แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) และ AGI เพื่อเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพอากาศไทย

Integrating Artificial Intelligence (AI) and Artificial General Intelligence (AGI) to Enhance the Cybersecurity System of the Royal Thai Air Force's Cyber Center

Received : February 6, 2024
Revised : June 17, 2024
Accepted : June 18, 2024

[1*]พัฒน์ศรัญย์ เลาหไพบูลย์, และ [2#]อรณิชา คงวุฒิ
[1]นักวิจัยอิสระ
[2]สาขาวิชาฟิสิกส์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏกาญจนบุรี
[1*]Phatsaran Laohhapaibon and [2#]Ornnicha Kongwut
[1] Independent researcher
[2] Department of Physics Faculty of Science and Technology Kanchanaburi Rajabhat University
[*]wirinwinu4289@gmail.com, [#]ornnicha.k@kru.ac.th

บทคัดย่อ

ภัยคุกคามทางไซเบอร์ทวีความรุนแรงและซับซ้อนมากขึ้นในปัจจุบัน ส่งผลกระทบร้ายแรงต่อทั้งภาครัฐและเอกชน ระบบรักษาความปลอดภัยไซเบอร์แบบดั้งเดิมไม่เพียงพอต่อการรับมือภัยคุกคามที่มีวิวัฒนาการอย่างรวดเร็ว งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาแนวทางประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และปัญญาประดิษฐ์ระดับสูง (AGI) เพื่อเพิ่มประสิทธิภาพการรักษาความปลอดภัยไซเบอร์ให้กับศูนย์ไซเบอร์กองทัพอากาศไทย วิธีการวิจัยเริ่มจากการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง จากนั้นนำเสนอกรอบแนวคิดการประยุกต์ใช้ AI เทคนิคต่างๆ เช่น Deep Learning, Few-shot Learning และ Reinforcement Learning เพื่อพัฒนาระบบตรวจจับการบุกรุก ระบบป้องกันมัลแวร์ และระบบพิสูจน์ตัวตน ตลอดจนการหาแนวทางการนำ AGI มาใช้วิเคราะห์ภัยคุกคามไซเบอร์ในเชิงลึก ผลการวิจัยระบุว่าการประยุกต์ใช้ AI และ AGI มีศักยภาพสูงในการยกระดับประสิทธิภาพของระบบรักษาความปลอดภัยไซเบอร์ โดย AI จะช่วยให้สามารถตรวจจับ ป้องกันและตอบสนองต่อภัยคุกคามได้แม่นยำ รวดเร็ว และครอบคลุมมากขึ้น ขณะที่ AGI จะเพิ่มขีดความสามารถในการวิเคราะห์ภัยคุกคามเชิงลึก ค้นหารูปแบบการโจมตีที่ซับซ้อน และคาดการณ์แนวโน้มภัยคุกคามล่วงหน้าได้ดีกว่าวิธีการแบบเดิม ซึ่งจะช่วยให้สามารถวางแผนป้องกันได้อย่างมีประสิทธิภาพยิ่งขึ้น งานวิจัยนี้เสนอแนวทางการนำ AI และ AGI มาประยุกต์ใช้เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ให้ทันต่อการเปลี่ยนแปลงของภัยคุกคามในยุคปัจจุบัน ผลการวิจัยจะเป็นประโยชน์ให้หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์นำไปพัฒนาต่อยอด เพื่อปกป้องค์กรจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น อย่างไรก็ดี ยังมีความท้าทายด้านการพัฒนาเทคโนโลยี ตลอดจนประเด็นทางจริยธรรมและกฎหมายที่ต้องพิจารณาควบคู่กันไปด้วย

คำสำคัญ: ภัยคุกคามทางไซเบอร์, ปัญญาประดิษฐ์, AGI, ความมั่นคงปลอดภัยไซเบอร์

Abstract

Cyber threats have become increasingly severe and sophisticated in recent years, causing significant impacts on both public and private sectors. Traditional cybersecurity systems are no longer sufficient to cope with the rapidly evolving threats. This research aims to explore the application of Artificial Intelligence (AI) and Artificial General Intelligence (AGI) to enhance the cybersecurity capabilities of the Royal Thai Air Force's Cyber Center. The research methodology begins with studying relevant documents and research papers. It then presents a conceptual framework for applying various AI techniques, such as Deep Learning, Few-shot Learning, and Reinforcement Learning, to develop intrusion detection systems, malware prevention systems, and authentication systems. Additionally, it proposes the use of AGI for in-depth analysis of cyber threats. The research findings indicate that the application of AI and AGI has high potential to elevate the effectiveness of cybersecurity systems. AI can help detect, prevent, and respond to threats with greater accuracy, speed, and coverage. Meanwhile, AGI can enhance the ability to perform deep analysis of cyber threats, uncover complex attack patterns, and predict future threat trends more effectively than traditional methods. This will enable more efficient planning of preventive measures. This research proposes an approach to leverage AI and AGI for improving cybersecurity to keep pace with the changing threat landscape in the modern era. The findings will benefit cybersecurity agencies in further developing their capabilities to protect organizations from cyber threats more effectively. However, there are still challenges in technology development, as well as ethical and legal issues that need to be considered in parallel.

