก็ตาม การใช้ปัญญาประดิษฐ์ ในทางการทหารก็มีความเสี่ยงที่ต้องระมัดระวังเช่นกัน จากการเจาะระบบความปลอดภัยของข้อมูล โดยปัญญาประดิษฐ์ สามารถถูกใช้ในการโจมตีระบบความปลอดภัย เช่น ไวรัส Pegasus Spyware ที่ถูกใช้ในการสอดแนมและล้วงข้อมูลส่วนบุคคล โดย Pegasus เป็นสปายแวร์ที่พัฒนาโดย NSO Group ของอิสราเอล ซึ่งสามารถติดตั้งโดยไม่ต้องมีการกระทำใด ๆ จากผู้ใช้ และสามารถเข้าถึงข้อมูลที่สำคัญในอุปกรณ์ของผู้ใช้ได้ นอกจากนี้การใช้ปัญญาประดิษฐ์ ในการโจมตีไซเบอร์ อาจถูกใช้โดยฝ่ายตรงข้ามในการโจมตีไซเบอร์ที่ซับซ้อนและมีประสิทธิภาพมากขึ้น ทำให้การป้องกันและตอบสนองต่อภัยคุกคามยากขึ้น

4.4 ผลกระทบต่อความมั่นคงทางคลาวด์

การโจมตีทางไซเบอร์ต่าง ๆ มักจะมีการโจมตีผ่านทางระบบเซิร์ฟเวอร์ต่าง ๆ ที่เป็นโครงสร้างพื้นฐานดิจิทัล ของหน่วยงานรัฐต่าง ๆ ทำให้แนวคิดการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการรักษาความปลอดภัยจึงมียิ่งขึ้นในปัจจุบัน ตัวอย่างเช่น การตรวจจับและแก้ไขการตั้งค่าที่ผิดพลาด เนื่องจากการตั้งค่าที่ผิดพลาดบนคลาวด์เป็นหนึ่งในความเสี่ยงด้านความปลอดภัยที่ร้ายแรงที่สุด ปัญญาประดิษฐ์สามารถวิเคราะห์โครงสร้างพื้นฐานและระบบเพื่อค้นหาความ

ผิดปกติและการตั้งค่าผิดพลาด แล้วทำการแก้ไขได้อย่างรวดเร็วและมีประสิทธิภาพมากกว่ามนุษย์ ปัจจุบันปัญญาประดิษฐ์มักจะเสนอการเปลี่ยนแปลงนโยบายหรือการตั้งค่าให้ผู้ปฏิบัติงานเป็นผู้อนุมัติหรือปฏิเสธ แต่การใช้ปัญญาประดิษฐ์เพื่อแก้ไขปัญหาโดยอิสระยังคงเป็นเรื่องที่มีความท้าทายอยู่ในปัจจุบัน

ต่อมาคือการวิเคราะห์พฤติกรรมผู้ใช้ โดยสามารถประมวลผลข้อมูลขนาดใหญ่และระบุรูปแบบการเข้าถึงที่ผิดปกติที่มนุษย์อาจมองข้ามได้ ปัญญาประดิษฐ์จะช่วยให้ทีมรักษาความปลอดภัยเข้าใจพฤติกรรมผู้ใช้ในบริบทของสภาพแวดล้อมคลาวด์และแจ้งเตือนเมื่อพบการกระทำที่ผิดปกติผ่านสร้างนโยบายและการควบคุมความปลอดภัยที่ปรับตัวได้ และประเมินคะแนนความเสี่ยงสำหรับพฤติกรรมแต่ละอย่าง นอกจากนี้ยังช่วยในการตรวจจับและตอบสนองต่อภัยคุกคามช่วยทีมรักษาความปลอดภัยระบุมัลแวร์และภัยคุกคามไซเบอร์ที่กำลังดำเนินอยู่ได้เร็วและแม่นยำยิ่งขึ้นโดยการวิเคราะห์สภาพแวดล้อมแบบเรียลไทม์และอ้างอิงข้อมูลข่าวกรองภัยคุกคาม อย่างระบบ AI-based investigation copilots (Irei, 2024) กำลังช่วยทีมตอบสนองต่อภัยคุกคามโดยแนะนำมาตรการเชิงรุกตามรูปแบบกิจกรรม การพัฒนาเทคโนโลยีปัญญาประดิษฐ์ทางการทหารยังเปลี่ยนแปลงภูมิทัศน์ของภัยคุกคาม โดยมีการโจมตีที่ใช้ ปัญญาประดิษฐ์ ที่ซับซ้อนมากขึ้น ปัญญาประดิษฐ์จะถูกใช้ในการโจมตีและเทคนิคการหลบหลีกที่ปรับตัวได้อย่างสูง การป้องกันที่ใช้ปัญญาประดิษฐ์จึงเป็นสิ่งจำเป็นที่องค์กรต้องลงทุนและพัฒนาอย่างต่อเนื่องเพื่อรับมือกับภัยคุกคามใหม่ ๆ

4.5 ผลกระทบต่อความมั่นคงเชิงปฏิบัติการ

OPSEC มีความสำคัญในการปฏิบัติการทางทหารหลากหลายรูปแบบ เช่น การสงครามด้านบัญชาการและควบคุม (C2W) และการปฏิบัติการข่าวสาร (IO) โดยส่งผลกระทบต่อมาตรการรักษาความปลอดภัยต่าง ๆ เช่น การรักษาความปลอดภัยการติดต่อสื่อสาร (COMSEC), มาตรการต่อต้านข่าวกรอง, การรักษาความปลอดภัยข้อมูลข่าวสาร (INFOSEC), การรักษาความปลอดภัยสัญญาณ (SIGSEC) และการรักษาความปลอดภัยการรับ-ส่งสัญญาณ (TRANSEC) จึงเป็นสิ่งสำคัญที่ทหารต้องเข้าใจและสามารถประยุกต์ใช้ทฤษฎี OPSEC ในการปฏิบัติงานทั้งในภาวะปกติและภาวะสงคราม(นิวัติ เนียมพลอย, 2557) ตัวอย่างเช่น บริษัท Red Hat ที่มีความร่วมมือกับกระทรวงกลาวโหมของสหรัฐอเมริกา โดยได้มีการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ใน ปฏิบัติการหลายโดเมน (Multidomain Operations - MDO) มุ่งหมายที่จะผสานสินทรัพย์ต่างๆ ข้ามพื้นที่บก อากาศ ทะเล อวกาศ และไซเบอร์ เพื่อให้บรรลุความสามารถสูงสุดที่เรียกว่าการรวม

พลัง (convergence) ทำให้ศัตรูไม่สามารถตอบโต้ได้ทันที ความต้องการในการปฏิบัติการเหล่านี้มีลักษณะเด่น 5 ประการคือ:

ปริมาณ (Volume): การเพิ่มสินทรัพย์ในสนามรบทำให้ปริมาณข้อมูลจากผู้ผลิตและผู้บริโภคข้อมูลหลายรายเพิ่มขึ้น

