บทความวิจัย

แนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่

THE GUIDELINES FOR COOPERATION BETWEEN PUBLIC SECTOR AND PRIVATE SECTOR IN CYBER SECURITY USING BIG DATA MANAGEMENT SYSTEMS

ธนบวร สิริคุณากรกุล[1], และตรีเนตร ตันตระกูล
Tanaboworn Sirikunakornkun[1], Treenet Tuntrakul
มหาวิทยาลัยเวสเทิร์น
Western University
E-mail: s.tanaboworn@gmail.com[1]

Received 11 June 2023; **Revised** 30 August 2024**; Accepted** 30 August 2024.

บทคัดย่อ

งานวิจัยครั้งนี้มีจุดมุ่งหมายเพื่อศึกษาแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ เป็นการวิจัยเชิงคุณภาพ โดยการสัมภาษณ์เชิงลึก (In-depth Interview) จำนวน 19 คน และการประชุมสนทนากลุ่ม (Focus Group) จำนวน 13 คน จากผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ และผู้มีหน้าที่เกี่ยวข้องโดยตรงในการป้องกันภัยคุกคามทางไซเบอร์และการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) โดยใช้ข้อมูลปฐมภูมิ (Primary Data)

ผลการศึกษาพบว่า ภาครัฐได้ระบบการจัดการฐานข้อมูลขนาดใหญ่ (Big Data) ที่เหมาะสม สามารถตรวจสอบภัยคุกคามไซเบอร์ได้รวดเร็วโดยการใช้ระบบบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) ภาคเอกชนได้ข้อมูลขนาดใหญ่ (Big Data) มาบริหารจัดการ ทำให้งานเกิดประสิทธิภาพในการป้องกันภัยคุกคามไซเบอร์ยกระดับความพร้อมในการรับมือกับความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ การใช้ AI (Artificial Intelligence) ในการบริหารจัดการข้อมูล ตัดข้อกังวลเรื่องการรักษาความลับข้อมูลออกไป สามารถรักษามาตรฐานได้โดยไม่มีความสัมพันธ์ระหว่างบุคคลในการแสวงหาผลประโยชน์จาก Big Data เข้ามาเกี่ยวข้อง ต้องมีการบูรณาการความร่วมมือระหว่างภาครัฐและเอกชน เพื่อยกระดับความพร้อมในการรับมือกับความมั่นคงปลอดภัยไซเบอร์ การนำกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ไปใช้ ควรมีการประชาสัมพันธ์ให้ประชาชนและทุกภาคส่วนที่เกี่ยวข้องทำความเข้าใจอย่างแท้จริงเกี่ยวกับวัตถุประสงค์ ประโยชน์ และผลกระทบที่จะตามมาของการนำกฎหมายฉบับนี้มาใช้

คำสำคัญ: แนวทางความร่วมมือ; การรักษาความมั่นคงปลอดภัยไซเบอร์; การบริหารจัดการข้อมูลขนาดใหญ่

Abstract

The objectives of this research were to study the guidelines for cooperation between public sector and private sector in cyber security using big data management systems. It is a qualitative research by in-depth interview with 19 people and focus group meeting of 13 people

from qualified persons, experts and people who directly get involved in cyber threat prevention and big data management by using primary data.

The research results were found that the public sector gets an appropriate big data management system that is able to detect cyber threats quickly by using a big data management system. The private sector gets big data for management resulting in effective protection against cyber threats. Enhance the readiness to deal with cyber security using a big data management system. Using AI (artificial intelligence) to manage information. Eliminate concerns about data confidentiality. Be able to maintain the standard without interpersonal involvement in the exploitation of big data. Must have an integration of cooperation between the public sector and private sector. To enhance the readiness for dealing with cyber security. Implementing cyber security related laws using big data management systems should have a public relations to the public and all relevant sectors. Truly understand about the objectives, benefits and consequences of the adoption of this law.

Keywords: The Guidelines for Cooperation; Cyber Security; Big Data Management

บทนำ

ด้วยสภาพแวดล้อมปัจจุบันมีการเปลี่ยนแปลงอย่างรวดเร็ว กระแสความตื่นตัวที่มาพร้อมกับการเปลี่ยนผ่านสู่โลกออนไลน์ที่เปลี่ยนแปลงสังคมรอบตัวของเราไปอย่างเห็นได้ชัด เทคโนโลยีมีการพัฒนาอย่างก้าวกระโดด ส่งผลให้เกิดภัยคุกคามต่อความมั่นคงของชาติซึ่งมีความอ่อนไหวมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งภัยคุกคามทางไซเบอร์ ในช่วงของการเปลี่ยนผ่านและการขับเคลื่อนองค์กรในยุคปัจจุบัน จะเห็นว่าไม่ใช่การ “ค่อย ๆ เปลี่ยน” แต่อย่างใด หากจะต้องเร่งและทำให้เร็วเพื่อให้สามารถปรับตัวทันตามกระแสที่โถมเข้ามา (Wongreanthong, N.)

ภายในองค์กรต่าง ๆ ของหน่วยงานภาครัฐกำลังเคลื่อนเข้าสู่รูปแบบดิจิทัล อุปกรณ์ดิจิทัลต่าง ๆ ที่เชื่อมต่อกับอินเทอร์เน็ตมีจำนวนมากขึ้น ซึ่งเข้ามามีบทบาทสำคัญในการทำงานของหน่วยงานต่าง ๆ ส่งผลให้เกิดข้อมูลจำนวนมหาศาล (Big Data) ข้อมูลมีจำนวนใหญ่ขึ้น นำมาซึ่งโอกาสใหม่ ๆ ตัวอย่างเช่น ปัจจุบันได้มีการใช้งานข้อมูลขนาดใหญ่ (Big Data) และปัญญาประดิษฐ์ (Artificial Intelligent : AI) มาเพิ่มประสิทธิภาพการทำงานในองค์กร โดยแนวโน้มของปริมาณข้อมูลมีการเพิ่มขึ้นเป็นอย่างมาก อันทำให้เกิดความเสี่ยงต่อการรักษาความปลอดภัยของข้อมูล และประเด็นที่สำคัญคืออาชญากรทางไซเบอร์ หรือแฮกเกอร์ ก็มีการพัฒนาเทคนิคและรูปแบบการโจมตีด้วยเทคโนโลยีสมัยใหม่อย่าง AI ด้วยเช่นกัน

พัฒนาการและการเปลี่ยนแปลงของระบบไอซีทีได้ส่งผลกระทบต่อกิจการและการดำเนินงานทางการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยาของทุกประเทศในโลกเป็นอย่างมาก ผลจากการพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีในหลายทศวรรษที่ผ่านมา ทำให้เกิดการปฏิวัติสารสนเทศ (Information Revolution) ซึ่งเกี่ยวข้องกับการประมวลผลและการกระจายสารสนเทศอย่างกว้างขวาง จนนำมาสู่การพัฒนาในสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดด จนก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “โลกไซเบอร์”