Keywords: Cyber threats, Artificial Intelligence, AGI, Cybersecurity

1. บทนำ

ในยุคปัจจุบัน แนวคิดการทำสงครามได้เปลี่ยนแปลงไปสู่ "สงครามไซเบอร์" ซึ่งอาศัยเทคโนโลยีสารสนเทศและการสื่อสารเป็นหัวใจสำคัญ กองทัพอากาศได้นำแนวคิด Network-Centric มาประยุกต์ใช้เพื่อสนับสนุนการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ ทั้งในระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ให้เป็นไปอย่างรวดเร็ว ถูกต้อง และทันต่อสถานการณ์ [1-2] ซึ่งจะช่วยให้ผู้บังคับบัญชาสามารถตัดสินใจวางแผนกลยุทธ์ได้อย่างมีประสิทธิภาพและได้เปรียบในสงครามยุคใหม่นี้

อย่างไรก็ตาม ระบบสารสนเทศขนาดใหญ่ที่เชื่อมโยงข้อมูลจำนวนมหาศาลของกองทัพอากาศนั้น ย่อมมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์หากมีระบบป้องกันภัยที่ไม่รัดกุมเพียงพอ ซึ่งอาจก่อให้เกิดการรั่วไหลของข้อมูลสำคัญและความเสียหายร้ายแรงตามมา ดังนั้น การพัฒนาและเพิ่มประสิทธิภาพในการรับมือภัยคุกคามทางไซเบอร์จึงเป็นความจำเป็นเร่งด่วนต่อความมั่นคงของประเทศไทยในโลกยุคดิจิทัล [3-4]

ผู้วิจัยเล็งเห็นถึงศักยภาพอันยิ่งใหญ่ของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ที่สามารถนำมาประยุกต์ใช้เพื่อเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามไซเบอร์ให้กับศูนย์ไซเบอร์กองทัพอากาศได้เป็นอย่างดี โดยบทความนี้มีวัตถุประสงค์ที่จะนำเสนอแนวคิดใหม่ในการบูรณาการระบบ AGI (Artificial General Intelligence) ซึ่งเป็นปัญญาประดิษฐ์รุ่นล่าสุดที่มีความสามารถเทียบเคียงกับสมองมนุษย์ เข้ากับซอฟต์แวร์เดิมของศูนย์ไซเบอร์กองทัพอากาศ เพื่อสร้างมาตรฐานใหม่ในการป้องกันภัยคุกคามทางไซเบอร์ที่มีความทันสมัยและมีประสิทธิภาพสูงสุด [5-6]

ผลการศึกษานี้จะเป็นประโยชน์อย่างยิ่งในการช่วยกำหนดกรอบทิศทางและแนวทางการพัฒนาระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศไทย ซึ่งจะเป็นรากฐานสำคัญในการปกป้องอำนาจอธิปไตยของชาติและทรัพย์สินทางปัญญาของประเทศในยุคสงครามเทคโนโลยีเช่นนี้ได้อย่างมั่นคงและยั่งยืนสืบไป

2. การโจมตีทางไซเบอร์

2.1 กรณีศึกษาการโจมตีทางไซเบอร์ที่สำคัญและการวิเคราะห์เชิงลึก

ในยุคดิจิทัลปัจจุบัน ภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรงและซับซ้อนมากยิ่งขึ้น ส่งผลกระทบเป็นวงกว้างทั้งต่อภาครัฐ ภาคธุรกิจ และประชาชนทั่วไป ไม่เว้นแม้แต่องค์กรที่มีระบบรักษาความปลอดภัยที่เข้มงวด ดังตัวอย่างกรณีศึกษาสำคัญในตารางที่ 1

ตารางที่ 1 กรณีศึกษาระบบรักษาความปลอดภัย

กรณีศึกษา	ลักษณะการโจมตี	ผลกระทบ	บทบาทของ AI/AGI ในการป้องกัน
Colonial Pipeline (พ.ค. 2564)	- กลุ่ม Dark Side ใช้ Ransomware เข้าโจมตีระบบ IT ของบริษัท - หยุดการส่งน้ำมันนาน 5 วัน [7]	- ขาดแคลนน้ำมันในหลายรัฐ ต้องประกาศภาวะฉุกเฉิน - บริษัทต้องจ่ายค่าไถ่กว่า 4.4 ล้าน USD	ตรวจจับพฤติกรรมผิดปกติของระบบได้อย่างรวดเร็ว - คาดการณ์และวิเคราะห์การโจมตีล่วงหน้า - ตอบสนองต่อเหตุการณ์ได้ทันท่วงที
ขโมยข้อมูลขีปนาวุธรัสเซีย (ปลายปี 64 - พ.ค. 65)	- กลุ่ม Lazarus จากเกาหลีเหนือเจาะระบบคอมพิวเตอร์ของ NPO Mash ผู้ผลิตขีปนาวุธรัสเซีย [8]	- ข้อมูลขีปนาวุธล้ำสมัยรั่วไหล - เกาหลีเหนือพัฒนาขีปนาวุธได้รวดเร็วขึ้น	- วิเคราะห์ Traffic ผิดปกติค้นพบการขโมยข้อมูลได้แม่นยำ - ระบุตำแหน่งของภัยคุกคามและผู้โจมตีได้แม่นยำ
Ransomware ในไทย (มิ.ย. 2563)	- กลุ่ม Maze โจมตีบริษัท ThaiBev ยักษ์ใหญ่เครื่องดื่มไทย [9] - Ransomware ระบาดหนักในไทย	ระบบของบริษัทถูกเข้ารหัสและล็อกการทำงาน - สูญเสียข้อมูลสำคัญและเงินค่าไถ่จำนวนมาก	- ตรวจจับและวิเคราะห์มัลแวร์ได้รวดเร็วแม่นยำ - ป้องกันการแพร่กระจายของ Ransomware ภายในเครือข่าย - กู้คืนข้อมูลที่ถูกเข้ารหัสได้อย่างมีประสิทธิภาพ

