การพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ของกองทัพอากาศ

The Development of the Simulated Situations for RTAF Cyber Range

พายัพ ศิรินาม[1*] และ เฉลิมขวัญ ศิริพันธุ์[2]

Payap Sirinam[1*] and Chalermkwan Siripanth[2]

ภาควิชาคอมพิวเตอร์ กองการศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช[1,2]

Computer Department Academic Faculty Navaminda Kasatriyadhiraj Royal Thai Air Force Academy[1,2]

E-Mail: payap_siri@rtaf.mi.th[1*], chalermkwan_s@rtaf.mi.th[2]

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษารูปแบบโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ตามความต้องการของกองทัพอากาศ 2) หาแนวทางการสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ตามความต้องการของผู้ใช้ 3) ประเมินความพึงพอใจในการนำองค์ความรู้สำหรับการสร้างโจทย์สถานการณ์ กลุ่มเป้าหมายของการประเมินจำนวน 16 คนประกอบไปด้วย 1) กลุ่มผู้เชี่ยวชาญจากศูนย์ไซเบอร์กองทัพอากาศ ซึ่งเป็นหน่วยงานที่รับผิดชอบหลักด้านความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศจำนวน 6 คน และ 2) กลุ่มผู้ใช้งานทั่วไป ประกอบด้วยนักเรียนนายเรืออากาศชมรมไซเบอร์ และนายทหารเทคโนโลยีสารสนเทศของหน่วยจำนวน 10 คน โดยใช้แบบประเมินผลความพึงพอใจในการประเมินผลการใช้งาน สหรับสถิติที่ใช้ในการวิเคราะห์ คือ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน

ผลการวิจัยพบว่า 1) รูปแบบการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ที่มีความเหมาะสมกับกองทัพอากาศควรประกอบด้วยโจทย์สำหรับฝึกทักษะการโจมตีระบบและโจทย์สำหรับฝึกทักษะการป้องกันระบบ 2) การสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ สามารถดำเนินการผ่านการศึกษาผังงานแสดงขั้นตอนการปฏิบัติการทางไซเบอร์เพื่อสร้างผังงานแสดงขั้นตอนการสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ ซึ่งช่วยอำนวยความสะดวก และลดช่องว่างทางทักษะของผู้สร้างโจทย์สถานการณ์ได้ 3) ผลการประเมินความพึงพอใจการนำองค์ความรู้การสร้างโจทย์สถานการณ์ไปใช้งานจริง พบว่าผลการประเมินความพึงพอใจโดยรวมอยู่ในระดับมาก ($\bar{X}$ = 4.48, S.D. = 0.49) และผลการประเมินระดับความพึงพอใจต่อความสามารถในการปรับแต่งโจทย์สถานการณ์ พบว่าผลการประเมินความพึงพอใจโดยรวมอยู่ในระดับมาก ($\bar{X}$ = 4.29, S.D. = 0.53) นอกจากนี้ ผลการสัมภาษณ์จากผู้เชี่ยวชาญเพื่อแสวงหาแนวทางในการพัฒนางานวิจัย พบว่างานวิจัยดังกล่าวสามารถพัฒนาต่อยอดเพื่อนำไปใช้ในการพัฒนางานวิจัยที่เกี่ยวข้องกับการพัฒนาสนามจำลองยุทธ์ทางไซเบอร์เพื่อฝึกฝนทางการทหาร การแปลงงานวิจัยไปสู่การจัดการองค์ความรู้เพื่อการเผยแพร่ต่อไป

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์, โจทย์สถานการณ์ทางไซเบอร์, การจำลองยุทธ์ทางไซเบอร์

ABSTRACT

The objectives of this research were to 1) study situational problems for the RTAF cyber range that are in line with the needs of the Royal Thai Air Force (RTAF), 2) explore a guideline to create a cyber range according to the RTAF requirements and 3) perform an assessment of

satisfaction in applying knowledge for creating a situational problem for a cyber range. The researchers evaluated a target group of 16 people consisting of 1) a group of 6 experts from the RTAF Cyber Center, which is the main agency responsible for the cybersecurity of the RTAF, 10 people and 2) a group of 10 general users consisting of cyber club's air cadets and information technology officers of the RTAF units, evaluating by the satisfaction assessment form to evaluate the usage. The statistics used in the analysis were the average and the standard deviation.

The research findings showed that 1) a pattern for developing a situation problem for a cyber warfare model suitable for the RTAF required the inclusion of problems for practicing offensive skills and problems for practicing defensive skills 2) creating a flow of creations for a cyber range helped facilitate and reduced the skill gaps of situation problem creators. 3) satisfaction assessment result of practically applying the knowledge showed that the overall score was at a high level ($\underline{\bar{X}}$ = 4.48, S.D. = 0.49). Moreover, the satisfaction assessment results on the ability to customize the situation problem revealed that the overall score was at a high level ($\underline{\bar{X}}$ = 4.29, S.D. = 0.53). In addition, the results of interviews with experts to seek guidelines for research development revealed that the research can be further developed and used for a higher level of cyber range for military training and be transformed into knowledge management for further dissemination.

Keywords: Cybersecurity, Cyber Situational Problems, Cyber Range

บทนำ

กองทัพอากาศได้ตระหนักถึงความสำคัญถึงการรักษาความมั่นคงของชาติในด้านต่าง ๆ โดยมิติทางไซเบอร์ถือเป็นมิติด้านความมั่นคงที่มีความสำคัญเป็นอย่างยิ่งในปัจจุบัน [1] ด้วยเหตุนี้กองทัพอากาศจัดทำแผนยุทธศาสตร์ที่มุ่งเน้นการพัฒนาบุคลากรที่มีความสามารถในการปฏิบัติการทางไซเบอร์หรือนักรบไซเบอร์ (Cyber Warrior) เพื่อรองรับภัยคุกคามทางไซเบอร์ (Cyber Threats) และสร้างความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ให้กับประเทศผ่านกระบวนการฝึกศึกษารวมถึงการแข่งขันการฝึกปฏิบัติทางไซเบอร์ โดยกระบวนการพัฒนานักรบไซเบอร์ประกอบด้วยภาคทฤษฎีและภาคปฏิบัติ โดยในภาคปฏิบัตินั้น กระบวนการจะมุ่งเน้นให้ผู้เข้ารับการศึกษาได้ทำการฝึกกับโจทย์สถานการณ์ (Simulated Situations) ผ่านแบบจำลองยุทธ์ทางไซเบอร์ (Cyber Range) ซึ่งใช้สำหรับการจำลองแบบจากภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ เช่น การปฏิบัติการในเชิงป้องกันและป้องปราม (Defensive & Offensive) รวมถึงการฝึกปฏิบัติทักษะทางไซเบอร์ที่มีความจำเป็น [4]

ถึงอย่างไรก็ตาม โจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ของกองทัพอากาศที่ใช้อยู่ในปัจจุบันมีข้อจำกัดคือ การขาดโจทย์สถานการณ์ที่มีความทันสมัย ส่งผลให้ไม่สามารถตอบสนองต่อความต้องการในการฝึกศึกษาเพื่อผลิตนักรบไซเบอร์ได้ เนื่องด้วยโจทย์สถานการณ์ที่ใช้อยู่ในปัจจุบันส่วนมาก ต้องแสวงหาจากแหล่งเรียนรู้ทางอินเทอร์เน็ตซึ่งอาจไม่ตรงต่อวัตถุประสงค์ในการฝึก [7] มากไปกว่านั้น หากต้องการสร้างโจทย์สถานการณ์ใหม่

ที่ทันสมัยและสอดคล้องกับวัตถุประสงค์การฝึกก็ถูกจำกัดด้วยงบประมาณ เพราะค่าใช้จ่ายในการออกแบบโจทย์สถานการณ์จากบริษัทผู้เชี่ยวชาญที่ค่อนข้างสูง เนื่องจากองค์ความรู้ในการออกแบบโจทย์สถานการณ์ยังจำกัดอยู่กับผู้ที่มีทักษะและความเชี่ยวชาญเท่านั้น [17]

จากข้อจำกัดในการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ งานวิจัยนี้จึงมุ่งเน้นในการศึกษารูปแบบโจทย์สถานการณ์ต่าง ๆ เพื่อสร้างองค์ความรู้ในการออกแบบและพัฒนาโจทย์ในการจำลองยุทธ์ทางไซเบอร์ ซึ่งในปัจจุบันองค์ความรู้สำหรับการสร้างโจทย์สถานการณ์ทางไซเบอร์นั้นถูกสงวนไว้ให้สามารถเข้าถึงได้โดยผู้เชี่ยวชาญเท่านั้น การศึกษาองค์ความรู้ดังกล่าวจะสามารถช่วยลดภาระทางงบประมาณและการพึ่งพาผู้เชี่ยวชาญจากภายนอกกองทัพอากาศ อีกทั้งเป็นการสร้างองค์ความรู้ที่เป็นระบบที่สามารถนำไปใช้พัฒนาต่อได้

1. วัตถุประสงค์การวิจัย

1.1 เพื่อศึกษารูปแบบโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ตามความต้องการของกองทัพอากาศ

1.2 เพื่อหาแนวทางการสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ตามความต้องการของผู้ใช้

1.3 เพื่อประเมินความพึงพอใจในการนำองค์ความรู้สำหรับการสร้างโจทย์สถานการณ์

2. เอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 แบบจำลองยุทธ์ทางไซเบอร์

แบบจำลองยุทธ์ทางไซเบอร์ (Cyber Range) เป็นการจำลองสภาพแวดล้อมเสมือนของระบบคอมพิวเตอร์ที่ประกอบไปด้วย ระบบฮาร์ดแวร์ ระบบปฏิบัติการ ระบบซอฟต์แวร์ ระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย รวมถึงรูปแบบและกลไกการป้องกันต่าง ๆ ที่ใช้ในการจำลองสภาพแวดล้อมของระบบคอมพิวเตอร์สำหรับการปฏิบัติการในสงครามทางไซเบอร์เพื่อใช้ในการฝึกทักษะ กระบวนการคิด รวมถึงเทคนิคในการโจมตีและการป้องกันภัยคุกคามต่าง ๆ ในมิติไซเบอร์ [17] โดยการฝึกก็จะมีสถานการณ์ต่าง ๆ มาให้ตามที่กำหนดเพื่อให้ผู้เข้ารับการฝึกฝนมีความชำนาญ