ความหลากหลาย (Variety): สินทรัพย์จากโดเมนต่างๆ สร้างข้อมูลที่หลากหลายประเภท

ความเร็ว (Velocity): ความเร็วในการไหลของข้อมูลเพิ่มขึ้นเมื่อการรวมพลังถึงจุดสูงสุด มีข้อมูลถูกสร้างและบริโภคมากขึ้น

ความถูกต้อง (Veracity): ความถูกต้องของข้อมูล ความทันเวลา และความสามารถในการนำไปใช้ได้มีความสำคัญอย่างยิ่งในช่วงการรวมพลัง

คุณค่า (Value): คุณค่าของข้อมูลได้รับผลกระทบจากความถูกต้อง ปริมาณ และความเร็วของข้อมูลในจุดตัดสินใจ

ทำให้การเชื่อมโยงระบบต่าง ๆ ที่เป็นปัจจัยสำคัญสำหรับความสำเร็จในภารกิจใช้เวลาน้อยลง โครงสร้างเครือข่ายที่มีการเชื่อมโยงของระบบ ข้อมูล และอุปกรณ์ต่าง ๆ ซึ่งการไหลเวียนของข้อมูลนี้มีความสำคัญมากในการบรรลุความสำเร็จในภารกิจ ข้อมูลต้องถูกส่งต่อไปยังผู้ปฏิบัติงานในเวลาจริงและปรับตัวตามความต้องการและสถานที่ที่ต้องการใช้งาน ตัวอย่างเช่น สำหรับกลุ่มเรือบรรทุกเครื่องบิน ขอบระบบอาจหมายถึงยานพาหนะที่นำทหารไปยังฝั่ง เมื่อยานพาหนะเหล่านี้เข้าสู่สนามรบ ขอบระบบจะเคลื่อนที่ไปพร้อมกับแนวหน้าของทหาร และในอวกาศที่ฝ่ายตรงข้ามควบคุม ข้อมูลที่ถูกจับได้ที่ขอบระบบช่วยให้สามารถตัดสินใจได้ดีขึ้นและรวดเร็วขึ้น (Red Hat, 2023) ทำให้แนวคิดดังกล่าวถูกนำไปใช้ในอุตสาหกรรมธุรกิจและหน่วยงานรัฐมากยิ่งขึ้น เพื่อเพิ่มความปลอดภัยขององค์กรนั้น ๆ และเชื่อมโยงไปถึงการวางระบบประมวลผลความปลอดภัยของคลาวด์ที่มีความร่วมมือกับ IBM อีกด้วย

4.6 ผลกระทบต่อการฝึกอบรมผู้ใช้

กองทัพของสหรัฐอเมริกาได้มีการร่วมมือกับ IBM ในการสร้างการเรียนรู้แก่ทหารนับล้านนายเพื่อให้เข้าถึงการพัฒนาทักษะต่าง ๆ ต่างผ่านการสร้างแพลตฟอร์มการเรียนรู้แบบอัตโนมัติโดยมีนโยบายการศึกษาต่อเนื่อง เนื่องจากเป็นสิ่งสำคัญสำหรับการรักษาความพร้อมในทุกสาขาของกองทัพสหรัฐ ไม่ว่าจะเป็นกองทัพบก กองทัพเรือ กองทัพอากาศ หรือกองทัพอวกาศ จากการตามทันเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วไปจนถึงการขยายทักษะการคิดเชิงวิพากษ์ การ

ฝึกอบรมอย่างต่อเนื่องเป็นสิ่งที่จำเป็น และแก้ไขปัญหาที่ขัดขวางการศึกษาอย่างมีประสิทธิภาพ ด้วยการ การขยายการสนับสนุนถึงระดับล้านคน การปรับปรุงการศึกษาและการฝึกอบรมอย่างทันสมัยและมีประสิทธิภาพ ต่อมาคือการผสมผสาน HR และการฝึกอบรมในอินเทอร์เฟซเดียว หมายถึง การสร้างอินเทอร์เฟซที่รวมข้อมูลทั้งหมดให้สามารถดูและจัดการได้ในจอเดียว และการประยุกต์ใช้ปัญญาประดิษฐ์กับกระบวนการอัตโนมัติในระบบที่ซับซ้อน เพื่อจัดการกับระบบการเรียนรู้ที่ซับซ้อน (IBM, 2024a)

โดยเฉพาะการสงครามยุคใหม่มีความซับซ้อนมากขึ้น ทั้งจากอาวุธขั้นสูง สภาพแวดล้อมที่ยุ่งยาก อาชญากรรมไซเบอร์ และภัยคุกคามผสมผสาน ทำให้การฝึกอบรมทหารจำเป็นต้องมีมิติที่หลากหลายมากขึ้น ปัญญาประดิษฐ์ จึงเข้ามาสร้างตัวแทนอัตโนมัติที่มีพฤติกรรมอัจฉริยะได้หลากหลาย ช่วยจำลองสถานการณ์สงครามผสมผสานและปฏิสัมพันธ์กับพันธมิตร ข้าศึกและพลเรือนได้อย่างสมจริง จากการสร้างการจำลองที่ครอบคลุมกลยุทธ์สงครามผสมผสานและสภาพสังคมการเมืองที่หลากหลาย โดยพฤติกรรมจะไม่ซ้ำแบบเดิมในแต่ละครั้ง ช่วยฝึกทหารให้มีปฏิกิริยาตอบสนองที่คล่องแคล่วและไม่สามารถคาดเดาได้ เพื่อฝึกให้ทหารมีความคล่องแคล่วในการตัดสินใจอย่างรวดเร็วท่ามกลางสถานการณ์ที่ไม่แน่นอน ซึ่งเป็นทักษะสำคัญในการสู้รบ (Sentient Digital, 2024)

4.7 ผลกระทบต่อนโยบายความมั่นคงทางไซเบอร์

ผลกระทบจากการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการปฏิบัติการทางทหาร ได้ส่งผลอย่างมีนัยสำคัญต่อความมั่นคงทางไซเบอร์ของรัฐต่าง ๆ ทั่วโลก การเผชิญหน้ากับภัยคุกคามที่ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็วนี้ ทำให้รัฐจำเป็นต้องดำเนินมาตรการป้องกันที่เข้มแข็งและวางนโยบายเชิงรุกเพื่อปกป้องโครงสร้างพื้นฐานทางไซเบอร์ของตนเอง

โดยเฉพาะอย่างยิ่ง ประเทศมหาอำนาจ เช่น สหรัฐอเมริกาและจีน ตลอดจนประเทศมหาอำนาจในภูมิภาคอาเซียนอย่างสิงคโปร์ ได้ตระหนักถึงความสำคัญของการพัฒนานโยบายความมั่นคงทางไซเบอร์ที่ทันสมัยและมีประสิทธิภาพ เพื่อรับมือกับความท้าทายที่เกิดจากการใช้ปัญญาประดิษฐ์ในภาคทหาร ทั้งนี้ เพื่อรักษาความมั่นคงและเสถียรภาพของรัฐท่ามกลางภูมิทัศน์เทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว (ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, 2563, น.46-62) ดังต่อไปนี้

