แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัย ของกองทัพบกในอนาคต

โดย

พลตรี วาสิฏฐ์ มณีโชติ
ผู้ทรงคุณวุฒิกองทัพบก
กองทัพบก

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๕๙
ประจำปีการศึกษา พุทธศักราช ๒๕๕๙-๒๕๖๐

บทคัดย่อ

เรื่อง แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย พล.ต. วาสิฏฐ์ มณีโชติ หลักสูตร วปอ. รุ่นที่ ๕๕

งานวิจัยเรื่องแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต มีวัตถุประสงค์เพื่อ ๑) ศึกษารูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน ๒) ศึกษารูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ ๓) ศึกษารูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบก และ ๔) นำเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ โดยศึกษาค้นคว้าเชิงเปรียบเทียบ และรวบรวมข้อมูลเพื่อนำมากำหนดเป็นรูปแบบที่เหมาะสมและร่างแนวทางที่จะนำมาใช้ในกองทัพบก กลุ่มเป้าหมาย ได้แก่ ผู้ที่เกี่ยวข้องกับการรักษาความปลอดภัยและความมั่นคงของกองทัพบก รวมถึงผู้เชี่ยวชาญด้านนวัตกรรมและเทคโนโลยี จำนวน ๑๒ คน ได้มาจากการเลือกแบบเจาะจงโดยอาศัยความสะดวก เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์แบบไม่มีโครงสร้าง การวิเคราะห์และสังเคราะห์ข้อมูลตามหลักการวิจัยเชิงคุณภาพโดยวิธีพรรณนาเชิงวิเคราะห์และตรวจสอบข้อมูลโดยใช้วิธีการสามเส้า

ผลการวิจัยพบว่ารูปแบบการรักษาความปลอดภัยในอดีตจนถึงปัจจุบันได้มีการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยตามระดับความสำคัญ หน้าที่ความรับผิดชอบ และกำลังงบประมาณ ส่วนรูปแบบการรักษาความปลอดภัยในต่างประเทศขึ้นอยู่กับการแบ่งประเภทโดยยึดรูปแบบการดำเนินการทางการทหารสมัยใหม่ตามรูปแบบของกองทัพสหรัฐอเมริกาเป็นส่วนใหญ่ รวมถึงมีการปรับปรุงรูปแบบและวิธีการให้เหมาะสมอยู่เสมอ อีกทั้งศักยภาพของรูปแบบและวิธีการอาจขึ้นอยู่กับลักษณะภูมิประเทศและสภาพทางเศรษฐกิจของประเทศนั้นด้วย รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคตจากการสัมมนาอิงผู้เชี่ยวชาญพบว่าประกอบด้วย ๕ องค์ประกอบ ได้แก่ ๑) นโยบายด้านความปลอดภัย ๒) การกำหนดโครงสร้าง แนวปฏิบัติ และรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง ๓) นวัตกรรมและเทคโนโลยี ๔) กระบวนการสร้างความเข้าใจกับประชาชนและเจ้าหน้าที่ และ ๕) การบริหารและการประเมินความเสี่ยง การรักษาความปลอดภัยของกองทัพให้ได้มาตรฐานถือว่าเป็นเรื่องสำคัญที่ต้องดำเนินการ ทั้งนี้ก็เพื่อกำหนดขีดความสามารถด้านการรักษาความปลอดภัยของบุคลากรและสถานที่ให้มีความมั่นคงปลอดภัยมากที่สุด

คำนำ

รายงานการวิจัยเรื่อง “แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต” จัดทำขึ้นเพื่อนำข้อมูลและรายงานการวิจัยดังกล่าวมาเป็นประโยชน์ในการกำหนดมาตรฐานการรักษาความปลอดภัยของกองทัพบก โดยการศึกษาครั้งนี้ได้ดำเนินการออกแบบวิเคราะห์ สังเคราะห์ เพื่อหาแนวทางและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยของกองทัพบกในยุคสังคมเศรษฐกิจดิจิทัลที่สามารถนำไปใช้งานได้จริงและมีความมั่นคงปลอดภัยต่อการรักษาความปลอดภัยของกองทัพบกไทย ดังนั้นการจัดทำวิจัยดังกล่าวจึงเป็นแนวทางเพื่อพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกไทยให้เป็นไปตามนโยบายของประเทศที่เปลี่ยนแปลงเข้าสู่ยุคไทยแลนด์ ๔.๐ ต่อไป

พล.ต.
(วาสิฏฐ์ มณีโชติ)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๕๙
ผู้วิจัย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

คำอธิบายคำย่อ

ภาษาไทย

กอ.รมน.	ย่อมาจาก	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร
ชกท.	ย่อมาจาก	ความชำนาญการทางทหาร

ภาษาต่างประเทศ

SSG	ย่อมาจาก	Security Sector Governance
SSR	ย่อมาจาก	Security Sector Reform
CCTV	ย่อมาจาก	Close Circuit Television System
IO	ย่อมาจาก	Information Operations
NIST	ย่อมาจาก	National Institute of Standards and Technology
IT	ย่อมาจาก	Information Technology

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

หลังสิ้นสุดสงครามเย็น โลกได้พัฒนาเข้าสู่ยุคแห่งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วและไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยีได้นำมาซึ่งการเคลื่อนย้ายอย่างเสรีของผู้คน สินค้าและการบริการได้เพิ่มจำนวนขึ้นในอัตราที่ไม่เคยปรากฏมาก่อน เกิดความเชื่อมโยงอย่างกว้างขวางที่ทำให้บุคคลหรือผู้แสดงบทบาทที่ไม่ใช่รัฐ (Non-State Actor) มีอิทธิพลมากขึ้นในการดำเนินกิจกรรมต่างๆ ทั้งในระดับโลก ภูมิภาค หรือ ภายในรัฐชาติหนึ่งรัฐชาติใด อันส่งผลให้เกิดความท้าทายต่อความเป็นรัฐชาติ รวมถึงองค์การ ระหว่างประเทศ ประเทศที่พัฒนาแล้วได้ให้ความสนใจกับธรรมาภิบาลในงานด้านความมั่นคง (Security Sector Governance : SSG) ของประเทศต่างๆ โดยเป็นเรื่องเกี่ยวกับความโปร่งใสของกระบวนการ การปฏิบัติ ทัศนคติ ค่านิยม ธรรมเนียม และความรับผิดชอบด้านความมั่นคงต่อสาธารณะ ซึ่งต้องเป็นการปฏิบัติที่ชอบด้วยกฎหมายทั้งในและต่างประเทศ สำหรับธรรมาภิบาลในงานด้านความมั่นคงเป็นเรื่องที่มีความสลับซับซ้อน และที่สำคัญจะต้องมีความสอดคล้องกับสภาพแวดล้อมของประเทศหรือสังคม ดังนั้นประเทศต่างๆ จึงจำเป็นต้องปฏิรูปงานด้านความมั่นคง (Security Sector Reform : SSR) ของประเทศให้เป็นที่ยอมรับทั้งในประเทศและในสังคมโลกสภาวะความมั่นคงในปัจจุบันมีลักษณะความสัมพันธ์เกิดขึ้นในหลากหลายมิติ (Multidimensional Characteristics) และมีสภาพความเชื่อมโยงในรูปแบบของความมั่นคงเชิงองค์รวม (Comprehensive Security) ที่สามารถแปรเปลี่ยนและส่งผ่านผลกระทบได้อย่างรวดเร็วระหว่างมิติ ไม่ว่าจะเป็นมิติทางเศรษฐกิจ สังคม การเมือง วิทยาศาสตร์ เทคโนโลยีสิ่งแวดล้อม หรือการทหาร ซึ่งไม่ใช่กระบวนการแก้ไขปัญหาด้านความมั่นคงโดยใช้กรอบวิธีคิดเฉพาะทางด้านกำลังและอาวุธในลักษณะเดิมอีกต่อไป หรือไม่สามารถใช้วิธีคิดแบบรัฐชาติเพราะกรอบและวิธีคิดดังกล่าวไม่สามารถสนองตอบกับสภาพปัญหาที่เกิดขึ้นในลักษณะไร้พรมแดนในปัจจุบัน ความเจริญเติบโตทางเศรษฐกิจได้ช่วยบรรเทาความยากจนของประชากรแต่ด้วยเทคโนโลยีทันสมัยที่นำมาใช้ในการแสวงหาและใช้ทรัพยากรธรรมชาติ ได้ช่วยเร่งการใช้ทรัพยากรธรรมชาติซึ่งส่งผลในการทำลายสิ่งแวดล้อม และนำไปสู่ปัญหาการขาดแคลนทรัพยากรและแหล่งพลังงาน รวมทั้งยังเป็นการเร่งให้เกิดภัยพิบัติทางธรรมชาติที่รุนแรงตามมา

