

แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร  
รองรับยุทธศาสตร์ชาติด้านความมั่นคง

เอกสารวิจัยส่วนบุคคล



โดย

พันเอกหญิง นริศรา พลอยประไพ  
รองผู้อำนวยการกองวิทยาการ ศูนย์ไซเบอร์ทหาร

วิทยาลัยการทัพบก

กันยายน 2564



เอกสารวิจัยเรื่อง แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร  
รองรับยุทธศาสตร์ชาติด้านความมั่นคง

โดย พันเอกหญิง นริศรา พลอยประไพ

อาจารย์ที่ปรึกษา พันเอกหญิง ธนิตา วงษ์จินดา

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตาม  
หลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2564 และเห็นชอบให้เป็นเอกสารวิจัย  
ส่วนบุคคลที่อยู่ในเกณฑ์ระดับ

พลตรี



( มหศักดิ์ เทพหัสติน ณ อยู่ธยา )

ผู้บัญชาการวิทยาลัยการทัพบก

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก



( ตูลธร นวพิตร )

ประธานกรรมการ

พลตรี ดร.



(ชาติชาย ชัยเกษม)

ผู้ทรงคุณวุฒิที่ปรึกษา

พันเอก



( สติชัยพันธ์ ประกอบผล )

กรรมการ

พันเอกหญิง



( ธนิตา วงษ์จินดา )

กรรมการ

## บทคัดย่อ

ผู้วิจัย	พินเอกหญิง นริศรา พลอยประไพ
เรื่อง	แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง
วันที่	กันยายน 2564 จำนวนคำ: 7,581 จำนวนหน้า: 22
คำสำคัญ	ขีดความสามารถ, บุคลากร, ไซเบอร์, หน่วยทหาร
ชั้นความลับ	ไม่มีชั้นความลับ

สงครามไซเบอร์เป็นภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของชาติในวงกว้าง ปัจจุบันบุคลากรของหน่วยไซเบอร์ทางทหารยังขาดทักษะและความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงจำเป็นต้องเร่งพัฒนาขีดความสามารถของบุคลากรของหน่วยดังกล่าว การวิจัยครั้งนี้มีวัตถุประสงค์เพื่ออธิบายสภาพปัญหาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร วิเคราะห์ปัจจัยที่สนับสนุนหรือขัดขวางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร และเสนอแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง ผลการวิจัยพบว่า หน่วยไซเบอร์ทางทหารของไทยขาดแคลนบุคลากรเช่นเดียวกับที่หลายประเทศทั่วโลกกำลังประสบอยู่ โดยสภาวะแวดล้อมด้านการเมือง การทหาร เศรษฐกิจ สังคมจิตวิทยา และเทคโนโลยีสารสนเทศ มีส่วนสนับสนุนในการพัฒนาขีดความสามารถบุคลากร สำหรับแนวทางที่เหมาะสมในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารคือ การปรับโครงสร้างหน่วยไซเบอร์ทางทหารโดยจัดตั้งโรงเรียนไซเบอร์ทางทหารขึ้นเพื่อเป็นศูนย์กลางในการถ่ายทอดความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นรูปธรรม ซึ่งจะทำให้บุคลากรของหน่วยไซเบอร์ทางทหารมีขีดความสามารถเพิ่มขึ้น สามารถปฏิบัติภารกิจรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้อย่างมีประสิทธิภาพต่อไป

## ABSTRACT

**AUTHOR:** Colonel Narisara Ployprapai

**TITLE:** Guidelines for the Development of Personnel Capabilities in Military Cyber Units to Support the National Security Strategy.

**DATE:** September 2021 **WORD COUNT:** 7,581 **PAGES:** 22

**KEYTERMS:** Capability, Personnel, Cyber, Military Unit

**CLASSIFICATION:** Unclassified

Cyber Warfare is a threat that effects National Security. Military Cyber Units also lack the skills and expertise to maintain Cyber Security. Therefore, the development of personnel capacity is an urgent necessity to be implemented. This research aims to explain Personnel Capabilities problems of Military Cyber Units, to analyze the factors that support or hinder capacity development of personnel capacity and to propose guidelines for personnel capacity development of Military Cyber Units to support National Security Strategy. The results of the research show that Military Cyber Units are short of personnel, a worldwide problem. Political Military Economics Social- Psychology and information factors contribute to the development of personnel capabilities. For the best approach to the development of personnel capabilities, Military Cyber Units have been restructured and established a Military Cyber School to be a hub for transferring knowledge of Cyber Security in a concrete way. In order to effectively respond to missions under the National Security Strategy.

## กิตติกรรมประกาศ

เอกสารวิจัยส่วนบุคคล เรื่อง “แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร รองรับยุทธศาสตร์ชาติด้านความมั่นคง” ฉบับนี้ สำเร็จลุล่วงได้ด้วยความอนุเคราะห์จากพันเอกหญิง ธนิตา วงษ์จินดา อาจารย์ที่ปรึกษา ที่กรุณาให้คำปรึกษา รวมทั้งปรับปรุงแก้ไขข้อบกพร่องต่างๆ ด้วยความเอาใจใส่อย่างยิ่ง และ พลตรี ชาติชาย ชัยเกษม ผู้อำนวยการศูนย์ไซเบอร์ทหาร ผู้ทรงคุณวุฒิที่ปรึกษาและผู้บังคับบัญชาที่กรุณาเปิดโอกาสให้ได้เข้ารับการศึกษานในวิทยาลัยการทัพบกแห่งนี้ และได้ให้แนวคิดในการศึกษาตลอดจนมุมมองเกี่ยวกับปัญหาและวิธีการพัฒนาบุคลากรด้านไซเบอร์ ผู้วิจัยขอขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบคุณ พลตรี มหศักดิ์ เทพหัสดิน ณ อยุธยา ผู้บัญชาการวิทยาลัยการทัพบก ที่กรุณาอนุมัติให้ผู้วิจัยรวบรวมข้อมูลอันเป็นประโยชน์จากผู้เกี่ยวข้อง พันเอก ตฤธร นวพิตร ประธานกรรมการควบคุมเอกสารวิจัยส่วนบุคคล พันเอก สติธย์พันธ์ ประกอบผล กรรมการ ที่กรุณาให้ข้อเสนอแนะอันเป็นประโยชน์อย่างยิ่งต่องานวิจัยฉบับนี้

ขอขอบคุณ นาวาอากาศเอก โสภณ ทับแหว่ และข้าราชการหน่วยไซเบอร์ทางทหารที่ได้กรุณาเสนอความคิดเห็นอันเป็นประโยชน์เพื่อนำมาวิเคราะห์และสรุปผลเพื่อให้ผู้ที่สนใจได้นำแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารไปประยุกต์ใช้เพื่อให้มีบุคลากรที่มีขีดความสามารถเป็นกำลังสำคัญของกองทัพต่อไป

สุดท้ายนี้ขอขอบคุณ ครอบครัวอันเป็นที่รักและเพื่อนนักศึกษาวิทยาลัยการทัพบก หลักสูตรหลักประจำ ชุดที่ 66 ที่ให้ความช่วยเหลือและเป็นกำลังใจให้กับผู้วิจัยในทุกขั้นตอนของการดำเนินการวิจัย ผู้วิจัยหวังเป็นอย่างยิ่งว่าวิจัยฉบับนี้ จะเป็นแนวทางและเป็นประโยชน์ต่อการพัฒนาบุคลากรของหน่วยไซเบอร์ทางทหารสืบไป

## สารบัญ

	หน้า
บทที่ 1 บทนำ.....	1
ที่มาและความสำคัญของปัญหา.....	1
วัตถุประสงค์การวิจัย.....	3
กรอบแนวคิดการวิจัย.....	3
วิธีการศึกษา.....	4
ประโยชน์ที่ได้รับ.....	5
บทที่ 2 บทวิเคราะห์.....	6
ปัญหาและสาเหตุที่เกี่ยวข้อง.....	6
สภาวะแวดล้อมทางยุทธศาสตร์.....	8
ทางเลือกทางยุทธศาสตร์ในการพัฒนาขีดความสามารถของบุคลากร.....	11
แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร.....	14
บทที่ 3 บทอภิปรายผล.....	17
การเปรียบเทียบกับวิธีปฏิบัติที่ดี.....	17
การเปรียบเทียบกับงานวิจัยที่เกี่ยวข้อง.....	17
บทที่ 4 บทสรุป.....	20
สรุปผลการวิจัย.....	20
ข้อเสนอแนะ.....	21
เอกสารอ้างอิง.....	23
ประวัติผู้วิจัย.....	25

## บทที่ 1

### บทนำ

#### ที่มาและความสำคัญของปัญหา

เทคโนโลยีสารสนเทศและการสื่อสารที่มีการเชื่อมโยงสิ่งต่างๆ เข้าสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถควบคุมการใช้งานอุปกรณ์ต่างๆ ในชีวิตประจำวันผ่านเครือข่ายอินเทอร์เน็ต เทคโนโลยีนี้มีประโยชน์อย่างมหาศาล ขณะเดียวกันก็นำมาซึ่งความเสี่ยงจากภัยคุกคามรูปแบบใหม่ เช่น ภัยคุกคามทางไซเบอร์ที่มีการโจมตีที่หลากหลายและซับซ้อนตามโครงสร้างพื้นฐานที่เปลี่ยนแปลงไป โดยมุ่งประสงค์ร้ายต่อหน่วยงานความมั่นคงภาครัฐและภาคเอกชนโดยเฉพาะบริษัทขนาดใหญ่ จากการก่ออาชญากรรมทางไซเบอร์พัฒนาเป็นการจารกรรมทางไซเบอร์ การก่อวินาศกรรมทางไซเบอร์ ท้ายสุดกลายเป็นการโจมตีในแบบรัฐต่อรัฐ โดยโจมตีโครงสร้างพื้นฐานสำคัญให้หยุดการทำงานหรือทำงานผิดพลาด ก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ตามสถิติที่ศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามระบบเทคโนโลยีสารสนเทศของบริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน) รายงานการจัดลำดับภัยคุกคามทางไซเบอร์ที่สูงที่สุด 5 อันดับแรก ประจำปี 2563 มีดังนี้ 1) การพยายามเข้าถึงระบบจากผู้ไม่หวังดีภายนอก 2) การโจมตีผ่านทางช่องโหว่ต่างๆ 3) การติดตั้งโปรแกรมประสงค์ร้ายโดยผู้ใช้ไม่รู้ตัว 4) การเจาะระบบจากผู้ไม่หวังดี 5) การปลอมแปลงข้อความ ภาพ เสียง วิดีโอ

