แนวทางการพัฒนารูปแบบการฝึกทหาร เพื่อรองรับภัยคุกคามรูปแบบใหม่ : ภัยคุกคามด้านไซเบอร์

โดย

พลตรี ศตวรรษ รามดิษฐ์
ผู้บัญชาการมณฑลทหารบกที่ ๑๒
กองทัพบก

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๕๙
ประจำปีการศึกษา พุทธศักราช ๒๕๕๙ - ๒๕๖๐

บทคัดย่อ

เรื่อง **แนวทางการพัฒนารูปแบบการฝึกทหาร เพื่อรองรับภัยคุกคามรูปแบบใหม่ : ภัยคุกคามด้านไซเบอร์**

ลักษณะวิชา **การทหาร**

ผู้วิจัย **พลตรี ศตวรรษ รามดิษฐ์ หลักสูตร วปอ. รุ่นที่ ๕๙**

งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพ มีวัตถุประสงค์เพื่อ ๑. เพื่อศึกษารูปแบบของภัยคุกคามรูปแบบใหม่ Cyber Attack ในลักษณะต่างๆ ๒. ศึกษา/วิเคราะห์ระบบการฝึกทหารใหม่ของทหารกองประจำการในกองทัพบกไทย ๓. เสนอแนวทางในการพัฒนาระบบการฝึกทหารใหม่เพื่อรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ด้วยการเพิ่มเติมรายการฝึกอบรมบางรายการเข้าไป โดยใช้การเก็บข้อมูลแบบทุติยภูมิ (Secondary Data) โดยผู้วิจัยได้ทำการศึกษาเกี่ยวกับภัยคุกคามรูปแบบใหม่ Cyber Attack ตลอดจนผลกระทบต่อความมั่นคงของชาติ รวมถึงได้ศึกษาเกี่ยวกับระบบการฝึกทบทวนทหารใหม่ในปัจจุบันของกองทัพบกไทย ตลอดจนเก็บข้อมูลแบบปฐมภูมิ (Primary Data) ซึ่งเกิดจากทำการสัมภาษณ์และกระทำแบบสอบถามของบุคคลที่เกี่ยวข้องกับการฝึกทหารใหม่ และบุคคลที่เป็นผู้บังคับบัญชาของทหารกองประจำการ หลังจากจบการฝึกทหารใหม่ หน่วยงานที่นำข้อมูลจากทุกแผนกมาทำการวิเคราะห์ เพื่อเสนอเป็นแนวทางในการติดตามรูปแบบการฝึกทหาร เพื่อรองรับภัยคุกคามรูปแบบใหม่ต่อไป สำหรับผลการวิจัยพบว่าภัยคุกคามรูปแบบใหม่ Cyber Attack นั้นมีผลกระทบต่อความมั่นคงของชาติอย่างร้ายแรง และกองทัพบกก็เป็นเป้าหมายการทำลายที่สำคัญ เนื่องจากเป็นเสาหลักของงานด้านความมั่นคงของชาติ สำหรับการฝึกทหารใหม่ในปัจจุบัน ยังคงเป็นการฝึกรูปแบบเดิมๆ มุ่งเน้นกำลังพลให้ปฏิบัติหน้าที่ต่างๆในหน่วยกำลังรบ และหน่วยอื่นๆ โดยไม่มีเนื้อหาการฝึกที่เกี่ยวข้องกับการต่อต้านภัยคุกคามรูปแบบใหม่แม้แต่น้อย ดังนั้นการบรรจุรายการฝึกที่เกี่ยวข้องกับการต่อต้านปฏิบัติการ Cyber Attack จึงมีความสำคัญและจำเป็นอย่างยิ่งสำหรับหลักสูตรทหารใหม่ เพื่อให้ทหารใหม่มีความรู้ความเข้าใจที่ถูกต้อง เกี่ยวกับการใช้เทคโนโลยี โดยเฉพาะอย่างยิ่งเครื่องมือติดต่อสื่อสารทั้งของบุคคล หรือของหน่วยงาน และมีจิตสำนึกในการต่อต้าน Cyber Attack และมีขีดความสามารถในการปฏิบัติงานกับเทคโนโลยีด้านความปลอดภัย ซึ่งจะต้องสนองนโยบายรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ของกองทัพบกและกระทรวงกลาโหมอย่างมีประสิทธิภาพ

ดังนั้นทุกๆหน่วยทหารจะต้องให้ความสำคัญในเรื่องการสร้างความรู้ ความเข้าใจและวินัยในการใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารให้กำลังพลในหน่วยอย่างจริงจัง ซึ่งแนวทางการเสริมสร้างความรู้อาจกระทำได้โดยการจัดการฝึกอบรมให้กำลังพลในโอกาสต่างๆ ซึ่งโดยปกติกองทัพบกมีระบบการฝึก - ศึกษา ที่ชัดเจนอยู่แล้วแต่เนื้อหาการฝึก - ศึกษารูปแบบปัจจุบันอาจไม่รองรับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack ซึ่งในงานวิจัยฉบับนี้จะเป็นการศึกษาวิจัยหาแนวทางในการพัฒนา การฝึกทหารของกองทัพบกให้สามารถรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack

โดยผู้วิจัยจะเริ่มต้นด้วยการเก็บข้อมูลทุติยภูมิ Secondary Data) โดยการทบทวนวรรณกรรมที่เกี่ยวข้องในเรื่อง เกี่ยวกับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack และจะทำการศึกษาหาข้อมูล และทำความเข้าใจเกี่ยวกับระบบการฝึก - ศึกษาของกองทัพบกไทย โดยมุ่งเน้นไปที่หลักสูตรการฝึกทหารใหม่ตลอดจนการศึกษางานวิจัยในอดีตที่เกี่ยวข้องกับเรื่องดังกล่าว หลังจากนั้นจะทำการเก็บข้อมูลปฐมภูมิ (Primary Data) โดยการทำการออกแบบสอบถาม (Questionnaire Survey) เพื่อเก็บข้อมูล หลังจากนั้นจะนำข้อมูลที่ได้ทั้งหมดมาทำการวิเคราะห์โดยละเอียด

จากการวิจัยพบว่าระบบการฝึก - ศึกษาของกองทัพบกในปัจจุบันยังไม่รองรับภัยคุกคามประเภทดังกล่าว เพราะระบบการฝึก - ศึกษาของกองทัพบกปัจจุบันยังคงมุ่งเน้นไปที่การรับมือภัยคุกคามรูปแบบเดิมๆ โดยใช้วิธีการปฏิบัติการทางทหาร ดังนั้นจึงสมควรอย่างยิ่งที่จะมีการพัฒนาระบบการฝึก – ศึกษา ทางทหารโดยเริ่มต้นการดำเนินการโดยหน่วยงานที่เกี่ยวข้องกับการฝึก – ศึกษาของกองทัพบกซึ่งคือกรมยุทธการทหารบกและ กรมยุทธศึกษาทหารบกจะต้องมีการดำเนินการวางแผนการกำหนดหลักสูตรการฝึกอบรมร่วมกับศูนย์ไซเบอร์กองทัพบก และดำเนินการฝึกอบรมอย่างเป็นขั้นเป็นตอน กองทัพบกควรทำคู่ขนานกันทั้งการบรรจุวิชาดังกล่าวในหลักสูตรการฝึกทหารใหม่ซึ่งจะอยู่ในวงรอบการฝึกประจำปี และให้ทุกหน่วยจัด Unit School ซึ่งเป็นการฝึกตามความริเริ่มของหน่วย โดยขั้นแรกวางแผน กำหนดขอบเขต ความมุ่งหมายของหลักสูตร กระทำร่วมกันระหว่างกรมยุทธการทหารบก ศูนย์ไซเบอร์กองทัพบก และกรมยุทธศึกษาทหารบก และเตรียมเปิดหลักสูตรและเตรียมบรรจุวิชา Cyber ในการฝึกทหารใหม่ จะเป็นหน้าที่ของกรมยุทธศึกษาทหารบก ดำเนินการเปิดหลักสูตร Cyber กระทำโดยกรมยุทธศึกษาทหารบก โดยหน่วยทหารในกองทัพบก ส่งกำลังพลมาเข้ารับการศึกษาเพื่อนำกลับไปเปิด Unit School และการฝึกทหารใหม่ที่มีวิชา Cyber บรรจุในหลักสูตรการฝึกจัดโดยหน่วย และประเมินผลโดยหน่วย/ยศ.ทบ.

ผู้วิจัยเชื่อว่าหากกองทัพบกมีการดำเนินการตามโครงร่าง (Frame Work) ตามที่ผู้วิจัยเสนอนี้ภายในระยะเวลา ๒ ปี กำลังพลในกองทัพบกจะมีความรู้ ความสามารถในเรื่องที่เกี่ยวกับเทคโนโลยีสารสนเทศ และการสื่อสาร สามารถปฏิบัติงานกับเทคโนโลยีของหน่วยงานของตนได้อย่างมีประสิทธิภาพ และมีความปลอดภัยรองรับนโยบายเกี่ยวกับด้านเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพบกและกระทรวงกลาโหมได้เป็นอย่างดี และมีภูมิต้านทานที่เข้มแข็งต่อภัยคุกคามรูปแบบใหม่ Cyber Attack ในยุคโลกไร้พรมแดน

คำนำ

ปัจจุบันเรากำลังอยู่ในยุคโลกไร้พรมแดน มนุษย์มีการใช้เทคโนโลยีสารสนเทศกันอย่างกว้างขวาง โดยมีวัตถุประสงค์ในการใช้งานที่แตกต่างกัน สามารถเข้าถึงแหล่งข้อมูลได้อย่างไม่มีขีดจำกัด และแสดงความคิดเห็น หรือเผยแพร่ข้อมูลสู่สาธารณะได้อย่างรวดเร็ว ตามสื่อสังคมออนไลน์ประเภทต่างๆ ซึ่งในแต่ละวันเราจะได้รับทราบข้อมูลข่าวสารในด้านต่างๆ ทั้งที่มีความสำคัญเป็นประโยชน์ รวมถึงข้อมูลที่ถูกบิดเบือน ที่ถูกปล่อยออกมาใส่ร้ายป้ายสี ทำลายล้างฝ่ายตรงข้ามเพื่อมุ่งผลประโยชน์อย่างใดอย่างหนึ่ง หลายๆ ครั้งเราจะพบว่าการโจมตีทางข้อมูลข่าวสาร Cyber Attack ไม่ใช่เพียงแต่มุ่งทำลายบุคคลเท่านั้น แต่ยังมีเป้าหมายทำลายล้างองค์กรสถาบัน ซึ่งกระทบกระเทือนต่อความมั่นคงของชาติเป็นอย่างมาก หน่วยงานด้านความมั่นคงของชาติทุกระดับ ตระหนักถึงภัยคุกคามดังกล่าว จึงได้ออกนโยบายมาตรการต่างๆ มาเพื่อรองรับภัยคุกคามรูปแบบนี้ แต่กระนั้นระดับการโจมตีทาง Cyber ก็มิได้ลดลงเลยในเวลาที่ผ่านมา ส่วนหนึ่งอาจเป็นเพราะบุคลากรที่เกี่ยวข้องกับงานด้านความมั่นคง ยังไม่มีความรู้ ความสามารถในการรับมือ ในส่วนของสถาบันทหาร ซึ่งนับว่าเป็นเสาหลักด้านความมั่นคงของชาติ กระทรวงกลาโหมเอง ก็มีการออกร่างแผนแม่บทในเรื่องดังกล่าว ทุกเหล่าทัพก็มีการจัดตั้งศูนย์ไซเบอร์ของเหล่าทัพเพื่อรองรับแผนของหน่วยเหนือ แต่งานมิได้จบแค่นั้น เพราะความสัมฤทธิ์ผลจะเกิดจากบุคลากร ถ้าองค์กรมีความรู้ความเข้าใจ มีจิตสำนึก และมีวินัย สามารถนำนโยบายของหน่วยเหนือมาสู่การปฏิบัติได้อย่างเป็นรูปธรรม สำหรับหน่วยงานกองทัพบก การที่จะทำอย่างนั้นได้ ต้องติดอาวุธทางปัญญา ให้กับกำลังพลในกองทัพ ซึ่งเมื่อเข้าไปพิจารณาเนื้อหาหลักสูตร พบว่าระบบการฝึก – ศึกษาของกองทัพบกในปัจจุบัน ไม่รองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ส่วนใหญ่มุ่งเน้นการรองรับภัยคุกคามรูปแบบเดิม แต่ระบบการฝึก - ศึกษาของกองทัพบกนั้น มีความอ่อนตัวมีการเปิดช่องว่างให้สามารถเพิ่มเติมหลักสูตรที่สำคัญเพื่อบรรจุเข้าไปได้ ในการวิจัยครั้งนี้ เป็นการค้นหาแนวทางในการพัฒนารูปแบบการฝึกทหารให้รองรับภัยคุกคามรูปแบบใหม่ ภัยคุกคามด้านไซเบอร์ เพื่อให้บุคลากรในกองทัพบกมีความรู้ ความสามารถเพียงพอที่จะปฏิบัติงานกับเทคโนโลยีใหม่ๆ สามารถตอบสนองนโยบายของหน่วยเหนือได้อย่างมีประสิทธิภาพ และกองทัพบกก็จะมีภูมิต้านทานที่แข็งแรงต่อภัยคุกคามรูปแบบใหม่ Cyber Attack ในยุคโลกไร้พรมแดน

พลตรี

(ศตวรรษ รามดิษฐ์)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๕๙
ผู้วิจัย

สารบัญ

	หน้า
บทคัดย่อ	**ก**
คำนำ	**ค**
กิตติกรรมประกาศ	**ง**
สารบัญ	**จ**
สารบัญแผนภาพ	**ช**
บทที่ ๑ บทนำ	**๑**
ความเป็นมาและความสำคัญของปัญหา	๑
วัตถุประสงค์ของการวิจัย	๒
ขอบเขตของการวิจัย	๒
วิธีดำเนินการวิจัย	๓
ประโยชน์ที่ได้รับจากการวิจัย	๓
คำจำกัดความ	๓
บทที่ ๒ การทบทวนวรรณกรรมที่เกี่ยวข้อง	**๗**
ภัยคุกคามรูปแบบใหม่ Cyber Attack	๗
แนวคิดเกี่ยวกับภัยคุกคาม Cyber Attack	๑๔
สถานการณ์และแนวโน้มความรุนแรงจาก Cyber Attack	๑๖
ผลกระทบของ Cyber Attack ต่อความมั่นคงของชาติ	๑๗
นโยบายในการเตรียมการรับมือ Cyber Attack ในปัจจุบัน	๑๙
ระบบการฝึกทหารใหม่ของกองทัพบกไทย	๒๒
เอกสารวิจัยที่เกี่ยวข้อง	๓๑
กรอบแนวคิดในการวิจัย	๓๖
สรุป	๓๗
บทที่ ๓ วิธีดำเนินการวิจัย	**๓๘**
วิธีดำเนินการวิจัย	๓๘
สรุป	๓๙

สารบัญ (ต่อ)

	หน้า
บทที่ ๔ แนวทางในการพัฒนาการฝึกทหาร	
เพื่อรองรับภัยคุกคามรูปแบบใหม่: ภัยคุกคามไซเบอร์	**๔๐**
การวิเคราะห์ข้อมูลทุติยภูมิ (Secondary Data Analysis)	๔๐
การวิเคราะห์ข้อมูลปฐมภูมิ (Primary Data Analysis)	๔๒
สรุป	๔๗
บทที่ ๕ สรุปและข้อเสนอแนะ	**๔๘**
สรุป	๔๘
ข้อเสนอแนะ	๔๙
บรรณานุกรม	**๕๒**
ภาคผนวก	**๕๔**
ผนวก ก ตัวอย่างแบบสอบถาม	๕๕
ผนวก ข ตัวอย่างแบบสัมภาษณ์	๕๘
ประวัติย่อผู้วิจัย	**๖๐**

สารบัญแผนภาพ

หน้า

แผนภาพที่

๒ - ๑ กรอบแนวคิดในการวิจัย ๓๖

๕ - ๑ โครงร่าง : แนวทางในการพัฒนาการฝึกทหารให้รองรับ
ภัยคุกคามรูปแบบใหม่ : Cyber Attack ๕๐

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเทคโนโลยีสารสนเทศ ได้เข้ามามีบทบาทและมีความสำคัญต่อการดำเนินชีวิตประจำวันของมนุษย์เป็นอย่างมาก จะเห็นได้ว่าแทบจะทุกคนเกี่ยวข้องกับโทรศัพท์มือถือและมีการใช้งานเครือข่ายสังคมออนไลน์อย่างแพร่หลาย ทั้งในด้านการติดต่อสื่อสาร การส่งข้อมูล การสืบค้นข้อมูลด้านต่างๆอย่างไม่มีขีดจำกัด ซึ่งสามารถกล่าวได้ว่าปัจจุบันเรากำลังอยู่ในยุคของโลกไร้พรมแดน

เทคโนโลยีสารสนเทศนั้น หากถูกนำมาใช้ในกิจกรรมเชิงสร้างสรรค์ ก็จะเป็นประโยชน์ต่อผู้ใช้และหน่วยงานอย่างมหาศาลแต่หากนำมาใช้ในทางที่ผิด เช่น นำมาเป็นเครื่องมือในการทำลายล้างฝ่ายตรงข้ามก็นับว่าเป็นภัยคุกคามรูปแบบใหม่ที่มีความร้ายแรงต่อมวลมนุษยชาติเช่นเดียวกัน

การโจมตีทางไซเบอร์ (Cyber Attack) ถือเป็นภัยคุกคามรูปแบบใหม่ซึ่งผู้ก่อการร้ายมุ่งกระทำต่อระบบเครือข่ายโทรคมนาคมและคอมพิวเตอร์ ด้วยวิธีการต่างๆ ที่หลากหลายโดยมุ่งไปสู่การทำลายล้างองค์กรของฝ่ายตรงข้าม ซึ่งโดยทั่วไปแล้วการโจมตีทางไซเบอร์ถูกแบ่งออกเป็น ๓ ลักษณะใหญ่ๆ ดังนี้

๑. การนำความลับขององค์กรออกมาเปิดเผย (Data Confidentiality)

๒. การเปลี่ยนแปลง/บิดเบือนข้อมูล (Data Integrity)

๓. การทำให้ระบบปฏิบัติการในเครือข่ายคอมพิวเตอร์หยุดให้บริการหรือไม่สามารถใช้งานได้ (System Availability)

ประเทศไทยเองก็ไม่แตกต่างจากประเทศอื่นๆทั่วโลก ที่มีโอกาสเป็นเป้าหมายในการโจมตีของอาชญากรทางไซเบอร์ โดยมีเหตุผลการโจมตีที่หลากหลาย และจากกลุ่มการโจมตีที่หลากหลาย ซึ่งล้วนแล้วแต่กระทบกระเทือนความมั่นคงของชาติเป็นอย่างมาก หน่วยงานที่เกี่ยวข้องกับความมั่นคงของประเทศทุกระดับต่างตระหนักถึงผลกระทบของภัยคุกคามดังกล่าวและมีการกำหนดมาตรการเพื่อรับมือจากการโจมตีรูปแบบนี้

สภาความมั่นคงแห่งชาติได้กำหนดเรื่องการเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ ในนโยบายความมั่นคงของชาติ พ.ศ.๒๕๕๘ - ๒๕๖๔ กระทรวงกลาโหมได้จัดทำร่างแผนแม่บทไซเบอร์เพื่อป้องกันประเทศกระทรวงกลาโหมปี พ.ศ.๒๕๖๐ – ๒๕๖๔ และในแต่ละเหล่าทัพได้จัดตั้งศูนย์ไซเบอร์เหล่าทัพ เพื่อปฏิบัติการแจ้งเตือน ป้องกัน และแก้ปัญหาภัยคุกคามด้านไซเบอร์

แม้มีการขับเคลื่อนในระดับนโยบายเพื่อรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ก็ตามก็ยังปรากฏข่าวสารตามสื่อต่างๆ ซึ่งเป็นข้อมูลในด้านลบ และทำลายความเชื่อมั่นและศรัทธาของสถาบันทหารซึ่งเป็นเสาหลักของความมั่นคงอยู่เสมอ ไม่ว่าจะเป็นการที่มีภาพหรือคลิปวีดีโอกิจกรรมที่ไม่เหมาะสมถูกเผยแพร่สู่สาธารณะ มีการนำความลับทางราชการที่เกี่ยวกับระบบการจัดซื้อยุทโธปกรณ์ทางทหารออกมาเผยแพร่สู่สาธารณะอย่างบิดเบือน ทำให้ประชาชนบางส่วนเชื่อว่ามีการทุจริตในระบบการจัดซื้อของทางราชการ มีการเผยแพร่แนวความคิดที่หมิ่นสถาบันเบื้องสูง มีการเผยแพร่ข้อมูลที่เป็นลบต่อรัฐบาลและกองทัพ และการสร้างความแตกแยกของคนในชาติ โดยใช้เครื่องมือเทคโนโลยีสารสนเทศ และการสื่อสารรวมทั้งสื่อสังคมออนไลน์ ทั้งหมดนี้ได้นำความเสียหายมาสู่รัฐบาลและกองทัพเป็นอย่างมาก ตลอดจนการดำเนินการจับกุมผู้กระทำผิดมาดำเนินคดีนั้นเป็นเรื่องที่ยากมาก

ดังนั้นการที่จะสนับสนุนให้การขับเคลื่อนทางนโยบายของหน่วยระดับกองทัพและกระทรวงกลาโหม มีประสิทธิภาพนั้น ทุกๆหน่วยทหารจะต้องให้ความสำคัญในเรื่องการสร้างความรู้ความเข้าใจ และวินัยในการใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารให้กำลังพลในหน่วยอย่างจริงจัง ซึ่งแนวทางการเสริมสร้างความรู้อาจกระทำได้โดยการจัดการฝึกอบรมให้กำลังพลในโอกาสต่างๆ ซึ่งโดยปกติกองทัพบกมีระบบการฝึก-ศึกษาที่ชัดเจนอยู่แล้ว แต่เนื้อหาการฝึก - ศึกษา รูปแบบในปัจจุบันอาจไม่รองรับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack ซึ่งในงานวิจัยฉบับนี้จะเป็นการศึกษาวิจัยหาแนวทางในการพัฒนาการฝึกทหารของกองทัพบก ให้สามารถรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ซึ่งนับเป็นก้าวสำคัญในการปรับตัวให้สามารถเผชิญกับภัยคุกคามรูปแบบใหม่ในยุคโลกไร้พรมแดนได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ของการวิจัย

๑. เพื่อทำการศึกษาหาข้อมูลภัยคุกคามรูปแบบใหม่ Cyber Attack ซึ่งมีผลกระทบด้านความมั่นคงของชาติ

๒. เพื่อทำการศึกษาระบบการฝึก - ศึกษาของกองทัพบกไทยในปัจจุบัน

๓. เพื่อทำการเสนอแนวความคิดในการสร้างการรับรู้และจิตสำนึกของบุคลากรในกองทัพบกในการใช้เทคโนโลยีสารสนเทศ และการสื่อสารอย่างเหมาะสม และปลอดภัยต่อ Cyber Attack โดยการจัดหลักสูตรการฝึกอบรมเพิ่มเติมจากการฝึก - ศึกษาปกติของหน่วยทหารในกองทัพบก

ขอบเขตของการวิจัย

๑. จะทำการวิจัยภัยคุกคามรูปแบบใหม่ ในเรื่อง Cyber Attack เท่านั้น

๒. การศึกษาผลกระทบของภัยคุกคามรูปแบบใหม่จะศึกษาเฉพาะกรณีความมั่นคงเท่านั้น

๓. จะทำการศึกษาระบบการฝึก - ศึกษาของกองทัพบกไทยเท่านั้น

วิธีดำเนินการวิจัย

ในการวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ ผู้วิจัยจะเริ่มต้นด้วยการเก็บข้อมูลทุติยภูมิ (Secondary Data) โดยการทบทวนวรรณกรรมที่เกี่ยวข้อง ในเรื่องเกี่ยวกับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack และจะทำการศึกษาหาข้อมูล และทำความเข้าใจเกี่ยวกับระบบการฝึก - ศึกษาของกองทัพบกไทย โดยมุ่งเน้นไปที่หลักสูตรการฝึกทหารใหม่ ตลอดจนการศึกษางานวิจัยในอดีตที่เกี่ยวข้องกับเรื่องดังกล่าว

หลังจากนั้นจะทำการเก็บข้อมูลปฐมภูมิ (Primary Data) โดยการทำการออกแบบสอบถาม (Questionnaire Survey) เพื่อเก็บข้อมูลจากผู้บังคับหน่วย ฝ่ายเสนาธิการ และครูฝึกทหารใหม่ในพื้นที่จังหวัดปราจีนบุรี จำนวน ๔๐ ชุด และได้ทำการสัมภาษณ์ พันเอก มหิธร บุญครอง หัวหน้ากองยุทธการมณฑลทหารบกที่ ๑๒ ซึ่งมีหน้าที่โดยตรงในการวางแผน อำนวยการ และกำกับดูแลระบบการฝึกและการใช้กำลังของหน่วยให้เป็นไปตามนโยบายของกองทัพบก

หลังจากนั้นจะนำข้อมูลที่ได้ทั้งหมดมาทำการวิเคราะห์โดยละเอียด และทำการสรุปผลการวิจัยและนำเสนอข้อเสนอแนะในบทสุดท้ายของงานวิจัยต่อไป

ประโยชน์ที่ได้รับจากการวิจัย

๑. ได้เข้าใจรูปแบบภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack และผลกระทบต่อความมั่นคงของชาติ

๒. ได้เข้าใจระบบการฝึก-ศึกษาของกองทัพบกไทยในปัจจุบัน

๓. ได้แนวความคิดในการพัฒนาระบบการฝึกทหาร ของกองทัพบกไทยให้สามารถรองรับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack

คำจำกัดความ

ภัยคุกคามรูปแบบใหม่ (Cyber Attack)

หมายถึง การโจมตีจุดสำคัญที่เป็นหัวใจของชาติผ่านระบบเครือข่ายโทรคมนาคมและคอมพิวเตอร์ โดยมีปฏิบัติการใน ๓ ลักษณะ คือ นำความลับไปเปิดเผย การบิดเบือนข้อมูล และการทำลายระบบปฏิบัติการในคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ (Computer Crime)

หมายถึง การกระทำผิดกฎหมายโดยวิธีการทางอิเล็กทรอนิกส์เพื่อโจมตีระบบคอมพิวเตอร์ และข้อมูลในระบบ

ความมั่นคงของชาติ (National Security)

หมายถึง ความต้องการมีเสรีภาพ มีอำนาจอธิปไตยเหนือดินแดนของตน มีอิสระต่อแรงกดดันต่างๆ มีความมั่นคงปลอดภัยและมีความผาสุกสมบูรณ์

การปฏิบัติการข่าวสาร (Information Operation: IO)

หมายถึง การปฏิบัติการจิตวิทยา การโฆษณาชวนเชื่อ การวิเทศสัมพันธ์ทางสื่อมวลชน และการลวงทางทหาร

ระบบโครงสร้างพื้นฐาน (Infrastructure)

หมายถึง โครงสร้างทางกายภาพ และโครงสร้างหลักขององค์กรเพื่อตอบสนองความจำเป็นในกิจกรรมต่างๆ ขององค์กร

การฝึกทหารใหม่ (New Military Training)

หมายถึง การฝึกบุคคลพลเรือนที่ได้รับการตรวจคัดเลือกมาเป็นทหารกองประจำการของกองทัพ จะเป็นการปรับสภาพจากพลเรือนมาเป็นทหารทั้งร่างกายและจิตใจ โดยจะมีการอบรมแบบธรรมเนียมทหารและฝึกวิชาทหารขั้นพื้นฐาน รวมทั้งฝึกยุทธวิธี ระยะเวลาการฝึก คือ ๑๐ สัปดาห์ ต่อ ๑ รุ่น ปีหนึ่งจะทำการฝึกด้วยกัน ๒ รุ่น

ทหารกองประจำการ (Military Service)

หมายถึง ผู้ที่ได้ขึ้นทะเบียนกองประจำการ และได้เข้ารับราชการในกรมกองต่างๆ ในกองทัพจนกว่าจะได้ปลดประจำการ

นายทหารชั้นสัญญาบัตร (Commissioned Officer)

หมายถึง บุคคลที่ประกอบอาชีพทหารและมีชั้นยศตั้งแต่ร้อยตรีขึ้นไป

นายทหารชั้นประทวน (Non - commissioned Officer)

หมายถึง บุคคลที่ประกอบอาชีพทหารและมีชั้นยศตั้งแต่สิบตรี - จ่าสิบเอก

กรมยุทธศึกษาทหารบก (Army Training Command)

หมายถึง หน่วยงานระดับกรมของกองทัพบกที่มีหน้าที่หลักในการวางแผน อำนวยการ กำหนดแนวทางและกำกับดูแลการฝึก-ศึกษาของหน่วยทหารต่างๆ ในกองทัพบกให้เป็นไปตามนโยบายการฝึกประจำปีของกองทัพบก

Unit School หมายถึง การจัดการฝึกการอบรมขึ้นเองภายในหน่วย ไม่ใช้งบประมาณกองทัพบก จะเน้นในการเพิ่มขีดความสามารถของกำลังพลของหน่วยนั้นๆ ในการปฏิบัติหน้าที่เฉพาะ

กรมยุทธการทหารบก (Directorate of Operations)

หมายถึง หน่วยงานในกองทัพบก ระดับกรมฝ่ายเสนาธิการที่มีหน้าที่วางแผน อำนวยการด้านยุทธศาสตร์ยุทธการ การใช้กำลังทหาร ในเรื่องที่ได้รับมอบตลอดจนวางแผนและอำนวยการในการจัดการฝึกศึกษาเฉพาะเรื่องที่เป็นนโยบายสำคัญของกองทัพบก

การฝึกทางยุทธวิธี (Tactical Training)