การขาดแคลนทรัพยากรและแหล่งพลังงานได้นำไปสู่ปัญหาความขัดแย้งเหนือพื้นที่อ้างสิทธิ์ทับซ้อน โดยเฉพาะพื้นที่ทางทะเลที่มีแนวโน้มเป็นแหล่งพลังงานใหม่และแหล่งการประมงที่อุดมสมบูรณ์ หรือเป็นเส้นทางการขนส่งที่สำคัญ และด้วยโลกที่เชื่อมต่อกันอย่างไม่เคยมีมาก่อน เหตุการณ์ในมุมหนึ่งของโลกย่อมเห็นและรับทราบได้ในอีกมุมหนึ่ง หลังเหตุการณ์ ๙/๑๑ เมื่อ พ.ศ. ๒๕๔๔ ที่มีกลุ่มผู้ก่อการร้ายได้ดำเนินการปล้นเครื่องบินชนตึกที่ประเทศสหรัฐอเมริกา หรือเหตุการณ์การก่อการร้ายสากลที่ฝรั่งเศส ในปี พ.ศ.๒๕๔๙ นี้ จะเห็นได้ว่ากลุ่มก่อการร้ายได้แผ่กระจายไปทั่วโลก และขยายวงไปสู่อุดมการณ์ความรุนแรงแม้ว่าจะไม่มีผู้นำและองค์กรที่ชัดเจน จึงมีโอกาสที่การก่อการร้ายจะดำรงอยู่และขยายตัวต่อไปตราบใดที่เงื่อนไขบ่มเพาะการก่อการร้ายยังไม่หมดไปกระแสโลกาภิวัตน์ทำให้การเชื่อมโยงในมิติต่างๆ รวดเร็วขึ้น โลกไซเบอร์มีผลต่อวัฒนธรรม วิถีชีวิต ทัศนคติ ความเชื่อ ความสัมพันธ์ระหว่างบุคคล กระบวนการเรียนรู้ และพฤติกรรมการบริโภคของประชาชน รวมทั้งทำให้แนวโน้มของความเสี่ยงต่อความมั่นคงด้านเทคโนโลยีสารสนเทศและเครือข่ายที่เกิดจากการคุกคามทางไซเบอร์มีสูงขึ้น โดยปัจจุบันหลายประเทศที่มีความขัดแย้งระหว่างกันได้มีการพัฒนาขีดความสามารถในการคุกคามทางไซเบอร์เพื่อลดความสามารถของฝ่ายตรงข้าม ทั้งความสามารถโดยทั่วไปของประเทศและกองทัพ ซึ่งทำให้หลายประเทศให้ความสำคัญต่อการคุกคามดังกล่าวและพัฒนาวิธีการป้องกันการคุกคามนี้มากขึ้น

นอกจากนี้สถานการณ์ในภูมิภาคเอเชีย-แปซิฟิก มีหลายพื้นที่และหลายประเด็นปัญหาซึ่งมีความเสี่ยงต่อเสถียรภาพด้านความมั่นคงของโลก อาทิ ข้อสงสัยเกี่ยวกับการพัฒนาขีดความสามารถด้านนิวเคลียร์ของบางประเทศ ปฏิบัติการของกลุ่มก่อการร้ายและกลุ่มหัวรุนแรงทั้งในระดับระหว่างประเทศและภายในประเทศรวมทั้งสถานการณ์ในทะเลจีนใต้ที่นับเป็นพื้นที่ศูนย์กลางที่สำคัญของภูมิภาคเอเชีย-แปซิฟิก ซึ่งความมั่นคงทางทะเลในบริเวณนี้ยังเป็นปัญหาที่มีความเปราะบางต่อการกระทบกระทั่ง ทั้งระหว่างประเทศที่มีข้อพิพาทด้านเส้นเขตแดนด้วยกันเองและกับประเทศนอกภูมิภาคเอเชียตะวันออกเฉียงใต้ กำลังกลายเป็นพื้นที่ที่หลายประเทศให้ความสนใจทั้งด้านความมั่นคงระดับภูมิภาคและผลประโยชน์แห่งชาติด้านการค้าและการลงทุนซึ่งสถานการณ์ดังกล่าวจะทำให้แต่ละประเทศในภูมิภาคมีแนวโน้มของการพัฒนาขีดความสามารถด้านการทหารเพื่อคุ้มครองผลประโยชน์ทางเศรษฐกิจของชาติ ทั้งด้วยตนเองและที่ได้รับการสนับสนุนจากประเทศอื่นในรูปแบบของความช่วยเหลือทางทหาร หรือการจัดหายุทโธปกรณ์ภายใต้เงื่อนไขและราคาที่เป็นพิเศษประเทศสมาชิกอาเซียนต่างมีความมุ่งมั่นในการสนับสนุนการรวมตัวเป็นประชาคมอาเซียนภายใน พ.ศ.๒๕๕๘ ซึ่งจะก่อให้เกิดความเปลี่ยนแปลงที่ดีทั้งด้านเศรษฐกิจสังคม และการเมือง รวมทั้งจะทำให้เกิดเสรีในการผ่านแดนมากขึ้น อย่างไรก็ตามการ

เปลี่ยนแปลงนี้อาจเอื้อให้เกิดการกระทำที่ผิดกฎหมายข้ามแดนได้ง่ายขึ้นเช่นกัน โดยเฉพาะการลักลอบค้ายาเสพติดปัญหาอาชญากรรมระหว่างประเทศ ปัญหาการหลบหนีเข้าเมืองโดยผิดกฎหมาย และการก่อการร้ายรวมทั้งอาจทำให้เกิดปัญหาโรคระบาดและโรคติดต่อ ซึ่งในเรื่องดังกล่าวน่าจะส่งผลให้ประเทศสมาชิกอาเซียนต้องกำหนดมาตรการป้องกันร่วมกันมากยิ่งขึ้นในขอบเขตประเทศรอบบ้านของประเทศไทยถึงแม้ยังคงมีปัญหาเส้นเขตแดนทั้งทางบกและทางทะเลเนื่องจากเป็นปัญหาที่สะสมมานับตั้งแต่ยุคล่าอาณานิคม อย่างไรก็ตามทุกประเทศได้พยายามแก้ไขปัญหาด้วยสันติวิธี และคาดหวังว่าเมื่อประเทศกลุ่มสมาชิกอาเซียนสามารถรวมตัวเป็นประชาคมอาเซียนได้แล้ว ปัญหาในเรื่องพรมแดนจะลดความสำคัญลงและประเทศเพื่อนบ้านจะมีความร่วมมือกันอย่างสร้างสรรค์ในทุกๆ ด้านมากยิ่งขึ้น โดยเฉพาะความร่วมมือในการแก้ไขปัญหาแนวชายแดนร่วมกันเพื่อให้เกิดความสงบสุขกับประชาชนตามแนวชายแดน

ในส่วนของประเทศไทยก็กำลังเผชิญกับยุคแห่งการเปลี่ยนแปลงที่รวดเร็วมากขึ้นและภายใต้กระแสประชาธิปไตย และสิทธิมนุษยชนของโลกในยุคปัจจุบันนั้น ประเทศไทยได้มีพัฒนาการทางการเมืองอย่างต่อเนื่อง ภายใต้การปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ซึ่งในทศวรรษที่ผ่านมาประชาชนได้มีความตื่นตัวในการมีส่วนร่วมทางการเมืองมากขึ้นและในหลายรูปแบบ อาทิ การจัดตั้งพรรคการเมืองขึ้นใหม่ การจัดตั้งกลุ่มผลประโยชน์และการรวมตัวกันเพื่อเรียกร้องสิทธิประโยชน์และความต้องการของกลุ่มมีจำนวนเพิ่มมากขึ้น ปัญหาการก่อเหตุรุนแรงอาทิ ก็อดอาร์มี่บุกยึดโรงพยาบาลศูนย์ราชบุรี การถูกปล้นปืน (คลังอาวุธ) ของกองพันพัฒนาที่ ๔ค่ายกรมหลวงนราธิวาสราชนครินทร์ บ้านปิเหล็งใต้ ตำบลมะรือโบออก อำเภอเจาะไอร้อง จังหวัดนราธิวาส โดยสังหารทหารที่เข้าเวรไป ๔๕ คนและปล้นอาวุธปืนไปทั้งหมด ๔๑๓ กระบอกเมื่อวันที่ ๔ ม.ค.๒๕๔๗ ซึ่งถือว่าเป็นจุดเริ่มต้นของความไม่สงบในจังหวัดชายแดนภาคใต้ของประเทศไทย โดยเรียกวันดังกล่าวว่า วันเสียงปืนแตก และในวันเดียวกันนั้นก็เกิดเหตุการณ์เผาโรงเรียนพร้อมกัน ๒๐ แห่งในจังหวัดนราธิวาสด้วยหลังจากนั้นได้มีเหตุการณ์ความรุนแรงหลายเหตุการณ์เกิดขึ้นตามมาอย่างต่อเนื่อง โดยตั้งแต่ พ.ศ.๒๕๔๗ เป็นต้นมาการก่อเหตุรุนแรงในจังหวัดชายแดนภาคใต้ยังคงมีอยู่ และได้นำมาซึ่งความรุนแรงของปัญหาทำให้เกิดความสูญเสียทั้งชีวิตประชาชนผู้บริสุทธิ์และเจ้าหน้าที่รัฐ รวมถึงงบประมาณจำนวนมากซึ่งยังคงเป็นปัญหาระดับชาติที่ทุกรัฐบาลกำหนดเป็นนโยบายเร่งด่วนในการแก้ไขปัญหาเพื่อความสงบสุขกลับคืนสู่พื้นที่โดยเร็วที่สุด ทั้งนี้จากการดำเนินการของทุกรัฐบาลอย่างจริงจัง ทำให้สถานการณ์ความรุนแรงมีแนวโน้มที่ดีขึ้น การที่ประเทศไทยมีที่ตั้งทางยุทธศาสตร์ที่สำคัญยิ่งโดยเป็นพื้นที่ศูนย์กลางของภูมิภาคเอเชียตะวันออกเฉียงใต้ที่สามารถเชื่อมโยงประเทศเพื่อนบ้าน

และอยู่ใกล้ประเทศที่มีประชากรโลกมากที่สุด ๒ ลำดับแรก คือ จีน และอินเดีย อีกทั้งเป็นจุดเชื่อมโยงเส้นทางการค้าและการขนส่งพลังงานที่สำคัญระหว่างมหาสมุทรแปซิฟิกและมหาสมุทรอินเดีย รวมทั้งพัฒนาการของสังคมโลกและภูมิภาคที่เปลี่ยนไปอย่างรวดเร็ว จึงได้นำมาซึ่งปัญหาความมั่นคงของไทยที่มีความยุ่งยากสลับซับซ้อนเพิ่มขึ้นในอีกหลายมิติ ไม่ว่าจะเป็นปัญหาอาชญากรรมข้ามชาติโดยเฉพาะการค้าอาวุธ การค้ายาเสพติด การค้ามนุษย์ การกระทำอันเป็นโจรสลัด อาชญากรรมคอมพิวเตอร์ และการก่อการร้ายสากล ประเทศไทยยังต้องเผชิญปัญหาการลักลอบเข้าเมืองโดยผิดกฎหมาย และปัญหาการแพร่ระบาดของยาเสพติดภายในประเทศ ซึ่งส่งผลกระทบต่อสภาพสังคมและความมั่นคงในระยะยาว นอกจากนี้ ปัญหาสิ่งแวดล้อมและภัยธรรมชาติเป็นอีกปัญหาหนึ่งที่สำคัญของไทยเป็นปัญหาที่เกิดจากความเสื่อมโทรมของธรรมชาติ และภัยพิบัติทางธรรมชาติ ดังที่กล่าวมาแล้วจะเห็นได้ว่าทุกเรื่องย่อมเกี่ยวข้องกับระบบรักษาความปลอดภัยแทบทั้งสิ้น ซึ่งภาครัฐควรเร่งหามาตรการในการรักษาความปลอดภัยโดยต้องพึ่งพานวัตกรรมและเทคโนโลยีสมัยใหม่อย่างหลีกเลี่ยงไม่ได้ (สำนักงานสภาความมั่นคงแห่งชาติ, ๒๕๕๘)

