AIGC
AI GOVERNANCE CENTER
by ETDA

การใช้ปัญญาประดิษฐ์ในวงการความมั่นคงทางไซเบอร์

นายเอกสิทธิ์ วินิจกุล
AIGC Expert Fellow
สำนักงานศาลปกครอง

ETDA

การใช้ปัญญาประดิษฐ์ในวงการความมั่นคงทางไซเบอร์: ประโยชน์และความเสี่ยง[1]

นาย เอกสิทธิ์ วินิจกุล
พนักงานคดีปกครอง สำนักงานศาลปกครองสูงสุด สำนักงานศาลปกครอง

บทสรุปผู้บริหาร

ในปัจจุบัน ระบบความปลอดภัยทางไซเบอร์เผชิญกับความท้าทายมากมาย ทั้งแฮ็กเกอร์ที่มีความซับซ้อนมากขึ้น รูปแบบการโจมตีที่หลากหลาย หรือแม้กระทั่งการโจมตีโครงสร้างพื้นฐานที่เพิ่มขึ้น ขณะเดียวกัน ในด้านความปลอดภัยทางไซเบอร์ มีการใช้งานปัญญาประดิษฐ์เป็นเครื่องมือในการปรับปรุงมาตรการรักษาความปลอดภัยสำหรับองค์กรต่างๆ ด้วยคุณลักษณะของปัญญาประดิษฐ์ที่อัลกอริธึมสามารถวิเคราะห์ข้อมูลจำนวนมหาศาล เป็นปัจจุบัน และระบุสิ่งบ่งชี้ของการโจมตีและความผิดปกติได้ในระยะอันรวดเร็ว ทำให้สามารถระบุภัยคุกคามและช่องโหว่ได้อย่างรวดเร็ว อันเป็นผลให้สามารถป้องกันการโจมตีได้อย่างรวดเร็ว ลดความเสี่ยง และความเสียหายได้ ยิ่งไปกว่านั้น ปัญญาประดิษฐ์ได้พัฒนาความสามารถในการควบคุมการเข้าถึงอย่างประสิทธิภาพมากขึ้น อาทิ กลไกการตรวจสอบสิทธิขั้นสูง ดังเช่นไบโอเมตริกซ์ ระบบการจดจำใบหน้า หรือระบบการสแกนลายนิ้วมือ เป็นต้น

อีกด้านหนึ่ง ด้วยเทคโนโลยีปัญญาประดิษฐ์ที่อยู่เบื้องหลังการทำงานของระบบความปลอดภัยทางไซเบอร์ ทำให้มีข้อกังวลตามมาหลายประการ ทั้งในเรื่องข้อกังวลด้านความเป็นส่วนตัวของข้อมูล โดยเฉพาะหากปัญญาประดิษฐ์ถูกใช้ในการวิเคราะห์พฤติกรรมผู้ใช้งาน อาจจำเป็นต้องเข้าถึงข้อมูลส่วนบุคคลที่ละเอียดอ่อนของผู้ใช้งาน หรือข้อกังวลด้านขาดความโปร่งใสที่ระบบปัญญาประดิษฐ์มักทำหน้าที่เป็นกล่องดำที่ยากที่จะเข้าใจว่าระบบเหล่านี้มีกระบวนการคิดอย่างไรจนได้มาซึ่งผลลัพธ์ของการตัดสินใจที่เฉพาะเจาะจง ทำให้ตรวจสอบความถูกต้องจะกลายเป็นเรื่องยาก ตลอดจนข้อกังวลด้านการฝึกอบรมและความลำเอียงของอัลกอริทึมที่อาจมีการทำงานอย่างมีอคติได้ ไม่ว่าจะเป็นอคติจากข้อมูลที่ใช้ในการฝึกอัลกอริธึมปัญญาประดิษฐ์ หรืออคติจากความลำเอียงของอัลกอริทึม ก็ตาม

---

[1] จัดทำโดยนาย เอกสิทธิ์ วินิจกุล ผู้เชี่ยวชาญในโครงการ AI Governance Center (AIGC) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

บทความนี้นำเสนอ 1) การใช้งานปัญญาประดิษฐ์ในด้านความปลอดภัยทางไซเบอร์เพื่อให้เห็นถึงการใช้งานปัญญาประดิษฐ์ในด้านที่เป็นประโยชน์สำหรับความปลอดภัยทางไซเบอร์ และ 2) ข้อกังวลของปัญญาประดิษฐ์ในการใช้งานในความปลอดภัยทางไซเบอร์ ที่จะต้องให้ความสำคัญและตระหนักถึงอยู่เสมอในการใช้งานปัญญาประดิษฐ์ และอาจเกิดผลกระทบอย่างมีนัยสำคัญกับมนุษย์ได้