หมายถึง การฝึกที่เกี่ยวข้องกับการใช้กำลังทางทหารในการปฏิบัติการรบในระดับกำลังต่างๆ ซึ่งจะถูกบรรจุอยู่ในวงรอบการฝึกประจำปีของกองทัพบก

การฝึกทหารใหม่เฉพาะหน้าที่ (New Military Training)

หมายถึง การฝึกที่จัดขึ้นหลังจากทหารใหม่จบการฝึกทหารใหม่ มีความมุ่งหมายเพื่อฝึกงานเฉพาะหน้าที่ให้ทหารได้มีขีดความสามารถจะปฏิบัติงานได้ตามตำแหน่งที่บรรจุ เมื่อเข้าประจำการในหน่วยต้นสังกัด

วงรอบการฝึกประจำปี (Annual Training Cycle)

หมายถึง การนำการฝึกต่างๆ มากำหนดลงในห้วงเวลาในปีงบประมาณตั้งแต่ เดือน ต.ค. - เดือน ก.ย. ของปีถัดไป โดยกำหนดเป็นห้วงๆ ว่าห้วงเวลาแต่ละห้วงหน่วยต้องทำการฝึกอะไรบ้าง

การฝึกพิเศษ (Special Training)	หมายถึง	การฝึกอื่นๆที่อยู่นอกเหนือการฝึกตามวงรอบประจำปี ซึ่งอาจเป็นการฝึกในเรื่องที่สำคัญตามนโยบายผู้บังคับบัญชา เช่น การฝึกหน่วยทหารขนาดเล็ก การฝึกหน่วยทหารทรหด ฯลฯ

บทที่ ๒
การทบทวนวรรณกรรมที่เกี่ยวข้อง

ภัยคุกคามรูปแบบใหม่ Cyber Attack

ภัยคุกคามรูปแบบใหม่ได้เริ่มขึ้นหลังจากการยุติลงของยุคสงครามเย็น (Cold War) ซึ่งเป็นสงครามแห่งการสร้างแสนยานุภาพทางการทหารของประเทศมหาอำนาจ เมื่อสงครามเย็นยุติลงถือว่าเป็นการสิ้นสุดของการแข่งขันในด้านการสะสมอาวุธ เทคโนโลยีอวกาศ การจารกรรม และการแข่งขันกันทางเศรษฐกิจของทั้งสองฝ่าย คือ ฝ่ายตะวันออกซึ่งปกครองด้วยระบอบคอมมิวนิสต์ และฝ่ายตะวันตกซึ่งปกครองด้วยระบอบเสรีประชาธิปไตย ทำให้หลังยุคสงครามเย็นเป็นยุคแห่งการเปลี่ยนแปลงและการเกิดภัยคุกคามรูปแบบใหม่ที่ไม่ใช่การใช้กำลังทหาร และอาวุธเหมือนในอดีต เช่น ปัญหาสิ่งแวดล้อม ปัญหาสารพิษ ปัญหาอาชญากรรมข้ามชาติ ปัญหาวิกฤตด้านพลังงาน ปัญหาวิกฤตน้ำหรือภัยธรรมชาติ เป็นต้น (สิงห์ทอง หมีทอง, ๒๕๕๗: ๑ - ๓)

การเปลี่ยนแปลงในยุคโลกาภิวัตน์เป็นปัจจัยหลักที่ทำให้ปัญหาภัยคุกคามซึ่งเกิดจากมนุษย์ มีการพัฒนารูปแบบไปอย่างซับซ้อน และสามารถก่อขยายตัวลุกลามไปได้อย่างรวดเร็ว ด้วยการใช้ประโยชน์จากความก้าวหน้าทางวิทยาศาสตร์และเทคโนโลยี การเชื่อมต่อของคอมพิวเตอร์ และอุปกรณ์อื่น ๆ ที่สามารถสื่อสารผ่านระบบเครือข่ายได้ด้วยอินเทอร์เน็ตโปรโตคอล เพื่อส่งข้อมูลระหว่างกันจำนวนมาก ลักษณะของการเคลื่อนที่ของข้อมูลและข่าวสารจากที่หนึ่งไปยังอีกที่หนึ่งได้อย่างรวดเร็วจนเกือบเป็นเวลาเดียวกัน (Near Real Time) ทุกสถานที่ ทุกเวลา (Any Where Any Time) ไร้ขอบเขตจำกัด (Borderless) และมีความเสมือนจริง (Virtualization) ในทศวรรษที่ผ่านมาประเทศไทยได้เผชิญกับปัญหา และผลกระทบจากภัยคุกคามที่เกิดขึ้นใหม่เป็นจำนวนมาก ในขณะที่เจ้าหน้าที่ฝ่ายความมั่นคงของรัฐคงมีสถานภาพและการจัดองค์กรในรูปแบบเดิม และยังขาดการพัฒนาขีดความสามารถของบุคลากรที่เป็นมาตรฐานเพื่อรองรับภัยคุกคามที่เกิดขึ้นจริงในปัจจุบัน (ณฐพนธ์ ศรีสวัสดิ์, ๒๕๕๗: ๗๗) ภัยคุกคามที่ภาครัฐเผชิญอยู่ในปัจจุบัน อาทิเช่น ปัญหาความไม่สงบในพื้นที่ ๓ จังหวัดชายแดนภาคใต้ ปัญหาการเมืองภายในประเทศ ปัญหาทางเศรษฐกิจ ปัญหาด้านสังคมจิตวิทยา ปัญหาด้านการต่างประเทศ ปัญหากลุ่มขบวนการ “รัฐอิสลาม (Islamic - State: IS) ปัญหาภัยคุกคามและผลกระทบด้านความมั่นคงจากการเข้าร่วมประชาคมอาเซียน เป็นต้น ดังนั้นภาครัฐจึงต้องเตรียมพร้อมเพื่อรับมือกับปัญหาภัยคุกคามต่าง ๆ อยู่ตลอดเวลา

ณฐพนธ์ ศรีสวัสดิ์ (๒๕๕๘: ๔๙-๕๓) ได้ประเมินลักษณะปัญหาภัยคุกคามรูปแบบใหม่ๆ ที่เกิดขึ้นซึ่งมีผลต่อความมั่นคงของรัฐ ได้แก่ ภัยจากการก่อการร้ายและการก่อเหตุรุนแรง ภัยจากยาเสพติด ภัยจากการบุกรุกและทำลายทรัพยากรทางธรรมชาติ ภัยจากสื่อทางสังคม และปัญหาความรุนแรงในพื้นที่จังหวัดชายแดนภาคใต้ ดังนี้

๑. ภัยจากการก่อการร้ายและการก่อเหตุรุนแรง ถึงแม้ว่าประเทศไทยไม่ใช่จุดกำเนิดและเกี่ยวพันกับความขัดแย้งของกลุ่มอิทธิพลทางศาสนาหรือชาติพันธุ์ใด ๆ แต่ด้วยการเป็นศูนย์กลางทางการคมนาคม และการเปลี่ยนผ่านการเดินทางได้ทุกประเภท จึงมีความเสี่ยงที่เกิดภัยของการก่อการร้าย เนื่องจากวัตถุประสงค์หลักของการก่อการร้ายนั้นคือความต้องการสร้างการรับรู้ที่กว้างขวาง รวดเร็ว และมีผลกระทบต่อความรู้สึกนึกคิดของผู้คนอย่างรุนแรง ดังนั้น พื้นที่ที่มีประชากรอาศัยอยู่หนาแน่น จึงเป็นจุดหมายในการลงมือ สำหรับประเทศไทยที่เห็นได้ชัดด้านการก่อการร้าย และการก่อเหตุรุนแรง คือ ในพื้นที่ ๓ จังหวัดชายแดนภาคใต้ ซึ่งยังมีการก่อเหตุอยู่เป็นระยะ นอกจากนั้นในกรุงเทพมหานครซึ่งเป็นเมืองหลวงและเป็นแหล่งเศรษฐกิจที่สำคัญของประเทศ เช่น การวางระเบิดศาลพระพรหมที่ใจกลางกรุงเทพมหานคร เป็นต้น ซึ่งอาจถูกใช้เป็นประเด็นขยายความรุนแรงหรือใช้เป็นแหล่งเชื่อมโยง ซ่อนเร้นของขบวนการต่าง ๆ ได้เป็นอย่างดี ดังนั้น ระบบงานข่าวกรองของภาครัฐ จึงต้องมีการปรับปรุงและพัฒนา โดยต้องมีการลงทุน และระดมขีดความสามารถด้านเทคโนโลยี การเฝ้าระวัง ตรวจสอบ โดยเพิ่มมาตรฐานการตรวจคัดกรองบุคคลต้องสงสัยอย่างเข้มงวด

๒. ภัยจากยาเสพติด การแพร่ระบาดของยาเสพติดมีวงจรและกระบวนการพื้นฐานที่เชื่อมโยงระหว่างแหล่งผลิต ซึ่งส่วนใหญ่ตั้งอยู่ในประเทศเพื่อนบ้าน จากนั้นจะมีขบวนการลักลอบลำเลียงนำเข้ามาในพื้นที่ชายแดนภาคเหนือ และภาคตะวันออกเฉียงเหนือ แล้วแทรกซึมส่งต่อไปยังลูกค้ารายย่อย ๆ ไปจนถึงตัวผู้เสพ ซึ่งขบวนการค้ายาเสพติดในส่วนของการลำเลียงขนส่ง และการกระจายยาเสพติด ได้มีการปรับเปลี่ยนแผนและวิธีการอยู่ตลอดเวลาเพื่อหลบหนีการตรวจสอบจากเจ้าหน้าที่ภาครัฐ ทั้งนี้การแก้ไขปัญหายังคนเน้นนโยบายการดำเนินงานแบบบูรณาการ โดยการจัดตั้งศูนย์อำนวยการพลังแผ่นดินเอาชนะยาเสพติดระดับชาติ และดำเนินงานตามแผนยุทธศาสตร์พลังแผ่นดินเอาชนะยาเสพติด โดยในระบบการป้องกันและปราบปราม มีการจัดตั้งหน่วยรับผิดชอบในกลุ่มพื้นที่ชายแดนและตอนใน ควบคู่ไปกับการดำเนินกิจกรรมสร้างภูมิคุ้มกันอันได้แก่ การจัดตั้งหมู่บ้าน/ ชุมชนเข้มแข็ง และสร้างเครือข่ายมวลชนในการรณรงค์แจ้งเตือนข่าวสารกับทางราชการ

๓. ภัยจากการบุกรุกและทำลายทรัพยากรทางธรรมชาติ ประเทศไทยประสบปัญหาการบุกรุก และทำลายป่าอย่างต่อเนื่อง พื้นที่ป่าในประเทศลดลงตามลำดับ พื้นที่ชายฝั่ง และเกาะแก่งต่างๆ ถูกแปรสภาพเป็นแหล่งที่พักอาศัย และสถานที่ท่องเที่ยวในรูปแบบต่าง ๆ ซึ่งเป็นการขยายตัวอย่างไร้ทิศทาง เมื่อมีแหล่งที่พักอาศัยและสถานที่ท่องเที่ยวย่อมเกิดความต้องการระบบสาธารณูปโภครองรับปัญหาขยะและน้ำเสีย รวมไปถึงมลภาวะทางเสียงและทางอากาศ สะท้อนให้เห็นถึงการวางแผนการจัดการ การใช้ทรัพยากรของชาติที่ล้มเหลวของภาครัฐ ซึ่งปัญหาที่เกิดขึ้นมีทั้งการบังคับใช้กฎหมายไม่ได้ผล เนื่องจาก

มีผู้ละเมิดฝ่าฝืนหรือไม่ได้บังคับใช้เพราะผู้ที่มีอำนาจออกเอกสารสิทธิ์มีหลายฝ่าย และต่างก็ถือกฎหมายกันคนละฉบับจนไม่สามารถเชื่อมโยงความถูกต้องได้ อย่างไรก็ตามการแก้ปัญหาในทุกมิติ คงตกเป็นวาระที่จะต้องใช้กฎหมายพิเศษ เช่น มาตรา ๔๔ เข้าดำเนินการซึ่งชี้ให้เห็นแล้วว่า กระบวนการแก้ปัญหาในเรื่องนี้เป็นเรื่องที่ซับซ้อนและเกี่ยวเนื่องไปยังหน้าที่ความรับผิดชอบของหลายกระทรวง

๔. ภัยจากสื่อทางสังคม ในทศวรรษที่ผ่านมา เป็นช่วงที่ประเทศไทยประสบปัญหาวิกฤตทางการเมือง คนไทยมีความตื่นตัวทางการเมืองเพิ่มมากขึ้น การมีส่วนร่วมในการรับรู้ข้อมูลข่าวสาร รวมถึงความสามารถในการแพร่กระจายข้อมูลข่าวสาร ความคิดเห็นของตนในสังคมออนไลน์กันอย่างเสรี ถึงแม้จะมีกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ออกมาควบคุมก็ตาม ประชาชนก็ยังมีการใช้ช่องทางในสังคมออนไลน์ในการแสวงหาคำตอบ แสดงความคิดเห็นให้บุคคลอื่นคล้อยตาม ระบายอารมณ์ หรือการนัดหมายรวมตัวกันเพื่อแสดงสัญลักษณ์ทางการเมืองต่าง ๆ บางกลุ่มได้ใช้ช่องทางออนไลน์ในการกดดันในรูปแบบต่าง ๆ ส่งผลให้เกิดการแบ่งแยกทางความคิดของคนในชาติ ซึ่งถือเป็นภัยคุกคามที่ภาครัฐไม่สามารถควบคุมได้

๕. ปัญหาความรุนแรงในพื้นที่จังหวัดชายแดนภาคใต้ นับตั้งแต่เกิดเหตุการณ์ปล้นอาวุธของทางราชการที่จังหวัดนราธิวาส เมื่อปี พ.ศ.๒๕๔๗ และปรากฏเป็นสถานการณ์ก่อเหตุรุนแรงลุกลามมาจนถึงปัจจุบัน สถิติการเกิดเหตุการณ์รุนแรงได้ปรับตัวลงตามลำดับ โดยในปี ๒๕๕๖-๒๕๕๗ ความรุนแรงที่เกิดขึ้นส่วนใหญ่ เป็นการตอบโต้เจ้าหน้าที่ภายหลังที่มีการจับกุมหรือวิสามัญฆาตกรรมระดับแกนนำคนสำคัญ อย่างไรก็ตามพบว่าแนวทางการต่อสู้ของกลุ่มผู้ก่อความรุนแรง ยังคงรักษาน้ำหนัก และทิศทางไปสู่ประเด็นการเรียกร้องเรื่องเอกราช ด้วยวิธีการปลุกระดมให้คนไทยมุสลิมเข้าร่วมญีฮาด ควบคู่ไปกับการสร้างข่าว สร้างประเด็น การถูกกดขี่ และละเมิดสิทธิมนุษยชน การถูกลิดรอนสิทธิและเสรีภาพจากกฎหมายความมั่นคงหลายฉบับในพื้นที่ ทั้งนี้ ยังดำรงความพยายามที่จะแสวงหาโอกาสในการเชื่อมโยงสถานการณ์ความรุนแรงในจังหวัดชายแดนภาคใต้ให้เป็นที่รับรู้ของเวทีมุสลิมโลก และขบวนการรัฐอิสลาม รวมไปถึงการแสดงพฤติกรรมต่อต้าน การพูดคุยด้วยสันติวิธีต่าง ๆ ซึ่งหน่วยงานด้านความมั่นคงและหน่วยงานการพัฒนายังขาดการบูรณาการ และขาดความมีเอกภาพทางความคิดของข้าราชการทุกระดับความต่อเนื่องในแผนการทำงานยังไม่ชัดเจน และโดยเฉพาะอย่างยิ่งการแก้ปัญหาในจังหวัดชายแดนภาคใต้ต้องใช้เวลานานมาก แต่ก็ยังไม่สามารถจำกัดหรือกำหนดเงื่อนไขที่เป็นตัวการหล่อเลี้ยงและสร้างการเจริญเติบโต หรือเป็นตัวเร่งการขยายตัวของกลุ่มขบวนการฯ อย่างได้ผล ซึ่งสิ่งที่สะท้อนให้เห็นถึงการไม่ประสบผลสำเร็จในเรื่องดังกล่าว คือการที่คนไทยมีความเชื่อฝังใจว่า จังหวัดชายแดนภาคใต้เป็นดินแดนอันตราย ใครก็ตามอยู่อาศัยหรือลงไปทำงานจะมีความเสี่ยงภัยต่ออันตราย เพราะไม่มีอะไรที่ไว้วางใจได้ และถ้าเลือกได้จะไม่ไปจังหวัดชายแดนภาคใต้แน่นอน เป็นต้น

ในวงการทหารถือว่าภัยคุกคามทางด้านไซเบอร์ (Cyber Threats) เป็นภัยที่คุกคามที่กระทบต่อความมั่นคงของชาติซึ่งเชื่อมโยงไปสู่ด้านต่าง ๆ การกระทำทั้งหมดนั้นเป็นภัยที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในทางที่ผิดกฎหมาย รวมทั้งการละเมิดต่อศีลธรรมและความสงบสุขของสังคม เป็นภัยร้ายแรงอีกรูปแบบหนึ่งในด้านการทหาร ซึ่งภัยคุกคามทางด้านไซเบอร์มีหลายรูปแบบดังนี้

๑. การโจมตีด้วยวิธีเจาะระบบ (Hacking) เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมแฮกหลากหลายรูปแบบที่สามารถดาวน์โหลดโปรแกรมแฮกมาใช้ได้ง่ายในโลกอินเทอร์เน็ต ไม่ต้องเป็นผู้เชี่ยวชาญก็สามารถเจาะระบบได้ ผู้ใช้งานอินเทอร์เน็ตจะต้องเฝ้าระวังและป้องกันตนเองให้ปลอดภัย แฮกเกอร์นั้นมีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการท้าทายโดยการเจาะระบบให้สำเร็จหรือมีจุดประสงค์เพื่อต้องการทำลายระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือ ระบบสารสนเทศเท่านั้น

๒. การโจมตีโดยทำการฝังโปรมแกรมลับลอบโจรกรรมข้อมูล คือ การใช้สปายแวร์ (Spyware) หรือประตูหลัง (Back Door) ระบบคอมพิวเตอร์มีระบบรักษาความมั่นคงแต่ยังมีรูรั่วหรือช่องโหว่ของระบบรักษาความมั่นคงที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว้โดยเป็นกลไกลับทางซอฟต์แวร์หรือฮาดแวร์จึงทำให้ผู้ไม่ประสงค์ดีสามารถใช้ช่องโหว่นี้ผ่านระบบรักษาความมั่นคงเข้ามาในระบบ และสร้างความเสียหายต่อระบบคอมพิวเตอร์ได้

๓. การโจมตีด้วยโปรแกรมมัลแวร์ (Malware) หมายถึงซอฟแวร์ที่เขียนขึ้นที่มีวัตถุประสงค์ในทางร้ายหรือเป็นภัยคุกคามต่อระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ให้ไปทำความเสียหายต่อคอมพิวเตอร์ที่เจ้าของหรือผู้ใช้ไม่ได้อนุญาต โปรแกรมมัลแวร์จะส่งผลให้คอมพิวเตอร์เสียหาย คือ สูญเสียความลับทางข้อมูล สูญเสียข้อมูลที่ถูกเปลี่ยนแปลงแก้ไขโดยเฉพาะส่วนสำคัญที่เกี่ยวโยงกับระบบภายในระบบปฏิบัติการ และสูญเสียเสถียรภาพของระบบปฏิบัติการของคอมพิวเตอร์โปรมแกรมมัลแวร์นั้นมีทั้งที่เป็นไวรัสคอมพิวเตอร์และหนอนคอมพิวเตอร์

๔. การโจมตีโดยใช้ไวรัสคอมพิวเตอร์ (Computer Virus) คือโปรแกรมคอมพิวเตอร์ที่บุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้คอมพิวเตอร์เครื่องนั้น ส่วนมากมีความประสงค์จะสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ โดยไวรัสจะฝังตัวอยู่ในแฟ้มข้อมูล เมื่อเปิดเครื่องคอมพิวเตอร์ และมีการเปิดแฟ้มข้อมูลใช้เครื่องคอมพิวเตอร์ก็จะติดไวรัส และจะแพร่ไปยังเครื่องอื่น ๆ ด้วย

๕. การโจมตีด้วยหนอนคอมพิวเตอร์ (Computer Worm) หนอนคอมพิวเตอร์จะแพร่กระจาย โดยไม่ผ่านการใช้งานของผู้ใช้โดยมากจะคัดลอกและกระจายตัวของหนอนคอมพิวเตอร์เองในเครือข่ายและข้ามเครือข่ายได้สามารถทำลายข้อมูลและสร้างความเสียหายให้กับคอมพิวเตอร์ได้

๖. การโจมตีด้วยระเบิดเวลา (Logic Bomb) อีกความหมายหนึ่งคือระเบิดตรรกะ หมายถึง ซอฟต์แวร์แอพพลิเคชั่นหรือชุดคำสั่งคอมพิวเตอร์โดยผู้เขียนโปรแกรมตั้งเวลากำหนดไว้อาจจะกำหนดเป็นวันที่หรือการกดปุ่มบนแป้นพิมพ์เพื่อให้มีการปิดระบบคอมพิวเตอร์หรือปิดเครือข่ายทั้งหมด รวมทั้งการลบข้อมูลหรือซอฟต์แวร์ต่างๆ บนเน็ตเวิร์กทิ้งทั้งหมด

๗. การโจมตีด้วยโทรจัน (Trojan) คือ โปรแกรมที่เป็นเหมือนโปรแกรมธรรมดาทั่วไป และอาจจะดูเหมือนไม่มีอันตรายอะไร แต่โปรแกรมนี้จะมีลักษณะแอบแฝงเพื่อทำอันตรายต่อระบบคอมพิวเตอร์โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมมาให้เมื่อผู้ใช้คอมพิวเตอร์นำโปรแกรมโทรจันไปติดตั้งในระบบเครือข่ายคอมพิวเตอร์ของตนเองแล้ว โปรแกรมนี้จะทำการขโมยข้อมูลผู้ใช้รหัสผ่าน หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ

๘. การโจมตีโดยใช้หุ่นยนต์ (Botnet) เป็นภัยคุกคามด้านสารสนเทศที่เกิดกับกลุ่มของเครื่องคอมพิวเตอร์ที่มีโปรแกรมไม่พึงประสงค์ติดตั้งอยู่ซึ่งโปรแกรมไม่พึงประสงค์นั้นจะทำการรับคำสั่งจากผู้ควบคุม ผ่านเครือข่ายอินเทอร์เน็ต โดยอาจจะเป็นคำสั่งที่ให้ทำการโจมตีระบบเครือข่ายหรือส่งสแปม และโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์นั้น

๙. การโจมตีแบบ Denial Of Service (DOS) คือ การโจมตีเพื่อให้ระบบหยุดการทำงาน ถ้ามีการใช้งานในระบบเครือข่ายโทรศัพท์ในบริเวณเดียวกันในปริมาณมากๆ ทั้งนี้เป็นเรื่องของระบบโทรศัพท์ อย่างไรก็ตามด้วยวิธีการเดียวกัน การใช้งานคอมพิวเตอร์ในระบบเครือข่ายโดยเฉพาะผ่านทางอินเตอร์เน็ตก็อาจประสบปัญหานี้ได้เช่นเดียวกัน ตัวอย่างเช่น การใช้งาน อีเมล์ เรามักจะมีการกำหนดของ mail ว่ามี mail box ขนาดเท่าใด เช่น ๑๐ mb, ๒๐ mb หรือ ๑๐๐ mb เป็นต้น ทั้งนี้ถ้ามีการโจมตี โดยการส่ง mail จำนวนมากๆ มาถึงเรา ผลก็คือเราไม่สามารถรับ mail อื่นๆ ได้ นอกจากการโจมตีผ่านทางอีเมล์แล้ว ยังมีการโจมตีผ่านทางเว็บไซต์ โดเมนเนม รวมทั้งบริการแชร์ไฟล์ นอกจากการถูกโจมตีแล้ว เรายังอาจเป็นหนึ่งในเครือข่ายของผู้โจมตีเครื่องคอมพิวเตอร์อื่นๆ ได้ โดยจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งานบางคน ที่อาจมีการติดตั้งโปรแกรมแบบไม่ตั้งใจ โดยอาจมีผู้แอบส่งโปรแกรมผ่านทางอีเมล์มากให้กับคุณ และเมื่อคุณรันโปรแกรมนี้ก็จะทำให้คุณกลายเป็นเครือข่ายของผู้ไม่ประสงค์ดีเหล่านี้

๑๐. การโจมตีด้วย (Ransomware) คือ มัลแวร์เรียกค่าไถ่เป็นซอฟต์แวร์ที่ได้รับการพัฒนาขึ้น เพื่อเข้ารหัสลับไฟล์ข้อมูลในเครื่องคอมพิวเตอร์หรือปิดกั้นไม่ให้ผู้ใช้เข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ได้โดย เรียกร้องให้เหยื่อจ่ายเงินเพื่อจะได้รับกุญแจถอดรหัสไฟล์หรือปลดล็อคการใช้งานเครื่องคอมพิวเตอร์ซึ่งปัจจุบัน จะมีภัยคุกคามลักษณะนี้เพิ่มมากขึ้น

๑๑. การปลอมหน้าเว็บไซต์ (Phishing) คือ การหลอกลวง หรือภัยทางอินเทอร์เน็ตชนิดหนึ่ง ที่เกิดจากการพยายามหลอกผู้ใช้งาน โดยการสร้างอีเมล์ หรือหน้าเว็บปลอมขึ้นมาเพื่อหวังผลในการให้ผู้ใช้งานเกิดความสับสน และทำธุรกรรมต่างๆบนเว็บไซต์ปลอมที่ถูกสร้างขึ้นมานั้น โดยข้อมูลต่างๆที่ผู้ใช้งานได้กรอกบนหน้าเว็บไซต์ปลอมเหล่านี้จะถูกดักกรองข้อมูลและบันทึกไว้เพื่อใช้ในการปลอมแปลง และเข้าถึงข้อมูลของผู้เสียกายโดยที่ไม่ได้รับอนุญาต

ภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรง และมีความซับซ้อนในการโจมตีมากขึ้น ความเสียหายที่เกิดจากการอาชญากรรมและการโจมตีทางไซเบอร์จะมีผลอย่างร้ายแรง ซึ่งในทุกองค์กรทั้งภาครัฐ และภาคเอกชน จะต้องตระหนักและต้องมีการกำหนดมาตรการในการป้องกันภัยคุกคามทางไซเบอร์ดังกล่าว แม้ว่าในบางองค์กรนั้นอาจจะยังไม่เคยถูกโจมตีทางไซเบอร์มาก่อนก็ตาม แต่ในองค์กรส่วนใหญ่ล้วนให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์ โดยมีการวางแนวทางป้องกันภัยคุกคามทางไซเบอร์ มีการปรับเปลี่ยนมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดรับกับการเปลี่ยนแปลงยุทธศาสตร์และการดำเนินการขององค์กร และเพื่อให้สอดคล้องกับการเปลี่ยนแปลงทางสภาพแวดล้อมภายนอก ซึ่งผู้บริหารองค์กรจะต้องมองลักษณะของภัยคุกคามทางไซเบอร์ให้รอบด้าน โดยมีประเด็นสำคัญดังนี้

๑. มีการคุกคามอย่างไร้ขอบเขต ทำให้ปัจจุบันภัยคุกคามทางไซเบอร์ยังคงมีเพิ่มมากขึ้นหลายเท่าตัวในโลกดิจิทัล และการเชื่อมต่อระหว่างกันของมนุษย์ อุปกรณ์อิเล็กทรอนิกส์ และองค์กร ที่ทำให้เกิดช่องโหว่ขึ้น และเปิดโอกาสให้เกิดภัยคุกคามได้ง่ายยิ่งขึ้น ดังนั้นในองค์กรต่างๆ ควรมีการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพและมีความซับซ้อนมากขึ้น เพื่อเป็นการป้องกันองค์กรจากการคุกคามทางไซเบอร์ที่มีเพิ่มขึ้น โดยสาเหตุของการคุกคามนั้น อันเนื่องมาจากการเปลี่ยนแปลงภายหลังเกิดวิกฤติเศรษฐกิจโลก ทำให้ภาคธุรกิจจำเป็นต้องปรับเปลี่ยนตัวเองอย่างรวดเร็ว มีการเปิดตัวผลิตภัณฑ์ใหม่ๆ การควบรวมกิจการ การขยายตลาด ตลอดจนมีการใช้เทคโนโลยีใหม่ๆ เพิ่มมากขึ้นเพื่อเชื่อมโยงองค์กรด้วยอินเทอร์เน็ตให้มีประสิทธิภาพสูงขึ้น ซึ่งการเปลี่ยนแปลงสิ่งต่าง ๆ เหล่านี้ ล้วนส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ขององค์กรด้วย ยกตัวอย่างการเปลี่ยนแปลงซึ่งก่อให้เกิดภัยคุกคามต่อการดำเนินงานขององค์กรดังนี้

๑.๑ การนำคอมพิวเตอร์และอุปกรณ์สื่อสารมาใช้ในการดำเนินงานขององค์กร ทำให้องค์กรต่างๆ มีความใกล้ชิดกันมากยิ่งขึ้น เนื่องจากการใช้งานอินเทอร์เน็ต สมาร์ทโฟน และแท็บเล็ต ทำให้เกิดการเชื่อมโยงและสามารถเข้าถึงข้อมูล สามารถแลกเปลี่ยนข้อมูลขององค์กรได้ทุกที่ทุกเวลา

๑.๒ ระบบนิเวศทางไซเบอร์ ปัจจุบันการดำรงชีวิต และการดำเนินงานในองค์กรต่างๆ ล้วนอยู่ภายใต้ระบบนิเวศทางไซเบอร์ ซึ่งเป็นไปได้อย่างมากที่จะเกิดอาชญากรทางไซเบอร์ที่เพิ่มขึ้นทั้งในการทำงาน และการใช้งานภายในที่พักอาศัย

๑.๓ การให้บริการประเภทคลาวด์ การบริหารจัดการข้อมูล และการจัดเก็บข้อมูล อาจกลายเป็นช่องทางทำให้เกิดความเสี่ยงใหม่ๆขึ้น