2.2 โจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์

โจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ (Cyber Situational Problems for a Cyber Range) เป็นการออกแบบและปรับแต่งรูปแบบของระบบซอฟต์แวร์ที่อยู่บนแบบจำลองยุทธ์ทางไซเบอร์ ให้มีลักษณะตรงตามเป้าประสงค์ของการฝึกทักษะ เช่น การเลือกหรือปรับแต่งระบบปฏิบัติการ (Operating System) การเปิดหมายเลขช่องทางการให้บริการ (Port Number) ของระบบเครือข่าย ให้มีช่องโหว่หรือมีจุดเปราะบางที่สามารถโจมตีได้ (ในกรณีที่ต้องการฝึกทักษะการโจมตี) หรือการแก้ไขเพื่ออุดช่องโหว่ดังกล่าว (ในกรณีที่ต้องการฝึกทักษะการป้องกัน) [17] รวมถึงการเข้ารหัสและถอดรหัสไฟล์ต่าง ๆ โดยรูปแบบโจทย์สถานการณ์อาจอยู่ในรูปแบบของไฟล์สำหรับติดตั้งเครื่องเสมือน (Virtual Machine) ซอฟต์แวร์ที่ถูกปรับแต่ง หรือไฟล์ต่าง ๆ ที่มีรหัสลับซ่อนอยู่เป็นต้น [6] สำหรับโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ สามารถแบ่งออกได้ 2 ประเภท [8] ดังนี้

2.2.1 โจทย์เพื่อฝึกทักษะการป้องกัน (Defensive Skill) ที่มุ่งเน้นการฝึกทักษะในการปกป้องภัยคุกคามทางไซเบอร์จากการโจมตีของผู้ไม่ประสงค์ดี มุ่งเน้นการดำเนินการเชิงรับ (Passive) เช่น การฝึกทักษะการตรวจสอบเพื่อเสาะหาช่องโหว่ของระบบ (Vulnerabilities) นอกจากนี้ยังรวมถึง การฝึกทักษะการเข้ารหัสข้อมูลและการถอดรหัสข้อมูล โดยนักรบไซเบอร์ที่ปฏิบัติการทางไซเบอร์โดยเน้นการป้องกันจะถูกเรียกว่าทีมสีน้ำเงิน (Blue Team)

2.2.2 โจทย์เพื่อฝึกทักษะการป้องปราม (Offensive Skill) ที่มุ่งเน้นการฝึกทักษะการโจมตีและเจาะระบบ รวมถึงสร้างความเสียหายต่อเป้าหมาย เช่น การเจาะเข้าสู่ระบบคอมพิวเตอร์ การทำลายความสามารถในการให้บริการต่าง ๆ ของระบบคอมพิวเตอร์ โดยนักรบไซเบอร์ที่ปฏิบัติการทางไซเบอร์โดยเน้นการโจมตีจะถูกเรียกว่าทีมสีแดง (Red Team)

2.3 เทคโนโลยีการสร้างสภาพแวดล้อมจำลอง

เทคโนโลยีการสร้างสภาพแวดล้อมจำลองของเครื่อง (Virtualization Technology) คือเทคโนโลยีที่ช่วยสร้างเครื่องคอมพิวเตอร์เสมือน (Virtual Machines: VMs) โดยจะทำหน้าที่ในการทำงานในการจำลองทรัพยากรต่าง ๆ บนเครื่องคอมพิวเตอร์ เช่น การจำลองหน่วยประมวลผลกลาง หน่วยความจำ ระบบเครือข่าย [5] โดยโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ จะถูกสร้างขึ้นบนคอมพิวเตอร์เสมือนเพื่อให้ง่ายต่อการติดตั้งใช้งาน รวมถึงมีความอ่อนตัวในการปรับแต่งรายละเอียดโจทย์สถานการณ์ โดยชุดซอฟต์แวร์ที่นิยมใช้งานในการสร้างสภาพแวดล้อมจำลองของเครื่องประกอบไปด้วย VMware and VirtualBox

2.4 การเจาะระบบอย่างมีจริยธรรม

การเจาะระบบอย่างมีจริยธรรม (Certified Ethical Hacking) เป็นหลักสูตรชั้นนำของโลกทางด้านความมั่นคงปลอดภัยไซเบอร์ที่มีวัตถุประสงค์หลักในการสร้างทักษะในการตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายขององค์กร รวมถึงการตรวจหาช่องโหว่โดยใช้เทคนิคและทักษะแบบเดียวกันกับที่ใช้โดยแฮ็กเกอร์ (Hacker) [13] โดยแนวทางการเจาะระบบอย่างมีจริยธรรมประกอบไปด้วย 5 ขั้นตอน ดังนี้

2.4.1 การสำรวจและรวบรวมข้อมูลเกี่ยวกับเป้าหมาย (Reconnaissance) คือ การรวบรวมข้อมูลเกี่ยวกับเครื่องเป้าหมาย เช่น ระบบปฏิบัติการ ชื่อโดเมน รวมทั้งข้อมูลที่เผยแพร่อยู่บนอินเตอร์เน็ต ซึ่งข้อมูลเหล่านี้จะช่วยให้แฮ็กเกอร์สามารถเข้าใจเครื่องเป้าหมายได้มากยิ่งขึ้น

2.4.2 การตรวจสอบระบบ (Scanning) คือ การนำข้อมูลที่ได้จากการสำรวจเพื่อใช้ในการระบุข้อมูลเพิ่มเติมหรือเฉพาะเจาะจงลงไป เช่น เวอร์ชั่นของระบบปฏิบัติการหรือแอปพลิเคชัน หมายเลขช่องทางที่เปิดอยู่หรือหมายเลขพอร์ตที่ให้บริการ ซึ่งจะช่วยในค้นหาช่องโหว่ที่เป็นไปได้ของระบบ

2.4.3 การเข้าถึงเป้าหมาย (Gaining Access) คือ การทดสอบเจาะระบบอย่างแท้จริง โดยการนำข้อมูลที่ได้จากขั้นตอนการตรวจสอบระบบมาทำการวิเคราะห์ถึงแนวทางและวิธีการโจมตีรวมถึงเครื่องมือต่าง ๆ เพื่อใช้ในการโจมตีช่องโหว่ และทำการโจมตีระบบในที่สุด

2.4.4 การคงสภาพการเข้าถึงเป้าหมาย (Maintaining Access) คือ ขั้นตอนหลังจากที่แฮ็กเกอร์ทำการโจมตีเพื่อเจาะเข้าสู่ระบบเป็นที่เรียบร้อยแล้ว แฮ็กเกอร์จะทำการเพิ่มสิทธิ์และเปิดช่องทางพิเศษสำหรับตนเอง (Backdoor) ไว้บนเครื่องเป้าหมายเพื่อให้สามารถย้อนกลับเข้ามาได้อีกครั้ง

2.4.5 การลบร่องรอย (Covering Tracks) คือ ขั้นตอนสุดท้ายที่แฮ็กเกอร์จะทำการลบร่องรอยของการโจมตีเพื่ออำพรางตนเองจากการถูกตรวจสอบจากผู้ดูแลระบบ เช่น การลบ Log File หรือข้อความแจ้งเตือนจากระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS)

จากแนวทางดังกล่าวทำให้ผู้วิจัยสามารถศึกษา และถอดรูปแบบของพฤติกรรมของแฮ็กเกอร์ต่อการโจมตีของระบบในแต่ละขั้นตอน จนทำให้สามารถออกแบบทรัพยากรที่มีความเหมาะสมกับตัวอย่างรูปแบบการโจมตีเพื่อสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ได้

2.5 ผังงาน

ผังงาน (Flowchart) เป็นเครื่องมือแสดงขั้นตอนหรือกระบวนการทำงานที่กระชับ เข้าใจง่าย ช่วยในการบันทึก ถ่ายทอด สื่อสารขั้นตอนการทำงานทำให้ผู้ปฏิบัติเห็นกระบวนงานในภาพรวม และเพิ่มความสะดวกต่อการพิจารณาลำดับขั้นตอนในการทำงาน ผังงานถูกนำไปประยุกต์ใช้ในงานที่เกี่ยวข้องกับวิทยาการคอมพิวเตอร์ เช่น การสร้างและจัดการซอฟต์แวร์ การออกแบบและสร้างอัลกอริทึม [4] จากประโยชน์ของการใช้ผังงานดังกล่าว ผู้วิจัยจึงได้ประยุกต์ใช้งานผังงาน เพื่ออธิบายกระบวนในภาพรวมโดยการศึกษารูปแบบการปฏิบัติการทางไซเบอร์ทั้งการป้องกันและป้องปราม เพื่อออกแบบผังงานในการอธิบายลำดับขั้นตอนของการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ของกองทัพอากาศต่อไป

2.6 งานวิจัยที่เกี่ยวข้อง

Ford et al. [10] ได้ให้มุมมองเกี่ยวกับความสำคัญของการฝึกทักษะทางไซเบอร์ว่า การวิจัยและพัฒนาแบบจำลองยุทธ์ทางไซเบอร์รวมถึงโจทย์สถานการณ์ มีจุดประสงค์หลักเพื่อใช้ในการฝึกฝนทักษะทางไซเบอร์ และสร้างแพลตฟอร์มการฝึกทักษะทางไซเบอร์ที่ผู้ฝึกฝนสามารถเรียนรู้ด้วยตัวเอง (Self-learning Platform) โดยการวิจัยในด้านดังกล่าวถือเป็นจุดเริ่มต้นของงานวิจัยด้านการให้การฝึกศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Education) และถือเป็นหัวข้องานวิจัยที่ได้รับความสนใจจากนักวิจัยเป็นอย่างมากในปัจจุบัน

Endicott & Popovsky [9] ได้ให้มุมมองถึงความท้าทายในเรื่องการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ว่า การฝึกศึกษาเพื่อพัฒนาศักยภาพนักรบไซเบอร์นั้นกำลังประสบปัญหาเกี่ยวกับช่องว่างทางทักษะ (Skill Gap Problem) เนื่องจากการเปลี่ยนแปลงที่รวดเร็วของสภาพแวดล้อมที่เกี่ยวเนื่องกับความมั่นคงปลอดภัยไซเบอร์ เช่น ภัยคุกคามที่เปลี่ยนไปอย่างรวดเร็ว ความซับซ้อนของภัยคุกคาม และภัยคุกคามที่เกิดขึ้นใหม่ในทุก ๆ วัน โดยปัญหาช่องว่างทางทักษะนั้น เป็นความท้าทายที่สำคัญของทั้งผู้ฝึกฝนที่ต้องเรียนรู้ทักษะใหม่ ๆ อยู่เสมอและผู้พัฒนาโจทย์สถานการณ์ที่ต้องมีองค์ความรู้ที่เท่าทันเช่นเดียวกัน ซึ่งสอดคล้องกับมุมมองของ Alotaibi et al. [3] ที่ชี้ให้เห็นว่า โจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ต้องเผชิญกับความท้าทายในการพัฒนารูปแบบโจทย์สถานการณ์ให้เท่าทันกับการเปลี่ยนแปลงของภัยคุกคามในปัจจุบัน

Gurnani et al. [11] ได้จัดประเภทของการฝึกทักษะการปฏิบัติการทางไซเบอร์ (Cybersecurity Exercises) ไว้ 2 ประเภท ได้แก่ 1) การเสวนาเพื่อแลกเปลี่ยนประสบการณ์เพื่อเสริมสร้างทักษะ (Table-top Discussion) และ 2) การฝึกปฏิบัติกับแบบฝึกหัดที่จำลองสถานการณ์จริง (Hands-on Operation-based Exercise) โดยการฝึกทักษะผ่านโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ ถือเป็นการฝึกทักษะการปฏิบัติทางไซเบอร์ในประเภทที่สอง