บทนำ

การถือกำเนิดของปัญญาประดิษฐ์ถือเป็นการเปลี่ยนแปลงที่สำคัญที่สุดประการหนึ่งในภาคส่วนความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะการเปลี่ยนแปลงจากกลไกที่เน้นการป้องกันไปเป็นการป้องกันเชิงรุก กล่าวคือ แต่เดิมการรักษาความปลอดภัยทางไซเบอร์อาศัยกฎและสัญญาณที่กำหนดไว้ล่วงหน้าในการตรวจจับและบรรเทาภัยคุกคามเป็นหลัก ซึ่งมักจะทำการตอบสนองต่อการโจมตีหลังจากที่เหตุเกิดขึ้นแล้ว ในขณะที่การทำงานของปัญญาประดิษฐ์กลายเป็นการทำงานโดยอาศัยการสืบสวนและการแทรกแซงเป็นหลัก

ประกอบกับเทคโนโลยีปัญญาประดิษฐ์ทำให้องค์กรต่างสามารถใช้แนวทางการป้องกันเชิงรุกที่สามารถนำหน้าการกระทำของผู้โจมตีทางไซเบอร์ได้อย่างไม่ยากนัก จากระบบที่สามารถวิเคราะห์ข้อมูลจำนวนมหาศาลแบบเรียลไทม์ ความสามารถในการระบุรูปแบบ การคาดการณ์ภัยคุกคามที่อาจเกิดขึ้น ตลอดจนตรวจจับและเฝ้าระวังกิจกรรมที่เป็นอันตรายก่อนที่จะก่อให้เกิดปัญหาร้ายแรงหรือความเสียหายขึ้น ยิ่งไปกว่านั้น โซลูชันความปลอดภัยทางไซเบอร์ที่ขับเคลื่อนด้วยปัญญาประดิษฐ์สามารถปรับตัวและเรียนรู้จากข้อมูลใหม่และภัยคุกคามที่เกิดขึ้นใหม่ได้อย่างต่อเนื่อง ปรับปรุงประสิทธิภาพเมื่อเวลาผ่านไปโดยไม่ต้องมีการเข้าแทรกแซงหรือดำเนินการโดยมนุษย์ ความสามารถในการเปลี่ยนแปลงนี้แสดงถึงการเปลี่ยนแปลงกระบวนทัศน์ด้านความปลอดภัยทางไซเบอร์ ช่วยให้องค์กรต่างๆ สามารถคาดการณ์และบรรเทาภัยคุกคามได้อย่างรวดเร็วและแม่นยำ

แม้ว่า ปัญญาประดิษฐ์ได้ปฏิวัติวิธีที่ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ใช้ในการทำงานก็ตาม ในขณะเดียวกัน อาชญากรรมไซเบอร์ก็ได้ลงทุนในปัญญาประดิษฐ์และการเรียนรู้ของเครื่องเช่นกัน ทำให้มีการโจมตีทางไซเบอร์ที่กำหนดเป้าหมายอย่างแม่นยำและขนาดขอบเขตใหญ่ขึ้น ทำให้จำนวนภัยคุกคามและแรนซัมแวร์เพิ่มขึ้นอย่างรวดเร็ว โดยเฉพาะมีความกังวลว่า ปัญญาประดิษฐ์จะถูกใช้เป็นช่องทางในการโจมตีทางไซเบอร์และการกระทำผิดทางอาญาอื่น ๆ ซึ่ง อาชญากรไซเบอร์สามารถเลี่ยงการป้องกันแบบเดิม ๆ ได้ง่ายขึ้น

บทความนี้นำเสนอข้อดีของการใช้ปัญญาประดิษฐ์ในด้านความปลอดภัยทางไซเบอร์เพื่อให้ผู้อ่านเห็นถึงการใช้งานปัญญาประดิษฐ์ทั้งในด้านที่เป็นประโยชน์ และในด้านที่การใช้งานปัญญาประดิษฐ์อาจเกิดผลกระทบได้

1. การใช้งานปัญญาประดิษฐ์ในด้านความปลอดภัยทางไซเบอร์

ปัญญาประดิษฐ์ถูกใช้เป็นเครื่องมือในการปรับปรุงมาตรการรักษาความปลอดภัยสำหรับองค์กรต่างๆ ด้วยคุณลักษณะของปัญญาประดิษฐ์ที่อัลกอริธึมสามารถวิเคราะห์ข้อมูลจำนวนมหาศาลและเป็นปัจจุบัน ทำให้สามารถระบุภัยคุกคามและช่องโหว่ได้อย่างรวดเร็ว อันเป็นผลให้สามารถป้องกันการโจมตีได้อย่างรวดเร็ว ลดความเสี่ยง และความเสียหายได้

การใช้งานปัญญาประดิษฐ์ในด้านความปลอดภัยทางไซเบอร์มีหลากหลายวิธีการ ซึ่งสามารถสรุปการใช้งานปัญญาประดิษฐ์ในด้านความปลอดภัยทางไซเบอร์เป็น 6 ประเภท ดังต่อไปนี้

1.1 การใช้ปัญญาประดิษฐ์เพื่อระบุสิ่งบ่งชี้ของการโจมตี[2]