4.7.1 สหรัฐอเมริกา

สหรัฐฯ เป็นผู้นำทางเทคโนโลยีระดับโลกและมีนโยบายความมั่นคงทางไซเบอร์ที่ชัดเจนและเป็นระบบ การศึกษาแนวทางและกลยุทธ์ของสหรัฐฯ จะให้ภาพรวมที่ครอบคลุมเกี่ยวกับวิธีการใช้ปัญญาประดิษฐ์ในการเสริมสร้างความมั่นคงแห่งชาติ การประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการปฏิบัติการทางทหารของสหรัฐอเมริกาได้รับการสนับสนุนอย่างเต็มที่จากภาครัฐผ่านการวางนโยบายและกลยุทธ์ที่ชัดเจนในหลายด้าน ดังนี้

1. การสนับสนุนเชิงนโยบายจากภาครัฐ กระทรวงกลาโหมสหรัฐฯ ได้ประกาศยุทธศาสตร์ที่สาม (Third Offset Strategy) เพื่อพัฒนาขีดความสามารถของเหล่าทัพ โดยมุ่งเน้นการใช้ AI ในการเสริมสร้างศักยภาพและเพิ่มประสิทธิภาพในการปฏิบัติการทางทหาร ยุทธศาสตร์นี้มีเป้าหมายเพื่อสร้างความได้เปรียบเชิงเทคโนโลยีเหนือคู่แข่ง

2. การจัดการบุคลากรให้มีความชำนาญและองค์ความรู้ การเพิ่มทักษะปัญญาประดิษฐ์ให้กับบุคลากรในกองทัพอย่างต่อเนื่องเป็นสิ่งสำคัญ โดยมีการฝึกอบรมและการศึกษาเพื่อเพิ่มพูนความรู้และความชำนาญด้านปัญญาประดิษฐ์ในกลุ่มบุคลากรในกองทัพ

3. การวิจัยและพัฒนา สหรัฐฯ ให้การสนับสนุนการวิจัยและพัฒนาเทคโนโลยีปัญญาประดิษฐ์ อย่างเข้มข้นโดยหน่วยงานต่าง ๆ เช่น DARPA (Defense Advanced Research Projects Agency) เพื่อสร้างนวัตกรรมและความก้าวหน้าทางเทคโนโลยีที่สามารถนำมาใช้ในทางทหารได้อย่างมีประสิทธิภาพ

4. ความร่วมมือภาครัฐและเอกชน รัฐบาลสหรัฐฯ ส่งเสริมความร่วมมือระหว่างภาครัฐและบริษัทเอกชนชั้นนำ เช่น Google, IBM, และ Microsoft เพื่อเสริมสร้างความแข็งแกร่งในด้าน AI ความร่วมมือนี้ช่วยในการเร่งพัฒนานวัตกรรมและการนำปัญญาประดิษฐ์ไปใช้ในภาคทหารได้อย่างรวดเร็วและมีประสิทธิภาพ

5. โครงสร้างหรือหน่วยงานจัดการด้านข้อมูลและความปลอดภัยไซเบอร์ สหรัฐฯ ได้จัดตั้งหน่วยงานพิเศษด้านไซเบอร์ เช่น Cyber Command และ AI Task Force เพื่อจัดการกับภัยคุกคามทางไซเบอร์และพัฒนาขีดความสามารถทางเทคโนโลยี การจัดตั้งหน่วยงานเหล่านี้ช่วยให้สามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ

4.7.2 สาธารณรัฐประชาชนจีน

จีนเป็นประเทศที่กำลังเติบโตอย่างรวดเร็วในด้านเทคโนโลยี โดยเฉพาะในด้านปัญญาประดิษฐ์และความมั่นคงทางไซเบอร์ การศึกษาแนวทางของจีนจะให้ความเข้าใจถึงวิธีการที่ประเทศนี้ใช้ AI ในการเพิ่มขีดความสามารถทางทหารและแข่งขันกับประเทศอื่น ๆ จีนได้มีการ

ประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการปฏิบัติการทางทหารอย่างจริงจัง โดยได้รับการสนับสนุนจากภาครัฐและการพัฒนากลยุทธ์ต่าง ๆ ดังนี้

1. การสนับสนุนเชิงนโยบายจากภาครัฐ จีนได้ประกาศยุทธศาสตร์ปัญญาประดิษฐ์ (New Generation Artificial Intelligence Development Plan: AIDP) เพื่อความมั่นคงแห่งชาติและการเพิ่มขีดความสามารถในการแข่งขันกับสหรัฐอเมริกา ยุทธศาสตร์นี้มุ่งเน้นการพัฒนาและประยุกต์ใช้ AI ในหลายภาคส่วน รวมถึงภาคการทหาร

2. การจัดการบุคลากรให้มีความชำนาญและองค์ความรู้ การสร้างและพัฒนาบุคลากร AI อย่างเร่งด่วน โดยมุ่งเน้นการฝึกอบรมและการศึกษาที่เข้มข้น เพื่อสร้างผู้เชี่ยวชาญด้านปัญญาประดิษฐ์ ที่มีความสามารถในการปฏิบัติงานในภาคทหารและภาคส่วนอื่นๆ

3. การวิจัยและพัฒนา การลงทุนในการวิจัยและพัฒนาปัญญาประดิษฐ์อย่างกว้างขวางในทุกภาคส่วน รวมถึงภาคทหาร โดยมีการสนับสนุนจากภาครัฐและหน่วยงานที่เกี่ยวข้อง

4. ความร่วมมือภาครัฐและเอกชน การร่วมมือกับบริษัทเทคโนโลยีใหญ่ๆ เช่น Huawei และ Alibaba เพื่อพัฒนาเทคโนโลยีปัญญาประดิษฐ์และการประยุกต์ใช้ในภาคทหาร ความร่วมมือนี้ช่วยในการเร่งพัฒนานวัตกรรมและเทคโนโลยีที่ทันสมัย

5. โครงสร้างหรือหน่วยงานจัดการด้านข้อมูลและความปลอดภัยไซเบอร์ การจัดตั้งศูนย์วิจัยและพัฒนาด้านปัญญาประดิษฐ์และหน่วยงานพิเศษด้านไซเบอร์ เช่น Cybersecurity Bureau เพื่อจัดการกับภัยคุกคามทางไซเบอร์และพัฒนาขีดความสามารถทางเทคโนโลยี การจัดตั้งหน่วยงานเหล่านี้ช่วยให้สามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ

4.7.3 สาธารณรัฐสิงคโปร์

สิงคโปร์เป็นศูนย์กลางเทคโนโลยีในภูมิภาคเอเชียตะวันออกเฉียงใต้ และมีนโยบายความมั่นคงทางไซเบอร์ที่เน้นการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ การศึกษาแนวทางของสิงคโปร์จะช่วยให้เห็นภาพการประยุกต์ใช้ AI ในการเสริมสร้างความปลอดภัยและความมั่นคงในระดับภูมิภาค โดยสิงคโปร์มีการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการปฏิบัติการทางทหารอย่างมีระบบและได้รับการสนับสนุนจากภาครัฐในหลายด้าน ดังนี้

1. การสนับสนุนเชิงนโยบายจากภาครัฐ สิงคโปร์ได้ประกาศยุทธศาสตร์ปัญญาประดิษฐ์ห่งชาติ (National Artificial Intelligence Strategy) และยุทธศาสตร์ป้องกันดิจิทัล (Digital Defence) ภายใต้ Total Defence เพื่อความมั่นคงของชาติและการป้องกันภัยคุกคาม

ทางไซเบอร์ ยุทธศาสตร์เหล่านี้มุ่งเน้นการพัฒนาและประยุกต์ใช้ปัญญาประดิษฐ์ในหลายภาคส่วน รวมถึงภาคการทหาร

2. การจัดการบุคลากรให้มีความชำนาญและองค์ความรู้ การฝึกอบรมบุคลากรและการนำเข้าผู้เชี่ยวชาญจากต่างประเทศ เพื่อเสริมสร้างความรู้และทักษะด้านปัญญาประดิษฐ์ในกลุ่มบุคลากรในกองทัพและภาคส่วนอื่นๆ

3. การวิจัยและพัฒนา การวิจัยและพัฒนาปัญญาประดิษฐ์โดยมีความร่วมมือกับสถาบันการศึกษาและบริษัทเอกชน การวิจัยนี้มุ่งเน้นการสร้างนวัตกรรมและเทคโนโลยีที่ทันสมัยเพื่อนำมาใช้ในทางทหารและภาคส่วนอื่นๆ

4. ความร่วมมือภาครัฐและเอกชน การร่วมมือกับบริษัทเทคโนโลยีระดับโลก เช่น Google และ Microsoft เพื่อพัฒนาเทคโนโลยีปัญญาประดิษฐ์และการประยุกต์ใช้ในภาคทหาร ความร่วมมือนี้ช่วยในการเร่งพัฒนานวัตกรรมและการนำปัญญาประดิษฐ์ไปใช้ในภาคทหารได้อย่างรวดเร็วและมีประสิทธิภาพ

5. โครงสร้างหรือหน่วยงานจัดการด้านข้อมูลและความปลอดภัยไซเบอร์ การจัดตั้งหน่วยงานพิเศษด้านไซเบอร์และการพัฒนาความปลอดภัยทางไซเบอร์เชิงลึก เช่น Defence Cyber Group เพื่อจัดการกับภัยคุกคามทางไซเบอร์และพัฒนาขีดความสามารถทางเทคโนโลยี การจัดตั้งหน่วยงานเหล่านี้ช่วยให้สามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ

จากการศึกษาแนวทางการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการปฏิบัติการทางทหารของสหรัฐอเมริกา จีน และสิงคโปร์ พบว่าแต่ละประเทศให้ความสำคัญกับการพัฒนาเทคโนโลยีและนวัตกรรมในด้านปัญญาประดิษฐ์อย่างจริงจัง โดยมีแนวทางที่คล้ายคลึงกันในหลายประเด็น ไม่ว่าจะเป็นการสนับสนุนเชิงนโยบายจากภาครัฐ การพัฒนาบุคลากร การวิจัยและพัฒนา ความร่วมมือระหว่างภาครัฐและเอกชน รวมถึงการจัดตั้งหน่วยงานเฉพาะทางด้านไซเบอร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์

สหรัฐอเมริกาเน้นการสร้างความได้เปรียบเชิงเทคโนโลยีเหนือคู่แข่งผ่านนโยบายยุทธศาสตร์ที่สาม (Third Offset Strategy) และการวิจัยโดยหน่วยงานต่าง ๆ เช่น DARPA ในขณะที่จีนใช้ยุทธศาสตร์ปัญญาประดิษฐ์แห่งชาติ (AIDP) เพื่อพัฒนาขีดความสามารถและแข่งขันกับสหรัฐฯ และเมื่อมองย้อนกลับมาที่สิงคโปร์นั้น ได้มีการมุ่งเน้นยุทธศาสตร์ป้องกันดิจิทัล (Digital Defence) เพื่อความมั่นคงของชาติและการป้องกันภัยคุกคามทางไซเบอร์

การพัฒนาและการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในภาคการทหารของทั้งสามประเทศแสดงให้เห็นถึงความสำคัญของการสนับสนุนจากภาครัฐ การพัฒนาบุคลากร การวิจัยและพัฒนา ความร่วมมือระหว่างภาครัฐและเอกชน และการจัดตั้งหน่วยงานด้านความปลอดภัยไซเบอร์ ประโยชน์ที่ได้รวมถึงการเสริมสร้างความมั่นคงและความปลอดภัย การเพิ่มประสิทธิภาพในการปฏิบัติการทางทหาร การสร้างนวัตกรรมและการพัฒนาทางเทคโนโลยี ความร่วมมือและการแลกเปลี่ยนความรู้ และการพัฒนาบุคลากร

จากมุมมองนี้ ทำให้เห็นว่า การนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในภาคการทหารเป็นสิ่งที่หลีกเลี่ยงไม่ได้และมีความจำเป็นอย่างยิ่งต่อความมั่นคงของชาติและความก้าวหน้าทางเทคโนโลยีในอนาคต นอกจากนี้ยังเป็นการเตรียมความพร้อมเพื่อรับมือกับความท้าทายและภัยคุกคามในยุคดิจิทัลที่เพิ่มขึ้นอย่างรวดเร็วขึ้นอีกด้วย

บทที่ 5
สรุป อภิปรายผล และข้อเสนอแนะ

ในการวิจัยเรื่องผลกระทบจากการใช้ปัญญาประดิษฐ์ทางทหารต่อความมั่นคงทางไซเบอร์ ผู้วิจัยได้ทำการประเมินผลกระทบและประสิทธิภาพของการใช้เทคโนโลยีปัญญาประดิษฐ์ในด้านต่าง ๆ โดยการประเมินผลการใช้งานปัญญาประดิษฐ์ในทางการทหารเพื่อให้ทราบถึงผลกระทบทั้งในเชิงบวกและเชิงลบ สามารถสรุปผลการดำเนินงาน โดยแบ่งหัวข้อในการสรุปผลได้ดังต่อไปนี้