Yamin & Katt [16] ได้จำแนกประเภทของการฝึกปฏิบัติทางไซเบอร์จากการจำลองสถานการณ์ออกเป็น 2 รูปแบบได้แก่ 1) การฝึกปฏิบัติการโจมตีทางไซเบอร์ (Cyber-attack Exercise) ที่มุ่งเน้นการฝึกหัดและประเมินสมรรถนะการเจาะ/ทำลายระบบ รวมถึงสร้างความเสียหายตามภารกิจหรือวัตถุประสงค์ที่ได้รับมอบหมาย 2) การฝึกปฏิบัติการป้องกันทางไซเบอร์ (Cyber-defense Exercise) ที่มุ่งเน้นการฝึกหัดและประเมินสมรรถนะการป้องกันต่อการโจมตีด้านไซเบอร์ รวมถึงทักษะการเข้ารหัส/ถอดรหัสไฟล์ข้อมูล

คณะผู้วิจัยจากโรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช กองทัพอากาศ ได้ริเริ่มดำเนินการวิจัยเพื่อพัฒนาแบบจำลองยุทธ์ทางไซเบอร์ ปุณณวิช ธรรมาธร และคณะ [2] ได้ทำการศึกษาวิจัยเกี่ยวกับงานวิจัยเกี่ยวกับการทำงานของระบบโครงสร้างพื้นฐานบนเทคโนโลยีการประมวลผลแบบคลาวด์เพื่อสร้างแบบจำลองยุทธ์ต้นแบบเพื่อเป็นแนวทางในการสร้างสนามจำลองการโจมตีทางไซเบอร์ของนักเรียนนายเรืออากาศ และใช้เป็นแพลตฟอร์มในการติดตั้งโจทย์สถานการณ์ในอนาคต โดยงานวิจัยดังกล่าวมุ่งเน้นการสร้างระบบโครงสร้างพื้นฐานของแบบจำลองยุทธ์ แต่ยังคงใช้โจทย์สถานการณ์สำเร็จรูปจากแหล่งข้อมูลในอินเทอร์เน็ตเป็นหลัก

จากผลการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องจะเห็นว่า งานวิจัยตั้งแต่อดีตจนถึงปัจจุบัน มุ่งเน้นการศึกษาถึงแนวทางการพัฒนาทักษะทางไซเบอร์ ประเภทโจทย์สถานการณ์ รวมถึงการพัฒนาระบบโครงสร้างพื้นฐานด้านฮาร์ดแวร์เพื่อรองรับแบบจำลองยุทธ์ทางไซเบอร์ ถึงอย่างไรก็ตาม ความท้าทายด้านวิธีการหรือแนวทางในการพัฒนาโจทย์สถานการณ์และข้อจำกัดด้านช่องว่างทางความรู้ที่จำเป็นต้องใช้ผู้เชี่ยวชาญ ยังคงเป็นโจทย์วิจัยที่สำคัญ และผู้วิจัยได้เลือกโจทย์วิจัยดังกล่าวในการศึกษาและพัฒนาเพื่อแก้ไขปัญหาและความท้าทายดังกล่าว

วิธีดำเนินการวิจัย

1. เครื่องมือการวิจัย

1.1 เครื่องมือในการสร้างแบบจำลองยุทธ์ทางไซเบอร์ รวมถึงโจทย์สถานการณ์ต่าง ๆ ประกอบไปด้วยระบบฮาร์ดแวร์ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวน 2 เครื่อง เพื่อใช้สร้างระบบเครื่องเสมือน (Virtual Machines) และ เครื่องคอมพิวเตอร์ลูกข่าย (Clients) จำนวน 10 เครื่อง เพื่อสร้างโจทย์สถานการณ์รวมถึงการทดสอบโจทย์สถานการณ์โดยนักรบไซเบอร์ สำหรับระบบซอฟต์แวร์ ผู้วิจัยใช้ โปรแกรม VMware Workstation เพื่อสร้างเครื่องจำลองที่ใช้บรรจุโจทย์สถานการณ์ทางไซเบอร์ที่ได้รับการออกแบบเรียบร้อยแล้ว ระบบปฏิบัติการ Kali Linux [15] ซึ่งเป็นระบบปฏิบัติการที่ใช้ในการสร้าง ปรับแต่ง และทดสอบระบบปฏิบัติการทางไซเบอร์ ร่วมกับระบบปฏิบัติการ Microsoft Windows 10

1.2 แบบประเมินความพึงพอใจในการนำองค์ความรู้การสร้างโจทย์สถานการณ์ไปใช้งานจริง รวมถึงความสามารถในการปรับแต่งโจทย์สถานการณ์จากผู้เชี่ยวชาญด้านการปฏิบัติการทางไซเบอร์และผู้ใช้งานทั่วไป ผู้วิจัยใช้แบบสอบถามประเมินความพึงพอใจ โดยลักษณะของแบบสอบถามเป็นแบบมาตราส่วนประมาณค่า (Rating Scale) 5 ระดับของลิเคิร์ท (Likert Scale) [12]

2. กลุ่มเป้าหมาย

2.1 ผู้เชี่ยวชาญด้านการปฏิบัติการทางไซเบอร์จากศูนย์ไซเบอร์กองทัพอากาศ จำนวน 6 คน ประกอบด้วย

- พลอากาศตรี วิสุทธิ์ สมภักดี ผู้อำนวยการศูนย์ไซเบอร์กองทัพอากาศ

- นาวาอากาศเอก อมร ชมเชย ผู้อำนวยการกองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ (ปัจจุบันดำรงตำแหน่ง เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ)
- นาวาอากาศตรี บุรีรัตน์ เข็มทอง กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
- เรืออากาศโท นพรัตน์ สุจินดา กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
- เรืออากาศตรี รักพงศ์ วงศ์ปัญญาดี กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
- เรืออากาศตรี วุฒิภัทร นัทธี กองฝึกและพัฒนาไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

2.2 กลุ่มผู้ใช้งานทั่วไป ประกอบด้วยนักเรียนนายเรืออากาศสาขาวิชาคอมพิวเตอร์ที่อยู่ในชมรมไซเบอร์และนายทหารเทคโนโลยีสารสนเทศของหน่วยที่ได้รับการอบรมขั้นต้นด้านวิทยาการคอมพิวเตอร์และมีความรู้พื้นฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ แต่ยังไม่เคยสอบผ่านและได้รับใบรับรองความเชี่ยวชาญด้านไซเบอร์ใด ๆ มาก่อน ซึ่งถือเป็นผู้ปฏิบัติงานจริงและเป็นผู้ได้รับผลกระทบต่อความท้าทายในด้านองค์ความรู้ด้านการพัฒนาโจทย์สถานการณ์ทางไซเบอร์ จำนวน 10 คน

3. ขั้นตอนการดำเนินการวิจัย

เนื่องจากการพัฒนาโจทย์สถานการณ์การจำลองยุทธ์ทางไซเบอร์ มีลักษณะคล้ายคลึงกับการพัฒนาซอฟต์แวร์ขึ้นมาใหม่ ดังนั้น ผู้วิจัยจึงใช้รูปแบบของขั้นตอนการพัฒนาซอฟต์แวร์รวมถึงการประยุกต์ใช้ผังงานในการช่วยให้ผู้นำไปประยุกต์ใช้สามารถเข้าใจในขั้นตอนการพัฒนาได้ง่ายขึ้น โดยผู้วิจัยได้ทำการดำเนินงานวิจัยโดยมีขั้นตอนดังนี้

3.1 ขั้นตอนการวิเคราะห์และออกแบบระบบ

ในขั้นตอนนี้ เป็นการวิเคราะห์ว่า ประเภทและโจทย์สถานการณ์ทางไซเบอร์ที่มีความเหมาะสมกับการพัฒนาทักษะทางไซเบอร์ของกองทัพอากาศมีลักษณะอย่างไร เพื่อเป็นข้อมูลพื้นฐานในการออกแบบระบบการพัฒนาโจทย์สถานการณ์ในขั้นตอนต่อไป

3.1.1 การศึกษาและรวบรวมข้อมูลเกี่ยวกับการแข่งขันทักษะทางไซเบอร์ของกองทัพอากาศย้อนหลัง 3 ปี (2561 - 2563) เพื่อนำข้อมูลมาวิเคราะห์โจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ เพื่อกำหนดประเภทและคัดเลือกโจทย์สถานการณ์ให้สอดคล้องและตรงตามความต้องการของกองทัพอากาศ

3.1.2 การศึกษาโจทย์สถานการณ์จากการทดลองปฏิบัติ

ผู้วิจัยได้เริ่มทำการศึกษาและลองทำโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์เพื่อศึกษาองค์ประกอบของโจทย์สถานการณ์ และวิเคราะห์แนวทางการปฏิบัติ ทำให้ผู้วิจัยสามารถวิเคราะห์เส้นทางการปฏิบัติการทางไซเบอร์ในแต่ละขั้นตอน (Step-by-step) เพื่อสร้างรูปแบบการปฏิบัติการผ่านผังงานแสดงขั้นตอนการปฏิบัติการทางไซเบอร์ (Flow of Actions)

จากนั้นผู้วิจัยทำการวิเคราะห์ผ่านผังงานแสดงขั้นตอนการปฏิบัติการทางไซเบอร์ เพื่อศึกษารูปแบบร่วมหรือแนวทางของกระบวนการสร้างโจทย์ โดยการสร้างโจทย์จะเริ่มจากการสร้างจุดประสงค์และการเลือกองค์ประกอบต่าง ๆ เช่น ระบบปฏิบัติการ ช่องโหว่ที่เข้าถึงได้ สภาพแวดล้อมของโจทย์ และข้อจำกัด

