

บทบาทของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. 2560-2565

The role of Army Cyber Center in the Royal Thai Army Headquarters 2017-2022

ธัชกร ภูริธรจินดา¹, เกรียงชัย ปิงประวัต², ณัฐพงศ์ บุญเหลือ³ และ นิพนธ์ โสเฮง⁴
Thatchakon Phurithornjinda¹, Kriangchai Pungprawat², Nattapong Boonlue³
and Nipon Sohng⁴

มหาวิทยาลัยรามคำแหง

Ramkhamhaeng University, Thailand

Corresponding Author, Email: thatchakon.p007@outlook.com¹

Received: 2024-7-30; Revised: 2024-9-24; Accepted: 2024-9-25

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์ 1) เพื่อศึกษาบทบาทหน้าที่ภารกิจขอบเขตความรับผิดชอบของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย พ.ศ. 2560-2565, 2) เพื่อวิเคราะห์ศึกษาแนวทางการพัฒนานโยบายของกระทรวงกลาโหมกองบัญชาการกองทัพไทย ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และ 3) เพื่อศึกษาถึงการสร้างองค์ความรู้ใหม่ด้านการจัดการความปลอดภัยทางไซเบอร์ของประเทศ ใช้การวิจัยเชิงคุณภาพ โดยเก็บข้อมูลด้วยวิธีการศึกษาข้อมูลจากเอกสารสำคัญและการสัมภาษณ์เชิงลึกกับผู้ทรงคุณวุฒิที่เกี่ยวข้องจำนวน 8 คน

ผลการวิจัยพบว่า 1) บทบาทหน้าที่ ประกอบด้วย (1) หน้าที่บทบาทความรับผิดชอบของศูนย์ไซเบอร์ทหารเกิดจาก พ.ร.บ. การจัดตั้งกองทัพไทย (2) การจัดตั้งศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย อาศัยความร่วมมือของทุกเหล่าทัพในการดำเนินการเพื่อให้เห็นภาพให้เห็นภาพสนามรบในมิติเดียว (3) การดำเนินการทางไซเบอร์เชิงรุกเพื่อสนับสนุนนโยบายรัฐบาล และ (4) หน่วยงานไซเบอร์ของแต่ละเหล่าทัพมีความเป็นเอกเทศสูงทำให้การบูรณาการร่วมทำได้ยาก 2) การพัฒนานโยบาย พบว่า (1) กระทรวงกลาโหมขาดทรัพยากรบุคคลที่มีความเชี่ยวชาญในการ กำหนดมาตรฐานของเทคโนโลยีที่เกี่ยวข้องในมิติไซเบอร์ให้มีประสิทธิภาพ (2) กระทรวงกลาโหมไม่ควรอนุญาตให้มีการจัดซื้ออุปกรณ์การป้องกันเครื่องปลายทางแบบแยกการ (3) กระทรวงกลาโหมไม่ควรอนุญาตให้มีการจัดซื้ออุปกรณ์การป้องกันที่ใช้ในการเชื่อมต่ออินเทอร์เน็ตแบบแยกการ และ (4) นโยบายการจัดซื้อโปรแกรมระบบปฏิบัติการและโปรแกรมมัลแวร์ประโยชน์ประเทของกระทรวงกลาโหมควรจัดหาในภาพรวม 3) การสร้างองค์ความรู้ใหม่ด้านจัดการจัดการความปลอดภัยทางไซเบอร์ของประเทศ พบว่า (1) เกิดความไม่คล่องตัวขององค์กรในเรื่องระเบียบปฏิบัติทางราชการ (2) มิติความร่วมมือระหว่างประเทศในเรื่องความปลอดภัยทางไซเบอร์ (3) ภาครัฐควรกำหนดหลักสูตรและองค์ความรู้ทางไซเบอร์ให้แก่โรงเรียนและมหาวิทยาลัย และ (4) ประเทศไทยยังขาดหน่วยงานที่เป็นเครื่องมือในการแก้ไขปัญหาทางไซเบอร์ให้กับประชาชนในพื้นที่

คำสำคัญ: ศูนย์ไซเบอร์ทหาร, กองบัญชาการกองทัพไทย, ความปลอดภัยทางไซเบอร์

Abstract

This research aimed: 1) to study the roles, duties, missions, and scope of responsibilities of Army Cyber Center in the Royal Thai Army Headquarters 2017-2022; 2) to analyze and study the policy development guidelines of the Ministry of Defense, the Royal Thai Army Headquarters, Cyber security aspect; and 3) to study the creation of new knowledge in cyber security management of the country. Use qualitative research Data were collected by studying information from important documents and in-depth interviews with 8 relevant experts.

The research results found that: 1) roles include (1) the duties, roles and responsibilities of Army Cyber Center arise from the Royal Thai Army Establishment Act; (2) The establishment of the Royal Thai Army Headquarters relies on the cooperation of all armed forces to provide a one-dimensional picture of the battlefield; (3) proactive cyber operations to support government policy; and (4) The cyber departments of each military force are highly independent, making integration difficult, 2) the policy development found that: (1) the Ministry of Defense lacks human resources with expertise in Set standards for technology related to the cyber dimension to be effective; (2) the Ministry of Defense should not permit the separate procurement of terminal protection equipment; (3) the Ministry of Defense should not permit the procurement of discrete Internet-connected defense equipment; and (4) the Ministry of Defense's policy for purchasing operating systems and office utility programs should be procured as a whole. 3) the creation of new knowledge in cyber security management of the country. It was found that: (1) there is instability in the organization regarding government regulations; (2) dimension of international cooperation in cyber security; (3) the Government should establish cyber curricula and knowledge for schools and universities, and (4) Thailand still lacks an agency that is instrumental in solving cyber problems for people in the area.

Keywords: Army Cyber Center, The Royal Thai Army Headquarters, Cyber Security

บทนำ

ปัจจุบันปฏิบัติการทางไซเบอร์ ถือเป็นมิติการรบที่ 5 ต่อจากมิติทางบกทางน้ำ ทางอากาศและทางอวกาศ เกือบทุกประเทศทั่วโลกได้มีการจัดตั้งหน่วยงานด้านไซเบอร์ ทางทหารขึ้นเพื่อรองรับ ภัยคุกคามทางด้านไซเบอร์ ซึ่งในส่วนของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย มีที่มาจากการที่ประเทศไทยได้เป็นส่วนหนึ่งของประเทศพันธมิตรที่เข้าร่วมกับองค์การสนธิสัญญาแอตแลนติกเหนือ (North Atlantic Treaty Organization-NATO) โดยมีจุดมุ่งหมายเน้นความร่วมมือให้เกิดความปลอดภัยและมีเสรีภาพระหว่างประเทศพันธมิตรทั้งด้าน

การเมืองและการทหาร เช่น เหตุการณ์การก่อการร้ายที่มาจากเหตุการณ์วินาศกรรม 11 กันยายน หรือ 9/11 ทำให้ทั่วโลกเกิดการประชุมกันเพื่อหาแนวทางการแก้ไขเหตุการณ์ก่อการร้ายที่เกิดขึ้น (NATO Cooperative Cyber Defence Centre of Excellence, 2017) การที่จะแก้ปัญหาได้นั้นจะต้องมี “กฎหมายสากล” ซึ่งเป็นกฎหมายความร่วมมือระหว่างประเทศทำให้เกิดนโยบายของรัฐบาลและข้อตกลงต่าง ๆ ขึ้นมา เรียกว่า MOU (Memorandum Of Understanding) และการประชุมได้กำหนดมติทางไซเบอร์เป็นโดเมนในการปฏิบัติการโดยอ้างอิงจากเอกสารยุทธศาสตร์ทางไซเบอร์(The Tallinn Paper) ว่าด้วย ธรรมชาติของบรรทัดฐานกฎหมายทางไซเบอร์ระหว่างประเทศ (The Nature of international law cyber norms)