1 สรุปผลการวิจัย

2 อภิปรายผลการวิจัย

3 ข้อเสนอแนะ

5.1 สรุปผลการวิจัย

ในการศึกษาผลกระทบจากการใช้ปัญญาประดิษฐ์ในทางการทหารต่อความมั่นคงทางไซเบอร์ได้พบว่าการพัฒนาและการนำปัญญาประดิษฐ์มาใช้ในทางการทหารนั้นมีผลกระทบทั้งในด้านบวกและด้านลบ โดยในด้านบวก ปัญญาประดิษฐ์สามารถเพิ่มประสิทธิภาพในการตรวจจับและตอบโต้ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม ในด้านลบ ปัญญาประดิษฐ์ก็สามารถถูกใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์ที่มีประสิทธิภาพมากขึ้นเช่นกัน ดังนั้นรัฐต่าง ๆ จึงควรให้ความสำคัญกับความมั่นคงทางไซเบอร์โดยการนำปัญญาประดิษฐ์ทางการทหารมาปรับใช้ ดังจะเห็นได้จากการที่ประเทศมหาอำนาจอย่างสหรัฐอเมริกา จีนและสิงคโปร์ ได้มีการให้ความสำคัญกับการสนับสนุนและพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ของประเทศ

5.2 อภิปรายผลการวิจัย

การวิจัยนี้ได้ศึกษาผลกระทบของการใช้ปัญญาประดิษฐ์ (AI) ต่อความมั่นคงในหลายด้าน โดยมีทั้งผลกระทบเชิงบวกและเชิงลบที่ต้องพิจารณาอย่างรอบคอบ ผลการวิจัยสรุปได้ดังนี้

เริ่มจากการศึกษาพัฒนาเทคโนโลยีปัญญาประดิษฐ์ทางการทหารที่ใช้ในความมั่นคงทางไซเบอร์ เทคโนโลยีปัญญาประดิษฐ์ได้มีการเริ่มใช้จากฐานความรู้ที่มีอยู่ดั้งเดิม ซึ่งยังคงต้องอาศัยข้อมูลที่มีมาก่อน หรือที่เรียกว่า ระบบผู้เชี่ยวชาญ (Expert Systems) ซึ่งเป็นการตรวจสอบ

การรับส่งข้อมูลเครือข่าย กิจกรรมของระบบ และพฤติกรรมผู้ใช้ เปรียบเทียบกับลายเซ็นหรือลักษณะของภัยคุกคามที่รู้จัก ดังนั้นเมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น หากไม่เป็นที่รู้จัก ก็ยังสามารถถูกโจมตีได้อยู่ ก่อนที่จะมีการเปลี่ยนถ่ายมายังยุคสมัยการเรียนรู้ของเครื่อง (Machine Learning) ซึ่ง สามารถทำงานและจดจำรูปแบบการโจมตีได้มากยิ่งขึ้น เนื่องจากสามารถตรวจจับความเบี่ยงเบนหรือความผิดปกติที่อาจบ่งบอกถึงภัยคุกคามถึงแม้จะไม่ได้รู้จักกันมาก่อนก็ตาม ซึ่งเป็นส่วนหนึ่งในการต่อยอดเมื่อเข้าสู่ยุคการเรียนรู้เชิงลึก (Deep Learning) ที่มีความสามารถตรวจจับภัยคุกคามได้ในเวลาจริงรวมไปถึงกลไกการตอบสนองอัตโนมัติและสามารถทำงานกับผู้เชี่ยวชาญได้อย่างต่อเนื่อง เนื่องจากสามารถสื่อสารได้ด้วยภาษาธรรมชาติ จึงสามารถทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ประเด็นถัดมาคือ การศึกษาการโจมตีทางไซเบอร์โดยเทคโนโลยีปัญญาประดิษฐ์ทางการทหาร พบว่า โจมตีทางไซเบอร์โดยเทคโนโลยีปัญญาประดิษฐ์ทางการทหารนั้นในส่วนมากยังคงอาศัยการประมวลผลโดยใช้โมเดลภาษาขนาดใหญ่ (Large Language Model: LLM) เพื่อใช้ในการวิจัยบริษัทและเครื่องมือด้านความปลอดภัยไซเบอร์ แปลเอกสารทางเทคนิค ค้นหาข้อมูล หน่วยงานข่าวกรอง ช่วยเขียนโค้ด และวิจัยวิธีซ่อนจากการตรวจจับไวรัสและข้อมูลของระบบโดยเทคโนโลยีปัญญาประดิษฐ์ นอกจากนี้แล้วยังมีการใช้ปัญญาประดิษฐ์ในการสังเคราะห์ข้อมูลขึ้นจากเทคโนโลยี Generative AI เพื่อสร้างภาพ เสียง เนื้อหาข้อความ โดยนำไปใช้งานเพื่อวัตถุประสงค์ทางการเมือง ซึ่งสามารถแบ่งกลุ่มเป้าหมายการโจมตีได้ออกเป็น 8 ประเภท คือ รัฐบาลและหน่วยงานรัฐ องค์กรวิจัยและกลุ่มคนที่ทำงานเกี่ยวกับการวิจัย (Think tank) องค์กรที่ไม่ใช่ภาครัฐและกลุ่มสิทธิมนุษยชน สถาบันการศึกษาและวิชาการ บริษัทผู้ให้บริการด้าน IT อุตสาหกรรมการป้องกันประเทศและผู้รับเหมาผลิตอาวุธ และสื่อมวลชน ซึ่งหมายความว่า ทั้งองค์กรภาครัฐและเอกชน ต่างก็สามารถเป็นเป้าหมายของการโจมตีทางไซเบอร์ได้เช่นกัน

และประเด็นสุดท้ายคือ การศึกษาผลกระทบความมั่นคงทางไซเบอร์ที่เกิดจากการใช้เทคโนโลยีปัญญาประดิษฐ์ เริ่มจาก ในด้านความมั่นคงทางเครือข่าย การใช้ปัญญาประดิษฐ์ช่วยเพิ่มความสามารถในการตรวจจับการโจมตีและการบุกรุกเครือข่ายได้อย่างแม่นยำ รวดเร็ว และมีประสิทธิภาพมากขึ้น โดยปัญญาประดิษฐ์สามารถวิเคราะห์ข้อมูลจำนวนมากและซับซ้อนได้แบบเรียลไทม์ ทำให้สามารถตอบสนองต่อภัยคุกคามได้ทันที อย่างไรก็ตาม ในขณะเดียวกันปัญญาประดิษฐ์เองก็สามารถถูกใช้เพื่อวิเคราะห์และเจาะช่องโหว่ของระบบเครือข่าย ทำให้การโจมตีมีประสิทธิภาพและยากต่อการป้องกัน การพัฒนาการป้องกันจึงต้องควบคู่ไปกับการเฝ้าระวังช่องโหว่ที่อาจถูกโจมตีได้