ด้วยคุณลักษณะของอัลกอริทึมปัญญาประดิษฐ์ การเรียนรู้ของเครื่อง และโมเดลการเรียนรู้เชิงลึก ทำให้สามารถวิเคราะห์ข้อมูลจำนวนมหาศาลและระบุรูปแบบที่นักวิเคราะห์ที่เป็นมนุษย์อาจมองข้ามได้ ความสามารถนี้ของปัญญาประดิษฐ์จะช่วยให้ตรวจจับภัยคุกคามและความผิดปกติได้ในระยะอันรวดเร็วแม่นยำสูง และอยู่ในระยะเริ่มต้น ทำให้สามารถป้องกันการละเมิดความปลอดภัย และช่วยให้ระบบสามารถดำเนินการเชิงรุกแทนการโต้ตอบกับภัยคุกคามภายหลังที่เกิดเหตุขึ้นแล้ว

ระบบปัญญาประดิษฐ์สามารถได้รับการฝึกฝนให้ทำการจดจำรูปแบบและตรวจจับการโจมตีจากแรนซัมแวร์หรือมัลแวร์ก่อนที่จะเข้าสู่ระบบ ซึ่งจะช่วยป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพมากยิ่งขึ้นตัวอย่างเช่น เทคโนโลยีการทำนายอัจฉริยะ (Predictive Intelligence) ที่ผสานเข้ากับการประมวลผลภาษาธรรมชาติ (NLP) สามารถรวบรวมและวิเคราะห์ข้อมูลจากข่าวสาร บทความ และรายงานการศึกษาต่าง ๆ เกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่ล่าสุด ทำให้สามารถรวบรวมข้อมูลเกี่ยวกับแนวโน้มการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต หรือเพื่อระบุสัญญาณเริ่มต้นของการโจมตีได้ เช่น การพยายามเข้าถึงข้อมูลหรือพฤติกรรมที่ผิดปกติในระบบ เมื่อตรวจพบสิ่งที่น่าสงสัย ระบบจะสามารถดำเนินการตอบสนองทันทีเพื่อป้องกันการโจมตีไม่ให้ขยายตัวจนกลายเป็นภัยคุกคามเต็มรูปแบบ

[2] Anser shah, The Role of Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation, p.3-4

1.2 การปรับปรุงข้อมูลภัยคุกคาม[3]

ปัญญาประดิษฐ์เชิงกำเนิด (Generative AI) เป็นประเภทของปัญญาประดิษฐ์ที่ใช้โมเดลการเรียนรู้เชิงลึกหรืออัลกอริธึมเพื่อสร้างข้อความ รูปภาพ วิดีโอ โค้ด และผลลัพธ์อื่น ๆ โดยอัตโนมัติตามชุดข้อมูลที่ได้รับการฝึกฝน เทคโนโลยีนี้ไม่เพียงแต่ช่วยให้นักวิเคราะห์สามารถระบุภัยคุกคามที่อาจเกิดขึ้นได้เท่านั้น แต่ยังช่วยให้เข้าใจภัยคุกคามเหล่านั้นได้ลึกซึ้งยิ่งขึ้น

อัลกอริธึมของปัญญาประดิษฐ์เชิงกำเนิด (Generative AI(สามารถสแกนโค้ดและเฝ้าระวังการรับส่งข้อมูลบนเครือข่ายเพื่อหาภัยคุกคาม จากนั้นจึงให้ข้อมูลเชิงลึกที่ช่วยให้นักวิเคราะห์เข้าใจพฤติกรรมของสคริปต์ที่เป็นอันตรายหรือภัยคุกคามในรูปแบบอื่น ๆ ได้ดียิ่งขึ้น ก่อนหน้านี้ หากไม่มีปัญญาประดิษฐ์ นักวิเคราะห์ต้องใช้ภาษาคิวรีที่ซับซ้อน (complex query languages) ดำเนินการขั้นตอนต่าง ๆ และทำวิศวกรรมย้อนกลับเพื่อวิเคราะห์ข้อมูลจำนวนมหาศาลเพื่อทำความเข้าใจภัยคุกคาม แต่ด้วยอัลกอริธึมของปัญญาประดิษฐ์เชิงกำเนิด (Generative AI) ทำให้สามารถตรวจจับภัยคุกคามจากการสแกนโค้ดและเฝ้าระวังการรับส่งข้อมูลบนเครือข่ายได้อย่างมีประสิทธิภาพ พร้อมกับให้ข้อมูลเชิงลึกที่ช่วยให้นักวิเคราะห์เข้าใจพฤติกรรมของสคริปต์ที่เป็นอันตรายหรือภัยคุกคามในรูปแบบอื่น ๆ ได้ดียิ่งขึ้น[4]

1.3 เสริมสร้างแนวทางปฏิบัติในการควบคุมการเข้าถึงและรหัสผ่าน[5]

ปัญญาประดิษฐ์ได้พัฒนาความสามารถในการควบคุมการเข้าถึงและแนวปฏิบัติเกี่ยวกับการใช้รหัสผ่านให้มีประสิทธิภาพมากขึ้น โดยใช้กลไกการตรวจสอบสิทธิขั้นสูง เช่น การรับรองความถูกต้องด้วยไบโอเมตริกซ์ ซึ่งรวมถึงการจดจำใบหน้าและการสแกนลายนิ้วมือ วิธีการเหล่านี้ช่วยเสริมความแข็งแกร่งให้กับมาตรการรักษาความปลอดภัยโดยลดการพึ่งพารหัสผ่านแบบเดิม ๆ