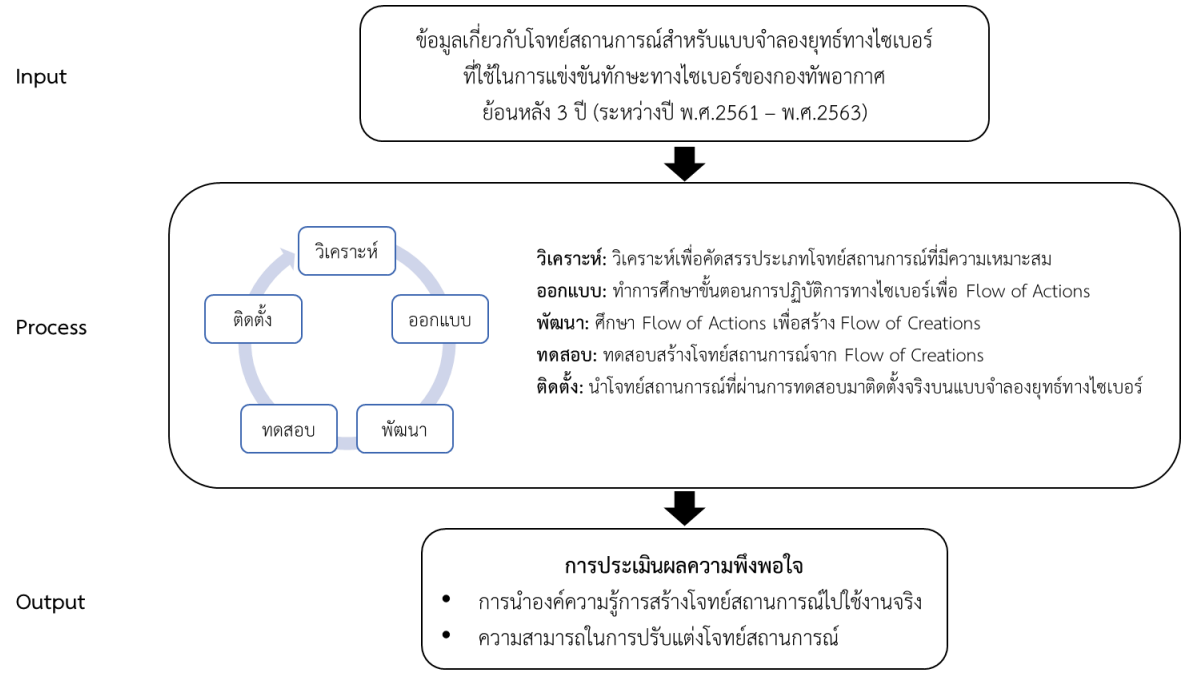
3.1.3 การสร้างองค์ความรู้ที่ใช้ในการสร้างโจทย์สถานการณ์

ผู้วิจัยนำผลการศึกษาโจทย์สถานการณ์จากการทดลองปฏิบัติ มาสร้างองค์ความรู้ในการสร้างโจทย์สถานการณ์และจัดทำผังงานแสดงขั้นตอนการสร้างโจทย์สถานการณ์ (Flow of Creations) และทดสอบการสร้างโจทย์สถานการณ์จริงจากผังงานดังกล่าว รวมถึงการติดตั้งบนแพลตฟอร์มแบบจำลองยุทธ์ทางไซเบอร์เพื่อทดสอบความถูกต้องและผลลัพธ์ของการสร้างโจทย์สถานการณ์ จากนั้นทำการทดสอบหาข้อผิดพลาดที่อาจเกิดขึ้น

3.2 ขั้นตอนการประเมินผลความพึงพอใจ

เมื่อผู้วิจัยดำเนินการจัดทำองค์ความรู้ด้านการสร้างโจทย์สถานการณ์ทางไซเบอร์ผ่านผังงานแสดงขั้นตอนการปฏิบัติการและการสร้างโจทย์สถานการณ์ พร้อมทั้งทดสอบสร้างโจทย์สถานการณ์เรียบร้อยแล้ว ขั้นตอนต่อไปผู้วิจัยได้ทำการวัดผลการวิจัยผ่าน การตอบแบบสอบถามความพึงพอใจรวมถึงการสัมภาษณ์ผู้เชี่ยวชาญด้านการปฏิบัติการทางไซเบอร์จากศูนย์ไซเบอร์กองทัพอากาศรวมถึงกลุ่มผู้ใช่งานทั่วไปซึ่งถือเป็นผู้ใช้งานหลัก โดยมีการตรวจสอบคุณภาพของเครื่องมือวิจัยผ่านการตรวจพิจารณาความเที่ยงตรงรายข้อหรือการหาค่า IOC (The Index of Item-Objective Congruence) ของแบบทดสอบจากผู้เชี่ยวชาญด้านสถิติจำนวน 3 ท่าน โดยผลการวิเคราะห์พบว่าข้อคำถามแต่ละข้อมีค่า IOC อยู่ระหว่าง 0.67-1.00 ซึ่งถือว่ามีความเที่ยงตรง

กรอบแนวคิดในการดำเนินการวิจัยตามรายละเอียดขั้นตอนการดำเนินการวิจัย ผู้วิจัยได้ดำเนินการตามหลักวงจรการพัฒนาซอฟต์แวร์ (Software Development Life Cycle: SDLC) [14] ซึ่งมีความสอดคล้องกับการพัฒนาโจทย์สถานการณ์ที่อยู่ในรูปแบบของการสร้างและการปรับแต่งซอฟต์แวร์ที่เกี่ยวข้องให้มีความเหมาะสมกับวัตถุประสงค์ของการปฏิบัติการทางไซเบอร์ แสดงดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดในการทำวิจัย

4. สถิติที่ใช้ในการวิจัย

ผู้วิจัยทำการประเมินการวิจัยผ่านการประเมินผลความพึงพอใจ ซึ่งได้จากแบบสอบถามที่ใช้มาตราส่วนประมาณค่า 5 ระดับของลิเคิร์ท (Likert Scale) โดยนำผลคะแนนเฉลี่ยที่ได้เทียบกับเกณฑ์การประเมิน ดังนี้

ค่าเฉลี่ยเท่ากับ 4.51 – 5.00	หมายความว่า ระดับมากที่สุด
ค่าเฉลี่ยเท่ากับ 3.51 – 4.50	หมายความว่า ระดับมาก
ค่าเฉลี่ยเท่ากับ 2.51 – 3.50	หมายความว่า ระดับปานกลาง
ค่าเฉลี่ยเท่ากับ 1.51 – 2.50	หมายความว่า ระดับน้อย
ค่าเฉลี่ยเท่ากับ 1.01 – 1.50	หมายความว่า ระดับน้อยที่สุด

ผลการวิจัย

1. ผลการศึกษาและรวบรวมข้อมูลเกี่ยวกับการแข่งขันทักษะทางไซเบอร์ของกองทัพอากาศ

ผู้วิจัยได้ทำการศึกษาและรวบรวมข้อมูลเกี่ยวกับโจทย์สถานการณ์จากการแข่งขันทักษะทางไซเบอร์กองทัพอากาศย้อนหลัง 3 ปี พบว่าโจทย์สถานการณ์ในปัจจุบันมีความหลากหลายเพิ่มขึ้นตามภัยคุกคามทางไซเบอร์และถูกแบ่งออกเป็น 2 ประเภท คือ ได้แก่ 1) โจทย์ Red Team ซึ่งเป็นโจทย์ที่มุ่งเน้นการป้องปรามหรือโจทย์ที่เกี่ยวข้องกับผู้ทำการโจมตีและ 2) โจทย์ประเภท Blue Team ซึ่งเป็นโจทย์ที่มุ่งเน้นการป้องกันซึ่งเกี่ยวข้องกับผู้ดูแลระบบในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ทางผู้วิจัยได้ทำการทดสอบโจทย์สถานการณ์กว่า 30 โจทย์สถานการณ์จากการแข่งขันทักษะทางไซเบอร์กองทัพอากาศ และทำการคัดเลือกตัวอย่างประเภทของโจทย์สถานการณ์เพื่อเป็นตัวอย่างในการทำวิจัย จำนวน 6 ข้อ โดยแบ่งเป็นประเภทของโจทย์ดังนี้

1.1 โจทย์ประเภท Red Team จำนวน 3 ข้อ ได้แก่

- *Upload Shell (WebDav)*
- *Command Injection*
- *SQL Injection Bypass Login*

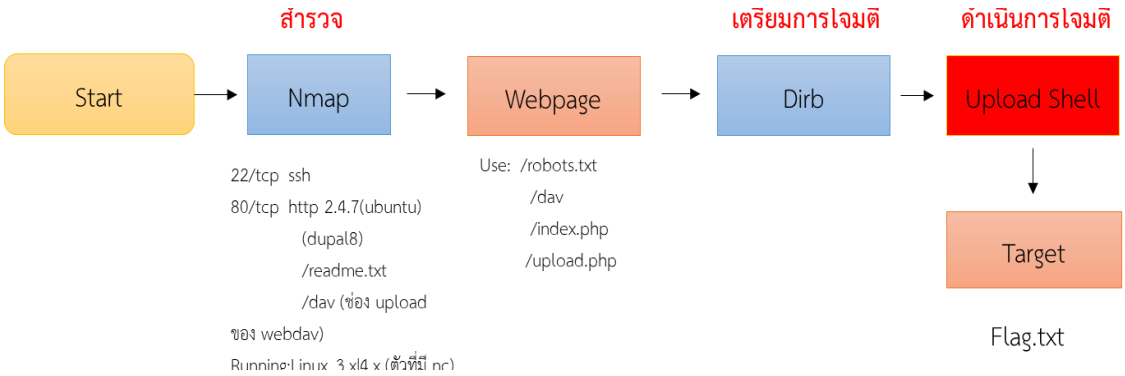
1.2 โจทย์ประเภท Blue Team จำนวน 3 ข้อ ได้แก่

- *Reverse flagflagflag*
- *Programming*
- *Forensic*

2. ผลการศึกษาโจทย์สถานการณ์ประเภท Red Team

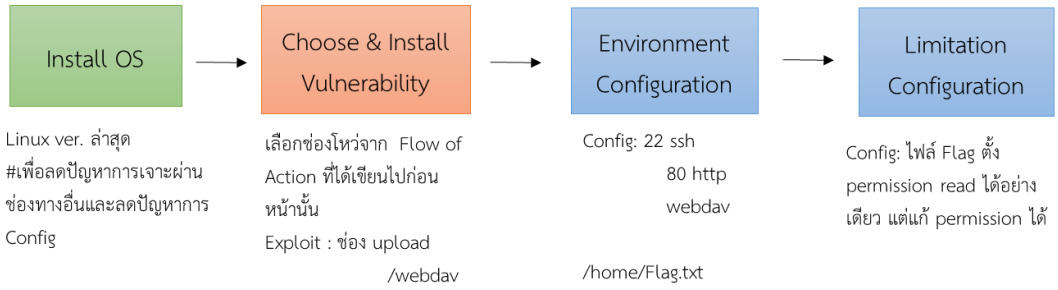
ผลการศึกษาและจากการทดลองทำโจทย์สถานการณ์ ทำให้ผู้วิจัยสามารถวิเคราะห์รูปแบบการปฏิบัติการทางไซเบอร์โดยพบว่า ขั้นตอนการปฏิบัติการทางไซเบอร์สำหรับโจทย์ประเภท Red Team มีความสอดคล้องเป็นไปตามแนวทาง 5 ขั้นตอนของการเจาะระบบอย่างมีจริยธรรม (Certified Ethical Hacking) ดังนั้น การเขียนผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) สามารถยึดโยงกับ 5 ขั้นตอนของการเจาะระบบอย่างมีจริยธรรม โดยผู้วิจัยสังเกตว่า ในทางปฏิบัติจริงผู้วิจัยสามารถผสานรวมขั้นตอนเพื่อให้เกิดความง่ายต่อความเข้าใจให้เหลือเพียง 3 ขั้นตอนหลักประกอบด้วย 1) การสำรวจและหาช่องโหว่ (Scanning) 2) การเตรียมการโจมตี (Preparation) และ