ในด้าน ความมั่นคงทางแอปพลิเคชัน ปัญญาประดิษฐ์ช่วยเพิ่มความปลอดภัยของแอปพลิเคชันโดยการตรวจสอบและป้องกันการบุกรุกแบบเรียลไทม์หรือการประมวลผลแบบทันที การใช้ปัญญาประดิษฐ์ในการตรวจสอบพฤติกรรมที่ผิดปกติและตอบสนองต่อการโจมตีช่วยลดความเสี่ยงในการถูกโจมตี อย่างไรก็ตาม หากปัญญาประดิษฐ์ถูกแฮกเกอร์นำมาใช้ในการโจมตี แอปพลิเคชันต่างๆ จะตกเป็นเป้าหมายที่มีความเสี่ยงสูง การป้องกันจึงต้องรวมถึงการเฝ้าระวังและป้องกันการใช้ปัญญาประดิษฐ์ในการโจมตีด้วย

เมื่อพิจารณาถึง ความมั่นคงของข้อมูล ปัญญาประดิษฐ์สามารถปกป้องข้อมูลสำคัญจากการเข้าถึงโดยไม่ได้รับอนุญาตและการโจมตีที่ซับซ้อน โดยการเข้ารหัสข้อมูลและการตรวจสอบการเข้าถึงอย่างละเอียด แต่ในทางกลับกัน ปัญญาประดิษฐ์ก็สามารถถูกใช้ในการขโมยและเปิดเผยข้อมูลสำคัญได้อย่างมีประสิทธิภาพ ดังนั้น การป้องกันต้องมีมาตรการที่ครอบคลุมและทันสมัยเพื่อต่อสู้กับการโจมตีที่ใช้ปัญญาประดิษฐ์

สำหรับ ความมั่นคงเชิงปฏิบัติการ ปัญญาประดิษฐ์ช่วยปรับปรุงกระบวนการและการตัดสินใจในองค์กรทางทหาร เพิ่มความแม่นยำและลดเวลาในการดำเนินงาน ทำให้องค์กรสามารถปฏิบัติการได้อย่างมีประสิทธิภาพมากขึ้น อย่างไรก็ตาม การโจมตีที่ใช้ปัญญาประดิษฐ์สามารถทำลายกระบวนการและสร้างความเสียหายอย่างใหญ่หลวงต่อการปฏิบัติการ จึงต้องมีการพัฒนาระบบป้องกันที่สามารถตอบสนองต่อการโจมตีที่ซับซ้อน

ในส่วนของ ความมั่นคงบนคลาวด์ การใช้ปัญญาประดิษฐ์ในการจัดการและปกป้องข้อมูลบนคลาวด์ช่วยเพิ่มความปลอดภัยและลดความเสี่ยงจากการโจมตี การใช้ปัญญาประดิษฐ์ในการตรวจสอบและตอบสนองต่อภัยคุกคามบนคลาวด์ทำให้ระบบปลอดภัยยิ่งขึ้น อย่างไรก็ตาม ปัญญาประดิษฐ์เองก็สามารถถูกใช้เพื่อเจาะระบบคลาวด์และขโมยข้อมูลสำคัญได้เช่นกัน ดังนั้นต้องมีการป้องกันที่มีประสิทธิภาพและอัปเดตอย่างต่อเนื่อง

และสุดท้ายในส่วนของการ ฝึกอบรมผู้ใช้ ปัญญาประดิษฐ์ช่วยในการฝึกอบรมและเพิ่มความรู้ให้กับผู้ใช้ในการป้องกันภัยคุกคามทางไซเบอร์ การใช้ปัญญาประดิษฐ์ในการจำลองสถานการณ์และการสอนช่วยให้ผู้ใช้มีความพร้อมในการป้องกันและตอบสนองต่อภัยคุกคาม อย่างไรก็ตาม หากปัญญาประดิษฐ์ถูกใช้ในการเผยแพร่ข้อมูลผิดๆ หรือการหลอกลวง ผู้ใช้จะเกิดความเข้าใจผิดและเพิ่มความเสี่ยงในการปฏิบัติงาน การฝึกอบรมจึงต้องมีการตรวจสอบและยืนยันข้อมูลที่ถูกต้อง

จากผลกระทบต่อความมั่นคงทางไซเบอร์ในด้านต่าง ๆ นั้น ได้สอดคล้องกับสมมุติฐานของวิจัยว่ารัฐต่าง ๆ ควรที่จะให้ความสำคัญในการพัฒนาโครงสร้างพื้นฐานทางดิจิตอล เนื่องจาก

การประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการปฏิบัติการทางทหารได้ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงทางไซเบอร์ของประเทศต่างๆ ทั่วโลก จากการศึกษาวิเคราะห์และเปรียบเทียบนโยบายด้านปัญญาประดิษฐ์และความมั่นคงทางไซเบอร์ของสามประเทศที่สำคัญ ได้แก่ สหรัฐอเมริกา จีน และสิงคโปร์ ซึ่งแสดงให้เห็นถึงแนวทางที่แตกต่างกันในการรับมือกับความท้าทายนี้พบว่า

ทั้งสามประเทศมีจุดร่วมที่สำคัญคือการให้การสนับสนุนเชิงนโยบายจากภาครัฐอย่างชัดเจน โดยมีการประกาศยุทธศาสตร์ระดับชาติเพื่อส่งเสริมการพัฒนาและการใช้งานปัญญาประดิษฐ์ในภาคการทหาร นอกจากนี้ ยังมีการลงทุนอย่างมากในการวิจัยและพัฒนา การสร้างความร่วมมือระหว่างภาครัฐและเอกชน ตลอดจนการพัฒนาบุคลากรให้มีความเชี่ยวชาญด้านปัญญาประดิษฐ์และความมั่นคงทางไซเบอร์ อย่างไรก็ตาม แต่ละประเทศมีจุดเน้นที่แตกต่างกัน สหรัฐอเมริกามุ่งเน้นการสร้างความได้เปรียบเชิงเทคโนโลยีเหนือคู่แข่ง ในขณะที่จีนพยายามพัฒนาปัญญาประดิษฐ์เพื่อแข่งขันกับสหรัฐอเมริกาโดยตรง ส่วนสิงคโปร์ให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์และการพัฒนาขีดความสามารถทางดิจิทัลของประเทศ

ผลลัพธ์ที่ได้จากการดำเนินนโยบายเหล่านี้มีหลายประการ ได้แก่ การเสริมสร้างความมั่นคงและความปลอดภัยของประเทศ การเพิ่มประสิทธิภาพในการปฏิบัติการทางทหาร การสร้างนวัตกรรมและการพัฒนาเทคโนโลยีใหม่ ๆ รวมถึงการส่งเสริมความร่วมมือและการแลกเปลี่ยนความรู้ระหว่างภาคส่วนต่าง ๆ นอกจากนี้ ยังช่วยพัฒนาทักษะและความเชี่ยวชาญของบุคลากรในด้านปัญญาประดิษฐ์และความมั่นคงทางไซเบอร์