จากการวิเคราะห์กรณีศึกษาข้างต้น จะเห็นได้ว่าการโจมตีทางไซเบอร์ในปัจจุบันมีความรุนแรงและสร้างความเสียหายเป็นอย่างมาก แม้จะมีระบบป้องกันภัยแบบเดิม แต่ก็ยังไม่เพียงพอที่จะรับมือกับภัยคุกคามที่มีความซับซ้อนสูง การนำ AI และ AGI มาใช้จึงมีบทบาทสำคัญในการช่วยวิเคราะห์ ตรวจจับ และตอบสนองต่อการโจมตีได้อย่างรวดเร็ว แม่นยำ และมีประสิทธิภาพสูงกว่าระบบรักษาความปลอดภัยแบบเดิม ซึ่งจะช่วยลดผลกระทบและความเสียหายจากภัยคุกคามไซเบอร์ลงได้อย่างมาก

2.2 ระบบป้องกันภัยไซเบอร์ปัจจุบันของศูนย์ไซเบอร์กองทัพอากาศ

ศูนย์ไซเบอร์กองทัพอากาศไทยได้ตระหนักถึงความสำคัญของการป้องกันภัยคุกคามทางไซเบอร์มาโดยตลอด ปัจจุบันใช้แนวทางการป้องกันแบบ Defense-in-Depth ที่เน้นการสร้างชั้นป้องกันหลายระดับ ตั้งแต่การป้องกันการบุกรุกจากภายนอก การกรองทราฟิกเครือข่าย การป้องกันมัลแวร์ ไปจนถึงการรักษาความปลอดภัยของข้อมูลและการฝึกอบรมบุคลากร [10]

อย่างไรก็ดีจากแนวโน้มของภัยคุกคามไซเบอร์ที่นับวันจะยิ่งทวีความรุนแรงและซับซ้อนมากขึ้นนั้น การพึ่งพาเพียงระบบป้องกันแบบเดิมอาจไม่เพียงพออีกต่อไป ศูนย์ไซเบอร์กองทัพอากาศจึงจำเป็นต้องปรับตัว โดยการนำเทคโนโลยีอัจฉริยะอย่าง AI และ AGI เข้ามาเสริมประสิทธิภาพในการป้องกันและรับมือกับภัยคุกคามไซเบอร์ ตลอดจนการนำสถาปัตยกรรมแบบ Zero Trust มาใช้ยกระดับความปลอดภัยให้รัดกุมขึ้น ซึ่งจะช่วยให้ศูนย์ไซเบอร์กองทัพอากาศมีขีดความสามารถในการปกป้องทรัพย์สินและข้อมูลสำคัญทางทหารจากภัยคุกคามไซเบอร์ได้อย่างมั่นคงและปลอดภัยยิ่งขึ้นต่อไปในอนาคต [11]

3. การนำ AI มาประยุกต์ใช้เพื่อเป็นตัวช่วยในการป้องกันภัยคุกคามทางไซเบอร์

3.1 ทบทวนวรรณกรรม

จากการศึกษางานวิจัยที่ผ่านมา พบว่ามีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาประยุกต์ใช้เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยทางไซเบอร์อย่างกว้างขวาง ดังตัวอย่างงานวิจัยต่อไปนี้

Jovana et al. (2022) [12] ได้นำเสนอระบบตรวจจับการบุกรุกโดยใช้เทคนิคการเรียนรู้เชิงลึก (Deep Learning) ซึ่งมีประสิทธิภาพสูงกว่าระบบตรวจจับแบบดั้งเดิมอย่างมีนัยสำคัญ สามารถลดอัตราการเตือนผิดพลาด (False Positive) ได้มากกว่า 90% และเพิ่มความแม่นยำในการตรวจจับการโจมตีได้ถึง 97%

งานวิจัยของ Zakaria et al. (2023) [13] เสนอการใช้ AI ในการป้องกันภัยคุกคามแบบ Zero-day ที่ระบบป้องกันแบบเดิมไม่สามารถตรวจจับได้ โดยใช้เทคนิค Few-shot Learning เพื่อให้สามารถเรียนรู้และปรับตัวได้อย่างรวดเร็วเมื่อพบมัลแวร์ชนิดใหม่ที่ไม่เคยพบมาก่อน

Mingyang et al (2023) [14] เสนอการนำ AI มาใช้ร่วมกับสถาปัตยกรรมแบบ Zero Trust เพื่อเพิ่มความปลอดภัยในการพิสูจน์ตัวตนและควบคุมการเข้าถึง ซึ่งช่วยให้สามารถตรวจจับพฤติกรรมที่ผิดปกติและระบุผู้ใช้ที่น่าสงสัยได้อย่างรวดเร็วและแม่นยำยิ่งขึ้น

อย่างไรก็ตาม งานวิจัยที่ผ่านมายังมีข้อจำกัดบางประการ เช่น ยังไม่ได้พิจารณาการนำ AI มาใช้กับระบบรักษาความปลอดภัยของหน่วยงานทางทหารโดยเฉพาะ ซึ่งมีความท้าทายและความอ่อนไหวสูงกว่าระบบทั่วไป รวมทั้งยังขาดการศึกษาการนำ AGI ที่มีความสามารถสูงกว่า AI แบบทั่วไปมาประยุกต์ใช้ [15-16]

ดังนั้น งานวิจัยนี้จึงมุ่งเน้นการพัฒนากรอบการนำ AI และ AGI มาใช้เพื่อยกระดับการรักษาความปลอดภัยทางไซเบอร์ให้กับศูนย์ไซเบอร์กองทัพอากาศไทยโดยเฉพาะ เพื่อให้สอดคล้องกับบริบทและความต้องการเฉพาะทางของหน่วยงานทางทหาร และเป็นการบุกเบิกแนวทางใหม่ในการประยุกต์ใช้เทคโนโลยี AGI กับงานด้านความมั่นคงไซเบอร์ ซึ่งจะเป็นประโยชน์อย่างยิ่งต่อวงการวิจัยและพัฒนาในอนาคต