นอกจากนี้ อัลกอริธึมปัญญาประดิษฐ์ ยังสามารถวิเคราะห์รูปแบบการเข้าสู่ระบบและพฤติกรรมของผู้ใช้งาน เพื่อระบุความผิดปกติทางพฤติกรรมและการพยายามเข้าสู่ระบบที่น่าสงสัย ซึ่งช่วย

---

[3]Armaan Sidhu, AI-Driven Threat Intelligence: Leveraging Machine Learning to Empower Cybersecurity Applications for Enhanced Threat Detection and Response, Department of Computer Science & Engineering, Manipal University Jaipur, Rajasthan, India, p.9-11

[4] Yagmur Yigit, Review of Generative AI Methods in Cybersecurity, available at https://arxiv.org/html/2403.08701v2 (last accessed 20/07/2024)

[5] Ramanpreet Kaur, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97, September 2023, available at https://www.sciencedirect.com/science/article/pii/S1566253523001136 (last accessed 20/07/2024)

ให้องค์กรสามารถบรรเทาภัยคุกคามและจัดการกับการละเมิดความปลอดภัยที่อาจเกิดขึ้นได้อย่างรวดเร็วมากขึ้น

1.4 การจัดลำดับความสำคัญและการลดความเสี่ยง[6]

เนื่องจากผู้คุกคามใช้ประโยชน์จากเทคโนโลยีใหม่ ๆ โดยเฉพาะเครื่องมือที่ขับเคลื่อนด้วยปัญญาประดิษฐ์เพื่อสร้างการโจมตีที่ซับซ้อนมากขึ้นเรื่อย ๆ เช่น การสแกนเครือข่ายเพื่อหาช่องโหว่เริ่มการโจมตี การสร้างอีเมลฟิชชิ่งที่น่าเชื่อถือ และการพัฒนามัลแวร์ที่ซับซ้อนยิ่งขึ้น ทำให้ซอฟต์แวร์และเทคนิคในการป้องกันแบบดั้งเดิมจึงไม่สามารถตามทัน ทำให้ความเสี่ยงต่อการถูกโจมตีขององค์กรยุคใหม่เพิ่มสูงขึ้นทุกวัน

ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง (ML) กลายเป็นเครื่องมือสำคัญสำหรับทีมรักษาความปลอดภัยทางไซเบอร์ โดยถูกนำมาใช้เพื่อลดความเสี่ยงจากการละเมิดและเพิ่มความปลอดภัยด้วยการอุดช่องโหว่ในระบบและเครือข่าย โมเดลการเรียนรู้ของเครื่องสามารถสแกนโครงสร้างพื้นฐาน โค้ด และการกำหนดค่าเพื่อค้นหาจุดอ่อนที่ผู้โจมตีอาจใช้ประโยชน์จากจุดอ่อนนั้นได้ อัลกอริธึมการเรียนรู้ของเครื่องมีความสามารถในการวิเคราะห์ รักษา และปรับปรุงช่องโหว่ อีกทั้ง ยังสามารถให้ข้อมูลเชิงลึกเกี่ยวกับความเสี่ยงและผลกระทบของการโจมตีประเภทต่าง ๆ จึงช่วยให้ทีมรักษาความปลอดภัยทางไซเบอร์สามารถจัดลำดับความสำคัญในการรับมือและบรรเทาผลกระทบได้อย่างมีประสิทธิภาพมากขึ้น และทำให้องค์กรสามารถประเมินความเสี่ยงและจัดสรรทรัพยากรได้อย่างมีประสิทธิภาพมากขึ้น

นอกจากการตรวจจับตั้งแต่เนิ่นๆ แล้ว ระบบการป้องกันอัตโนมัติที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ ยังสามารถกรองผลบวกลวงออกไปโดยการใช้ข้อมูลจากการเตือนที่ผิดพลาดก่อนหน้าเพื่อเพิ่มความสามารถในการตรวจจับภัยคุกคามและลดเวลาที่ใช้ในการตรวจสอบปัญหาที่ ที่เป็นผลบวกลวง ตัวอย่างเช่น IBM ในการศึกษาของพวกเขาอ้างว่า Cyber Assistant ของ QRadar EDR ซึ่งเป็นระบบการจัดการการแจ้งเตือนที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ ได้ช่วยให้ลูกค้าลดจำนวนผลบวกลวง ซึ่งช่วยปรับปรุง

[6] Ragesh K R, Vulnerability management using AI, 29 Jun 2023,available at https://beaglesecurity.com/blog/article/vulnerability-management-using-ai.html#:~:text=AI%20leverages%20advanced%20analytics%20and%20machine%20learning%20techniques,exploited.%20This%20predictive%20capability%20enhances%20proactive%20security%20measures. (last accessed 20/07/2024)

ความแม่นยำของการตรวจจับภัยคุกคามและช่วยให้ผู้เชี่ยวชาญด้านไซเบอร์สามารถมุ่งเน้นความพยายามของพวกเขาไปที่ภัยคุกคามที่มีผลกระทบสูง[7]

1.5 การตรวจจับและตอบสนองภัยคุกคามอัตโนมัติ[8]