ในส่วนของประเทศไทยได้มีมติจากการประชุมสภาทนายความครั้งที่ 5/2556 เมื่อวันที่ 30 พฤษภาคม พ.ศ. 2556 ให้กองบัญชาการกองทัพไทยไปพิจารณาแนวทางในการจัดตั้งหน่วยงานขึ้นมารับผิดชอบภัยคุกคามทางไซเบอร์ โดยเป็นหน่วยงานที่ขึ้นตรงของสำนักปฏิบัติการกรมยุทธการทหารและสามารถปฏิบัติงานได้อย่างเต็มรูปแบบนับตั้งแต่วันที่ 1 ตุลาคม พ.ศ. 2557 เป็นต้นมา ซึ่งส่งผลให้กองบัญชาการกองทัพไทยเกิดการพัฒนางานด้านไซเบอร์อย่างต่อเนื่องโดยมีผลงานที่สำคัญ ได้แก่ การจัดทำยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทยในปี พ.ศ. 2558 และได้ดำเนินการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์กองทัพไทย รวมทั้งจัดตั้งประชาคมไซเบอร์กองทัพไทยขึ้นในปีเดียวกัน ต่อมา พลเอก ประวิตร วงษ์สุวรรณ รัฐมนตรีว่าการกระทรวงกลาโหมในขณะนั้นได้กรุณานุมัติให้จัดตั้งศูนย์ไซเบอร์ทหารเมื่อวันที่ 27 กรกฎาคม พ.ศ. 2560 เป็นหน่วยขึ้นตรงกับสำนักผู้บัญชาการทหารสูงสุดกองทัพไทย และ พลเอก สุรพงษ์ สุวรรณอัตถ์ ผู้บัญชาการทหารสูงสุดได้กรุณานุมัติให้แก้ตรากองทัพไทยเมื่อ 11 สิงหาคม พ.ศ. 2560 ได้มีการจัดตั้งศูนย์ไซเบอร์ทหารตั้งแต่ 1 ตุลาคม พ.ศ. 2560 เป็นต้นมา โดยมีภารกิจในการเสนอความเห็น กำหนดนโยบาย วางแผน อำนวยการประสานงาน บูรณาการ ปฏิบัติการและกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ ดำเนินการจัดการฝึก ศึกษาวิทยาการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Schmitt, 2013)

ศูนย์ไซเบอร์ทหารได้จัดโครงสร้างการจัดกำลังพล ประกอบด้วย 5 กองหลัก ได้แก่ (1) กองธุรการรับผิดชอบงานด้านธุรการ กำลังพลและส่งกำลังบำรุง (2) กองยุทธการและการข่าวรับผิดชอบงานข่าวกรองทางไซเบอร์ งานด้านยุทธการและการฝึก รวมถึงงานด้านกิจการพลเรือนที่เกี่ยวข้อง (3) กองวิทยาการรับผิดชอบงานเป็นแหล่งสายวิทยาการด้านไซเบอร์ของกองบัญชาการกองทัพไทยและการเป็นหน่วยรับผิดชอบในการฝึกอบรมกำลังพลด้านไซเบอร์ให้กับกองทัพไทยและหน่วยงานต่าง ๆ ตามที่ได้รับการร้องขอ รวมทั้งการตรวจสอบประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ งานการวิจัยและพัฒนาในมิติทางไซเบอร์ทั้งปวง (4) กองปฏิบัติการรับผิดชอบด้านการปฏิบัติการทางไซเบอร์เชิงรุก การรับมือเหตุการณ์ทางไซเบอร์ เช่น การทดสอบเจาะระบบและการพิสูจน์หลักฐานทางดิจิทัล (5) กองรักษาความมั่นคงปลอดภัยรับผิดชอบงานด้านการป้องกัน ภัยคุกคามทางไซเบอร์เชิงรับ โดยจะรับผิดชอบระบบเฝ้าระวังและแจ้งเตือนเหตุการณ์ทางไซเบอร์ สำหรับเครือข่ายสารสนเทศด้านการบริหารระบบเครือข่ายควบคุมบังคับบัญชา กองทัพไทยมีอำนาจหน้าที่หลักสำหรับการปฏิบัติการทางไซเบอร์ ในส่วนของการเตรียมกำลังและการใช้กำลังเพื่อการป้องกันประเทศตามที่กำหนดไว้ในรัฐธรรมนูญและตามพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รองรับอำนาจหน้าที่เหล่านี้จะเป็นตัวกำหนดบทบาทและความรับผิดชอบในการพัฒนาขีดความสามารถและความเชี่ยวชาญในบริบทของการปฏิบัติการทางไซเบอร์เพื่อสนับสนุน

การแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของกองทัพไทยและระดับประเทศเมื่อมีการร้องขอหรือการสั่งการโดยตรงจากผู้บังคับบัญชา (นริศรา พลอยประไพ, 2564)

สรุปประเด็นปัญหาการวิจัย การปฏิบัติการทางไซเบอร์ถือเป็นมิติการรบที่ 5 ซึ่งประเทศต่างๆ กำลังพัฒนาศูนย์ไซเบอร์ทางทหารเพื่อตอบสนองภัยคุกคามที่เพิ่มขึ้น โดยประเทศไทยได้จัดตั้งศูนย์ไซเบอร์ทหารตั้งแต่ปี 2557 เพื่อเสริมสร้างความมั่นคงไซเบอร์ตามยุทธศาสตร์ระดับชาติ ศูนย์ไซเบอร์มีหน้าที่หลักในการวางแผนและดำเนินการด้านความมั่นคงไซเบอร์ รวมถึงการฝึกอบรมและการวิจัย โดยมีโครงสร้างแบ่งออกเป็น 5 กองหลัก เช่น การข่าวกรองและการรักษาความปลอดภัย. การจัดตั้งศูนย์ไซเบอร์นี้ มีความสำคัญในการพัฒนาขีดความสามารถในการป้องกันประเทศในยุคดิจิทัล ผู้วิจัยจึงเห็นความสำคัญของการพัฒนาบทบาทและนโยบายความมั่นคงปลอดภัยไซเบอร์ของกองบัญชาการกองทัพไทย ซึ่งต้องดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 ยุทธศาสตร์ชาติ และแผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง เพื่อสนับสนุนการทำงานร่วมกันของหน่วยงานราชการและภาคเอกชนอย่างมีประสิทธิภาพ

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาบทบาทหน้าที่ภารกิจขอบเขตความรับผิดชอบของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย พ.ศ. 2560-2565
2. เพื่อวิเคราะห์ศึกษาแนวทางการพัฒนานโยบายของกระทรวงกลาโหมกองบัญชาการกองทัพไทยด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2560-2565
3. เพื่อศึกษาถึงการสร้างองค์ความรู้ใหม่ด้านจัดการจัดการความปลอดภัยทางไซเบอร์ของประเทศ พ.ศ. 2560-2565

การทบทวนวรรณกรรม

แนวคิดการนำนโยบายไปปฏิบัติ

วิลเลียม (Williams, 1971) ชี้ว่า กิริยาที่เรียกว่า นำไปปฏิบัติ (implement) มีความหมาย อยู่สองประการ ประการแรก คือ การจัดหาหรือเตรียมวิธีการทั้งหลายทั้งปวงที่จะทำให้ดำเนินการสำเร็จลุล่วงให้พร้อม ประการที่สอง คือ การดำเนินการให้สำเร็จลุล่วงการนำไปปฏิบัติในหน่วยงานหนึ่งสามารถเกี่ยวข้องกับ ความหมายทั้งสองประการได้ในขณะเดียวกันนั้น คือ ความหมายการพยายามอย่างต่อเนื่องตลอดช่วงเวลาหนึ่งใน อันที่จะยกระดับความสามารถของหน่วยงานนั้นหรือหน่วยงานอื่นที่เกี่ยวข้องเพื่อที่จะนำนโยบายไปปฏิบัติให้ สำเร็จลุล่วงในทัศนะของวิลเลียมการนำนโยบายไปปฏิบัติ คือ การดำเนินการเพื่อให้นโยบายสำเร็จลุล่วง ซึ่งเป็น ความหมายที่คล้ายคลึงกับความหมายที่ Pressman and Wildavsky and Sabatier ยึดถือนั่นเอง