(Cyberspace) ด้วยเหตุนี้ ความมั่นคงแห่งชาติ (National Security) จึงได้รับผลกระทบจากการปฏิวัติและปรากฏการณ์ของโลกไซเบอร์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “ความมั่นคงด้านไซเบอร์” (Cyber Security) ในบริบทของความมั่นคงแห่งชาติมากขึ้น (Arunrangsri ,R.,2018)

จากยุทธศาสตร์ชาติ พ.ศ. 2561-2580 (Srimuangkanjana, C., 2018) ยุทธศาสตร์ชาติด้านความมั่นคง ประเด็นข้อที่ 3 การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ เพื่อยกระดับขีดความสามารถของกองทัพและหน่วยงานด้านความมั่นคง โดย 1) การพัฒนาระบบงานข่าวกรองแห่งชาติแบบบูรณาการอย่างมีประสิทธิภาพ 2) การพัฒนาและผนึกพลังอำนาจแห่งชาติ กองทัพและหน่วยงานความมั่นคง รวมทั้งภาครัฐและภาคประชาชน ให้พร้อมป้องกันและรักษาอธิปไตยของประเทศ และเผชิญกับภัยคุกคามได้ทุกมิติทุกรูปแบบและทุกระดับ และ 3) การพัฒนาระบบเตรียมพร้อมแห่งชาติและการบริหารจัดการภัยคุกคามให้มีประสิทธิภาพ ซึ่งจากยุทธศาสตร์ดังกล่าวเป็นการเตรียมความพร้อมของกองทัพไทยเพื่อให้ก้าวทันต่อสถานการณ์การเปลี่ยนแปลงที่รุนแรงอย่างเฉียบพลันทางเทคโนโลยีดิจิทัล (Digital Disruption) ในขณะที่กรอบและกติการะหว่างประเทศเป็นไปตามพลวัตของโลก ตลอดจนให้สอดคล้องกับบริบทการเปลี่ยนแปลงทั้งในประเทศและต่างประเทศ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 (Ministry of Digital Economy and Society, n.d.) โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

ความร่วมมือระหว่างภาครัฐและภาคเอกชนเพื่อรองรับการเปลี่ยนแปลง ต้องมีความพร้อมในการป้องกันและแก้ไขปัญหาความมั่นคงไซเบอร์ ในอดีตการทำงานของภาครัฐต้องการข้อมูลเพื่อการตัดสินใจ สิ่งที่ภาครัฐต้องทำคือการสร้างระบบฐานข้อมูลขึ้นมา และสร้างวิธีการจัดเก็บข้อมูลขึ้นมาเอง ปัจจุบันหลาย ๆ หน่วยงานหรือตัวบุคคลแต่ละคนมีการเปิดเผยข้อมูล (Open Data) ผ่านระบบออนไลน์ ทั้งในรูปแบบ เว็บไซต์, บล็อก, สื่อสังคมต่าง ๆ ทำให้ข้อมูลมีการเปลี่ยนแปลง เคลื่อนที่อย่างรวดเร็วแบบทันทีทันใด มีลักษณะกระจัดกระจายไร้รูปแบบและมีขนาดมหาศาล (Big Data) เป็นข้อมูลที่มีขนาดใหญ่และยิ่งมีการเปิดเผยข้อมูลกันมากขึ้น ขนาด ขอบเขตของข้อมูลที่มีขนาดใหญ่ (Big Data) ก็ยิ่งขยายใหญ่มากขึ้นเรื่อย ๆ

จากเหตุผลดังกล่าว ผู้วิจัยจึงเห็นความสำคัญของแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ การวิเคราะห์ข้อมูลขนาดใหญ่และการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์ การตรวจสอบข้อมูลเชิงรุกโดยสังเกตจากความผิดปกติของข้อมูล เพื่อที่จะสามารถหาวิธีการป้องกันหรือแก้ปัญหาได้ทันเวลา และแนวทางการบูรณาการการทำงานร่วมกันระหว่างภาครัฐและภาคเอกชนเพื่อดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และยุทธศาสตร์ชาติ พ.ศ. 2561–2580 ยุทธศาสตร์ชาติด้านความมั่นคง รวมทั้งการนำแผนหลักที่เกี่ยวข้องเข้ามาสนับสนุนและเอื้ออำนวยประโยชน์ในการบริหารจัดการข้อมูลขนาดใหญ่ของหน่วยงานราชการ

วัตถุประสงค์การวิจัย

1. ศึกษาสถานการณ์ภัยคุกคามทางไซเบอร์ของภาครัฐและภาคเอกชน และการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

2. ศึกษาปัญหาความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

3. ศึกษาแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

ระเบียบวิธีวิจัย

1. รูปแบบการวิจัย เป็นการวิจัยแบบผสานวิธี (Mixed Methods Research) โดยใช้วิธีการวิจัยเอกสาร (Documentary Research) สัมภาษณ์เชิงลึก (In-depth Interview) และการประชุมสนทนากลุ่ม (Focus Group) โดยใช้ข้อมูลปฐมภูมิ (Primary Data)

1) การวิจัยเอกสาร (Documentary Research) ด้วยการสังเคราะห์เอกสารทั้งในประเทศ และต่างประเทศ ศึกษาแนวคิด ทฤษฎี งานวิจัยต่าง ๆ ที่เกี่ยวข้อง ตลอดจนรายงานวิจัยเฉพาะเรื่องของกรณีศึกษาสถานการณ์ภัยคุกคามทางไซเบอร์ของภาครัฐและภาคเอกชน ภัยคุกคามและการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การดำเนินการด้านความร่วมมือของภาครัฐและภาคเอกชน

2) สัมภาษณ์เชิงลึก (In-depth Interview) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) จำนวน 19 คน ภาครัฐ ได้แก่ กรรมการผู้ทรงคุณวุฒิ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน 2 คน เจ้าหน้าที่ที่ควบคุมข้อมูลไซเบอร์ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (NT cyfence) จำนวน 2 คน เจ้าหน้าที่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (TCSD) จำนวน 6 คน เจ้าหน้าที่ศูนย์ปราบปรามอาชญากรรมทางอิเล็กทรอนิกส์ของตำรวจภูธร ภาค 4 จำนวน 5 คน ภาคเอกชน ได้แก่ Senior Employee Engagement Strategy Officer ธนาคารไทยพาณิชย์ จำกัด (มหาชน) สำนักงานใหญ่ จำนวน 1 คน บุคคลที่มีประสบการณ์ในการลักลอบปรับแก้หรือดัดแปลงโปรแกรมคอมพิวเตอร์โดยไม่ถูกต้องตามกฎหมาย จำนวน 3 คน

3) ประชุมสนทนากลุ่ม (Focus Group) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) จากผู้มีบทบาทที่สำคัญเกี่ยวกับแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ จำนวน 13 คน