ระบบรักษาความปลอดภัยทางไซเบอร์ที่มีปัญญาประดิษฐ์เป็นส่วนประกอบ ไม่เพียงแต่สามารถระบุความเสี่ยงและช่องโหว่ได้เท่านั้น แต่ยังสามารถตอบสนองต่อภัยคุกคามโดยอัตโนมัติอีกด้วย อัลกอริธึมการเรียนรู้ของเครื่องสามารถวิเคราะห์การรับส่งข้อมูลเครือข่าย พฤติกรรมผู้ใช้ เชื่อมโยงเหตุการณ์ต่างๆ และให้ข้อมูลเชิงลึกเพื่อสนับสนุนการตัดสินใจระหว่างเกิดเหตุการณ์ นอกจากนี้ยังสามารถบันทึกการทำงานของระบบอย่างต่อเนื่องเพื่อระบุกิจกรรมที่น่าสงสัย ตัวอย่างเช่น ในเรื่องความปลอดภัยของอีเมล โดยปัญญาประดิษฐ์จะกลั่นกรององค์ประกอบต่างๆ ของอีเมล เช่น เนื้อหา รายละเอียดผู้ส่ง ไฟล์แนบ และลิงก์ เป็นต้น โดยหากเห็นว่ามีความพยายามโจมตี จะตั้งค่าสถานะอีเมลฉบับนั้นว่าเป็นอันตรายในทันที

นอกจากการตรวจจับภายในระยะเวลาอันรวดเร็วแล้ว ปัญญาประดิษฐ์ยังสามารถตรวจสอบแบบเรียลไทม์และตอบสนองในเวลาที่รวดเร็ว เช่น การบล็อกที่อยู่ IP ที่เป็นอันตรายโดยอัตโนมัติ หรือการปิดระบบหรือปิดบัญชีของผู้ใช้งานที่บุกรุกทันที หรือสามารถวิเคราะห์อีเมลล์และหน้าเว็บเพื่อระบุการกระทำฟิชชิ่งที่อาจเกิดขึ้น เป็นต้น ด้วยคุณสมบัติเหล่านี้ องค์กรจึงสามารถตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที

1.6 เพิ่มประสิทธิภาพและประสิทธิผลในการทำงานของเจ้าหน้าที่ที่เป็นมนุษย์

จากสถิติพบว่าประมาณร้อยละ 82 ของการละเมิดข้อมูลมีสาเหตุมาจากข้อผิดพลาดของมนุษย์ เช่น การกำหนดค่าที่ไม่ถูกต้อง การรั่วไหลของข้อมูลโดยไม่ได้ตั้งใจ หรือข้อผิดพลาดอื่น ๆ ที่อาจส่งผลต่อความปลอดภัย เป็นต้น ซึ่งกรณีนี้ ปัญญาประดิษฐ์จึงมีบทบาทสำคัญในการลดโอกาสเกิดข้อผิดพลาดดังกล่าวได้ สำหรับการสนับสนุนทีมรักษาความปลอดภัยทางไซเบอร์ที่มีเจ้าหน้าที่ที่เป็นมนุษย์ ปัญญาประดิษฐ์สามารถจัดเตรียมข้อมูลเชิงลึก รวมถึงการวิเคราะห์ข้อมูลจำนวนมหาศาล และสามารถเฝ้า

[7] KPMG, The AI Cyber Security Challenge, available at https://kpmg.com/nl/en/home/insights/2024/06/ai-cyber-security-challenge.html (last accessed 20/07/2024)

[8] Alexis Porter, AI Threat Intelligence: Unlocking the Power of Automation in Cybersecurity, available at https://bigid.com/blog/ai-threat-intelligence/ (last accessed 20/07/2024)

ระวังภัยคุกคามใหม่ ๆ ที่ช่วยให้ทีมเข้าใจภาพรวมของภัยคุกคามได้ครบถ้วนและตอบสนองต่อเหตุการณ์ได้รวดเร็วและแม่นยำขึ้น ทำให้สามารถวางมาตรการป้องกันเชิงรุกได้อย่างมีประสิทธิภาพมากขึ้น

การโจมตีกับการป้องกัน[9]