๑.๔ โครงสร้างพื้นฐาน ระบบเครือข่ายที่ใช้งานอยู่ในขณะนี้ ยังคงต้องมีการกำหนด IP Address ซึ่งอาจทำให้เกิดภัยคุกคามทางไซเบอร์ขึ้นเนื่องจากผู้โจมตีทราบถึงตำแหน่งเป้าหมาย และจากระบบ Back Office ขององค์กรเอง หรือมีการเจาะระบบในโครงสร้างพื้นฐานที่สำคัญ

๒. ความสามารถของอาชญากรทางไซเบอร์ที่มีจำนวนเพิ่มมากขึ้นอย่างไม่น่าเชื่อ ผู้โจมตีจะมีความสามารถในการเข้าถึงข้อมูลการลงทุนที่สำคัญ การโจมตีมีความซับซ้อนมากกว่าเดิม และผู้โจมตีจะมองหาช่องโหว่ในสภาพแวดล้อมการทำงานในองค์กรได้อย่างง่ายดาย ซึ่งจากการสำรวจที่ผ่านมาพบว่าบุคลากรในองค์กรมีโอกาสถูกโจมตีได้มากที่สุดโดยผู้โจมตีที่มาจากภายนอกองค์กร

๓. อุปสรรคที่องค์กรต้องเผชิญในปัจจุบัน เพื่อให้องค์กรสามารถเอาชนะอาชญากรทางไซเบอร์ได้ มีดังนี้คือ

๓.๑ ไม่มีความคล่องตัวในการดำเนินการ ไม่เพียงแต่ภัยคุกคามที่มีเพิ่มมากขึ้นเท่านั้น ในองค์กรจะต้องรู้ว่าอะไรคือช่องโหว่ขององค์กร เพื่อจะป้องกันภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม ในบางองค์กรอาจมีความเข้าใจถึงอันตรายที่จะเกิดขึ้นได้อย่างชัดเจน แต่ว่าไม่สามารถแก้ไขช่องโหว่นั้นได้อย่างรวดเร็วเพียงพอ นั่นเป็นเพราะไม่ได้รับรู้ถึงภัยคุกคามที่เกิดขึ้นแบบ Real time หรือในบางครั้งองค์กรก็มีความล้าหลังในด้านความมั่นคงปลอดภัยไซเบอร์

๓.๒ องค์กรไม่มีงบประมาณสำหรับความมั่นคงปลอดภัยไซเบอร์ ปัญหาการขาดงบประมาณถือเป็นหนึ่งในอุปสรรคที่มีความท้าทายมาก และงบประมาณสำหรับไซเบอร์สเปซถือว่ามีความจำเป็นอย่างยิ่ง เนื่องจากในการป้องกันภัยคุกคามทางไซเบอร์จำเป็นจะต้องใช้ทั้งงบประมาณและทรัพยากรที่มากขึ้น เพื่อให้เกิดประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้น

๓.๓ ขาดทักษะด้านความมั่นคงปลอดภัยไซเบอร์ อุปสรรคที่สำคัญที่สุดสำหรับการรักษาความปลอดภัยไซเบอร์คือ การขาดทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งปัญหาการขาดแคลนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์มีเพิ่มมากขึ้นอย่างต่อเนื่อง นอกจากนี้องค์กรยังมีความจำเป็นที่จะต้องสร้างทักษะที่ไม่ใช่ทักษะทางด้านเทคนิค เพื่อบูรณาการความมั่นคงปลอดภัยไซเบอร์กับธุรกิจหลักเข้าด้วยกัน โดยในการดำเนินการขององค์กรนั้น ไม่เพียงแต่ต้องทำการป้องกันตัวเองจากการโจมตีทางไซเบอร์เท่านั้น แต่ควรจะมีความสามารถในการวิเคราะห์ เพื่อคาดการณ์สิ่งที่อาจจะเกิดขึ้นและเพื่อสร้างความเชื่อมั่นและเตรียมความพร้อมในการดำเนินการในสภาพแวดล้อมที่เปลี่ยนแปลงไป

๔. การใช้งานเทคโนโลยีทำให้เกิดภัยคุกคามเพิ่มมากขึ้นเนื่องจากการพัฒนาเทคโนโลยีใหม่ ๆ การกำกับดูแล และความต้องการทางธุรกิจที่เปลี่ยนแปลงไป ทำให้องค์กรต้องมีการตื่นตัว และให้ความสำคัญในความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้น อย่างไรก็ตาม การรักษาความปลอดภัยของระบบงานในองค์กรนั้น ไม่ใช่เรื่องง่าย เนื่องจากความซับซ้อนของสภาพแวดล้อม การดำเนินการด้านเทคโนโลยี ระบบขับเคลื่อนองค์กรที่พัฒนาสืบทอดต่อกันมา รูปแบบของผู้ผลิตเทคโนโลยีที่แตกต่างกัน และวัฒนธรรมที่แตกต่างกันไปจนถึงมุมมองของความเข้าใจในเรื่อง Cyber ระหว่างผู้บริหารและทีมงานด้าน IT ที่มีความแตกต่างกัน ก็เป็นอุปสรรคสำคัญในการขับเคลื่อนกระบวนการด้าน Cyber security และจากที่ได้กล่าวไปแล้ว ความสะดวกในการเข้าถึงระบบโดยใช้เทคโนโลยี IP Address

จึงทำให้มีการเชื่อมต่อองค์กรกับโลกภายนอกอย่างหลีกเลี่ยงไม่ได้ ซึ่งจะเป็นเป้าหมายสำหรับอาชญากรทางไซเบอร์ที่สูงขึ้น และควรจะมีแนวทางในการดำเนินการเพื่อพัฒนาวิธีการป้องกันไซเบอร์อย่างจริงจัง

Cyber Crime ที่มีความถี่และความรุนแรงที่เพิ่มขึ้น ทำให้ทุกองค์กรจะต้องหันมาให้ความสำคัญในการวางยุทธศาสตร์ Cyber security แต่เนื่องจากเรื่องดังกล่าวถือว่าเป็นเรื่องใหม่ และเป็นเรื่องที่ยากยิ่งต่อการดำเนินการ เนื่องจากการเปลี่ยนแปลงอย่างรวดเร็วในด้านเทคโนโลยี จึงทำให้ฝ่ายบริหารระดับสูงจำนวนมากไม่สามารถปรับตัวได้ทันและยังไม่เข้าใจถึงบริบท ยังไม่สามารถกำหนดทิศทางของการดำเนินการด้าน Cyber security ได้อย่างมีประสิทธิภาพ

สรุปได้ว่า ในปัจจุบันภัยคุกคามรูปแบบใหม่ที่ส่งผลต่อความมั่นคงของประเทศชาติได้เกิดขึ้นอย่างต่อเนื่อง โดยไม่ได้เกิดจากมิติของการก่อสงครามเหมือนเช่นในอดีต แต่เป็นภัยคุกคามที่เกิดขึ้นในลักษณะของปัญหาทางการเมือง ปัญหาสังคม ปัญหาสิ่งแวดล้อม และภัยธรรมชาติที่เกิดจากการเปลี่ยนแปลงของสภาพสังคมและสิ่งแวดล้อม ปัญหาการก่อความรุนแรงและปัญหาอาชญากรรมข้ามชาติ การพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีสารสนเทศ ที่มีการพัฒนาอย่างต่อเนื่อง ทำให้ปัญหาอาชญากรรมทางไซเบอร์และภัยคุกคามจากเครือข่ายสังคมออนไลน์มีการขยายตัวอย่างรวดเร็ว รุนแรงในระบบสารสนเทศทุกแขนง การบิดเบือนข้อมูลข่าวสารผ่านการกระจายข่าวสารทางสื่อสาธารณะและสังคมเครือข่ายออนไลน์ เป็นตัวการสำคัญที่ทำให้เกิดการรับรู้การตีความและการพิจารณาตัดสินใจในการแก้ไขปัญหามีความยุ่งยากและมีความเสี่ยงเป็นภัยคุกคามที่ภาครัฐได้หันมาให้ความสำคัญมากขึ้น ซึ่งผู้วิจัยเห็นว่า ภัยคุกคามด้านไซเบอร์เป็นภัยคุกคามรูปแบบใหม่ที่ยิ่งจะทวีความรุนแรงเพิ่มขึ้นเรื่อย ๆ หน่วยงานความมั่นคงจึงควรมีการพัฒนาและเตรียมพร้อมรับภัยคุกคามทางไซเบอร์ให้มากยิ่งขึ้น

แนวคิดเกี่ยวกับภัยคุกคาม Cyber Attack

ภายใต้กระแสโลกาภิวัตน์ การพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสารที่มีการพัฒนาไปอย่างรวดเร็ว มีการรับและส่งข้อมูลข่าวสารจากที่หนึ่งไปยังอีกที่หนึ่งได้ทุกสถานที่ ทุกเวลา ไร้ขอบเขตจำกัด และมีความเสมือนอยู่ในเหตุการณ์ และสถานที่นั้นเอง การสร้าง พัฒนาและปรับปรุงแอพพลิเคชั่นต่าง ๆ ขึ้นมาเพื่อรองรับความต้องการของผู้ใช้งานเพิ่มมากขึ้น รวมถึงความสามารถในการเข้าถึงข้อมูลข่าวสารของผู้บริโภคผ่านทางอุปกรณ์อิเล็กทรอนิกส์ก็มีมากขึ้น ซึ่งมีความสามารถในการเข้าถึงในทุกระดับผ่านอุปกรณ์การสื่อสาร และอุปกรณ์อิเล็กทรอนิกส์ เช่น โทรศัพท์เคลื่อนที่ (Smart Phone) อุปกรณ์คอมพิวเตอร์ และอุปกรณ์อื่นๆ ที่สามารถสื่อสารผ่านระบบเครือข่ายได้ด้วยอินเทอร์เน็ตโปรโตคอล (Internet Protocol) เพื่อส่งข้อมูลระหว่างกันจำนวนมาก ทำให้ยากต่อการควบคุมขึ้นเป็นลำดับ ผู้ไม่หวังดีหรือผู้ก่อการร้ายสามารถใช้ช่องทางนี้ในการเข้าถึงข้อมูล หรือเข้าแทรกแซงการทำงานของระบบเพื่อกระทำการอย่างใดอย่างอื่นต่อไป

ได้ด้วยขนาดและความซับซ้อนของระบบอินเทอร์เน็ตทำให้เกิดคำนิยามใหม่ที่เรียกว่า “โลกไซเบอร์”หรือ“มิติไซเบอร์” (Cyberspace) เกิดขึ้น

โลกไซเบอร์ หรือ มิติไซเบอร์ (Cyberspace) เป็นยุคของการปฏิบัติการด้านข่าวสาร (Information Operations) เนื่องจากมีการกระจายข้อมูลข่าวสารทั้งข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เพื่อการประชาสัมพันธ์ การโฆษณาชวนเชื่อ การยุยงปลุกปั่น เป็นต้น ไปในวงกว้าง สามารถเข้าถึงกลุ่มเป้าหมายด้วยความรวดเร็วเพียงไม่กี่วินาที และสามารถแชร์ข้อมูลต่อ ๆ กันไป รวมถึงสามารถแสดงความคิดเห็นต่าง ๆ ทั้งทางบวกและทางลบ และมีอิทธิพลต่อความรู้สึกนึกคิด ทัศนคติ และมีผลต่อการตัดสินใจของคนจำนวนมาก ซึ่งในปัจจุบันโลกไซเบอร์ ได้เข้ามาเป็นส่วนหนึ่งของคนธรรมดาสามัญตลอด ๒๔ ชั่วโมง ตั้งแต่เกิดจนตาย ทั้งในด้านของการใช้งานส่วนตัว และการให้บริการของภาครัฐ ยกตัวอย่าง เช่น ข้อมูลบุคคลตั้งแต่แรกเกิดจะถูกบันทึกใน ระบบดิจิตอล ต่อมาเมื่ออายุ ครบ ๗ ปี ก็ต้องทำบัตรประชาชนอิเล็กทรอนิกส์สำหรับเด็ก ข้อมูลก็จะถูกบันทึกเก็บเพิ่มเติมไว้ในโลกไซเบอร์ อีกเช่นกัน นอกจากนี้สิ่งอำนวยความสะดวกต่าง ๆ ที่มีความจำเป็นต่อความต้องการพื้นฐานของมนุษย์ และการทำงานต่าง ๆ ต่างก็มีความเกี่ยวข้องกับมิติไซเบอร์ทั้งสิ้น ดังนั้น เมื่อมีข้อดีก็ย่อมมีข้อเสีย การเก็บข้อมูลส่วนตัวไว้ในระบบเครือข่ายคอมพิวเตอร์หรือโลกไซเบอร์นั้น หากมีการรั่วไหลของข้อมูล หรือข้อมูลถูกเจาะ ถูกแก้ไขดัดแปลง ถูกทำลาย ก็จะทำให้เกิดความเสียหายอย่างใหญ่หลวง อีกทั้งในปัจจุบันบุคคลผู้ไม่หวังดีหรือผู้ก่อการร้าย ได้มีการปรับรูปแบบในการโจมตีทางการทหารมาเป็นการโจมตีผ่านทางโลกไซเบอร์ ไม่ว่าจะเป็นการโจรกรรมข้อมูล การระงับ ก่อกวน หรือควบคุมการปฏิบัติงานของเครื่องมือสื่อสาร เป็นต้น ทำให้ในปัจจุบันภาครัฐเริ่มตระหนักถึงภัยคุกคามรูปแบบใหม่ที่กระทำผ่านทางโลกไซเบอร์ (Cyberspace) และให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ทั้งนี้เพื่อให้มีความพร้อมด้านขีดความสามารถในการปกป้อง รับมือ ลดความเสี่ยง รวมถึงการฟื้นฟูสถานการณ์ภัยคุกคามจากโลกไซเบอร์ในระดับและรูปแบบต่าง ๆ จากสถานการณ์การโจมตีในโลกไซเบอร์ (Cyber Attack) ของโลกที่มีแนวโน้มความรุนแรง และความถี่ในการเกิดเพิ่มสูงขึ้นในแต่ละปี ถือเป็นภัยคุกคามในการก่อการร้ายรูปแบบใหม่ ไม่ว่าจะเป็นการหลอกเอาข้อมูลส่วนบุคคลจากประชาชนทั่วไป รวมถึงการโจมตีหน่วยงานที่มีข้อมูลสำคัญ เช่น หน่วยงานทางทหาร หน่วยงานความมั่นคง และความปลอดภัยของประเทศ โดยเหตุการณ์ Cyber Attack ได้เกิดขึ้นทั้งในประเทศมหาอำนาจรวมถึงประเทศอื่น ๆ ในประชาคมโลก ซึ่งการคุกคามจากไซเบอร์นั้นย่อมส่งผลกระทบต่อความมั่นคงทั้งทางตรงและทางอ้อม ไม่ว่าจะเป็นความเสียหายที่สามารถประเมินมูลค่าได้หรือจะเป็นการสูญเสีย “เสรีภาพ” ของหน่วยงานและประชาชนผู้ถูกคุกคาม (ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย, ๒๕๕๙)

สถานการณ์และแนวโน้มความรุนแรงจาก Cyber Attack

ปี พ.ศ. ๒๕๕๖ นายเอ็ดวาร์ด สโนว์เดน ได้กล่าวหาว่าสำนักงานความมั่นคงแห่งชาติ (National Security Agency: NSA) ของสหรัฐอเมริกา ใช้ระบบ “ ปริซึม ” ในการสอดแนมผู้ใช้อินเทอร์เน็ตโดยสามารถเข้าถึงข้อมูลได้ทุกชนิด ไม่ว่าจะเป็นอีเมล์ ภาพถ่าย รวมถึงการดักฟังโทรศัพท์ หรือโปรแกรมติดต่อสื่อสารระหว่างกันผ่านอินเทอร์เน็ต เพื่อสืบหาข้อมูลที่เป็นภัยต่อความมั่นคง ของประเทศ ทั้งนี้ สโนว์เดนยังอ้างว่าสหรัฐอเมริกา แอบแฮกข้อมูลเครือข่ายคอมพิวเตอร์ของจีนและฮ่องกงมานานหลายปีเช่นกัน และในปีเดียวกัน บริษัท Spamhaus ที่มีสำนักงานอยู่ในกรุงเจนีวาและลอนดอน ถูกนักเจาะระบบโจมตีด้วยเทคนิค Distributed Denial of Service (DDoS) ก่อกวนทำให้เว็บไซต์ล่ม ส่งผลกระทบต่อโครงข่ายอินเทอร์เน็ตในยุโรป ทำให้ผู้ใช้อินเทอร์เน็ตทั่วไปและบริการออนไลน์อื่นๆได้รับผลกระทบอย่างมาก เช่น London Internet Exchange: LINX ศูนย์แลกเปลี่ยนเครือข่ายอินเทอร์เน็ตไม่สามารถทำงานได้นับชั่วโมง ทำให้ชาวออนไลน์ในยุโรปและเอเชียหลายประเทศต้องพบกับภาวะอินเทอร์เน็ตช้า และส่งผลให้เว็บไซต์ของรัฐบาลบางประเทศ บริษัทและธนาคารไม่สามารถให้บริการตามปกติได้

ปี พ.ศ. ๒๕๕๗ แฮกเกอร์ได้ขโมยข้อมูลของผู้ใช้บริการยาฮู (Yahoo) ราว ๕๐๐ ล้านราย ซึ่งถือเป็นการล้วงข้อมูลทางไซเบอร์ครั้งใหญ่ที่สุดในประวัติศาสตร์ โดยสิ่งที่แฮกเกอร์ ได้ไปมีตั้งแต่ข้อมูลส่วนตัวของผู้ใช้ อีเมล์ หมายเลขโทรศัพท์ วันเดือนปีเกิด และพาสเวิร์ด

ปี พ.ศ. ๒๕๕๘ พบมัลแวร์ (encounter rate: ER) ในประเทศไทยเพิ่มสูงขึ้น ๖.๙ % ในขณะที่จำนวนเฉลี่ยของเครื่องคอมพิวเตอร์ที่ต้องการกำจัดมัลแวร์ด้วยเครื่องมือของไมโครซอฟท์ (Computers cleaned per mille: CCM) สูงขึ้นเกินกว่าหนึ่งเท่าจาก ๒๒.๒ เป็น ๔๖.๓ ต่อ ๑,๐๐๐ เครื่อง สถิติทั้งสองนี้แสดงให้เห็นว่าเป็นเทศไทยกำลังเผชิญกับภัยร้ายในโลกดิจิทัลเพิ่มมากขึ้น ทั้งยังมีรูปแบบการจู่โจมที่ซับซ้อนมากขึ้น โดยความเปลี่ยนแปลงเหล่านี้ล้วนเป็นผลกระทบที่หลีกเลี่ยงไม่ได้จากการพัฒนาสู่ยุคสังคมดิจิทัล หากไม่มีการกำจัดภัยร้ายมัลแวร์ ประชาชนคนไทยต้องเผชิญกับอันตรายนับตั้งแต่การสูญเสียข้อมูลส่วนบุคคลเล็กๆน้อยๆ ไปจนถึงความเสียหายทางการเงินมูลค่ามหาศาล

จากภัยคุกคามทางด้านไซเบอร์ องค์กรต่างๆ ได้ให้ความสำคัญในการรับมือกับ Cyber Attack เช่น หน่วยงาน National Institute of Standards and Technology: NIST ของสหรัฐอเมริกา ที่ทำหน้าที่กำหนดมาตรฐานเทคโนโลยีสาระสนเทศ ได้จัดทำแนวทางรักษาความปลอดภัยทางไซเบอร์ (Cyber security framework) เพื่อให้หน่วยงานภาครัฐ ภาคเอกชน รวมถึงสถาบันการเงินต่างๆ ใช้เป็นแนวทาง ในขณะที่ธนาคารกลางของอังกฤษ สหรัฐอเมริกา และสิงคโปร์ก็จัดให้มีการทดสอบการรับมือ Cyber Attack ในระดับประเทศมาตั้งแต่ปี ๒๕๕๔ ข้อมูลข้างต้นแสดงให้เห็นว่าแต่ละประเทศมีการตื่นตัวในการป้องกัน

ภัยคุกคามทางไซเบอร์ ประเทศไทยโดยเฉพาะอย่างยิ่งกองทัพไทยที่เป็นหน่วยงานหลักความมั่นคงของประเทศจึงจำเป็นต้องมีการตื่นตัวในเรื่องดังกล่าว

ผลกระทบของ Cyber Attack ต่อความมั่นคงของชาติ

ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ เป็นภัยคุกคามในระดับประเทศ หรือระดับชาติผู้ที่ก่อภัยคุกคามอาจใช้วิธีนำข่าวสารเหล่านั้นลงเผยแพร่ในเว็บไซต์ของประเทศตนเอง เพื่อให้ข่าวสารเหล่านั้นเผยแพร่เข้ามาสู่ประเทศไทย จนสงผลกระทบต่อความมั่นคงภายในประเทศไทย และทำให้เกิดความได้เปรียบทางการเมืองหรือด้านความมั่นคง รวมทั้งการเผยแพร่ข้อมูลความลับของประเทศไทย และการแพร่กระจายโปรแกรมไม่พึงประสงค์สำหรับการทำลายเครือข่ายระบบคอมพิวเตอร์

ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ เป็นการใช้ไซเบอร์ที่เป็นภัยคุกคามต่อความมั่นคงของชาติในการเผยแพร่ข่าวสารของผู้ก่อความไม่สงบ เช่น การเผยแพร่ข่าวลือ ข่าวที่ไม่ เป็นจริง โดยการกล่าวหาว่าเจ้าหน้าที่ของรัฐทำการละเมิดสิทธิมนุษยชน เพื่อให้สื่อมวลชนกระแสหลักนำข่าว ไปเผยแพร่ต่อเพื่อต้องการให้ประชาชนทั่วไปหวาดกลัวจนทำให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่รัฐถือเป็น การปฏิบัติการข่าวสาร (Information Operation) ที่เป็นการปฏิบัติการจิตวิทยาอย่างหนึ่ง นอกจากนั้นยังมีการเผยแพร่ผลงานของผู้ก่อความไม่สงบที่อาจจะส่งผลกระทบทำให้เกิดแนวร่วมของผู้ก่อความไม่สงบเพิ่มมากขึ้น

ภัยคุกคามที่ส่งผลกระทบต่อสถาบันของชาติเป็นสิ่งที่กระทำได้ง่าย และยากต่อการดำเนินคดีต่อผู้กระทำผิดคือการเผยแพร่ภาพที่หมิ่นสถาบันพระมหากษัตริย์ การวิจารณ์สถาบันในทางเสื่อมเสีย ซึ่งเจ้าหน้าที่ของรัฐบาลไทยไม่สามารถดำเนินการตามกฎหมายไทยได้เพราะส่วนหนึ่งของผู้กระทำความผิด ไม่ได้อยู่ในประเทศไทย แต่ได้ใช้เว็บไซต์หรือสื่อโซเชียลในต่างประเทศเผยแพร่ข่าวสารเข้ามายังประเทศไทย

ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพ เพื่อทำให้ภาพลักษณ์ของกองทัพหรือผู้นำกองทัพเสื่อมเสีย หรือลดความน่าเชื่อถือในสังคม ย่อมจะสร้างความไม่เชื่อมั่นต่อการปกป้อง หรือพิทักษ์อธิปไตยของชาติ อาจจะเป็นการแสดงให้ประชาชนเชื่อว่า กองทัพมีแต่กำลังพลที่ขาดวินัย ไม่รักษากฎระเบียบของกองทัพ การกระทำผิดกฎหมายของประเทศ ล้วนแล้วแต่เป็นหัวข้อที่ผู้ที่ต้องการกระทำต่อกองทัพใช้เป็นประเด็นหลัก ๆ ในการดำเนินการ สิ่งเหล่านั้นหรือข้อมูลที่ได้รับอาจจะได้มาจากการกระทำผิดของกำลังพลเพียงบางคนของกองทัพ แต่เมื่อมีการเผยแพร่ในโลกไซเบอร์จะเกิดผลกระทบในวงกว้างและจะขยายผลเหตุการณ์ต่าง ๆ ดำเนินไปได้อย่างรวดเร็วมาก การพยายามจะชี้แจงข้อเท็จจริงของกองทัพอาจจะต้องดำเนินการภายหลังจากเหตุการณ์ทางไซเบอร์เกิดขึ้นแล้ว หรืออาจจะแค่การประชาสัมพันธ์ในเชิงตอบโต้ผ่านทางสื่อกระแสหลักทั้งหลายสำหรับการแก้ไขปัญหาทางไซเบอร์กระทำได้ยาก เนื่องจากการเผยแพร่หรือกระจายข่าวสารเป็นการกระทำในแบบเครือข่ายที่เชื่อมต่อกันไปเรื่อย ๆ ไม่รู้จบ นอกจากนั้นยังมีประเด็นที่เกี่ยวข้องกับด้านการเมือง หรือในด้านของความไม่พอใจของคนในกองทัพเป็นการส่วนตัว

ก็เป็นประเด็นที่จะสร้างความเสื่อมเสียภาพลักษณ์ต่อกองทัพในภาพรวมได้เช่นกัน นอกจากนั้น ยังมีประเด็นสำคัญที่มักจะเกิดขึ้นบ่อยๆ เช่น เอกสารลับของทางราชการถูกนำไปเผยแพร่ในโลกไซเบอร์ ผู้กระทำอาจจะต้องการเพียงเพื่อให้ประชาชนทั่วไป หรือฝ่ายที่ไม่พอใจของกองทัพ ได้นำไปเผยแพร่ ขยายผล แต่กลับส่งผลกระทบต่อหน่วยงานที่เกี่ยวข้องอย่างมาก เพราะนอกจากเสื่อมเสียภาพลักษณ์แล้ว ยังจะแสดงถึงการขาดประสิทธิภาพในการทำงานด้านการรักษาความลับของทางราชการกระทำไม่ได้ตามที่ระเบียบกำหนดไว้นั่นเอง สื่อสังคมออนไลน์ถูกนำมาใช้เพื่อหวัง ผลประโยชน์ในทางการเมือง เศรษฐกิจ สังคม มากขึ้น การถูกคุกคามจากฝ่ายที่ไม่เห็นด้วยจึงเป็นไปได้ง่าย และด้วยความสามารถในการเข้าถึงกลุ่มคนหมู่มากอย่างทันถ่วงทีการคุกคามจึงเป็นไปอย่างรวดเร็ว เช่น การโฆษณาชวนเชื่อ การปลุกระดมคน การหมิ่นประมาท การละเมิดสิทธิส่วนบุคคล การสร้างความหวาดกลัวแก่คนในสังคมให้รู้สึกสะเทือนใจ อันส่งผลต่อการปฏิบัติการทางจิตวิทยา รวมถึงการส่งไวรัสเข้าคุกคามสื่อสังคมออนไลน์ที่ตกเป็นเป้าหมาย ซึ่งการกระทำดังกล่าวถือว่าเป็นการคุกคามประชาชนผู้บริโภคสื่อ และผู้ตกเป็นเป้าหมาย รวมทั้งเป็นการสร้างพฤติกรรมการสื่อสารที่ไม่มีการคัดกรองอย่างละเอียดขาดจิตสำนึกในการบริโภคสื่อ และส่งเสริมให้มีการกระทำผิดมากขึ้น

ในปัจจุบันผู้คนหันมาใช้สื่อสังคมออนไลน์แทนสื่อแบบเดิม ๆ ในการสื่อสารข้อมูลถึงกัน ซึ่งในช่วงเริ่มแรก การใช้สื่อสังคมออนไลน์มักใช้ในลักษณะของงานอดิเรกสื่อสารกันระหว่างตนเองกับ คนรู้จัก จากนั้นได้ขยายการประยุกต์ใช้สู่ภาคธุรกิจ ซึ่งได้รับการตอบรับจากผู้คนอย่างกว้างขวางสาเหตุสำคัญที่ทำให้สื่อสังคมออนไลน์ได้รับความนิยมขึ้นเรื่อยๆ มาจากการใช้งานที่ง่าย เข้าถึงกลุ่มคนได้รวดเร็ว มีการแสดงความคิดเห็นไปมา และสื่อที่นำมาแบ่งปันมีลักษณะหลากหลาย รวมทั้งการพัฒนาตลอดเวลาของเทคโนโลยีการสื่อสารและอินเทอร์เน็ต ทำให้มีความชัดเจนว่าสื่อสังคมออนไลน์จะเป็นสื่อหลักของผู้คนในโลกอนาคตอย่างแท้จริงและเมื่อผู้คนให้ความสนใจและหาประโยชน์จากสื่อสังคมออนไลน์แน่นอน ก็ย่อมมีคนที่สร้างความปั่นป่วนและวุ่นวายแก่ชุมชนเสมือน (Virtual Communities) และกระทบต่อชุมชนแห่งความเป็นจริงประเทศไทย ในด้านการปฏิบัติการเป็นนักจารกรรมข้อมูลออนไลน์, จารชน, จารบุรุษ, ผู้สอดแนม, นักสืบ, นักสืบราชการลับ ฯลฯ ในโลกไซเบอร์ในระดับประเทศต่อประเทศยังไม่ค่อยจะมีข่าวปรากฏ อาจจะมีหรือไม่ไม่ทราบแน่ชัด แต่ในระดับภายในประเทศ โดยเฉพาะทางด้านวงการการเมือง การค้าการขาย ก็มีข่าวอยู่บ่อยครั้ง ที่มีทั้งภาพนิ่ง ภาพเคลื่อนไหว ภาพจากกล้องวงจรปิด การใช้วิทยุโทรศัพท์ หรือเอกสารสำคัญทางราชการ ถูกนำมาเผยแพร่ตามสื่อออนไลน์ต่าง ๆ เพื่อการทำลายเครดิตหรือแบล็คเมล์ เรียกร้องผลประโยชน์ การเจรจาต่อรอง การสร้างภาพความชอบธรรมในการปฏิบัติการใดการหนึ่ง ฯลฯ