2. เครื่องมือการวิจัย

1) แบบสัมภาษณ์เชิงลึก (In-depth Interview) โดยมีประเด็นคำถามที่เกี่ยวกับสภาพการณ์ ณ ปัจจุบันของภัยคุกคามไซเบอร์และการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) วิธีการรับมือกับภัยคุกคามและการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) และแนวทางที่ควรจะดำเนินการแก้ไขหรือพัฒนาความร่วมมือการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) ให้มีประสิทธิภาพเพิ่มขึ้น

2) แบบประชุมสนทนากลุ่ม (Focus Group) เพื่อใช้เก็บข้อมูลการประชุมกลุ่มเกี่ยวกับแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีเนื้อหาในการสนทนา

กลุ่ม ดังนี้ การจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ในแต่ละด้าน ปัญหาและอุปสรรคที่เกิดขึ้นในการนำพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาบังคับใช้ การดำเนินการด้านความร่วมมือของภาครัฐและภาคเอกชนในการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ และแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ ที่สามารถนำผลการวิจัยไปใช้ประโยชน์อย่างเป็นรูปธรรม

3. วิธีเก็บรวบรวมข้อมูล

1) การเก็บรวบรวมข้อมูลจากการศึกษาค้นคว้าข้อมูลจากเอกสารทางวิชาการและข้อมูลจากสื่อเทคโนโลยีสารสนเทศ

ผู้วิจัยได้ดำเนินกระบวนการในการเก็บรวบรวมข้อมูลจากการทบทวนความเป็นมาของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 แนวคิดเรื่องสงครามไซเบอร์ แนวคิดเกี่ยวกับความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน แนวคิดเรื่องความมั่นคงแห่งชาติ บทบาทของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC) การบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) งานวิจัยและวรรณกรรมที่เกี่ยวข้อง รวมทั้งข้อมูลจากแหล่งต่าง ๆ ที่เกี่ยวข้อง โดยเฉพาะแหล่งข้อมูลทางเว็บไซต์ที่ปรากฏบนอินเทอร์เน็ต เพื่อนำมาใช้เป็นแนวทางในการออกแบบหรือสร้างแบบสัมภาษณ์เชิงลึก รวมทั้งเพื่อนำมาใช้เป็นส่วนประกอบในกระบวนการวิเคราะห์และประมวลผลข้อมูลในการวิจัย

2) การเก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึก (In-depth Interview) ผู้วิจัยได้กำหนดแนวทางการเก็บรวบรวมข้อมูล โดยการติดต่อผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญที่มีหน้าที่เกี่ยวข้อง มีความสำคัญ หรือมีส่วนเกี่ยวข้องกับการวิจัยในการสัมภาษณ์อย่างเป็นทางการ และผู้วิจัยได้ดำเนินการสัมภาษณ์ โดยมีประเด็นคำถามเป็นเครื่องมือในการสัมภาษณ์ ทำการบันทึกภาพ และจดบันทึกข้อมูลของผู้ให้สัมภาษณ์ เพื่อนำมาใช้ในการตรวจสอบและตรวจทานความถูกต้องย้อนกลับในภายหลัง

3) การประชุมสนทนากลุ่ม (Focus Group) ผู้วิจัยได้กำหนดแนวทางการเก็บรวบรวมข้อมูลจาก บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ซึ่งมีบทบาทที่สำคัญในการจัดเก็บและบริหารข้อมูลขนาดใหญ่ (Big Data) ของหน่วยงานในภาครัฐ เนื่องจาก บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (National Telecom Public Company Limited) หรือที่รู้จักทั่วไปในชื่อย่อว่า เอ็นที (NT Plc.) เป็นรัฐวิสาหกิจที่ดูแลการสื่อสารโทรคมนาคมในประเทศไทยในรูปแบบบริษัทมหาชนจำกัด ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เกิดจากการควบรวมกิจการระหว่าง กสท โทรคมนาคม และทีโอที เพื่อลดการดำเนินงานที่ซ้ำซ้อนกัน และเพิ่มศักยภาพในการแข่งขัน ตามมติของคณะรัฐมนตรี โดยมีกระทรวงการคลังถือหุ้นทั้งหมด NT cyfence เป็นหน่วยงานหนึ่งใน บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) หรือ NT ทำหน้าที่ Cybersecurity Monitoring คือ บริการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ และความปลอดภัยของระบบเทคโนโลยีสารสนเทศผ่านศูนย์ปฏิบัติการ Cybersecurity Operations Center (CSOC) โดยมีผู้เชี่ยวชาญที่มีประสบการณ์ (Security Analyst) ในการวิเคราะห์ภัยคุกคามทางด้านไซเบอร์ แจ้งเตือนเหตุการณ์ภัยคุกคาม รวมถึงแนวทางในการจัดการ การแก้ไขปัญหาเบื้องต้นไปยังลูกค้า เมื่อพบเหตุการณ์ต้องสงสัย หรือเหตุการณ์ผิดปกติที่มีความเสี่ยงซึ่งอาจจะส่งผลกระทบกับความปลอดภัยทางด้านเทคโนโลยีสารสนเทศแบบ Real-time ตลอด 24 ชั่วโมง โดยประกอบไปด้วยบริการ 2 รูปแบบ ดังนี้

1. Cybersecurity Monitoring by CSOC การเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ และความปลอดภัยของระบบเทคโนโลยีสารสนเทศผ่านศูนย์ CSOC

2. Cybersecurity Monitoring by On-Site การเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ณ องค์กรของผู้ใช้บริการ

ซึ่ง NT มีความสำคัญหรือมีส่วนเกี่ยวข้องกับการวิจัยในการประชุมสนทนากลุ่ม (Focus Group) อย่างเป็นทางการ โดยผู้วิจัยได้ดำเนินการบันทึกภาพและจดบันทึกข้อมูลของผู้สนทนากลุ่ม (Focus Group) เพื่อนำมาใช้ในการตรวจสอบและตรวจทานความถูกต้องย้อนกลับในภายหลัง

ผลการวิจัย

จากวัตถุประสงค์ของงานวิจัยสามารถสรุปผลการวิจัย ดังนี้

1. ศึกษาสถานการณ์ภัยคุกคามทางไซเบอร์ของภาครัฐและภาคเอกชน และการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

ประเทศไทยถือได้ว่าเป็นหนึ่งในประเทศที่เอื้ออำนวยต่อการก่อภัยคุกคามทางไซเบอร์ เนื่องจากเป็นพื้นที่ที่ระบบสัญญาณเครือข่ายอินเทอร์เน็ตดี เมื่อมีปัญหาเรื่องภัยคุกคามไซเบอร์ควรต้องมี Cybersecurity เพื่อป้องกันความเสียหายของข้อมูล ปัญหาภัยคุกคามไซเบอร์และการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) สามารถสรุปได้ดังนี้

1) บุคลากรขาดความรู้ความเชี่ยวชาญในการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