การป้องกันโดยใช้ปัญญาประดิษฐ์	การโจมตีโดยใช้ปัญญาประดิษฐ์
การตรวจจับภัยคุกคามที่ขับเคลื่อนด้วยปัญญาประดิษฐ์: การใช้ประโยชน์จากปัญญาประดิษฐ์ เพื่อเพิ่มความสามารถในการตรวจจับภัยคุกคาม โดยโมเดลปัญญาประดิษฐ์สามารถวิเคราะห์ข้อมูลเครือข่ายจำนวนมหาศาลเพื่อระบุรูปแบบที่ผิดปกติซึ่งบ่งบอกถึงการโจมตี	**ความเร็วและประสิทธิภาพ:** ปัญญาประดิษฐ์ช่วยให้ผู้คุกคามสามารถโจมตีอัตโนมัติและดำเนินการอย่างรวดเร็วได้ อัลกอริทึมแมชชีนเลิร์นนิงสามารถสแกนหาช่องโหว่เพื่อเริ่มการโจมตีและปรับกลยุทธ์แบบเรียลไทม์อย่างรวดเร็วทำให้ฝ่ายป้องกันตามได้ยาก
การตอบสนองแบบเรียลไทม์: การใช้ปัญญาประดิษฐ์สำหรับการตอบสนองต่อเหตุการณ์อัตโนมัติสามารถลดเวลาตอบสนองได้อย่างมาก ปัญญาประดิษฐ์สามารถแยกระบบที่ได้รับผลกระทบได้ เช่น บล็อก IP ที่เป็นอันตรายหรือการห้ามการเข้าถึงฐานข้อมูลในส่วนที่สำคัญโดยอัตโนมัติ เป็นต้น	**ความซับซ้อน:** ปัญญาประดิษฐ์สามารถพัฒนาวิธีการโจมตีที่ซับซ้อนยิ่งขึ้น ตัวอย่างเช่น อัลกอริทึมแมชชีนเลิร์นนิงสามารถสร้างอีเมลฟิชชิ่งที่น่าเชื่อถือยิ่งขึ้นโดยการวิเคราะห์ฟิชชิ่งที่ประสบความสำเร็จมาก่อน
การป้องกันเชิงคาดการณ์: ปัญญาประดิษฐ์สามารถวิเคราะห์เชิงคาดการณ์เพื่อคาดการณ์เวกเตอร์การโจมตีที่อาจเกิดขึ้น ด้วยการวิเคราะห์แนวโน้มและรูปแบบในภัยคุกคามทางไซเบอร์ และปัญญาประดิษฐ์สามารถช่วยให้องค์กรคาดการณ์และลดความเสี่ยงก่อนที่จะเกิดการโจมตีขึ้นจริง	**ความสามารถในการปรับขนาด:** ปัญญาประดิษฐ์ช่วยให้ผู้คุกคามสามารถปรับขอบเขตการโจมตีได้ โดยกำหนดเป้าหมายหลายระบบพร้อมกันและมีการแทรกแซงของมนุษย์น้อยที่สุด ทำให้กลไกการป้องกันแบบดั้งเดิมทำงานอย่างไม่มีประสิทธิภาพ
การเรียนรู้และการปรับตัวอย่างต่อเนื่อง: ระบบปัญญาประดิษฐ์ต้องได้รับการฝึกอบรมอย่างต่อเนื่องด้วยข้อมูลใหม่เพื่อปรับให้เข้ากับภัย	

[9] KPMG, The AI Cyber Security Challenge, available at https://kpmg.com/nl/en/home/insights/2024/06/ai-cyber-security-challenge.html (last accessed 20/07/2024)

การป้องกันโดยใช้ปัญญาประดิษฐ์	การโจมตีโดยใช้ปัญญาประดิษฐ์
คุกคามที่เกิดขึ้นใหม่ กระบวนการต่อเนื่องนี้ทำให้มั่นใจได้ว่ากลไกการป้องกันยังคงมีประสิทธิภาพต่อกลยุทธ์การโจมตีที่ทันสมัย	
การตรวจจับภัยคุกคามที่ขับเคลื่อนด้วยปัญญาประดิษฐ์: การใช้ประโยชน์จากปัญญาประดิษฐ์เพื่อเพิ่มความสามารถในการตรวจจับภัยคุกคามสำคัญ โมเดลปัญญาประดิษฐ์สามารถวิเคราะห์ข้อมูลเครือข่ายจำนวนมหาศาลเพื่อระบุรูปแบบที่ผิดปกติ ซึ่งบ่งบอกถึงการโจมตีที่เริ่มต้นขึ้น	

2. ข้อกังวลของปัญญาประดิษฐ์ในการใช้งานในความปลอดภัยทางไซเบอร์

2.1 ข้อกังวลด้านความเป็นส่วนตัวของข้อมูล[10]

ระบบปัญญาประดิษฐ์ต้องการข้อมูลจำนวนมากเพื่อนำไปใช้ ซึ่งอาจก่อให้เกิดความเสี่ยงด้านข้อมูลส่วนบุคคลและความเป็นส่วนตัวของเจ้าของข้อมูลได้ เช่น หากปัญญาประดิษฐ์ถูกใช้ในการวิเคราะห์พฤติกรรมผู้ใช้งาน อาจจำเป็นต้องเข้าถึงข้อมูลส่วนบุคคลที่ละเอียดอ่อนของผู้ใช้งาน จึงเกิดคำถามสำหรับองค์กรที่ใช้งานปัญญาประดิษฐ์ว่า ข้อมูลเหล่านั้นที่ปัญญาประดิษฐ์นำไปใช้ จะถูกเก็บไว้ที่ไหนอย่างไร? บุคคลใดสามารถเข้าถึงข้อมูลเหล่านั้นได้? และเมื่อไม่จำเป็นต้องใช้ข้อมูลอีกต่อไป จะมีการดำเนินการอย่างไร? ดังนั้น หลายองค์กรที่มีการใช้งานปัญญาประดิษฐ์ จึงต้องปรับวิธีการทำงานให้มีความสมดุลระหว่างประโยชน์จากการใช้งานปัญญาประดิษฐ์กับความเป็นส่วนตัวของผู้ใช้งาน ซึ่งความเป็นส่วนตัวของเจ้าของข้อมูลต้องได้รับความสำคัญในทุกขั้นตอนและตลอดวงจรชีวิตของข้อมูลทั้งหมด ตั้งแต่การรวบรวมข้อมูล การประมวลผล การเข้าถึงข้อมูล ไปจนถึงการกำจัดข้อมูล โดยไม่ลดทอนประโยชน์ของข้อมูลสำหรับการใช้งานปัญญาประดิษฐ์