3) การดำเนินการโจมตี (Operations) เนื่องจากในขั้นตอนที่ 4 และขั้นตอนที่ 5 ซึ่งเกี่ยวข้องกับการสร้างช่องทางการโจมตีในอนาคตและการลบร่องรอยการโจมตีสามารถผนวกรวมในขั้นตอนที่ 3 ได้



ภาพที่ 2 ผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) ของโจทย์ *Upload Shell (WebDav)*

ภาพที่ 2 แสดงผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) ของโจทย์ *Upload Shell (WebDav)* ซึ่งเป็นการสร้างโจทย์สถานการณ์ที่จำลองเครื่องเป้าหมายที่มีช่องโหว่ในช่องทางการอัปโหลดที่ไม่ได้มีการตรวจสอบประเภทของไฟล์ให้ถี่ถ้วน ทำให้แฮ็กเกอร์สามารถใช้ช่องโหว่ดังกล่าวในการโจมตีระบบได้ จะเห็นว่า Flow of Actions มีความสอดคล้องกับ 3 ขั้นตอนที่กล่าวไปข้างต้นซึ่งประกอบไปด้วย การสำรวจโดยการใช้เครื่องมือ *Nmap* เพื่อหาหมายเลขช่องทางการให้บริการที่เปิดอยู่ รวมถึงหาช่องโหว่ที่เป็นไปได้ของระบบซึ่งต้องใช้เครื่องมือที่เกี่ยวข้องได้แก่เครื่องมือ *Dirb* ซึ่งเป็นโปรแกรมในการทำการตรวจหาไฟล์จากเครื่องเป้าหมาย จากนั้นก็ทำการโจมตีต้องทำการอัปโหลดโปรแกรมที่ถูกเขียนขึ้นสำหรับการโจมตี (Shell) เข้าไปเพื่อทำการยึดเครื่องเป้าหมาย



ภาพที่ 3 ผังงานแสดงขั้นตอนการสร้าง (Flow of Creations) ของโจทย์ *Upload Shell (WebDav)*

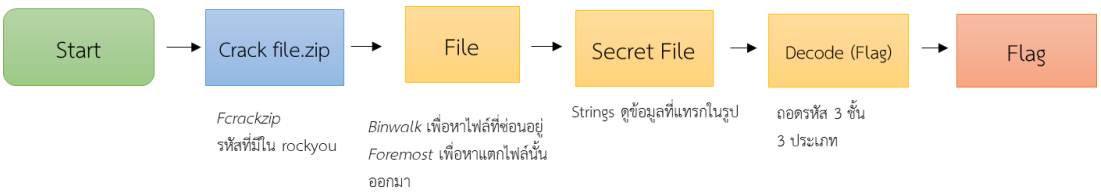
เมื่อได้ผังงานการสร้างโจทย์สถานการณ์เรียบร้อยแล้ว ขั้นตอนต่อไปเป็นการนำเอาผังงานการสร้างโจทย์เพื่อศึกษารูปแบบการปรับแต่งต่าง ๆ เช่น ช่องโหว่ที่มี ไฟล์ที่ต้องมี หมายเลขช่องทางการให้บริการที่เปิดไว้ รวมถึงคุณลักษณะของระบบปฏิบัติการ เพื่อนำไปออกแบบผังงานแสดงขั้นตอนการสร้าง (Flow of Creations) แสดงดังภาพที่ 3 ผู้วิจัยพบว่า ในโจทย์ประเภท Red Team ในทุก ๆ โจทย์มีขั้นตอนการสร้างที่มีลักษณะคล้ายคลึงกันประกอบไปด้วย 1) ขั้นตอนการติดตั้งระบบปฏิบัติการ (Install OS) ซึ่งเป็นการระบุข้อมูลระบบปฏิบัติการที่ต้องใช้

ในการติดตั้งบนเครื่องเสมือน 2) การเลือกช่องโหว่ที่จะทำการฝังไว้ในโจทย์สถานการณ์ (Choose & Install Vulnerability) ซึ่งเป็นการทำเครื่องเสมือนที่ไม่มีช่องโหว่ให้เกิดช่องโหว่ที่ต้องการขึ้น 3) การปรับแต่งสภาพแวดล้อมของเครื่อง (Environment Configuration) ซึ่งเป็นการปรับแต่งเครื่องเสมือนเพื่อทำให้สามารถเข้าถึงได้ เช่น การเปิดช่องทางการให้บริการหรือหมายเลขพอร์ทรวมถึงการอัปโหลดไฟล์ที่เกี่ยวข้อง และ 4) การกำหนดข้อจำกัดเพิ่มเติมต่าง ๆ (Limitation Configuration) เพื่อเพิ่มความท้าทายของโจทย์สถานการณ์ จะเห็นว่าข้อมูลในขั้นตอนที่ 1 ถึงขั้นตอนที่ 4 ในการสร้างโจทย์สถานการณ์ เป็นผลลัพธ์จากการศึกษาและความเข้าใจข้อมูลผังงานแสดงขั้นตอนการปฏิบัติในขั้นตอนก่อนหน้านี้

ผลการศึกษาพบว่า โจทย์สถานการณ์ประเภท Red Team ทุก ๆ โจทย์มีความสอดคล้องในขั้นตอนการออกแบบผังงานแสดงขั้นตอนการปฏิบัติ รวมถึงขั้นตอนในการออกแบบผังงานแสดงขั้นตอนการสร้าง ซึ่งถือเป็นจุดเด่นที่แสดงให้เห็นว่า องค์ความรู้ในการสร้างโจทย์สถานการณ์ประเภท Red Team สามารถถูกจัดรูปแบบให้เป็นระบบได้ ซึ่งจะเป็นประโยชน์ต่อการพัฒนาโจทย์สถานการณ์ประเภทดังกล่าวได้ในอนาคต

3. ผลการศึกษาโจทย์สถานการณ์ประเภท Blue Team

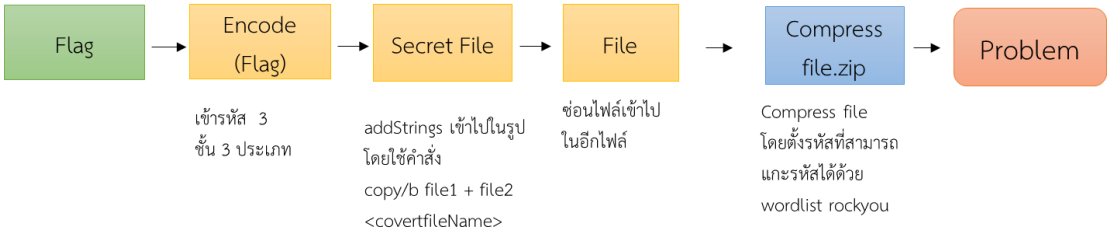
สำหรับขั้นตอนการปฏิบัติการทางไซเบอร์สำหรับโจทย์ประเภท Blue Team มีลักษณะที่แตกต่างจากโจทย์ประเภท Red Team เนื่องจากไม่สามารถจัดขั้นตอนการปฏิบัติเพื่อสร้างผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) ที่แน่นอนและเหมือนกันในทุก ๆ โจทย์สถานการณ์ได้ เนื่องจากรูปแบบการปฏิบัติการทางไซเบอร์ประเภท Blue Team มีความหลากหลาย ตั้งแต่การปกป้องระบบเครือข่าย จนถึงการเข้ารหัส/ถอดรหัสข้อมูล อย่างไรก็ตาม แนวคิดการประยุกต์ใช้ผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) เพื่อให้เกิดความเข้าใจแนวทางการในการสร้างโจทย์ผ่านผังงานแสดงขั้นตอนการสร้าง (Flow of Creations) เพื่อสร้างความเข้าใจในขั้นตอนการปฏิบัติยังสามารถใช้งานได้ โดยผู้ปฏิบัติสามารถเรียนรู้คุณลักษณะของโจทย์ ช่องโหว่ของระบบ เทคนิคการเข้ารหัสในขั้นตอนการปฏิบัติการทางไซเบอร์ เพื่อใช้เป็นข้อมูลพื้นฐานในการดำเนินสร้างโจทย์ได้ โดยผู้วิจัยประสบความสำเร็จในการสร้างโจทย์จากผังงานแสดงขั้นตอนการสร้าง ที่เป็นผลลัพธ์จากการศึกษาผังงานแสดงขั้นตอนการปฏิบัติในทุก ๆ โจทย์สถานการณ์ ซึ่งแสดงให้เห็นว่าการประยุกต์ใช้ผังงานแสดงขั้นตอนการปฏิบัติและผังงานแสดงขั้นการสร้าง มีส่วนช่วยอำนวยความสะดวก และลดช่องว่างทางทักษะในการสร้างโจทย์สถานการณ์ทางไซเบอร์ได้



ภาพที่ 4 ผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) ของโจทย์ *Forensic*

จากภาพที่ 4 ผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) ของโจทย์ *Forensic* ซึ่งเป็นโจทย์สถานการณ์ในการฝึกทักษะของ Blue Team ในการถอดรหัสไฟล์จากข้อมูลที่ถูกบีบอัดพร้อมตั้งรหัสผ่านในรูปแบบ

ของ Zip File จากผังงานแสดงให้เห็นขั้นตอนการปฏิบัติการทางไซเบอร์ที่ละขั้น ตั้งแต่การใช้เครื่องมือ *Fcrackzip* ในการแก้รหัสผ่านจากฐานข้อมูลชุดรหัสผ่าน rockyou จากนั้นทำการหาไฟล์ที่มีข้อมูลที่น่าสงสัยซ่อนอยู่ เช่น ข้อมูลที่มีรูปแบบการเรียงตัวซึ่งมีลักษณะจำเพาะผ่านเครื่องมือ *Binwalk* และ *Foremost* จากนั้นทำการถอดรหัส (Decoding) ด้วยเครื่องมือการถอดรหัสต่าง ๆ จำนวน 3 ครั้งอย่างต่อเนื่องโดยทดลองกับอัลกอริทึมที่แตกต่างกัน เพื่อให้ได้ธงคำตอบ (Flag) ซึ่งเป็นข้อความลับที่ถูกซ่อนไว้



ภาพที่ 5 ผังงานแสดงขั้นตอนการสร้าง (Flow of Creations) ของโจทย์ *Forensic*

เมื่อได้ผังงานการสร้างโจทย์สถานการณ์เรียบร้อยแล้ว ผู้วิจัยได้ทดสอบสร้างโจทย์สถานการณ์โดยใช้ข้อมูลที่ได้จากผังงานการสร้างโจทย์เพื่อศึกษารูปแบบการปรับแต่งค่าต่าง ๆ สำหรับขั้นตอนประกอบด้วย

ขั้นตอนที่ 1 ทำการทดลองสร้างไฟล์เครื่องจำลองโจทย์สถานการณ์ซ้ำขึ้นมาใหม่โดยอ้างอิงจาก ผังงานแสดงขั้นตอนการสร้าง (Flow of Creations) โดยมีดำเนินการปรับแต่งไฟล์และสภาพแวดล้อมของระบบเครื่องจำลองให้สอดคล้องกับผังงาน เช่น การเลือกระบบปฏิบัติการ การเปิดหมายเลขการให้บริการ (Port Numbers) การแก้ไขไฟล์ของระบบ (System Files) เพื่อเปิดช่องโหว่ หรือช่องทางในการโจมตี