สัญญา เคนาภูมิ และบุรฉัตร จันทร์แดง (2562) ในบทความ "ตัวแบบทฤษฎีการนำนโยบายสาธารณะ ไปสู่การปฏิบัติ" ได้อธิบายว่าการนำเสนอและการปฏิบัตินโยบายสาธารณะมีความสำคัญต่อการพัฒนาประเทศ โดยเสนอโมเดลที่ช่วยในการวิเคราะห์กระบวนการต่าง ๆ ตั้งแต่วางแผนจนถึงการดำเนินงานจริง รวมถึงปัจจัย

ที่มีผลต่อความสำเร็จของนโยบาย ซึ่งประกอบด้วยการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย การสื่อสารที่ชัดเจน และการประเมินผลที่มีประสิทธิภาพ เพื่อให้สามารถบรรลุเป้าหมายของนโยบายอย่างแท้จริง

จากการทบทวนวรรณกรรมทฤษฎีการนำนโยบายไปปฏิบัติและการศึกษาให้ความหมายแนวทางการนำนโยบายไปปฏิบัติของนักวิชาการไทยและชาวต่างประเทศที่ให้ความหมายของการนำนโยบายไปปฏิบัติ เพื่อที่จะได้นำองค์ความรู้ประกอบรูปแบบต่าง ๆ ของการนำนโยบายไปปฏิบัติ พร้อมทั้งการศึกษาตัวแบบที่เกี่ยวข้องในการนำนโยบายไปปฏิบัติ เพื่ออธิบายถึงการปฏิบัติงานของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทยในรูปแบบของการนำนโยบายไปปฏิบัติใน 2 มิติ ได้แก่ (1) มิติของการศึกษาบทบาทหน้าที่ภารกิจขอบเขตการรับผิดชอบของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย มิติที่ (2) เพื่อศึกษาแนวทางการพัฒนานโยบายของกระทรวงกลาโหม กองบัญชาการกองทัพไทย ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หลังจากการก่อตั้งศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย นโยบายแผนงานต่าง ๆ ของศูนย์ไซเบอร์ทหารจะมีแนวทางการนำนโยบายไปปฏิบัติเช่นไร เพื่อให้เกิดรูปธรรมที่ชัดเจนในการป้องกันภัยคุกคามทางไซเบอร์ และความมั่นคงทางเทคโนโลยีของประเทศหรือเหล่าทัพ หน่วยงานราชการและเอกชน ซึ่งเป็นสิ่งที่มีความสำคัญอย่างยิ่งต่อการปฏิบัติงานของบุคลากรของศูนย์ไซเบอร์ทหาร กองบัญชาการ กองทัพไทย (สำนักงานปลัดกระทรวงกลาโหม, 2666)

แนวคิดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560-2564)

สำนักงานสภาความมั่นคงแห่งชาติได้จัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560-2564) (National Cybersecurity Strategy 2017-2021) เพื่อเป็นแนวนโยบายระดับชาติฉบับแรกของไทย ในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้รับกับสภาพสังคมที่เข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบในอนาคต โดยมีเป้าหมายหลักคือการสร้างความพร้อมของ ประเทศไทย ในการรับมือกับภัยคุกคามทางไซเบอร์ ที่จะทวีความรุนแรงมากขึ้น ให้ครอบคลุมรอบด้านตามสภาวะแวดล้อม เอื้ออำนวยเสริมขีดความสามารถของไทยให้มีความเข้มแข็งยิ่งขึ้น โดยมุ่งเน้นการมีกลไกกลางในการบริหาร จัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างสาธารณูปโภคพื้นฐาน การสร้างความตระหนักรู้ในทุกภาคส่วนและสร้างความร่วมมือกับต่างประเทศ โดยกำหนดกลยุทธ์เพื่อให้การดำเนินงานประสบผลสำเร็จ ไว้ 6 กลยุทธ์ ได้แก่ (สำนักงานสภาความมั่นคงแห่งชาติ, 2561)

กลยุทธ์ที่ 1 พัฒนาขีดความสามารถทั้งองค์กรภาครัฐ ทั้งฝ่ายทหาร พลเรือนและตำรวจ และภาคส่วนต่าง ๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาคความมั่นคงทางไซเบอร์ ตลอดจนรองรับสังคมดิจิทัล

กลยุทธ์ที่ 2 พัฒนารอบความร่วมมือระหว่างประเทศและอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

กลยุทธ์ที่ 3 พัฒนาทรัพยากรมนุษย์องค์ความรู้ และความตระหนักรู้ถึงความสำคัญ ของภัยคุกคามความมั่นคงทางไซเบอร์

กลยุทธ์ที่ 4 ปกป้อง ป้องกัน ภัยคุกคามทางไซเบอร์ สงคราม ไซเบอร์ และเสริมสร้างความปลอดภัยทางไซเบอร์ โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ และเสริมสร้างเครือข่ายความร่วมมือกับทุกภาคส่วนทั้งภายในและภายนอกประเทศ

กลยุทธ์ที่ 5 พัฒนาการบังคับใช้กฎหมาย ระเบียบต่าง ๆ เพื่อให้เกิดความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมทางไซเบอร์

กลยุทธ์ที่ 6 ส่งเสริมการพัฒนาขีดความสามารถขององค์กรทุกภาคส่วนรวมถึงบุคลากรที่เกี่ยวข้องให้มีความรู้ ความชำนาญด้านไซเบอร์อย่างต่อเนื่อง

แนวคิดเกี่ยวกับนโยบายความมั่นคงแห่งชาติ

นโยบายความมั่นคงแห่งชาติ เมื่อสงครามเย็นสิ้นสุดลงเป็นที่ชัดเจนในหมู่นักคิดและนักทฤษฎีด้านความมั่นคงว่าประเด็นและปัญหาของความมั่นคงแห่งชาติของรัฐต่าง ๆ ได้เปลี่ยนแปลงไป ซึ่งที่จริงก็คือการเปลี่ยนกระบวนทัศน์ (Paradigm) ของการจัดระเบียบโลกที่เปลี่ยนผ่านเข้าสู่ยุคหลังสงครามเย็น อันส่งผลโดยตรงให้เกิดความเปลี่ยนแปลงต่อสิ่งที่ถูกพิจารณาว่าเป็นประเด็นและปัญหาด้านความมั่นคงที่รัฐจะต้องเผชิญ ดังจะเห็นได้ว่าในยุคสงครามเย็นนั้น น้ำหนักในกระบวนการพิจารณาประเด็นและปัญหาด้านความมั่นคงมุ่งไปสู่เรื่องทางทหารเป็นสำคัญ โดยเฉพาะการแสวงหาและกำหนดมาตรการในการตอบโต้กับภัยคุกคาม ทางทหารของรัฐศัตรู ซึ่งอาจกล่าวได้ว่า ในยุคดังกล่าวความมั่นคงของรัฐก็คือความมั่นคงทางทหาร นักทฤษฎีด้านความมั่นคงเรียกแนวคิดเช่นนี้ว่าเป็นความมั่นคงแบบดั้งเดิม (Traditional Security) หรือความมั่นคงแบบเก่า และแนวคิดหลักที่ถูกนำมาใช้อธิบายในกระบวนการทำนโยบาย ก็คือ เรื่องของการป้องกันปราม อันเป็นมาตรการที่ถูกสร้างขึ้นเพื่อยับยั้งการตัดสินใจของรัฐข้าศึกในการเปิดการรุกทางทหาร แต่เมื่อกระบวนทัศน์แบบเดิมได้เปลี่ยนไป อันเนื่องมาจากผลการสิ้นสุดของการเผชิญหน้าทางทหารระหว่างค่ายทางการเมืองสภาพแวดล้อมใหม่เช่นนี้ทำให้ปัญหาความมั่นคงแต่เดิมซึ่งตั้งอยู่บนรากฐานของประเด็นทางทหารได้เปลี่ยนไปด้วย (สำนักนายกรัฐมนตรี, สำนักงานสภาความมั่นคงแห่งชาติ, 2560)