คงปฏิเสธไม่ได้ว่าในปัจจุบัน Social Network หรือสังคมออนไลน์กำลังมีบทบาทต่อชีวิตเรามากยิ่งขึ้น ภาพข่าวที่เห็นในสื่อหลักอื่น ๆ ทั้งวิทยุและโทรทัศน์ก็ถูกกระแสของ Social Network เข้ามามีอิทธิพลอย่างหลีกเลี่ยงไม่ได้ โดยหากมองอิทธิพลของสังคมออนไลน์ที่ผ่านมาไม่ว่าจะเป็นในคราวที่ประเทศไทยประสบกับมหาอุทกภัยเมื่อปี ๒๕๕๔

นั้น มีการใช้ Social Media อย่างกว้างขวางเพื่อเผยแพร่ข่าวสารผ่านเว็บไซต์หรืออินเตอร์เน็ต ซึ่งทำให้ข่าวสารถูกแพร่กระจายออกไปอย่างรวดเร็ว ผู้คนสามารถติดตามสถานการณ์น้ำท่วมได้อย่างต่อเนื่อง สรุปได้ว่าเทคโนโลยีด้านไซเบอร์เปรียบเสมือนเหรียญที่มี ๒ ด้าน เป็นเครื่องมือที่มีทั้งคุณประโยชน์อย่างมหาศาล และในทำนองเดียวกันก็มีโทษอย่างรุนแรงขึ้นอยู่ที่ว่าเราใช้เทคโนโลยีด้านไซเบอร์ไปในทางใด ที่สำคัญคือเราต้องมีมาตรการป้องกันตนเองที่รอบคอบรัดกุม และใช้พลังของเทคโนโลยีด้านไซเบอร์ไปในทางที่ก่อประโยชน์กับสังคมและประเทศชาติ

นโยบายในการเตรียมพร้อมรับมือ Cyber Attack ในปัจจุบัน

สำหรับประเทศไทย สภาความมั่นคงแห่งชาติ โดยสำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำนโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ - ๒๕๖๔ เพื่อเป็นกรอบในการดำเนินการด้านความมั่นคงของประเทศไทยในระยะ ๗ ปี เพื่อใช้เป็นกรอบทิศทางหลักในการรักษาผลประโยชน์และความมั่นคงของชาติให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ เอกภาพ และประสานสอดคล้องกันทั้งประเทศ ทั้งนี้รวมถึงการเตรียมพร้อมเพื่อส่งเสริมความมั่นคงทั้งในด้านของการป้องกัน และลดความเสี่ยงจากภัยคุกคามต่าง ๆ ทั้งในประเทศและระหว่างประเทศ ประกอบด้วย ๑๖ ประเด็นนโยบาย โดยกำหนดเป็นสองส่วน

๑.นโยบายสำคัญเพื่อเสริมสร้างความมั่นคงที่เป็นแก่นหลักของชาติ จำนวน ๓ นโยบาย ได้แก่

๑.๑ การเสริมสร้างความมั่นคงของสถาบันหลักของชาติและการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

๑.๒ การสร้างความเป็นธรรม ความปรองดองและความสมานฉันท์ในชาติ

๑.๓ การป้องกันและแก้ไขการก่อความไม่สงบในจังหวัดชายแดนภาคใต้

๒. นโยบายความมั่นคงแห่งชาติทั่วไป ๑๓ นโยบาย โดยมุ่งสร้างภูมิคุ้มกันของสังคมในทุกระดับให้พร้อมเผชิญปัญหาและภัยคุกคามต่าง ๆ ได้แก่

๒.๑ การจัดระบบการบริหารจัดการชายแดนเพื่อป้องกันและแก้ไขปัญหาข้ามพรมแดน

๒.๒ การเสริมสร้างศักยภาพการป้องกันและแก้ไขปัญหาภัยคุกคามข้ามชาติ

๒.๓ การปกป้องรักษาผลประโยชน์แห่งชาติทางทะเล

๒.๔ การจัดระบบป้องกันและแก้ไขปัญหาของผู้หลบหนีเข้าเมือง

๒.๕ การเสริมสร้างความเข้มแข็งและภูมิคุ้มกันความมั่นคงภายใน

๒.๖ การเสริมสร้างความมั่นคงของชาติจากภัยการทุจริตคอร์รัปชั่น

๒.๗ การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์

๒.๘ การรักษาความมั่นคงของฐานทรัพยากรธรรมชาติและสิ่งแวดล้อม

๒.๙ การเสริมสร้างความมั่นคงทางพลังงานและอาหาร

๒.๑๐ การพัฒนาระบบการเตรียมพร้อมแห่งชาติเพื่อเสริมสร้างความมั่นคงของชาติ

๒.๑๑ การเสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ

๒.๑๒ การพัฒนาระบบงานข่าวกรองให้มีประสิทธิภาพ

๒.๑๓ การเสริมสร้างดุลยภาพในการดำเนินความสัมพันธ์ระหว่างประเทศ

สภาความมั่นคงแห่งชาติ ได้กำหนดนโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ - ๒๕๖๔ ที่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์ ไว้ในนโยบายข้อที่ ๑๐ เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ (นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘-๒๕๖๔, หน้า ๑๗) ดังนี้

๑. จัดให้มีการปกป้องภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยการบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ การประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ บุคลากร องค์กร และผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างประเทศ การเฝ้าระวัง และการพัฒนาระบบป้องกันการโจมตีระบบสารสนเทศ การพัฒนาความพร้อมต่อสงครามไซเบอร์ การปกป้องโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ การกู้คืนข้อมูล ระบบ/เครือข่ายและการพัฒนามาตรฐานด้านความปลอดภัยในทุกด้าน

๒. จัดให้มีการพัฒนาการบังคับใช้กฎหมาย โดยการพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ และการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ ให้สามารถลดภัยคุกคามหรืออันตรายที่ส่งผลกระทบต่อบุคคล ข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยเฉพาะที่อยู่ในรูปของการทำธุรกรรมทางอิเล็กทรอนิกส์ การละเมิดทรัพย์สินทางปัญญา การโจรกรรมข้อมูลสารสนเทศ การละเมิดสิทธิเสรีภาพของบุคคล การกรรโชกข้อมูลสารสนเทศ การกระทำผิดตลอดจนการก่อวินาศกรรมหรือทำลายระบบสารสนเทศ รวมถึงการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

๓. จัดให้มีการพัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ โดยการส่งเสริมการวิจัย พัฒนาและจดสิทธิบัตรเทคโนโลยีสารสนเทศที่ผลิตโดยคนไทย การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ การบูรณาการเชื่อมโยงระบบฐานข้อมูลภาครัฐ การพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ รวมถึงการใช้ระบบรัฐบาลอิเล็กทรอนิกส์เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ระบบคลาวด์ภาครัฐ (G-Cloud) (G-Cloud คือ โครงสร้างพื้นฐานบนอินเทอร์เน็ต (Internet) แบบใช้ทรัพยากรร่วมกัน โดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.) ให้บริการแก่หน่วยงานภาครัฐด้วยเทคโนโลยี Cloud) ตลอดจนการพัฒนาบุคลากรภาครัฐ องค์กร ทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ความชำนาญทางด้านระบบเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยทางไซเบอร์ เพื่อให้บุคลากรภาครัฐและองค์กรทุกภาคส่วนที่เกี่ยวข้องมีข้อมูลข่าวสารและความรู้ทางด้านเทคโนโลยีที่ทันสมัย และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในเชิงปริมาณและคุณภาพอย่างต่อเนื่อง

สำหรับหน่วยงานทางทหารนั้น กองทัพไทยเป็นหน่วยงานหลักทางความมั่นคงของประเทศไทย ได้มีการตื่นตัวในเรื่องของภัยคุกคามไซเบอร์ (Cyber Attack) ดังกล่าวล่าสุดกระทรวงกลาโหมได้เห็นชอบ “ร่างแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ. ๒๕๖๐-๒๕๖๔” เพื่อใช้ในการป้องกันการคุกคามจาก Cyber Attack ที่อาจจะมีผลกระทบต่อความมั่นคง ตลอดถึงความเชื่อมั่นในการพัฒนาเข้าสู่ระบบโลกดิจิทัล โดยมีสาระครอบคลุม ๖ แผนงานหลัก ดังนี้

๑. แผนการจัดองค์กรด้านไซเบอร์ โดยกระทรวงกลาโหม, กองบัญชาการกองทัพไทย และเหล่าทัพ ดำเนินการจัดตั้งหน่วยงานไซเบอร์ หรือศูนย์ไซเบอร์ ขึ้นมารองรับภารกิจด้านไซเบอร์โดยตรง

๒. แผนการป้องกันระบบโครงสร้างพื้นฐาน โดยกระทรวงกลาโหม, กองบัญชาการกองทัพไทย และเหล่าทัพ เตรียมจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center: CSOC) ของตนขึ้นมาเพื่อรองรับภัยคุกคามด้านไซเบอร์ที่จะมาโจมตีระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ระบบฐานข้อมูลรวมทั้งการจัดตั้งทีมจัดการปัญหาฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident Response Team/Computer Security Incident Response Team: CSIRT) เพื่อตอบสนองการแก้ไขปัญหาฉุกเฉินด้านความปลอดภัยไซเบอร์ได้อย่างรวดเร็วและทันเวลา

๓. แผนการพัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุก และการปฏิบัติการสงครามไซเบอร์ เป็นการพัฒนาบุคลากรของกองทัพให้มีขีดความสามารถด้านการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ เพื่อการป้องกันการสกัดกั้น การยับยั้งการโจมตี และการตอบโต้ฝ่ายตรงข้ามที่มีผลกระทบต่อความมั่นคงของชาติ และความมั่นคงด้านการทหาร โดยการพัฒนาเสริมสร้างขีดความสามารถกำลังพล เครื่องมือ และเทคโนโลยีต่างๆ รวมถึงการจัดให้มีการแข่งขันทักษะการปฏิบัติการไซเบอร์ (Cyber Contest)

๔. แผนการดำรงและพัฒนาศักยภาพด้านไซเบอร์ เพื่อดำรงความต่อเนื่องและยั่งยืนอย่าง เป็นรูปธรรม รวมทั้งการวิจัย และพัฒนาเทคโนโลยีด้านไซเบอร์ (R&D) เพื่อวิจัยพัฒนา และติดตามความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพราะภัยคุกคามด้านไซเบอร์นับวันจะทวีความรุนแรง ส่งผลกระทบและความเสียหายในวงกว้างอย่างรวดเร็ว

๕. แผนการสนับสนุนศักยภาพทางไซเบอร์ระดับชาติ เนื่องจากกองทัพเป็นหน่วยงานหลักด้านความมั่นคงแห่งชาติ จึงต้องมีความพร้อมในการสนับสนุนและเป็นเครื่องมือให้กับรัฐบาล เพื่อเสริมสร้างศักยภาพด้านไซเบอร์ของชาติ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยคุกคามในระดับชาติด้านไซเบอร์โดเมน (Cyber Domain)

๖. แผนงานความร่วมมือ และผนึกกำลังด้านไซเบอร์ เป็นการประสานความร่วมมือทุกภาคส่วน ทั้งภาครัฐ ธุรกิจเอกชน และประชาชนทั่วไป ในการผนึกกำลังด้านไซเบอร์ ซึ่งเป็นกำลังอำนาจที่ไม่มีตัวตน และนำไปสู่การระดมสรรพกำลังของประเทศด้านไซเบอร์ที่มีพลังอำนาจที่ยิ่งใหญ่

จากร่างแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๖๐ - ๒๕๖๔ แสดงให้เห็นถึงความสำคัญของภัยคุกคามด้านไซเบอร์ ที่กองทัพจะต้องมีการเตรียมพร้อม เพื่อรับมือต่อการโจมตีในโลกไซเบอร์ (Cyber Attack) ที่อาจจะมีผลกระทบต่อความมั่นคงของประเทศชาติในอนาคต

ระบบการฝึกทหารใหม่ของกองทัพบกไทย

การฝึกทหารใหม่ คือ การฝึกอบรมพลทหารที่ยังไม่เคยรับราชการทหารมาก่อน ให้มีความรู้ในวิชาการทหารเบื้องต้นที่ทหารใหม่ทุกเหล่าของกองทัพบกจะต้องรู้เหมือนกันทั้งหมด คือ

๑. เพื่อปรับสภาพทางร่างกายและทางจิตใจจากการดำเนินชีวิตแบบพลเรือนมาเป็นการดำเนินชีวิตแบบทหาร ดังต่อไปนี้

๑.๑ เพื่อให้ทราบถึงคุณลักษณะและท่าทางของทหารที่จะนำไปปรับปรุงตนเองให้มีความคุ้นเคยกับชีวิตแบบทหาร กับให้เรียนรู้ถึงวิธีปฏิบัติตนเพื่อการอยู่และปฏิบัติงานร่วมกันได้อย่างมีระบบและเป็นระเบียบ

๑.๒ เพื่อให้ทราบถึงแบบธรรมเนียมของทหารที่จำเป็นจะต้องนำไปใช้ประพฤติปฏิบัติตนตลอดห้วงเวลาที่รับราชการอยู่ในกองประจำการและในขณะที่เป็นทหารกองหนุน

๑.๓ เพื่อปลูกฝังจิตใจให้มีคุณธรรมที่ดีงาม ซึ่งจะเป็นเครื่องส่งเสริมให้ทหารใหม่เป็นบุคคลที่มีคุณค่าต่อกองทัพบก มีอุดมการณ์เพื่อชาติ ศาสนา พระมหากษัตริย์และประชาชน

๑.๔ เพื่อปลูกฝังให้มีส่วนร่วมและรักษาไว้ซึ่งระบบการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์เป็นประมุข

๑.๕ เพื่อปลูกฝังให้มีกิริยามารยาทที่ดีงาม, เป็นผู้มีระเบียบวินัยและขวัญอันสูงส่ง เป็นผู้มีคุณค่าทางสังคมเป็นพลเมืองดีของประเทศชาติ และยังเป็นที่เลื่อมใสศรัทธาจากประชาชน ตลอดจนให้สามารถเป็นผู้นำของท้องถิ่นได้ เมื่อปลดออกจากกองประจำการไปแล้ว

๑.๖ เพื่อเสริมสร้างให้มีร่างกายที่สมบูรณ์แข็งแรงเป็นมาตรฐานเดียวกัน อดทนต่อการปฏิบัติงานอย่างตรากตรำและทรหด และปฏิบัติหน้าที่ต่างๆ ได้ทั้งยามสงบและยามสงคราม

๒. ฝึกฝนให้มีความรู้ในวิชาการทหารเบื้องต้นที่ทหารทุกเหล่าจำเป็นต้องรู้ในวิชาการต่างๆ ดังต่อไปนี้คือ

๒.๑ วิชาทหารทั่วไป: เพื่อให้ทหารใหม่มีความรู้ในเรื่องการติดต่อสื่อสาร รู้จักหลักและวิธีในการติดต่อสื่อสารประเภททางสายและวิทยุวิธีรับ - ส่งข่าว และการใช้ทัศนสัญญาณเสียงสัญญาณ, การข่าวเบื้องต้น มีความรู้ความเข้าใจ ในเรื่องการข่าวทางทหารให้มากพอ แก่ความจำเป็น เท่าที่พลทหารควรจะต้องทราบ และสามารถนำไปใช้ปฏิบัติงานตามหน้าที่ของตนในสนามรบได้เป็นอย่างดี รวมทั้งมีทักษะในการเป็นคนช่างสังเกตและมีทักษะเบื้องต้นในการสะกดรอย, การอ่านแผนที่และการใช้เข็มทิศให้เพียงพอที่จะนำไปปฏิบัติหน้าที่ของพลทหารได้, การปฐมพยาบาลและสุขอนามัย รู้จักขบวนการที่สำคัญ และสิ่งที่เป็นอันตรายต่อชีวิต และให้ทราบถึงแนวทางในการป้องกันและแก้ไขอันตรายที่เกิดขึ้นกับให้สามารถช่วยเหลือตนเอง และเพื่อนทหารเมื่อได้รับบาดเจ็บ

๒.๒ วิชาการใช้อาวุธ: ให้ทหารใหม่นั้นมีความรู้ในเรื่องการใช้อาวุธประจำกาย, ลูกระเบิดขว้าง, การใช้ดาบปลายปืน และการปรนนิบัติบำรุงอาวุธยุทโธปกรณ์, ทราบถึงคุณลักษณะทั่วไป การถอดประกอบ การทำงานของเครื่องกลไก การระวังรักษาและการทำความสะอาด ตลอดจนฝึกให้ทำการยิงปืนได้อย่างแม่นยำ, มีความรู้ในเรื่องคุณลักษณะและขีดความสามารถของ ลูกระเบิดขว้าง โดยเน้นให้สามารถขว้างลูกระเบิดขว้างได้อย่างแม่นยำ, ให้ทหารใหม่มีความรู้ และมีความคุ้นเคยในการใช้ดาบปลายปืนต่อสู้กับข้าศึกในระยะประชิดได้ทุกลักษณะ ทั้งนี้เป็นการการฝึก ให้ทหารใหม่รู้จักและสามารถปฏิบัติในขั้นพื้นฐานได้ โดยเน้นเพียงความแข็งแรงและความแม่นยำในการปฏิบัติ สำหรับความชำนาญและความคล่องแคล่วนั้นให้ทำการฝึกเพิ่มเติมในวิชากายบริหาร/ศิลปะการต่อสู้ป้องกันตัว

๒.๓ วิชายุทธวิธี: ให้ทหารใหม่นั้นมีความรู้เกี่ยวกับการปฏิบัติการรบเป็นบุคคลและเป็นหน่วยในเรื่องการพรางบุคคล เครื่องสนาม และยุทโธปกรณ์ รวมทั้งการเลือกใช้ที่กำบังและ การซ่อนพรางอย่างเหมาะสม เพื่อให้สามารถนำไปปฏิบัติได้เมื่ออยู่ในสนามรบ, การเรียนรู้หลักและวิธีปฏิบัติการฝึกบุคคลทำการรบในเวลากลางวันและกลางคืนเพื่อนำไปใช้เป็นพื้นฐานของการปฏิบัติการเป็นหน่วยทางยุทธวิธี, เพิ่มพูนประสิทธิภาพในการรบของทหารให้สามารถปฏิบัติการรบได้ทุกสภาพภูมิประเทศและทัศนวิสัยที่จำกัด, เสริมสร้างให้ทหารใหม่แต่ละคนเกิดความมั่นใจในตัวเองในการรบในเวลากลางคืน, มีความรู้และสามารถสร้างหลุมบุคคลได้, เรียนรู้ถึงลักษณะของเครื่องกีดขวางต่อต้านเป็นบุคคลและเครื่องกีดขวางต่อต้านยานพาหนะ พร้อมทั้งสามารถสร้างเครื่องกีดขวางลวดหนามได้, มีความรู้เกี่ยวกับการยิงปืนประกอบการเคลื่อนที่ เพื่อให้เกิดความคุ้นเคยกับอาวุธประจำกายมากยิ่งขึ้น รวมทั้งสามารถปฏิบัติการยิงปืนเป็นคู่ได้อย่างมีประสิทธิภาพ, ให้มีความรู้เกี่ยวกับหลักการลาดตระเวนเบื้องต้นและทราบหน้าที่การปฏิบัติในฐานะเป็นพลลาดตระเวน โดยเฉพาะการลาดตระเวนหาข่าวเป็นหลัก ตลอดจนฝึกให้ทหารใหม่มีจิตใจที่ไม่หวาดกลัวต่อเสียงปืน เสียงระเบิดในสนามรบจนเกิดความเชื่อมั่นในตนเอง, มีความรู้ในเรื่องการเคลื่อนที่ทางยุทธวิธีและพักแรมในสนาม โดยเฉพาะเรื่องที่ทหารใหม่จำเป็นจะต้องทราบ สามารถไปใช้ในการปฏิบัติการรบได้จริง

ความมุ่งหมายในการฝึก: เพื่อให้ทหารใหม่ในทุกเหล่าของกองทัพบกได้รับการฝึก - ศึกษาในวิชาการทหารเบื้องต้นเป็นรายบุคคล เพื่อนำไปใช้เป็นพื้นฐานในการรับการฝึกศึกษาในหลักสูตรการฝึกเบื้องสูงของแต่ละเหล่าต่อไปได้อย่างต่อเนื่อง

การจัดการฝึก: การฝึกทหารใหม่จะดำเนินการฝึกปีละ ๒ รุ่นๆ ละ ๑๐ สัปดาห์ ตามระเบียบและหลักสูตรการฝึกทหารใหม่เบื้องต้นทั่วไป สำหรับทหารทุกเหล่าของกองทัพบก (๑๐ สัปดาห์) พ.ศ.๒๕๕๑ โดยรุ่นที่ ๑ (ผลัดที่ ๑) ฝึกตั้งแต่ ๑ พฤษภาคม - กรกฎาคม และรุ่นที่ ๒ (ผลัดที่ ๒) ฝึกตั้งแต่ ๑ พฤศจิกายน - มกราคม

การเตรียมการฝึก

๑. การจัดตั้งหน่วยฝึก : การจัดตั้งหน่วยฝึกทหารใหม่มีความมุ่งหมายเพื่อให้มีคณะบุคคลคณะหนึ่งดำเนินการฝึก อบรม อำนวยการ กำกับดูแล รวมถึงการเตรียมการด้านธุรการหรืออื่นๆ ที่เกี่ยวข้องกับการฝึกทหารใหม่ให้บรรลุผลตามความมุ่งหมายของ ทบ. อันจะทำให้ทหารใหม่ทุกนายในทุกเหล่าของ ทบ. ได้รับการฝึกศึกษาวิชาการทหารเบื้องต้น ที่เป็นมาตรฐานเดียวกัน และเป็นพื้นฐานที่เหมาะสมในการฝึกศึกษาหลักสูตรการฝึกของแต่ละเหล่าต่อไปได้อย่างต่อเนื่องและมีประสิทธิภาพสูงสุดต่อไป โดยทั้งนี้ การเรียกชื่อหน่วยฝึกทหารใหม่ ให้ใช้ชื่อว่า หน่วยฝึกทหารใหม่ นามหน่วย เช่น “หน่วยฝึกทหารใหม่ มทบ.๑๒” เพื่อให้เป็นแบบอย่างเดียวกันทั้ง ทบ. การจัดตั้งหน่วยฝึกทหารใหม่ นขต.ทบ. เป็นผู้พิจารณาจัดตั้งหน่วยฝึกทหารใหม่ของหน่วยรองของตนระดับหน่วยที่รับผิดชอบการฝึกทหารใหม่ ควรเป็นหน่วยระดับกองพันหรือเทียบเท่าขึ้นไป นขต.ทบ. ที่ไม่มีหน่วยรองให้พิจารณาฝากฝึกกับหน่วยข้างเคียง ทั้งนี้เป็นไปตามวิทยุ ยศ.ทบ.ที่ กห ๐๔๖๑/๒๓๐๙ ลง ๓๐ เม.ย.๔๔ โดยหน่วยฝึกทหารใหม่จะต้องมีคุณสมบัติดังนี้

๑.๑ จำนวนทหารใหม่ใน ๑ หน่วยฝึก ต้องมีทหารใหม่จำนวน ๘๐ - ๑๖๐ นาย

๑.๒ มีพื้นที่ฝึก/สนามฝึก สนามยิงปืนของหน่วยเอง สามารถดำเนินการฝึกได้ทุกเวลา โดยไม่ต้องขอรับการสนับสนุนจากหน่วยอื่น

๑.๓ มีอาคารสถานที่ และสิ่งอำนวยความสะดวกเป็นสัดส่วน มีเอกภาพในการควบคุมบังคับบัญชาและต้องได้ตามเกณฑ์มาตรฐานตามคำสั่ง ทบ. ที่ ๖๕/๒๕๔๒ ลง ๓ ก.พ.๔๒ เรื่อง การพัฒนาคุณภาพชีวิตทหารกองประจำการ

๑.๔ มีเครื่องช่วยฝึกเพียงพอและเหมาะสมต่อจำนวนทหารใหม่ที่รับการฝึก

๑.๕ หน่วยฝึกที่ได้รับการจัดตั้งจะต้องดำเนินการฝึกครูทหารใหม่ และทหารใหม่ทั้งสองผลัด คือ ผลัดที่ ๒ และ ผลัดที่ ๑ โดยไม่เปลี่ยนแปลงหน่วยฝึก เว้นในปีงบประมาณต่อไป

๒. ผู้บังคับหน่วยทุกระดับชั้น : จะต้องให้ความสำคัญต่อการฝึกทหารใหม่ตั้งแต่การมอบนโยบายการฝึกทหารใหม่, การเตรียมการฝึก, การดำเนินการฝึก ตลอดจนการสนับสนุนอาวุธยุทโธปกรณ์เครื่องช่วยฝึก และทรัพยากรในการฝึก รวมทั้งต้องทำการตรวจและกำกับดูแลการฝึกอย่างต่อเนื่องสม่ำเสมอ ทั้งนี้หน่วยฝึกทหารใหม่จะต้องรวบรวมนโยบายการฝึกทหารใหม่แต่ละระดับและนำมาใช้เป็นแนวทางในการฝึก เพื่อให้การฝึกทหารใหม่ของหน่วยเป็นไปอย่างมีประสิทธิภาพ

๓. เจ้าหน้าที่ในหน่วยฝึกทหารใหม่ : ประกอบด้วย ผบ.หน่วยฝึก เจ้าหน้าที่ธุรการประจำหน่วยฝึก ผู้ฝึก ผู้ช่วยผู้ฝึก ครูนายสิบ และครูทหารใหม่

๓.๑ ผบ.หน่วยฝึก : จัดจากนายทหารชั้นสัญญาบัตรภายในหน่วยที่มีอาวุโสด้วยคุณวุฒิ โดยปกติแล้วควรจะเป็นผู้บังคับกองร้อยหรือบุคคลที่มียศสูงกว่าผู้ฝึกฯ โดยมีหน้าที่ อำนวยการ และกำกับดูแลให้การฝึกเป็นไปตามความมุ่งหมาย และเจตนารมณ์ของหน่วย และดำเนินการด้านธุรการ การสนับสนุนสิ่งอุปกรณ์ต่างๆ รวมถึงการจัดเตรียมสิ่งอุปกรณ์, เครื่องช่วยฝึก และสนามฝึก เพื่อให้การฝึกมีประสิทธิภาพสูงสุด

๓.๒ เจ้าหน้าที่ธุรการประจำหน่วยฝึก : จัดจากกำลังพลภายในหน่วย จัดขึ้นเพื่อช่วยเหลือ และเป็นลูกมือให้กับ ผบ.หน่วยฝึก ในการปฏิบัติงานด้านธุรการและการสนับสนุนการฝึกทหารใหม่ รวมถึงงานการบริการและการรักษาความปลอดภัยด้วย

๓.๓ ผู้ฝึก : จัดจาก ผบ.มว.อาวุโสที่มีประสบการณ์ในการฝึก หรืออย่างน้อยได้ผ่านการทำหน้าที่เป็นผู้ช่วยผู้ฝึกมาแล้ว มีหน้าที่เป็นผู้รับผิดชอบการฝึก และทำหน้าที่ปกครองทหารใหม่ พร้อมๆ กันไปด้วย

๓.๔ ผู้ช่วยผู้ฝึก : จัดจาก ผบ.มว. ที่มีอาวุโสต่ำกว่าผู้ฝึก หรือ จ.ส.อ. อาวุโสที่มีประสบการณ์ในด้านการฝึกทหารใหม่มาแล้ว โดยให้จัดตามความเหมาะสมอย่างน้อย ๑ นาย

๓.๕ ครูนายสิบ : จัดจากนายสิบที่มีความรู้ ความสามารถ มีลักษณะท่าทางที่ดี เพื่อทำหน้าที่ฝึกสอนตามวิชาที่ได้รับมอบ และดูแลทหารใหม่อย่างใกล้ชิด โดยให้จัดครูนายสิบ ๑ นาย ต่อครูทหารใหม่ ๑ นาย เช่น ครูทหารใหม่ทั้งสิ้น จำนวน ๑๕ นาย ให้จัดครูนายสิบจำนวน ๑๕ นาย ด้วยเช่นกัน (ยอดครูนายสิบจะไม่รวมยอดอะไหล่ร้อยละ ๒๐ ของจำนวนครูทหารใหม่)

๓.๖ ครูทหารใหม่ : จัดจากพลทหารที่สำเร็จการฝึกหลักสูตรครูทหารใหม่ เพื่อทำหน้าที่ช่วยเหลือ ครูนายสิบ โดยจำนวนครูทหารใหม่ให้ถือเกณฑ์ จำนวนทหารใหม่ ๘ นาย ต่อครูทหารใหม่ ๑ นาย เศษให้ตัดทิ้งและให้มียอดอะไหล่ร้อยละ ๒๐ ของจำนวนครูทหารใหม่ของหน่วย

๔. คุณลักษณะพึงประสงค์ของ ผู้ฝึก, ครูนายสิบ และครูทหารใหม่

๔.๑ ผู้ฝึก

๔.๑.๑ มีลักษณะทหารที่ดี และความประพฤติเรียบร้อยอยู่ในระเบียบวินัยอย่างเคร่งครัด

๔.๑.๒ การแต่งกายเรียบร้อยถูกต้องตามระเบียบและเหมาะสมตามกาลเทศะ

๔.๑.๓ มีความรู้ความสามารถและกระตือรือร้นในการฝึก

๔.๑.๔ มีความมุ่งมั่น จริงจัง จริงใจ ตั้งใจในการฝึก

๔.๑.๕ มีการควบคุมบังคับบัญชาครูฝึก อย่างแน่นแฟ้น คุ้นเคย และเป็นอันหนึ่งอันเดียวกัน

๔.๑.๖ อยู่ใกล้ชิดทหารใหม่ตลอดเวลา ดูแลทุกข์สุขของทหารใหม่อย่างทั่วถึง เอาใจใส่ต่อการเจ็บป่วยของทหารใหม่

๔.๑.๗ มีการเตรียมการในเรื่องที่จะฝึกสอนเป็นอย่างดีและพร้อมที่จะแก้ไขปัญหาข้อขัดข้องต่าง ๆ ให้ลุล่วงไปด้วยดีได้