ภารกิจทางทหารในปัจจุบันต้องเผชิญกับภัยคุกคามทางไซเบอร์ ซึ่งส่งผลกระทบต่อความมั่นคงของชาติในวงกว้าง สงครามไซเบอร์มีการโจมตีกันหลายรูปแบบ ตั้งแต่การโจมตีเว็บไซต์ การเจาะข้อมูลลับและเปลี่ยนแปลงข้อมูล ที่รุนแรงที่สุดเป็นการโจมตีต่อระบบสาธารณสุขุบัติภาคที่สำคัญ การทำลายชีวิตและทรัพย์สินของประชาชนผู้บริสุทธิ์ เช่น การทำให้รถไฟตกราง เครื่องบินตก ทำลายระบบไฟฟ้า หรือระบบธุรกรรมทางการเงิน เป็นเหตุให้ระบบเศรษฐกิจหยุดชะงัก ซึ่งสามารถสร้างความหวาดวิตกแก่ประชาชนเป็นวงกว้างได้อย่างรวดเร็ว (อภิชาติ วรรณารศน์, พ.อ., 2561) กองทัพจึงต้องมีการเตรียมความพร้อมเพื่อรับมือกับสงครามไซเบอร์ที่อาจจะเกิดขึ้นได้ทุกที่และตลอดเวลา กระทรวงกลาโหมได้ขับเคลื่อนการปฏิรูปกองทัพด้านไซเบอร์ ให้สอดรับกับยุทธศาสตร์ชาติด้านความมั่นคง มีการนำนโยบายมาสู่การปฏิบัติ โดยได้จัดทำแผนแม่บทไซเบอร์ เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ. 2560 - 2564 และกำหนดให้ไซเบอร์เป็นมิติหนึ่งของสงคราม



ที่ต้องจัดเตรียมกำลังและใช้กำลัง เช่นเดียวกับมิติของการสงครามอื่นๆ โดยการจัดตั้งหน่วยไซเบอร์ทางทหารขึ้น เพื่อรองรับภารกิจการรักษาความมั่นคงปลอดภัยไซเบอร์โดยตรง ประกอบด้วย 1) ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม 2) ศูนย์ไซเบอร์ทางทหาร กองบัญชาการกองทัพไทย 3) ศูนย์ไซเบอร์กองทัพบก 4) ศูนย์ไซเบอร์กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ และ 5) ศูนย์ไซเบอร์กองทัพอากาศ เพื่อให้กองทัพไทยมีพลังอำนาจทางไซเบอร์ที่เพียงพอต่อการปฏิบัติการในมิติไซเบอร์ ตลอดจนสามารถบูรณาการและให้การสนับสนุนความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในภาพรวมได้อย่างมีประสิทธิภาพ

ในส่วนของกองบัญชาการกองทัพไทย ผู้บัญชาการทหารสูงสุด ได้กรุณานุมัติแผนปฏิบัติราชการกองบัญชาการกองทัพไทย พ.ศ. 2563 - 2565 เพื่อเป็นกรอบแนวทางในการปฏิบัติราชการและจัดสรรทรัพยากร โดยมีการบริหารจัดการด้วยเทคโนโลยีที่ทันสมัย แม่นยำ ทันเวลา มีระบบที่สนับสนุนการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางเพื่อเพิ่มขีดความสามารถในการปฏิบัติงาน ให้เป็นที่ยอมรับและได้รับความเชื่อมั่นจากเหล่าทัพรวมทั้งส่วนราชการที่เกี่ยวข้อง พร้อมเข้าสู่การเป็น Digital Headquarter ในปี 2565 และเป็น AI Headquarter ในปี 2575 และมีวิสัยทัศน์ที่ก้าวไปสู่ SMART Headquarter ในปี 2580 สอดคล้องกับเป้าหมายยุทธศาสตร์ชาติ (กองบัญชาการกองทัพไทย, 2563) ในส่วนที่เกี่ยวข้องกับงานด้านไซเบอร์ได้กำหนดให้มีการพัฒนาขีดความสามารถด้านไซเบอร์ตั้งนั้นการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร จึงเป็นความจำเป็นเร่งด่วนที่ต้องดำเนินการ เพื่อให้การพัฒนาขีดความสามารถด้านไซเบอร์เป็นไปตามแผนที่ได้วางไว้ เพราะบุคลากรเหล่านี้มีความสำคัญต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเนื่องจากที่ผ่านมา ยังไม่มีงานวิจัยหรือองค์ความรู้ใด ที่ศึกษาในเรื่องของขีดความสามารถบุคลากรในด้านนี้มาก่อน ผู้วิจัยจึงมีความสนใจที่จะศึกษาว่า 1) ขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารในปัจจุบัน มีความเหมาะสมเพียงพอต่อการตอบสนองต่อยุทธศาสตร์ชาติด้านความมั่นคงหรือไม่ 2) มีสถานะแวดล้อมใดบ้างที่สนับสนุนหรือขัดขวางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารเพื่อรองรับยุทธศาสตร์ชาติด้านความมั่นคง และ 3) ควรมีแนวทางอย่างไรในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารเพื่อรองรับยุทธศาสตร์ชาติ ด้านความมั่นคง ทั้งนี้ เพื่อให้ได้ข้อมูลที่เป็นประโยชน์สำหรับหน่วยไซเบอร์ทางทหารในการพัฒนาบุคลากรให้มีขีดความสามารถที่เหมาะสมเพียงพอ สามารถตอบสนองต่อการปฏิบัติการกิจภายใต้ยุทธศาสตร์ชาติ ด้านความมั่นคงได้อย่างมีประสิทธิภาพต่อไป

### วัตถุประสงค์การวิจัย

1. เพื่ออธิบายสภาพปัญหาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารในการตอบสนองต่อยุทธศาสตร์ชาติด้านความมั่นคง
2. เพื่อวิเคราะห์สภาวะแวดล้อมที่สนับสนุนหรือขัดขวางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง
3. เพื่อเสนอแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง

### กรอบแนวคิดการวิจัย



ภาพที่ 1 แสดงแผนผังความสัมพันธ์ของกรอบแนวคิดการวิจัย

## วิธีการศึกษา

1. รูปแบบการวิจัย ใช้รูปแบบการวิจัยเชิงยุทธศาสตร์ตามที่วิทยาลัยการทัพบกกำหนด โดยใช้วิธีการศึกษาเชิงเอกสาร

### 2. ขอบเขตในการวิจัย

2.1 ขอบเขตด้านเนื้อหา ศึกษา วิเคราะห์สภาพปัญหาและสาเหตุขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร วิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ที่ส่งผลต่อการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร และเสนอแนะแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง

2.2 ขอบเขตด้านระยะเวลา เก็บรวบรวมข้อมูล ตั้งแต่ห้วงเดือน มกราคม - กุมภาพันธ์ 2564

### 3. การเก็บรวบรวมข้อมูล ประกอบด้วย

3.1 เอกสารที่เกี่ยวข้อง ได้แก่ ยุทธศาสตร์ชาติ พ.ศ. 2561 - 2580 แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง พ.ศ. 2561 - 2580 แผนปฏิบัติการกองบัญชาการกองทัพไทย พ.ศ. 2563 - 2565

3.2 เอกสารทางวิชาการ ได้แก่ เอกสารวิจัยส่วนบุคคลของนักศึกษา วิทยาลัยป้องกันราชอาณาจักร และวิทยาลัยการทัพบก วารสารวิชาการของสถาบันการศึกษา เช่น มหาวิทยาลัยวลัยลักษณ์ มหาวิทยาลัยราชภัฏลำปาง เป็นต้น

3.3 ข้อมูลจากเครือข่ายอินเทอร์เน็ตเกี่ยวกับแนวคิดและทฤษฎีด้านการพัฒนาบุคลากร รวมถึงสถิติต่างๆ

### 4. การวิเคราะห์ข้อมูล

ใช้กรอบการคิดเชิงยุทธศาสตร์ (Strategic thinking framework) ในการวิเคราะห์และสังเคราะห์ข้อมูลเพื่อพัฒนาแนวทางที่เหมาะสมในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง

## 5. ขั้นตอนการดำเนินงาน

รายการ	ปี 2563	ปี 2564				
	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.
1) พัฒนาและเสนอโครงการวิจัย	←→					
2) การเก็บรวบรวมข้อมูล		←→				
3) การวิเคราะห์ข้อมูล				←→		
4) การสรุปผลและอภิปรายผล					←→	←→
5) การจัดทำรูปเล่มวิจัย						←→
6) การนำเสนอผลการวิจัย						←→

ตารางที่ 1 แสดงแผนการดำเนินงานวิจัย

### ประโยชน์ที่ได้รับ

1. ได้ทราบถึงขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารและสภาวะแวดล้อมที่มีผลต่อการพัฒนาขีดความสามารถของบุคลากรดังกล่าว
2. ได้แนวทางการพัฒนาขีดความสามารถของหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคงที่สามารถนำไปประยุกต์ใช้ให้เกิดประโยชน์ต่อหน่วยไซเบอร์ทางทหารของไทยได้จริง
3. ได้องค์ความรู้ใหม่ที่เป็นประโยชน์ต่อการพัฒนาขีดความสามารถของบุคลากรด้านไซเบอร์รองรับยุทธศาสตร์ชาติด้านความมั่นคง สามารถนำไปต่อยอดในการศึกษาวิจัยเพื่อพัฒนาบุคลากรรองรับการขับเคลื่อนยุทธศาสตร์ชาติให้บรรลุผลสำเร็จได้ต่อไป

## บทที่ 2

### บทวิเคราะห์

การพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร นับว่าเป็นความจำเป็นเร่งด่วนที่ต้องดำเนินการ เพราะบุคลากรเหล่านี้มีความสำคัญต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพ ผู้วิจัยได้รวบรวมข้อมูลจากเอกสารที่เกี่ยวข้อง แนวคิดทฤษฎีต่าง ๆ เพื่อนำมาวิเคราะห์ใน 4 ประเด็นหลัก ได้แก่ สภาพปัญหาและสาเหตุที่เกี่ยวข้อง สภาวะแวดล้อมทางยุทธศาสตร์ที่ส่งผลต่อการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร ทางเลือกทางยุทธศาสตร์ในการพัฒนาขีดความสามารถบุคลากรหน่วยไซเบอร์ทางทหาร และแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร

#### ขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร: ปัญหาและสาเหตุที่เกี่ยวข้อง

ขีดความสามารถ (Competency) หมายถึง ทักษะความรู้ ความสามารถหรือพฤติกรรมของบุคลากรที่จำเป็นในการปฏิบัติงานใดงานหนึ่ง สิ่งเหล่านี้ช่วยให้องค์กรทราบว่ “คุณสมบัตินี้หรือคุณลักษณะที่ดีในการทำงานในองค์กรนั้นเป็นอย่างไร” (เดชา เดชะวัฒน์ไพศาล, 2543) ซึ่งผู้วิจัยได้นำมาใช้ในการวิเคราะห์ปัญหาและสาเหตุที่เกี่ยวข้องในเรื่องขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารตามหลัก 4 M ได้แก่ บุคลากร (Man) งบประมาณ (Money) วัสดุอุปกรณ์ (Material) และการจัดการ (Management) (เกียรติพงษ์ อุตมธนะธีระ, 2560) เพื่อให้สามารถวิเคราะห์ทรัพยากรในการบริหารรวมไปถึงความสามารถในการจัดการทรัพยากรในการบริหารงานด้านไซเบอร์ครบทุกมิติ ดังนี้

1. บุคลากร (Man) จากการกำหนดนโยบายในการสรรหาบุคลากรเข้ามาปฏิบัติงานในหน่วยงานไซเบอร์ทางทหารเป็นการเร่งด่วนเพื่อให้สามารถปฏิบัติงานที่รับมอบหมายได้ ทำให้พบปัญหาและสาเหตุดังนี้

1.1 การขาดแคลนบุคลากรที่เชี่ยวชาญด้านการรักษาความปลอดภัยไซเบอร์ โดยมีผู้ที่มีความรู้และทักษะเฉพาะด้านจำนวนน้อย เนื่องจากเป็นเทคโนโลยีสมัยใหม่ที่มีการพัฒนารวดเร็ว

1.2 บุคลากรส่วนใหญ่ที่มีอยู่ในปัจจุบันขาดทักษะด้านไซเบอร์ จึงทำงานได้ไม่มีประสิทธิภาพ สาเหตุจากใช้บุคลากรจากหน่วยงานเดิมที่แปรสภาพมาเป็นหน่วยงานด้านไซเบอร์

1.3 บุคลากรที่บรรจุเข้ามาใหม่ในตำแหน่งงานด้านไซเบอร์ ไม่มีทักษะในการปฏิบัติงาน สาเหตุจากบรรจุบุคคลที่มีคุณสมบัติไม่ตรงตามคุณวุฒิกับตำแหน่งที่ต้องการ

1.4 บุคลากรขาดแรงจูงใจในการทำงาน มีสาเหตุมาจากความก้าวหน้าของการรับราชการที่ถูกจำกัดด้วยจำนวนอัตรา รวมถึงไม่มีเงินเพิ่มพิเศษสำหรับผู้ปฏิบัติงานด้านไซเบอร์

1.5 บุคลากรมีภาระงานมากและต้องไปปฏิบัติงานที่ได้รับมอบหมายในสายงานอื่นที่ไม่เกี่ยวข้องกั้งงานตามตำแหน่งอีกด้วย สาเหตุเพราะการขาดแคลนบุคลากร

1.6 ปัญหาสมองไหล บุคลากรลาออกราชการเพื่อไปทำงานกับภาคเอกชนมีสาเหตุจากการได้รับค่าตอบแทนและสวัสดิการที่ต่ำกว่าภาคเอกชน

1.7 บุคลากรเข้ารับการฝึกอบรมได้จำนวนน้อย ไม่เพียงพอต่อความต้องการในการพัฒนาขีดความสามารถของหน่วยงานต่าง ๆ สาเหตุมาจากหลักสูตรที่ทางราชการเปิดฝึกอบรมให้กับบุคลากรของหน่วยไซเบอร์ทางทหารนั้นมีที่นั่งจำกัดเพียง 30 ที่ต่อปี และใช้ระยะเวลาอบรมนานถึง 15 สัปดาห์

1.8 การผลิตบุคลากรด้านไซเบอร์ที่เป็นมืออาชีพต้องใช้ระยะเวลานาน สาเหตุมาจากต้องใช้เวลาสั่งสมทักษะและประสบการณ์

2. งบประมาณ (Money) เนื่องจากเทคโนโลยีด้านไซเบอร์นั้นเปลี่ยนแปลงเร็ว หากจะให้ก้าวหน้า เทคโนโลยีและพัฒนาอย่างต่อเนื่องนั้นต้องได้รับการจัดสรรงบประมาณ เพื่อจัดหาเทคโนโลยีใหม่ๆ ค่าลิขสิทธิ์ที่เกี่ยวข้อง รวมถึงการต้องเร่งพัฒนาขีดความสามารถของบุคลากรให้มีความรู้ความสามารถเพียงพอต่อการปฏิบัติงาน แต่การจัดสรรงบประมาณที่ผ่านมานั้น ไม่ครอบคลุมความต้องการเทคโนโลยีใหม่และการพัฒนาขีดความสามารถของบุคลากรอย่างเป็นทางการและเป็นรูปธรรมและต่อเนื่อง ทำให้บุคลากรเรียนรู้ไม่ทันต่อการเปลี่ยนแปลงของเทคโนโลยี

3. วัสดุอุปกรณ์ (Material) อุปกรณ์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการจัดหาอุปกรณ์ใหม่ทั้งเชิงป้องกันและป้องปราม อีกทั้งเทคโนโลยีด้านนี้จะเปลี่ยนแปลงเร็วจึงเป็นสาเหตุทำให้บุคลากรขาดทักษะและความชำนาญในการปฏิบัติงาน

4. การจัดการ (Management) การรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ดำเนินการตามกรอบที่ระบุไว้ในยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ. 2558 และแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ. 2560 - 2564 รวมทั้งแผนปฏิบัติราชการ

กองบัญชาการกองทัพไทย พ.ศ. 2563 - 2565 การปฏิบัติการในด้านต่าง ๆ ที่ผ่านมาเป็นไปตามแผนที่กำหนดไว้ แต่ยังไม่มามีประสิทธิภาพเท่าที่ควร โดยมีสาเหตุมาจากการขาดแคลนบุคลากรที่มีความรู้ ความเชี่ยวชาญและทักษะด้านการรักษาความปลอดภัยไซเบอร์

**สภาวะแวดล้อมทางยุทธศาสตร์ที่ส่งผลต่อการพัฒนาขีดความสามารถของบุคลากร**

ความสัมพันธ์ระหว่างความมั่นคงแห่งชาติกับยุทธศาสตร์ชาตินั้นเป็นสิ่งที่แยกออกจากกันไม่ได้ยาก โดยเฉพาะอย่างยิ่งในการวางแผนและปฏิบัติการต่าง ๆ เพื่อรักษาผลประโยชน์แห่งชาติ ซึ่งจำเป็นต้องใช้เครื่องมือของชาติทั้งปวง เครื่องมือนี้ก็คือ “พลังอำนาจแห่งชาติ” อันประกอบไปด้วย 5 ด้านได้แก่ การเมือง การทหาร เศรษฐกิจ สังคมจิตวิทยาและเทคโนโลยีสารสนเทศ (วิทยาลัยการทัพบก, ม.ป.ป.) ผู้วิจัยจึงได้วิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ในมิติต่างๆ ตามพลังอำนาจแห่งชาติทั้งที่สนับสนุนและขัดขวางต่อการพัฒนาขีดความสามารถของบุคลากรของหน่วยไซเบอร์ทางทหารในปัจจุบันและแนวโน้มในอนาคต รายละเอียดดังนี้

### 1. สภาวะแวดล้อมทางการเมือง

การเมืองโลกเป็นเวทีที่มีสหรัฐอเมริกาเป็นผู้มีบทบาทหลัก มาตั้งแต่หลังสิ้นสุดสงครามเย็น การก้าวขึ้นสู่การเป็นรัฐมหาอำนาจใหญ่ของจีน กลายเป็นความท้าทายทางยุทธศาสตร์โดยตรงต่อสหรัฐฯ และนำไปสู่การแข่งขันในเชิงอำนาจและอิทธิพลครั้งสำคัญระหว่างสองฝ่าย ซึ่งทำให้เกิดความกังวลว่าโลกเรากำลังก้าวสู่การก่อตัวของสงครามเย็นในศตวรรษที่ 21 ซึ่งสภาวะเช่นนี้ จะมีผลมากต่อการคาดเดาความเป็นไปของโลก ความขัดแย้งระหว่างสหรัฐอเมริกากับจีนมีประเด็นที่สำคัญ ดังนี้

- 1) สงครามการค้าในเวทีการเมืองโลกจะนำไปสู่มาตรการของการตั้ง “กำแพงภาษี” ของสหรัฐอเมริกา ซึ่งส่งผลกระทบต่อสภาวะทางเศรษฐกิจของโลกโดยตรง
- 2) ความขัดแย้งในลักษณะภูมิรัฐศาสตร์ โครงการความริเริ่มแถบและเส้นทางของจีนซึ่งมุ่งสร้างเส้นทางเชื่อมต่อข้ามภูมิภาคทั้งทางบกและทางทะเล จะทำให้ภูมิภาคต่างๆ ที่อยู่แยกจากกันในบริบททางภูมิรัฐศาสตร์จะถูกดึงเข้ามาให้มีความใกล้ชิดต่อกัน ทั้งในทางเศรษฐกิจและสังคม แต่ในอีกด้านก็ทำให้หลายประเทศเกิดความกังวลว่า การสร้างเครือข่ายของโครงสร้างพื้นฐานของรัฐบาลจีนนั้น จะนำไปสู่การขยายอิทธิพลของจีนเข้าไปในพื้นที่หรือเป็นการส่งออกอิทธิพลจีนผ่านระบบโลกดิจิทัลใหม่ ทั้งยังทำให้อำนาจในการปิดล้อมของสหรัฐอเมริกา ตามแนวคิดของยุคสงครามเย็นที่มีจีนเป็นเป้าหมาย ไม่อาจกระทำได้จริงเช่นในอดีต สหรัฐอเมริกาจึงต้องการชะลอการพัฒนาแสนยานุภาพของจีนในทุกด้านโดยเฉพาะด้านการค้าและ

ด้านเทคโนโลยีที่จีนพัฒนาไปไกลมาก (สุรชาติ บำรุงสุข, 2563) จากสถานการณ์การเมืองโลกดังกล่าวส่งผลให้ประเทศไทยต้องพยายามเร่งพัฒนาให้ก้าวทันการเปลี่ยนแปลง และต้องสอดคล้องกับนโยบาย “ไทยแลนด์ 4.0” และจากการที่รัฐบาลมีนโยบายให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับชาติ ตั้งแต่อดีต ปัจจุบัน และอนาคต เนื่องจากอาจสร้างความเสียหายแก่ความมั่นคงของชาติอย่างรุนแรงได้ จึงกล่าวได้ว่า สถานะแวดล้อมทางการเมืองนั้นเป็นปัจจัยที่สนับสนุนต่อการพัฒนาขีดความสามารถของบุคลากรของหน่วยไซเบอร์ทางทหาร