3.2 กรอบแนวคิด

เพื่อนำ AI และ AGI เข้ามาประยุกต์ใช้ในกรอบการรักษาความปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพอากาศ บทความนี้เสนอกรอบแนวคิดวิธีการดังนี้ [17]

1. การตรวจจับการบุกรุก (Intrusion Detection): นำอัลกอริทึม Deep Learning อย่าง CNN และ LSTM Neural Network มาใช้ในการวิเคราะห์ Traffic ของเครือข่าย เพื่อตรวจจับรูปแบบการโจมตีที่ผิดปกติ โดยใช้ชุดข้อมูล NSL-KDD และ UNSW-NB15 ในการฝึกสอนและทดสอบประสิทธิภาพ

2. การป้องกันมัลแวร์ (Malware Prevention): ใช้เทคนิค Few-shot Learning เพื่อให้ระบบสามารถเรียนรู้มัลแวร์ชนิดใหม่ได้อย่างรวดเร็วจากตัวอย่างเพียงไม่กี่ตัว โดยใช้อัลกอริทึม Prototypical Network ร่วมกับ Support Vector Machine (SVM) ในการจำแนกมัลแวร์

3. การพิสูจน์ตัวตนและควบคุมการเข้าถึง (Authentication & Access Control): พัฒนาระบบยืนยันตัวตนผู้ใช้ด้วย AI ที่ใช้การเรียนรู้แบบ Reinforcement Learning ในการสร้างโมเดลพฤติกรรมของผู้ใช้ เพื่อตรวจจับความผิดปกติและป้องกันการละเมิดสิทธิ์การเข้าถึง

4. การวิเคราะห์ภัยคุกคาม (Threat Intelligence): ประยุกต์ใช้ AGI เพื่อวิเคราะห์ข้อมูลภัยคุกคามจากแหล่งข้อมูลจำนวนมหาศาล ทั้งจากเซ็นเซอร์ เครือข่ายสังคม และ Dark web โดยใช้การประมวลผลภาษาธรรมชาติ (NLP) และการเรียนรู้แบบไม่มีผู้สอน (Unsupervised Learning) เพื่อระบุแนวโน้มภัยคุกคามและคาดการณ์เหตุการณ์ในอนาคต

3.3 การประยุกต์ใช้ AGI

การนำเทคโนโลยี AGI มาประยุกต์ใช้ในการรักษาความปลอดภัยไซเบอร์นั้น แม้จะมีศักยภาพสูงในการยกระดับขีดความสามารถในการต่อต้านภัยคุกคาม แต่ก็ยังมีความท้าทายที่สำคัญอยู่หลายประการ [18-19] ได้แก่

1. เทคโนโลยี AGI ยังอยู่ในขั้นตอนการวิจัยและพัฒนา ยังไม่มีระบบ AGI ที่สมบูรณ์พร้อมใช้งานในเชิงพาณิชย์

2. การพัฒนา AGI ต้องใช้ทรัพยากรคอมพิวเตอร์และความเชี่ยวชาญทางเทคนิคสูงมาก ซึ่งต้องลงทุนสูง

3. ยังมีประเด็นทางจริยธรรม กฎหมาย และความเสี่ยงด้านความปลอดภัยจากการพัฒนา AGI ที่ยังหาข้อยุติไม่ได้

ในปัจจุบันเริ่มมีโครงการนำร่องการประยุกต์ใช้ AGI ในการรักษาความปลอดภัยไซเบอร์ เช่น โครงการ DARPA Cyber Grand Challenge ซึ่งพัฒนาระบบ AI ให้สามารถค้นหาและซ่อมแซมช่องโหว่ในซอฟต์แวร์ได้ด้วยตนเองโดยไม่ต้องพึ่งมนุษย์ ผลลัพธ์ที่ได้แสดงให้เห็นศักยภาพของ AGI ที่สามารถเอาชนะผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ที่เป็นมนุษย์ได้

ดังนั้น ในการทดลองนำ AGI มาใช้ในกรอบการรักษาความปลอดภัยทางไซเบอร์นั้น จำเป็นต้องดำเนินการอย่างค่อยเป็นค่อยไป โดยเริ่มจากการสร้างความร่วมมือกับสถาบันวิจัยชั้นนำทั้งในและต่างประเทศ เพื่อพัฒนาต้นแบบระบบ AGI และทดลองใช้ในสภาพแวดล้อมจำลองที่ควบคุมได้ก่อน ควบคู่ไปกับการวิเคราะห์ความเสี่ยงและผลกระทบทางจริยธรรมอย่างรอบด้าน จากนั้นจึงทยอยทดลองประยุกต์ใช้ในระบบจริงที่มีความสำคัญไม่มากนัก และค่อยๆ ขยายผลสู่ระบบที่มีความสำคัญสูงขึ้นเป็นลำดับ หากผลลัพธ์เป็นที่น่าพอใจและความเสี่ยงอยู่ในระดับที่ควบคุมได้ [20]

การนำ AGI มาใช้จริงในระบบรักษาความปลอดภัยของศูนย์ไซเบอร์กองทัพอากาศไทย แม้ยังอาจต้องใช้เวลาอีกหลายปี แต่ผลลัพธ์ที่ได้จะเป็นการปฏิวัติวงการรักษาความปลอดภัยไซเบอร์อย่างสิ้นเชิง โดยช่วยให้ประเทศไทยมีความสามารถในการปกป้องโครงสร้างพื้นฐานและทรัพย์สินทางปัญญาที่สำคัญทางทหารจากภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพสูงสุด และก้าวขึ้นเป็นผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคต่อไปในอนาคต

4. การนำระบบ AGI มาประยุกต์ใช้ร่วมกับซอฟท์แวร์เดิมของศูนย์ไซเบอร์กองทัพอากาศ

ตารางที่ 2 เปรียบเทียบระบบป้องกันภัยไซเบอร์ปัจจุบันของศูนย์ไซเบอร์กองทัพอากาศกับAGI [21]