ดังนั้นจากปัญหาและการเปลี่ยนแปลงข้างต้นการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยควรเป็นไปเพื่อรองรับตามระดับความสำคัญ หน้าที่ความรับผิดชอบและกำลังงบประมาณของหน่วยงาน เนื่องจากส่วนงานต่างๆ ตามโครงสร้างที่ประกอบขึ้นเป็นหน่วยงานของกองทัพแต่ละส่วนมีระดับความสำคัญต่อหน่วยงานต่างกัน ตัวอย่างเช่น ส่วนงานเครื่องมืออุปกรณ์ของหน่วยงานหนึ่งมีความสำคัญมากกว่าส่วนงานระบบคอมพิวเตอร์ และในทางกลับกันสำหรับอีกหน่วยงาน ส่วนงานระบบคอมพิวเตอร์เป็นส่วนงานที่มีความสำคัญที่สุด เป็นต้น ฉะนั้น การวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยสถานที่ภายในหน่วยงานของกองทัพ จึงต้องมีระดับความเข้มงวดต่างกัน เพื่อมิให้เกิดบรรยากาศที่กดดันแก่ผู้ปฏิบัติงานในหน่วยงานนั้น อย่างไรก็ตาม การรักษาความปลอดภัยโดยเฉพาะสถานที่ทำการทางการทหารที่มีความสำคัญทางความมั่นคงนั้น จำเป็นต้องมีมาตรการป้องกันหรือป้องปรามที่เหมาะสม โดยมุ่งให้มีประสิทธิภาพสูงสุดเท่าที่จะดำเนินการได้และมีความพร้อมต่อการเผชิญกับเหตุร้าย และในโลกยุคดิจิทัล ภัยคุกคามและความท้าทายทางความมั่นคงของประเทศมักจะเข้ามาในรูปแบบใหม่ที่มีความซับซ้อนเพิ่มมากขึ้น โดยเฉพาะอย่างยิ่งเมื่อมีการนำเทคโนโลยีสมัยใหม่เข้ามาใช้ในการคุกคามจะทำให้เกิดการเปลี่ยนแปลงทั้งภาครัฐ ภาคเอกชน และภาคสังคม ซึ่งถือเป็นยุคเปลี่ยนผ่านและมีสภาพไม่แตกต่างจากยุคของการปฏิวัติอุตสาหกรรมในศตวรรษที่ ๑๙ เพียงแต่ในปัจจุบันนี้เป็นการปฏิวัติทางนวัตกรรมและเทคโนโลยีนั้นเอง โดยได้มีการพัฒนานวัตกรรมและเทคโนโลยีด้านการรักษาความปลอดภัยเพื่อนำมาใช้ควบคู่กับการรักษาความปลอดภัยตามมาตรการปกติ โดยเฉพาะ

อย่างยิ่งทางด้านฮาร์ดแวร์ที่มีระบบอิเล็กทรอนิกส์สมัยใหม่และซอฟต์แวร์ที่มีรูปแบบมาตรฐานตลอดจนความสามารถในการทำให้ระบบเป็นอัจฉริยะมากยิ่งขึ้น ซึ่งส่งผลให้เกิดโอกาสและถือเป็นความท้าทายต่องานรักษาความปลอดภัยด้านสถานที่ของหน่วยงาน โดยเฉพาะหน่วยงานที่มีความสำคัญทางความมั่นคงให้ได้ตระหนักถึงภัยคุกคาม และผลกระทบต่อความมั่นคงที่มีต่อสถานที่สำคัญ ซึ่งจะสร้างความยากลำบากให้กับหน่วยงานที่รับผิดชอบด้านการรักษาความปลอดภัย จึงมีความจำเป็นที่จะนำเทคโนโลยีสมัยใหม่มาใช้เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยและความมั่นคง โดยการนำเทคโนโลยีมาใช้นั้นมีความจำเป็นต้องมีการศึกษาและตรวจสอบอย่างละเอียดเพื่อให้มีความเป็นไปได้และเหมาะสมกับระเบียบรวมถึงมาตรการในการรักษาความปลอดภัยของกองทัพหรือหน่วยงานทางความมั่นคงอื่นๆ ที่มีคุณลักษณะใกล้เคียงกัน

อย่างไรก็ตามจากปัญหาด้านการรักษาความปลอดภัยและความสำคัญของหน่วยงานทางความมั่นคง จึงมีความจำเป็นในการพัฒนามาตรฐานการรักษาความปลอดภัย โดยทำการศึกษาเทคโนโลยีที่ทันสมัยและเหมาะสมมาใช้ในการรักษาความปลอดภัย มาตรฐานการรักษาความปลอดภัยจึงเป็นแนวทางหนึ่งที่เหมาะสมที่สามารถนำมาใช้แก้ปัญหาและสร้างความมั่นคงให้กับความปลอดภัยของหน่วยงานทางความมั่นคงได้เป็นอย่างดี ผู้วิจัยจึงเกิดแนวคิดและความสนใจที่จะศึกษาแนวทางและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยของกองทัพในอนาคต โดยการศึกษาค้นคว้าเพื่อดำเนินการออกแบบ วิเคราะห์ และสังเคราะห์แนวทางและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยของกองทัพในยุคสังคมเศรษฐกิจดิจิทัล ส่งผลให้เกิดแนวทางมาตรฐานที่สามารถนำไปใช้งานได้จริงและมีความมั่นคงปลอดภัยต่อการรักษาความปลอดภัยของกองทัพบกหรือเป็นรูปแบบสำหรับกองทัพและหน่วยงานความมั่นคงอื่นๆ ดังนั้นการจัดทำวิจัยดังกล่าวจึงสามารถแก้ปัญหาและเป็นไปตามนโยบายของประเทศที่จะเปลี่ยนแปลงในอนาคตต่อไป

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษารูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน

๒. เพื่อศึกษารูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ

๓. เพื่อศึกษารูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

๔. เพื่อนำเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

ขอบเขตของการวิจัย

การศึกษาวิจัยครั้งนี้เป็นการศึกษาหาแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต โดยการศึกษา ค้นคว้า รวบรวม ทบทวน วิเคราะห์และสังเคราะห์ ตามระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยกำหนดขอบเขตการวิจัยดังนี้

๑. ศึกษาค้นคว้าเชิงเปรียบเทียบแนวคิดและความเป็นมาของรูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน

๒. ศึกษาค้นคว้าเชิงเปรียบเทียบแนวคิดและความเป็นมาของรูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ

๓. ศึกษารวบรวม วิเคราะห์และสังเคราะห์รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

๔. ศึกษาทบทวนและให้ข้อเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกให้มีประสิทธิภาพมากยิ่งขึ้น และรองรับภัยคุกคามและความท้าทายในอนาคต

วิธีดำเนินการวิจัย

การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพและการประยุกต์ใช้องค์ความรู้อื่นทางสังคมศาสตร์ในลักษณะสหวิทยาการ (Inter-disciplinary Approach) เพื่อประกอบการพรรณนาเชิงวิเคราะห์ (Descriptive Analysis) โดยมีจุดมุ่งหมายเพื่อนำเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในยุคสังคมเศรษฐกิจดิจิทัลโดยการศึกษา ค้นคว้าเชิงเปรียบเทียบและรวบรวมข้อมูลที่เกี่ยวข้องกับการรักษาความปลอดภัยของกองทัพในยุคสังคมเศรษฐกิจดิจิทัล ได้แก่ ๑) รูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน และ ๒) รูปแบบการรักษาความปลอดภัยในต่างประเทศทั้งนี้เพื่อนำข้อมูลดังกล่าวมากำหนดเป็นรูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกที่มีประสิทธิภาพและสามารถนำไปใช้ได้จริง รวมถึงร่างแนวทางการรักษาความปลอดภัยของกองทัพบกไทยที่สามารถรองรับภัยคุกคามและความท้าทายในอนาคตพร้อมข้อเสนอแนะเชิงนโยบายโดยมีขั้นตอนการดำเนินการวิจัยตามลำดับดังต่อไปนี้

๑. ศึกษาเอกสาร รายงาน งานวิจัยที่เกี่ยวข้อง รายงานการวิจัย และบทความวิชาการต่างๆ (Documentation Method) รวมถึงบันทึกและรายงานของกองทัพที่เกี่ยวกับรูปแบบและระบบรักษาความปลอดภัย เพื่อสร้างกรอบแนวคิดการวิจัย (Conceptual Framework)

๒. ออกแบบเครื่องมือที่ใช้ในการวิจัยและทดสอบการใช้เครื่องมือเชิงคุณภาพเบื้องต้น โดยเครื่องมือที่ใช้ต้องผ่านการตรวจสอบความเที่ยงตรงจากผู้เชี่ยวชาญด้านการวิจัยเพื่อตรวจสอบความตรงเชิงเนื้อหา (Content Validity) ตลอดจนความเหมาะสมของภาษาและการใช้ถ้อยคำ (Wording)