## 2. สถานะแวดล้อมทางการทหาร

ประเทศมหาอำนาจเสริมสร้างแสนยานุภาพทางทหารให้เหนือกว่าคู่แข่ง เพื่อใช้เป็นอำนาจในการเจรจาผลประโยชน์ของตนเอง ปัจจุบันสหรัฐอเมริกาเร่งยกระดับขีดความสามารถทางทหาร เพื่อช่วงชิงอิทธิพลเหนือภูมิภาคอินโดแปซิฟิกกับจีน โดยทบทวนแผนยุทธศาสตร์ที่เกี่ยวข้อง และมีปัจจัยสำคัญคือ การขยายขอบเขตการติดตั้งอาวุธนำวิถีพิสัยไกลให้ครอบคลุมทั้งทางบก ทางทะเล และทางอากาศ ซึ่งนับเป็นการสร้างปัญหาทางการทหารในระดับโลก เพราะอาจก่อให้เกิดความจำเป็นในการต้องเลือกข้างระหว่างสหรัฐอเมริกาและจีนในอนาคตอันใกล้ สำหรับกองทัพไทยนั้น จากการจัดลำดับแสนยานุภาพทางการทหารของกองทัพทั่วโลกโดยเว็บไซต์ Global Fire Power (2021) พบว่า ไทยอยู่ในลำดับที่ 26 ของโลก และเป็นลำดับที่ 3 ของอาเซียน รองจากอินโดนีเซียและเวียดนาม นอกจากนี้แสนยานุภาพทางอาวุธยุทโธปกรณ์แล้ว ไทยก็ยังให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กระทรวงกลาโหมได้ขับเคลื่อนการปฏิรูปกองทัพด้านไซเบอร์ให้สอดคล้องกับยุทธศาสตร์ชาติด้านความมั่นคง และยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม โดยมีการจัดตั้งหน่วยไซเบอร์ทางทหารขึ้น เพื่อให้ปฏิบัติภารกิจด้านไซเบอร์โดยตรง จึงกล่าวได้ว่า สถานะแวดล้อมทางการทหารนั้นเป็นปัจจัยที่สนับสนุนต่อการพัฒนาขีดความสามารถของบุคลากรของหน่วยไซเบอร์ทางทหาร

## 3. สถานะแวดล้อมทางเศรษฐกิจ

กองทุนการเงินระหว่างประเทศ (IMF) ประเมินว่าในปี 2564 เศรษฐกิจโลกอาจขยายตัว 6.0% ดีขึ้นจากที่คาดไว้ 5.5% เป็นผลจากการปรับเพิ่ม GDP ของประเทศแกนหลัก นำโดยสหรัฐฯ จีน ยุโรป และญี่ปุ่น GDP ของจีนไตรมาส 1/2564 เติบโตสูงสุดเป็นประวัติการณ์ ปัจจัยเสี่ยงที่จะฉุดรั้งการฟื้นตัวของเศรษฐกิจโลกที่สำคัญ คือ การแพร่ระบาดของโรค COVID-19 ระลอกใหม่ รัฐบาลหลายประเทศกำลังเผชิญอุปสรรค ด้านนโยบายการเงินและการคลังอย่างหนักในขณะนี้ สำหรับ



เศรษฐกิจไทยปี 2564 เติบโต 2.2% จากเดิมที่คาดไว้ 2.5% และมีแนวโน้มฟื้นตัวกลับมาได้ช้า ส่งผลกระทบทำให้ GDP ต่ำลง ธนาคารกรุงศรีอยุธยา (20 เม.ย. 64) ประกอบกับหนี้สาธารณะที่สูงขึ้นเพราะรายได้ที่ไม่พอกับรายจ่าย ทำให้รัฐบาลต้องกู้เงินเพื่อชดเชยการขาดดุลงบประมาณ และกู้เงินนอกงบประมาณตามพระราชกำหนดซึ่งให้อำนาจกระทรวงการคลังกู้เงินเพื่อแก้ไขปัญหา โดยปัจจัยหลักที่จะช่วยขับเคลื่อนเศรษฐกิจ คือ การท่องเที่ยว การส่งออก และการลงทุนจากภาครัฐ แต่อาจถูกรงับไปถ้าเกิดการแพร่ระบาดระลอกใหม่และความขัดแย้งทางการเมืองภายใน รวมถึงเกิดภัยคุกคามด้านไซเบอร์ซึ่งส่งผลกระทบและความเสียหายในวงกว้าง ทั้งนี้ การรักษาความมั่นคงปลอดภัยไซเบอร์ให้ดำรงสภาพความต่อเนื่อง การจ้างผู้เชี่ยวชาญเฉพาะด้าน การฝึกอบรมและการศึกษาดูงาน เพื่อให้ก้าวทันต่อความเปลี่ยนแปลงที่เกิดขึ้น แม้จำเป็นต้องใช้งบประมาณจำนวนมาก แต่ด้วยความที่เป็นเรื่องของความมั่นคงของชาติและส่งผลกระทบที่ยิ่งใหญ่ได้ทุกที่ทุกเวลา กอปรกับเป็นนโยบายที่เร่งด่วนและต้องดำเนินการ รัฐบาลจึงพร้อมให้การสนับสนุนงบประมาณ จึงกล่าวได้ว่า สภาวะแวดล้อมทางเศรษฐกิจเป็นปัจจัยที่สนับสนุนต่อการพัฒนาขีดความสามารถของบุคลากรของหน่วยไซเบอร์ทางทหาร

#### 4. สภาวะแวดล้อมทางสังคมจิตวิทยา

กระแสโลกาภิวัตน์นำไปสู่การเปลี่ยนวิถีชีวิตผู้คนในสังคม อินเทอร์เน็ตกลายเป็นสิ่งจำเป็นในชีวิตประจำวัน และเป็นช่องทางสำหรับการแลกเปลี่ยนความคิดเห็น วัฒนธรรมในยุคโลกาภิวัตน์มีอิทธิพลต่อชีวิตและความเป็นอยู่ของสมาชิกในสังคมและความเจริญของประเทศชาติ ความก้าวหน้าของวิทยาการและเทคโนโลยีสมัยใหม่ นำไปสู่การเปลี่ยนแปลงทางสังคม ส่งผลกระทบต่อการพัฒนาที่ยั่งยืน ทุกประเทศทั่วโลกกำลังวิตกกังวลกับภัยคุกคามด้านไซเบอร์ ซึ่งหลายประเทศกำลังถูกคุกคามอย่างต่อเนื่องจากการโจมตีทางไซเบอร์

สำหรับประเทศไทย มีการเปลี่ยนแปลงตามกระแสโลกาภิวัตน์ เช่น รับเอาวัฒนธรรมสากลเข้ามาใช้นำเทคโนโลยีสารสนเทศเข้ามาเป็นส่วนหนึ่งของชีวิต สื่อสังคมออนไลน์นำมาซึ่งความรู้ ข่าวสารความบันเทิงรวมถึงภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นได้ทุกที่ทุกเวลา ดังนั้นทุกคนจึงต้องเรียนรู้และปรับตัวให้เข้ากับวิถีชีวิตรูปแบบใหม่ ให้มีความสำคัญกับการตระหนักรู้ในการรักษาความปลอดภัยทางไซเบอร์ ซึ่งจะทำให้ทุกคนอยู่ก้าวหน้าทันโลกอย่างปลอดภัย (พิณสุดา สิริธรังศรี, 2560) จึงกล่าวได้ว่า สภาวะแวดล้อมทางสังคมจิตวิทยานั้นเป็นปัจจัยที่สนับสนุนต่อการพัฒนาขีดความสามารถของบุคลากรของหน่วยไซเบอร์ทางทหาร

## 5. สภาวะแวดล้อมทางเทคโนโลยีสารสนเทศ

กระแสโลกาภิวัตน์ทำให้เกิดการเชื่อมโยงโลกเข้าด้วยกันจนเป็นโลกไร้พรมแดน ความเชื่อมโยงในมิติต่าง ๆ นำมาซึ่งสารสนเทศ นวัตกรรม ความเจริญทางด้านการศึกษา วิทยาศาสตร์และเทคโนโลยี ความรู้เป็นกลไกหลักและรากฐานของการพัฒนาในทุกมิติ โลกก้าวเข้าสู่สังคมแห่งการเรียนรู้ จึงเป็นโลกของการสืบหาความรู้จากสารสนเทศเพื่อการพัฒนาที่ยั่งยืน

สำหรับประเทศไทย จากการเข้าถึงข้อมูลและองค์ความรู้ในรูปของสารสนเทศที่ง่ายและไร้ขีดจำกัด เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทในการเรียนรู้ของประชาชนทุกระดับและเป็นเครื่องมือสำคัญในการผลักดันให้ประชาชนชาวไทยก้าวเข้าสู่สังคมแห่งการเรียนรู้ ทั้งนี้ สิ่งสำคัญ คือ การตระหนักรู้ในเรื่องภัยคุกคาม ที่มาควบคู่กับสารสนเทศ ต้องเรียนรู้ที่จะป้องกันและใช้สารสนเทศให้เกิดประโยชน์ต่อตนเองและสังคม จึงอาจกล่าวได้ว่า สภาวะแวดล้อมทางเทคโนโลยีสารสนเทศนั้น เป็นปัจจัยที่สนับสนุนต่อการพัฒนาขีดความสามารถของบุคลากรของหน่วยไซเบอร์ทางทหาร

### ทางเลือกทางยุทธศาสตร์ในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร

จากการวิเคราะห์ถึงสาเหตุของปัญหา และการวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ทั้ง 5 ด้านแล้ว ทางเลือกทางยุทธศาสตร์ในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารยังต้องพิจารณาร่วมกับแนวคิดและทฤษฎีที่เกี่ยวข้องกับการพัฒนาขีดความสามารถบุคลากร ดังนี้

#### ทางเลือกที่ 1 การพัฒนาขีดความสามารถของบุคลากร ตามแนวคิดเกี่ยวกับกระบวนการพัฒนาบุคลากร

แนวคิดเรื่องกระบวนการพัฒนาบุคลากรตามที่ พิไลวรรณ อินทรักษา (2550) ได้อธิบายไว้ ประกอบด้วย 3 ขั้นตอน ได้แก่ ขั้นแรกเป็นการวิเคราะห์ความต้องการและความจำเป็นในการพัฒนาบุคลากร โดย

- 1) วิเคราะห์องค์การทั้งในปัจจุบันและอนาคต
- 2) วิเคราะห์ความต้องการของกลุ่มงานเฉพาะ และ
- 3) วิเคราะห์ความต้องการรายบุคคล