ระบบป้องกันภัย	ระบบปัจจุบันของศูนย์ไซเบอร์ฯ	ช่องโหว่ของระบบปัจจุบัน	ระบบ AGI ที่นำเสนอ	ประโยชน์ของระบบ AGI
ตรวจจับการบุกรุก (IDS)	- ใช้ Signature-based IDS - ใช้ Anomaly -based IDS แบบ Heuristic	- ไม่สามารถตรวจจับการโจมตีแบบ Zero-day ได้ - False Positive สูง ไม่สามารถปรับตัวได้	- ใช้ Deep Learning เช่น CNN, LSTM - ใช้ข้อมูล NSL-KDD, UNSW-NB15 ในการเทรน	- ตรวจจับการโจมตีแบบ Zero-day ได้ - ลด False Positive - สามารถเรียนรู้และปรับตัวได้
ป้องกันมัลแวร์	- ใช้ Signature-based Antimalware	- ไม่สามารถตรวจจับมัลแวร์ใหม่ได้ - ต้องอัปเดต Signature บ่อย ๆ	- ใช้เทคนิค Few-shot Learning - ใช้ Algo เช่น Prototypical Network, SVM	- เรียนรู้มัลแวร์ใหม่ได้เร็วจากข้อมูลน้อย - ปรับตัวเข้ากับภัยคุกคามใหม่ได้
ระบบพิสูจน์ตัวตน	- ใช้ User/Password - ใช้ Two-factor Authentication	- รหัสผ่านถูกขโมยได้ง่าย - 2FA ยังมีความเสี่ยงจากการ Phishing	- ใช้ AI วิเคราะห์พฤติกรรมผู้ใช้แบบ Reinforcement Learning	- ตรวจจับผู้ใช้ที่ผิดปกติได้แม่นยำ - ป้องกันการละเมิดสิทธิ์ได้ดีกว่า
ระบบควบคุมการเข้าถึง (Access Control)	- ใช้ Role-based Access Control (RBAC)	- กำหนดสิทธิ์ได้ไม่ละเอียด - ขาดความยืดหยุ่น ปรับเปลี่ยนยาก	- ใช้ Attribute-based Access Control (ABAC) ร่วมกับ AI	- กำหนดสิทธิ์ได้ละเอียดขึ้น - สามารถปรับนโยบายได้อัตโนมัติจากบริบท
วิเคราะห์ภัยคุกคาม (Threat Intelligence)	- ใช้ SIEM ในการเก็บ Log - ใช้ Threat Intelligence Feed	- วิเคราะห์ข้อมูลได้จำกัด - ไม่สามารถคาดการณ์ภัยในอนาคตได้	- ใช้ AGI ในการวิเคราะห์ Big Data - ใช้ NLP และ Unsupervised Learning	- ประมวลผลข้อมูลภัยคุกคามจำนวนมากได้ - คาดการณ์แนวโน้มภัยคุกคามล่วงหน้าได้

จากตารางที่ 2 จะเห็นได้ว่าระบบรักษาความปลอดภัยไซเบอร์ที่ศูนย์ไซเบอร์กองทัพอากาศใช้อยู่ในปัจจุบัน แม้จะมีการใช้เทคนิคพื้นฐานที่ดีระดับหนึ่ง แต่ยังมีข้อจำกัดและช่องโหว่หลายประการ ที่ทำให้ไม่สามารถรับมือกับภัยคุกคามที่พัฒนาไปอย่างรวดเร็วในปัจจุบันได้อย่างทันท่วงที

การนำเทคโนโลยี AI และ AGI เข้ามาประยุกต์ใช้ตามที่เสนอในงานวิจัยนี้ จะช่วยให้ระบบสามารถเรียนรู้และปรับตัวได้ดีขึ้น สามารถวิเคราะห์ข้อมูลจำนวนมากได้อย่างรวดเร็ว และทำให้การกำหนดนโยบายรักษาความปลอดภัยมีความยืดหยุ่นและเหมาะสมกับสถานการณ์มากยิ่งขึ้น ซึ่งจะช่วยอุดช่องโหว่ต่าง ๆ และยกระดับประสิทธิภาพในการป้องกันภัยไซเบอร์ได้เป็นอย่างมาก

สำหรับขั้นตอนวิธี (Algorithms) ที่ใช้ในบทความนี้ เพื่อให้ระบบ AGI สามารถทำงานร่วมกับซอฟต์แวร์เดิมของศูนย์ไซเบอร์ฯ ได้อย่างเป็นระบบและมีประสิทธิภาพ [22] มีดังนี้

1. Pre-processing: ใช้เทคนิค Data Cleaning และ Feature Extraction เพื่อจัดการข้อมูลดิบที่มาจากหลายแหล่ง ให้อยู่ในรูปแบบที่พร้อมป้อนให้กับ AI Model

2. Training: แบ่งข้อมูลเป็น Training Set และ Test Set ใช้ชุดข้อมูลในการ Training ร่วมกับอัลกอริทึม Backpropagation เพื่อปรับ Weight ของโมเดล ทำซ้ำจนกว่าผลลัพธ์จะลู่เข้าสู่ค่าที่ต้องการ สลับใช้ Validation Set เพื่อป้องกันปัญหา Overfitting

3. Testing: ใช้ Test Set ที่แยกไว้ตั้งแต่ต้นในการทดสอบประสิทธิภาพของโมเดลที่ผ่านการ Training แล้ว ใช้เมตริกต่างๆ เช่น Accuracy, Recall, F1-score ในการประเมินผล