2) การบริหารข้อมูลขนาดใหญ่ (Big Data) ยังไม่สามารถรวบรวมข้อมูลเพื่อนำมาไว้ที่ศูนย์กลางได้

3) ประเทศไทยเอื้อต่อภัยคุกคามทางไซเบอร์ เนื่องจากมีระบบสารสนเทศที่ดี ทันสมัย

4) กฎหมาย พ.ร.บ. ไซเบอร์ ฉบับปัจจุบัน ยังมีความบกพร่องหลายประการต่อการนำไปใช้

จากผลการสัมภาษณ์ Senior Employee Engagement Strategy Officer ธนาคารไทยพาณิชย์ จำกัด (มหาชน) สำนักงานใหญ่ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พบว่า ธนาคารไทยพาณิชย์ต้องมีการปรับปรุงพัฒนาระบบข้อมูล (Big Data) เพื่อสร้างความเข้มแข็งในด้านเทคโนโลยีสารสนเทศให้ครบทั้ง 3 ด้าน คือ 1) การใช้เทคโนโลยีที่เหมาะสมกับการบูรณาการในด้านเทคนิค เช่น การยืนยันตัวบุคคลอย่างบูรณาการ Hyper Converged หรือซอฟต์แวร์พัฒนาคลังข้อมูลกลาง (Big Data) 2) มีการสร้างแนวทางปฏิบัติสำหรับผู้ปฏิบัติงานเพื่อลดความเสี่ยงหรือภัยคุกคามที่มาจากความผิดพลาดของมนุษย์ 3) มีการเตรียมรับมือหรือมาตรการรองรับภัยคุกคามไซเบอร์ที่อาจจะเกิดขึ้นซึ่งจะมาในรูปแบบต่าง ๆ

วิธีรับมือกับภัยคุกคามไซเบอร์ที่ดีที่สุด คือ การกระทำหรือดำเนินกิจกรรมทางออนไลน์ต่าง ๆ ต้องใช้สติและไม่รีบร้อนในการกระทำนั้น ๆ หากจะทำต้องมั่นใจว่าปลอดภัยและไม่ส่งผลกระทบเสียหายต่อตนเองหรือผู้อื่น การนำข้อมูลเข้าในระบบต้องมีการตรวจสอบความถูกต้องของข้อมูล และจัดเก็บข้อมูลให้เป็นปัจจุบัน รวมทั้งทำการสำรองข้อมูลสำคัญไว้ในระบบออฟไลน์ พัฒนาระบบในการจัดเก็บข้อมูล กำหนดมาตรการในการเข้าถึงข้อมูล ใช้ระบบรักษาความปลอดภัยหลายรูปแบบ วิธีรับมือกับภัยคุกคามและการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) สามารถสรุปได้ดังนี้

1) การมีระบบ Cybersecurity ที่ทันสมัย เพื่อป้องกันข้อมูลรั่วไหล พร้อมรับมือกับภัยคุกคามไซเบอร์ทุกรูปแบบ

2) การระมัดระวังเรื่องข้อมูลส่วนตัวในการเผยแพร่ทางสังคมออนไลน์

3) จัดทำฐานข้อมูลภัยคุกคามเพื่อวิเคราะห์ และใช้เป็นกรณีศึกษา ป้องกันไม่ให้เกิดขึ้นอีก

4) การตั้งรหัสผ่านในการใช้งานอินเทอร์เน็ตที่รัดกุม

5) การศึกษาหาความรู้ วิธีการรับมือกับภัยคุกคามทางไซเบอร์ตลอดเวลา

6) การจัดแบ่งข้อมูลขนาดใหญ่ (Big Data) ให้เป็นระบบ

การจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ในแต่ละด้าน สรุปได้ดังนี้

1) ขั้นตอนการติดตามและตรวจสอบ

เมื่อเกิดภัยคุกคามทางด้านไซเบอร์ในภาพรวมของประเทศ จึงจำเป็นต้องมีระบบจัดการปฏิบัติการด้านข่าวสาร (Information Operation : IO) ระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) เพื่อกรองข่าวมาเป็นภัยคุกคามทางด้านไซเบอร์ เมื่อตกผลึกต้องมีการกระจายข่าวสารดังกล่าวไปยังหน่วยงานภาครัฐและภาคเอกชนด้านไซเบอร์ว่าภัยคุกคามที่เกี่ยวข้องมีผลกระทบต่อหน่วยงานของตนหรือไม่ แล้วนำข้อมูลมาแบ่งปันกัน

2) แนวทางการแจ้งเตือนเมื่อพบภัยคุกคาม

ภาครัฐและภาคเอกชนย่อมต้องมีระบบการจัดเก็บข้อมูลด้านภัยคุกคามทางไซเบอร์ของตนเอง หลังจากตรวจพบภัยคุกคามอาจจะต้องสร้างระบบการบริหารจัดการข้อมูลในการแจ้งเตือนเมื่อพบภัยคุกคามร่วมกัน โดยรู้เท่าทันสถานการณ์ภัยคุกคามที่ตรวจพบและนำไปสู่แนวทางป้องกันภัยคุกคามที่เกิดขึ้น

3) การแลกเปลี่ยนข้อมูลการโจมตีจากภัยคุกคาม

ระบบตรวจสอบภัยคุกคามทางด้านไซเบอร์ที่ภาครัฐและภาคเอกชนมีนั้น เมื่อระบบตรวจพบการโจมตีทางไซเบอร์ในแต่ละประเภท ควรมีระบบกลางที่ร่วมแบ่งปันข้อมูลการโจมตีทางด้านไซเบอร์ในแต่ละประเภท โดยมีเนื้อหาระดับความรุนแรง พฤติกรรมของภัยคุกคาม รูปแบบการโจมตีและ/หรือข้อมูลที่เกี่ยวกับการโจมตีด้านไซเบอร์ในแต่ละประเภทอื่น ๆ

4) การเตรียมความพร้อมและประสานความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่

ควรมีความร่วมมือระดับนโยบาย โดยตั้งเป้าหมายที่สอดคล้องระหว่างภาครัฐและภาคเอกชน และต้องจัดให้มีกลไกที่ทำงานร่วมกันระหว่างภาครัฐและภาคเอกชน โดยมีกฎหมายเป็นตัวควบคุม

5) ประสิทธิภาพในการดำเนินงานของหน่วยงานที่มีหน้าที่รับผิดชอบ

ประสิทธิภาพในการดำเนินงานของหน่วยงานที่มีหน้าที่รับผิดชอบ ประสิทธิภาพย่อมเกิดจากการดำเนินงานด้วยกลยุทธ์ที่ดี แผนงานที่ดี และระบบการจัดการที่ดี ถ้าทุกอย่างครบถ้วนสมบูรณ์ หน้าที่ความรับผิดชอบที่แต่ละหน่วยงานต้องปฏิบัติย่อมมีประสิทธิภาพ อันจะมีประโยชน์ต่อการทำงานร่วมกันต่อไป

2. ศึกษาปัญหาความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

ผลการวิจัยนี้ชี้ให้เห็นว่าการขาดแคลนบุคลากรด้านไซเบอร์สำคัญอย่างยิ่งในการรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารระดับสูงต้องให้ความสำคัญเป็นลำดับต้น ๆ และต้องลงมาให้ความร่วมมือกับผู้บริหารในทุกระดับขององค์กร โดยองค์กรจะต้องมีการบูรณาการตั้งแต่นโยบาย เชื่อมโยงไปสู่แนวทางความร่วมมือสอดคล้องกับกลยุทธ์หลักขององค์กรและแผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์

การพัฒนาระบบข่าวกรองไซเบอร์ให้มีประสิทธิภาพสูงขึ้น แลกเปลี่ยนเรียนรู้กันระหว่างภาครัฐและภาคเอกชน ซึ่งผู้บริหารทุกระดับจะต้องให้ความร่วมมือกัน ข้อมูลที่เป็นระบบฐานข้อมูลขนาดใหญ่ (Big Data) ที่ใช้งบประมาณสูง ต้องได้รับการสนับสนุนและส่งเสริมเรื่องงบประมาณค่าใช้จ่ายในเรื่องนี้ การต่อยอดองค์ความรู้ เมื่อพัฒนาแล้วก็ต้องมีแผนในการดำเนินการอย่างต่อเนื่อง หลังจากพัฒนาองค์ความรู้แล้วควรสร้างนวัตกรรมร่วมกันจึงจะเกิดความคุ้มค่าต่อการลงทุน เพื่อการนำระบบฐานข้อมูลขนาดใหญ่ (Big Data) มาใช้ในเรื่องของการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อไป

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีสาระสำคัญ คือ การจัดตั้งคณะกรรมการระดับนโยบายในภาพรวมขึ้นมา ซึ่งเรียกว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (NCSC) หรือที่เรียกย่อ ๆ ว่า กมช. มีนายกรัฐมนตรีเป็นประธาน ซึ่งในส่วนนี้จะมีส่วนราชการต่าง ๆ ทั้งภาครัฐ ภาคเอกชน ประชาชน เข้ามามีส่วนเกี่ยวข้องทั้งสิ้น เมื่อกล่าวถึงตัวบทกฎหมายนั้นมีความชัดเจนมากในเรื่องของการกำหนดบทบาทของแต่ละหน่วยงาน ซึ่งปัญหาแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ คือ การเห็นความสำคัญของ พ.ร.บ. ฉบับนี้ ตลอดจนความรับผิดชอบของผู้มีส่วนได้ส่วนเสีย (Stakeholder) ซึ่งภาครัฐและภาคเอกชนควรเริ่มต้นด้วยหลักการสนับสนุนที่ว่า ผู้มีส่วนเกี่ยวข้องทั้งหมดต้องเข้าใจหลักสำคัญของ พ.ร.บ. ฉบับดังกล่าว ทั้งนี้ หน่วยงานภาครัฐและภาคเอกชนยังขาดทักษะความรู้เกี่ยวกับขั้นตอนที่ต้องปฏิบัติงานร่วมกันในการป้องกัน ภัยคุกคามทางไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) อีกทั้งยังขาดงบประมาณและบุคลากรที่มีความรู้ความสามารถในการพัฒนาความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์

3. ศึกษาแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

ควรมีการนำข้อมูลมาแบ่งชั้นความสำคัญ แล้วส่งไปยังส่วนกลางเพื่อให้มีการบริหารจัดการข้อมูล ทำการวิเคราะห์ข้อมูล (Big Data) ด้วยเทคโนโลยีที่มีประสิทธิภาพสูง ใช้ AI ในการวิเคราะห์ข้อมูล เพิ่มความรู้พัฒนาบุคลากรในองค์กรให้มีความรู้ความสามารถตลอดเวลา เพราะข้อมูลมีการเปลี่ยนแปลงไปตามเทคโนโลยีที่ไม่หยุดนิ่ง แนวทางที่ควรจะดำเนินการแก้ไขหรือพัฒนาการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) ให้มีประสิทธิภาพเพิ่มขึ้น สามารถสรุปได้ดังนี้

1) การพัฒนาคนให้มีความรู้ ความเข้าใจในการพัฒนาระบบ Cybersecurity จะทำให้ข้อมูลขนาดใหญ่ (Big Data) มีความเสถียรและมีประสิทธิภาพในการใช้งาน

2) หน่วยงานแต่ละแห่งทำงานแยกข้อมูล (Big Data) ที่สามารถเปิดเผยได้ออกมาไว้ส่วนกลาง

การปรับเปลี่ยนความคิด วัฒนธรรมขององค์การในเรื่องการแชร์ข้อมูล การหวงข้อมูล ต้องทำความเข้าใจในองค์กร ประชุมร่วมกันภายในองค์กรและระหว่างองค์กร เพื่อประโยชน์ในการแชร์ข้อมูลให้ได้มาซึ่งข้อมูลที่ถูกต้อง สมบูรณ์ อีกทั้งเพื่อเรียนรู้ถึงสิทธิเสรีภาพทางไซเบอร์ของบุคลากรด้วย

เรื่องของการต่อยอดความรู้ เมื่อพัฒนาแล้วก็ต้องช่วยกันต่อยอด พัฒนาองค์ความรู้ และสร้างนวัตกรรมร่วมกันจึงจะเกิดความคุ้มค่าต่อการลงทุนในการนำระบบการจัดการฐานข้อมูลขนาดใหญ่ (Big Data) มาใช้ในเรื่องของการรักษาความมั่นคงปลอดภัยไซเบอร์

อภิปรายผล

จากวัตถุประสงค์การวิจัยมีประเด็นในการอภิปรายผลการวิจัย 3 ประเด็น ดังนี้

ประเด็นที่ 1 จากผลการศึกษาสถานการณ์ภัยคุกคามทางไซเบอร์ของภาครัฐและภาคเอกชน และการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) พบว่า ปัญหาภัยคุกคามทางไซเบอร์ของภาครัฐและภาคเอกชนมีอัตราการเพิ่มขึ้นในทุก ๆ ปี มีระดับความรุนแรงมากยิ่งขึ้น สอดคล้องกับบทความวิจัยของ กริน ธัญญวิกรม และธีระ กุลสวัสดิ์ (Thanwikrom, G., and Kulsawat, T.,a (2021) ปัญหาภัยคุกคามทางไซเบอร์ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็วและมีความซับซ้อนมากขึ้น ในประเทศไทยพบภัยคุกคามไซเบอร์ที่มีจุดประสงค์ทางการเงินในรูปแบบต่าง ๆ เช่น ฟิชชิ่งอีเมล เว็บไซต์ธนาคารปลอมเพื่อหลอกขโมยรหัสผ่านผู้ที่ใช้งานอิเล็กทรอนิกส์