๓. เก็บรวบรวมข้อมูลเชิงลึกตามกระบวนการวิจัยเชิงคุณภาพและใช้ตรวจสอบข้อมูลโดยใช้เทคนิควิธีการสามเส้า (Triangulation Technique) (Somarie Holtzhausen, 2001 และ Rothbauer Paulette, 2008) ของผู้ที่มีหน้าที่เกี่ยวข้องกับการรักษาความปลอดภัยในกองทัพทั้งในอดีตและปัจจุบันจากนั้นนำข้อมูลไปสังเคราะห์เพื่อนำไปใช้ในการร่างและตรวจสอบแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต โดยมีเอกสารหลักฐานเชิงประจักษ์และข้อเท็จจริง ประกอบด้วย

๓.๑ ข้อมูลปฐมภูมิ (Primary) ดำเนินการโดยการสัมภาษณ์แบบเชิงลึกผู้ที่มีหน้าที่เกี่ยวข้องกับการรักษาความปลอดภัยในกองทัพบก จำนวน ๓ คน และสัมภาษณ์แบบเชิงลึกผู้เชี่ยวชาญด้านนวัตกรรมการรักษาความปลอดภัย จำนวน ๒ คน

๓.๒ ข้อมูลทุติยภูมิ (Secondary) ได้จากเอกสารที่เกี่ยวข้อง อาทิ กฎหมาย ระเบียบ วารสาร บทความทางวิชาการ รายงานวิจัย และเอกสารสื่อสิ่งพิมพ์อิเล็กทรอนิกส์ทั้งในและต่างประเทศ รวมทั้งผลการสัมมนาและการทบทวนแนวทางด้านการรักษาความปลอดภัยของกองทัพบก รวมถึงฝ่ายพลเรือนในแต่ละกระทรวง

ทั้งนี้เพื่อนำข้อมูลดังกล่าวมาสังเคราะห์ร่วมกับการวิจัยเชิงประจักษ์จากสภาพและปัจจัยในการรักษาความปลอดภัยที่เหมาะสม และกำหนดเป็นแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยรวมถึงข้อเสนอแนะเชิงนโยบาย

๔. การวิเคราะห์และสังเคราะห์ข้อมูลตามหลักการวิจัยเชิงคุณภาพโดยวิธีพรรณนาเชิงวิเคราะห์ (Patton MQ, 2001)

๕. ร่างแนวทาง กำหนดแผนงานที่เกี่ยวข้อง และข้อเสนอแนะเชิงนโยบาย

๖. ตรวจสอบแนวทางโดยการสัมมนาอิงผู้เชี่ยวชาญ (Focus Group Discussion) โดยอาศัยความรู้ ความเชี่ยวชาญและประสบการณ์ของผู้วิจัย ร่วมกับความเห็นของผู้ทรงคุณวุฒิในด้าน

การรักษาความปลอดภัยที่มีประสิทธิภาพ เพื่อยืนยันแนวทาง (Confirmatory) แสดงความคิดเห็นและให้ข้อเสนอแนะ จากนั้นนำผลการตรวจสอบไปปรับปรุงแนวทางที่สมบูรณ์

๗. สรุปและเขียนรายงานการวิจัยฉบับสมบูรณ์

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบรูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน

๒. ทำให้ทราบรูปแบบการรักษาความปลอดภัยในต่างประเทศเพื่อนำมาเปรียบเทียบและปรับปรุงกระบวนการรักษาความปลอดภัยของกองทัพบกให้ได้มาตรฐานยิ่งขึ้น

๓. ทำให้ได้แนวทางที่มีมาตรฐานและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกที่มีประสิทธิภาพและสามารถนำไปใช้ได้จริง

๔. ได้ผลการวิจัยที่สามารถตีพิมพ์และเผยแพร่ผลงานการวิจัยทั้งในระดับชาติหรือนานาชาติ

คำจำกัดความ

รูปแบบการรักษาความปลอดภัยสถานที่	หมายถึง	รูปแบบหรือวิธีการรักษาความปลอดภัยของกองทัพบกไทยที่นำมาใช้เพื่อรักษาความปลอดภัย ให้กับบุคคลและกระบวนการทำงาน เพื่อให้องค์กรดำรงอยู่ได้อย่างมั่นคงตลอดจน การสร้างมาตรฐานด้านการรักษาความปลอดภัยในอนาคต
รูปแบบที่เหมาะสมของการรักษาความปลอดภัย	หมายถึง	รูปแบบการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกไทยที่มีประสิทธิภาพ สามารถนำไปใช้ได้จริงและสามารถรองรับภัยคุกคามและความท้าทายในอนาคต

บทที่ ๒
ทฤษฎีและแนวคิดการรักษาความปลอดภัยของกองทัพ

การวิจัยเรื่อง “แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต” มีทฎษฎี แนวคิด และงานวิจัยที่เกี่ยวข้องในประเด็นต่อไปนี้

๑. ความเป็นมาของการรักษาความปลอดภัยเกี่ยวกับสถานที่

๒. มาตรการการรักษาความปลอดภัยสถานที่

๓. แนวคิดเกี่ยวกับการรักษาความปลอดภัยแห่งชาติ

๔. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ

๕. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๖. ทฤษฎีภัยคุกคามและภัยคุกคามรูปแบบใหม่

๗. เทคโนโลยีการรักษาความปลอดภัย

๘. งานวิจัยและวรรณกรรมที่เกี่ยวข้อง

๙. กรอบความคิดของการวิจัย

๑๐.สรุป

ความเป็นมาของการรักษาความปลอดภัยเกี่ยวกับสถานที่

ความจริงการรักษาความปลอดภัยสถานที่มาจากสามัญสำนึกและสัญชาติญาณของมนุษย์ในการระวังภัยอันตราย นับแต่ยุคหินที่อาศัยอยู่ตามถ้ำ มนุษย์ยุคหินที่อยู่เป็นกลุ่มรวมกันภายในถ้ำเดียวกันจะร่วมมือกันปกป้องแหล่งที่อยู่อาศัย ไม่ให้มนุษย์ต่างกลุ่มหรือสัตว์ป่าเข้ามาหรือเข้าใกล้พื้นที่อาศัยของกลุ่มตน วิธีป้องกัน เช่น ก่อกองไฟไว้ที่ปากถ้ำ มียามเฝ้าทางเข้า และเมื่อรู้จักเลี้ยงสุนัขก็ใช้สุนัขช่วยเฝ้าระวัง เป็นต้น ต่อมาเมื่อเจริญขึ้น จึงรู้จักประดิษฐ์เครื่องทุ่นแรงสำหรับปกป้องพื้นที่อาศัย เช่น ทำรั้วแบ่งอาณาเขตไปพร้อมกับการป้องกันภัยจากการรุกล้ำ จากกองไฟบนพื้นดินกลายเป็นคบไฟ และเป็นแสงไฟจากโคมส่องสว่างหรือไฟฉาย การประดิษฐ์เครื่องมือประเภทต่างๆ มาช่วยหรือเสริมการเฝ้าระวัง สังเกตการณ์ และการป้องกันจึงมีพัฒนาการเรื่อยมาพร้อมกับมีประสิทธิภาพที่เพิ่มมากขึ้น จากที่เกริ่นนำมา การรักษาความปลอดภัยสถานที่ จึงหมายถึง มาตรการป้องกันหรือป้องปรามที่กำหนดไว้ โดยมุ่งให้มีประสิทธิภาพสูงสุดเท่าที่จะ

ดำเนินการได้และมีความพร้อมต่อการเผชิญกับเหตุร้ายที่อาจจะเกิดขึ้นได้ (องค์การรักษาความมั่นคงฝ่ายพลเรือน, ๒๕๖๐)

จุดมุ่งหมายของการรักษาความปลอดภัยเกี่ยวกับสถานที่

จุดมุ่งหมายในการใช้งานยังคงเดิม คือ การเฝ้าระวังและตรวจตรามิให้เกิดการบุกรุก กับแจ้งเตือน ป้องกัน และขัดขวางการลุกล้ำเข้ามาในพื้นที่ในครอบครอง อย่างไรก็ดี อาคาร สิ่งก่อสร้าง หรือสถานที่ตั้งในปัจจุบันมีทั้งขนาดที่ใหญ่และมีความสลับ ซับซ้อนของอาคารมากขึ้น จากสภาพนี้จึงต้องมีการวางแนวทางป้องกันมากยิ่งกว่าถ้ำในยุคหิน ดังนั้น ระบบการป้องกันจึงมีความซับซ้อนตามไปด้วย

ขอบเขตของมาตรการการรักษาความปลอดภัย

ขอบเขตของมาตรการการรักษาความปลอดภัย เพื่อให้เกิดประสิทธิภาพ ได้แก่

๑. ต้องมีการกำหนดพื้นที่ที่จะดำเนินการรักษาความปลอดภัย

๒. ต้องมีการกำหนดมาตรการการรักษาความปลอดภัยเช่น จัดทำรั้ว/กำแพงแบ่งพื้นที่ จัดทำแสงส่องสว่าง จัดทำเครื่องกีดขวาง กำหนดจุดที่อนุญาตให้ผ่านเข้า-ออก หรือระบบสัญญาณเตือนภัย

๓. ต้องมีระบบและช่องทางติดต่อสื่อสาร

๔. ต้องควบคุมบุคคล สิ่งของ และยานพาหนะที่ผ่านเข้า-ออก

๕. ต้องมีเจ้าหน้าที่รักษาความปลอดภัย หรือยามรักษาการณ์ เพื่อการตรวจตราและเฝ้าระวังเหตุผลที่ต้องกำหนดมาตรการการรักษาความปลอดภัยสถานที่

๖. วางแนวทางป้องกันมิให้เกิดภัยอันตรายที่จะเกิดหรืออาจจะเกิดขึ้นภายในพื้นที่ตั้ง หรือกำหนดแนวทางจัดการและปฏิบัติ เพื่อบรรเทาภัยอันตรายที่เกิดขึ้นแล้วและการสูญเสียให้เหลือน้อยที่สุด