ขั้นที่สองเป็นการกำหนดเป้าหมายและเกณฑ์การพัฒนาบุคลากร และขั้นที่สามเป็นการเลือกแนวทางการพัฒนาบุคลากร เพิ่มพูนทักษะในงานอาชีพและปรับตัวให้ทันกับเทคโนโลยีและสิ่งแวดล้อมที่เปลี่ยนแปลง เมื่อได้รับการพัฒนาแล้วความสามารถและความประพฤติดของบุคลากรจะเปลี่ยนแปลงไปในทิศทางที่หน่วยงานต้องการ

จากแนวคิดดังกล่าว สามารถนำมาประยุกต์ใช้กำหนดแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร ได้ดังนี้

1. การปรับโครงสร้างหน่วยและอัตรากำลังพลให้เหมาะสมกับปริมาณงานที่ต้องดำเนินการ ทั้งในปัจจุบันและอนาคต
2. การจัดทำ Unit school เพื่อพัฒนาบุคลากรในหน่วยงานให้ทันกับการเปลี่ยนแปลงของเทคโนโลยี เครื่องมือ กระบวนการทำงาน ใช้ระยะเวลาสั้น ๆ ไม่กระทบต่อการปฏิบัติงานหลักและไม่ใช้งบประมาณ
3. In-house training โดยการส่งบุคลากรไปฝึกอบรมภายนอกและนำความรู้มาสร้างเป็นหลักสูตร การฝึกอบรมภายใน มีการคัดเลือกผู้เชี่ยวชาญมาอบรมซึ่งจะส่งผลดีต่อองค์กรและผู้เข้ารับการอบรม
4. Training program เป็นการฝึกอบรมอย่างต่อเนื่องที่รวบรวมหลักสูตรย่อยๆ ไว้หลายหลักสูตร เป็นการพัฒนาบุคลากรในระยะยาว โดยเน้นที่การลงมือฝึกปฏิบัติ (Workshop) เพื่อให้เกิดทักษะในการทำงาน
5. ให้การสนับสนุนงบประมาณในการพัฒนาบุคลากรด้านไซเบอร์ในระดับต่างๆ รวมถึงการจัดให้มีการฝึกอบรมเกี่ยวกับไซเบอร์ในระดับมาตรฐานสากล ซึ่งเป็นที่ยอมรับจากหน่วยงานความมั่นคงและสนับสนุนให้สอบเพื่อได้ใบประกาศนียบัตรวิชาชีพ (Certificate) ด้านไซเบอร์

## ทางเลือกที่ 2 การพัฒนาขีดความสามารถของบุคลากรตามทฤษฎีการจูงใจในการทำงาน

จากการทบทวนทฤษฎีการจูงใจในการทำงาน พบว่า กมลพร กัลยาณมิตร (2559) เสนอทฤษฎีสองปัจจัยของเฮอริซเบิร์ก (Herzberg's two factors) โดยเชื่อว่าปัจจัยสำคัญที่จะทำให้เกิดแรงจูงใจในการทำงาน สามารถแยกได้เป็น 2 ลักษณะ ได้แก่

1. องค์ประกอบแรงจูงใจ (Motivation factors) หมายถึง องค์ประกอบที่เกี่ยวกับตัวงานและความสำเร็จก้าวหน้าของงาน ประกอบด้วยปัจจัย 5 ประการ ดังนี้ ความสำเร็จของงาน การได้รับความยอมรับนับถือ ลักษณะของงาน ความรับผิดชอบและความก้าวหน้าในตำแหน่งงาน
2. องค์ประกอบค้ำจุน (Maintenance factors) หมายถึง องค์ประกอบที่เกี่ยวกับสิ่งแวดล้อมในการทำงาน ประกอบด้วย ปัจจัย 11 ประการ ดังนี้ ความก้าวหน้าในอนาคต ฐานะของอาชีพ รายได้ ความสัมพันธ์กับผู้บังคับบัญชา ความสัมพันธ์กับผู้บังคับบัญชา ความสัมพันธ์กับเพื่อนร่วมงาน วิธีการปกครองบังคับบัญชา นโยบายและการบริหารงานของหน่วยงาน สภาพการทำงาน ความเป็นอยู่ส่วนตัว และความมั่นคงในงาน

การนำทฤษฎีสองปัจจัยของเฮอริชเบอร์เกอร์มาประยุกต์ใช้ในการพัฒนาขีดความสามารถของบุคลากร หน่วยไซเบอร์ทางทหาร ทำให้สามารถกำหนดแนวทางได้ดังนี้

1. จัดทำแนวทางความก้าวหน้าในอาชีพ (Career path) บุคลากรด้านไซเบอร์ให้เป็นเช่นเดียวกับแนวทางสำหรับวิศวกรหรือแพทย์ ที่ต้องใช้บุคลากรที่มีขีดความสามารถและทักษะต่างๆ สูงกว่าบุคคลทั่วไป
2. พิจารณาเงินเพิ่มสำหรับตำแหน่งที่มีเหตุพิเศษของผู้ปฏิบัติงานไซเบอร์ และผู้ที่มีประกาศนียบัตรวิชาชีพด้านไซเบอร์ตามที่หน่วยงานกำหนด
3. จัดสภาพแวดล้อมที่ดีในการทำงาน เช่น มีสิ่งอำนวยความสะดวก มีห้องพักผ่อนคลายเครียด
4. สร้างความสัมพันธ์ที่ดีต่อผู้ร่วมงานในทุกระดับ เช่น จัดกิจกรรมเพื่อสร้างความสามัคคี
5. ส่งเสริมการทำงานเป็นทีม ร่วมกันแก้ปัญหาเพื่อให้งานสำเร็จ
6. สร้างเครือข่ายสำหรับผู้ปฏิบัติงานทางด้านไซเบอร์อย่างเป็นรูปธรรม

### ทางเลือกที่ 3 การพัฒนาขีดความสามารถของบุคลากรตามแนวคิดในการจัดการเรียนรู้ ในศตวรรษที่ 21

อมรรัตน์ เตชะนอก, รัชณี จรุงศิริวัฒน์ และพระฮอนด้า วาทสพโท (2560) ได้กล่าวว่า ต้องจัดการเรียนรู้ เพื่อใช้ในการดำรงชีวิตในสังคมแห่งการเปลี่ยนแปลง ครูจะเป็นผู้สอนไม่ได้ แต่ต้องให้ผู้เรียนนั้นเรียนรู้ด้วยตนเอง โดยผสมผสานความรู้ความชำนาญ เพื่อความสำเร็จของผู้เรียน ทั้งด้านการทำงานและการดำเนินชีวิต ครูจะออกแบบการเรียนรู้ ฝึกฝนให้เหมือนโค้ช ส่งเสริมการค้นคว้าด้วยตนเอง โดยนำเทคโนโลยีเข้ามาช่วยให้มากที่สุด การนำแนวคิดในการจัดการเรียนรู้ในศตวรรษที่ 21 มาประยุกต์ใช้ในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร มีแนวทางดังนี้

1. การจัดการเรียนการสอนในรูปแบบใหม่ โดยใช้แนวคิดการพัฒนาขีดความสามารถของบุคลากรบนพื้นฐาน 70:20:10 Learning model ซึ่งองค์กรทั้งภาครัฐและภาคเอกชนนำมาจัดทำเป็นยุทธศาสตร์การพัฒนาทรัพยากรมนุษย์ โดยมุ่งเน้นการเรียนรู้จากการปฏิบัติจริง พัฒนาทักษะการทำงานให้บุคลากรมีความรู้ ความเข้าใจ มีทักษะและความเชี่ยวชาญ สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ โดย 70% เป็นการลงมือปฏิบัติและเรียนรู้จากประสบการณ์การทำงานจริงและการคิดแก้ปัญหา 20% เป็นการแลกเปลี่ยนความรู้จากการสอนงานหรือจากผู้เชี่ยวชาญ ที่เลี้ยงที่ให้คำปรึกษาแนะนำ รวมถึงการประชุมหารือ แลกเปลี่ยนความรู้เกี่ยวกับการทำงาน และ 10% เป็นการศึกษา

หาความรู้ผ่านหลักสูตรการฝึกอบรมสัมมนาทั้งภายในและภายนอกองค์กร รวมถึงการเรียนรู้ด้วยตนเอง

2. เรียนรู้และพัฒนาผ่านการทำงานที่ท้าทาย การลงมือปฏิบัติและประสบการณ์ ครูเป็นผู้ชี้แนะแนวทางในการเรียนรู้ ให้เรียนรู้และพัฒนาผ่านการสอนงาน

### แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร

จากการวิเคราะห์ถึงสาเหตุของปัญหา การวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ แนวคิดและทฤษฎีที่เกี่ยวข้อง จึงได้ทางเลือกทางยุทธศาสตร์ในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารที่ดีที่สุด โดยเป็นการบูรณาการแนวคิดและทฤษฎีที่เกี่ยวข้องจากทางเลือกทางยุทธศาสตร์ทั้ง 3 ทางเลือก เนื่องจากทางเลือกที่ 1 การใช้แนวคิดเกี่ยวกับกระบวนการพัฒนาบุคลากรเพียงอย่างเดียวยังไม่สามารถแก้ไขปัญหาได้ ทำให้ต้องมองถึงปัจจัยต่าง ๆ ตามทฤษฎีการจูงใจในการทำงานตามทางเลือกที่ 2 เข้ามาประกอบ เช่น การสร้างแนวทางการก้าวหน้าในอาชีพของบุคลากรด้านไซเบอร์ การพิจารณาเงินเพิ่มสำหรับตำแหน่งที่มีเหตุพิเศษของผู้ปฏิบัติงานไซเบอร์และผู้ที่มีการศึกษาระดับปริญญาตรีด้านไซเบอร์ตามที่หน่วยงานกำหนด การจัดสภาพแวดล้อมที่ดีในการทำงานให้มีสิ่งอำนวยความสะดวกและมุมผ่อนคลาย การสร้างความสัมพันธ์ที่ดีต่อผู้ร่วมงานในทุกๆระดับ การจัดกิจกรรมเพื่อสร้างความสามัคคีในหมู่คณะ การทำงานเป็นทีมเพื่อร่วมกันแก้ปัญหาให้งานสำเร็จ รวมถึงการสร้างเครือข่ายสำหรับผู้ปฏิบัติงานทางด้านไซเบอร์อย่างเป็นรูปธรรม เพื่อให้บุคลากรมีขวัญกำลังใจและเกิดทัศนคติที่ดีต่อการปฏิบัติงานมากขึ้น รวมทั้งทางเลือกที่ 3 เป็นการปรับเปลี่ยนการเรียนรู้ให้ตรงกับแนวคิดในการจัดการเรียนรู้ในศตวรรษที่ 21 โดยต้องจัดการเรียนรู้เพื่อใช้ในการดำรงชีวิตในสังคมแห่งการเปลี่ยนแปลง ผู้เรียนต้องเรียนรู้ด้วยตนเอง โดยนำเทคโนโลยีเข้ามาช่วยให้มากที่สุด ต้องผสมผสานความรู้ ความชำนาญเพื่อความสำเร็จของผู้เรียน ทั้งด้านการทำงานและการดำเนินชีวิต ครูจะออกแบบการเรียนรู้ ฝึกฝนให้เหมือนโค้ชแต่ไม่ได้ทำหน้าที่สอน ซึ่งจะทำให้การพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารมีประสิทธิภาพมากขึ้น โดยมีแนวทางดังนี้