ขั้นตอนที่ 2 ทำการทดสอบความสามารถในการใช้งานได้ของโจทย์สถานการณ์ที่ถูกสร้างขึ้นจากขั้นตอนที่ 1 โดยผู้เชี่ยวชาญซึ่งเป็นผู้ที่มีทักษะและประสบการณ์ในการสร้างโจทย์สถานการณ์ทางไซเบอร์มาก่อนเพื่อตรวจสอบว่า โจทย์สถานการณ์มีคุณลักษณะตามที่ต้องการหรือไม่ผ่าน เช่น การทดสอบการปฏิบัติการโจมตีทางไซเบอร์เพื่อตรวจสอบว่ามีช่องโหว่ครบตามวัตถุประสงค์ และสามารถปฏิบัติการโจมตีทางไซเบอร์ได้ตามขั้นตอนที่ต้องการ รวมถึงการทดสอบความสามารถในติดตั้งและประมวลผลบนเครื่องคอมพิวเตอร์ที่ระบุไว้

การทดสอบถูกดำเนินการมากกว่า 1 ครั้งบนสภาพแวดล้อมที่แตกต่างกัน เช่น การติดตั้งและทดสอบโจทย์บนโปรแกรมจำลองระบบทั้ง VMware และ VirtualBox บนระบบปฏิบัติการ Microsoft Windows และ Ubuntu จนมั่นใจว่า โจทย์สถานการณ์สามารถใช้งานได้ ถึงอย่างไรก็ตาม หากโจทย์สถานการณ์บางประเภทมีความต้องการของระบบที่อาจเป็นข้อจำกัด เช่น หน่วยความจำพื้นฐานขั้นต่ำ ความเร็วของหน่วยประมวลผลกลางขั้นต่ำ

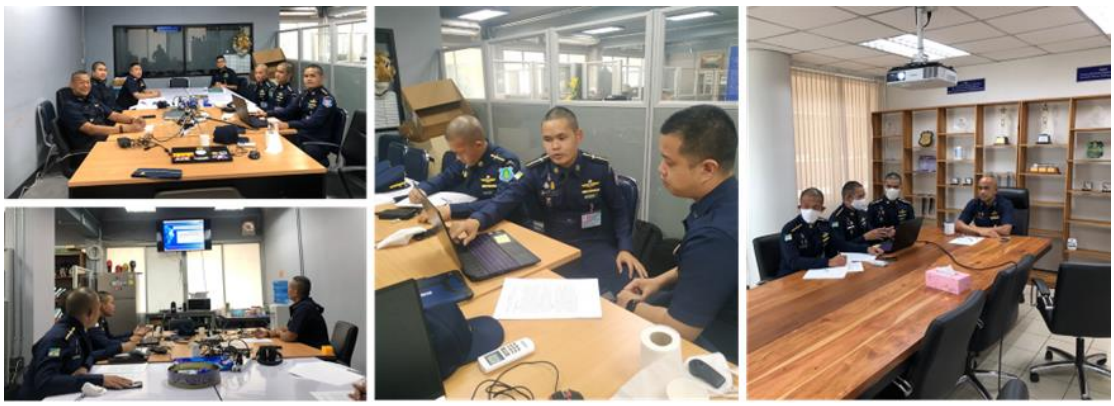
สำหรับลักษณะเด่นของการสร้างโจทย์ประเภท Blue Team คือ การสร้างโจทย์แบบย้อนกลับจะเริ่มต้นจากคำตอบของโจทย์ ซึ่งในกรณีนี้คือไฟล์ข้อมูลลับ และทำการเข้ารหัสไฟล์ดังกล่าว 3 ครั้งด้วยเทคนิคที่แตกต่างกัน จากนั้นจึงผังข้อมูลที่เข้ารหัสเข้าไปในไฟล์และทำการบีบอัดในรูปแบบ Zip File ที่มีการตั้งรหัสผ่านที่อยู่ในฐานข้อมูลของ rockyou เข้าไปเพื่อสร้างโจทย์ในขั้นสุดท้าย

ผลการศึกษาพบว่า ผู้วิจัยสามารถสร้างโจทย์สถานการณ์ประเภท Blue Team ขึ้นมาใหม่ได้ในทุก ๆ โจทย์ โดยใช้ข้อมูลจากผังงานแสดงขั้นตอนการปฏิบัติ พร้อมทั้งทำซ้ำเป็นวงรอบเช่นนี้หลาย ๆ ครั้งจนเกิดความมั่นใจว่า แนวทางดังกล่าวสามารถนำไปประยุกต์ใช้งานเพื่อสร้างโจทย์สถานการณ์ได้จริง

ท้ายที่สุด ผู้วิจัยได้ทดสอบในการนำโจทย์สถานการณ์ที่สร้างขึ้น จัดให้อยู่ในรูปแบบไฟล์เครื่องเสมือน (VMware File) และทดสอบการติดตั้งบนระบบเครื่องจำลอง (Virtual Machine) พร้อมทดลองการใช้งาน ผู้วิจัยพบว่า โจทย์สถานการณ์ที่ถูกสร้างขึ้น สามารถติดตั้งได้อย่างเรียบร้อยไม่มีอุปสรรคใด ๆ ในการใช้งาน

4. ผลการประเมินโดยผู้ใช้งาน

ถึงแม้ว่าผลการทดสอบโดยผู้วิจัยชี้ให้เห็นว่า แนวทางการสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ด้วยการสร้างผังงานแสดงขั้นตอนการปฏิบัติเพื่อนำไปสู่การออกแบบผังงานแสดงขั้นตอนการสร้างสามารถดำเนินการได้อย่างมีประสิทธิผล ผู้วิจัยตระหนักถึงความสำคัญของการประเมินผลการใช้งานจริงผ่านการประเมินผลโดยผู้ใช้งาน



ภาพที่ 6 การสัมภาษณ์ผู้เชี่ยวชาญและการทดสอบการใช้งานจริง ณ ศูนย์ไซเบอร์กองทัพอากาศ

เพื่อให้ผลลัพธ์ที่รอบด้าน ผู้วิจัยจึงได้ทำการประเมินความพึงพอใจจากทั้งผู้เชี่ยวชาญด้านการปฏิบัติการทางไซเบอร์จากศูนย์ไซเบอร์กองทัพอากาศ จำนวน 6 คน และผู้ใช้งานจริงที่มีความรู้ขั้นต้นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ไม่ใช่ผู้เชี่ยวชาญด้านไซเบอร์ (ไม่มีใบรับรองคุณวุฒิด้านไซเบอร์) ซึ่งประกอบไปด้วยนักเรียนนายอากาศชมรมไซเบอร์และนายทหารเทคโนโลยีสารสนเทศของหน่วย จำนวน 10 คน รวมทั้งสิ้น 16 คน แสดงดังภาพที่ 6 โดยก่อนทำการประเมินความพึงพอใจ ผู้วิจัยได้มีการถ่ายทอดองค์ความรู้ในการใช้ประโยชน์จากการใช้ผังงาน พร้อมอธิบายแนวทางประยุกต์ใช้ผังงานแสดงขั้นตอนการปฏิบัติและผังงานแสดงขั้นตอนการสร้าง พร้อมทั้งให้ผู้ประเมินได้ทำการทดสอบสร้างโจทย์ตามแนวทางดังกล่าวอย่างน้อยคนละ 3 โจทย์ รวมถึงการให้ผู้ประเมินได้ทำความเข้าใจในกลไกการสร้างโจทย์ผ่านการทดลองปรับแต่งโจทย์สถานการณ์ตามความต้องการของตนเอง เช่น การปรับแต่งอัลกอริทึมในการเข้ารหัส การปรับแต่งช่องโหว่เพื่อสร้างโจทย์สถานการณ์ใหม่ จากนั้นนำผลการทดสอบความพึงพอใจมาวิเคราะห์ด้วยค่าสถิติพื้นฐานเทียบกับเกณฑ์และสรุป แสดงดังตารางที่ 1 และตารางที่ 2

ตารางที่ 1 ผลการประเมินระดับความพึงพอใจต่อการนำองค์ความรู้การสร้างโจทย์สถานการณ์ไปใช้งานจริง

รายการ	$\bar{x}$	S.D.	ระดับความคิดเห็น
1. ผู้สร้างโจทย์สามารถเข้าใจขั้นตอนในการสร้างโจทย์สถานการณ์ได้ดีขึ้น	4.38	0.48	มาก
2. ผู้สร้างโจทย์สามารถรู้ถึงองค์ประกอบต่าง ๆ ที่ใช้ในการสร้างโจทย์สถานการณ์	4.56	0.50	มากที่สุด
3. ผู้สร้างโจทย์สามารถสร้างแนวทางในการทำโจทย์สถานการณ์ที่สร้างขึ้นให้กับผู้ปฏิบัติได้ดีขึ้น	4.31	0.46	มาก
4. องค์ความรู้ดังกล่าวสามารถทำให้สร้างโจทย์สถานการณ์ได้ง่ายขึ้น	4.63	0.48	มากที่สุด
โดยรวม	**4.48**	**0.49**	**มาก**

จากตารางที่ 1 ผลการประเมินระดับความพึงพอใจต่อการนำองค์ความรู้การสร้างโจทย์สถานการณ์ไปใช้งานจริง พบว่าผลการประเมินความพึงพอใจโดยรวมอยู่ในระดับมาก ($\bar{x}$ = 4.48, S.D. = 0.49) เมื่อพิจารณารายด้านพบว่า ด้านที่มีผลการประเมินความพึงพอใจที่ได้รับคะแนนสูงสุด ได้แก่ องค์ความรู้ดังกล่าวสามารถทำให้สร้างโจทย์สถานการณ์ได้ง่ายขึ้น ($\bar{x}$ = 4.63, S.D. = 0.48) ซึ่งอยู่ในระดับมากที่สุด โดยผลดังกล่าวชี้ให้เห็นว่าการใช้ประโยชน์ของการสร้างผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) และผังงานแสดงขั้นตอนการสร้าง (Flow of Creations) มีส่วนช่วยในการสร้างโจทย์สถานการณ์ได้ง่ายขึ้น

ตารางที่ 2 ผลการประเมินระดับความพึงพอใจต่อความสามารถในการปรับแต่งโจทย์สถานการณ์

รายการ	$\bar{x}$	S.D.	ระดับความคิดเห็น
1. โจทย์สถานการณ์ที่ถูกสร้างโดยใช้องค์ความรู้ดังกล่าวสามารถปรับแต่งได้ตามความเหมาะสม	4.44	0.50	มาก
2. ผู้สร้างโจทย์สามารถทำการประยุกต์และพัฒนารูปแบบโจทย์สถานการณ์ได้มากขึ้น	4.19	0.53	มาก
3. ผู้สร้างโจทย์สามารถเข้าถึงและปรับแต่งโจทย์สถานการณ์ได้ตรงตามความต้องการ	4.25	0.56	มาก
โดยรวม	**4.29**	**0.53**	**มาก**