๗. ลด แก้ไข และหาหนทางป้องกันข้อบกพร่อง สิ่งที่ล่อแหลม หรือจุดเสี่ยงที่อาจก่อให้เกิดอันตรายหรือความเสียหายต่ออาคาร สิ่งก่อสร้าง ทรัพย์สิน หรือชีวิตของบุคคลที่อยู่ในพื้นที่ตั้งนั้นต่อกรณีที่ภัยอันตรายเกิดขึ้นแล้ว จะเป็นแนวทางสำหรับสั่งการและการปฏิบัติ เพื่อลดความเสียหายที่จะเกิดขึ้นหรือที่เกิดขึ้นแล้วให้เหลือน้อยที่สุดหรือมิให้ลุกลามต่อไปได้

ประโยชน์ของการรักษาความปลอดภัยสถานที่

๑. เพื่อให้มีการเฝ้าระวัง ดูแล สังเกต และตรวจตรา ในบริเวณพื้นที่หรือที่ตั้งสำนักงานอยู่ตลอดเวลา (Detection)

๒. เพื่อให้พิสูจน์ทราบตัวบุคคล สิ่งของ และยานพาหนะที่ผ่านเข้า-ออกในบริเวณพื้นที่หรือที่ตั้งสำนักงาน (Identification)

๓. เพื่อป้องกันหรือขัดขวางการบุกรุก ลุกล้ำ หรือการลักลอบเข้ามาในบริเวณพื้นที่หรือที่ตั้งสำนักงาน (Interception)

มาตรการการรักษาความปลอดภัยสถานที่

การวางมาตรการและการกำหนดวิธีปฏิบัติ เพื่อรักษาความปลอดภัยสถานที่ควรเป็นไปเพื่อรองรับตามระดับความสำคัญ หน้าที่ความรับผิดชอบ และกำลังงบประมาณของหน่วยงานของรัฐ เนื่องจากส่วนงานต่าง ๆ ตามโครงสร้างที่ประกอบขึ้นเป็นหน่วยงานของรัฐแต่ละส่วนมีระดับความ สำคัญต่อหน่วยงานต่างกัน ตัวอย่างเช่น ส่วนงานเครื่องมืออุปกรณ์ของหน่วยงานหนึ่งมีความสำคัญมากกว่าส่วนงานระบบคอมพิวเตอร์ และในทางกลับกันสำหรับอีกหน่วยงาน ส่วนงานระบบคอมพิวเตอร์เป็นส่วนงานที่มีความสำคัญที่สุด เป็นต้น ฉะนั้น การวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยสถานที่ภายในหน่วยงานของรัฐ จึงต้องมีระดับความเข้มงวดต่างกัน เพื่อมิให้เกิดบรรยากาศที่กดดันแก่ผู้ปฏิบัติงานในหน่วยงานนั้น (องค์การรักษาความมั่นคงฝ่ายพลเรือน, ๒๕๖๐)

ข้อพิจารณาเบื้องต้นสำหรับการวางมาตรการเพื่อการรักษาความปลอดภัยมีดังนี้

๑. การแบ่งพื้นที่สำหรับการรักษาความปลอดภัย

วัตถุประสงค์

- เพื่อจัดระบบการรักษาความปลอดภัยในแต่ละส่วนงาน ให้มีมาตรการการรักษาความปลอดภัยที่แตกต่างกันออกไปตามความสำคัญของพื้นที่นั้น

- เพื่อทำการตรวจสอบบุคคล ยานพาหนะ หรือสิ่งของ ก่อนที่จะนำเข้าสู่พื้นที่ควบคุมชั้นอื่น

๑.๑ พื้นที่ควบคุม คือ พื้นที่ติดต่อที่อนุญาตให้บุคคลทั่วไปเข้าถึงได้ โดยแบ่งออกจากพื้นที่ปฏิบัติงานของเจ้าหน้าที่ หรือเป็นพื้นที่ที่อยู่ติดหรืออยู่ใกล้เคียง โดยรอบพื้นที่หวงห้าม

๑.๒ พื้นที่หวงห้าม เป็นพื้นที่ที่มีการกำหนดการรักษาความปลอดภัย เพื่อควบคุมดูแลรักษาสิ่งที่เป็นความลับ บุคคล ทรัพย์สินของทางราชการ หรือสิ่งที่อาจก่อให้เกิดภัยอันตรายหรือความเสียหายอย่างรุนแรงขึ้นได้ พื้นที่หวงห้ามต้องมีป้ายแสดงความเป็นพื้นที่ที่อยู่ในการควบคุมแยกออกจากพื้นที่ทั่วไปและป้ายนี้ต้องให้เห็นได้อย่างชัดเจน พื้นที่หวงห้ามแบ่งออกเป็น

- เขตหวงห้ามเฉพาะได้แก่ ที่เก็บเชื้อเพลิง ที่เก็บอาวุธ ห้องควบคุมการสื่อสาร ห้องทำงานของเจ้าหน้าที่ระดับผู้อำนวยการกองขึ้นไป และห้องควบคุมระบบไฟฟ้า

- เขตหวงห้ามเด็ดขาด ได้แก่ ห้องทดลอง ห้องปฏิบัติการทางเคมี-ชีวภาพ ห้องประชุมหรือสถานที่ที่จัดการประชุมลับ ห้องทำงานของผู้บังคับบัญชาระดับสูง ห้องนิรภัย ศูนย์ข้อมูลระบบคอมพิวเตอร์ และห้องจัดเก็บเครื่องประกอบพระราชพิธีของพระมหากษัตริย์

๒. เครื่องกีดขวางเพื่อการรักษาความปลอดภัยสถานที่

วัตถุประสงค์ การกำหนดเครื่องมือ อุปกรณ์ และระบบสำหรับการรักษาความปลอดภัยสถานที่

- เครื่องมือ อุปกรณ์ และระบบแต่ละประเภทจะช่วยเสริมประสิทธิภาพการทำงานให้เจ้าหน้าที่รักษาความปลอดภัยและยามรักษาการณ์ในด้านการตรวจตรา ตรวจสอบ ป้องกันและป้องปราม หรือยับยั้งการบุกรุกหรือหลบซ่อนของฝ่ายตรงข้ามหรือโจรขโมย

- สร้างเสริมความมั่นใจและลดภาระในการปฏิบัติงานให้แก่เจ้าหน้าที่รักษาความปลอดภัยและยามรักษาการณ์

- สร้างสภาวะกดดันทางจิตวิทยาต่อผู้บุกรุก ทำให้ต้องเพิ่มการไตร่ตรองก่อนที่จะทำการรุกล้ำเข้ามาในพื้นที่หรือที่ทำการ

- เพิ่มประสิทธิภาพในการควบคุมการผ่านเข้า-ออกพื้นที่และที่ทำการของหน่วยงานของรัฐ

๒.๑ เครื่องกีดขวางที่จัดทำขึ้นหรือนำสิ่งตามธรรมชาติมาปรับใช้เป็นเครื่องกีดขวาง

เครื่องกีดขวาง หมายถึง สิ่งใดๆ อุปกรณ์เครื่องมือที่สามารถนำมาใช้ป้องกันขัดขวาง หรือหน่วงเหนี่ยวบุคคลหรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่ควบคุมของหน่วยงานของรัฐ ซึ่งแบ่งออกเป็น เครื่องกีดขวางตามธรรมชาติ เช่น แม่น้ำ คูน้ำ ลำคลอง ภูเขา กับเครื่องกีดขวางที่ประดิษฐ์ขึ้นเพื่อใช้ป้องกันการล่วงล้ำ เช่น ความแข็งแรงของกำแพงหรือรั้ว หรือเครื่องกั้นประจำประตูหรือช่องทางเข้า-ออก

ก) กำแพงหรือรั้ว เพื่อกำหนดความชัดเจนของอาณาเขตและใช้แบ่งระดับความสำคัญของพื้นที่ควบคุม การสร้างกำแพงหรือรั้วต้องพิจารณาจากความสำคัญของหน่วยงาน อาณาเขต และงบประมาณที่ต้องใช้จ่าย กำแพงหรือรั้วของหน่วยงานของรัฐให้ก่อสร้างแบบนี้

- ต้องสูงอย่างน้อย ๑๘๐ เซนติเมตรขึ้นไป และมีความแข็งแรงทนทานต่อการงัดแงะเจาะทำลาย ขอบบนกำแพงหรือรั้ว ควรทำกระบังหรือเหล็กยื่นออกมา ทำมุม ๔๕ องศา ช่องห่างระหว่างกระบังหรือเหล็กประมาณ ๔๐- ๕๐ เซนติเมตร โดยให้ขึงลวดหนามตามยาวประมาณ ๔-๖ เส้นไปตลอด หรือจะทำเป็นเหล็กปลายแหลมโค้งงอ ๒ ด้าน เรียงบนขอบกำแพงหรือตลอดแนวกำแพงหรือรั้วให้ปลูกต้นไม้พุ่มที่มีกิ่งก้านหนาแน่นและมีหนามแหลม เช่น ไผ่ ต้น

กระบองเพชร และต้นกุหลาบพุกาม เป็นต้น ในกรณีที่เป็นหน่วยงานที่มีความสำคัญด้านนโยบาย ความมั่นคงหรือเป็นที่เก็บรักษาทรัพย์สินมีค่า ควรใช้กำแพงทึบ การใช้กำแพงประกอบรั้วเหล็กดัด ต้องเป็นเหล็กดัดที่มีความแข็งแรงมั่นคง การใช้กำแพงประกอบรั้วอัลลอยด์นั้น ความทนทานแข็งแรงจะน้อยกว่าเหล็กส่วนหน่วยงานที่มีความสำคัญระดับรองลงมาหรืออยู่ในส่วนภูมิภาคที่มิได้เป็นเป้าหมายการโจมตีใดๆ สามารถใช้รั้วโปร่ง รั้วเหล็กดัด รั้วขึงตาข่ายเหล็กหรือรั้วลวดหนาม ซึ่งประหยัดงบประมาณการก่อสร้างได้มากกว่ากำแพงหรือรั้วเหล็ก แต่ต้องคอยดูแลและซ่อมบำรุงรักษา