ความมั่นคงของชาติ (National Security) คือ การดำรงอยู่ของชาติ เป็นความมั่นคงแบบเบ็ดเสร็จ ต้องมีการบูรณาการด้านต่าง ๆ เป็นความมั่นคงที่ครอบคลุมหลายมิติของทุกด้าน ซึ่งมีความเชื่อมโยงกันทั้งด้านการเมืองภายในประเทศ การเมืองระหว่างประเทศ เศรษฐกิจ สังคมจิตวิทยา วิทยาศาสตร์ เทคโนโลยี พลังงาน ทรัพยากรธรรมชาติและสิ่งแวดล้อม การป้องกันประเทศ และความสัมพันธ์ระหว่างประเทศ เป็นต้น (สำนักงานสภาความมั่นคงแห่งชาติ, 2566)

จากการทบทวนวรรณกรรมแนวคิดเกี่ยวกับนโยบายความมั่นคงแห่งชาติได้มีนักวิชาการให้ความหมายของความมั่นคงแห่งชาติไว้หลายความหมาย ซึ่งผู้วิจัยสนใจที่จะศึกษาถึงบทบาทการปฏิบัติงานของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย ซึ่งจะเห็นได้ว่าโลกมีการเปลี่ยนแปลงของภัยคุกคาม ที่เป็นสงครามซึ่งก่อนหน้านี้มีการใช้ยุทธโศภรณ์ในการต่อสู้เพื่อปกป้องประเทศให้ปลอดภัยและมั่นคงจากศัตรู แต่ในปัจจุบันภัยคุกคาม ได้มาในรูปแบบไซเบอร์หรือสื่อเทคโนโลยีที่ทันสมัยต่อการดำเนินชีวิตพร้อมกับภัยที่เป็นอันตรายได้ง่ายและทั่วถึงกับประชาชนเนื่องจากภัยคุกคามมาในรูปแบบที่ใกล้ชิดและส่งผลกระทบต่อความมั่นคงของชาติเป็นอย่างมาก ศูนย์ไซเบอร์ทหาร (2563) กองบัญชาการ กองทัพไทย มีบทบาทในการจัดการต่อภัยคุกคามทางไซเบอร์ ตามวิวัฒนาการของนโยบายความมั่นคงแห่งชาติว่าทหารซึ่งเป็นกำลังหลักในการป้องกันประเทศมีความพร้อมและหลักปฏิบัติการในการรับมือของภัยคุกคามทางไซเบอร์โดยให้ประเทศมีความมั่นคงปลอดภัย

วิธีดำเนินการวิจัย

การวิจัยเรื่อง บทบาทของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. 2560-2565 ผู้วิจัยเลือกใช้วิธีวิจัยคุณภาพ (Qualitative Research) เนื่องจากเป็นระเบียบวิธีที่เหมาะสม ทำให้ผู้วิจัยสามารถนำข้อมูลมาวิเคราะห์ สรุปผลการวิจัย และนำไปสู่ข้อเสนอแนะ สามารถใช้เป็นแนวทางนำไปปฏิบัติได้อย่างเหมาะสมกับบริบทของการศึกษาบทบาทของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย

ผู้ให้ข้อมูลหลัก

ผู้วิจัยได้คัดเลือกผู้บริหารในหน่วยงานภาครัฐในการออกนโยบายหรือผู้มีส่วนเกี่ยวข้องในหน่วยงานราชการเป็นผู้บริหาร ผู้บังคับบัญชาที่เกี่ยวข้อง รวมทั้งหมด 8 คน ประกอบด้วย ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร สถาบันป้องกันประเทศ ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก ผู้อำนวยการศูนย์ไซเบอร์กองทัพอากาศ เลขานุการ คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ผู้อำนวยการศูนย์ไซเบอร์ทหาร รองผู้อำนวยการศูนย์ไซเบอร์ทหาร และ ผู้อำนวยการศูนย์ไซเบอร์กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม เป็นการคัดเลือกแบบเจาะจง (Purposive Sampling)

เครื่องมือที่ใช้ในการวิจัย คือ แบบสอบถาม แบ่งออกเป็น 3 ส่วนดังนี้ เครื่องมือสำหรับเก็บรวบรวมข้อมูลในการวิจัยครั้งนี้ ผู้วิจัยจัดทำเครื่องมือการจัดเก็บข้อมูลขึ้น ทั้งหมด 2 เครื่องมือ คือ (1) แบบบันทึกข้อมูลในการวิจัยเอกสาร (Memorandum Data Form) (2) แบบคำถามนำการสัมภาษณ์เชิงลึกกึ่งโครงสร้าง (Semi-structured Interview Guideline) เพื่อให้ได้ข้อมูลรอบด้านมากที่สุด กล่าวคือ เครื่องมือสำหรับเก็บรวบรวมข้อมูล ประกอบด้วย อุปกรณ์จัดบันทึกข้อมูล เครื่องมือบันทึกเสียง กล้องถ่ายภาพ และตัวผู้วิจัย

การเก็บรวบรวมข้อมูล

ดังที่ได้กำหนดการเก็บรวบรวมข้อมูลไว้ 2 วิธี โดยแต่ละวิธีมีขั้นตอนการดำเนินการ ดังนี้

1. การเก็บรวบรวมข้อมูลในการวิจัยเอกสาร (Documentary Research) ลักษณะการดำเนินงานแบบ Workshop เป็นการค้นคว้าข้อมูลจากเอกสาร ทั้งข้อมูลแบบปฐมภูมิ (Primary Data) ได้แก่ แนวคิด ทฤษฎี กฎหมายที่เกี่ยวข้อง กฎกระทรวง ประกาศของหน่วยงานราชการ บันทึกเหตุการณ์ทางประวัติศาสตร์ และข้อมูลแบบทุติยภูมิ (Secondary Data) เป็นการรวบรวมข้อมูลบทวิเคราะห์ วารสารวิชาการ บทความวิชาการ เอกสารประกอบการประชุมวิชาการ วิทยานิพนธ์/Dissertations ข่าวสารจากสื่อมวลชน บทวิเคราะห์ หรือวิพากษ์วิจารณ์ที่นำเสนอบนอินเทอร์เน็ตตลอดจนการสืบค้นข้อมูลอื่น ๆ ที่เกี่ยวข้อง ทั้งที่เป็นภาษาไทยและภาษาต่างประเทศ

2. การเก็บรวบรวมข้อมูลด้วยวิธีสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ให้ข้อมูลคนสำคัญ โดยผ่านการคัดเลือกจากตำแหน่งหน้าที่ คุณสมบัติ ที่สามารถให้ข้อมูลได้อย่างชัดเจนแม่นยำและเป็นข้อมูลที่เชื่อถือ โดยเป็นผู้ทรงคุณวุฒิในกองทัพบกและมีบทบาทต่อการบริหารงานของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย และเหล่าทัพอื่นที่มีความรู้ความเข้าใจในเรื่องไซเบอร์และความมั่นคงทางไซเบอร์ในระดับองค์กร ระดับชาติ และระดับนานาชาติที่ได้รับการฝึกอบรมเป็นอย่างดี

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลผู้วิจัยใช้วิธีวิเคราะห์เชิงเนื้อหา (Content Analysis) โดยประมวลคุณลักษณะเฉพาะด้วยการพิจารณาประเด็นหลัก (Major Themes) จากแต่ละแนวคิดเข้าด้วยกันอย่างเป็นระบบ และใช้กรอบแนวคิดทฤษฎีในการวิเคราะห์ข้อมูล เพื่อให้เกิดความแม่นยำ (Rigor) ตามหลักเหตุและผล (Causality) เพื่อตอบวัตถุประสงค์การวิจัย แบบพรรณนา(Descriptive Research) พร้อมสรุปการวิจัย และข้อเสนอแนะ