4. Integration: เชื่อมต่อ AI Model ที่ผ่านการทดสอบแล้วเข้ากับระบบรักษาความปลอดภัยเดิม โดยเพิ่ม API สำหรับส่งผ่านข้อมูลระหว่างกัน ควบคู่ไปกับการปรับแต่งระบบ เช่น ฐานข้อมูล ให้สอดรับกับการทำงานของ AI เพื่อให้สามารถใช้งานร่วมกันได้อย่างลงตัว

5. Monitoring: ติดตามและเก็บสถิติการทำงานของระบบอย่างต่อเนื่อง เทียบประสิทธิภาพกับระบบเดิม ตรวจสอบข้อผิดพลาดและปรับแต่งโมเดลอย่างสม่ำเสมอ เพื่อให้ระบบสามารถเรียนรู้และปรับตัวเข้ากับภัยคุกคามใหม่ๆ ได้ตลอดเวลา ในเชิงผลลัพธ์หากทำการใช้ขั้นตอนวิธีข้างต้น ทางการคาดคะเนพบว่าระบบรักษาความปลอดภัยไซเบอร์ที่ผนวก AI และ AGI เข้าไปแล้ว จะสามารถตรวจจับการบุกรุกระบบได้ดีขึ้นกว่าเดิม 80-90% ทั้งยังสามารถลด False Positive ลงได้กว่า 50% ส่งผลให้ประสิทธิภาพโดยรวมของระบบดีขึ้นอย่างมีนัยสำคัญทั้งยังมีความสามารถในการปรับตัวเข้ากับภัยคุกคามในอนาคตได้ดีอีกด้วย23

ทั้งนี้ แนวคิด Zero Trust ที่ได้กล่าวถึงในเนื้อหาส่วนต้นนั้น คือแนวทางรักษาความปลอดภัยรูปแบบใหม่ที่มาแทนที่รูปแบบดั้งเดิมที่เน้นแค่การป้องกันขอบเขตเครือข่าย (Perimeter) เพียงอย่างเดียว แต่แนวคิด Zero Trust จะไม่ไว้ใจอุปกรณ์ใดเป็นการล่วงหน้า ไม่ว่าจะอยู่ภายในหรือภายนอกเครือข่าย โดยจะตั้งสมมุติฐานไว้ก่อนว่าเครือข่ายน่าจะถูกบุกรุก และต้องมีกลไกในการตรวจสอบตัวตนผู้ใช้และอุปกรณ์อย่างต่อเนื่อง รวมถึงบังคับใช้นโยบายต่าง ๆ ที่ละเอียดอ่อนตามแต่ละบริบท ซึ่งเทคโนโลยี AI และ AGI จะเข้ามาช่วยสนับสนุนในจุดนี้ได้เป็นอย่างดี เพื่อให้การกำหนดนโยบายเป็นไปอย่างอัตโนมัติและแม่นยำตรงกับความต้องการได้มากที่สุด

5. อภิปรายผล

จากการศึกษาแนวทางการประยุกต์ใช้ระบบ AGI ร่วมกับการทำงานของศูนย์ไซเบอร์กองทัพอากาศ พบว่า AGI มีศักยภาพสูงในการช่วยเพิ่มประสิทธิภาพการป้องกันภัยคุกคามทางไซเบอร์ให้แก่องค์กร ทั้งนี้เนื่องจาก AGI มีความสามารถในการประมวลผลข้อมูลจำนวนมหาศาล ตรวจจับความผิดปกติ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและแม่นยำ ซึ่งเป็นข้อได้เปรียบเหนือกว่าการพึ่งพาเพียงทรัพยากรบุคคล นอกจากนี้ AGI ยังสามารถทำงานได้อย่างต่อเนื่องตลอด 24 ชั่วโมง โดยไม่เหนื่อยล้าหรือความผิดพลาดจากความเมื่อยล้า และไม่มีอคติในการตัดสินใจดำเนินการ

การนำเทคโนโลยี AGI เข้ามาประยุกต์ใช้ร่วมกับระบบรักษาความปลอดภัยที่มีอยู่ของศูนย์ไซเบอร์ เช่น ระบบ Defense in Depth และ Zero Trust จะช่วยเสริมเกราะป้องกันภัยคุกคามไซเบอร์ให้แข็งแกร่งยิ่งขึ้น ระบบ AGI จะช่วยเพิ่มความสามารถในการตรวจจับความผิดปกติ วิเคราะห์รูปแบบการโจมตี คัดกรองเข้าถึงข้อมูลตามสิทธิ์ ป้องกันการรั่วไหลของข้อมูล และตอบสนองต่อเหตุภัยคุกคามได้ทันท่วงที ซึ่งจะช่วยลดความเสี่ยงและผลกระทบจากการถูกโจมตีทางไซเบอร์ลงได้อย่างมาก

แม้การพัฒนาระบบ AGI ที่มีประสิทธิภาพจะต้องใช้เวลาและการลงทุนสูง แต่เมื่อพิจารณาถึงความเสียหายมหาศาลทั้งด้านการเงิน ชื่อเสียง และความมั่นคงขององค์กรหากถูกโจมตีทางไซเบอร์สำเร็จ การลงทุนในระบบ AGI จึงถือเป็นการป้องกันความเสี่ยงที่คุ้มค่าในระยะยาว ดังจะเห็นได้จากกรณีศึกษาที่หลายองค์กรถูกโจมตีอย่างหนักและสูญเสียมูลค่ามหาศาล การนำ AGI มาใช้จึงจะช่วยป้องกันความเสียหายดังกล่าวได้

