การมาถึงของ AI Security

วิชญ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา แห่งมหาวิทยาลัยธรรมศาสตร์

บทความในตอนนี้ ผมจะกล่าวถึง**บทบาทของเทคโนโลยีปัญญาประดิษฐ์หรือ** AI (Artificial Intelligence) ที่ในปีนี้เราจะได้เห็นว่า**จะมีอิทธิพลต่อทิศทางในการพัฒนา และนำเอาเทคโนโลยีมาประยุกต์ใช้งานในองค์การเป็นอย่างมาก** โดยเฉพาะอย่างยิ่งในเรื่องที่คนในแวดวง IT ให้ความสนใจในขณะนี้นั่นคือ เรื่องการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ที่ปัจจุบันไม่ได้เป็นเพียงแค่ทฤษฎีหรือการวิจัยทดลอง แต่อยู่ในขั้นที่สามารถนำมาประยุกต์ใช้งานได้จริง และมีความน่าเชื่อถือ จนองค์การชั้นนำที่พัฒนา solution ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศดำเนินการพัฒนาจนกลายเป็นผลิตภัณฑ์ และนำเสนอในตลาด

ก่อนอื่นเรามาทำความเข้าใจสถานการณ์ของ AI ในปัจจุบันกันก่อน ผมขอยกเอาเนื้อหาจากหนังสือ AI Superpowers ที่เขียนโดย Dr.Kai-Fu Lee ท่านจบปริญญาเอกด้าน AI จากมหาวิทยาลัย Carnegie Mellon มีประสบการณ์เคยทำงานที่องค์การ IT ชั้นนำระดับโลก อาทิ Apple, Microsoft ดำรงตำแหน่งประธานของ Google China และปัจจุบันเป็น CEO ของ Sinovation Ventures องค์การด้านการลงทุนที่เน้นพัฒนาเทคโนโลยีแห่งอนาคตของจีน ทำให้ Dr.Kai-Fu Lee กลายเป็นผู้ทรงอิทธิพลด้าน AI ของจีน

Dr.Kai-Fu Lee กล่าวไว้ในหนังสือว่า การพัฒนา AI ว่าในปัจจุบันได้ผ่านขั้นตอนวิจัยที่มีความยุ่งยากไปแล้ว ขั้นต่อไปคือการ

ที่ผู้ประกอบการนำมาปรับใช้กับธุรกิจ ซึ่งปัจจุบันองค์การด้านเทคโนโลยีชั้นนำของโลกทั้งในอเมริกา และในจีน ได้มีการประยุกต์ใช้งาน AI กันอย่างเต็มรูปแบบ อาทิ Amazon, Microsoft, Google, Facebook, Alibaba, Tencent, Baidu เป็นต้น ผลจากการดำเนินการนี้ ทำให้ตำแหน่ง AI Engineer เป็นที่ต้องการมากขึ้นในตลาดแรงงาน และมีการเปลี่ยนรูปแบบจาก The Age of Expertise มาเป็น The Age of Data กล่าวคือ เปลี่ยนกลยุทธ์การแข่งขันที่ให้ความสำคัญกับผู้เชี่ยวชาญมาสู่ยุคที่ให้ความสำคัญกับข้อมูลหรือ Big Data มากขึ้น โดย Dr.Kai-Fu Lee กล่าวว่าปัจจัยความสำเร็จของ AI มีอยู่ 3 ประการ คือ