จากตารางที่ 2 ผลการประเมินระดับความพึงพอใจต่อความสามารถในการปรับแต่งโจทย์สถานการณ์ พบว่าผลการประเมินความพึงพอใจโดยรวมอยู่ในระดับมาก ($\bar{x}$ = 4.29, S.D. = 0.53) เมื่อพิจารณารายด้านพบว่าด้านที่มีผลการประเมินความพึงพอใจที่ได้รับคะแนนสูงสุด ได้แก่ โจทย์สถานการณ์ที่ถูกสร้างโดยใช้องค์ความรู้ดังกล่าวสามารถปรับแต่งได้ตามความเหมาะสม ($\bar{x}$ = 4.44, S.D. = 0.50) ซึ่งอยู่ในระดับมาก โดยผลดังกล่าวชี้ให้เห็นว่าความเข้าใจในการใช้งานผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) และผังงานแสดงขั้นตอนการสร้าง (Flow of Creations) สามารถทำให้ผู้สร้างโจทย์สถาณการณ์ได้เรียนรู้และสามารถปรับแต่งโจทย์สถานการณ์ให้มีความเหมาะสมได้ด้วยตนเอง ซึ่งถือเป็นการส่งเสริมการเรียนรู้ทักษะทางไซเบอร์ในการสร้างโจทย์สถานการณ์และลดช่องว่างความต้องการทักษะทางไซเบอร์จากผู้เชี่ยวชาญได้

นอกจากการประเมินผลความพึงพอใจจากผู้ใช้งานแล้ว ผู้วิจัยยังได้ทำการสัมภาษณ์ผู้เชี่ยวชาญในประเด็นข้อคิดเห็นเพิ่มเติมต่อองค์ความรู้ในการสร้างโจทย์สถานการณ์สำหรับแบบจำลองทางไซเบอร์โดยสามารถสรุปเป็นประเด็นต่าง ๆ ได้ดังนี้

1) ความง่ายของการใช้งาน

1.1) *"เข้าใจง่ายและมีลำดับขั้นตอนชัดเจน บ่งบอกวัตถุประสงค์ได้ชัดเจนในการวัดผล สังเกตได้จากการวาดโครงสร้างการหาคำตอบ ทำให้เห็นถึงลำดับการแก้ปัญหาของโจทย์นั้น ๆ ได้"*

1.2) *"ผู้สร้างโจทย์ใส่ใจและเก็บข้อมูลของผู้ใช้อย่างละเอียด จึงสามารถสร้างโจทย์สถานการณ์ได้สมจริง และสามารถทำให้ผู้ที่มีความรู้ด้านไซเบอร์ เข้าใจได้ง่ายและรวดเร็ว"*

2) การลดช่องว่างขององค์ความรู้

2.1) *"สามารถคิดได้ตามขั้นตอน แต่เมื่อโจทย์มีความซับซ้อนมากขึ้น กรอบความคิดเดิมอาจจะต้องมีการพัฒนาในขั้นต่อไป"*

2.2) *"เมื่อมีขั้นตอนชัดเจน สามารถนำไปต่อยอดหรือพัฒนาได้อย่างต่อเนื่อง ไม่ต้องย้อนกระบวนการหรือเริ่มต้นใหม่ทั้งหมด เพราะถือว่าเป็น KM ที่สามารถใช้ทันที"*

3) ความใหม่ของงานวิจัยและการพัฒนาต่อยอด

3.1) *"ผลงานชิ้นนี้คือผลงานชิ้นแรก ๆ เกี่ยวกับการพัฒนาโจทย์สถานการณ์ด้านการจำลองยุทธ์ทางไซเบอร์ซึ่งเป็นก้าวที่สำคัญสำหรับการพัฒนาบุคลากรด้านไซเบอร์"*

3.2) *"การส่งต่อองค์ความรู้นี้เพื่อพัฒนานำไปสู่การใช้งานจริงเป็นสิ่งที่น่าสนใจ เมื่อจบการวิจัยครั้งนี้ ซึ่งศูนย์ไซเบอร์กองทัพอากาศ จะนำความรู้จากผลงานชิ้นนี้นำไปสู่การสร้างแบบจำลองยุทธ์ (Cyber Range) ระดับสูงถัดไป"*

3.3) *"หากมีการเพิ่มสถานการณ์จำลองยุทธ และมีการกล่าวถึงสถานการณ์จริงของภัยคุกคามทางไซเบอร์จะทำให้สามารถนำไปใช้ในการฝึกทางทหารได้ง่ายขึ้น"*

จากผลการสัมภาษณ์ข้อคิดเห็นเพิ่มเติมเกี่ยวกับ ผลการวิจัยเรื่องการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ของกองทัพอากาศจะเห็นว่า ได้รับผลการตอบรับเชิงบวกรวมถึงแนวทางการพัฒนาต่อยอดงานวิจัยเพื่อนำไปใช้งานจริงให้มีประสิทธิภาพมากยิ่งขึ้นต่อไปในหน่วยงานของกองทัพอากาศ นอกจากนี้ผลการสัมภาษณ์จากผู้เชี่ยวชาญยังให้หาแนวทางในการพัฒนางานวิจัย เช่น งานวิจัยดังกล่าวสามารถพัฒนาต่อยอดเพื่อนำไปใช้ในการพัฒนางานวิจัยที่เกี่ยวข้องกับการพัฒนาสนามจำลองยุทธ์ทางไซเบอร์เพื่อฝึกฝนทางการทหาร ซึ่งถือว่าเป็นงานวิจัยในอนาคตที่น่าสนใจและจะเป็นประโยชน์ต่อการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของชาติ การแปลงงานวิจัยไปสู่การจัดการองค์ความรู้เพื่อการเผยแพร่ต่อไปซึ่งจะเป็นประโยชน์ต่อการส่งเสริมกระบวนการถ่ายทอดความรู้เพื่อสร้างกระบวนการฝึกศึกษาด้านไซเบอร์ที่สามารถพึ่งพาตนเองได้ต่อไป

5. การนำผลการวิจัยไปใช้ประโยชน์

ผู้วิจัยได้ดำเนินการขยายผลการวิจัย เพื่อนำองค์ความรู้ในการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ไปใช้งานต่อในกองทัพอากาศ โดยในปี พ.ศ. 2564 ผู้วิจัยได้นำองค์ความรู้ที่ได้ไปจัดรูปแบบเพื่อให้สามารถส่งต่อและถ่ายทอดต่อบุคลากรในวงกว้างของกองทัพอากาศ ผ่านการจัดทำผลงานการจัดการองค์ความรู้

(Knowledge Management) ในหัวข้อเรื่อง การพัฒนาแพลตฟอร์มสถานการณ์การจำลองยุทธ์ทางไซเบอร์ เพื่อส่งเสริมการพึ่งพอตนเองและพัฒนาที่ยั่งยืนในมิติไซเบอร์ของกองทัพอากาศ ซึ่งได้รับรางวัลระดับชนะเลิศ Excellence Innovation Award ซึ่งถือเป็นรางวัลระดับสูงสุดอันดับที่ 1 จากผลงานการจัดการองค์ความรู้จากหน่วยงานภายในกองทัพอากาศกว่า 52 ผลงานตามหนังสือที่ กห 0604.4/7651 เรื่อง รายงานผลการขับเคลื่อน ทอ.ให้เป็นองค์กรแห่งการเรียนรู้ และได้ดำเนินการเผยแพร่ไปสู่ทุกหน่วยงานของกองทัพอากาศ นอกจากนี้ ชมรมไซเบอร์ โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช ได้ใช้องค์ความรู้ดังกล่าวในการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ด้วยตนเอง และใช้ในการฝึกอบรมนักเรียนนายเรืออากาศจนสามารถคว้ารางวัลในระดับกองทัพและระดับชาติได้อย่างต่อเนื่องจนถึงปัจจุบัน จึงถือเป็นหลักฐานเชิงประจักษ์ในการนำผลงานวิจัยดังกล่าวไปใช้ประโยชน์

อภิปรายผลการวิจัย

1. ผลการวิจัยเรื่องการพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ของกองทัพอากาศ ผู้วิจัยได้พัฒนาองค์ความรู้ผ่านการศึกษาข้อมูลโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ที่ใช้ในการแข่งขันทักษะทางไซเบอร์ของกองทัพอากาศย้อนหลังเป็นเวลา 3 ปี เพื่อหาประเภทโจทย์สถานการณ์ที่มีความเหมาะสมกับกองทัพอากาศ และพบว่าโจทย์สถานการณ์ที่มีความเหมาะสมประกอบไปด้วย 1) โจทย์ Red Team ซึ่งเป็นโจทย์ที่มุ่งเน้นการป้องปรามหรือโจทย์ที่เกี่ยวข้องกับผู้ทำการโจมตีและ 2) โจทย์ประเภท Blue Team ซึ่งเป็นโจทย์ที่มุ่งเน้นการป้องกันซึ่งเกี่ยวข้องกับผู้ดูแลระบบในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ซึ่งผลการศึกษาดังกล่าว มีความสอดคล้องกับผลการวิจัยของ Gurnani et al. [12] ที่ได้จัดประเภทของการฝึกทักษะจากการฝึกปฏิบัติจริงผ่านการทำโจทย์สถานกาณ์เป็นหนึ่งในการฝึกทักษะทางไซเบอร์ที่มีความสำคัญ รวมถึงสอดคล้องกับผลการวิจัยของ Yamin et al. [13] ที่จำแนกรูปแบบการฝึกปฏิบัติทางไซเบอร์ออกเป็น 2 รูปแบบ ได้แก่ 1) การฝึกปฏิบัติการโจมตีทางไซเบอร์ (Cyber-attack Exercise) ที่มุ่งเน้นการฝึกหัดและประเมินสมรรถนะการเจาะ ทำลายรวมถึงสร้างความเสียหายตามภารกิจหรือวัตถุประสงค์ที่ได้รับมอบหมาย 2) การฝึกปฏิบัติการป้องกันทางไซเบอร์ (Cyber-defense Exercise) ที่มุ่งเน้นการฝึกหัดและประเมินสมรรถนะการป้องกันต่อการโจมตีด้านไซเบอร์ รวมถึงทักษะการเข้ารหัส/ถอดรหัส ซึ่งบรรลุวัตถุประสงค์ของงานวิจัยข้อที่ 1 ในการศึกษารูปแบบโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ที่มีความเหมาะสมและสอดคล้องกับความต้องการของกองทัพอากาศ