1. การปรับโครงสร้างหน่วยและอัตรากำลังพลให้เหมาะสมกับปริมาณงานที่ต้องดำเนินการทั้งในปัจจุบันและอนาคต
2. การจัดตั้งโรงเรียนไซเบอร์ทางทหาร เพื่อให้เป็นหน่วยงานหลักในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารในภาพรวม

3. ให้การสนับสนุนงบประมาณในการพัฒนาบุคลากรด้านไซเบอร์ในระดับต่างๆ รวมถึงการจัดให้มีการฝึกอบรมเกี่ยวกับไซเบอร์ในระดับมาตรฐานสากล ซึ่งเป็นที่ยอมรับจากหน่วยงานความมั่นคง และสนับสนุนให้สอบเพื่อได้ใบประกาศนียบัตรวิชาชีพ (Certificate) ด้านไซเบอร์
4. จัดทำแนวทางความก้าวหน้าในอาชีพ (Career Path) บุคลากรด้านไซเบอร์ให้เป็นเช่นเดียวกับแนวทางสำหรับวิศวกรหรือแพทย์ ที่ต้องใช้บุคลากรที่มีขีดความสามารถและทักษะต่างๆ สูงกว่าบุคคลทั่วไป
5. การพิจารณาเงินเพิ่มสำหรับตำแหน่งที่มีเหตุพิเศษของผู้ปฏิบัติงานไซเบอร์และผู้ที่มีการประกาศนียบัตรวิชาชีพด้านไซเบอร์ตามที่หน่วยงานกำหนด
6. จัดสภาพแวดล้อมที่ดีในการทำงานและการสร้างความสัมพันธ์ที่ดีต่อผู้ร่วมงานในทุกๆ ระดับ
7. มีการทำงานเป็นทีม ร่วมกันแก้ปัญหาเพื่อให้งานสำเร็จ
8. มีการสร้างเครือข่ายสำหรับผู้ปฏิบัติงานทางด้านไซเบอร์อย่างเป็นรูปธรรม
9. การจัดการเรียนการสอนในรูปแบบใหม่ โดยใช้แนวคิดการพัฒนาขีดความสามารถของบุคลากรบนพื้นฐาน 70:20:10 Learning model
10. การบูรณาการหลักสูตรในสายวิทยาการไซเบอร์และปรับปรุงให้มีความทันสมัย สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอยู่เสมอ เพื่อเพิ่มพูนความรู้ให้กับหน่วยที่เกี่ยวข้องอย่างต่อเนื่อง
11. การจัดการแข่งขันและเข้าร่วมการแข่งขันทักษะทางไซเบอร์ที่เกี่ยวข้อง
12. การฝึกอบรมด้านทักษะทางไซเบอร์ระหว่างหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน

ทั้งนี้ ทางเลือกใหม่ที่เป็นการปรับโครงสร้างหน่วยและจัดตั้งโรงเรียนไซเบอร์ทางทหารนั้น สามารถแก้ไขปัญหาบุคลากรหน่วยไซเบอร์ทางทหารได้เป็นอย่างดี เนื่องจากเมื่อได้รับการฝึกอบรมบุคลากรก็จะมีทักษะในการปฏิบัติงานด้านไซเบอร์เพิ่มมากขึ้น สามารถทำงานได้อย่างมีประสิทธิภาพมากกว่าเดิม ส่วนแนวทางอื่นๆ ที่กล่าวมาข้างต้นนั้น สามารถดำเนินการควบคู่ไปได้ในทันที

จากผลการวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ทั้ง 5 ด้าน พบว่าสถานะแวดล้อมทางการเมืองและการทหารเป็นจุดแข็ง เนื่องจากรัฐบาลมีนโยบายที่ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับชาติ ทั้งในปัจจุบันและอนาคต ทำให้เป็นปัจจัยที่สนับสนุนการพัฒนาขีดความสามารถบุคลากรหน่วยไซเบอร์ทางทหารได้

เป็นอย่างดี สำหรับสภาวะแวดล้อมทางสังคมจิตวิทยาและเทคโนโลยีสารสนเทศถือได้ว่าเป็นโอกาส เพราะในสังคมโลกที่มีกระแสโลกาภิวัตน์ทำให้เป็นโลกที่ไร้พรมแดน มีการติดต่อสื่อสารเพื่อแลกเปลี่ยนเรียนรู้ ให้บริการข้อมูลข่าวสารระหว่างกันในมิติทางไซเบอร์เป็นหลัก โดยมีอินเทอร์เน็ตเป็นโครงสร้างพื้นฐาน มีคอมพิวเตอร์รวมถึงอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต จึงนับว่าเป็นปัจจัยที่สนับสนุนส่วนสภาวะแวดล้อมทางเศรษฐกิจนั้น ไม่มีผลกระทบเพราะการปรับโครงสร้างและจัดตั้งโรงเรียนไซเบอร์ทางทหาร สามารถใช้ทรัพยากร บุคลากร อาคารสถานที่และเครื่องมืออุปกรณ์เดิมที่มีอยู่ ในอดีตการก่อตั้งหน่วยไซเบอร์ทางทหารทั้ง 5 หน่วยนั้น ก็ผ่านกระบวนการปรับโครงสร้างหน่วย ปรับเกลี้ยอัตรากำลังพลและทรัพยากรมาแล้วเช่นกัน จึงกล่าวได้ว่าสภาพแวดล้อมทางยุทธศาสตร์จากพลังอำนาจทั้ง 5 ด้าน เป็นปัจจัยที่สนับสนุนการพัฒนาขีดความสามารถบุคลากรหน่วยไซเบอร์ทางทหาร

ที่สำคัญ แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารที่เสนอข้างต้นจะช่วยสนับสนุนแผนปฏิบัติการกองบัญชาการกองทัพไทย พ.ศ. 2563 - 2565 ในด้านการพัฒนาขีดความสามารถด้านไซเบอร์สนับสนุนแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคงแผนย่อยที่ 2 การป้องกันและแก้ไขปัญหามีผลกระทบต่อความมั่นคง ในส่วนของการรักษาความมั่นคงภายในราชอาณาจักรและการพัฒนาประเทศ และแผนย่อยที่ 3 การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ ซึ่งรองรับยุทธศาสตร์ชาติด้านความมั่นคง นอกจากนี้มีแนวคิดการพัฒนากุศลกร โดยใช้แนวคิดและทฤษฎีด้านการพัฒนากุศลกรมารองรับซึ่งสอดคล้องกับแนวทางการปฏิบัติที่ดีของกองทัพประเทศสหรัฐอเมริกา และงานวิจัยที่ผ่านมาจำนวน 3 เล่ม จึงกล่าวได้ว่าการบูรณาการจากทางเลือกทางยุทธศาสตร์ทั้ง 3 ทางเลือกเพื่อเป็นแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารนั้น เป็นทางเลือกที่ดีที่สุดและสามารถนำไปแก้ไขปัญหากุศลกรหน่วยไซเบอร์ทางทหารได้อย่างยั่งยืน

## บทที่ 3

### บทอภิปรายผล

จากทางเลือกทางยุทธศาสตร์ในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารที่ดีที่สุด เป็นการปรับโครงสร้างหน่วยและจัดตั้งโรงเรียนไซเบอร์ทางทหารขึ้น เพื่อให้เป็นหน่วยงานหลักในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร ผู้วิจัยได้ศึกษาข้อมูลจากการเปรียบเทียบแนวทางการปฏิบัติที่ดี (Good practices) รวมทั้งศึกษาจากการเปรียบเทียบกับงานวิจัยที่เกี่ยวข้อง โดยมีรายละเอียดดังนี้

#### การเปรียบเทียบกับวิธีปฏิบัติที่ดี

จากผลการวิเคราะห์ในบทที่ 2 ทำให้ได้ทางเลือกใหม่ที่เป็นแนวทางในการจัดตั้งโรงเรียนไซเบอร์ทางทหารขึ้นเพื่อแก้ไขปัญหาเรื่องการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร ซึ่งสอดคล้องกับวิธีปฏิบัติที่ดีของกองทัพสหรัฐอเมริกา ดังที่ ศรีศักดิ์ จามรมาน (2557) ได้เขียนไว้ในวารสาร TELECOM & INNOVATION JOURNAL ว่า ทั้งกองทัพบก กองทัพเรือ กองทัพอากาศและนาวิกโยธิน ดำเนินการฝึกอบรมนักรบไซเบอร์ โดยตั้งสถาบันการศึกษาทางทหารเพื่อผลิตนักรบไซเบอร์และจัดตั้งสถาบันฝึกอบรมสงครามไซเบอร์ขึ้นหลายแห่ง ดังนี้ 1) ศูนย์ความเป็นเลิศทางไซเบอร์กองทัพบกที่ฐานทัพออร์ดอน รัฐจอร์เจีย 2) ศูนย์แห่งความโดดเด่นด้านสารสนเทศกองทัพเรือที่เมืองเพนซาโคลา รัฐฟลอริดา 3) กองทัพอากาศได้ตั้งกองบินที่ 24 ให้เป็นกองบินด้านไซเบอร์ที่ซานอันโตนิโอ แลคแลนด์ รัฐเท็กซัส 4) กองทัพอากาศได้ตั้งกองบินที่ 24 มีหน่วยงานรับสมัครและฝึกอบรมนักรบไซเบอร์ 5) มหาวิทยาลัยป้องกันแห่งชาติ (National Defense University) ทั้งนี้กระทรวงกลาโหมสหรัฐอเมริกา จะฝึกอบรมนักรบไซเบอร์ให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี โดยมีการจัดอบรมด้านการรักษาความปลอดภัยไซเบอร์ เทคโนโลยีสงครามไซเบอร์และความรู้ที่ไม่มีในคู่มือการปฏิบัติงานหรือตำราเรียน ซึ่งนับว่านักรบไซเบอร์จะต้องเรียนรู้อยู่ตลอดเวลา