การศึกษานี้ชี้ให้เห็นว่าการแข่งขันด้านปัญญาประดิษฐ์ระหว่างประเทศมหาอำนาจอาจนำไปสู่การพัฒนาเทคโนโลยีที่รวดเร็วยิ่งขึ้น แต่ในขณะเดียวกันก็เผยให้เห็นถึงความสำคัญของการสร้างสมดุลระหว่างการพัฒนาเทคโนโลยีและการรักษาความปลอดภัยทางไซเบอร์ นอกจากนี้ยังมีความท้าทายในการกำกับดูแลการใช้ปัญญาประดิษฐ์ในภาคทหารและผลกระทบทางจริยธรรมที่อาจเกิดขึ้น

สรุปได้ว่า การพัฒนานโยบายด้านปัญญาประดิษฐ์ และความมั่นคงทางไซเบอร์ที่ครอบคลุมและยืดหยุ่นมีความสำคัญอย่างยิ่งในการรับมือกับการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว และประเทศต่างๆ ควรพิจารณาการสร้างความร่วมมือระหว่างประเทศเพื่อจัดการกับภัยคุกคามร่วมกัน ทั้งนี้ เพื่อรักษาความมั่นคงและเสถียรภาพในยุคที่ปัญญาประดิษฐ์มีบทบาทสำคัญในการปฏิบัติการทางทหารและความมั่นคงของชาติ

การวิจัยนี้ชี้ให้เห็นว่า แม้ปัญญาประดิษฐ์จะมีประโยชน์มากมายในการเพิ่มความมั่นคงของระบบต่างๆ แต่ก็มีความเสี่ยงที่ต้องระมัดระวังในแต่ละด้าน ซึ่งมีความสอดคล้องกับองค์ประดิบของความมั่นคงทางไซเบอร์ตามทฤษฎีความมั่นคงทางไซเบอร์ การวิจัยนี้ยังสนับสนุนผลการวิจัยของ Yamin et al., (2021) ที่พบว่าปัญญาประดิษฐ์ สามารถนำมาใช้ในการตรวจจับและวิเคราะห์ข้อมูลปริมาณมากได้อย่างรวดเร็วและมีประสิทธิภาพ และยังสอดคล้องกับงานวิจัยของ Lehto (2015) ที่แบ่งระดับของภัยคุกคามตามแรงจูงใจ การใช้ปัญญาประดิษฐ์ ในการวิเคราะห์และประเมินภัยคุกคามในระดับต่าง ๆ ช่วยให้เข้าใจถึงผลกระทบและความเสี่ยงที่อาจเกิดขึ้นจากการนำปัญญาประดิษฐ์ มาใช้ในทางการทหาร

ผลการวิจัยนี้ยังพบว่าการพัฒนาปัญญาประดิษฐ์ทางการทหารนั้นได้ส่งผลต่อความมั่นคงทางไซเบอร์ ที่เป็นหนึ่งในประเด็นที่รัฐควรให้ความสำคัญในการศึกษาและนำมาใช้ในการออกแบบนโยบายเพื่อสร้างความมั่นคงทางไซเบอร์และป้องกันภัยคุกคาม เห็นได้จากประเทศมหาอำนาจที่ได้มีการวางรากฐานนโยบายเกี่ยวกับประเด็นความมั่นคงนี้ ซึ่งสอดคล้องกับงานวิจัยของ ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ (2563) ที่ได้ศึกษาแนวทางการพัฒนาเทคโนโลยีปัญญาประดิษฐ์ต่อกองทัพไทยและการพัฒนานโยบายที่เกี่ยวข้องกับทางไซเบอร์ของประเทศสหรัฐอเมริกา สาธารณรัฐจีนและสาธารณรัฐสิงคโปร์ ด้วยเช่นกัน

5.3 ข้อเสนอแนะเชิงนโยบาย

จากการศึกษาพบว่าการใช้ปัญญาประดิษฐ์สามารถช่วยเพิ่มความปลอดภัยทางไซเบอร์ได้อย่างมาก แต่ก็มีความเสี่ยงที่ต้องระวังเช่นกัน ดังนั้น ข้อเสนอแนะสำหรับการเพิ่มความมั่นคงทางไซเบอร์ของไทยจึงมีดังนี้

ประการแรก ประเทศไทยควรสนับสนุนการวิจัยและพัฒนาปัญญาประดิษฐ์เพื่อช่วยตรวจจับและป้องกันการโจมตีทางไซเบอร์ เช่น การพัฒนาระบบไฟร์วอลล์และระบบป้องกันการบุกรุกที่สามารถทำงานได้อย่างรวดเร็วและแม่นยำ

ประการที่สอง ควรมีระบบเฝ้าระวังที่สามารถตรวจสอบพฤติกรรมที่ผิดปกติและตอบสนองต่อการโจมตีได้ทันที ซึ่งจะช่วยป้องกันข้อมูลสำคัญไม่ให้ถูกขโมยหรือนำไปใช้ในทางที่ผิด

ประการที่สาม การฝึกอบรมและเพิ่มความรู้ให้กับบุคลากรทุกระดับเกี่ยวกับภัยคุกคามทางไซเบอร์และการใช้ปัญญาประดิษฐ์ในการป้องกันภัยคุกคามเป็นสิ่งจำเป็น การฝึกอบรมนี้จะช่วยให้บุคลากรพร้อมรับมือกับภัยคุกคามที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

ประการที่สี่ ควรปรับปรุงกฎหมายและนโยบายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ให้ทันสมัยและสอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี เพื่อสนับสนุนการใช้ปัญญาประดิษฐ์ในการป้องกันภัยคุกคาม

สุดท้ายนี้ การสร้างความร่วมมือระหว่างภาครัฐและเอกชน รวมถึงความร่วมมือกับประเทศอื่นๆ เป็นสิ่งสำคัญในการแลกเปลี่ยนข้อมูลและเทคโนโลยีเพื่อรับมือกับภัยคุกคามทางไซเบอร์ การทำงานร่วมกันนี้จะช่วยเสริมสร้างความปลอดภัยทางไซเบอร์ในระดับสากล

การนำข้อเสนอแนะเหล่านี้มาปรับใช้จะช่วยให้ประเทศไทยมีความพร้อมและมีประสิทธิภาพในการรับมือกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็วในอนาคต ทั้งยังช่วยเสริมสร้างความมั่นคงปลอดภัยให้กับระบบและข้อมูลสำคัญของประเทศ

5.4 ข้อเสนอแนะสำหรับการวิจัยในอนาคต

ควรมีการศึกษาถึงผลกระทบของปัญญาประดิษฐ์ ต่อความมั่นคงทางไซเบอร์ในบริบทของประเทศไทยเพิ่มเติม เพื่อให้มีความเข้าใจและสามารถพัฒนานโยบายที่เหมาะสมในการป้องกันภัยคุกคามทางไซเบอร์ในระดับชาติ

บรรณานุกรม

Anyoha, R. (2017). The History of Artificial Intelligence. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Apportugal. (2024). *The latest example of AI's evolving role, the Pegasus spyware, and what a 'retweet' and a 'quote tweet' are*. https://blog.apportugal.com/en/the-latest-example-of-ais-evolving-role-the-pegasus-spyware-and-what-a-retweet-and-a-quote-tweet-is

Artit Sagoolmuang, Ananwat Tippawat, & Papoj Thamjaroenporn. (2023). สร้าง *AI* เข้าใจภาษามนุษย์ด้วย *Natural Language Processing*. Big Data Institute (Public Organization). https://bdi.or.th/big-data-101/what-is-natural-language-processing/

Browne, R. (2024, April 8). *State-backed cyberattacks, AI deepfakes, and more: Experts reveal UK election cyber threats*. https://www.cnbc.com/2024/04/08/state-backed-cyberattacks-ai-deepfakes-top-uk-election-cyber-risks.html

Department of Justice. (2024). *U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure* https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

Ertan, A. (2022). *Exploring the Security Implications of Artificial Intelligence in Military Contexts* [Doctoral Thesis].