แบงก์กิ้ง (E-banking) การแพร่ระบาดของ มัลแวร์เรียกค่าไถ่ (Ransomware) สายพันธุ์ต่าง ๆ ที่เข้ารหัสลับข้อมูลในเครื่องทำให้เปิดใช้งานไม่ได้ ฯลฯ ประเทศไทยเป็นประเทศที่เอื้อต่อการก่อภัยคุกคามทางไซเบอร์ เนื่องจากการมีระบบสัญญาณเครือข่ายอินเทอร์เน็ตที่ดี มีระบบการเงินการธนาคารที่สะดวก จึงตกเป็นเป้าประสงค์ของผู้ก่อการร้ายอาชญากรรมไซเบอร์ และเนื่องด้วยระบบรักษาความปลอดภัยไซเบอร์ Cybersecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ ของภาครัฐและเอกชนยังไม่มีความรัดกุมมากพอ จึงทำให้เห็นการตกเป็นเหยื่อของอาชญากรรมไซเบอร์อยู่บ่อยครั้ง การจะมีระบบรักษาความปลอดภัยไซเบอร์ Cybersecurity ที่ดีและมีประสิทธิภาพต้องใช้งบประมาณที่สูงในการดำเนินการติดตั้งระบบ

ประเด็นที่ 2 ศึกษาปัญหาความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

1. การกำหนดรูปแบบความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่

ปัจจุบันประเทศไทยได้ให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์มากขึ้น มีการดำเนินงานของหน่วยปฏิบัติหลาย ๆ หน่วย เช่น การทำงานของศูนย์ประสานความมั่นคงปลอดภัยไซเบอร์ (The Computer Emergency Response Team) หรือไทยเซิร์ต (ThaiCERT) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ช่วยในการปกป้องและประสานการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ หรือมีการดำเนินงานของกองป้องกันและปรามปรามการกระทำความผิดทางเทคโนโลยี ภายใต้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ภายใต้สำนักงานตำรวจแห่งชาติ สำนักคดีเทคโนโลยีและสารสนเทศ ภายใต้กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยี ศูนย์เทคโนโลยีสารสนเทศ ภายใต้สำนักป้องกันและปราบปรามการฟอกเงิน หรือธนาคารแห่งประเทศไทย แล้วก็ตาม แต่รูปแบบการทำงานดังกล่าวเป็นการทำงานเชิงป้องกันและตั้งรับเมื่อมีภัยคุกคามทางไซเบอร์เท่านั้น

<u>แนวทางการปฏิบัติ</u>

1) เสริมสร้างความรู้ ความเข้าใจ และประโยชน์ในการทำงานร่วมกัน ให้กับหน่วยงานที่เกี่ยวข้องเพื่อรับมือกับภัยคุกคามประเภทต่าง ๆ

2) พิจารณาการทำงานร่วมกัน จัดทำระเบียบปฏิบัติประจำหน่วยงาน ในการดำเนินงานร่วมกันระหว่างภาครัฐและภาคเอกชน เพื่อให้สามารถปฏิบัติงานร่วมกันได้อย่างมีประสิทธิภาพ และป้องกันปัญหาความสับสนในการปฏิบัติงานของแต่ละหน่วยงาน

2. การพัฒนาขีดความสามารถความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ และต่อยอดการพัฒนาในอนาคต

ภาครัฐและเอกชนต้องเตรียมความพร้อมด้านบุคลากรให้มีขีดความสามารถและประสบการณ์ที่เหมาะสม พร้อมทั้งเสริมสร้างองค์ความรู้ให้กับบุคลากร สามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามไซเบอร์ประเภทต่าง ๆ ได้อย่างมีประสิทธิภาพ

<u>แนวทางการปฏิบัติ</u>

ประสานความร่วมมือระหว่างภาครัฐและภาคเอกชน รวมถึงหน่วยงานที่เกี่ยวข้อง จัดส่งบุคลากรเข้ารับการฝึกอบรมตามหลักสูตรต่าง ๆ ทั้งหลักสูตรระยะสั้นและระยะยาว อบรมโดยผู้เชี่ยวชาญที่มีศักยภาพและความรู้ พร้อมรับรองความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ให้แก่บุคลากรที่ผ่านการฝึกอบรม เป็นการเพิ่มศักยภาพให้กับบุคลากรของหน่วยงานให้

มีความรู้และประสบการณ์ที่เหมาะสม หน่วยงานจึงต้องวางแผนพัฒนาบุคลากรและส่งเสริมให้มีการเรียนรู้ อบรมให้บุคลากรเกิดความรู้ความเข้าใจเฉพาะด้าน

3. การเตรียมการด้านงบประมาณของภาครัฐและเอกชน เพื่อรองรับการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่

การดำเนินการวิจัยและพัฒนาเทคโนโลยีทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้องในการรับมือกับภัยคุกคามไซเบอร์ยังขาดการสนับสนุนงบประมาณ ทำให้ประเทศไทยต้องพึ่งพาเทคโนโลยีจากต่างประเทศและสูญเสียงบประมาณเป็นจำนวนมาก

<u>แนวทางการปฏิบัติ</u>

ผู้บริหารของหน่วยงานทำการจัดสรรงบประมาณด้านงานวิจัยและพัฒนาเทคโนโลยีทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ โดยจัดทำเป็นแผนเร่งด่วนเพื่อรองรับกับภัยคุกคามไซเบอร์ที่จะเกิดขึ้นได้อย่างมีประสิทธิภาพ

4. การกำหนดรูปแบบความร่วมมือของภาครัฐและเอกชนให้มีความเป็นรูปธรรมในการดำเนินงาน

หน่วยงานหรือองค์กรบางแห่งยังไม่ให้ความสำคัญกับภัยคุกคามไซเบอร์ เนื่องจากยังไม่เห็นความจำเป็นหรือยังไม่เคยได้รับผลกระทบที่เกิดขึ้น จึงยังไม่ให้ความสนใจที่จะร่วมมือหรือจัดตั้งทีมงานมาดูแลโดยตรง การรักษาความมั่นคงปลอดภัยไซเบอร์มีลักษณะต่างฝ่ายต่างดำเนินการ จึงขาดการประสานความร่วมมือที่ดี ซึ่งเป็นส่วนสำคัญที่สุดของงานด้านการเฝ้าระวังและรักษาความมั่นคงปลอดภัยไซเบอร์

<u>แนวทางการปฏิบัติ</u>

1) จัดทำแผนปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ เพื่อเป็นกรอบการดำเนินงานในภาพรวม และเป็นเครื่องมือกำกับดูแล ประเมินผลการปฏิบัติงาน

2) ปรับปรุงโครงสร้างการจัดหน่วยในการรองรับภารกิจด้านความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่

5. การสนับสนุนการบูรณาการความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ โดยใช้งบประมาณในภาพรวมของประเทศมุ่งเน้นบูรณาการการใช้ประโยชน์ร่วมกันในทุกภาคส่วนที่เกี่ยวข้อง

การพัฒนาความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ มีความจำเป็นต้องใช้งบประมาณจำนวนมาก และการบริหารจัดการที่มีประสิทธิภาพ หากภาครัฐและเอกชนเป็นผู้ดำเนินการทั้งหมดอาจมีภาระด้านงบประมาณและการบริหารบุคลากร ซึ่งจำเป็นต้องมีการพัฒนาองค์ความรู้เพื่อนำไปสู่การพึ่งตนเองได้ในอนาคต สอดคล้องกับ ตรีเนตร ตันตระกูล (2018) ทำการศึกษาเรื่อง การจัดการความรู้และการพัฒนาการเรียนรู้ของผู้ใหญ่ในองค์การ พบว่า การพัฒนาองค์การให้เจริญก้าวหน้าและเป็นไปอย่างยั่งยืนและถาวรด้วยวิธีการจัดการความรู้ที่เป็นเครื่องมือที่สำคัญในการสร้างความสามารถในการพัฒนาองค์การ สร้างความสามารถในการทำงานร่วมกัน สร้างสรรค์ผลงานที่มีคุณภาพ และสร้างความสามารถในการทำงานที่ยากในระดับ “เป็นไปไม่ได้” ให้เป็นไปได้ หรือเรียกว่า เพื่อให้ได้ประสิทธิผล ซึ่งหน่วยงานที่เกี่ยวข้องทุกภาคส่วนในประเทศควรสนับสนุนด้านงบประมาณ มุ่งเน้นการบูรณาการความร่วมมือกันเพื่อเป็นการรวมการใช้ทรัพยากรส่วนกลาง เช่น บุคลากร โครงสร้างพื้นฐาน ข้อมูล ระบบงาน ที่สามารถทำงานร่วมกันได้

<u>แนวทางการปฏิบัติ</u>

สนับสนุนการจัดทำโครงการความร่วมมือของทุกภาคส่วนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ โดยใช้งบประมาณของทุกหน่วยงานที่เกี่ยวข้อง มุ่งเน้นให้มีการใช้ทรัพยากรร่วมกันอย่างมีประสิทธิภาพ สนับสนุนการบูรณาการใช้ประโยชน์จากโครงการร่วมกันในทุกภาคส่วน สร้างความเชื่อมั่นให้กับหน่วยงานที่จะเข้าร่วม เพื่อประโยชน์และความคุ้มค่าสูงสุด

ประเด็นที่ 3 ศึกษาแนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data)

การปฏิบัติภารกิจด้านความมั่นคงปลอดภัยไซเบอร์มีองค์ประกอบหลายส่วน ซึ่งแต่ละส่วนมีความจำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับงานวิจัยของ ชฎาภรณ์ สิงห์แก้ว (Singhkaew, C., 2021) พบว่า บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ รัฐบาลจำเป็นต้องใช้มาตรการทางกฎหมาย รวมถึงการกำกับดูแลตนเอง และการกำกับดูแลร่วมกันของทุกภาคส่วน ได้แก่ ภาครัฐ ภาคเอกชน และภาคประชาสังคม

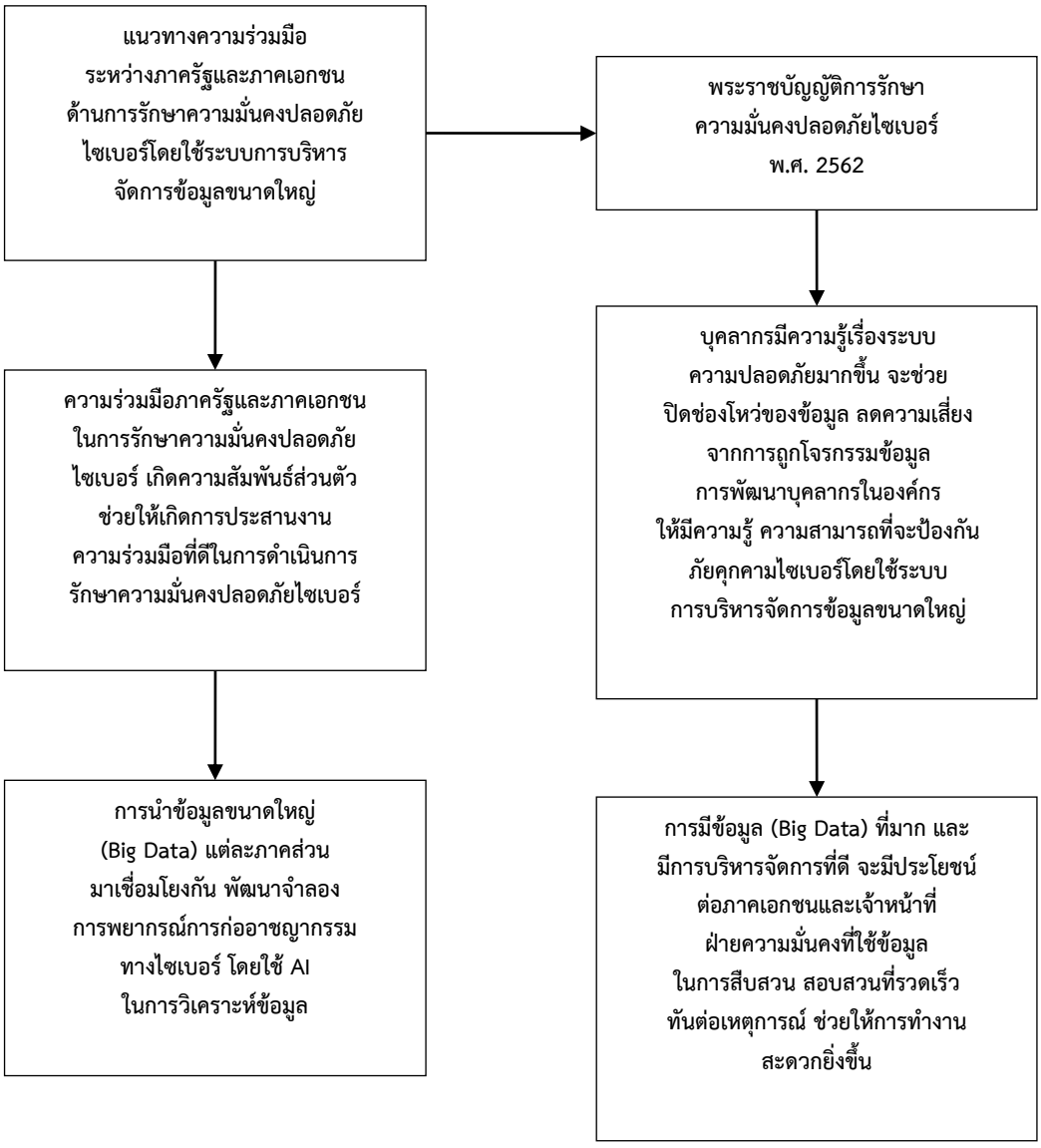
การเตรียมความพร้อมในด้านความร่วมมือระหว่างภาครัฐและเอกชนในการรับมือกับภัยอันตรายจากการสื่อสาร การเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตของระบบเครือข่ายคอมพิวเตอร์นับล้าน ๆ เครื่อง ทำให้เกิดความเสียหายเป็นวงกว้าง เสียหายต่อความมั่นคงของประเทศ ความร่วมมือในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ของภาครัฐและเอกชน มี 3 ประการ ดังนี้ 1) การป้องกัน (Identify & Protect) 2) การเฝ้าระวังแบบเรียลไทม์ (Detect) และ 3) การสนองตอบภัยคุกคามแบบเรียลไทม์ (Respond)

ความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ เป็นกระบวนการทำงานที่เอื้อให้ภาคส่วนต่าง ๆ มีเวทีเจรจาต่อรองซึ่งกันและกัน ตลอดจนเอื้อต่อการทำงานแบบเปิดกว้างและเสริมสร้างขีดความสามารถของภาครัฐและเอกชนผ่านการแลกเปลี่ยนข้อมูลและการใช้ทรัพยากร เป็นวิธีการบริหารร่วมกันเป็นกลุ่ม ซึ่งอาจประกอบด้วย ผู้มีส่วนได้ส่วนเสีย ภาคเอกชน ภาครัฐ และภาคประชาชน โดยมีเป้าหมายในการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ ในกระบวนการทำงานนี้จะเกิดแนวทางความร่วมมือกัน ไม่ใช่การแข่งขันกัน การพัฒนาศักยภาพความร่วมมือของภาครัฐและเอกชนในการป้องกันและรับมือกับภัยคุกคามด้านไซเบอร์นั้น เพื่อขับเคลื่อนเศรษฐกิจและสังคมดิจิทัลที่มั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ และเป็นแนวทางความร่วมมือในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศต่อไป

แม้การโจมตีความมั่นคงปลอดภัยทางคอมพิวเตอร์จะรุนแรงและอาจสร้างความเสียหายร้ายแรงต่อรัฐบาลและต่อโครงสร้างพื้นฐานที่สำคัญ แต่ทรัพยากรที่ประเทศใช้เพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศยังถูกกว่าค่าใช้จ่ายด้านการป้องกันภัยแบบเดิมมากนัก ความลังเลที่จะเพิ่มค่าใช้จ่ายด้านทรัพยากรในด้านนี้จะส่งผลเสียต่อความมั่นคงของประเทศ และเป็นจุดอ่อนในยุทธศาสตร์การป้องกันในภาพรวม บวกกับข้อเท็จจริงที่ว่าการฟื้นตัวจากการโจมตีทางคอมพิวเตอร์มีค่าใช้จ่ายสูงกว่าการวางมาตรการที่ถูกต้องเพื่อป้องกันไม่ให้เกิดขึ้นตั้งแต่แรก ยิ่งไปกว่านั้น ยังมิได้มีการพิจารณาถึงผลกระทบที่วัดปริมาณไม่ได้ เช่น การสูญเสียความเชื่อมั่นต่อรัฐบาล และผลกระทบต่อประเทศในระยะยาว

องค์ความรู้จากการวิจัย

จากการศึกษาวิจัย ผู้วิจัยได้ข้อค้นพบกรอบแนวคิดเชิงคุณภาพจากงานวิจัย เรื่อง แนวทางความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ ดังนี้



ภาพ 1 การสร้างความร่วมมือระหว่างภาครัฐและภาคเอกชนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่

สรุป

จากการวิจัยได้ข้อสรุปว่า ภาครัฐได้ระบบการจัดการฐานข้อมูลขนาดใหญ่ (Big Data) ที่เหมาะสม สามารถตรวจสอบภัยคุกคามไซเบอร์ได้รวดเร็วโดยการใช้ระบบบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) ภาคเอกชนได้ข้อมูลขนาดใหญ่ (Big Data) มาบริหารจัดการ ทำให้งานเกิดประสิทธิภาพในการป้องกันภัย

คุกคามไซเบอร์ ยกระดับความพร้อมในการรับมือกับความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ ที่มีผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ ใช้ AI (Artificial Intelligence) ในการบริหารจัดการข้อมูล ตัดข้อกังวลเรื่องการรักษาความลับข้อมูลออกไป สามารถรักษามาตรฐานได้โดยไม่มีความสัมพันธ์ระหว่างบุคคลในการแสวงหาผลประโยชน์จาก Big Data เข้ามาเกี่ยวข้อง นอกจากนี้ AI ยังสามารถใช้วิเคราะห์ข้อมูลโดยการนำข้อมูลขนาดใหญ่ (Big Data) แต่ละภาคส่วนมาเชื่อมโยงกันและทำการพัฒนาจำลองการพยากรณ์การก่ออาชญากรรมทางไซเบอร์ การที่บุคลากรมีความรู้เรื่องระบบความปลอดภัยมากขึ้น จะช่วยปิดช่องโหว่ของข้อมูล ลดความเสี่ยงจากการถูกโจรกรรมข้อมูล การพัฒนาบุคลากรในองค์กรให้มีความรู้ ความสามารถที่จะป้องกันภัยคุกคามไซเบอร์โดยใช้ระบบการบริหารจัดการข้อมูลขนาดใหญ่ การมีข้อมูล (Big Data) ที่มาก และมีการบริหารจัดการที่ดี จะมีประโยชน์ต่อภาคเอกชนและเจ้าหน้าที่ฝ่ายความมั่นคงที่ใช้ข้อมูลในการสืบสวน สอบสวนที่รวดเร็ว ทันต่อเหตุการณ์ ช่วยให้การทำงานสะดวกยิ่งขึ้น

References

Ministry of Digital Economy and Society. (n.d.). About the Digital Economy and Society Development Agency. Retrieved April 11, 2022, from https://www.mdes.go.th/mission/detail/2481

Thanyawikrom, K., & Kulsawat, T., (2021). Information security management: A case study of personal data protection in electronic transactions of Thai commercial banks. Journal of Buddhist Social Science and Anthropology, 6(3), 371-386.

Srimuangkanjana, C., (2018). National security strategy framework. Retrieved April 25, 2022, from https://dl.parliament.go.th/backoffice/viewer2300/web/viewer.php

Singkaew,C., (2021). The role of the government in preventing cybercrime for economic and social security. Journal of Management and Technology Eastern University, 18(1), 539-552.

Tantrakool, T., (2018). Knowledge management and adult learning development in organizations. 12th National Academic Conference and Research Presentation, Western University, July 7-8.

Arunrangsri ,R., (2018). Cyber threat management strategy in the southern border provinces. National Security Course, Class 60, National Defense College.

Wongreanthong, N. (2018). *4 แนวทางที่ผู้บริหารควรทำเพื่อรับมือ Digital Disruption*. Retrieved April 8, 2022, from https://www.nuttaputch.com/forbesglobalceo-4-ways-ceo-to-deal-with-disruption