เหตุผลที่ดำเนินการ

- การสร้างกำแพงหรือรั้วทึบจะทำให้การยืนสังเกตการณ์จากภายนอกไม่สามารถทำได้ เพราะแนวความสูงอยู่เหนือเกินระดับสายตา หากเป็นกำแพงหรือรั้วโปร่ง ความสูงจะเป็นอุปสรรคในการปีนข้าม ต้องใช้บันไดหรือต้องกระโดดเกาะขอบบน ก่อนโหนตัวขึ้นไป การกระทำที่ผิดสังเกตเหล่านี้จะเป็นเหตุให้บุคคลทั่วไปหรือยามรักษาการณ์สังเกตเห็นได้ง่าย

- กำแพงหรือรั้วที่แข็งแรงจะช่วยป้องกันโจร ขโมย และปะทะการพยายามรุกล้ำเข้ามา โดยเฉพาะในกรณีที่เกิดการใช้กำลังประท้วงหรือการจลาจล

- การติดกระบังเหล็กขึงลวดหนาม หรือเหล็กแหลมที่ขอบบนกำแพงหรือการปลูกไม้หนามตลอดแนวกำแพงหรือรั้ว จะช่วยยับยั้ง หน่วงเหนี่ยว กีดขวางการบุกรุกหรือการปีนป่าย เพื่อเข้ามาในพื้นที่ที่ทำการได้ดี

- หากสามารถดำเนินการได้ ควรสร้างแนวกำแพงหรือรั้วให้ห่างจากตัวอาคารที่ทำการอย่างน้อย ๑๐ เมตรขึ้นไป

เหตุผลที่ดำเนินการ

- ระยะห่างระหว่างอาคารกับกำแพงหรือรั้วจะช่วยชะลอเวลาการบุกรุกเข้ามาในพื้นที่ได้ชั่วขณะ ซึ่งจะเป็นโอกาสให้สามารถดำเนินการป้องกันการบุกรุก และรายงานผู้บังคับบัญชา เพื่อขอรับคำสั่งดำเนินการ หรือแจ้งขอความช่วยเหลือจากเจ้าหน้าที่ตำรวจได้ทัน

- ระยะห่างจะช่วยลดอันตรายที่เกิดจากการใช้อาวุธ สิ่งของหรือด้วยเครื่องมือ อุปกรณ์ใดๆ โจมตีหรือขว้างปาจากภายนอกที่ทำการได้

- แม่น้ำ คู คลอง หรือภูเขานับเป็นสิ่งกีดขวางตามธรรมชาติที่ให้ประโยชน์สำหรับการรักษาความปลอดภัยสถานที่ โดยเฉพาะกรณีที่ที่ทำการติดแม่น้ำ คูคลองและใช้เป็นแนวกั้นพื้นที่ตามธรรมชาติ เพื่อลดค่าใช้จ่ายในการก่อสร้างกำแพงหรือรั้วลงได้บางส่วน หากสร้างรั้วเสริมขึ้นอีกชั้นจะเป็นแนวป้องกันชั้นที่ ๒ จะยิ่งทำให้การป้องกันมีประสิทธิภาพยิ่งขึ้น

เหตุผลที่ดำเนินการ

- ในกรณีที่แม่น้ำ คลองที่นำมาใช้เป็นแนวกั้นของที่ทำการ เป็นแม่น้ำคลองที่สามารถใช้เป็นเส้นทางสัญจรสาธารณะแล้ว แนวกั้นส่วนนี้ควรมีการดูแลเพิ่มขึ้น เพราะฝ่ายตรงข้ามสามารถใช้เป็นทั้งเส้นทางบุกรุกหรือเส้นทางหลบหนี หลังก่อเหตุร้ายได้

- การจัดและดูแลพื้นที่ติดหรือใกล้เคียงกำแพงหรือรั้ว

- ไม่ควรนำพัสดุครุภัณฑ์ชำรุด ถังขยะ บันได หรือสิ่งอื่นใด ไปพัก ทิ้งไว้ติดหรือใกล้กำแพงหรือรั้ว ไม่ว่าจะเป็นด้านนอกหรือภายในพื้นที่ก็ตาม

- กำแพงหรือรั้วที่อยู่ติดหรือใกล้กับอาคารหรือสิ่งก่อสร้างภายนอกบริเวณ ซึ่งมีระดับสูงกว่ากำแพงหรือรั้ว จะต้องมั่นตรวจตราดูแล เพื่อไม่ให้เกิดการกระทำที่เป็นการรุกล้ำเข้ามา ซึ่งอาจจะกลายเป็นการเอื้อประโยชน์ต่อการบุกรุกขึ้นได้ในภายหลัง

- ตัดแต่งกิ่งก้านต้นไม้ใหญ่ที่รุกล้ำหรือพาดกำแพงหรือรั้วให้เรียบร้อยอยู่เสมอ

เหตุผลที่ดำเนินการ

- เพื่อไม่ให้ฝ่ายตรงข้ามหรือโจร ขโมยสามารถใช้ประโยชน์ในการบุกรุกเข้ามาหรือเป็นที่กำบังหลบซ่อนภายในพื้นที่ที่ทำการได้

- เพื่อไม่ให้บดบังการตรวจตราด้วยสายตาของยามรักษาการณ์หรือเจ้าหน้าที่ทั่วไป

ข) เครื่องกั้นช่องทางผ่านเข้า-ออกหรือเครื่องกั้นถนนอัตโนมัติ ช่องทางเข้า-ออกทุกช่องทางของหน่วยงานของรัฐต้องมีอุปกรณ์กั้นช่องทาง เพื่อชะลอหรือหน่วงเหนี่ยวการเข้าสู่พื้นที่ของบุคคลหรือยานพาหนะชั้นแรก ได้แก่ ไม้กั้น ไม้กระดก รั้วเหล็กแบบเลื่อนด้วยคน และประตูเหล็กเลื่อนอัตโนมัติ (Sliding Gate) เหล็กแผ่นหรือเหล็กแหลมสำหรับขวางถนน (Road Block)

เหตุผลที่ดำเนินการ

- เพื่อให้เวลาแก่ยามรักษาการณ์ที่ช่องทางเข้า-ออกได้ตรวจสอบเบื้องต้น และสังเกตพฤติกรรมผู้ที่ต้องการผ่านเข้าพื้นที่ภายใน นอกจากนี้ ยังเป็นส่วนแรกที่ต้องปะทะในกรณีที่มีผู้พยายามบุกรุก

๓. ระบบแสงสว่าง

วัตถุประสงค์ การให้แสงสว่างเป็นระบบที่ทุกหน่วยงานของรัฐจำเป็นต้องจัดทำ ทั้งนี้ก็เพื่อวัตถุประสงค์ ได้แก่

- ให้มองเห็นบริเวณโดยรอบได้อย่างทั่วถึงและชัดเจน เพื่อไม่ให้เกิดจุดอ่อนในการรักษาความปลอดภัยสถานที่ในเวลากลางคืนและในพื้นที่มืดหรืออับแสง

- ให้ผลทางจิตวิทยาด้านบวกต่อเจ้าหน้าที่เวรประจำวันและยามรักษาการณ์ เพราะความสว่างช่วยสร้างความรู้สึกมั่นใจให้มีมากขึ้นในการปฏิบัติงานตอนกลางคืน และให้ผลทางจิตวิทยาด้านลบต่อผู้บุกรุกหรือโจรขโมย เพราะแสงสว่างเป็นอุปสรรคต่อการแอบซ่อน หลบหลีก หรือการเข้ามาเคลื่อนไหว เพราะไม่สามารถแสวงประโยชน์จากความมืดหรือจุดอับแสงได้

- ต้องพิจารณาจากระดับความสำคัญและงบประมาณค่าใช้จ่าย เพราะนอกจากค่าใช้จ่ายในการก่อสร้างแล้ว ยังมีค่าใช้จ่ายสำหรับการบำรุงรักษาและค่าไฟฟ้าเป็นภาระผูกพันอีกด้วย

๓.๑ พื้นที่ที่ต้องให้แสงสว่างอย่างทั่วถึง

- บริเวณกำแพงหรือรั้ว ตามแนวกำแพงหรือรั้วควรให้แสงสว่างทั้งด้านในและด้านนอก โดยเฉพาะที่เป็นกำแพงหรือรั้วทึบ

- บริเวณโดยรอบตัวอาคารที่ทำการและเขตหวงห้าม ได้แก่ บริเวณที่กำหนดไว้เป็นพิเศษ อาคาร ชั้น ห้อง สถานที่ที่เป็นที่เก็บทรัพย์สินมีค่า หรือทรัพย์สินที่มีความสำคัญ หรือข้อมูลที่มีความสำคัญ หรือเป็นความลับของทางราชการ

- ทางเข้า-ออก ได้แก่ ประตูทางเข้า-ออกทุกแห่งในพื้นที่ที่ตั้งอาคาร สิ่งก่อสร้างของหน่วยงานของรัฐ ประตูทางเข้า-ออกภายในอาคาร สิ่งก่อสร้าง โรงเก็บวัสดุอุปกรณ์ ปั๊มจ่ายน้ำมัน

๓.๒ การใช้แสงสว่าง ควรให้อยู่ในระดับที่สูงเพียงพอและควรเป็นแสงสีขาว เช่น แสงจากหลอดฟลูไลท์เซนต์ ซึ่งจะทำให้มองเห็นบริเวณโดยรอบได้ชัดเจน วิธีการใช้แสงสว่างแบ่งออกเป็น

- การใช้แสงส่องโดยตรงคือ การใช้แสงไฟส่องไปยังจุดที่ต้องการให้มีความสว่าง เช่น บริเวณประตูทางเข้า-ออกทุกประเภท เป็นต้น การใช้แสงวิธีนี้ไม่ควรใช้ดวงไฟที่ให้กำลังแสงจ้ามาก เช่น แสงไฟสปอตไลท์ เพราะแสงที่ให้ความสว่างมากเกินไปทำให้นัยตาพร่ามัวไม่มีความชัดเจน