#### การเปรียบเทียบกับงานวิจัยที่เกี่ยวข้อง

สำหรับประเด็นการจัดตั้งโรงเรียนไซเบอร์ทางทหารซึ่งเป็นการปรับโครงสร้างหน่วยให้สอดคล้องกับภารกิจที่เปลี่ยนแปลงไปในยุคไซเบอร์ที่ผู้วิจัยเสนอนั้นมีความสอดคล้องกับงานวิจัย



ของ ฌอง-เวต์ตี เรืองจวง, น.อ. (2561) เรื่อง แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ ซึ่งเป็นกรวิจัยเชิงคุณภาพที่ได้ศึกษาและวิเคราะห์จากข้อมูลข่าวสารด้านไซเบอร์ที่เผยแพร่โดยทั่วไป นโยบายระดับต่าง ๆ และเอกสารที่เกี่ยวข้อง เก็บข้อมูลจากข้าราชการชั้นสัญญาบัตรของกองทัพอากาศที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ผลการวิจัยพบว่า ปัจจัยที่มีผลกระทบต่อขีดความสามารถในการปฏิบัติการด้านไซเบอร์คือ บุคลากรมีไม่เพียงพอ ขาดความรู้และทักษะในการปฏิบัติงานด้านไซเบอร์ ดังนั้นต้องพัฒนาบุคลากรด้วยการให้การศึกษา การฝึกปฏิบัติ และโครงสร้างการจัดหน่วยไซเบอร์ของกองทัพอากาศ สามารถรองรับบุคลากรที่ปฏิบัติงานได้ในปัจจุบันเท่านั้น หากมีภารกิจด้านไซเบอร์มากขึ้นจากปัจจุบัน ควรพิจารณาทบทวนโครงสร้างการจัดหน่วยให้สอดคล้องกับการปฏิบัติภารกิจด้วย

ในประเด็นที่ผู้วิจัยเสนอให้มีการกำหนดให้มีเงินเพิ่มสำหรับตำแหน่งที่มีเหตุพิเศษของผู้ปฏิบัติงานไซเบอร์และผู้ที่มีประกาศนียบัตรวิชาชีพด้านไซเบอร์ สอดคล้องกับงานวิจัยของ ปรัชญา เฉลิมวัฒน์ (พล.ต., 2561) เรื่อง แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ ด้วยการวิจัยเชิงผสมผสาน ซึ่งได้ใช้แบบสอบถามเก็บข้อมูลจากผู้ปฏิบัติงานด้านไซเบอร์ของสำนักงานปลัดกระทรวงกลาโหม และมีการวิเคราะห์ข้อมูลเชิงคุณภาพจากเอกสารและการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญด้านการบริหารจำนวน 6 คน และผู้เชี่ยวชาญด้านยุทธศาสตร์ชาติจำนวน 7 คน ผลการวิจัยพบว่า บุคลากรด้านไซเบอร์เป็นกลุ่มบุคคลที่มีความสำคัญมาก ภาครัฐประสบปัญหาการขาดแคลนบุคลากรด้านนี้ การพัฒนาบุคลากรโดยการสร้างแรงจูงใจจากค่าตอบแทนพิเศษที่ได้รับเพิ่มจากการมีประกาศนียบัตร ใบรับรองต่าง ๆ ในแต่ละบุคคลจึงถือเป็นเรื่องสำคัญในแผนการปฏิบัติระดับชาติ ซึ่งจะต้องมีการดำเนินการอย่างเร่งด่วน เริ่มจากการกำหนดหลักสูตรในสถานศึกษาและสถานที่ฝึกอบรมตามมาตรฐานสากลเพื่อรองรับการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นตามความก้าวหน้าของเทคโนโลยีและการขยายตัวของการใช้งานระบบเทคโนโลยีสารสนเทศ

สำหรับประเด็นการจัดการเรียนรู้รูปแบบใหม่ที่ต้องใช้เทคโนโลยีสมัยใหม่เข้ามาช่วยและครูเป็นเพียงผู้ชี้แนะแนวทางแต่ผู้เรียนต้องศึกษาด้วยตนเองเป็นหลักนั้น สอดคล้องกับบทความวิชาการของ อติพร เกิดเรือง (2560) เรื่อง การส่งเสริมการเรียนรู้ในศตวรรษที่ 21 เพื่อรองรับสังคมไทยในยุคดิจิทัล ซึ่งเป็นการวิจัยเชิงคุณภาพโดยการสังเคราะห์และวิเคราะห์เอกสารและงานวิจัยในต่างประเทศ ผลการวิจัยพบว่าการเปลี่ยนผ่านการเรียนรู้จากยุคเดิมสู่ยุคดิจิทัล

ต้องจัดการเรียนรู้ โดยคำนึงถึงความสัมพันธ์ระหว่างการเรียน การทำงาน และการดำรงชีวิต เน้นการจัดการเรียนรู้ตลอดชีวิต ส่งเสริมการค้นคว้าด้วยตนเอง โดยนำเทคโนโลยีเข้ามาช่วยในการจัดการเรียนรู้ให้มากที่สุด ครูเป็นเพียงผู้ชี้แนะแนวทางในการเรียนรู้ตามหลักสูตร และมุ่งการวัดผล และประเมินผล เพื่อดูพัฒนาการมากกว่าการวัดผลสัมฤทธิ์ การจัดการศึกษาในยุคดิจิทัล ต้องคำนึงถึงการปรับตัวให้ทันต่อการเปลี่ยนแปลง เน้นการสร้างสรรค์ปรับแต่ง การเรียนรู้ การศึกษาข้อมูลจากการเปรียบเทียบแนวทางการปฏิบัติที่ดี จำนวน 1 เรื่อง รวมทั้งการเปรียบเทียบกับงานวิจัยที่เกี่ยวข้องจำนวน 3 เรื่องนั้น กล่าวได้ว่าข้อมูลข้างต้นเป็นหลักฐานในการสนับสนุนทางเลือกทางยุทธศาสตร์ในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารว่าเป็นทางเลือกที่ดีที่สุดและสามารถนำไปแก้ไขปัญหามูลกรหน่วยไซเบอร์ทางทหารได้อย่างยั่งยืน

## บทที่ 4

### บทสรุป

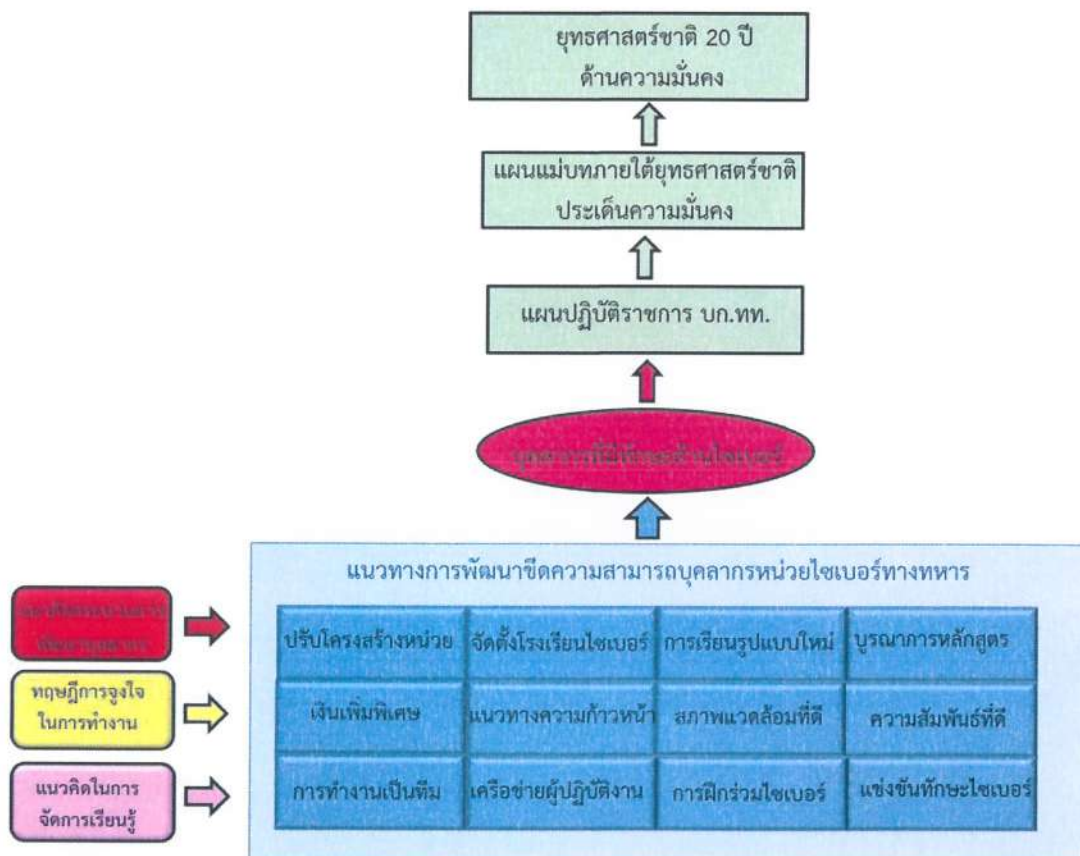
การศึกษาวิจัยเรื่องแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง มีวัตถุประสงค์เพื่ออธิบายสภาพปัญหาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารในการตอบสนองต่อยุทธศาสตร์ชาติด้านความมั่นคง วิเคราะห์ปัจจัยที่สนับสนุนหรือขัดขวางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคงและเพื่อเสนอแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง ผู้วิจัยใช้รูปแบบการวิจัยเชิงยุทธศาสตร์ตามแนวทางที่วิทยาลัยการทัพบกกำหนด โดยใช้วิธีการศึกษาเชิงเอกสาร การรวบรวมข้อมูลจากเอกสารทางวิชาการ เอกสารการวิจัย วิทยานิพนธ์ แนวคิดและทฤษฎีที่เกี่ยวข้อง