ผลการวิจัย

1. บทบาทหน้าที่ภารกิจขอบเขตความรับผิดชอบของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย พ.ศ. 2560-2565 ผลการวิจัย พบว่า

1.1 บทบาทหน้าที่ความรับผิดชอบของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย มาจากพระราชบัญญัติพระราชบัญญัติจัดระเบียบราชการ กระทรวงกลาโหม พ.ศ. 2551 เนื่องจากกฎหมายฉบับนี้กำหนดหน้าที่ภารกิจขอบเขตความรับผิดชอบของหน่วยงานภายใต้สังกัดกระทรวงกลาโหม ศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทยเกิดภายใต้นโยบายของกฎหมายฉบับนี้ประกอบด้วยภัยคุกคามทางเบอร์และการตระหนักถึงความปลอดภัยทางไซเบอร์ และผู้วิจัยมองว่า กฎหมายฉบับนี้และยุทธศาสตร์ชาติ เป็นนโยบายสาธารณะชนิดหนึ่งที่จะต้องมีความเกี่ยวข้องนำนโยบายไปปฏิบัติ

1.2 การจัดตั้งศูนย์ไซเบอร์ทหารของกองบัญชาการกองทัพไทยอาศัยความร่วมมือของทุกเหล่าทัพในการดำเนินการเพื่อให้เห็นภาพสนามรบทางไซเบอร์ในมิติเดียวกัน โครงสร้างขององค์กรศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทยเป็นการทำงานร่วมกันของทุกเหล่าทัพในการปฏิบัติการทางไซเบอร์ซึ่งทำหน้าที่เฝ้าระวังแก้ไขและตรวจสอบภัยคุกคามทางไซเบอร์ของประเทศ

1.3 การดำเนินการทางไซเบอร์เชิงรุกเพื่อสนับสนุนนโยบายรัฐบาล ศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย เป็นหน่วยงานที่มีการปฏิบัติการเชิงรุกเพื่อสนับสนุนนโยบายรัฐบาลในการป้องกันปราบปรามแก้ไข ภัยคุกคามทางไซเบอร์ทุกชนิด ที่อาจจะส่งผลกระทบต่อความเดือดร้อนของหน่วยงานภาครัฐและเอกชนที่ถูกโจรกรรมข้อมูลและถูกโจมตีทางไซเบอร์การปฏิบัติการทางไซเบอร์ ถือว่าเป็นองค์กรที่ตอบสนองนโยบายของรัฐบาลและเป็นเครื่องมือของรัฐบาลในการดำเนินการทางไซเบอร์ทุกชนิด

1.4 หน่วยงานไซเบอร์ของแต่ละเหล่าทัพมีความเป็นเอกเทศสูงทำให้การบูรณาการร่วมกันทำได้ยาก ปัจจุบันนโยบายของกระทรวงกลาโหมมีคำสั่งให้แต่ละเหล่าทัพจะต้องมีศูนย์ ปฏิบัติการทางไซเบอร์เป็นของตนเองและการทำงานของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทยเป็นร่วมกันของแต่ละเหล่าทัพ ซึ่งผลวิจัยพบว่า ศูนย์ไซเบอร์ทหารของแต่ละเหล่าทัพมีความเป็นเอกเทศสูงมากเนื่องจากคำสั่งนโยบายวิสัยทัศน์ของผู้บริหารในหน่วยงานแต่ละเหล่าทัพ มีความแตกต่างและไม่สอดคล้องกันจึงทำให้แผนการทำงานร่วมกันระหว่างศูนย์ไซเบอร์ทหารของแต่ละเหล่าทัพเมื่อมาทำงานร่วมกันจึงทำให้การทำงานไม่ประสิทธิภาพเท่าที่ควรตามแผนและนโยบายการบูรณาการร่วมกันของเหล่าทัพ

2. แนวทางการพัฒนานโยบายของกระทรวงกลาโหมกองบัญชาการกองทัพไทย ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2560-2565 ผลการวิจัย พบว่า

2.1 กระทรวงกลาโหมขาดทรัพยากรบุคคลที่มีความเชี่ยวชาญในการกำหนดมาตรฐานของเทคโนโลยีที่เกี่ยวข้องในมิติไซเบอร์ให้มีประสิทธิภาพ เพื่อให้นโยบายด้านความปลอดภัยทางไซเบอร์กำหนดทิศทางในการจัดหายุทธโพรกณ์ทั้งมวลได้มีมาตรฐานและบูรณาการร่วมกันได้อย่างมีประสิทธิภาพ เนื่องจากผู้เชี่ยวชาญด้านเทคโนโลยีและการจัดการทางไซเบอร์เป็นบุคลากรที่มีจำนวนจำกัดในบรรดาทรัพยากรทั้งหมดสืบเนื่องจากกองบัญชาการกองทัพไทยเป็นหน่วยงานราชการความคล่องตัวและการปฏิบัติงานตามระเบียบข้อบังคับของกระทรวงกลาโหมมีความซับซ้อนทำให้การคัดสรรบุคลากรที่มีความเชี่ยวชาญในด้านไซเบอร์มีน้อย และด้วยข้อจำกัดในเรื่องงบประมาณและค่าตอบแทนสำหรับบุคลากร ที่เป็นผู้เชี่ยวชาญด้านไซเบอร์ยังไม่เพียงพอต่อความต้องการของหน่วยงานภาครัฐที่สังกัด ภายใต้กระทรวงกลาโหมปัจจัยหลักมาจากเรื่องค่าตอบแทน เงินเดือนสวัสดิการ

2.2 กระทรวงกลาโหมไม่ควรอนุญาตให้มีการจัดซื้ออุปกรณ์การป้องกันเครื่องปลายทาง (Hardware and Software) แบบแยกการ เพื่อให้การวางมาตรการการจัดการห่วงโซ่อุปทานที่เปลี่ยนไปผู้ให้บริการในปัจจุบันมีแนวโน้มที่จะกำหนดวิธีการเพื่อให้จ่ายเป็นรายปี (Subscription) ทำให้การต่อรองราคาไม่เกิดประโยชน์สูงสุดต่อกองทัพ

2.3 กระทรวงกลาโหมไม่ควรอนุญาตให้มีการจัดซื้ออุปกรณ์การป้องกันที่ใช้ในการเชื่อมต่ออินเทอร์เน็ตแบบแยกการ เพื่อให้การวางมาตรการการจัดการห่วงโซ่อุปทานที่เปลี่ยนไปผู้ให้บริการในปัจจุบันมีแนวโน้มที่จะกำหนดวิธีการเพื่อให้จ่ายเป็นรายปี (Subscription) ทำให้การต่อรองราคาไม่เกิดประโยชน์สูงสุดต่อกองทัพ

2.4 นโยบายการจัดซื้อโปรแกรมระบบปฏิบัติการและโปรแกรมอรรถประโยชน์ประเภทออฟฟิศของกระทรวงกลาโหมควรจัดหาในภาพรวม เพื่อให้การวางมาตรการการจัดการห่วงโซ่อุปทานที่เปลี่ยนไปผู้ให้บริการในปัจจุบันมีแนวโน้มที่จะกำหนดวิธีการเพื่อให้จ่ายเป็นรายปี (Subscription) ทำให้การต่อรองราคาไม่เกิดประโยชน์สูงสุดต่อกองทัพ

3. การสร้างองค์ความรู้ใหม่ด้านการจัดการจัดการความปลอดภัยทางไซเบอร์ของประเทศ พ.ศ. 2560-2565 ผลการวิจัย พบว่า

3.1 เกิดการไม่คล่องตัวขององค์กรในเรื่องระเบียบปฏิบัติทางราชการการจัดการด้านความปลอดภัยทางไซเบอร์ของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทยพบว่าองค์กรไม่มีความคล่องตัวในเรื่องของการบริหารจัดการเพราะเป็นเรื่องของการทำงานประสานงาน ร่วมกันระหว่างการบูรณาการระหว่างเหล่าทัพจึงทำให้การสร้างองค์ความรู้นวัตกรรมวิจัยและเทคโนโลยีเกี่ยวกับการจัดการ ความปลอดภัยทางไซเบอร์ยังไม่ประสบความสำเร็จเท่าที่ควร