- การใช้แสงส่องกระจายโดยรอบ โดยให้รัศมีของดวงไฟแต่ละดวงส่องทับเลยรัศมีของดวงไฟข้างเคียง เพื่อไม่ให้เกิดพื้นที่อับแสงในเวลากลางคืน เช่น ให้ติดดวงไฟตลอดแนวถนน

- ต้องจัดระบบไฟฟ้าสำรอง เพราะหากเกิดเหตุไฟฟ้าขัดข้อง จะสามารถใช้ระบบไฟฟ้าสำรองได้ทันที เพื่อให้พื้นที่ภายในหน่วยงานมีแสงสว่างตลอดเวลา

๔. ระบบควบคุมพื้นที่ภายในหน่วยงาน

วัตถุประสงค์

- เพื่อควบคุม ดูแลการเข้า-ออกพื้นที่ของเจ้าหน้าที่และผู้มาติดต่อ และตรวจตรายานพาหนะหรือการนำสิ่งของผ่านเข้า-ออกในบริเวณและในพื้นที่ควบคุมของหน่วยงานของรัฐ

- เพื่อหน่วงเหนี่ยว ปะทะ หรือป้องกันการลุกล้ำจากบุคคลภายนอกที่ไม่มีกิจเกี่ยวข้องกับหน่วยงานของรัฐ

๔.๑ ทางเข้า-ออกพื้นที่ทำการ

- ช่องทางผ่านเข้า-ออกของบุคคลและยานพาหนะทุกแห่งในที่ทำการของหน่วยงานของรัฐ ต้องมีป้ายแสดงทางเข้าและทางออกที่ชัดเจน และควรมีป้ายแสดงกำหนดเวลาการผ่านเข้า-ออกในวันราชการ วันหยุดราชการ รวมถึงข้อบังคับยกเว้นอื่นๆ ให้เห็นได้ชัดเจน

- ช่องทางผ่านเข้า-ออกต้องมีประตูเหล็กที่แข็งแรงมั่นคงเป็นแนวป้องกันชั้นแรก โดยจะเป็นประตูแบบทึบหรือโปร่งก็ได้ ซึ่งในช่วงนอกเวลาราชการและวันหยุดราชการควรปิดให้เหลือช่องทางผ่านเพียงช่องทางเดียว ยกเว้นหน่วยงานที่อนุญาตให้บุคคลภายนอกผ่านเข้า-ออกเพื่อประกอบกิจกรรมต่างๆ ทั้งในช่วงเวลาราชการ นอกเวลาราชการ หรือวันหยุดราชการ จึงให้เปิดประตูเช่นเดียวกับในวันราชการปกติ เช่น ช่องทางเข้า-ออกของกรมชลประทานที่อำเภอปากเกร็ดจังหวัดนนทบุรี ต้องเปิดเป็นปกติโดยตลอด เพราะมีโรงพยาบาลชลประทานตั้งอยู่ภายในพื้นที่จำเป็นต้องรับผู้มาติดต่อกับโรงพยาบาลตลอด ๒๔ ชั่วโมง เป็นต้น

- ต้องมีเครื่องกั้นการผ่านเข้า-ออกของยานพาหนะ เพื่อชะลอการผ่านเข้า-ออกอีกชั้น หากเป็นหน่วยงานที่สำคัญ ควรติดตั้งเครื่องกั้นการผ่านเข้า-ออกบุคคลไว้ด้วย จะช่วยเสริมการรักษาความปลอดภัยสถานที่ให้ดียิ่งขึ้น เครื่องกั้นเหล่านี้จะช่วยชะลอให้ยามรักษาการณ์ได้มีเวลาตรวจตราบุคคลและยานพาหนะที่จะผ่านเข้าพื้นที่ในชั้นต้น ตัวอย่างอุปกรณ์กั้นช่องทาง เช่น ไม้กั้น ไม้กระดก รั้วเหล็กแบบเลื่อน เหล็กแผ่นหรือเหล็กแหลม (งาแซง) การควบคุมอุปกรณ์กั้นช่องทางมีทั้งแบบเลื่อนด้วยมือและระบบอัตโนมัติ

- ช่องทางเข้า-ออกพื้นที่ทำการต้องจัดระบบแสงสว่างแบบส่องโดยตรงและต้องให้มีแสงสว่างตลอดเวลากลางคืนหรือในช่วงเวลาที่มืดมัว โดยเฉพาะหน่วยงานที่มีภารกิจด้านนโยบาย ความมั่นคง หรือดูแลทรัพย์สินมีค่าของชาติ ให้มีระบบไฟฟ้าสำรองหรือฉุกเฉินที่ช่องทางเข้า-ออก ซึ่งจะเป็นระบบไฟฟ้าสำรองแบบเคลื่อนที่ก็ได้ บริเวณโดยรอบและช่องทางเข้า-ออกต้องมีแสงสว่างทดแทนตลอดเวลา เพื่อให้ยามรักษาการสามารถตรวจสอบสิ่งผิดปกติที่อาจเกิดขึ้นชั่วขณะที่ขาดแสงไฟหรือในกรณีที่คนร้ายใช้เหตุไฟฟ้าดับอำพรางเข้ามาก่อเหตุร้ายได้

- ให้จัดที่จอดพักยานพาหนะสำหรับผู้มาติดต่อแยกออกจากที่จอดพักยานพาหนะของเจ้าหน้าที่ภายในหน่วยงาน โดยติดเครื่องหมายหรือป้ายแจ้งให้ทราบอย่างชัดเจน

- ในพื้นที่ที่จัดเพื่อการติดต่อนี้ควรมีป้ายแสดงให้ทราบข้อมูลที่จำเป็น เช่น เครื่องหมายจราจร จุดห้ามจอดพักยานพาหนะ เส้นทางติดต่อประชาสัมพันธ์ ข้อปฏิบัติเบื้องต้นในการมาติดต่อกับหน่วยงานของรัฐซึ่งข้อปฏิบัตินี้จะแตกต่างกันตามความจำเป็นและความเหมาะสมที่แต่ละหน่วยงานจะกำหนดขึ้น

๔.๒ ประตูทางเข้า-ออกอาคารที่ทำการหรือสิ่งก่อสร้างอื่นๆ

- ประตูเข้า-ออกภายในอาคารที่ทำการ และควรมีมากกว่า 1 แห่ง โดยประตูเข้า-ออกหลักควรอยู่ด้านหน้าอาคาร ในกรณีที่ยังมีการปฏิบัติงานนอกเวลาหรือในวันหยุดราชการควรกำหนดให้เปิดใช้ประตูเข้าออกเพียงทางเดียวเท่านั้น โดยจะเปิดใช้ประตูหลักหรือประตูแห่งอื่นก็ได้ ประตูเข้า-ออกอาคารทุกแห่งต้องมีความมั่นคงแข็งแรง มีระบบล็อกหรือติดกลอน-กุญแจที่แน่นหนา เพื่อใช้ปิดล็อก หลังยุติการปฏิบัติงานแล้ว นอกจากนี้ อาจติดตั้งประตูเหล็กม้วนติดกุญแจเพื่อใช้ปิดอีกชั้นหนึ่ง หลังปิดประตูปกติแล้ว

- ที่ประตูเข้า-ออกหลักของอาคารหรือสิ่งก่อสร้างของหน่วยงานควรติดป้ายแสดงกำหนดเวลาที่อนุญาตให้ผ่านเข้า-ออกให้ชัดเจน

- ประตูทางเข้า-ออกของอาคารหรือในชั้นอาคารของเอกชนที่เช่าพื้นที่เป็นที่ทำการ ต้องมีป้ายแสดงความเป็นหน่วยงานของรัฐที่ชัดเจนแยกออกจากพื้นที่อื่นที่เป็นส่วนของเอกชนและ มีลักษณะเหมือนเช่นที่กล่าวมาแล้ว และควรมีกลอนติดกุญแจหรือระบบปิดล็อกที่แน่นหนา เพื่อแยกพื้นที่ออกต่างหากจากพื้นที่ส่วนอื่นที่เป็นของเอกชน นอกจากนี้ ต้องมีแสงไฟส่องสว่างที่บริเวณประตูทางเข้า-ออกทุกแห่งในทันทีที่เกิดความมืดมัวหรือในเวลากลางคืน

- สิ่งก่อสร้างอื่นๆ เช่น โกดังเก็บพัสดุและโรงเก็บสารเคมี ควรมีประตูทางเข้า-ออกอย่างน้อย ๒ แห่ง แบ่งเป็นประตูเข้า-ออกปกติและประตูฉุกเฉิน ซึ่งในเวลาปกติ ให้ใช้ประตูเข้า-ออกปกติเพียงประตูเดียว และให้มีดวงไฟส่องสว่างที่บริเวณหน้าประตูเข้า-ออกทุกแห่งตลอดเวลากลางคืนหรือในช่วงที่อากาศมืดมัว ประตูทางเข้า-ออกทุกแห่งต้องมีการปิดล็อกที่แน่นหนาแข็งแรงตลอดระยะเวลาที่ยังไม่มีการเข้าไปทำงาน หรือในช่วงนอกเวลาราชการและวันหยุดราชการ นอกจากนี้ ควรแสดงความเป็นพื้นที่ควบคุม โดยการติดป้ายหรือเขียนที่ผนังด้านข้างประตูทางเข้า-ออกทุกแห่งให้เห็นอย่างชัดเจนก็ได้

- ประตูฉุกเฉิน ต้องอยู่ตามเส้นทางหลบภัยและอยู่ในตำแหน่งที่สามารถใช้เพื่อหลบภัยอันตรายได้จริง และให้ติดป้ายแสดงฐานะไว้ให้ชัดเจน ในเวลาปกติ ประตูฉุกเฉินควรปิดไม่ใช้งานและห้ามวางสิ่งของปิดขวางประตูฉุกเฉินเด็ดขาด