2. ผู้วิจัยได้เสนอแนวทางการใช้กระบวนการสร้างผังงาน (Flowchart) ในการลดช่องว่างทางทักษะ (Skill Gap) ในแง่ความต้องการผู้เชี่ยวชาญด้านไซเบอร์ในการสร้างโจทย์สถานการณ์ โดยผู้วิจัยได้เสนอแนวคิดในการสร้างขั้นตอนการสร้างโจทย์สถานการณ์จำนวน 2 ขั้นตอนได้แก่ ขั้นตอนที่ 1 ได้แก่ การสร้างผังงานแสดงขั้นตอนการปฏิบัติ (Flow of Actions) ซึ่งเป็นการถอดรูปแบบการปฏิบัติการทางไซเบอร์ทีละขั้นตอน เพื่อสร้างความเข้าใจให้แก่ผู้สร้างโจทย์เกี่ยวกับสภาพแวดล้อมของระบบ ช่องโหว่ของการโจมตี ผ่านการทดลองการทำโจทย์สถานการณ์เพื่อเป็นข้อมูลพื้นฐานในขั้นตอนที่ 2 ได้แก่ การสร้างผังงานแสดงขั้นตอนการสร้างโจทย์ (Flow of Creations) ซึ่งอาศัยความรู้ความเข้าใจที่ได้จากขั้นตอนที่ 1 ในการสร้างเครื่องเสมือนที่บรรจุซอฟต์แวร์ที่เป็นโจทย์สถานการณ์ผ่านขั้นตอนการสร้างทีละขั้นตอน ตั้งแต่การเลือกระบบปฏิบัติการคอมพิวเตอร์ การติดตั้งช่องโหว่ การเปิดช่อง

บริการหรือหมายเลขพอร์ทเพื่อการเข้าถึง รวมถึงการตั้งค่าอื่น ๆ เพื่อให้ตอบสนองต่อวัตถุประสงค์ของโจทย์สถานการณ์ โดยผลการวิจัยพบว่าผู้วิจัยประสบความสำเร็จในการใช้ประโยชน์ของผังงานในการสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ได้ ซึ่งบรรลุวัตถุประสงค์ของงานวิจัยข้อที่ 2 ในการแสวงหาแนวทางการสร้างโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ ที่สามารถปรับแต่งได้ตามวัตถุประสงค์เพื่อการฝึกปฏิบัติทางไซเบอร์ได้ตามความเหมาะสมและความต้องการของผู้ใช้

3. ผลการประเมินระดับความพึงพอใจต่อการนำองค์ความรู้การสร้างโจทย์สถานการณ์ไปใช้งานจริงและผลการประเมินระดับความพึงพอใจต่อความสามารถในการปรับแต่งโจทย์สถานการณ์อยู่ในระดับมาก โดยผลการวิจัยดังกล่าวสะท้อนศักยภาพในการใช้องค์ความรู้ผ่านการกระบวนการใช้ประโยชน์จากผังงานในมุมมองและประสบการณ์การใช้งานจริง ซึ่งสอดคล้องกับงานวิจัยของ Chapin [5] and Zhang et al. [18] ที่ได้ชี้ให้เห็นถึงประโยชน์ของการใช้ผังงาน เพื่อช่วยลดช่องว่างของทักษะการเรียนรู้รวมถึงส่งเสริมความเข้าใจในกระบวนการทางคอมพิวเตอร์ที่มีความซับซ้อนได้ นอกจากนี้ ผลการสัมภาษณ์จากผู้เชี่ยวชาญ พบว่างานวิจัยดังกล่าวสามารถพัฒนาต่อยอดเพื่อนำไปใช้ในการพัฒนางานวิจัยที่เกี่ยวข้องกับการพัฒนาสนามจำลองยุทธ์ทางไซเบอร์เพื่อฝึกฝนทางการทหาร การแปลงงานวิจัยไปสู่การจัดการองค์ความรู้เพื่อการเผยแพร่ให้ผู้สนใจนำไปใช้งานต่อไป ซึ่งบรรลุวัตถุประสงค์ของงานวิจัยข้อที่ 3 ในการวัดความสำเร็จขององค์ความรู้ในการสร้างโจทย์สถานการณ์ผ่านการประเมินความพึงพอใจในการนำองค์ความรู้สำหรับการสร้างโจทย์สถานการณ์ไปใช้งานจริงและได้รับแนวทางในการพัฒนางานวิจัยดังกล่าวให้ดีขึ้นในอนาคต

ข้อเสนอแนะ

งานวิจัยนี้เป็นการพัฒนาองค์ความรู้เกี่ยวกับการพัฒนาโจทย์สถานการณ์สำหรับแบบการจำลองยุทธ์ทางไซเบอร์งานแรกของกองทัพอากาศ ซึ่งเป็นก้าวที่สำคัญสำหรับการพัฒนาบุคลากรด้านไซเบอร์ ผลงานวิจัยชี้ให้เห็นว่าความเข้าใจในขั้นตอนการปฏิบัติการทางไซเบอร์ที่มีความชัดเจน จะส่งผลโดยตรงให้ผู้พัฒนาโจทย์สถานการณ์สามารถนำไปต่อยอดหรือพัฒนาได้อย่างต่อเนื่อง ดังนั้น การให้ความสำคัญกับการเขียนผังงานแสดงขั้นตอนการปฏิบัติการทางไซเบอร์ รวมถึงการมีองค์ความรู้พื้นฐานด้านคอมพิวเตอร์ที่เพียงพอ จึงถือเป็นหัวใจสำคัญและเป็นจุดเริ่มต้นของการสร้างทักษะในการสร้างโจทย์สถานการณ์ทางไซเบอร์ มากไปกว่านั้น การเพิ่มประสิทธิภาพของการฝึกทักษะทางไซเบอร์ ด้วยการออกแบบโจทย์สถานการณ์สำหรับแบบจำลองยุทธ์ทางไซเบอร์ ให้มีการกล่าวถึงสถานการณ์จริง (Scenario-based Cyber Simulation) ของภัยคุกคามทางไซเบอร์จะทำให้สามารถนำไปใช้ในการฝึกทางการทหารได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

นอกจากนี้ การส่งต่อองค์ความรู้ดังกล่าวไปยังองค์กรหรือหน่วยงานอื่น ๆ ทั้งภาครัฐ ภาคเอกชนที่ต้องการพัฒนาบุคลากรด้านไซเบอร์ แต่ยังขาดผู้เชี่ยวชาญด้านการพัฒนาโจทย์สถานการณ์รวมถึงมีข้อจำกัดด้านงบประมาณในการจ้างพัฒนาจากบริษัทเอกชน เป็นสิ่งที่ควรดำเนินการต่อไป มากไปกว่านั้น งานวิจัยที่เกี่ยวข้องกับการพัฒนารูปแบบโจทย์สถานการณ์ทางไซเบอร์ที่มีความน่าสนใจในอนาคตที่ผู้วิจัยท่านอื่นอาจนำไปพัฒนาต่อยอดประกอบด้วย การศึกษาผลการพัฒนาทักษะของผู้เข้ารับการอบรมทางไซเบอร์ผ่านกระบวนการใช้ผังงานในการสร้างโจทย์สถานการณ์ การพัฒนารูปแบบการสร้างโจทย์สถานการณ์ให้มีความสะดวก รวดเร็ว และทำได้โดยอัตโนมัติ

มากยิ่งขึ้น รวมถึงการออกแบบแนวทางการสร้างโจทย์สถานการณ์เพื่อรองกับการเปลี่ยนแปลงจากภัยคุกคามในมิติไซเบอร์ที่มีแนวโน้มจะเกิดขึ้นใหม่และมีความท้ามายเพิ่มขึ้นอย่างต่อเนื่อง

เอกสารอ้างอิง

[1] กองทัพอากาศ. (2563). *ยุทธศาสตร์กองทัพอากาศ 20 ปี (พ.ศ.2561 - 2580) (ฉบับปรับปรุง พ.ศ. 2563)*. จาก www.rtaf.mi.th/th/Documents/Publication/RTAF%20Strategy_Final_04122563.pdf

[2] ปุณณวิช ธรรมาธร, ธนบัตร ปลัดศรี และ พงศ์วิจักขณ์ กุดั่นนิล. (2556). *การพัฒนาสนามทดสอบการโจมตีทางไซเบอร์ สำหรับนักเรียนนายเรืออากาศ บนระบบการประมวลผลแบบคลาวด์* (รายงานการวิจัย). กรุงเทพฯ: โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช.

[3] Alotaibi, F., Furnell, S., Stengel, I. & Mavroudis, D. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness. *International Journal for Information Security Research,* 6(2). From https://doi.org/10.20533/ijisr.2042.4639.2016.0076

[4] Chapin, N. (2003). 'Flowchart', in *Encyclopedia of Computer Science*. GBR: John Wiley and Sons Ltd.

[5] Chiueh, S. N. T. C., & Brook, S. (2005). A survey on virtualization technologies. *Rpe Report, 142*.

[6] Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L. A., Pantziou, G. & Ferrag, M. A. (2021). Cyber Ranges and TestBeds for Education, Training, and Research. *Applied Sciences,* 11(4), 1809. From https://doi.org/10.3390/app11041809

[7] Davis, J., & Magrath, S. (2013). *A Survey of Cyber Ranges and Testbeds Executive.* Australia: Cyber Electronic Warfare Division.

[8] Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity, attack and defense strategies : infrastructure security with Red Team and Blue Team tactics.* Birmingham, UK : Packt Publishing.

[9] Endicott-Popovsky, B. E. & Popovsky, V. M. (2014). Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals. *ACM Inroads*, 5(1), 57-68.

[10] Ford V., Siraj A., Haynes A., & Brown E. (2017). Capture the Flag Unplugged: An Offline Cyber Competition. in *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, ser. SIGCSE '17*. New York, NY, USA: ACM, pp. 225–230. From http://doi.acm.org/10.1145/3017680.3017783

[11] Gurnani, R., Pandey, K. M., & Rai, S. K. (2014). A scalable model for implementing Cyber Security Exercises. In *International Conference on Computing for Sustainable Global Development.* From https://doi.org/10.1109/indiacom.2014.6828048

[12] Likert, R. (2017). The method of constructing an attitude scale. In *Scaling*. (pp. 233-242). Routledge.

[13] Messier, R. (2019). *CEH v10 Certified Ethical Hacker Study Guide.* Indianapolis, Indiana: Sybex, a Wiley brand.

[14] Richard Scroggins. (2014). SDLC and Development Methodologies. *Global Journal of Computer Science and Technology, 14*(C7), 21–22. From https://computerresearch.org/index.php/computer/article/view/148

[15] Sinha, S. (2018). Beginning Ethical Hacking with Kali Linux. *Apress EBooks*. From https://doi.org/10.1007/978-1-4842-3891-2

[16] Yamin, M., & Katt, B. (2019). Cyber Security Skill Set Analysis for Common Curricula Development. *Availability, Reliability and Security*. From https://doi.org/10.1145/3339252.3340527

[17] Yamin, M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security, 88,* 101636. From https://doi.org/10.1016/j.cose.2019.101636

[18] Zhang, J., Meng, B., Zou, L., Zhu, Y., & Hwang, G. (2021). Progressive flowchart development scaffolding to improve university students' computational thinking and programming self-efficacy. *Interactive Learning Environments, 1–18*. From https://doi.org/10.1080/10494820.2021.1943687