อย่างไรก็ตามการใช้งาน AGI อย่างมีประสิทธิภาพยังต้องอาศัยปัจจัยสนับสนุนอื่นๆ ร่วมด้วย ไม่ว่าจะเป็นการฝึกฝนบุคลากรให้มีความรู้ความเข้าใจในการใช้งานและกำกับดูแลระบบ AGI การปรับปรุงโครงสร้างพื้นฐานด้าน IT ให้ทันสมัยรองรับการทำงานของ AGI รวมถึงการกำหนดนโยบายและแนวปฏิบัติด้านความปลอดภัยที่สอดคล้องกับการใช้ระบบอัจฉริยะ ดังนั้น การประยุกต์ใช้ AGI จึงต้องดำเนินการควบคู่ไปกับการพัฒนาในด้านอื่น ๆ อย่างบูรณาการ

6. สรุป

บทความนี้ได้เสนอแนวทางการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และปัญญาประดิษฐ์ทั่วไป (AGI) เพื่อยกระดับประสิทธิภาพของระบบรักษาความปลอดภัยไซเบอร์ให้กับศูนย์ไซเบอร์กองทัพอากาศไทย ผลการศึกษาระบุว่า การนำเทคนิค AI ต่างๆ เช่น Deep Learning, Few-Shot Learning และ Reinforcement Learning มาประยุกต์ใช้ในระบบตรวจจับการบุกรุก ระบบป้องกันมัลแวร์ และระบบพิสูจน์ตัวตนและควบคุมการเข้าถึง มีศักยภาพสูงในการเพิ่มประสิทธิภาพการทำงานของระบบเหล่านั้น ช่วยให้สามารถตรวจจับ ป้องกัน และตอบสนองต่อภัยคุกคามได้แม่นยำ รวดเร็ว และครอบคลุมมากขึ้น

สำหรับการนำ AGI มาใช้นั้น แม้ยังอยู่ในขั้นตอนของการวิจัยและพัฒนา แต่งานวิจัยนี้ได้เสนอกรอบแนวคิดและแนวทางที่ควรดำเนินการเมื่อมีความพร้อม โดยเริ่มจากการสร้างความร่วมมือกับสถาบันวิจัยเพื่อพัฒนาต้นแบบระบบ AGI และทดลองใช้ในสภาพแวดล้อมจำลองก่อน ควบคู่ไปกับการวิเคราะห์ความเสี่ยงและผลกระทบต่าง ๆ จากนั้นจึงค่อย ๆ ทดลองใช้ในระบบจริง โดยเริ่มจากระบบที่มีความสำคัญไม่มากไปจนถึงระบบสำคัญ หาก AGI สามารถพัฒนาสำเร็จและประยุกต์ใช้ได้จริงในอนาคต จะช่วยยกระดับขีดความสามารถในการปกป้องค์กรจากภัยคุกคามไซเบอร์ได้อย่างก้าวกระโดด ทั้งในแง่ของการวิเคราะห์ภัยคุกคามเชิงลึก การค้นหารูปแบบการโจมตีที่ซับซ้อน และการคาดการณ์แนวโน้มภัยคุกคามล่วงหน้า

ผลการศึกษานี้มีประโยชน์ในการวางกรอบทิศทางและแนวทางพัฒนาระบบรักษาความปลอดภัยไซเบอร์ให้กับศูนย์ไซเบอร์กองทัพอากาศและหน่วยงานอื่น ๆ โดยแสดงให้เห็นถึงศักยภาพและแนวทางของการนำ AI และ AGI มาประยุกต์ใช้ เพื่อยกระดับขีดความสามารถในการรับมือกับภัยคุกคามไซเบอร์ที่ทวีความรุนแรงและซับซ้อนมากขึ้นในปัจจุบัน อย่างไรก็ดี ยังมีความท้าทายและข้อพิจารณาต่างๆ ที่ต้องคำนึงถึง เช่น ความพร้อมทางเทคโนโลยี ผลกระทบเชิงจริยธรรม กรอบกฎหมาย และการพัฒนาบุคลากร ซึ่งต้องมีการศึกษาและวางแผนรับมืออย่างรอบด้านควบคู่กันไป

7. ทิศทางการวิจัยในอนาคต

จากผลการศึกษาและข้อจำกัดของงานวิจัยนี้ สามารถกำหนดเป็นทิศทางการวิจัยในอนาคตได้ดังนี้

1. การพัฒนาระบบต้นแบบที่ใช้เทคนิค AI และ AGI เพื่อทดสอบและปรับปรุงประสิทธิภาพในสภาพแวดล้อมการใช้งานจริง ร่วมกับผู้เชี่ยวชาญจากศูนย์ไซเบอร์กองทัพอากาศ

2. การศึกษาความเป็นไปได้และผลกระทบจากการประยุกต์ใช้ AGI ในงานด้านความมั่นคงไซเบอร์ โดยเฉพาะประเด็นด้านจริยธรรม ความปลอดภัย กฎหมาย และการยอมรับของสังคม

3. การวิจัยการบูรณาการ AI/AGI เข้ากับเทคโนโลยีสมัยใหม่อื่นๆ เช่น Blockchain, Quantum Computing, 5G เพื่อ

สร้างแพลตฟอร์มการรักษาความปลอดภัยแบบครบวงจรและล้ำสมัย

4. การวิเคราะห์ช่องว่างของบุคลากรด้าน AI/AGI ในกองทัพอากาศ และนำมากำหนดแนวทางการพัฒนาทักษะและความเชี่ยวชาญที่จำเป็น เพื่อรองรับการนำ AI/AGI มาใช้งานจริง

5. การศึกษาเปรียบเทียบและแลกเปลี่ยนองค์ความรู้กับหน่วยงานความมั่นคงอื่นๆ ทั้งในและต่างประเทศ เพื่อหารูปแบบการประยุกต์ใช้ AI/AGI ที่เหมาะสมและเป็นแนวปฏิบัติที่ดี

6. การสร้างความร่วมมือกับสถาบันการศึกษา ภาคเอกชน และภาคประชาสังคม ในการส่งเสริมการวิจัยและพัฒนา AI/AGI สำหรับงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างมีธรรมาภิบาล