1. Big Data
2. Computing Power
3. AI Algorithm Engineer

เนื่องจากเทคโนโลยี AI ต้องอาศัยการทำงานกับข้อมูลจำนวนมาก ดังนั้นการพัฒนา AI ในระยะยาวจะนำไปสู่รูปแบบของการผูกขาดของบางองค์การ เพราะยิ่งมีข้อมูลมากยิ่งทำให้ AI สามารถพัฒนาประสิทธิภาพได้เพิ่มมากขึ้น ยิ่งถ้าองค์การสามารถขยายข้อมูลได้อย่างต่อเนื่อง จะส่งผลให้องค์การใหม่ๆ เข้ามาทำการแข่งขันได้ยากขึ้น ซึ่งมีการคาดการณ์ไว้ว่า ภายในปี ค.ศ.2030 AI จะช่วยสร้างมูลค่าเพิ่มให้เศรษฐกิจโลกถึง 15.7 ล้านล้านเหรียญ แต่ 70% ของมูลค่าดังกล่าวนี้ จะตกไปอยู่กับจีน และสหรัฐอเมริกา ทำให้ประเทศที่กำลังพัฒนาจะมีความสามารถในการแข่งขันที่ลดลง เพราะว่าจุดแข็งเดิมของประเทศกำลังพัฒนาคือเรื่องแรงงานที่มีราคาถูก จะถูกทดแทนด้วยการทำงานของเครื่องจักรที่ขับเคลื่อนด้วย AI แทนแรงงานคน ในอนาคต AI จึงส่งผลกระทบในระยะยาวทำให้ความเหลื่อมล้ำสูงขึ้น งานในสำนักงานโดยเฉพาะเรื่องของบัญชี การคำนวณภาษี การวิเคราะห์กฎหมาย หรือแม้แต่แรงงานในโรงงานจะถูกทดแทนด้วยหุ่นยนต์ และยังสามารถส่งมอบบริการบางอย่างให้ผู้ใช้งานจากทั่วโลกผ่านทางเครือข่าย Internet ได้ในทันที ซึ่งยกเว้นเฉพาะกับงานที่มีความละเอียด และไม่แน่นอน ต้องใช้คนในการพิจารณาตัดสินใจ

นอกจากนี้ Dr.Kai-Fu Lee ได้กล่าวถึง Online-Merge-Offline โดยเทคโนโลยี AI จะเป็นตัวประสานให้ประสบการณ์ Online และ

Offline ของผู้ใช้งานกลมกลืนกันผ่านอุปกรณ์พวก mobile device ต่างๆ ซึ่ง Offline ก็คือการบริโภคหรือใช้งานที่ตัวสินค้า ผลิตภัณฑ์ ทั้งอาหาร เครื่องแต่งกาย อุปกรณ์อำนวยความสะดวก ที่อยู่อาศัย การเดินทาง เป็นต้น ส่วน Online คือการส่งมอบบริการของสินค้าผลิตภัณฑ์ รวมถึงการบริหารจัดการด้านข้อมูล ประวัติต่างๆ ที่เกิดจากการใช้งานสินค้า ผลิตภัณฑ์ เหล่านั้น แล้วนำมาใช้ในการพัฒนาปรับปรุงประสิทธิภาพ

จากเนื้อหาที่ Dr.Kai-Fu Lee ได้กล่าวไว้ทำให้เห็นถึงศักยภาพของ AI และทิศทางของเทคโนโลยี ซึ่งในมุมของความสามารถในการวิเคราะห์ข้อมูลที่มีความซับซ้อนได้อย่างรวดเร็ว AI มีความโดดเด่นเป็นอย่างมาก ซึ่งสามารถให้ผลการวิเคราะห์ที่แม่นยำ สามารถนำไปใช้เพื่อคาดการณ์สถานการณ์ต่างๆ ได้อย่างมีประสิทธิภาพ ดังนั้น AI จึงถูกมองเป็นเทคโนโลยีที่จะช่วยสร้างความเข้มแข็งให้กับงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ หรือ IT Security

ในแวดวงการรักษาความมั่นคงปลอดภัยทางสารสนเทศ มีการนำเอา AI เข้ามาช่วยวิเคราะห์พฤติกรรมการใช้งานระบบสารสนเทศ และระบบเครือข่าย เพื่อประเมินความน่าจะเป็นในการเกิดภัยคุกคามในเหตุการณ์ใดเหตุการณ์หนึ่ง และเลือกแนวทางในการตอบโต้ต่อภัยคุกคามนั้นๆ วิธีการนี้จะช่วยให้ AI สามารถเรียนรู้และสร้างข้อกำหนดได้ด้วยตัวเองโดยอาศัยการติดตาม และศึกษากิจกรรมต่างๆ ที่เกิดขึ้นบนเครือข่าย ยิ่ง AI อยู่ในระบบนานเท่าใด ระยะเวลาในการเรียนรู้ยิ่งมากขึ้นทำให้การแจ้งเตือนภัยคุกคามมีความแม่นยำขึ้น

ฉบับหน้ามาดูตัวอย่างการประยุกต์ใช้ AI เพื่อใช้สนับสนุนงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

อ่านต่อฉบับหน้า