๔.๑.๘ มีความเข้าใจในแนวทางการฝึกที่มุ่งเน้นผลการปฏิบัติ

๔.๑.๙ เป็นตัวอย่างที่ดีแก่ครูนายสิบ, ครูทหารใหม่และทหารใหม่ได้เป็นอย่างดีในทุกๆ เรื่อง

๔.๒ ผู้ช่วยผู้ฝึก, ครูนายสิบ และครูทหารใหม่ มีคุณลักษณะเช่นเดียวกับผู้ฝึก

๕. การจัดเตรียมเครื่องช่วยฝึก, แผ่นภาพเครื่องช่วยฝึกและอุปกรณ์การฝึก: หน่วยฝึกทหารใหม่ จะต้องเบิก - รับเครื่องช่วยฝึก, แผ่นภาพเครื่องช่วยฝึก และอุปกรณ์การฝึกให้เรียบร้อยก่อนดำเนินการฝึก โดยให้ปฏิบัติดังนี้

๕.๑ เตรียมไว้ให้เพียงพอกับการใช้ในการฝึกทหารใหม่ ทุกวิชา ทุกเรื่อง

๕.๒ ตรวจสภาพให้เรียบร้อย มีการเก็บรักษาที่เหมาะสม และมีการซ่อมบำรุงให้พร้อมใช้งาน

๕.๓ มีบัญชีคุมและสมุดยืมเรียบร้อย

๕.๔ นำมาใช้ให้เกิดประโยชน์อย่างแท้จริงโดยนำมาใช้ประกอบการฝึกหรือสอนทุกครั้ง

๖. พื้นที่การฝึกและสนามฝึกต่างๆ หน่วยฝึกทหารใหม่จะต้องเตรียมไว้ให้อยู่ในสภาพที่เรียบร้อย พร้อมทำการฝึก และมีความปลอดภัยเมื่อใช้ทำการฝึก สนามฝึกที่ใช้ทำการฝึกทหารใหม่ มีดังนี้

๖.๑ สนามฝึกบุคคลเบื้องต้น และแถวชิด ควรเป็นสนามหญ้า พื้นเรียบมีแท่นสูงสำหรับผู้ฝึก สามารถรองรับทหารใหม่ขณะทำการฝึกได้เพียงพอ การฝึกท่าอยู่กับที่และการฝึกท่าเคลื่อนที่ต่างๆ รวมถึงการฝึกแบบรวมการได้ทั้งหน่วยฝึก

๖.๒ สนามฝึกกายบริหาร

๖.๒.๑ กายบริหารอยู่กับที่ เป็นลานพื้นเรียบ มีแท่นสูงสำหรับผู้ฝึก พื้นที่เพียงพอสำหรับการขยายระยะต่อและระยะเคียงของทหารใหม่ทั้งหน่วยฝึกได้ดี

๖.๒.๒ ราวดึงข้อ มีการยึดตรึง แข็งแรง และเกิดความปลอดภัยขณะปฏิบัติ

๖.๒.๓ สนามฝึกวิ่ง มีระยะทางรวม ๒,๐๐๐ เมตร ขนาดความกว้างเพียงพอ และการจราจร ไม่พลุกพล่าน

๖.๓ สนามฝึกยิงปืนเบื้องต้น ตั้งอยู่ในที่โล่งได้ระยะตามคู่มือการฝึก (แบบวงกลมหรือ แบบคู่ขนาน)

๖.๔ สนามฝึกทางยุทธวิธี ให้เลือกพื้นที่และภูมิประเทศที่สามารถทำการฝึกได้เหมาะสมกับ ภูมิประเทศในการรบ ให้มีความกว้าง และความลึกในระดับหมู่ปืนเล็กลักษณะการวางเครื่องกีดขวางให้วางสลับ มิใช่วางเป็นแถวตรงกัน ป้อมสนาม และหลุม

บุคคล ควรอยู่ในพื้นที่ที่ต้องมีการปกปิดกำบัง และซ่อนพราง การดัดแปลงภูมิประเทศต่าง ๆ ให้คำนึงถึงความเหมาะสมในการฝึกให้เกิดความเข้าใจ เมื่อต้องนำไปใช้ปฏิบัติทางยุทธวิธี และหน่วยต้องจัดทำโต๊ะทรายหรือภูมิประเทศจำลอง อธิบายให้ทหารใหม่เข้าใจภาพการปฏิบัติทางยุทธวิธีในระดับ บุคคล, คู่บัดดี้, ชุดยิง และหมู่

๖.๕ สนามฝึกยิงปืนระยะ ๒๕ เมตร (๑,๐๐๐ นิ้ว) เน้นความปลอดภัยของสนามฝึกยิงปืนและบริเวณโดยรอบขณะทำการฝึก ช่องยิง แนวยิง และเป้าต้องมีความสมบูรณ์พร้อมใช้งาน รวมทั้งหน่วยต้องกำหนดให้มีมาตรการรักษาความปลอดภัยในการใช้สนามฝึกดังกล่าวด้วย

๖.๖ สนามฝึกขว้างลูกระเบิด ต้องอยู่ในที่โล่ง รูปแบบตามคู่มือการฝึกฯ

๖.๗ สนามฝึกการใช้ดาบปลายปืนตั้งอยู่ในพื้นที่ที่สามารถทำการฝึกได้อย่างเหมาะสม ตามระยะที่กำหนด และต้องตรวจสอบเครื่องช่วยฝึกให้ใช้งานได้ และมีความปลอดภัยอยู่ตลอดเวลา

๖.๘ สนามฝึกเดินทางด้วยเข็มทิศ ลักษณะพื้นที่เป็นป่าโปร่ง ควรอยู่แยกต่างหากจากสนามฝึกอื่นๆ

๖.๙ สนามฝึกบุคคลทำการรบ ให้สามารถทำการฝึกได้ทั้งเวลากลางวันและกลางคืน มีความเหมาะสมใกล้เคียงกับความเป็นจริงของการรบให้มากที่สุด หากมีการดัดแปลงภูมิประเทศต้องให้มีความสมจริง

๖.๑๐ สนามฝึกสร้างเครื่องกีดขวาง ให้มีภูมิลักษณะประเทศที่เหมาะสมสำหรับเป็นการรั้งหน่วง หยุดการเคลื่อนที่ของข้าศึก

๖.๑๑ พื้นที่การฝึกลาดตระเวน ให้พิจารณาภูมิประเทศที่มีทั้งที่โล่งแจ้ง, ป่าเขา, ลำธารและเส้นทาง สามารถทำการฝึกได้ทั้งเวลากลางวันและกลางคืน

๖.๑๒ พื้นที่การฝึกป้อมสนามควรมีระยะที่สามารถปฏิบัติในระดับหมู่ ปล.ได้ เมื่อดัดแปลงภูมิประเทศแล้ว ต้องกลมกลืนกับสภาพแวดล้อมในพื้นที่นั้นๆ

๖.๑๓ พื้นที่การฝึกเคลื่อนที่ทางยุทธวิธีและการพักแรมในสนาม เป็นพื้นที่ที่ห่างจากหน่วยประมาณ ๔ ชม. และมีความพร้อมสำหรับการค้างแรมในสนาม เช่น แหล่งน้ำ เส้นทางส่งกำลังบำรุง เป็นต้น

การฝึกครูทหารใหม่ จำนวน ๔ สัปดาห์ (๑๖๐ ชม.) มีวัตถุประสงค์ของการฝึกครูทหารใหม่

๑. เพื่อเสริมสร้างความรู้และฟื้นฟูวิชาทหารที่จำเป็นที่ได้รับการฝึกศึกษาไปแล้วตามระเบียบและหลักสูตรการฝึกทหารใหม่ และการฝึกเฉพาะหน้าที่ของแต่ละเหล่า ตลอดจนอบรมลักษณะแห่งการเป็นผู้นำให้แก่ผู้ที่จะทำหน้าที่ครูทหารใหม่ ให้มีความรู้ความชำนาญในการฝึกการนำทหาร และการสอน พร้อมที่จะเป็นผู้วางรากฐานพื้นความรู้วิชาทหารให้แก่ทหารใหม่ นับตั้งแต่โอกาสแรกที่ทหารใหม่ได้รับการฝึก

๒. เพื่อให้มีความสามารถในการทำหน้าที่ครูทหารใหม่ ในการฝึกสอนวิชาการต่างๆ ที่จะต้องทำการฝึกในสนามฝึกตามขอบเขตวิชาที่กำหนดไว้ในระเบียบและหลักสูตรการฝึกทหารใหม่

๓. เพื่อให้มีขีดความสามารถในการทำหน้าที่ครูทหารใหม่ สำหรับการสอนอบรมเป็นบางวิชาในห้องเรียนได้

๔. เพื่อเป็นการเพิ่มคุณวุฒิพลทหารกองประจำการให้ครบถ้วน ก่อนที่จะได้รับการคัดเลือกตัวส่งเข้าฝึกอบรมต่อไปในหลักสูตรการฝึกสิบตรีกองประจำการ

๕. เพื่อปลูกฝังให้เป็นบุคคลที่เคร่งครัดในระเบียบวินัยทหาร และมีความประพฤติเรียบร้อย เพื่อเป็นแบบอย่างแก่ทหารใหม่ได้

๖. เพื่อทำหน้าที่เป็นพี่เลี้ยงแก่ทหารใหม่ตามความจำเป็น

เรื่องที่ทหารใหม่ต้องทำการฝึก

สถานีที่ ๑ : การทดสอบความสมบูรณ์แข็งแรงทางร่างกาย
- ท่าดึงข้อ
- ท่าลุก-นั่ง
- ท่าดันพื้น
- การวิ่งระยะทาง ๒ กม.

สถานีที่ ๒ : การฝึกบุคคลท่าเบื้องต้น
- การฝึกบุคคลท่ามือเปล่า
- การฝึกบุคคลท่าอาวุธ
- การฝึกแถวชิด
- การสวนสนาม

สถานีที่ ๓ : การใช้อาวุธประจำกาย
- อาวุธศึกษาของอาวุธประจำกายหลัก
- การปรนนิบัติบำรุงอาวุธ ซองกระสุน และการทำความสะอาดกระสุน
- การแก้ไขโดยฉับพลัน เมื่อเกิดการติดขัดของ ปลย. ขณะทำการยิง
- การบรรจุกระสุนใส่ลงในซองกระสุน และการนำกระสุนออกจากซองกระสุน
- การปรับและจัดศูนย์และการรมศูนย์
- การจัดภาพศูนย์พอดีและการจัดภาพการเล็ง
- การใช้คานเล็ง
- การเล็ง ๓ จุด
- การถอดอาวุธประจำกาย การปรนนิบัติบำรุง และการประกอบอาวุธประจำกาย
- ท่ายิง, การบรรจุ, การลั่นไก และเลิกบรรจุ
- การใช้ลูกระเบิดขว้าง

สถานีที่ ๔ : การยิงปืนด้วยกระสุนจริง
- การนอนยิง
- การนั่งราบยิง
- การนั่งสูงยิง
- การนั่งคุกเข่ายิง
- การยืนยิง

สถานีที่ ๕ : วิชาทหารทั่วไปและการฝึกทางยุทธวิธี
- การติดต่อสื่อสาร
- การอ่านแผนที่และการใช้เข็มทิศ
- การปฐมพยาบาลและสุขวิทยาอนามัย
- การข่าวเบื้องต้น/การสังเกตและการสะกดรอย
- การป้องกันนิวเคลียร์ ชีวะ และเคมีเป็นบุคคล
- การฝึกบุคคลทำการรบในเวลากลางวัน
- การฝึกบุคคลทำการรบในเวลากลางคืน
- การกำบังและการซ่อนพราง
- ป้อมสนาม
- เครื่องกีดขวาง
- การยิงประกอบการเคลื่อนที่เป็นคู่
- การลาดตระเวน/การระวังป้องกัน
- การเคลื่อนที่ทางยุทธวิธีและการพักแรมในสนาม

สถานีที่ ๖ : การสอนอบรม
- คุณลักษณะของทหาร
- แบบธรรมเนียมทหาร
- คุณธรรมของทหาร
- มารยาทและวินัยทหาร
- หน้าที่พลเมืองดี
- ความรักและการป้องกันประเทศชาติ
- การปกครองระบอบประชาธิปไตย
- สถาบันพระมหากษัตริย์ไทย
- การเสริมสร้างอุดมการณ์ความรักชาติ
- รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๕๐
- ประวัติศาสตร์ชาติไทย
- เศรษฐกิจพอเพียง
- ค่านิยม ๑๒ ประการ

ระเบียบประจำวันของทหารใหม่ : เวลาในการฝึกสัปดาห์ละ ๔๕ ชั่วโมง

๑. กำหนดการฝึกประจำวัน

๑.๑ วันจันทร์ - วันพฤหัสบดี

๐๕๓๐	ตื่นนอน
๐๖๐๐ - ๐๗๐๐	ออกกำลังกาย
๐๗๐๐	รับประทานอาหาร
๐๘๐๐	เคารพธงชาติ
๐๘๐๐ - ๑๒๐๐	การฝึกประจำวัน (๔ ชม.)
๑๒๐๐	รับประทานอาหาร
๑๓๐๐ - ๑๖๐๐	การฝึกประจำวัน (๓ ชม.)
๑๖๐๐ - ๑๗๐๐	กายบริหาร (๑ ชม.)
๑๗๐๐ - ๑๘๐๐	กีฬา
๑๘๐๐	เคารพธงชาติ/รับประทานอาหาร
๑๙๐๐ - ๒๐๐๐	การสอนอบรม (๑ ชม.)
๒๐๓๐	สวดมนต์
๒๑๐๐	นอน

๑.๒ วันศุกร์

๐๕๓๐	ตื่นนอน
๐๖๐๐ - ๐๗๐๐	ออกกำลังกาย
๐๗๐๐	รับประทานอาหาร
๐๘๐๐	เคารพธงชาติ
๐๘๐๐ - ๑๒๐๐	การฝึกประจำวัน (๔ ชม.)
๑๒๐๐	รับประทานอาหาร
๑๓๐๐ - ๑๕๐๐	การฝึกประจำวัน (๒ ชม.)
๑๕๐๐ - ๑๗๐๐	การทดสอบสมรรถภาพร่างกาย (๒ ชม.)
๑๗๐๐ - ๑๘๐๐	กีฬา
๑๘๐๐	เคารพธงชาติ/รับประทานอาหาร
๑๙๐๐ - ๒๐๐๐	การอบรม (๑ ชม.)
๒๐๓๐	สวดมนต์
๒๑๐๐	นอน

๑.๓ วันเสาร์

๐๘๐๐ - ๑๐๐๐	การปรนนิบัติบำรุงอาวุธยุทโธปกรณ์, คลัง, อาคารและที่พัก
๑๐๐๐ - ๑๒๐๐	เวลาผู้บังคับบัญชา

เอกสารวิจัยที่เกี่ยวข้อง

จากการศึกษาเอกสารวิจัยส่วนบุคคลของ พลตำรวจโท เดชณรงค์ สุทธิชาญบัญชา และคณะ ซึ่งทำการศึกษาเรื่อง แนวทางการพัฒนาการฝึกของกองทัพไทยกับประเทศสมาชิกอาเซียนต่อภัยคุกคามรูปแบบใหม่ (เดชณรงค์ สุทธิชาญบัญชา, ๒๕๕๕: ๑๐๗-๑๐๘) พบว่า

๑. บทบาท และความร่วมมือระหว่างกองทัพไทยกับกองทัพประเทศสมาชิกอาเซียนด้านการฝึกผสม และการฝึกร่วมและผสมในด้านภัยคุกคามรูปแบบใหม่นั้น มีความร่วมมือในด้านการปฏิบัติการช่วยเหลือด้านมนุษยธรรม และการบรรเทาภัยพิบัติที่เกิดจากการเปลี่ยนแปลงสภาพแวดล้อมทางธรรมชาติเป็นหลัก นอกจากนั้นยังมีด้านการก่อการร้าย และอาชญากรรมข้ามชาติ สอดแทรกบ้าง และรูปแบบของการฝึกต่อภัยคุกคามรูปแบบใหม่ควรจะต้องมีการดำเนินการในกรอบความร่วมมือ ๖ ด้าน ได้แก่ การให้ความช่วยเหลือด้านมนุษยธรรม และการบรรเทาภัยพิบัติความมั่นคงทางทะเล การปฏิบัติการรักษาสันติภาพ การต่อต้านการก่อการร้าย การแพทย์ทางทหาร และการปฏิบัติการทุ่นระเบิดเพื่อมนุษยธรรม ซึ่งภัยคุกคามรูปแบบใหม่ที่ยังไม่ได้กล่าวถึงก็ยังมีอีกหลายรายการ เช่น การค้ามนุษย์ อาชญากรรมข้ามชาติ การฟอกเงิน ยาเสพติด สิ่งแวดล้อม เป็นต้น ซึ่งความร่วมมือเหล่านี้ยังมีความร่วมมือด้านการฝึกไม่ชัดเจนเหมือนอย่างความร่วมมือทั้ง ๖ ด้านที่กล่าวมาแล้ว

๒. บทบาท และรูปแบบการฝึกของกองทัพไทยกับกองทัพประเทศสมาชิกอาเซียนต่อภัยคุกคามรูปแบบใหม่ที่ผ่านมา อาจจะไม่ได้มีการเน้นในเรื่องภัยคุกคามรูปแบบใหม่มากนักแต่จะเน้นภัยคุกคามรูปแบบดั้งเดิม ต่อมาจึงมีการให้ความสำคัญในเรื่องการปฏิบัติการเพื่อสันติภาพ การต่อต้านการก่อการร้าย ความมั่นคงทางทะเล การให้ความช่วยเหลือด้านมนุษยธรรม และการบรรเทาภัยพิบัติรวมทั้งการแพทย์ทหารมากขึ้น ดังนั้น บทบาทกองทัพไทยกับกองทัพประเทศสมาชิกอาเซียนในด้านการฝึกจะเป็นความร่วมมือในลักษณะพหุภาคีเป็นหลัก คือ มีจำนวนประเทศ ที่เข้าร่วมการฝึกจำนวนหลายชาติ ตามความพร้อมในเรื่องงบประมาณ และความชำนาญของแต่ละชาติ ซึ่งแตกต่างจากเดิมที่เป็นความร่วมมือแบบทวิภาคีที่มีชาติร่วมการฝึกเพียงสองชาติเท่านั้น และรูปแบบการฝึกจะประกอบด้วยการฝึกปัญหาที่บังคับการ (CPX) หรือการฝึกแก้ปัญหาบนโต๊ะ (Table Top Exercise) และการฝึกภาคสนาม (FTX) ดังนั้น กองทัพไทยจะต้องมีการเตรียม ความพร้อมของกำลังพลที่จะเข้าร่วมการฝึกกับมิตรประเทศต่าง ๆ ให้มีความพร้อมทางวิชาการ และการปฏิบัติในแต่ละเรื่องจนมีความชำนาญ โดยเฉพาะในเรื่องการปฏิบัติการช่วยเหลือด้านมนุษยธรรมและการบรรเทาภัยพิบัติ

๓. การจัดทำแนวทางการพัฒนาการฝึกของกองทัพไทยกับกองทัพประเทศอาเซียนต่อภัยคุกคามรูปแบบใหม่ ควรจะต้องมีการฝึกร่วมกันอย่างสม่ำเสมอเพื่อสร้างความคุ้นเคย มีการจัดทำคู่มือการใช้งานร่วมกันโดยมีลักษณะการพัฒนาอย่างค่อยเป็นค่อยไป เพื่อสร้างความยอมรับร่วมกันในเรื่องหลักนิยม คู่มือ และระเบียบปฏิบัติ

ที่แตกต่างกัน ซึ่งกองทัพไทยควรต้องมีการปรับปรุงการจัดหน่วย และยุทโธปกรณ์ให้สามารถรองรับความร่วมมือตามกรอบทั้ง ๖ ด้าน

จากการศึกษาเอกสารวิจัยส่วนบุคคลของ พลตรี ณฐพนธ์ ศรีสวัสดิ์

ซึ่งทำการศึกษาเรื่อง การพัฒนาบุคลากรของกองทัพและภาครัฐ เพื่อเอาชนะปัญหาภัยคุกคามต่อความมั่นคงของชาติ (ณฐพนธ์ ศรีสวัสดิ์, ๒๕๕๗: ๗๓-๗๗) พบว่า

การเปลี่ยนแปลงในยุคโลกาภิวัตน์เป็นปัจจัยหลักที่ทำให้ปัญหาภัยคุกคามซึ่งเกิดจากฝีมือของมนุษย์ มีการพัฒนารูปแบบไปอย่างซับซ้อน พลิกผัน และสามารถก่อขยายตัวลุกลามไปได้อย่างรวดเร็ว ภัยคุกคามที่เกิดขึ้นได้เปลี่ยนแปลงไปจากเดิมอย่างกว้างขวาง และรวดเร็ว ตามการปรับตัวของสังคมในยุคโลกาภิวัตน์ ซึ่งภัยคุกคามที่ประเทศชาติกำลังเผชิญอยู่นับวันจะมีความเข้มแข็ง ทันสมัย มีนวัตกรรมเป็นเครือข่ายทางสังคมที่ทรงอิทธิพล และมีเสรีสูงในการเคลื่อนไหว ในขณะที่องค์กรฝ่ายความมั่นคงของไทยยังคงมีอุปสรรค และข้อจำกัดในการรับมือด้วยหลายปัจจัย และแม้ว่าจะมีจุดแข็งที่มาจากพื้นฐานการเป็นองค์กรของรัฐที่มีระเบียบแบบแผนสืบสานมายาวนาน แต่การมีจุดอ่อนและอุปสรรคมากมายกลับกลายเป็นความล่อแหลม สร้างผลกระทบและฉุดรั้งความมีประสิทธิภาพขององค์กรในทุกๆ ด้าน ได้แก่

๑. การบริหารจัดการกำลังพลภาครัฐที่ขาดหลักธรรมาภิบาล ทำให้บุคลากรที่มีความรู้ ความสามารถ และประสบการณ์ไม่มีหลักประกันความสำเร็จ และความก้าวหน้าในอาชีพการงาน ส่งผลเสียต่อการทำงาน และการตัดสินใจ ไม่แก้ปัญหาตามหลักการและไม่ตอบสนองเป้าหมายของส่วนรวม รวมทั้งยังเกิดการสืบสานวัฒนธรรมที่บกพร่องต่อไปยังอนุชนรุ่นหลัง

๒. การที่เจ้าหน้าที่ฝ่ายความมั่นคงเองเข้าไปมีส่วนเกี่ยวข้องในขบวนการภัยคุกคามรูปแบบต่างๆ ตั้งแต่ต้นทาง กลางทาง และปลายทาง ซึ่งบางส่วนมีความผูกพันกันโดยสังคม วัฒนธรรมที่ต้องพึ่งพากัน หรือการพึ่งพิงอำนาจบารมีเพื่อความอยู่รอด

๓. การตกอยู่ในวงการทุจริตและประพฤติมิชอบในวงราชการทั้งที่ตั้งใจ และไม่ตั้งใจ รวมไปถึงการติดกับดักทางวัฒนธรรมที่ต้องแสวงหาความมีฐานะ และบารมีจากช่องทางหรือโอกาสที่เปิดต่างๆ

๔. การขาดการปรับตัวของบุคลากร และองค์กรทำให้ไม่สามารถเผชิญกับการเปลี่ยนแปลงของยุคสมัย ซึ่งมาจากหลายสาเหตุ อาทิ การมีค่านิยมในการสร้างและแสดงภาพลักษณ์ความสำเร็จของบุคคลให้โดดเด่นมากกว่าการสร้างผลงานเชิงคุณภาพ การไม่เห็นแก่เป้าหมาย และผลประโยชน์ของส่วนรวมเป็นที่ตั้ง การขาดการพัฒนาและใช้องค์ความรู้ขององค์กร และการขาดการพัฒนาคุณภาพ ประสิทธิภาพในการปฏิบัติงานร่วมกัน รวมไปถึงการขาดความคิดเชิงบูรณาการ และการปฏิบัติงานเชิงรุก ซึ่งสิ่งเหล่านี้เป็นปัจจัยสำคัญยิ่งที่จะเป็นอุปสรรค และข้อจำกัดในการปรับตัวให้ทันต่อการเปลี่ยนแปลงที่จะมีมาในอนาคต

๕. การขาดการจัดการด้านทรัพยากรมนุษย์ โดยเฉพาะระดับเจ้าหน้าที่ปฏิบัติการและผู้เชี่ยวชาญเฉพาะทางในสาขาที่มีความจำเป็นต่องานด้านความมั่นคง ซึ่งปัจจุบันแต่ละหน่วยงาน ต่างประสบปัญหาขาดแคลนบุคลากรสำคัญกันทุกหน่วยงาน แต่ก็ยังมุ่งปฏิบัติภารกิจหน้าที่ของตนเอง และมาตรฐานขององค์กรตนเองต่อไป เพื่อให้บรรลุผลสำเร็จภายใต้ทรัพยากรที่มีอยู่เป็นหลัก โดยไม่คำนึงถึงหรือไม่มีแนวคิด และใช้กำลังอำนาจโดยรวมที่จะจัดการปัญหาความขาดแคลนเหล่านั้น

จากการศึกษาเอกสารวิจัยส่วนบุคคลของ ธนาวรรณ จันทรัตนไพบูลย์และอัจกิต อุฒาธรรม ซึ่งทำการศึกษาเรื่อง การวิเคราะห์ปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในองค์กรของประเทศไทย (วารสารวิชาการพระจอมเกล้าพระนครเหนือ, ปีที่ ๒๓ ฉบับที่ ๓ ก.ย.-ธ.ค. ๒๕๕๖: ๖๙๖ - ๗๐๕) พบว่า

ปัจจัยที่ได้จากการศึกษามี ๒๔ ปัจจัย ได้แก่

๑. การป้องกันในระบบเครือข่าย
๒. การอัพเดทระบบป้องกัน
๓. อายุการใช้งานฮาร์ดแวร์
๔. สภาพแวดล้อมของฮาร์ดแวร์
๕. จำนวนเครื่องเซฟเวอร์
๖. การป้องกันการเข้าถึงไฟล์ข้อมูล
๗. การแบ็คอัพข้อมูล
๘. ความขัดแย้งภายในองค์กร
๙. ความใส่ใจความปลอดภัย
๑๐. ขาดผู้เชี่ยวชาญ
๑๑. การตั้งรหัสคอมพิวเตอร์
๑๒. การใช้คอมพิวเตอร์ร่วมกัน
๑๓. มีการเปิดเผยรหัสผ่าน
๑๔. เก็บรักษารหัสไม่ดีพอ
๑๕. สั่งงานผ่านอีเมล์ส่วนตัว
๑๖. การอบรมความปลอดภัย
๑๗. อายุขององค์กร
๑๘. นโยบายความปลอดภัย
๑๙. บทลงโทษ
๒๐. การแบ่งหน้าที่การทำงาน
๒๑. งบประมาณ
๒๒. ขาดการสนับสนุน
๒๓. การใช้เอาท์ซอส
๒๔. ระบบที่ใช้บริการไม่มีคุณภาพ เช่น ไฟฟ้าอินเทอร์เน็ต

จากปัจจัยทั้ง ๒๔ ปัจจัยจะนำไปเข้าสู่กระบวนการวิเคราะห์องค์ประกอบเพื่อนำไปใช้ในการวิเคราะห์ เพื่อสร้างโมเดลทำนายความเสี่ยงต่อไป

จากการศึกษาเอกสารวิจัยส่วนบุคคลของ อัจกิต อุฌาธรรม ซึ่งทำการศึกษาเรื่อง การวิเคราะห์หาปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในประเทศไทย (อัจกิต อุฌาธรรม, ๒๕๕๕) พบว่า

การศึกษาและสำรวจปัจจัยทั้งหมด ๒๔ ปัจจัยและจากการวิเคราะห์ได้โมเดลที่สามารถทำนายการเกิดภัยคุกคาม ๗ ประเภทด้วยกัน ซึ่งได้แก่

๑. ความผิดพลาดที่มาจากมนุษย์

๒. การบุกรุก

๓. การกรรโชกข้อมูล

๔. การทำลายระบบหรือข้อมูล

๕. การโจรกรรม

๖. การโจมตีจากซอฟต์แวร์

๗. ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ โดยมีนัยสำคัญเป็น ๐.๐๕ ผลการทดสอบพบว่า โมเดลมีความสอดคล้องกับปัจจัยที่กล่าวมาข้างต้น

จากการศึกษาเอกสารวิจัยส่วนบุคคลของ ศิวลีย์ สิริโรจน์บริรักษ์ ซึ่งทำการศึกษาเรื่อง การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม (วารสารสถาบันวิชาการป้องกันประเทศ ปีที่ ๖ ฉบับที่ ๓, ๒๕๕๘ : ๑๙ - ๒๙) พบว่า

๑. กรอบนโยบาย ยุทธศาสตร์ และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ได้แก่ พ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม พ.ศ.๒๕๕๑, นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.๒๕๕๔, ยุทธศาสตร์กระทรวงกลาโหมอิเล็กทรอนิกส์ (e-defence), แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม ฉบับที่ ๓ พ.ศ.๒๕๕๗-๒๕๖๑, การจัดตั้งศูนย์บัญชาการไซเบอร์ กระทรวงกลาโหม

๒. มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO ๒๗๐๐๑: ๒๐๐๕, มาตรฐาน FIPS PUB ๒๐๐, มาตรฐาน NIST ๘๐๐-๑๔, มาตรฐาน COBIT, และมาตรฐาน IT BPM

๓. แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ให้ได้มาตรฐานในระดับสากลเชิงนโยบาย ได้แก่ ส่วนบังคับการต้องเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร เพื่อดำเนินการตอบสนองต่อปัญหา/ เหตุการณ์บุกรุกระบบของหน่วยขึ้นตรงได้อย่างรวดเร็ว ส่วนนโยบายและแผนต้องมีการบรรจุข้อกำหนดในกระบวนการจัดซื้อจัดจ้าสง อุปกรณ์ฮาร์ดแวร์/ ซอฟต์แวร์ เพื่อให้อุปกรณ์มีความปลอดภัยในระดับสากล ส่วนปฏิบัติการไซเบอร์จะต้องมีหน่วยปฏิบัติการเชิงรับส่งข้อมูลข่าวสารส่วนวิจัยและพัฒนาไซเบอร์จะต้องจัดตั้งส่วนงาน