3.2 มิติความร่วมมือระหว่างประเทศในเรื่องความปลอดภัยทางไซเบอร์ อีกหนึ่งองค์ความรู้และการเผยแพร่นวัตกรรมเรื่องการจัดการทางไซเบอร์ของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทยเป็นความร่วมมือระหว่างประเทศ เป็นหน้าที่บทบาทความรับผิดชอบในการประสานงานความร่วมมือระหว่างประเทศใน

การแลกเปลี่ยนข้อมูลข่าวสารจากภัยคุกคามทางไซเบอร์และการป้องกันอาชญากรรมทางไซเบอร์ระหว่างประเทศตลอดจนความร่วมมือการพัฒนาเทคโนโลยีไซเบอร์ของกองทัพและการพัฒนาไซเบอร์ มิติของความร่วมมือระหว่างประเทศ ในมิติของเศรษฐกิจระหว่างประเทศ

3.3 ภาครัฐควรกำหนดหลักสูตรและองค์ความรู้ทางไซเบอร์ให้แก่โรงเรียนและมหาวิทยาลัย ผู้วิจัยมองว่าภาครัฐควรจะนำหลักสูตรองค์ความรู้ขั้นพื้นฐานของไซเบอร์ในการป้องกันอาชญากรรมและการเผยแพร่ข้อมูลที่เป็นอันตรายให้กับหลักสูตรของโรงเรียนและมหาวิทยาลัยในประเทศสืบเนื่องจากเด็กนักเรียนนิสิตนักศึกษาสามารถใช้คอมพิวเตอร์ได้ในระดับสั่งการในโรงเรียนและส่วนตัวทำให้การเข้าถึงข้อมูลและการป้องกันการจัดการข้อมูลผ่านในระบบคอมพิวเตอร์บริหารจัดการในขั้นพื้นฐานได้

3.4 ประเทศไทยยังขาดหน่วยงานที่เป็นเครื่องมือหลักในการแก้ไขปัญหาทางไซเบอร์ให้กับประชาชนในพื้นที่ ผลการวิจัยอีกหนึ่งประเด็นที่ผู้วิจัยมองว่ามีความสำคัญอย่างยิ่งพบว่าประเทศไทยยังขาดหน่วยงานที่เป็นเครื่องมือหลักในการแก้ไขปัญหาทางไซเบอร์ให้กับประชาชนในพื้นที่กรณีประชาชนนั้นได้รับผลกระทบและได้รับความเดือดร้อนจากการโจรกรรมข้อมูลทางไซเบอร์มีงานวิจัยเชิงคอลเลกชันเตอร์ในปัจจุบัน หากมีหน่วยงานที่เป็นเครื่องมือหลักในการแก้ไขปัญหาทางไซเบอร์ให้กับประชาชนในพื้นที่ก็จะทำให้สามารถแก้ไขปัญหาได้ทันทั่วถึง

อภิปรายผล

1. บทบาทหน้าที่ภารกิจขอบเขตความรับผิดชอบของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย พ.ศ. 2560-2565 อภิปรายผลดังนี้ การปฏิบัติหน้าที่ตามมาตรฐานของหน่วยงานทางไซเบอร์ โดยมีกองบัญชาการกองทัพไทยเป็นหน่วยงานหลักของการรักษาความปลอดภัยทางไซเบอร์นับว่าเป็นหน่วยงานที่มีความพร้อมสุดในการขับเคลื่อนนโยบายที่ภาครัฐเป็นผู้ออกนโยบาย โดยมีหลักของการวางแผนป้องกัน ฝ้าติดตาม และระวังการโจมตีทางไซเบอร์ สอดคล้องกับบทความของ ชฎาภรณ์ สิงห์แก้ว. (2564) ที่ศึกษาบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจ พบว่า การพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์ในประเทศไทยนำมาซึ่งความท้าทายด้านอาชญากรรมไซเบอร์ที่ไม่สามารถหลีกเลี่ยงได้ เช่น การโจมตีระบบ การขโมยข้อมูล และการปลอมแปลงบัญชีโซเชียลมีเดีย ซึ่งเป็นภัยคุกคามที่ส่งผลกระทบต่อผลประโยชน์ทางเศรษฐกิจและความมั่นคงของประเทศ โดยภาครัฐเห็นความสำคัญในการรักษาความมั่นคงไซเบอร์ และได้ผลักดันการออกพระราชบัญญัติที่เกี่ยวข้อง รวมถึงการจัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยชี้ให้เห็นว่าการปกป้องโครงสร้างพื้นฐานทางไซเบอร์และการรับมือกับภัยคุกคามไซเบอร์มีบทบาทสำคัญในการรักษาความมั่นคงของรัฐและความปลอดภัยของประชาชน การพัฒนานโยบายและกลยุทธ์ที่มีประสิทธิภาพจึงเป็นสิ่งจำเป็นในการจัดการความเสี่ยงทางไซเบอร์ กองทัพไทยมีการแบ่งบทบาทหน้าที่ของหน่วยงานที่อยู่ภายในองค์กรแตกต่างกันออกไปตามภารกิจที่ได้รับมอบหมาย โดยทุกหน่วยงานล้วนมีความเกี่ยวข้องต่อการประสานงานเพื่อนำกระบวนการด้านนโยบายไปปฏิบัติซึ่งเป็นสิ่งสำคัญต่อการบริหารความเสี่ยงที่ทุกหน่วยต้องร่วมมือต่อกันจากทุกภาคส่วนทั้งในประเทศและต่างประเทศเนื่องจากปัจจุบันไซเบอร์มีความร่วมมือกับหน่วยงานที่เกี่ยวข้องที่จะเป็นรูปแบบการตั้งเซอร์วิส

ดิจิทัลให้กับกองทัพ แนวทางในการขับเคลื่อนพัฒนาบุคลากรและเทคโนโลยีทางด้านไซเบอร์ โดยสรุปบทบาทหน้าที่ทางไซเบอร์ในปัจจุบันของ ศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย เน้นให้ความร่วมมือกับหน่วยงานเอกชนหน่วยงานราชการเพื่อพัฒนาองค์กร และเป็นผู้นำด้านดิจิทัลร่วมกับเจ้าหน้าที่ตำรวจในการป้องกันอาชญากรรมทางไซเบอร์ ตลอดจนการฝึกฝนกำลังพลให้มีความชำนาญและเชี่ยวชาญทางไซเบอร์เพื่อป้องกันภัยคุกคามในมิติอื่น ๆ สอดคล้องกับงานวิจัยของ Olga et al. (2020) ที่ศึกษาความมั่นคงไซเบอร์ในฐานะที่เป็นองค์ประกอบของความมั่นคงแห่งชาติ กล่าวถึงความสำคัญของการปกป้องข้อมูลและโครงสร้างพื้นฐานทางไซเบอร์ในการรักษาความมั่นคงของรัฐ โดยเน้นถึงความท้าทายที่เกิดจากภัยคุกคามไซเบอร์ และเสนอแนวทางในการพัฒนานโยบายและกลยุทธ์ที่มีประสิทธิภาพเพื่อจัดการกับความเสี่ยงเหล่านี้ โดยการเสริมสร้างความร่วมมือระหว่างภาครัฐและเอกชนเป็นสิ่งสำคัญในการสร้างระบบความปลอดภัยไซเบอร์ที่ยั่งยืน