#### สรุปผลการวิจัย

ผลจากการวิจัยพบว่า ขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารมีปัญหาการขาดทักษะและความเชี่ยวชาญด้านการรักษาความปลอดภัยไซเบอร์ โดยมีสาเหตุมาจากการขาดแคลนบุคลากรที่มีทักษะและความเชี่ยวชาญดังกล่าว การบรรจุบุคคลที่มีคุณสมบัติไม่ตรงตามคุณวุฒิกับตำแหน่งที่ต้องการ การลาออกจากราชการเพื่อไปทำงานกับภาคเอกชน ซึ่งให้ค่าตอบแทนและสวัสดิการที่มากกว่า การขาดแรงจูงใจในการทำงานจากการไม่มีความก้าวหน้าในการรับราชการ การเลื่อนยศและตำแหน่งถูกจำกัดด้วยจำนวนอัตรา และการมีจำนวนที่นิ่งในการเข้ารับการฝึกอบรมด้านไซเบอร์ไม่เพียงพอต่อการพัฒนาขีดความสามารถของบุคลากร ซึ่งจากการวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ในมิติต่างๆ ตามพลังอำนาจแห่งชาติ พบว่าสภาวะแวดล้อมทางยุทธศาสตร์ทั้งทางการเมือง การทหาร เศรษฐกิจ สังคม จิตวิทยาและเทคโนโลยีสารสนเทศนั้นสนับสนุนต่อการพัฒนาขีดความสามารถของบุคลากรของหน่วยไซเบอร์ทางทหาร

สำหรับการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคงพบว่า มีทางเลือกทางยุทธศาสตร์ 3 ทาง ทางเลือกที่ 1 คือ การพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารตามแนวคิดเกี่ยวกับกระบวนการพัฒนาบุคลากร ทางเลือกที่ 2 คือ

การพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารตามทฤษฎีการจูงใจในการทำงาน และทางเลือกที่ 3 คือ การพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร ตามแนวคิดในการจัดการเรียนรู้ในศตวรรษที่ 21 ซึ่งแนวทางในการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารที่บูรณาการทั้ง 3 ทางเลือกข้างต้นนั้นเป็นทางเลือกที่ดีที่สุด เนื่องจากสอดคล้องกับแนวทางการปฏิบัติที่ดีของต่างประเทศและงานวิจัยที่ผ่านมา และสามารถแก้ปัญหาดังกล่าวได้อย่างเป็นรูปธรรม โดยมีภาพสรุปแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง ดังนี้



ภาพที่ 2 แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหาร

### ข้อเสนอแนะ

เพื่อให้การพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารเกิดประสิทธิภาพสูงสุดและมีความต่อเนื่อง ควรจะต้องมีการนำผลการวิจัยไปประยุกต์ใช้และดำเนินการจัดทำวิจัยเพิ่มเติมเพื่อให้ได้ข้อมูลและแนวคิดอื่นๆ ที่มีรายละเอียดมากยิ่งขึ้นดังนี้

### ข้อเสนอแนะในการนำผลวิจัยไปประยุกต์ใช้

1. ศูนย์ไซเบอร์ทหารควรมีการศึกษาโครงสร้างและอัตรากำลังพลที่เหมาะสมกับการจัดตั้งโรงเรียนไซเบอร์ทางทหาร และกรมยุทธการทหารควรศึกษาเรื่องการปรับโครงสร้างศูนย์ไซเบอร์ทหาร เพื่อจัดตั้งโรงเรียนไซเบอร์ทางทหาร
2. ควรมีการจัดทำแนวทางความก้าวหน้าในอาชีพของบุคลากรด้านไซเบอร์ให้เป็นรูปธรรม พร้อมกำหนดตำแหน่ง หน้าที่และมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ โดยหน่วยไซเบอร์ทางทหาร รวมทั้งจัดการประชุมบูรณาการหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อใช้เป็นแนวทางในการพัฒนาขีดความสามารถของบุคลากรในภาพรวม
3. กรมกำลังพลทหารควรดำเนินการตรวจสอบหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผ่านการบูรณาการ ตามที่ศูนย์ไซเบอร์ทหารเสนอ เพื่อขออนุมัติบรรจุให้เป็นหลักสูตรเฉพาะของสายวิทยาการไซเบอร์
4. หน่วยไซเบอร์ทางทหารควรส่งเสริมให้มีการศึกษาวิจัยด้านไซเบอร์อย่างกว้างขวาง ทั้งเชิงรุกและเชิงรับ

### ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

1. ควรมีการนำผลการวิจัยในครั้งนี้ไปศึกษาต่อยอดโดยการเก็บรวบรวมข้อมูลปฐมภูมิ (Primary data) จากผู้กำหนดนโยบายและบุคลากรที่ปฏิบัติงานด้านไซเบอร์โดยตรงด้วยวิธีการเชิงคุณภาพ เช่น การสัมภาษณ์เชิงลึก (In-depth interview) การสนทนากลุ่ม (Focus group) เพื่อให้ได้ความคิดเห็นและมุมมองที่รอบด้านมาเสริมแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารให้สมบูรณ์ยิ่งขึ้น และสอดคล้องกับความต้องการที่แท้จริงของผู้มีส่วนได้ส่วนเสีย
2. ควรมีการศึกษาวิจัยเพื่อประเมินประสิทธิภาพและประสิทธิผลของแนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารหากมีการนำไปใช้ปฏิบัติจริง
3. หน่วยงานด้านไซเบอร์อื่นๆ สามารถนำแนวทางการวิจัยและผลการวิจัยครั้งนี้ไปประยุกต์ใช้ในการทำวิจัยเพื่อกำหนดแนวทางการพัฒนาขีดความสามารถของบุคลากรให้สอดคล้องกับบริบทของหน่วยงานต่อไป

## เอกสารอ้างอิง

- กมลพร กัลยาณมิตร. (2559). แรงจูงใจ 2 ปัจจัย พลังสู่ความสำเร็จ. *วารสารวไลย  
อลงกรณ์ปริทัศน์ มนุษยศาสตร์และสังคมศาสตร์*, 6(3), 179.
- กองบัญชาการกองทัพไทย. (2563). *เรื่อง แผนปฏิบัติการราชการกองบัญชาการกองทัพไทย  
พ.ศ. 2563 - 2565*. สืบค้นจาก <https://bit.ly/2THEDsW>
- เกียรติพงษ์ อุดมธนะธีระ. (2560). *หลักการ 4M*. สืบค้นจาก <https://bit.ly/3vTrZoT>
- ณรงค์เวทย์ เรืองจวง. (2561). *แนวทางการพัฒนาขีดความสามารถบุคลากรด้าน  
ไซเบอร์ของกองทัพอากาศ*. (เอกสารวิจัยส่วนบุคคลวิทยาลัยป้องกันราชอาณาจักร).  
สืบค้นจาก <https://bit.ly/2Rrmxus>
- เดชา เดชะวัฒน์ไพศาล. (2543). Competency-Based Human Resource Management.  
*วารสารบริหารคน*, 31(4), 11.
- ปรัชญา เฉลิมรัตน์. (2561). *แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัย  
คุกคามระดับชาติ*. (เอกสารวิจัยส่วนบุคคล วิทยาลัยป้องกันราชอาณาจักร). สืบค้น  
จาก <https://bit.ly/3gcqk73>
- พิณสุตา สิริธรงค์ศรี. (2560). *การรู้สารสนเทศกลไกการเรียนรู้ในยุคโลกาภิวัตน์*. สืบค้น  
จาก <https://bit.ly/3ijlxT6>
- ไพโรวรรณ อินทร์รักษา. (2553). *แนวความคิดและทฤษฎีการพัฒนาบุคลากร*. สืบค้นจาก <https://bit.ly/2Sffwx0>
- วิทยาลัยการทัพบก. (ม.ป.ป.). *กระบวนการคิดเชิงยุทธศาสตร์*. สืบค้นจาก <https://bit.ly/3z2pZfW>
- ศรีศักดิ์ จามรมาน. (2557). ตัวอย่างการเร่งรัดพัฒนานักรบไซเบอร์ในประเทศต่างๆ *Telecom &  
Innovation Journal*, 22(983), 16.
- สุรชาติ บำรุงสุข. (2564, 11 พฤษภาคม). ภูมิรัฐศาสตร์ 2020. *มติชนรายสัปดาห์*, น. 12
- อมรรัตน์ เตชะนอก, รัชนิจรุงศิริวัฒน์ และพระฮอนด้า วาทสทุโท (2560). การจัดการศึกษา  
ในศตวรรษที่ 21. *วารสารมหาจุฬานาครทรรศน์*, 7(9), 3.

อติพร เกิดเรือง. (2560). การส่งเสริมการเรียนรู้ในศตวรรษที่ 21 เพื่อรองรับสังคมไทย  
ในยุคดิจิทัล. วารสารวิชาการ มหาวิทยาลัยราชภัฏลำปาง, 6(1), 176.

อภิชาติ วรรณารศน์, พ.อ. (2561). การเสริมสร้างและพัฒนานักวิชาชีพเบอร์ของกองทัพบก  
สำหรับการปฏิบัติการเชิงรุก.(เอกสารวิจัยส่วนบุคคล วิทยาลัยการทัพบก).

## ประวัติย่อผู้วิจัย

ยศ ชื่อ	พันเอกหญิง นริศรา พลอยประไพ
วัน เดือน ปี เกิด	26 มิถุนายน 2514
ประวัติสำเร็จการศึกษา	
พ.ศ. 2530	โรงเรียนสาธิตมหาวิทยาลัยศรีนครินทรวิโรฒ ปทุมวัน
พ.ศ. 2535	ศิลปศาสตรบัณฑิต (บริหารรัฐกิจ) มหาวิทยาลัยเกษตรศาสตร์
พ.ศ. 2542	วิทยาศาสตร์มหาบัณฑิต (วิทยาการคอมพิวเตอร์) มหาวิทยาลัยเกษตรศาสตร์
พ.ศ. 2550	ศิลปศาสตรมหาบัณฑิต (รัฐศาสตร์) มหาวิทยาลัยรามคำแหง
ประวัติการทำงาน	
พ.ศ. 2547 - 2548	หัวหน้าแผนกจำลองสถานการณ์ กองสารสนเทศทางทหาร ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร
พ.ศ. 2551 - 2553	หัวหน้าแผนกบริหารเครือข่าย กองระบบควบคุมบังคับบัญชา ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร
พ.ศ. 2554 - 2556	หัวหน้าแผนกบริการสารสนเทศ กองปฏิบัติการเทคโนโลยี สารสนเทศศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร
พ.ศ. 2556 - 2557	ผู้ช่วยผู้อำนวยการกองพัฒนาระบบงาน กรมการสื่อสารทหาร
พ.ศ. 2557 - 2559	ผู้ช่วยผู้อำนวยการกองวิทยาการ กรมการสื่อสารทหาร
พ.ศ. 2559 - 2561	ผู้ช่วยผู้อำนวยการกองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร
พ.ศ. 2561 - 2562	ผู้ช่วยผู้อำนวยการกองรักษาความปลอดภัย ศูนย์ไซเบอร์ทหาร
ตำแหน่งปัจจุบัน	
พ.ศ. 2562 - ปัจจุบัน	รองผู้อำนวยการกองวิทยาการ ศูนย์ไซเบอร์ทหาร