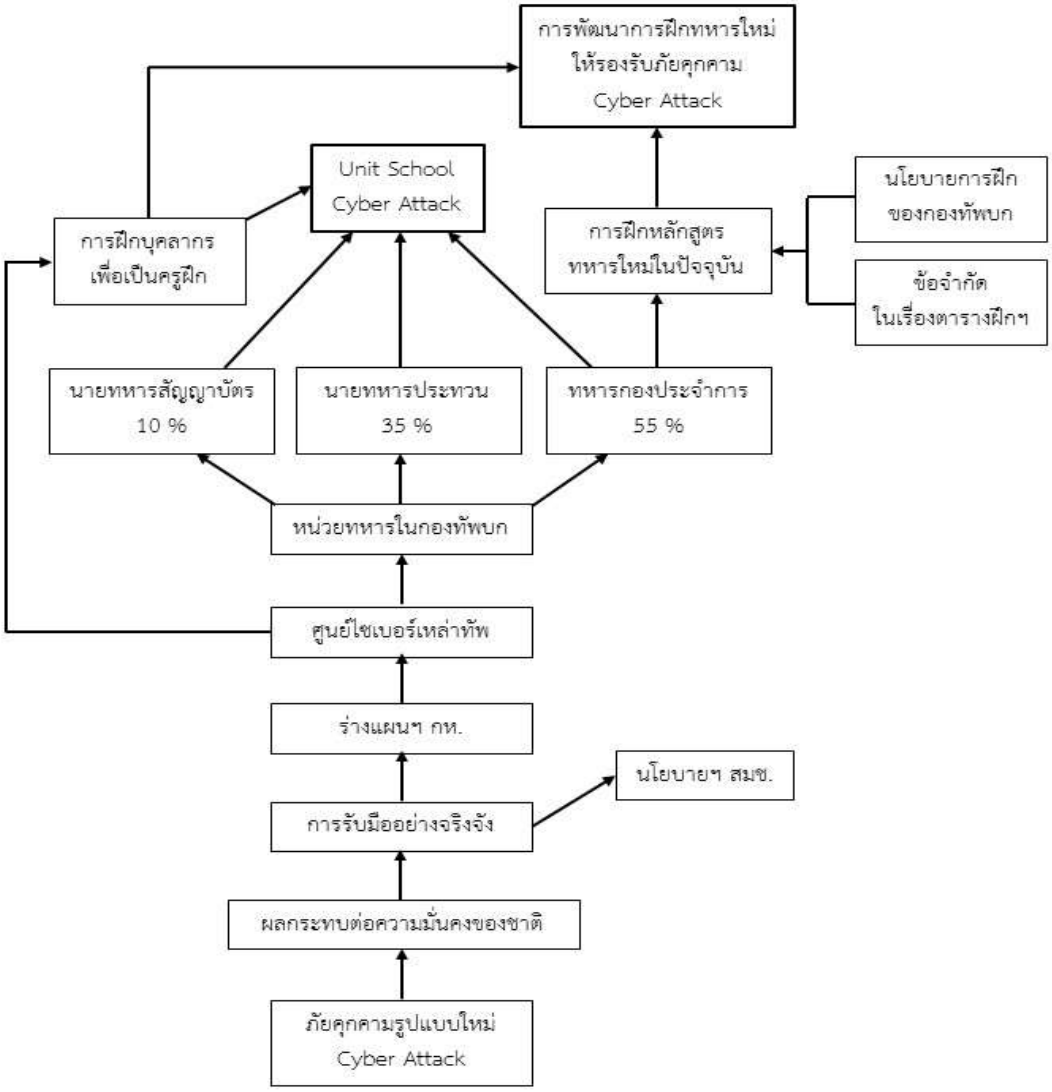
Information Warfare System Research เพื่อพัฒนาระบบการรักษาความปลอดภัยของข้อมูลข่าวสารให้มีประสิทธิภาพมากยิ่งขึ้น และต้องบรรจุอัตราจเรทหารที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อดำเนินการตรวจสอบตามหลักการ ICT Audit เชิงปฏิบัติการ ได้แก่

๓.๑ ควรจัดทำหลักสูตร Cyber Training เพื่ออบรมความรู้เกี่ยวกับการใช้งานซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งการให้ทุนการศึกษาต่อในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แก่บุคลากรทุกระดับ

๓.๒ ควรมีการจัดการองค์ความรู้ด้านไซเบอร์ (Cyber Knowledge Management: KM) ในหน่วยงาน และควรนำ E-Document มาใช้ในการปฏิบัติราชการมากยิ่งขึ้น

กรอบแนวคิดของการวิจัย

๒ - ๑ กรอบแนวคิดในการวิจัย



สรุป

วิวัฒนาการและความเจริญก้าวหน้าด้านเทคโนโลยีสารสนเทศและการสื่อสารของโลกยุคปัจจุบันที่เจริญเติบโต ขยายตัว และมีการพัฒนาขีดความสามารถ ประสิทธิภาพ และนวัตกรรมต่าง ๆ มากยิ่งขึ้นเพื่อรองรับความต้องการในการใช้งานของมนุษย์ ซึ่งหากบุคคลหาประโยชน์ของเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในทางก็ดี เช่น ใช้เพื่อเพิ่มขีดความสามารถในการให้บริการและการเข้าถึงบริการของภาครัฐผ่านระบบอิเล็กทรอนิกส์ การใช้เทคโนโลยีเพื่อพัฒนาระบบการปฏิบัติงานของภาคเอกชน หรือแม้แต่การใช้เทคโนโลยีในการติดต่อสื่อสารของประชาชน เป็นต้น ก็จะมีคุณประโยชน์อย่างอเนกอนันต์ แต่หากบุคคลอาศัยเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เพื่อผลทางมิชอบหรือนำมาใช้เป็นเครื่องมือมุ่งในทางร้าย ปลุกระดม มุ่งทำลาย ก็จะเป็นภัยคุกคามด้านไซเบอร์ (Cyber Threats) ที่มีโทษมหันต์เช่นกัน ตัวอย่างเช่น การเจาะระบบ (Hack/ Crack) การฝังโปรแกรมลักลอบโจรกรรมข้อมูล เช่น สปายแวร์ (Spyware) การโจมตีด้วยโปรแกรมมัลแวร์ (Malware) อาทิเช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนคอมพิวเตอร์ (Computer Warm) หรือม้าโทรจัน (Trojan Horse) การใช้โปรแกรมตั้งเวลาทางานเพื่อทาลาย (Logic Bomb) การใช้โปรแกรมหุ่นยนต์โจมตีเพื่อเป็นฐานโจมตีอุปกรณ์คอมพิวเตอร์บนเครือข่ายสารสนเทศ (Robot Network) การสร้างข้อมูลขยะ (Spam) เป็นต้น ซึ่งหากนามาใช้เป็นเครื่องมือทางการทหารก็จะส่งผลต่อความมั่นคงของประเทศชาติอย่างใหญ่หลวง จากภัยคุกคามดังกล่าวประเทศไทยจึงต้องมีการเตรียมพร้อมให้ประเทศมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามบนโลกไซเบอร์ ที่มีผลกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ โดยสภาความมั่นคงแห่งชาติ ได้กำหนดนโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘-๒๕๖๔ ที่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์ไว้ในนโยบายข้อที่ ๑๐ เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ เพื่อเป็นกรอบในการดาเนินการด้านความมั่นคงของประเทศไทยในระยะ ๗ ปี เพื่อใช้เป็นกรอบทิศทางหลักในการรักษาผลประโยชน์และความมั่นคงของชาติให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ เอกภาพและประสานสอดคล้องกันทั้งประเทศ

บทที่ ๓
วิธีดำเนินการวิจัย

วิธีดำเนินการวิจัย

๑. ในการวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ ผู้วิจัยได้ใช้การเก็บข้อมูลแบ่งเป็น ๒ วิธี ดังนี้

๑.๑ การเก็บข้อมูลทุติยภูมิ (Secondary Data) จากการทบทวนวรรณกรรมที่เกี่ยวข้องในขอบเขตเนื้อหาของภัยคุกคามรูปแบบใหม่รวมทั้งผลกระทบ และได้ศึกษานโยบายการรับมือของหน่วยงานด้านความมั่นคงของชาติในทุกระดับ ตลอดจนได้ศึกษาระบบการศึกษาระบบการฝึกของทหารกองประจำการของกองทัพบกไทยในปัจจุบัน เกี่ยวกับเนื้อหาสาระ และรูปแบบการฝึก

๑.๒ การเก็บข้อมูลแบบปฐมภูมิ (Primary Data ผู้วิจัยได้วางแผนจะทำแบบสอบถามและทำการสัมภาษณ์บุคลากรที่เกี่ยวข้องกับระบบการฝึก - ศึกษาของกองทัพบก โดยได้ออกแบบคำถาม สำหรับกรอกแบบสอบถาม และคำถามในการสัมภาษณ์ รายละเอียดตามภาคผนวก (อนุผนวก ก และอนุผนวก ข)

๒. ประชากรทั้งหมดที่ใช้ในการศึกษา คือ กำลังพลทั้งหมดของกองทัพบก ประกอบด้วย กำลังพลนายทหารสัญญาบัตร นายทหารชั้นประทวน และทหารกองประจำการ

๓. ประชากรที่จะนำมาเป็นกลุ่มตัวอย่างในการสำรวจข้อมูล ซึ่งถือว่าเป็นตัวแทนของประชากรทั้งหมด คือ นายทหารสัญญาบัตรที่ปฏิบัติราชการในหน้าที่ผู้บังคับหน่วย และฝ่ายเสนาธิการของหน่วย และนายทหารชั้นประทวนที่ทำหน้าที่ครูฝึกทหารใหม่ รุ่นปี ๒๕๖๐ ผลัดที่ ๑ ของหน่วยฝึกทหารใหม่ ในจังหวัดปราจีนบุรี โดยทั้งหมดจะทำการตอบแบบสอบถาม ตามอนุผนวก ก ในภาคผนวก

๔. การสัมภาษณ์จะทำการสัมภาษณ์ พันเอก มหิธร บุญครอง หัวหน้ากองยุทธการมณฑลทหารบกที่ ๑๒ ซึ่งเป็นนายทหารที่มีหน้าที่โดยตรงต่อการวางแผน อำนวยการ และกำกับดูแลการจัดการฝึก และการดำเนินการฝึกทุกประเภทของหน่วย ให้เป็นไปตามนโยบายการฝึกของกองทัพบก คำถามที่จะสัมภาษณ์เป็นไปตาม อนุผนวก ข ในภาคผนวก

๕. การวิเคราะห์ข้อมูล ผู้วิจัยนำผลการตอบแบบสอบถามในแต่ละข้อมาประเมินเป็นเปอร์เซ็นต์ เพื่อให้ได้มาซึ่งความคิดเห็นในเรื่องต่างๆ ที่เกี่ยวข้องกับการวิจัย ซึ่งผลการวิจัยจะถูกวิเคราะห์ ในบทที่ ๔ ผลการวิจัยอย่างละเอียดต่อไป ส่วนข้อมูลจากการสัมภาษณ์นั้นจะถูกนำมาวิเคราะห์ ในบทที่ ๔ ผลการวิจัย เช่นกัน

สรุป

ในบทนี้ผู้วิจัยได้กำหนดรูปแบบวิธีวิจัย โดยการรวบรวมข้อมูลทุติยภูมิ (Secondary Data) จากการทบทวนวรรณกรรมที่เกี่ยวข้อง และรวบรวมข้อมูลแบบปฐมภูมิ (Primary Data) จากการทำแบบสอบถามและการสัมภาษณ์บุคลากรที่เกี่ยวข้องโดยตรงกับการฝึก โดยการวิเคราะห์จะเกิดขึ้นในบทต่อไป

บทที่ ๔
แนวทางการพัฒนารูปแบบการฝึกทหาร เพื่อรองรับภัยคุกคามรูปแบบใหม่ : ภัยคุกคามด้านไซเบอร์

การวิเคราะห์ข้อมูลทุติยภูมิ (Secondary data Analysis)

จากการทบทวนวรรณกรรมในเรื่อง เกี่ยวกับภัยคุกคามรูปแบบใหม่ Cyber Attack จะเห็นได้ว่า Cyber Attack เป็นภัยคุกคามที่มากับความเจริญก้าวหน้าทางเทคโนโลยี โดยการนำเทคโนโลยีสารสนเทศมาใช้ในทางผิดกฎหมายละเมิดต่อศีลธรรม ความสงบสุขของสังคม โดยมีรูปแบบการดำเนินการโจมตีหลากหลายรูปแบบ โดยหลักๆแล้วลักษณะของการโจมตีสามารถสรุปได้ ๓ ลักษณะใหญ่ๆ ดังนี้

๑. การนำความลับขององค์กรออกมาเปิดเผยสาธารณะ (Data Confidentiality)

๒. การบิดเบือนข้อมูลที่แท้จริง (Data Integrity)

๓. การทำลายระบบปฏิบัติการในเครือข่ายคอมพิวเตอร์ (System Availability)

ซึ่งทั้งหมดนี้ได้ก่อให้เกิดความเสียหายอย่างใหญ่หลวงต่อความมั่นคงของชาติในด้านต่างๆ รวมทั้งความเสียหายด้านเศรษฐกิจและสังคมอย่างใหญ่หลวง

ผู้วิจัยมีความเห็นว่าการปฏิบัติการ Cyber Attack เป็นการปฏิบัติการที่มีประสิทธิภาพ มีต้นทุนการดำเนินการต่ำ และส่งผลสัมฤทธิ์ในการทำลายล้างอย่างรุนแรงและรวดเร็ว โดยไม่มีเงื่อนไขของเวลามาเป็นตัวจำกัดเป้าหมายในการโจมตี วิเคราะห์ได้ยากและเตรียมการรับมือกระทำได้ยาก ดังนั้น การเตรียมการรับมือภัยคุกคามรูปแบบนี้ซึ่งเป็นสิ่งที่สำคัญที่ผู้บริหารทุกองค์กร ในประเทศต้องตระหนักและขับเคลื่อนให้เป็นรูปธรรมในหน่วยงานของตน โดยเฉพาะอย่างยิ่งต้องให้ความสำคัญกับบุคลากรทุกคนเพราะมีความล่อแหลมจะตกเป็นเครื่องมือเพราะเป็นส่วนหนึ่งของการโจมตีได้ กลับมาที่การพิจารณาในกองทัพซึ่งสถาบันทหารถือเป็นเสาหลักของความมั่นคงของชาติ โดยเฉพาะอย่างยิ่งในห้วงเวลาปัจจุบันที่คณะรักษาความสงบแห่งชาติ (คสช.) ได้มามีบทบาทสำคัญในการปฏิรูปประเทศตั้งแต่ ๒๒ พ.ค.๕๗ เป็นต้นมา ทหารในกองทัพถูกใช้งานในการเป็นกองกำลังรักษาความสงบเรียบร้อย ในการขับเคลื่อนงานสนับสนุนการทำงานของรัฐบาล และ คสช. จึงไม่แปลกเลยที่สถาบันทหารจะเป็นเป้าหมายอันดับหนึ่งในการถูกโจมตีจากฝ่ายตรงข้ามและฝ่ายที่มาเห็นด้วยกับการทำงานของรัฐบาล และ คสช.ฝ่ายที่พยายามจะทำให้เกิดความไม่สงบในบ้านเมืองเป็นเครื่องมืออันทรงประสิทธิภาพในการโจมตี อันนั้นก็ คือ Cyber Attack ซึ่งเป็นเครื่องมือที่มีประสิทธิภาพและต้นทุนต่ำและการดำเนินการสืบหาต้นตอผู้กระทำเป็นไปได้ยากโดยการกระทำดังกล่าวมุ่งเน้นไปในเรื่องการนำข้อมูลของกองทัพหรือเรื่องราวที่เกิดขึ้นในกองทัพมาบิดเบือนและแพร่กระจายต่อสาธารณะใน Social Network ต่างๆ เพื่อทำลายความน่าเชื่อถือ

ความเชื่อมั่น ศรัทธาต่อสถาบันทหารซึ่งเป็นเสาหลักด้านความมั่นคงของชาติ หากพิจารณาภายในกองทัพบก จะเห็นได้ว่ามีกำลังพลจำนวนทั้งสิ้นประมาณ ๒๙๐,๐๐๐ นาย ซึ่งเป็นนายทหารสัญญาบัตรประมาณ ๓๐,๐๐๐ นาย คิดเป็นร้อยละ ๑๐ ของกำลังพลทั้งหมด นายทหารชั้นประทวนประมาณ ๑๐๐,๐๐๐ นาย คิดเป็นร้อยละ ๓๕ ของกำลังพลทั้งหมด และทหารกองประจำการประมาณ ๑๖๐,๐๐๐ นาย คิดเป็นร้อยละ ๕๕ ของกำลังพลทั้งหมด ซึ่งแนวทางในการรับมือภัยคุกคามรูปแบบใหม่ Cyber Attack ที่ดีที่สุด คือ การเสริมสร้างความรู้ความเข้าใจปลูกจิตสำนึกให้กับบุคลากรในกองทัพ ซึ่งต้องทำอย่างเร่งด่วนและมีประสิทธิภาพ ซึ่งจากการส่งแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๖๐ - ๒๕๖๔ นำมาซึ่งการตั้งศูนย์ไซเบอร์ของแต่ละเหล่าทัพ เพื่อขับเคลื่อนการปฏิบัติการทางไซเบอร์เชิงรุกและเชิงรับ พร้อมรับมือต่อไปการโจมตีทาง Cyber Attack ต่อหน่วยงานทหารซึ่งกระทบต่อความมั่นคงของชาติ และหน่วยทหารทุกหน่วยในกองทัพบกเองเช่นกัน ผู้บังคับหน่วยต้องตระหนักในภัยคุกคามดังกล่าว และเตรียมแผนการปฏิบัติรองรับนโยบายการรับมือ Cyber Attack ของกองทัพบกและกระทรวงกลาโหม

ผู้วิจัยเห็นว่า การเสริมสร้างความพร้อมของบุคลากรในกองทัพบกควรทำคู่ขนานไปพร้อมๆ กันทั้ง ๓ ระดับ ทั้ง นายทหารสัญญาบัตร นายทหารชั้นประทวน และพลทหารกองประจำการ แต่ควรจะเน้นไปที่ทหารกองประจำการ เนื่องจากเป็นกำลังพลส่วนใหญ่ของกองทัพบก (ร้อยละ ๕๕ ของกำลังพลทั้งหมด)

ในกรณีของทหารกองประจำการ โดยทั่วไปจะเกี่ยวข้องกับการฝึกตามวงรอบของกองทัพบก โดยการฝึกที่สำคัญและเกี่ยวข้องมากที่สุด คือ “การฝึกทหารใหม่” ซึ่งปัจจุบันกองทัพบกให้มีการฝึกทหารใหม่ปีละ ๒ ผลัดๆ ละ ๑๐ สัปดาห์ โดยให้หน่วยในกองทัพบกดำเนินการจัดตั้งหน่วยฝึกทหารใหม่เอง และดำเนินการฝึกทหารใหม่ให้เป็นตามนโยบายการฝึกที่กองทัพบกกำหนด ภายใต้การกำกับดูแลของกรมยุทธศึกษาทหารบก จากที่ผู้เรียนพิจารณาดูเนื้อหาในระเบียบหน่วยหลักสูตรการฝึกทหารใหม่ และพบว่าการฝึกทหารใหม่นั้น เน้นการอบรมพลทหารที่ไม่เคยรับราชการมาก่อน ให้มีความรู้ความเข้าใจแบบธรรมเนียม และวิชาทหารเบื้องต้น เป็นการปรับสภาพร่างกาย จิตใจให้มีความพร้อม ในการเป็นพลทหารกองประจำการ เพื่อสามารถปฏิบัติงานในกรมกองต่างๆ ในกองทัพบกได้เมื่อจบหลักสูตรทหารใหม่ โดยเนื้อหาการฝึกจะแบ่งออกเป็น ๖ สถานี ดังนี้

สถานีที่ ๑ : การเสริมสร้างความสมบูรณ์แข็งแรงทางร่างกาย
สถานีที่ ๒ : การฝึกบุคคลท่าเบื้องต้น และแถวชิด
สถานีที่ ๓ : การใช้อาวุธสงคราม
สถานีที่ ๔ : การยิงปืนด้วยกระสุนจริง
สถานีที่ ๕ : วิชาทหารทั่วไปและยุทธวิธีเบื้องต้น
สถานีที่ ๖ : การสอนอบรม

และเมื่อเข้าไปพิจารณาในรายละเอียดของแต่ละพื้นที่พบว่า ไม่มีเนื้อหาในวิชาใดเกี่ยวข้องกับการฝึกเพื่อรับมือภัยคุกคามรูปแบบใหม่ Cyber Attack แม้แต่น้อย ผู้วิจัยจึงมีความเห็นว่าห้วงเวลาที่ดีที่สุดในการปลูกฝังทหารกองประจำการ ให้มีความรู้ในการรับมือกับภัยคุกคามรูปแบบใหม่ Cyber Attack ควบคู่กันไป และมีจิตสำนึกในเรื่องต่างๆ ก็ควรเป็นห้วงเวลาในการฝึกทหารใหม่ ดังนั้น แนวความคิดที่จะปรับปรุงหลักสูตรการฝึกทหารใหม่ เพื่อรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack โดยการเพิ่มรายวิชาที่เกี่ยวข้องในเรื่องดังกล่าวน่าจะเป็นความจำเป็นเร่งด่วน ที่กรมยุทธศึกษาทหารบกควรพิจารณา อย่างไรก็ดี กองทัพบกต้องเร่งผลิตบุคลากรที่มีขีดความสามารถในการถ่ายทอดเรื่องดังกล่าวออกมา และกรมยุทธศึกษาทหารบกเองต้องกำหนดรายละเอียดวิชาที่สอน หาหลักฐานการสอนกำหนดความมุ่งหมายและจัดทำเครื่องช่วยฝึก เพื่อรองรับการฝึกในเรื่องดังกล่าว เพื่อให้ทุกหน่วยมีบุคลากรส่วนใหญ่ที่มีความรู้ความสามารถในเรื่องการใช้เทคโนโลยีสารสนเทศ อย่างมีวินัยและเป็นการตอบสนองนโยบายของกองทัพบก และกระทรวงกลาโหม เกี่ยวกับการรับมือ Cyber Attack อย่างมีประสิทธิภาพ

การวิเคราะห์ข้อมูลปฐมภูมิ (Primary Data Analysis)

ข้อมูลปฐมภูมิที่ผู้วิจัยได้ทำการรวบรวม จะมีทั้งหมด ๒ ส่วน

ส่วนที่ ๑ ได้มาจากการกรอกแบบสอบถามของ ผู้บังคับหน่วยทหาร ฝ่ายเสนาธิการในจังหวัดปราจีนบุรี และครูฝึกทหารใหม่ในจังหวัดปราจีนบุรี

ส่วนที่ ๒ ได้จากการสัมภาษณ์ พันเอก มหิธร บุญครอง หัวหน้ากองยุทธการมณฑลทหารบกที่ ๑๒ ซึ่งมีหน้าที่โดยตรงเกี่ยวกับ การวางแผนและกำกับดูแลการฝึกทั้งหมดของมณฑลทหารบกที่ ๑๒

๑. การวิเคราะห์ข้อมูลจากการกรอกแบบสอบถาม

๑.๑ เกี่ยวกับระดับความเข้าใจในเรื่องภัยคุกคามรูปแบบใหม่ Cyber Attack

๑.๑.๑ พบว่ามีเพียง ร้อยละ ๑๐ ที่มีความเข้าใจอยู่ในระดับที่สูง ซึ่งผู้ที่มีความเข้าใจระดับสูงทั้งหมดเป็นนายทหารระดับ ผู้บังคับหน่วย และฝ่ายเสนาธิการ

๑.๑.๒ มี ร้อยละ ๓๐ ที่ตอบว่า เข้าใจปานกลาง

๑.๑.๓ มีถึง ร้อยละ ๖๐ ที่ตอบว่า มีความเข้าใจเรื่องดังกล่าวน้อยมาก

จากคำตอบข้อนี้สามารถวิเคราะห์ว่า กำลังพลส่วนใหญ่มีความเข้าใจเกี่ยวกับ Cyber Attack ในระดับที่ต่ำ

๑.๒ เกี่ยวกับระดับที่กองทัพบกต้องเผชิญกับภัยคุกคาม Cyber Attack

๑.๒.๑ พบว่า ร้อยละ ๑๐๐ ตอบว่า ปัจจุบันกองทัพบกต้องเผชิญกับภัยคุกคามดังกล่าวในระดับที่สูง

จากคำตอบข้อนี้วิเคราะห์ได้ว่า ทุกคนเห็นตรงกันว่าภัยคุกคาม Cyber Attack เป็นภัยคุกคามรูปแบบใหม่ ที่มีผลกระทบต่อกองทัพบกในระดับที่สูง และถือว่าเป็นภัยคุกคามที่สำคัญ

๑.๓ เกี่ยวกับระดับความรู้ของกำลังพล ในกองทัพบกเกี่ยวกับภัยคุกคามรูปแบบใหม่ Cyber Attack

๑.๓.๑ พบว่า ร้อยละ ๒๐ ตอบว่า ความรู้กำลังพลในเรื่องดังกล่าวอยู่ในระดับปานกลาง

๑.๓.๒ มีถึง ร้อยละ ๘๐ ที่ตอบว่า ความรู้กำลังพลในเรื่องดังกล่าวอยู่ในระดับต่ำ

จากคำตอบข้อนี้สามารถวิเคราะห์ว่า กำลังพลในกองทัพบกรู้จัก Cyber Attack อยู่ในระดับที่ต่ำ

๑.๔ เกี่ยวกับการรู้จักหน่วยงาน “ศูนย์ไซเบอร์กองทัพบก” ในเรื่องภารกิจของหน่วย

๑.๔.๑ พบว่าเพียง ร้อยละ ๒๐ ของผู้ตอบที่รู้จักหน่วยงาน “ศูนย์ไซเบอร์กองทัพบก” เป็นอย่างดีนั้น เป็นผู้บังคับหน่วย และฝ่ายเสนาธิการทั้งสิ้น

๑.๔.๒ มี ร้อยละ ๓๕ ตอบว่า รู้จักหน่วยงานนี้ ในระดับปานกลาง

๑.๔.๓ มี ร้อยละ ๔๕ ที่ไม่รู้จักหน่วยงานนี้เลย

จากคำตอบข้อนี้วิเคราะห์ได้ว่า กำลังพลส่วนใหญ่ยังไม่ค่อยรู้จักหน่วยงาน “ศูนย์ไซเบอร์กองทัพบก”

๑.๕ เกี่ยวกับการประสานงานกับ ศูนย์ไซเบอร์กองทัพบก

๑.๕.๑ เพียง ร้อยละ ๑๐ ของผู้ตอบ เคยประสานงานกับศูนย์ไซเบอร์กองทัพบก

๑.๕.๒ และมีถึง ร้อยละ ๙๐ ไม่เคยประสานงานกับศูนย์ไซเบอร์กองทัพบก

๑.๖ เกี่ยวกับความจำเป็นของกำลังพล ในการมีความรู้เกี่ยวกับ การใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม

๑.๖.๑ ร้อยละ ๑๐๐ ของผู้ตอบ เห็นว่ามีความจำเป็นอย่างมาก

๑.๗ ประวัติการฝึกอบรมเรื่องเกี่ยวกับเทคโนโลยีสารสนเทศในหน่วยงาน

๑.๗.๑ ร้อยละ ๑๕ ของผู้ตอบ ตอบว่ามีการฝึกในเรื่องดังกล่าว แต่น้อยครั้ง

๑.๗.๒ ร้อยละ๘๕ ของผู้ตอบ ตอบว่าไม่เคยมีการฝึกอบรมภายในหน่วยงานเลย

จากการตอบข้อนี้วิเคราะห์ว่าการฝึก Unit School เรื่องนี้ในหน่วยงานมีค่อนข้างน้อยหรือไม่มีเลย

๑.๘ เกี่ยวกับกำลังพลระดับใดที่มีความล่อแหลม ในการตกเป็นเครื่องมือของ Cyber Attack

๑.๘.๑ ร้อยละ ๑๐๐ ของผู้ตอบ ตอบว่าเป็นกำลังพลระดับพลทหารกองประจำการ

๑.๙ เกี่ยวกับการอบรมเกี่ยวกับ Cyber Attack ในหน่วยทหาร

๑.๙.๑ ร้อยละ ๑๐๐ ของผู้ตอบ คิดว่าควรมีการอบรมเกี่ยวกับ Cyber Attack ในหน่วยทหาร

๑.๑๐ เกี่ยวกับการฝึกอบรมเรื่อง Cyber Attack

๑.๑๐.๑ ไม่มีผู้ใดตอบว่า ควรสอดแทรกในการฝึกต่างๆ ตามวงรอบประจำปี

๑.๑๐.๒ ร้อยละ ๒๕ เห็นว่า ควรสอดแทรกในการฝึกทหารใหม่อย่างเดียว

๑.๑๐.๓ ร้อยละ ๖๕ เห็นว่า ควรสอดแทรกในการฝึกทหารใหม่ และควรจัด Unit School

๑.๑๐.๔ ร้อยละ ๑๐ เห็นว่า ควรส่งกำลังพลไปอบรมนอกหน่วยอย่างเดียว

๑.๑๑ เกี่ยวกับการฝึกทหารใหม่ในปัจจุบันของกองทัพบก รองรับภัยคุกคามรูปแบบใหม่ Cyber Attack หรือไม่

๑.๑๑.๑ร้อยละ ๑๐๐ ของผู้ตอบ ตอบว่าการฝึกของกองทัพบกในปัจจุบันไม่รองรับภัยคุกคามรูปแบบใหม่ Cyber Attack