2. แนวทางการพัฒนานโยบายของกระทรวงกลาโหมกองบัญชาการกองทัพไทย ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2560-2565 อภิปรายผลดังนี้ การนำนโยบายไปปฏิบัติตามนโยบายยุทธศาสตร์ชาติที่รัฐบาลกำหนดว่ารัฐมีหน้าที่ในการจัดการการเฝ้าระวังรักษาความปลอดภัยจากภัยคุกคามทางไซเบอร์ โดยมีผู้อำนวยการศูนย์ไซเบอร์ทหารเป็นผู้อำนวยการในการวางแผนนโยบายและสั่งการ ตลอดจนยุทธการและการประสานงานร่วมกันของศูนย์ไซเบอร์ทหารของแต่ละเหล่าทัพ ตลอดจนศูนย์ไซเบอร์ของหน่วยงานราชการอื่น บุคลากรที่ปฏิบัติการทางด้านไซเบอร์ควรมีทักษะทางไซเบอร์ โดยใช้มาตรการจากนโยบายที่ภาครัฐเป็นผู้กำหนดและใช้มาตรฐานการปฏิบัติงานทางไซเบอร์เพื่อบูรณาการร่วมกันระหว่างภาครัฐเอกชน (Bartholomees, 2012) โดยมุ่งเน้นเป็นพิเศษในเรื่องของการตัดสินใจในเชิงนโยบายและการพัฒนาหน่วยงานทางไซเบอร์ ศูนย์ไซเบอร์ทหารเป็นมิติการรบในทางยุทธวิธีใหม่ประเภทหนึ่งที่กำลังจะเกิดขึ้นภายใต้บริบทโลกของการพัฒนาขีดความสามารถทางไซเบอร์ของนานาประเทศ (Meinhart, 2010) และบทบาทหน้าที่ของแนวทางการปฏิบัติของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศ มาตรฐาน การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ในระดับสากล และแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์งานวิจัยเรื่องพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม พบว่า การดำเนินนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นระดับสากลและเป็นแนวทางพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัย ทางไซเบอร์ ของกระทรวงกลาโหมตามยุทธศาสตร์ชาติ ที่ได้กำหนดไว้เป็นแนวทางในการปฏิบัติการออกแผนแม่บทของการสื่อสารทางเทคโนโลยี และการจัดการเรื่องความปลอดภัยทางไซเบอร์ซึ่งเป็นภัยคุกคามใหม่ของมิติรบ มิติที่ 5 ที่กำลังจะเกิดขึ้น

3. การสร้างองค์ความรู้ใหม่ด้านจัดการจัดการความปลอดภัยทางไซเบอร์ของประเทศ พ.ศ. 2560-2565 อภิปรายผลดังนี้ ยุทธศาสตร์ชาติและการกำหนดในแผนยุทธศาสตร์ด้านความมั่นคงทางไซเบอร์นับว่าเป็นนโยบายสาธารณะที่มีการคำนึงถึงความปลอดภัยในชีวิตและทรัพย์สินของประชาชนและความมั่นคงแห่งรัฐ เนื่องจากบริบทของโลกปัจจุบันมีการแข่งขันและการพัฒนาด้านนวัตกรรมเทคโนโลยีทางไซเบอร์และทางด้านความมั่นคงทางทหารมีการบรรจุมิติรบ (สนามรบ) ทางไซเบอร์ (Kello, 2017) การสร้างองค์ความรู้ใหม่ด้านการจัดการความปลอดภัยทางไซเบอร์ของประเทศในทางทหารมีการพัฒนาขีดศักยภาพของการรบด้วยวิธีการทางไซเบอร์และการโจมตีข้อมูลโจรกรรม ตลอดจนบริบทของโลกมีการพัฒนาของเทคโนโลยี

ระบบสารสนเทศเรื่องของการโจรกรรมข้อมูลและการโจมตีทางไซเบอร์ที่เกิดขึ้น (Singer and Friedman, 2014) การจัดการการสร้างองค์ความรู้ด้านไซเบอร์เป็นหน้าที่หลักของศูนย์บัญชาการทางไซเบอร์ของกองบัญชาการกองทัพไทยและศูนย์ไซเบอร์ของแต่ละเหล่าทัพศูนย์ไซเบอร์ของหน่วยงานราชการที่จะต้องมีการเรียนรู้เทคโนโลยีความเข้าใจเกี่ยวกับการใช้อุปกรณ์และการสั่งการด้านการจัดการทางไซเบอร์ศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทยมีความพร้อมในเรื่องของการนำองค์ความรู้นวัตกรรมด้านการจัดการเพื่อเป็นการแลกเปลี่ยน เรียนรู้ระหว่างหน่วยงานราชการด้วยกันหรือการส่งต่อองค์ความรู้ด้านการจัดการภัยหน่วยงานของกระทรวงกลาโหมภายใต้สังกัดกองบัญชาการกองทัพไทยยังมีความพร้อมในเรื่องของเทคโนโลยีงบประมาณบุคลากรที่จะเป็นแนวทางในการพัฒนาศูนย์ปฏิบัติการทางไซเบอร์ให้กับประเทศ และถ่ายทอดองค์ความรู้และเทคโนโลยีไปยังหน่วยงานอื่นได้ ตามขีดศักยภาพแต่ทั้งหมดจะต้องได้รับการสนับสนุนในเรื่องงบประมาณบุคลากร และแนวทางการพัฒนาการวิจัยจากภาครัฐประเด็นที่สำคัญผู้วิจัยมองว่ารัฐบาลควรให้ความสำคัญ ในเรื่องของความปลอดภัยทางไซเบอร์ทุกรัฐบาลเพราะเป็นหน่วยงานที่รักษาความมั่นคง ทางด้านเศรษฐกิจ สังคม การเมือง วัฒนธรรม เทคโนโลยีให้กับประเทศ ซึ่งสอดคล้องกับการศึกษาของ จินดา สระสมบูรณ์ (2558) ที่ศึกษาเรื่องปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย ที่มีการศึกษาองค์ความรู้การปฏิบัติการทางไซเบอร์สำหรับเตรียมการหรือรองรับภัยคุกคามรูปแบบใหม่ โดยนำเสนอรูปแบบที่เหมาะสม ประกอบด้วย ฝ่ายกำลังพล ฝ่ายการข่าว ฝ่ายยุทธการ ฝ่ายส่งบำรุงกำลัง ฝ่ายกิจการพลเรือนและฝ่ายสื่อสาร รวมทั้งมีมาตรการส่งเสริมการปฏิบัติที่มีประสิทธิภาพ โดยการปฏิบัติที่สอดคล้องกันระหว่างฝ่ายยุทธการที่ต้องกระทำต่อฝ่ายตรงข้ามและฝ่ายสื่อสารที่ต้องปกป้องฝ่ายเราและสนับสนุนการปฏิบัติฝ่ายยุทธการรวมถึงการให้กองบัญชาการกองทัพไทยสนับสนุนการปฏิบัติศูนย์บัญชาการทางทหาร แต่ผู้วิจัยครั้งนี้ก็ยังมีความเห็นว่า ข้อค้นพบของจินดา สระสมบูรณ์ ที่ได้ยังไม่ลงลึกในรายละเอียดมากเท่ากับการศึกษาวิจัยในครั้งนี้ สืบเนื่องมาจากระดับการศึกษาของงานวิจัย มีความแตกต่างกันประเด็น เรื่องของงานวิจัยที่เกี่ยวข้องเกี่ยวกับศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย บทบาทหน้าที่ของศูนย์ไซเบอร์ทหารแต่ละเหล่าทัพ ตลอดจนการศึกษาภัยคุกคามและการเฝ้าระวังภัยคุกคามทางไซเบอร์และความร่วมมือระหว่างประเทศในเรื่องไซเบอร์

องค์ความรู้ใหม่ ด้านการจัดการความปลอดภัยทางไซเบอร์

1. การสร้างเครือข่ายการทำงานร่วมกันระหว่างหน่วยงานภาครัฐ เอกชน และองค์กรระหว่างประเทศเพื่อแลกเปลี่ยนข้อมูลภัยคุกคามและแนวทางการป้องกันจะช่วยเสริมสร้างความแข็งแกร่งในการรับมือกับภัยคุกคามไซเบอร์ในระดับชาติ โดยการสร้างแพลตฟอร์มกลางที่สามารถแชร์ข้อมูลได้อย่างรวดเร็วและมีประสิทธิภาพ
2. การลงทุนในโปรแกรมฝึกอบรมและการพัฒนาทักษะด้านไซเบอร์สำหรับบุคลากรในทุกกระดับ โดยเฉพาะในหน่วยงานที่เกี่ยวข้องกับความมั่นคง จะช่วยให้เกิดความพร้อมในการตอบสนองต่อภัยคุกคามที่เกิดขึ้น โดยการสร้างหลักสูตรที่เข้มข้นและเป็นมาตรฐานสำหรับการอบรม