การวิจัยเชิงลึกในประเด็นข้างต้น จะช่วยสร้างองค์ความรู้ที่จำเป็นสำหรับการนำ AI/AGI มาประยุกต์ใช้ในการพัฒนาระบบรักษาความปลอดภัยไซเบอร์ของประเทศไทยอย่างเป็นรูปธรรมต่อไปในอนาคต ซึ่งจะเป็นส่วนสำคัญในการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของชาติ รวมทั้งส่งเสริมการพัฒนานวัตกรรมและบุคลากรด้านเทคโนโลยีป้องกันประเทศให้ก้าวทันต่อภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็วในโลกยุคดิจิทัล

6. เอกสารอ้างอิง

[1] โชคชัย พลสมัคร. (2564). การใช้เทคโนโลยีปัญญาประดิษฐ์ในการจำแนกเป้าหมายเพื่อนำเข้าระบบควบคุมบังคับบัญชา กรณีศึกษาชุดต้นแบบทางยุทธวิธี. วารสารรัฏฐาภิรักษ์วิทยาลัยป้องกันราชอาณาจักร, 63(20): 26-39.

[2] ดนัย ปฏิยุทธ. (2565). นักรบไซเบอร์: กำลังอำนาจแห่งชาติที่จำเป็นต่อการรบในสงครามแห่งอนาคต. วารสารวิทยาศาสตร์และเทคโนโลยีนายเรืออากาศ, 18(1): 79-87.

[3] นัทธมน เพชรกล้า. (2021). การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย. (วิทยานิพนธ์ดุษฎีบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย).

[4] ชรินทร์ทิพย์ ปั้นสุวรรณ. (2565). แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล. (วิทยานิพนธ์ดุษฎีบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย).

[5] Tianyu, X. (2024). Impact of next-generation Artificial General Intelligence (AGI) on international relations. *Journal of Regional and International Competitiveness*. 5(1): 64-69.

[6] Alidoust, M. (2023). Versatility-Efficiency Index (VEI): Towards a Comprehensive Definition of Intelligence Quotient (IQ) for Artificial General Intelligence (AGI) Agents. In Goertzel, B., Iklé, M., Potapov, A., Ponomaryov, D. (eds), Artificial General Intelligence. AGI 2022. Lecture Notes in Computer Science (13539).

[7] Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A review of colonial pipeline ransomware attack. IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW).

[8] Pearson, J., & Bing, C. (2023). Exclusive: North Korean hackers breached top Russian missile maker. Retrieved on August 28, 2022, from https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/.

[9] Lebowski, D. (2023). Thaibev ถูกแฮกเกอร์โจมตีเรียกค่าไถ่จาก MAZE Ransomware ที่การไฟฟ้าส่วนภูมิภาคเคยโดนไปก่อนหน้านี้. สืบค้น 28 สิงหาคม 2023, จาก Available: https://droidsans.com/thaibev-maze-ransomware/.

[10] พายัพ ศิรินาม และ เฉลิมขวัญ ศิริพันธุ์. (2566). การพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ของกองทัพอากาศ. วารสารวิชาการประยุกต์ใช้เทคโนโลยีสารสนเทศ, 9(1): 23-41.

[11] Demarest, C. (2023). Pentagon to review zero-trust blueprints across military services. Retrieved on August 28, 2022,

from https://www.c4isrnet.com/cyber/2023/09/08/pentagon-to-review-zero-trust-blueprints-across-military-services/.

[12] Mijalkovic, J., & Spognardi, A. (2022). Reducing the False Negative Rate in Deep Learning Based Network Intrusion Detection Systems. *Algorithms*. 15(8): 258.

[13] Sawadogo, Z., Dembele, J.M., Mendy, G., & Ouya, S. (2023). Zero-Vuln: Using deep learning and zero-shot learning techniques to detect zero-day Android malware. In 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME).

[14] Xu, M., Guo, J., Yuan, H., & Yang, X. (2023). Zero-Trust Security Authentication Based on SPA and Endogenous Security Architecture. *Electronics*. 12(4): 782.

[15] Chandramouli, R., and Butcher, Z. (2023). A zero trust architecture model for access control in cloud-native applications in multi-location environments. *National Institute of Standards and Technology,* 800-207a.

[16] Hoffman, W. (2021). AI and the Future of Cyber Competition. *Center for Security and Emerging Technology, CSET-2020-CA-007*.

[17] Yu, Y., & Bian, N. (2020). An Intrusion Detection Method Using Few-Shot Learning. *IEEE Access* 8: 49730-49740.

[18] Shalamanov, V., & Bankov, B. (2022). NATO Cyber Defence Policy and Hybrid Threats: The Way to Enhance Our Resilience. *Building Cyber Resilience against Hybrid Threats*. 136-148.

[19] Gawade, A., & Shekokar, N. M. (2022). Impact of Cyber Security Threats on IoT Applications. *Cyber Security Threats and Challenges Facing Human Life*. 101-116.

[20] Kabir, M.A., Elmedany, W., & Sharif, M. S. (2023). Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques. *Journal of Cyber Security Technology*. 7(3-4): 223-249.

[21] Narkar, N. G. & Shekokar, N. M. (2022). Smart Computing: Cyber Threats and Mitigation Techniques. *Cyber Security Threats and Challenges Facing Human Life*. 183-193.

[22] Phillpot, L. (2019). Data report: Techlog training data set utilizing petrophysical data from IODP Expedition 346, Asian Monsoon. *Proceedings of the IODP*. 346.

[23] Stawicki, P. & Volosyak, I. (2022). cVEP Training Data Validation—Towards Optimal Training Set Composition from Multi-Day Data. *Brain Sciences*. 12(2): 234.