๑.๑๒ เกี่ยวกับการนำเรื่อง Cyber Attack มาบรรจุในการฝึกทหารใหม่

๑.๑๒.๑ ร้อยละ ๖๐ ของผู้ตอบ เห็นด้วยในการนำเรื่อง Cyber Attack มาบรรจุในการฝึกทหารใหม่

๑.๑๒.๒ ร้อยละ ๔๐ ของผู้ตอบซึ่งส่วนใหญ่เป็นครูฝึกทหารใหม่บอกไม่เห็นด้วย เนื่องจากหากบรรจุเรื่องนี้เข้ามาจะทำให้เวลาการฝึกของวิชาอื่นน้อยลง ทหารใหม่ควรได้รับการฝึกในเรื่องพื้นฐานมากกว่า สำหรับเรื่องนี้ควรทำการฝึกอบรมหลังจากจบการฝึกทหารใหม่

๑.๑๓ หากมีแนวคิดในการบรรจุเรื่อง Cyber Attack ลงในหลักสูตรทหารใหม่ ควรให้ความรู้เรื่องอะไรบ้าง ผู้ตอบได้ให้คำตอบดังนี้

๑.๑๓.๑ ความรู้เบื้องต้นเกี่ยวกับการใช้เทคโนโลยีสารสนเทศ

๑.๑๓.๒ การสื่อสารและข้อมูลเครือข่ายเบื้องต้น

๑.๑๓.๓ ความปลอดภัยของระบบสารสนเทศ

๑.๑๓.๔ ภัยคุกคามรูปแบบใหม่ Cyber Attack

๑.๑๓.๕ วินัย/จิตสำนึก ในการใช้อุปกรณ์ติดต่อสื่อสาร และการใช้สื่อสาธารณะ

๑.๑๓.๖ ผลกระทบของ Cyber Attack ต่อองค์กร

๑.๑๔ รวบรวมความเห็นสิ่งที่จำเป็นต้องเตรียมการ เมื่อจะนำเรื่อง Cyber Attack มาบรรจุในหลักสูตรทหารใหม่

๑.๑๔.๑ ครูฝึกที่มีความรู้ และขีดความสามารถ ในการถ่ายทอด

๑.๑๔.๒ กำหนดชื่อเรื่อง/วิชา ที่จะถ่ายทอด

๑.๑๔.๓ มีหลักฐาน/เอกสาร การฝึกรองรับ

๑.๑๔.๔ มีการกำหนดชั่วโมงการฝึกให้ชัดเจน

๑.๑๔.๕ มีการกำหนดความมุ่งหมายในการฝึกชัดเจน

๑.๑๔.๖ จัดทำเครื่องช่วยฝึก

๒. การวิเคราะห์ข้อมูลจากการสัมภาษณ์

การสัมภาษณ์ครั้งนี้ผู้วิจัยได้ทำการสัมภาษณ์นายทหารท่านหนึ่งของกองทัพบก คือ พันเอก มหิธร บุญครอง ซึ่งปัจจุบันปฏิบัติงานในตำแหน่ง หัวหน้ากองยุทธการ มณฑลทหารบกที่ ๑๒ รับผิดชอบโดยตรงในเรื่อง การวางแผน อำนวยการ กำกับดูแลการฝึกทุกประเภท ตลอดจนการใช้กำลังของหน่วย ท่านจบการศึกษาปริญญาโท การบริหารจัดการทรัพยากรมนุษย์ (Human Resource Management) จากมหาวิทยาลัย Warwick ประเทศอังกฤษ และเคยมีบทความทางวิชาการเรื่อง “The design of a training programme measurement model” ซึ่งตีพิมพ์ในนิตยสาร European Journal of training and Develment ปี ค.ศ.๒๐๐๐ นอกจากนั้นท่านยังเคยดำรงตำแหน่งที่สำคัญในอดีตที่เกี่ยวข้องกับระบบการฝึกต่างๆ ของกองทัพบก เช่น เป็นนายทหารฝ่ายยุทธการของกองพันทหารม้าที่ ๓ รักษาพระองค์ ซึ่งท่านได้ให้ข้อมูลในการสัมภาษณ์ ดังนี้

๒.๑ เกี่ยวกับระบบการฝึกของกองทัพบกไทยในภาพรวม

๒.๑.๑ ระบบการฝึกของกองทัพบกไทย มีหน่วยงานระดับสูงที่เกี่ยวข้องคือ กรมยุทธการทหารบก ในส่วนของกองการฝึกและศึกษา ซึ่งมีหน้าที่อำนวยการฝึกและศึกษาในเรื่องที่เกี่ยวข้องกับนโยบายที่สำคัญ หรือหลักการสำคัญๆ เท่านั้น แต่การวางแผน กำหนดแนวทาง และการอำนวยการหลักๆแล้ว เป็นหน้าที่ของกรมยุทธศึกษาทหารบก โดยมีหน่วยรองสายวิชาการที่สำคัญคือ ศูนย์การทหารราบ ศูนย์การทหารม้า ศูนย์การทหารปืนใหญ่ โดยมีแผนการฝึกตามวงรอบประจำปีของกองทัพบก จะถูกจัดทำโดย กรมยุทธศึกษาทหารบก และจะถูกแจกจ่ายมายังหน่วยทหารต่างๆ ก่อนเริ่มปีงบประมาณ โดยแต่ละประเภทหน่วยจะได้รับแผนการฝึก ซึ่งระบุประเภทของการฝึกและงบประมาณในการฝึก ซึ่งประกอบด้วย งบประมาณที่เป็นเงิน เป็นน้ำมัน และเป็นกระสุนแตกต่างกัน ทั้งนี้ขึ้นอยู่กับจำนวนและประเภทการฝึกที่ได้รับ แต่หลักๆแล้วแต่ละหน่วยจะมีการจัดการฝึกทหารใหม่, การฝึกเฉพาะหน้าที่, การฝึก หมู่ ตอน หมวด, การฝึกภาคกองร้อย, การฝึกยิงปืนประจำปี แต่ละหน่วยดำเนินกลยุทธ์ที่เป็นหน่วยเป้าหมายเพิ่มเติม การฝึกภาคกองพันและภาคกรมทหารราบ/ทหารม้าเฉพาะกิจเข้าไป

๒.๑.๒ โดยการฝึกทั้งหมดที่หน่วยได้รับจากกรมยุทธศึกษาทหารบกจะถูกกำหนดให้กระทำการฝึกตามห้วงที่กรมยุทธศึกษากำหนด และทุกการฝึกจะมีการประเมินผล อาจกระทำโดยคณะกรรมการของหน่วย หรือหน่วยเหนือ แล้วส่งผลการประเมินให้ กรมยุทธศึกษาทหารบก หรือกรมยุทธศึกษาทหารบก อาจส่งคณะกรรมการประเมินผลโดยตรงเป็นบางหน่วยก็ได้

๒.๑.๓ สำหรับเนื้อหาของการฝึกแต่ละประเภท ก็จะแตกต่างกันออกไปตามความมุ่งหมาย ยกตัวอย่าง การฝึกทหารใหม่ ก็จะมุ่งเน้นการปรับสภาพร่างกาย จิตใจจากบุคคลพลเรือนมาเป็นทหาร ให้ความรู้ด้านวิชาทหารเบื้องต้น ยุทธวิธีเบื้องต้น และแบบธรรมเนียมการฝึกเฉพาะหน้าที่ ก็จะมุ่งเน้นขีดความสามารถของกำลังพลที่จะลงไปปฏิบัติงานในตำแหน่งหน้าที่ที่ตนเองได้รับ หลังจากจบการฝึกทหารใหม่ไปประจำการในหน่วยต่างๆ

๒.๑.๔ สำหรับการฝึกทางยุทธวิธี ภาคหมู่ ตอน หมวด, ภาคกองร้อย, ภาคกองพัน หรือ กรมทหารราบ/ทหารม้าเฉพาะกิจนั้น มุ่งเน้นการรบตามแบบ และเป็นการรองรับตามแบบ และเป็นการรองรับภัยคุกคามรูปแบบเดิม เน้นการใช้ยุทธวิธี ใช้กำลังทหารในการเอาชนะฝ่ายตรงข้าม เพื่อปกป้องดินแดน นอกเหนือจากการฝึกตามวงรอบประจำปี หน่วยต่างๆอาจมีการฝึกพิเศษ ซึ่งเกิดขึ้นจากนโยบายผู้บังคับบัญชาและมีความมุ่งหมายเฉพาะเรื่อง เช่น การฝึกหน่วยทหารขนาดเล็ก, การฝึกหน่วยทหารทรหด, การฝึกเพื่อเตรียมไปปฏิบัติภารกิจพิเศษอย่างใดอย่างหนึ่งนอกเหนือจากนั้น เพื่อเป็นการเสริมสร้างความมีประสิทธิภาพ ในการปฏิบัติงานเฉพาะของหน่วย กองทัพบกได้ส่งเสริมให้หน่วยจัดตั้ง Unit School เฉพาะของหน่วย เพื่อให้หน่วยได้ดำเนินการฝึกอบรมกำลังพลในเรื่องต่างๆ ที่สำคัญและเกี่ยวข้องในการเพิ่มประสิทธิภาพในการปฏิบัติงานของกำลังพลของหน่วย นอกเหนือจากการฝึกต่างๆ แล้ว กองทัพบกยังมีแนวทางการพัฒนาตัวบุคคล โดยกำหนดให้หน่วยต้องส่งบุคลากรมาเข้ารับการศึกษา หลักสูตรตามแนวทางรับการราชการ เช่น หลักสูตรนายสิบชั้นต้น, หลักสูตรนายสิบอาวุโส, หลักสูตรชั้นนายร้อย, หลักสูตรชั้นนายพันเหล่าต่างๆ โรงเรียนเสนาธิการทหารบก เพื่อเพิ่มคุณวุฒิและเตรียมความพร้อมให้กำลังพลในการปฏิบัติงานในตำแหน่งที่สูงขึ้น นอกจากหลักสูตรพิเศษเพื่อเพิ่มพูนขีดความสามารถของกำลังพลในหน้าที่ต่างๆ เช่น หลักสูตรช่าง, หลักสูตรด้านการข่าว, หลักสูตรปลัดบัญชี, หลักสูตรจู่โจม, หลักสูตรส่งทางอากาศ ฯลฯ

๒.๒ ระบบการฝึกของกองทัพบกไทย รองรับภัยคุกคามรูปแบบใหม่ Cyber Attack หรือไม่

๒.๒.๑ ระบบการฝึกของกองทัพบกไทยปัจจุบัน ถ้าพิจารณาแล้วไม่รองรับภัยคุกคามรูปแบบใหม่ แต่ระบบการวางแผนการฝึกมีความอ่อนตัว สามารถจัดการฝึกอบรมพิเศษได้ นอกเหนือจากการฝึกตามวงรอบประจำปี หรือจัดการฝึกเพิ่มเติมจากหลักสูตรพิเศษต่างๆได้ โดยกำหนดหน่วยรับผิดชอบในการวางแผนให้ชัดเจน เช่น ถ้าเป็นเรื่องเกี่ยวกับเทคโนโลยีสารสนเทศก็อาจเป็นหน่วย ศูนย์ไซเบอร์กองทัพบก ทำการวางแผนร่วมกับกรมยุทธศึกษาทหารบก ในการดำเนินหลักสูตรการฝึกอบรม หลังจากนั้นจึงสามารถขยายผลมายังหน่วยต่างๆ ในกองทัพบก

๒.๓ ท่านมีแนวคิดที่จะทำให้กำลังพลของกองทัพบก มีความรู้เรื่องเทคโนโลยีสารสนเทศ และใช้เครื่องมือทางเทคโนโลยีอย่างมีวินัย และไม่ตกเป็นเครื่องมือของ Cyber Attack

๒.๓.๑ ถ้าต้องการให้กำลังพลมีความรู้ มีจิตสำนึก และมีวินัยในการใช้เทคโนโลยีสารสนเทศก็ต้องทำการฝึกอบรม ซึ่งปัจจุบันผมมองว่าหน่วยยังไม่มีขีดความสามารถเพียงพอที่จะเปิด Unit School ในเรื่องดังกล่าว เพราะไม่มีบุคลากรจะเป็นครูผู้สอนและไม่มีหลักฐาน การสอนที่ชัดเจน ไม่รู้จะเริ่มต้นจากตรงไหน หน่วยทำได้ในปัจจุบันแค่เพียงสั่งการให้กำลังพลใช้โทรศัพท์มือถืออย่างระมัดระวังไม่ถ่ายภาพ/แพร่ภาพที่ไม่เหมาะสมและมีผลกระทบกับหน่วยหรือกับกองทัพบก ซึ่งหน่วยทำได้แค่นั้นจริงๆ

๒.๓.๒ หากจะเริ่มต้นการให้ความรู้เรื่องนี้อย่างจริงจัง กรมยุทธศึกษาทหารบกต้องร่วมกับศูนย์ไซเบอร์กองทัพบก กำหนดหลักสูตรการฝึกเรื่องดังกล่าว และจัดการฝึกอบรมในภาพรวมขึ้นมา เพื่อสร้างบุคลากรเริ่มต้นในระยะแรก หลังจากนั้นในระยะที่สอง นำบุคลากรเหล่านั้นกลับเข้าไป ขยายผลในหน่วยของตน โดยอาจจะเข้า Unit School เพื่อเพิ่มจำนวนบุคลากรที่มีความรู้ ในระยะที่สาม คือ พิจารณานำเรื่องดังกล่าวกำหนดเข้ารายวิชา ลงไปในหลักสูตรการฝึกทหารใหม่โดยมีกรมยุทธศึกษาเป็นผู้กำหนดมาตรฐานของวิชา

สรุป

ภัยคุกคามทางด้านไซเบอร์ถือว่าเป็นอันตรายต่อความมั่นคงของชาติ เป็นภัยร้ายแรงสร้างความเสียหายในวงกว้าง กระทบต่อพลเมืองเป็นจำนวนมาก ในประเทศไทยมีระดับความรุนแรงของภัยคุกคามไซเบอร์ (Cyber Attack) ไม่รุนแรงเหมือนประเทศมหาอำนาจ ส่วนใหญ่เป็นเพียงภัยคุกคามในลักษณะของการปล่อยไวรัสคอมพิวเตอร์ และการปล่อยมัลแวร์ รวมทั้งการแก้หน้าเว็ปไซต์ เป็นต้น ซึ่งกองทัพบกได้มีการดำเนินการจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) โดยเน้นการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์และรักษาความปลอดภัยทางด้านไซเบอร์ของกองทัพ ทั้งด้านการป้องกัน การเฝ้าระวังแบบเรียลไทม์ และการสนองตอบภัยคุกคามแบบเรียลไทม์ เช่นกัน จะดีมากแค่ไหนหากการเฝ้าระวังความปลอดภัยและการรักษาความปลอดภัยทางด้านไซเบอร์ของกองทัพไม่ได้เป็นหน้าที่เฉพาะของศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) เท่านั้น แต่กลายเป็นหน้าที่ของทหารกองประจำการทุกนาย ด้วยการฝึกอบรมให้นายทหารทุกนายมีความรู้เบื้องต้นเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อร่วมกันป้องกันภัยคุกคามทางไซเบอร์ซึ่งเป็นภัยคุกคามที่ใกล้ตัว ไม่ว่าจะอยู่ในฐานะของทหารของกองทัพ หรือเมื่อออกไปใช้ชีวิตเป็นประชาชนของประเทศ

การจะทำให้ทหารทุกนายได้มีความรู้เกี่ยวกับภัยคุกคามไซเบอร์นั้น กรมยุทธศึกษาทหารบกต้องร่วมกับศูนย์ไซเบอร์กองทัพบก กำหนดหลักสูตรการฝึกเรื่องดังกล่าว และจัดการฝึกอบรมในภาพรวมขึ้นมา เพื่อสร้างบุคลากรเริ่มต้นในระยะแรก หลังจากนั้นในระยะที่สอง นำบุคลากรเหล่านั้นกลับเข้าไป ขยายผลในหน่วยของตน โดยอาจจะเข้า Unit School เพื่อเพิ่มจำนวนบุคลากรที่มีความรู้ในระยะที่สาม คือ พิจารณานำเรื่องดังกล่าวกำหนดเข้ารายวิชา ลงไปในหลักสูตรการฝึกทหารใหม่ โดยมีกรมยุทธศึกษา เป็นผู้กำหนดมาตรฐานของวิชาต่อไป

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

การศึกษาเรื่องแนวทางการพัฒนารูปแบบการฝึกทหาร เพื่อรองรับภัยคุกคามรูปแบบใหม่ : ภัยคุกคามด้านไซเบอร์ มีวัตถุประสงค์เพื่อ

๑. เพื่อทำการศึกษาหาข้อมูลภัยคุกคามรูปแบบใหม่ Cyber Attack ซึ่งมีผลกระทบด้านความมั่นคงของชาติ

๒. เพื่อทำการศึกษาระบบการฝึก - ศึกษาของกองทัพบกไทยในปัจจุบัน

๓. เพื่อทำการเสนอแนวความคิดในการสร้างการรับรู้และจิตสำนึกของบุคลากรในกองทัพบกในการใช้เทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม และปลอดภัยต่อ Cyber Attack โดยการจัดหลักสูตรการฝึกอบรมเพิ่มเติมจากการฝึก - ศึกษาปกติของหน่วยทหารในกองทัพบก

ซึ่งในการวิจัยครั้งนี้ ผู้วิจัยได้ทำการศึกษา เกี่ยวกับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack นโยบายการรับมือภัยคุกคามด้านไซเบอร์ของหน่วยงานความมั่นคง ทำการศึกษาเกี่ยวกับ ระบบการฝึก-ศึกษาของกองทัพบกไทย ทำการวิเคราะห์ข้อมูลทั้งหมด ซึ่งสามารถสรุปผลการศึกษาได้ ดังนี้

๑. ภัยคุกคามรูปแบบใหม่ Cyber Attack เป็นภัยคุกคามที่สำคัญ มีผลกระทบโดยตรงกับความมั่นคงของชาติ โดยวิธีการดำเนินการจะแบ่งออกเป็น ๓ ลักษณะใหญ่ๆ คือ

๑.๑ การล้วงความลับขององค์กร ออกมาเปิดเผยสาธารณะ (Data Confidentiality)

๑.๒ การเปลี่ยนแปลง/บิดเบือน ข้อมูลขององค์กร (Data Integrity)

๑.๓ การทำลายระบบปฏิบัติการของเครือข่ายคอมพิวเตอร์ในองค์กร (System Availability)

๒. หน่วยงานด้านความมั่นคงทุกระดับ ให้ความสำคัญในการรับมือ ภัยคุกคามรูปแบบใหม่ Cyber Attack

จากการศึกษาพบว่า หน่วยงานด้านความมั่นคงของประเทศทุกระดับ ให้ความสำคัญกับการรับมือภัยคุกคามรูปแบบใหม่ Cyber Attack สภาความมั่นคงแห่งชาติ กำหนดให้มีการออกแนวทางการเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศ และไซเบอร์ ซึ่งเป็นข้อที่ ๑๐ ในนโยบายความมั่นคงของชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔

กระทรวงกลาโหม เช่นกัน ได้ร่างแผนแม่บทไซเบอร์ เพื่อป้องกันประเทศ กระทรวงกลาโหม ปี พ.ศ. ๒๕๖๐ - ๒๕๖๔ และแต่ละเหล่าทัพ ซึ่งคือ กองทัพบก กองทัพเรือ กองทัพอากาศ ได้มีการจัดตั้งศูนย์ไซเบอร์เหล่าทัพ ในส่วนของกองทัพบกเอง ได้จัดตั้งศูนย์ไซเบอร์กองทัพบก และเริ่มดำเนินการตั้งแต่ ๑ ต.ค.๕๗ เป็นต้นมา มีหน้าที่ปฏิบัติการทางไซเบอร์ ในการเฝ้าระวัง แจ้งเตือน ป้องกัน แก้ปัญหาภัยคุกคามด้านไซเบอร์ ให้ความรู้ สร้างความตระหนัก และกำหนดมาตรการรักษาความปลอดภัยด้านไซเบอร์ ให้แก่หน่วยทหารในกองทัพบก และปฏิบัติการข่าวสาร (IO) ด้านไซเบอร์เพื่อสนับสนุนภารกิจอื่นๆ ของกองทัพบก

๓. ระบบการฝึก - ศึกษา ของกองทัพบก ปัจจุบันยังไม่รองรับ ภัยคุกคามรูปแบบใหม่ Cyber Attack

จากการศึกษาของผู้วิจัยพบว่ากำลังพลส่วนใหญ่ของกองทัพบก มีความรู้เรื่องดังกล่าวน้อย ตลอดจนระบบการฝึก - ศึกษา ของกองทัพบกในปัจจุบันไม่ว่า การฝึกตามวงรอบประจำปีของกองทัพบก การฝึกพิเศษ หรือแม้กระทั่ง การฝึกที่หน่วยกำหนดขึ้นเองตามความริเริ่มของหน่วย (Unit School) ยังไม่รองรับภัยคุมคามในเรื่องดังกล่าว ทั้งนี้อาจเป็นเพราะ

๑. ยังไม่มีนโยบายชัดเจนจากกองทัพบก ให้ดำเนินการฝึกในเรื่องดังกล่าว

๒. ยังไม่มีการจัดทำเป็นหลักสูตรการฝึก ซึ่งมีการกำหนดความมุ่งหมายวิชาในการฝึก หลักฐานการฝึก ตลอดจนเครื่องช่วยฝึก

๓. ขาดบุคลากรในการเป็น ครูฝึก - อบรม

ข้อเสนอแนะ

ผู้วิจัยขอเสนอแนะแนวทางในการพัฒนารูปแบบการฝึกทหาร เพื่อรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ดังนี้

๑. กรมยุทธศึกษาทหารบก เสนอผู้บังคับบัญชาในการอนุมัติให้มีการฝึก - อบรม เกี่ยวกับวิชาเทคโนโลยีสารสนเทศและการสื่อสาร ในหลักสูตรเพิ่มพูนความรู้ ให้กับกำลังพลประจำการและให้กรมยุทธศึกษาทหารบก บรรจุวิชาดังกล่าวในหลักสูตรการฝึกทหารใหม่

๒. ศูนย์ไซเบอร์กองทัพบก ร่วมกับ กรมยุทธศึกษาทหารบก ในการกำหนดหลักสูตร ความมุ่งหมาย ขอบเขตเนื้อหา เตรียมเครื่องช่วยฝึก เพื่อเตรียมเปิดการฝึก - อบรม และเตรียมบรรจุในหลักสูตรทหารใหม่

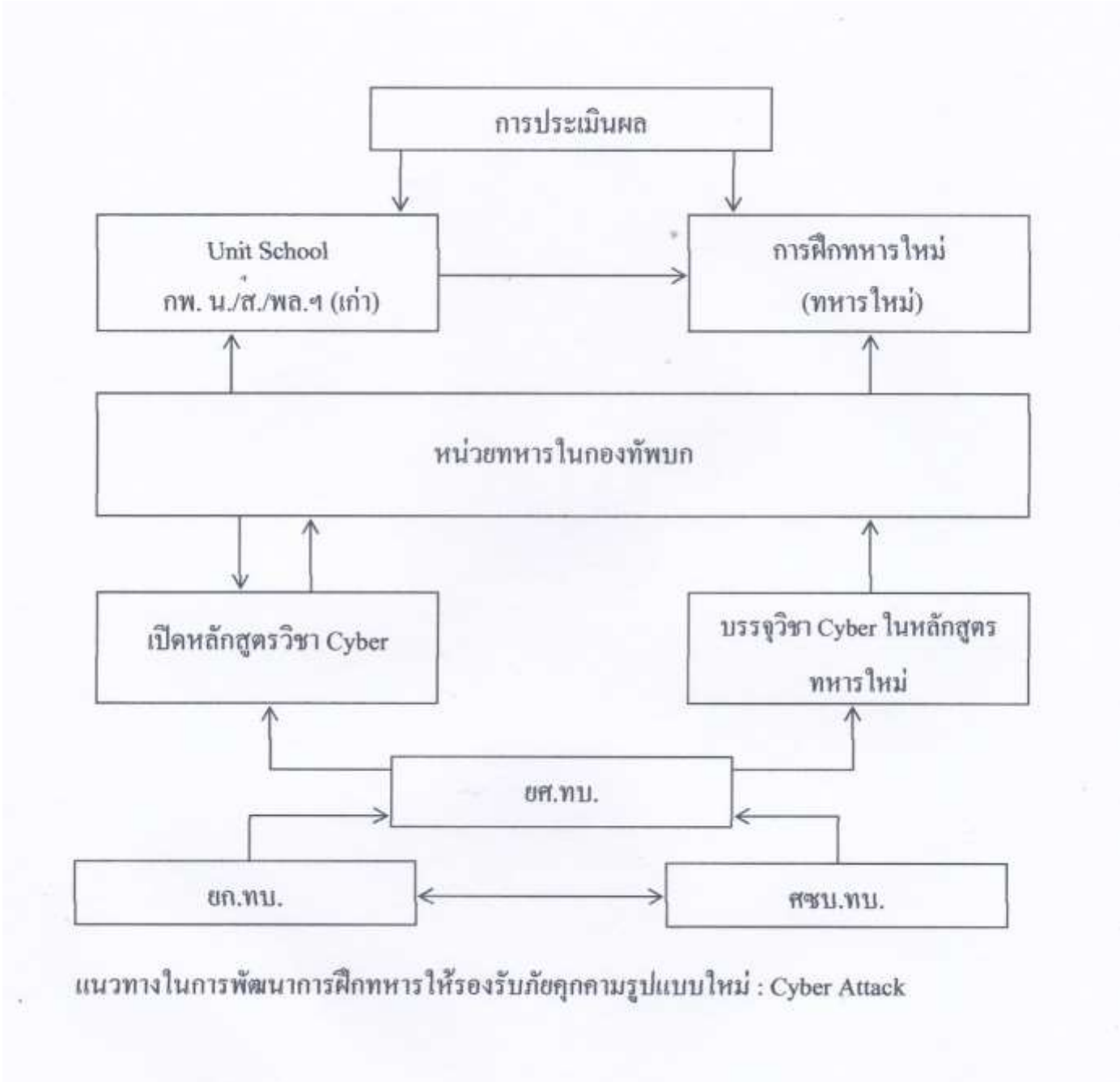
๓. กรมยุทธศึกษาทหารบก ทำการเปิดหลักสูตรที่ส่วนกลาง โดยให้หน่วยในกองทัพบกส่งกำลังพลมาทำการฝึก - อบรม

๔. หลังจากรับการฝึก - อบรมแล้ว ให้กำลังพลที่ผ่านการอบรมกลับหน่วยไปขยายผลใน Unit School ของหน่วย โดยพิจารณากำลังพลที่ผ่านการอบรม และมีขีดความสามารถในการถ่ายทอดได้ ส่วนหนึ่งไปเป็นครูฝึกทหารใหม่ เพื่อฝึก - อบรม ให้แก่ทหารใหม่ ในรายวิชาเทคโนโลยีสารสนเทศ และการสื่อสาร กรมยุทธศึกษาทหารบก บรรจุเข้าไปใหม่ในหลักสูตรทหารใหม่

๕. มีการประเมินผลการฝึก - อบรม ทั้งการจัดการฝึก การฝึกของหน่วยเอง Unit School และการฝึกทหารใหม่ โดยคณะกรรมการจาก กรมยุทธศึกษาทหารบก และศูนย์ไซเบอร์ทหารบก

ผู้วิจัยขอเสนอ โครงร่าง (Frame Work) ประกอบข้อเสนอแนะตามแผนภาพที่ ๕ - ๑ ดังนี้

แผนภาพที่ ๕ - ๑ โครงร่าง แนวทางในการพัฒนาการฝึกทหาร ให้รองรับภัยคุกคามรูปแบบใหม่ Cyber Attack



แนวทางในการพัฒนาการฝึกทหารให้รองรับภัยคุกคามรูปแบบใหม่ : Cyber Attack

ผู้วิจัยเชื่อมั่นเป็นอย่างยิ่งว่า หากกองทัพบกได้ดำเนินการตามโครงร่าง (Frame Work) ที่ผู้วิจัยนำเสนอนี้ ภายในระยะเวลา ๒ ปี กำลังพลของกองทัพบกในทุกระดับ จะมีความรู้ความสามารถ เกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร สามารถปฏิบัติงานกับเทคโนโลยีในหน่วยงานของตนได้อย่างมีประสิทธิภาพ และมีความปลอดภัย สามารถรองรับนโยบายเกี่ยวกับด้านเทคโนโลยีสารสนเทศ ของกองทัพบก และกระทรวงกลาโหมเป็นอย่างดี ตลอดจนกองทัพบกจะมีภูมิต้านทานที่เข้มแข็งต่อภัยคุกคามรูปแบบใหม่ Cyber Attack ในยุคโลกไร้พรมแดน

บรรณานุกรม

วารสาร

ศิวลีย์ สิริโรจน์บริรักษ์. “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม”, วารสารสถาบันวิชาการป้องกันประเทศ. ปีที่ ๖ (ฉบับที่ ๓), พฤษภาคม - สิงหาคม ๒๕๕๘. หน้า ๑๙ - ๒๙.

เอกสารวิจัย

ณฐพนธ์ ศรีสวัสดิ์. “การพัฒนาบุคลากรของกองทัพและภาครัฐเพื่อ เอาชนะปัญหาภัยคุกคามต่อความมั่นคงของชาติ”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๘.

เดชณรงค์ สุทธิชาญบัญชา. “แนวทางการพัฒนาการฝึกของกองทัพไทยกับประเทศสมาชิกอาเซียนต่อภัยคุกคามรูปแบบใหม่”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๖.

สิงห์ทอง หมีทอง. “การพัฒนารูปแบบการจัดการภัยคุกคามรูปแบบใหม่ กรณีศึกษาภัย จากความยากจน”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๘.

เอกสารไม่ตีพิมพ์

กองทัพบก. “แบบฝึกบุคคลท่ามือเปล่า”. คู่มือการฝึก. ๒๕๕๙.