[10] European data protection supervisor, Artificial Intelligence, available at https://www.edps.europa.eu/data-protection/our-work/subjects/artificial-intelligence_en (last accessed 20/07/2024)

2.2 ข้อกังวลในเรื่องความน่าเชื่อถือและความแม่นยำ[11]

แม้ว่าระบบปัญญาประดิษฐ์ จะสามารถประมวลผลข้อมูลจำนวนมหาศาลได้อย่างรวดเร็วก็ตาม แต่ก็ยังไม่สามารถรับประกันความถูกต้องสมบูรณ์แบบได้ทั้งหมด โดยผลบวกลวงและผลลบลวงยังสามารถเกิดขึ้นได้ และอาจทำให้ภัยคุกคามบางประเภทถูกมองข้าม กล่าวคือ ประสิทธิภาพของอัลกอริธึมนั้น ขึ้นอยู่กับคุณภาพของข้อมูลที่นำเข้าทั้งในกรณีของปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง ดังนั้นองค์กรต่างๆ จึงต้องให้ความสำคัญในกระบวนการจัดเตรียมข้อมูล เพื่อจัดระเบียบและทำความสะอาดชุดข้อมูลให้มีความน่าเชื่อถือและแม่นยำมากที่สุด ในทางกลับกัน หากข้อมูลมีปัญหาหรือการจัดการข้อมูลไม่เหมาะสม ย่อมส่งผลกระทบต่อการฝึกโมเดลปัญญาประดิษฐ์และกระทบต่อความแม่นยำของผลลัพธ์ที่ได้ ซึ่งข้อมูลการฝึกที่มีข้อบกพร่องเพียงเล็กน้อย อาจทำให้ความแม่นยำของปัญญาประดิษฐ์คลาดเคลื่อนอย่างมีนัยสำคัญ และมีผลต่อการใช้งาน

2.3 ข้อกังวลด้านขาดความโปร่งใส[12]

ระบบปัญญาประดิษฐ์ โดยเฉพาะโมเดลการเรียนรู้เชิงลึก มักทำหน้าที่เป็นกล่องดำที่ยากที่จะเข้าใจว่าระบบเหล่านี้มีกระบวนการคิดอย่างไรจนได้มาซึ่งผลลัพธ์ของการตัดสินใจหรือการคาดการณ์ที่เฉพาะเจาะจงได้ ซึ่งหากไม่มีความโปร่งใส การตัดสินใจของระบบปัญญาประดิษฐ์และตรวจสอบความถูกต้องจะกลายเป็นเรื่องยาก โดยเฉพาะอย่างยิ่ง เมื่อเป็นเรื่องเกี่ยวกับภัยคุกคามหรือความปลอดภัย นอกจากนี้ ระบบปัญญาประดิษฐ์อาจสร้างผลบวกลวง หรือผลลบลวง ที่อาจทำให้ทีมรักษาความปลอดภัยมีการทำงานผิดพลาดได้ การขาดความโปร่งใสทำให้ยากต่อการปรับแต่งโมเดลปัญญาประดิษฐ์ ปรับปรุงความแม่นยำ และแก้ไขปัญหาที่แท้จริง ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์จำเป็นต้องสามารถเข้าใจสาเหตุของข้อผิดพลาด และตรวจสอบกระบวนการตัดสินใจของระบบปัญญาประดิษฐ์เพื่อป้องกันภัยคุกคามทางไซเบอร์ที่มีการพัฒนาอย่างต่อเนื่อง

2.4 ข้อกังวลด้านการฝึกอบรมและความลำเอียงของอัลกอริทึม[13]

---

[11] Zihao Li, Accuracy of training data and model outputs in Generative AI: CREATe Response to the Information Commissioner's Office (ICO) Consultation, CREATe Centre, School of Law, University of Glasgow, p.3-5

[12] Kassidy Kelly, Solving the AI black box problem through transparency, 16 August 2021, available at https://www.techtarget.com/searchenterpriseai/feature/How-to-solve-the-black-box-AI-problem-through-transparency (last accessed 20/07/2024)

[13] IBM Data and AI Team, Shedding light on AI bias with real world examples, available at https://www.ibm.com/blog/shedding-light-on-ai-bias-with-real-world-examples/ (last accessed 20/07/2024)

การทำงานของปัญญาประดิษฐ์อาจเกิดอคติได้ โดยปัจจัยสำคัญสองประการที่อาจก่อให้เกิดอคติสำหรับปัญญาประดิษฐ์ ได้แก่ “ข้อมูลการฝึกอบรม” และ “ความลำเอียงของอัลกอริทึม” แต่ละส่วนมีรายละเอียด ดังนี้