Field, H. (2024, 2024/01/17). OpenAI quietly removes ban on military use of its AI tools. *CNBC*. https://www.cnbc.com/2024/01/16/openai-quietly-removes-ban-on-military-use-of-its-ai-tools.html

Fortinet. (2024, May 26). *What Is Network Security?* https://www.fortinet.com/resources/cyberglossary/what-is-network-security

Government Digital Service. (2024, May 24). *Defence Artificial Intelligence Centre*. https://www.gov.uk/government/groups/defence-artificial-intelligence-centre

IBM. (2024a). *Modernizing US Armed Forces' training with the IBM Learning Platform*. https://www.ibm.com/industries/government/defense-

intelligence/resources/interactive/pages/data-centric.html

IBM. (2024b). *What is artificial intelligence (AI)?* https://www.ibm.com/topics/artificial-intelligence

Irei, A. (2024, April 25). *3 ways AI is transforming cloud security, according to experts*. https://www.techtarget.com/searchsecurity/tip/Ways-AI-is-transforming-cloud-security-according-to-experts

Johnson, D. B. (2024, April 5). *Chinese hackers turn to AI to meddle in elections*. CyberScoop. https://cyberscoop.com/microsoft-ai-election-taiwan/

Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, *6*, 2024ss0219. https://doi.org/10.31893/multiscience.2024ss0219

Leendert van Bochoven, C. N., Mike Raker. (2022, August 15). *IBM and Improbable in partnership to deliver a new technology edge*. IBM. https://www.ibm.com/blogs/think/uk-en/ibm-and-improbable-in-partnership-to-deliver-a-new-technology-edge/

Lehto, M. (2015). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. *International Journal of Cyber Warfare and Terrorism*, *3*(3), 1-18. https://doi.org/10.4018/ijcwt.2013070101

Microsoft. (2022). Microsoft Threat Modeling Tool threats. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Microsoft. (2024a). Crimson Sandstorm. https://www.microsoft.com/en-us/security/security-insider/crimson-sandstorm

Microsoft. (2024b). Digital Threats from East Asia Increase in Breadth and Effectiveness. https://www.microsoft.com/en-us/security/business/security-insider/reports/nation-state-reports/digital-threats-from-east-asia-increase-in-breadth-and-effectiveness/

Microsoft. (2024c). Forest Blizzard. https://www.microsoft.com/en-us/security/security-insider/forest-blizzard

OpenAI. (2024). Disrupting Malicious Uses of AI by State-Affiliated Threat Actors. https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-

actors/

Piasak, A. (2023). Claude AI. https://data-espresso.com/claude-ai/

Red Hat. (2023). *Mission Edge: How Red Hat can help the DoD accelerate mission outcomes*. https://www.redhat.com/en/solutions/public-sector/dod

Russell, S., & Norvig, P. (2016). *Artificial Intelligence: A Modern Approach*. Pearson. https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf

Sentient Digital. (2024). *MILITARY TRAINING SIMULATION SOFTWARE: ARTIFICIAL INTELLIGENCE FOR ARMED SERVICEMEMBERS*. https://sdi.ai/blog/military-training-simulation-software-ai/

Sipola, T., Kokkonen, T., & Karjalainen, M. (2023). *Artificial Intelligence and Cybersecurity: Theory and Applications*. Springer. https://doi.org/10.1007/978-3-031-15030-2

Szabadföldi, I. (2021). Artificial Intelligence in Military Application – Opportunities and Challenges. *Land Forces Academy Review*, *26*, 157-165. https://doi.org/10.2478/raft-2021-0022

Thairath. (2024). *ChatGPT* คืออะไร ทำอะไรได้บ้าง แนะนำวิธีใช้งาน *ChatGPT* ง่ายๆ ที่นี่. https://www.thairath.co.th/lifestyle/tech/2729975

Turing, A. M. (1950). I.—COMPUTING MACHINERY AND INTELLIGENCE. *Mind*, *LIX*(236), 433-460. https://doi.org/10.1093/mind/LIX.236.433

VC3. (2023). The Evolution Of Artificial Intelligence In Cybersecurity. https://www.vc3.com/blog/the-evolution-of-artificial-intelligence-in-cybersecurity

Vicens, A. (2024, January 9). *Ai is helping us spies catch stealthy Chinese hacking ops, NSA official says*. CyberScoop. https://cyberscoop.com/ai-china-hacking-operations/

Vmware. (2024). *What is application security?* https://www.vmware.com/topics/glossary/content/application-security.html

Winder, D. (2024, April 25). *State-sponsored attackers backdoor Cisco firewalls to hack into government networks*. TechFinitive. https://www.techfinitive.com/state-sponsored-attackers-backdoor-cisco-firewalls-to-hack-into-government-networks/

Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks.

Journal of Information Security and Applications, *57*, 102722. https://doi.org/10.1016/j.jisa.2020.102722

ไทยพีบีเอส. (2561, 31 พฤษภาคม). ย้อนวิวัฒนาการในรอบ *75* ปี ปัญญาประดิษฐ์. https://www.thaipbs.or.th/news/content/272538

ธนาคารกรุงเทพ. (2566). เมื่อ ‘เอไอ’ ยังไม่หยุดเปลี่ยนโลก ธุรกิจไหนปรับตัวไม่ทัน ระวัง! ถูกทิ้งไว้ข้างหลัง. https://bangkokbanksme.com/en/23-2sme1-ai-has-not-stopped-changing-the-world

นิวัติ เนียมพลอย. (2557). การรักษาความปลอดภัยในการปฏิบัติการ (*Operations Security)*. https://nniwat.wordpress.com/2014/05/30/การรักษาความปลอดภัยในก

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. (2563). ปัญญาประดิษฐ์ (*Artificial Intelligence: AI)* กับจุดเปลี่ยนของสงครามในอนาคต (พิมพ์ครั้งที่ 1.). ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. https://ssccthailand.org/uploads_ssc/research_20201125160627676744051 6.pdf

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2565). แผนปฏิบัติการประจำปีงบประมาณ พ.ศ. *2566*. https://drive.ncsa.or.th/s/JwPmxYwRnJJwmTc

ประวัติผู้เขียน