กองทัพบก. “แบบฝึกบุคคลท่าอาวุธ”. คู่มือการฝึก. ๒๕๕๙.

ยุทธศึกษาทหารบก, กรม “การฝึกทหารใหม่เบื้องต้นทั่วไป สำหรับทหาร ทุกเหล่าของกองทัพบก (๑๐ สัปดาห์)”. ระเบียบและหลักสูตรการฝึก. ๒๕๕๑.

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย. “เอกสารวิเคราะห์สถานการณ์ยุทธศาสตร์และความมั่นคง” (ฉบับที่ ๗/๖๐), ๑๔ - ๒๐ พ.ย.๒๕๕๙. หน้า ๑ – ๒.

ฐานข้อมูลอิเล็คทรอนิกส์

คณะอนุกรรมาธิการพิจารณาศึกษาสื่อสังคมออนไลน์กับภัยคุกคามต่อความมั่นคงของชาติ. “รายงานการพิจารณาศึกษา เรื่อง สื่อสังคมออนไลน์ ภัยคุกคามต่อความมั่นคงของชาติ”. (ออนไลน์).เข้าถึงได้จาก : http://www.senate.go.th/w3c/senate/pictures/comm/66/file_1353298809.pdf, ๒๕๕๐.

คมศักดิ์ เจียมวัฒนาเลิศ, พันเอก. “Social Network – IO กับความมั่นคงของชาติ”. (ออนไลน์). เข้าถึงได้จาก : http://6969.canadianforum.net/t8-topic, ๒๕๕๕.

ปรัชญา เฉลิมวัฒน์. “Cyberspace Doctrine หลักนิยมการรบในมิติไซเบอร์”. (ออนไลน์). เข้าถึงได้จาก : http://dopns.mi.th/KM/?p=176, ๒๕๕๘.

ยุทธศึกษาทหารบก, กรม. “คำแนะนำการฝึกทหารใหม่ ประจำปีงบประมาณ ๒๕๖๐”. (ออนไลน์). เข้าถึงได้จาก : http://www.attc-rta.com/download, ๒๕๖๐.

ฤทธี อินทราวุธ. “กองทัพบกกับความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ”. (ออนไลน์). เข้าถึงได้จาก: Dop.rta.mi.th/Web/data/Other/Block3/coo1.pdf. ๒๕๕๙.

ฤทธี อินทราวุธ. “ประชาคมไซเบอร์ของกองทัพ: ก้าวแรกสู่ประชาคมไซเบอร์ของชาติ”. (ออนไลน์). เข้าถึงได้จาก: http://rittee1834.blogspot.com/2016/02/blog-post.html. ๒๕๕๙.

ฤทธี อินทราวุธ, พลตรี. “สงครามข่าวสารกับสงครามสื่อ (Information warfare VS Media Warfare)”. (ออนไลน์). เข้าถึงได้จาก:http://6969.canadianforum.net/t8-topic, ๒๕๕๘.

ฤทธี อินทราวุธ. “ศูนย์ไซเบอร์กองทัพบก: เขี้ยวเล็บหรือเสือกระดาษ”. (ออนไลน์). เข้าถึงได้จาก: http://rittee1834.blogspot.com/2014/12/blog-post.html, ๒๕๕๗.

เศรษฐพงค์ มะลิสุวรรณ, พันเอก. “อาชญากรรมไซเบอร์ (Cyber Crime)”. (ออนไลน์). เข้าถึงได้จาก : https://www.it24hrs.com/2015/cyber-crime-cyber-attack/, ๒๕๕๘.

สภาความมั่นคงแห่งชาติ, สำนักงาน. “นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘-๒๕๖๔”. (ออนไลน์). เข้าถึงได้จาก:http://www.nsc.go.th/Download1/policy58.pdf, ๒๕๖๐.

ภาคผนวก

ผนวก ก
แบบสอบถาม
เรื่อง แนวทางการพัฒนารูปแบบการฝึกทหารเพื่อรองรับภัยคุกคามรูปแบบใหม่: ภัยคุกคามด้านไซเบอร์

วันเดือนปีที่กรอกแบบสอบถาม.....

ส่วนที่ ๑ ข้อมูลทั่วไปของผู้กรอกแบบสอบถาม

ชื่อ-นามสกุล..... เพศ.....อายุ.....ปี

ตำแหน่ง..... สังกัด .....

ส่วนที่ ๒ แบบสอบถามเกี่ยวกับภัยคุกคามรูปแบบใหม่ Cyber Attack

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย (/) เพียงหนึ่งข้อเท่านั้น เพื่อแสดงว่าท่านมีความคิดเห็นมากหรือน้อยเพียงใดกับข้อความข้างล่างนี้

๑.ท่านมีความเข้าใจเกี่ยวกับภัยคุมคามรูปแบบใหม่ Cyber Attack ระดับใด

❒ มาก ❒ ปานกลาง ❒ น้อย

๒. ท่านคิดว่าปัจจุบันกองทัพบก มีระดับความรู้เกี่ยวข้องกับภัยคุกคาม Cyber Attack ระดับใด

❒ มาก ❒ ปานกลาง ❒ น้อย

๓. ท่านคิดว่าปัจจุบันกำลังพลของกองทัพบก มีระดับความรู้เกี่ยวข้องกับภัยคุกคาม Cyber Attack ระดับใด

❒ มาก ❒ ปานกลาง ❒ น้อย

๔. ท่านรู้จักหน่วยงาน “ศูนย์ไซเบอร์กองทัพบก” ในเรื่องภารกิจของหน่วยระดับใด

❒ มาก ❒ ปานกลาง ❒ น้อย

๕. ท่านเคยมีการประสานงานกับศูนย์ไซเบอร์กองทัพบก ในอดีตที่ผ่านมาหรือไม่

❒ หลายครั้ง ❒ น้อยครั้ง ❒ ไม่เคย

๖. ท่านคิดว่ากำลังพลในกองทัพบก มีความรู้เรื่องเทคโนโลยีสารสนเทศอย่างเหมาะสม และรู้วิธีเบื้องต้นในการต่อต้าน Cyber Attack หรือไม่

❒ จำเป็น ❒ ไม่จำเป็น

๗. เคยมีการฝึกอบรมเกี่ยวกับ Cyber Attack ในหน่วยงานที่ท่านสังกัดหรือไม่

❒ หลายครั้ง ❒ น้อยครั้ง ❒ ไม่เคยมี

๘. ท่านคิดว่ากำลังพลระดับใด ล่อแหลมต่อการตกเป็นเครื่องมือของ Cyber Attack มากที่สุด

❒ นายทหารสัญญาบัตร ❒ นายทหารประทวน ❒ ทหารกองประจำการ

๙. ท่านคิดว่ากำลังพลระดับใดล่อแหลมต่อการตกเป็นเครื่องมือของ Cyber Attack มากที่สุด

❒ ควรมี ❒ ไม่ควรมี/เพราะ.....

๑๐. หากมีการฝึกอบรมเรื่องดังกล่าว ควรมีการอบรม (ตอบได้มากกว่า ๑ ข้อ)

❒ สอดแทรกตารางการฝึกตามวงรอบประจำปี

❒ สอดแทรกตอนฝึกทหารใหม่

❒ จัด Unit School ภายในหน่วย

❒ ควรส่งไปอบรมนอกหน่วย (หลักสูตรที่หน่วยที่เกี่ยวข้องจัดให้)

๑๑. ท่านคิดว่าการฝึกทหารใหม่ในปัจจุบันรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack หรือไม่

❒ รองรับ ❒ ไม่รองรับ

๑๒. ท่านคิดว่าหากนำเรื่อง Cyber Attack บรรจุลงในการฝึกทหารใหม่จะมีความเหมาะสมหรือไม่

❒ เหมาะสม ❒ ไม่เหมาะสม

๑๓. หากมีการบรรจุเรื่อง Cyber Attack ในหลักสูตรทหารใหม่ ควรให้ความรู้เรื่องอะไรบ้าง

๑๓.๑ .....

๑๓.๒ .....

๑๓.๓ .....

๑๓.๔ .....

๑๓.๕ .....

๑๔. สิ่งที่จำเป็นต้องเตรียมการหากนำเรื่อง Cyber Attack มาบรรจุในหลักสูตรทหารใหม่ควรมีอะไรบ้าง

๑๔.๑ .....

๑๔.๒ .....

๑๔.๓ .....

๑๔.๔ .....

๑๔.๕ .....

ขอขอบคุณในการกรอกแบบสอบถาม ข้อมูลของท่านจะเป็นประโยชน์ต่อการดำเนินการวิจัย เรื่อง แนวทางการพัฒนารูปแบบการฝึกทหารเพื่อรองรับภัยคุกคามรูปแบบใหม่ : ภัยคุกคามด้านไซเบอร์ เป็นอย่างมาก

ผนวก ข
แบบสัมภาษณ์ผู้ให้ข้อมูลสำคัญ
เรื่อง แนวทางการพัฒนารูปแบบการฝึกทหารเพื่อรองรับภัยคุกคามรูปแบบใหม่: ภัยคุกคามด้านไซเบอร์

วันเดือนปีที่สัมภาษณ์.....

ส่วนที่ ๑ ข้อมูลทั่วไปของผู้ถูกสัมภาษณ์

ชื่อ-นามสกุล..... เพศ.....อายุ.....ปี

ตำแหน่ง..... สังกัด .....

ส่วนที่ ๒ คำถาม

๑. ระบบการฝึกของกองทัพบกไทยในภาพรวม

.....

.....

.....

๒. ระบบการฝึกของกองทัพบกไทย รองรับภัยคุกคามรูปแบบใหม่ Cyber Attack หรือไม่

.....

.....

.....

๓. มีแนวคิดอย่างไร ในการทำให้กำลังพลของกองทัพบกสามารถใช้เทคโนโลยีสารสนเทศ และการสื่อสาร อย่างมีวินัย ไม่ตกเป็นเครื่องมือของ Cyber Attack

.....

.....

.....

ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

.....

ขอขอบคุณในการให้สัมภาษณ์ ข้อมูลของท่านจะเป็นประโยชน์ต่อการดำเนินการวิจัย เรื่อง แนวทางการพัฒนารูปแบบการฝึกทหารเพื่อรองรับภัยคุกคามรูปแบบใหม่ : ภัยคุกคามด้านไซเบอร์ เป็นอย่างมาก

ประวัติย่อผู้วิจัย

ชื่อ พลตรีศตวรรษ รามดิษฐ์

วัน เดือน ปีเกิด ๑๖ กันยายน พ.ศ.๒๕๐๔

การศึกษา
โรงเรียนเตรียมทหาร
โรงเรียนนายร้อยพระจุลจอมเกล้า
หลักสูตรปฐมนิเทศนายทหารใหม่ รุ่นที่ ๗
หลักสูตรเจ้าหน้าที่ฝ่ายปฏิบัติการรบร่วมอากาศ-พื้นดิน รุ่นที่ ๗๔
หลักสูตรปรับการยิงปืนใหญ่โดยทหารพลรบ รุ่นที่ ๑
หลักสูตรชั้นนายร้อย รุ่นที่ ๗๖ (ชกท.๑๕๔๒)
หลักสูตรชั้นนายพัน รุ่นที่ ๕๕ (ชกท.๑๕๔๒)
หลักสูตรประจำ รร.สธ.ทบ. ชุดที่ ๗๖ (ชกท.๐๐๑๒)
หลักสูตรนายทหารปลัดบัญชีระดับบริหาร รุ่นที่ ๑๕

ประวัติการทำงานโดยย่อ
รองผู้บังคับการกรมทหารราบที่ ๒ รักษาพระองค์
ผู้บังคับการกรมทหารราบที่ ๒ รักษาพระองค์
รองผู้บัญชาการมณฑลทหารบกที่ ๑๒
ผู้ทรงคุณวุฒิกองทัพบก

ตำแหน่งปัจจุบัน ผู้บัญชาการมณฑลทหารบกที่ ๑๒

สรุปย่อ

ลักษณะวิชา การทหาร

เรื่อง แนวทางการพัฒนารูปแบบการฝึกทหารเพื่อรองรับภัยคุกคามรูปแบบใหม่

ผู้วิจัย พลตรี ศตวรรษ รามดิษฐ์ หลักสูตร วปอ. รุ่นที่ 59

ตำแหน่ง ผู้บัญชาการมณฑลทหารบกที่ 12

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทและมีความสำคัญต่อการดำเนินชีวิตประจำวัน ของมนุษย์เป็นอย่างมาก จะเห็นได้ว่าแทบจะทุกคนเกี่ยวข้องกับโทรศัพท์มือถือและมีการใช้งานเครือข่ายสังคมออนไลน์อย่างแพร่หลาย ทั้งในด้านการติดต่อสื่อสาร การส่งข้อมูล การสืบค้นข้อมูลด้านต่างๆ อย่างไม่มีขีดจำกัด ซึ่งสามารถกล่าวได้ว่าปัจจุบันเรากำลังอยู่ในยุคของโลกไร้พรมแดน

เทคโนโลยีสารสนเทศนั้นหากถูกนำมาใช้ในกิจกรรมเชิงสร้างสรรค์ ก็จะเป็นประโยชน์ต่อผู้ใช้และหน่วยงานอย่างมหาศาลแต่หากนำมาใช้ในทางที่ผิด เช่นนำมาเป็นเครื่องมือในการทำลายล้างฝ่ายตรงข้ามก็นับว่าเป็นภัยคุกคามรูปแบบใหม่ที่มีความร้ายแรงต่อมวลมนุษยชาติเช่นเดียวกัน

การโจมตีทางไซเบอร์ (Cyber Attack) ถือเป็นภัยคุกคามรูปแบบใหม่ซึ่งผู้ก่อการร้ายมุ่งกระทำต่อระบบเครือข่ายโทรคมนาคม และคอมพิวเตอร์ ด้วยวิธีการต่างๆ ที่หลากหลาย โดยมุ่งไปสู่การทำลายล้างองค์กรของฝ่ายตรงข้ามซึ่งโดยทั่วไปแล้วการโจมตีทางไซเบอร์ถูกแบ่งออกเป็น 3 ลักษณะใหญ่ๆ ดังนี้

1. การนำความลับขององค์กรออกมาเปิดเผย (Data Confidentiality)
2. การเปลี่ยนแปลง / บิดเบือนข้อมูล (Data Integrity)
3. การทำให้ระบบปฏิบัติการในเครือข่ายคอมพิวเตอร์หยุดให้บริการหรือไม่สามารถใช้งานได้ (System Availability)

ประเทศไทยเองก็ไม่แตกต่างจากประเทศอื่นๆ ทั่วโลกที่มีโอกาสเป็นเป้าหมายในการโจมตีของอาชญากรทางไซเบอร์ โดยมีเหตุผลการโจมตีที่หลากหลายและจากกลุ่มการโจมตีที่หลากหลาย ซึ่งล้วนแล้วแต่กระทบกระเทือนความมั่นคงของชาติเป็นอย่างมาก หน่วยงานที่เกี่ยวข้องกับความมั่นคงของประเทศทุกระดับต่างตระหนักถึงผลกระทบของภัยคุกคามดังกล่าวและมีการกำหนดมาตรการเพื่อรับมือจากการโจมตีรูปแบบนี้

สภาความมั่นคงแห่งชาติได้กำหนดเรื่องการเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ ในนโยบายความมั่นคงของชาติ พ.ศ.2558 - 2564 กระทรวงกลาโหมได้จัดทำร่างแผนแม่บทไซเบอร์เพื่อป้องกันประเทศ กระทรวงกลาโหม ปี พ.ศ.2560 - 2564 และในแต่ละเหล่าทัพได้จัดตั้งศูนย์ไซเบอร์เหล่าทัพเพื่อปฏิบัติการแจ้งเตือน ป้องกัน และแก้ปัญหาภัยคุกคามด้านไซเบอร์

แม้มีการขับเคลื่อนในระดับนโยบายเพื่อรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ก็ตามก็ยังปรากฏข่าวสารตามสื่อต่างๆ ซึ่งเป็นข้อมูลในด้านลบ และทำลายความเชื่อมั่นและศรัทธาของสถาบันทหารซึ่งเป็นเสาหลักของความมั่นคงอยู่เสมอ ไม่ว่าจะเป็นการที่มีภาพหรือคลิปวีดีโอกิจกรรมที่ไม่เหมาะสมถูกเผยแพร่สู่สาธารณะ มีการนำความลับทางราชการที่เกี่ยวกับระบบการจัดซื้ออุทโธปกรณ์ทางทหารออกมาเผยแพร่สู่สาธารณะอย่างบิดเบือน ทำให้ประชาชนบางส่วนเชื่อว่ามีการทุจริตในระบบการจัดซื้อของทางราชการ มีการเผยแพร่แนวความคิดที่หมิ่นสถาบันเบื้องสูง มีการเผยแพร่ข้อมูลที่เป็นลบต่อรัฐบาลและกองทัพ และการสร้างความแตกแยกของคนในชาติโดยใช้เครื่องมือเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งสื่อสังคมออนไลน์ ทั้งหมดนี้ได้นำความเสียหายมาสู่รัฐบาลและกองทัพเป็นอย่างมาก ตลอดจนการดำเนินการจับกุมผู้กระทำผิดมาดำเนินคดี เป็นเรื่องที่ยากมาก

ดังนั้นการที่จะสนับสนุนให้การขับเคลื่อนทางนโยบายของหน่วยระดับกองทัพและกระทรวงกลาโหม มีประสิทธิภาพนั้น ทุกๆหน่วยทหารจะต้องให้ความสำคัญในเรื่องการสร้างความรู้ความเข้าใจ และวินัยในการใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารให้กำลังพลในหน่วยอย่างจริงจังซึ่งแนวทางการเสริมสร้างความรู้อาจกระทำได้โดยการจัดการฝึกอบรมให้กำลังพลในโอกาสต่างๆ ซึ่งโดยปกติกองทัพบกมีระบบการฝึก-ศึกษา ที่ชัดเจนอยู่แล้วแต่เนื้อหาการฝึก - ศึกษารูปแบบปัจจุบันอาจไม่รองรับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack ซึ่งในงานวิจัยฉบับนี้จะเป็นการศึกษาวิจัยหาแนวทางในการพัฒนา การฝึกทหารของกองทัพบกให้สามารถรองรับภัยคุกคามรูปแบบใหม่ Cyber Attack ซึ่งนับเป็นก้าวสำคัญในการปรับตัวให้สามารถเผชิญกับภัยคุกคามรูปแบบใหม่ในยุคโลกไร้พรมแดนได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ของการวิจัย

1. เพื่อทำการศึกษาหาข้อมูลภัยคุกคามรูปแบบใหม่ Cyber Attack ซึ่งมีผลกระทบด้านความมั่นคงของชาติ

2. เพื่อทำการศึกษาระบบการฝึก - ศึกษาของกองทัพบกไทยในปัจจุบัน

3. เพื่อทำการเสนอแนวความคิดในการสร้างการรับรู้และจิตสำนึกของบุคลากรในกองทัพบกในการใช้เทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม และปลอดภัยต่อ Cyber Attack โดยการจัดหลักสูตรการฝึกอบรมเพิ่มเติมจากการฝึก - ศึกษาปกติของหน่วยทหารในกองทัพบก

ขอบเขตของการวิจัย

1. จะทำการวิจัยภัยคุกคามรูปแบบใหม่ ในเรื่อง Cyber Attack เท่านั้น
2. การศึกษาผลกระทบของภัยคุกคามรูปแบบใหม่จะศึกษาเฉพาะกรณี ความมั่นคง เท่านั้น
3. จะทำการศึกษาระบบการฝึก - ศึกษา ของกองทัพบกไทย เท่านั้น

วิธีดำเนินการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยจะเริ่มต้นด้วยการเก็บข้อมูลทุติยภูมิ (Secondary Data) โดยการทบทวนวรรณกรรมที่เกี่ยวข้องในเรื่อง เกี่ยวกับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack และจะทำการศึกษาหาข้อมูล และทำความเข้าใจเกี่ยวกับระบบการฝึก - ศึกษาของกองทัพบกไทย โดยมุ้งเน้นไปที่หลักสูตรการฝึกทหารใหม่ตลอดจนการศึกษางานวิจัยในอดีตที่เกี่ยวข้องกับเรื่องดังกล่าว

หลังจากนั้นจะทำการเก็บข้อมูลปฐมภูมิ (Primary Data) โดยการทำการออกแบบสอบถาม (Questionnaire Survey) เพื่อเก็บข้อมูลจากผู้บังคับหน่วย ฝ่ายเสนาธิการ และครูฝึกทหารใหม่ในพื้นที่ จังหวัดปราจีนบุรี จำนวน 40 ชุด และได้ทำการสัมภาษณ์ พ.อ.มหิธร บุญครอง หัวหน้ากองยุทธการ มณฑลทหารบกที่ 12 ซึ่งมีหน้าที่โดยตรงในการวางแผน อำนวยการ และกำกับดูแลระบบการฝึก และการใช้กำลังของหน่วยให้เป็นไปตามนโยบายของกองทัพบก

หลังจากนั้นจะนำข้อมูลที่ได้ทั้งหมดมาทำการวิเคราะห์โดยละเอียด และทำการสรุปผลการวิจัย และนำเสนอข้อเสนอแนะในบทสุดท้ายของงานวิจัยต่อไป

ผลการวิจัย

จากการดำเนินการวิจัยในเรื่องแนวทางการพัฒนารูปแบบการฝึกทหารเพื่อรองรับภัยคุกคามรูปแบบใหม่ : Cyber Attack มีผลการวิจัยสรุปได้ดังนี้

ภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack มีผลกระทบที่ร้ายแรงต่อความมั่นคงของชาติโดยมีการโจมตีได้ 3 ลักษณะใหญ่ๆ คือ

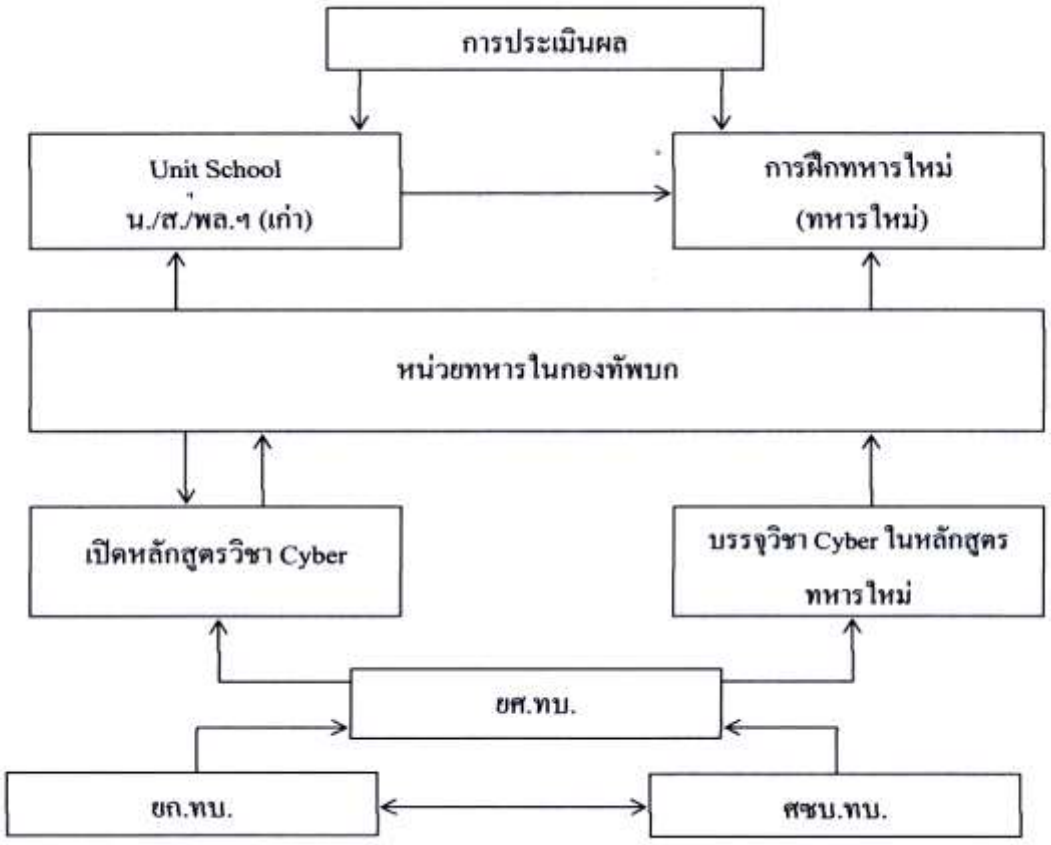
1. การล้วงความลับขององค์กรและนำออกมาเปิดเผยสู่สาธารณะ (Data Confidentiality)
2. การเปลี่ยนแปลง/บิดเบือนข้อมูลขององค์กร (Data Integrity)
3. การทำลายระบบปฏิบัติการของเครือข่ายคอมพิวเตอร์ขององค์กร (System Availability)

ซึ่งปัจจุบันหน่วยงานด้านความมั่นคงทุกระดับของประเทศได้ให้ความสำคัญในการรับมือกับภัยคุกคามรูปแบบดังกล่าว แต่ปัญหาของกองทัพบกที่ผู้วิจัยได้พบคือกำลังพลส่วนใหญ่ของกองทัพบกยังขาดความรู้ ความเข้าใจ ขาดวินัย และจิตสำนึกในการใช้เทคโนโลยีสารสนเทศตลอดจนขาดองค์ความรู้เกี่ยวกับภัยคุกคามรูปแบบใหม่ด้าน Cyber Attack แม้ทุกคนตระหนักดีว่าเป็นภัยคุกคามที่สำคัญและมีผลกระทบที่รุนแรงต่อความมั่นคงของชาติ จากการวิจัยพบว่า

ระบบการฝึก - ศึกษาของกองทัพบกในปัจจุบันยังไม่รองรับภัยคุกคามประเภทดังกล่าว เพราะระบบการฝึก - ศึกษาของกองทัพบกปัจจุบันยังคงมุ่งเน้นไปที่การรับมือภัยคุกคามรูปแบบเดิมๆ โดยใช้วิธีการปฏิบัติการทางทหาร ดังนั้นจึงสมควรอย่างยิ่งที่จะมีการพัฒนาระบบการฝึก – ศึกษา ทางทหาร โดยเริ่มต้นการดำเนินการโดยหน่วยงานที่เกี่ยวข้องกับการฝึก - ศึกษาของกองทัพบกซึ่งคือกรมยุทธการทหารบกและ กรมยุทธศึกษาทหารบกจะต้องมีการดำเนินการวางแผนการกำหนดหลักสูตรการฝึกอบรมร่วมกับศูนย์ไซเบอร์กองทัพบก และดำเนินการฝึกอบรมอย่างเป็นขั้นเป็นตอนให้หน่วยทหารในกองทัพบกและมีระบบการขยายผลในเรื่องดังกล่าวอย่างเป็นรูปธรรมต่อไป

ข้อเสนอแนะ

จากการรวบรวมและวิเคราะห์ข้อมูลทั้งหมดผู้วิจัยมีความเห็นว่าความรู้เกี่ยวกับเรื่อง Cyber เป็นเรื่องจำเป็นสำหรับกำลังพลทุกระดับและทุกนายในกองทัพบก ทุกนายควรได้รับรู้และมีทัศนคติไปในทิศทางเดียวกันทั้งกองทัพบก โดยแนวความคิดในการพัฒนาการฝึกเป็นไปตามโครงร่าง (Frame Work) ด้านล่าง



แนวทางในการพัฒนาการฝึกทหารให้รองรับภัยคุกคามรูปแบบใหม่ : Cyber Attack

การนำเรื่อง Cyber มาถ่ายทอดความรู้แก่กำลังพลในกองทัพบกควรทำคู่ขนานกันทั้งการบรรจุวิชาดังกล่าวในหลักสูตรการฝึกทหารใหม่ซึ่งจะอยู่ในวงรอบการฝึกประจำปี และให้ทุกหน่วยจัด Unit School ซึ่งเป็นการฝึกตามความริเริ่มของหน่วย

โดยขั้นตอนการดำเนินการผู้วิจัยขอเสนอเป็นขั้นตอนดำเนินการดังนี้

ขั้นที่ 1 : ขั้นวางแผน กำหนดขอบเขต ความมุ่งหมายของหลักสูตร กระทำร่วมกันระหว่างกรมยุทธการทหารบก ศูนย์ไซเบอร์กองทัพบก และกรมยุทธศึกษาทหารบก

ขั้นที่ 2 : ขั้นการเตรียมเปิดหลักสูตรและเตรียมบรรจุวิชา Cyber ในการฝึกทหารใหม่จะเป็นหน้าที่ของกรมยุทธศึกษาทหารบก

ขั้นที่ 3 : ขั้นการดำเนินการเปิดหลักสูตร Cyber กระทำโดย กรมยุทธศึกษาทหารบก โดยหน่วยทหารในกองทัพบกส่งกำลังพลมาเข้ารับการศึกษา

ขั้นที่ 4 : ขั้นการเปิด Unit School และการฝึกทหารใหม่ที่มีวิชา Cyber บรรจุในหลักสูตรการฝึกจัดโดยหน่วย

ขั้นที่ 5 : ขั้นการประเมินผลโดยหน่วย/ยศ.ทบ.

ผู้วิจัยเชื่อว่าหากกองทัพบกมีการดำเนินการตามโครงร่าง (Frame Work) ตามที่ผู้วิจัยเสนอนี้ภายในระยะเวลา 2 ปี กำลังพลในกองทัพบกจะมีความรู้ ความสามารถในเรื่องที่เกี่ยวกับเทคโนโลยีสารสนเทศ และการสื่อสาร สามารถปฏิบัติงานกับเทคโนโลยีของหน่วยงานของตนได้อย่างมีประสิทธิภาพ และมีความปลอดภัยรองรับนโยบายเกี่ยวกับด้านเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพบกและกระทรวงกลาโหมได้เป็นอย่างดี และมีภูมิต้านทานที่เข้มแข็งต่อภัยคุกคามรูปแบบใหม่ Cyber Attack ในยุคโลกไร้พรมแดน