-ข้อมูลการฝึกอบรม: เมื่อข้อมูลที่ใช้ในการฝึกอัลกอริธึมปัญญาประดิษฐ์ และการเรียนรู้ของเครื่อง (ML) ไม่หลากหลายหรือไม่ครอบคลุมภัยคุกคามทั้งหมด อัลกอริธึมอาจทำงานผิดพลาดและมีอคติได้ เช่น มองข้ามภัยคุกคามบางอย่าง หรือระบุพฤติกรรมที่ไม่เป็นอันตรายว่าเป็นอันตราย กรณีนี้มักเกิดจากชุดข้อมูลการฝึกอบรมที่ผิดพลาด ตัวอย่างเช่น หากนักพัฒนาปัญญาประดิษฐ์ เชื่อว่าแฮกเกอร์จากรัสเซียเป็นภัยคุกคามใหญ่ที่สุดสำหรับบริษัทในสหรัฐฯ โมเดลปัญญาประดิษฐ์จะถูกฝึกอบรมด้วยข้อมูลที่เน้นภัยคุกคามจากภูมิภาครัสเซียเป็นหลัก ทำให้อาจมองข้ามภัยคุกคามจากภูมิภาคอื่นๆ หรือภัยคุกคามที่มาจากภายในประเทศ

-ความลำเอียงของอัลกอริทึม: อัลกอริธึมปัญญาประดิษฐ์เองก็สามารถทำให้เกิดอคติได้เช่นกัน ตัวอย่างเช่น หากระบบใช้เทคนิคการจับคู่รูปแบบ (pattern matching) เพื่อตรวจจับภัยคุกคาม อาจเกิดผลบวกลวงเมื่อกิจกรรมที่ไม่เป็นอันตรายตรงกับรูปแบบ ซึ่งอัลกอริธึมที่สร้างผลบวกลวงเช่นนี้ อาจนำไปสู่การแจ้งเตือนที่ไม่ถูกต้อง นอกจากนี้ ระบบปัญญาประดิษฐ์ที่ใช้การจับคู่รูปแบบยังอาจล้มเหลวในการตรวจจับความภัยคุกคามที่มีสัญญาณเพียงเล็กน้อย ทำให้เกิดผลลบลวงและภัยคุกคามที่ไม่ถูกตรวจพบ

อคติที่เกิดขึ้นจากทั้งข้อมูลการฝึกอบรมและความลำเอียงของอัลกอริทึม หากไม่ได้รับการแก้ไข อาจนำไปสู่การตรวจจับภัยคุกคามที่ไม่แม่นยำ การแจ้งเตือนที่ไม่ตรงกับความเป็นจริง และเพิ่มความเสี่ยงต่อภัยคุกคามใหม่และที่กำลังพัฒนาขึ้น นอกจากนี้ ยังอาจเกิดความเสี่ยงทางกฎหมายและข้อบังคับต่างๆ ที่เกี่ยวข้องได้

จากข้อมูลที่นำเสนอข้างต้น เห็นได้ว่าปัญญาประดิษฐ์มีคุณประโยชน์อย่างมากในวงการความมั่นคงปลอดภัยทางไซเบอร์ ขณะที่ในอีกด้านหนึ่งก็ปรากฏความเสี่ยงในหลายประเด็นอย่างไม่อาจคาดหมายได้เช่นกัน ดังนั้น องค์กรที่นำปัญญาประดิษฐ์มาใช้ ควรจะต้องเรียนรู้การใช้งานปัญญาประดิษฐ์ให้สอดคล้องกับวิถีทางธุรกิจ และสอดคล้องกับความปลอดภัยทางไซเบอร์ในเวลาเดียวกัน และรวมถึงกการพัฒนาความเชี่ยวชาญของบุคคลากรควบคู่กันไปด้วย เนื่องจากการสร้างทีมรักษาความปลอดภัยทางไซเบอร์ที่เจ้าหน้าที่ที่เป็นมนุษย์ทำงานร่วมกับเทคโนโลยีปัญญาประดิษฐ์ถือเป็นสิ่งสำคัญยิ่ง เพื่อเพิ่มประสิทธิภาพการทำงานได้อย่างมีประสิทธิภาพและต่อเนื่อง ขณะที่หลายองค์กรอาจนำโซลูชันความ

ปลอดภัยทางไซเบอร์ที่มีปัญญาประดิษฐ์เป็นส่วนประกอบในรูปแบบสำเร็จรูปมาใช้ กรณีนี้ควรดำเนินการประเมินความแข็งแกร่งของโมเดลปัญญาประดิษฐ์และการรักษาความเป็นส่วนตัวด้านข้อมูลขององค์กร ไม่ว่าจะเป็นการทดลองความแข็งแกร่งของความมั่นคงปลอดภัยของโซลูชัน หรือการประเมินว่าโซลูชันดังกล่าวทำงานร่วมกับโครงสร้างพื้นฐานด้านความปลอดภัยทางไซเบอร์ที่มีอยู่ได้ดีเพียงใด และสอดคล้องกับข้อกำหนดด้านความปลอดภัยขององค์กร ตลอดจนกฎระเบียบต่างๆ หรือไม่