3. การนำเทคโนโลยีใหม่ ๆ เช่น ปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง (Machine Learning) มาใช้ในการวิเคราะห์และตอบสนองต่อภัยคุกคามไซเบอร์ จะช่วยเพิ่มประสิทธิภาพในการป้องกันและตรวจจับภัยคุกคามได้อย่างรวดเร็วและแม่นยำ

4. การส่งเสริมความรู้และความตระหนักรู้เกี่ยวกับความปลอดภัยไซเบอร์ในสังคม เช่น การให้ข้อมูลเกี่ยวกับวิธีป้องกันตนเองจากการโจมตีไซเบอร์และการตรวจสอบความปลอดภัยของข้อมูลส่วนบุคคล จะช่วยลดความเสี่ยงและเพิ่มความปลอดภัยให้กับประชาชน

5. การพัฒนานโยบายและมาตรฐานด้านความมั่นคงไซเบอร์ที่ชัดเจนและยืดหยุ่น สามารถปรับเปลี่ยนตามสถานการณ์และเทคโนโลยีใหม่ ๆ จะทำให้การปฏิบัติการในด้านนี้มีความเป็นระบบและมีประสิทธิภาพมากยิ่งขึ้น

6. การเข้าร่วมเครือข่ายความร่วมมือในระดับนานาชาติ จะช่วยให้ประเทศไทยสามารถเรียนรู้จากประสบการณ์ของประเทศอื่น ๆ และปรับใช้กลยุทธ์ที่เหมาะสมกับบริบทของประเทศ

สรุป

การสร้างองค์ความรู้ใหม่ด้านความปลอดภัยไซเบอร์ต้องอาศัยความร่วมมือจากหลายภาคส่วน ทั้งการบูรณาการข้อมูล การพัฒนาทักษะบุคลากร การใช้เทคโนโลยีใหม่ การส่งเสริมความตระหนักรู้ในสังคม และการสร้างนโยบายที่ชัดเจนและร่วมมือกับประเทศอื่น ๆ เพื่อสร้างความมั่นคงในโลกไซเบอร์อย่างยั่งยืน

ข้อเสนอแนะ

ข้อเสนอแนะที่ได้จากผลการวิจัย

1. รัฐบาลควรสนับสนุนการสร้างฐานข้อมูลกลางภายในประเทศที่มีความทันสมัยและอัปเดตอย่างต่อเนื่อง เพื่อปรับปรุงการเก็บและแชร์ข้อมูลระหว่างหน่วยงานของกองทัพที่มีปฏิบัติการทางไซเบอร์
2. รัฐบาลควรจัดตั้งหน่วยงานเฉพาะด้านเพื่อกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ พร้อมกำหนดนโยบายและแผนปฏิบัติการที่ชัดเจน โดยส่งเสริมความร่วมมือจากภาครัฐ เอกชน และประชาชนในการสร้างความตระหนักรู้และพัฒนาบุคลากรด้านนี้
3. ศูนย์บัญชาการทางไซเบอร์ของกองบัญชาการกองทัพไทยควรทำหน้าที่เป็นศูนย์กลางในการสร้างและแลกเปลี่ยนองค์ความรู้ด้านไซเบอร์ รวมถึงการส่งต่อข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ให้กับประชาชน.

ข้อเสนอแนะในการวิจัยครั้งต่อไป

1. ควรศึกษาเพิ่มเติมเกี่ยวกับการสนับสนุนจากรัฐบาลในด้านงบประมาณและบทบาทของกระทรวงกลาโหมภายใต้การกำกับของศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย รวมถึงนโยบายสาธารณะเกี่ยวกับความปลอดภัยไซเบอร์ ซึ่งจะเป็นประโยชน์ต่อการวิจัยและการนำไปปฏิบัติ
2. หากมีการเปลี่ยนแปลงอำนาจทางการเมืองและการเปลี่ยนแปลงยุทธศาสตร์ชาติ ควรมีการศึกษาเกี่ยวกับผลกระทบที่เกิดขึ้นต่อศูนย์ไซเบอร์และการเปลี่ยนแปลงเชิงนโยบาย เพื่อให้ข้อมูลเหล่านี้สามารถนำไปใช้ในการพัฒนานโยบายภาครัฐต่อไป

เอกสารอ้างอิง

- จินดา สระสมบูรณ์. (2558). ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย. *รัฐสารศึกษ*, 57(2), 57-69.
- ชฎาภรณ์ สิงห์แก้ว. (2564). บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม. *วารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น*, 18(1), 539-552.
- นริศรา พลอยประไพ. (2564). แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง. ค้นเมื่อ 23 กันยายน 2567, จาก <http://awc.ac.th/storage/docs/research/570.pdf>
- ศูนย์ไซเบอร์ทหาร. (2563). แนวทางการดำเนินการจัดการความเสี่ยงด้านไซเบอร์ของ สปช. ทหาร. กรุงเทพฯ: สำนักงานปลัดบัญชาทหาร.
- สัญญา เคนาภูมิ และ และบุรฉัตร จันทรแดง (2562) ตัวแบบทฤษฎีการน านโยบายสาธารณะไปสู่การปฏิบัติ. *วารสารการบริหารการปกครองและนวัตกรรมท้องถิ่น*, 3(1), 95-116.
- สำนักงานสภาพความมั่นคงแห่งชาติ. (2566). แผนปฏิบัติการด้านการบริหารจัดการชายแดนด้านความมั่นคง (2566-2670). สำนักงานสภาพความมั่นคงแห่งชาติ. ค้นเมื่อ 23 กันยายน 2567, จาก <https://www.nsc.go.th/>
- สำนักงานปลัดกระทรวงกลาโหม. (2666). แผนการพัฒนาดิจิทัล กระทรวงกลาโหม (พ.ศ. 2566-2570). ค้นเมื่อ 23 กันยายน 2567, จาก <https://opsd.mod.go.th/Content/PDF/66-70.aspx>
- สำนักงานสภาความมั่นคงแห่งชาติ. (2561). ยุทธศาสตร์การรักษาความ มั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560-2564). กรุงเทพฯ: คณะรัฐมนตรีและราชกิจจานุเบกษา.
- สำนักนายกรัฐมนตรี, สำนักงานสภาความมั่นคงแห่งชาติ. (2560). นโยบายและแผนระดับชาติ ว่าด้วยความมั่นคง แห่ง ชาติ (พ.ศ. 2560-2564). กรุงเทพฯ: สำนักงานสภาความมั่นคงแห่งชาติ.
- Bartholomees, J. B. Jr. (Ed.). (2012). *U.S. Army War College guide to national security issues volume II: National security policy and strategy* (5th ed.). Carlisle, PA: Strategic Studies Institute, U.S. Army War College.
- Kello, L. (2017). The virtual weapon and international order. *JSTOR*. <https://doi.org/10.2307/j.ctt1trkj1>
- Meinhart, R. M. (2010). Chapter 7: National military strategies: 1990 to 2009. *The U.S. Army War College guide to national security issues*, 103-118. <https://www.jstor.org/stable/resrep12024.9>
- NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence is Expanding*. Retrieved September 23, 2024, from <https://ccdcoe.org/news/2017/tallinn-based-nato-cooperative-cyber-defence-centre- of-excellence-is-expanding/>

- Olga, V., et al. (2020). Cybersecurity as a Component of National Security of the State. *Journal of Security and Sustainability Issues*, 9(3), 775-784.
- Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press.
- Singer, P. W., and Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press.
- Williams, W. (1971). *Social policy research and analysis: The experience in the federal social agencies (Policy sciences book series)*. New York: American Elsevier Pub.