๕. พื้นที่สำหรับผู้มาติดต่อ

วัตถุประสงค์

- เป็นพื้นที่ที่ทุกหน่วยงานของรัฐต้องจัดไว้สำหรับควบคุม ดูแลบุคคลที่ไม่มีหน้าที่เกี่ยวข้องกับหน่วยงาน มาติดต่อ

๕.๑ ให้จัดห้องประชาสัมพันธ์และห้องพักรับรองสำหรับผู้มาติดต่อ ซึ่งควรเป็นส่วนเฉพาะแยกจากอาคารที่ทำการ หากไม่สามารถทำได้ ควรจัดพื้นที่ชั้นล่างของอาคารที่ตั้งอยู่ส่วนหน้าสุด ไม่ควรให้อยู่ลึกเข้ามาในพื้นที่หรือใกล้เขตที่กำหนดเป็นพื้นที่ควบคุม เพื่อให้สะดวกแก่การควบคุม

๕.๒ ในกรณีที่เป็นหน่วยงานของรัฐที่จัดข้อมูลข่าวสารของราชการให้ประชาชนสามารถเข้าไปตรวจสอบหรือร้องขอตามที่บัญญัติไว้ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐ นั้น ควรจัดห้องแยกออกจากประชาสัมพันธ์และห้องพักรับรอง แต่ให้อยู่ในพื้นที่ใกล้เคียงกันก็ได้ ทั้งนี้ให้ติดป้ายแสดงฐานะห้องข้อมูลข่าวสารให้ชัดเจน และควรจัดเจ้าหน้าที่ประจำอยู่ที่นี้อย่างน้อย ๑ นาย

๖. ระบบควบคุมแหล่งกำเนิดไฟฟ้า และระบบไฟฟ้าสำรอง-ไฟฉุกเฉิน

วัตถุประสงค์

- ป้องกันมิให้มีการทำลายระบบไฟฟ้าหรือทำให้ระบบขัดข้อง เพราะ

๑) ปัจจุบันไฟฟ้าถือเป็นส่วนประกอบสำคัญในการดำรงชีวิตมากที่สุดประการหนึ่ง ฉะนั้นแหล่ง กำเนิดไฟฟ้าของหน่วยงานถือได้ว่าเป็นเป้าหมายแรกที่ฝ่ายตรงข้ามมุ่งโจมตีโดยเฉพาะในการก่อวินาศกรรม หากสามารถทำลาย หรือทำให้ระบบไฟฟ้าขัดข้อง หรือหยุดชะงักลงชั่วระยะหนึ่งได้แล้ว จะเป็นผลให้การปฏิบัติงานของเจ้าหน้าที่รัฐด้วยอุปกรณ์เครื่องมือทางอิเล็กทรอนิกส์หรือระบบงานที่ใช้ไฟฟ้าต้องหยุดชะงัก

๒) หากระบบไฟฟ้าขัดข้องในช่วงเวลากลางคืน จะเป็นโอกาสให้ทำการบุกยึดหรือเข้าโจมตีหน่วยงานของรัฐในช่วงนั้นได้ง่ายยิ่งขึ้น

- ระบบไฟฟ้าสำรองหรือไฟฉุกเฉินจะช่วยให้มีแสงสว่างต่อเนื่องอีกระยะหนึ่งในช่วงที่ไฟขัดข้อง

๖.๑ ต้องให้ความสำคัญและดำเนินการควบคุม ดูแล และบำรุงรักษาไม่ให้เกิดเหตุขัดข้องขึ้นได้ ระบบควบคุมไฟฟ้าแต่ละอาคารควรกำหนดให้อยู่ภายในพื้นที่ควบคุม โดยเป็นส่วนเฉพาะที่บุคคลภายนอกไม่สามารถเข้าถึงได้โดยง่าย

๖.๒ ระบบไฟฟ้าสำรอง-ไฟฉุกเฉินต้องใช้งานทดแทนได้ทันทีที่แหล่งกำเนิดไฟฟ้าปกติขัดข้อง เช่น โคมไฟฉุกเฉินอัตโนมัติ ระบบไฟฟ้าสำรองมีทั้งแบบติดตั้งถาวรและแบบเคลื่อนที่ได้ การนำใช้ให้พิจารณาตามความเหมาะสมของภารกิจภายในหน่วยงาน

๖.๓ ควรติดตั้งระบบป้องกันภัยจากกระแสไฟฟ้าในทุกอาคาร เช่น ระบบป้องกันกระแสไฟฟ้ารัดวงจร เครื่องป้องกันไฟฟ้าดูด-ช็อต (Automatic Electric Protector)สวิทซ์ตัดตอนกระแสไฟฟ้าอัตโนมัติ (Fire Alarm System) เป็นต้น นอกจากนี้ หากในพื้นที่ที่ตั้งที่ทำการอยู่ในทำเลที่เคยเกิดเหตุฟ้าผ่าอาคารหรือสิ่งก่อสร้างที่มีความสูงหรือเป็นกลุ่มอาคารที่ตั้งกลางพื้นที่โล่งและกว้าง ควรติดตั้งเครื่องป้องกันฟ้าผ่า-ไฟกระโชก หรืออุปกรณ์ป้องกันฟ้าผ่า (Lightning and Serge Protection) แต่ต้องพิจารณาถึงความจำเป็นและความเหมาะสมของงบประมาณค่าใช้จ่ายด้วย เพราะเครื่องมืออุปกรณ์ดังกล่าวมีราคาสูง

๗. การควบคุมเส้นทางที่ไม่ใช้งาน

วัตถุประสงค์

- ป้องกันทั้งเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องและบุคคลอื่นลุกล้ำเข้าไปในพื้นที่ควบคุม ทั้งโดยตั้งใจหรือไม่ตั้งใจก็ตาม

๗.๑ เส้นทางคมนาคมในพื้นที่หน่วยงานทั้งที่อยู่ในหรือนอกพื้นที่ควบคุม หากไม่ต้องการให้ยานพาหนะผ่าน ต้องทำเครื่องกั้นถาวรขวางเส้นทาง เช่น ปักเสาเข็มหรือทำไม้กั้นถาวร

๗.๒ ช่องทางระหว่างอาคารหรือช่องทางระหว่างอาคารกับกำแพงหรือรั้ว ถ้าไม่ต้องการให้ใช้เป็นเส้นทางเดินผ่าน ให้ขึงตาข่ายเหล็กปิดไว้ โดยเฉพาะอาคารจอดรถ หากอยู่ติดกับกำแพงหรือรั้ว ความสูงของกำแพงหรือรั้วจะช่วยให้ปีนข้ามไปยังชั้นที่ ๒ ของอาคารจอดรถได้โดยง่าย ฉะนั้น ควรขึงตาข่ายเหล็กปิดช่องว่างระหว่างชั้นอาคารไว้ตลอดแนวด้วย

๗.๓ ดาดฟ้าหรือเฉลียงระหว่างอาคารที่ตั้งต่อเนื่องกันหรือใกล้เคียงกัน ควรทำรั้วโปร่งหรือกั้นตาข่าย เพื่อกันการปีนข้ามระหว่างตัวอาคาร

๘. ระบบป้องกันอัคคีภัย

วัตถุประสงค์

- ป้องกันมิให้เกิดอัคคีภัย หรือบรรเทาความเสียหายที่เกิดจากอัคคีภัยลงให้มากที่สุด เพราะสาเหตุที่เกิดอัคคีภัยส่วนใหญ่มาจากความประมาทเลินเล่อ ความบกพร่องและขาดการดูแล ซ่อมบำรุงของระบบไฟฟ้า เครื่องจักรกล หรือเกิดจากความร้อนสะสมในพื้นที่ที่มีวัสดุไวไฟ

๘.๑ ทุกหน่วยงานของรัฐต้องจัดอุปกรณ์ดับเพลิงเบื้องต้น เช่น กองทราย ถังน้ำ สายฉีดน้ำดับเพลิง และขวาน เป็นต้น ไว้ในจุดที่สามารถใช้งานได้ทันทีที่เกิดเพลิงไหม้

๘.๒ ทุกอาคารและสิ่งก่อสร้างให้ติดตั้งถังดับเพลิง ทั้งนี้ให้พิจารณาน้ำยาดับเพลิงที่เหมาะสมกับประเภทวัสดุที่อาจก่อให้เกิดเพลิงไหม้ โดยประเมินจากวัสดุสิ่งของที่มีอยู่ใน

อาคารและสิ่งก่อสร้างนั้น เช่น น้ำมันเชื้อเพลิง สารเคมี กระดาษเอกสาร และวัสดุไวไฟต่างๆ ประเภทของเพลิงไหม้ที่เกิดจากเชื้อเพลิงประเภทต่างๆ ดังนี้

ก) เพลิงประเภท ก (Class A) เกิดจากเชื้อเพลิงที่เป็นของแข็งทั่วไป ได้แก่ ไม้ กระดาษ ผ้า ยาง พลาสติก ให้ใช้เครื่องดับเพลิงชนิดน้ำธรรมดา (Water Gas) หรือชนิดฟองโฟมเคมี (Foam) หรือชนิดผงเคมีแห้ง (Dry Chemical) หรือชนิดเหลวระเหย (BCF Halon)

ข) เพลิงประเภท ข (Class B) เกิดจากของเหลวหรือก๊าซที่เป็นสารไวไฟ เช่น น้ำมันเชื้อเพลิงชนิดต่างๆ ทินเนอร์ ให้ใช้เครื่องดับเพลิงชนิดฟองโฟมเคมี หรือชนิดผงเคมีแห้ง หรือชนิดเหลวระเหย หรือชนิดก๊าซคาร์บอนไดออกไซด์

ค) เพลิงประเภท ค (Class C) เกิดจากการชำรุด บกพร่องของระบบหรืออุปกรณ์ไฟฟ้า ต้องใช้เครื่องดับเพลิงชนิดผงเคมีแห้ง หรือชนิดเหลวระเหย หรือชนิดก๊าซคาร์บอนไดออกไซด์

ง) เพลิงประเภท ง (Class D) เกิดจากโลหะติดไฟ สารเคมีที่ทำปฏิกิริยากับน้ำและลุกเป็นไฟได้ เช่น สารแมกนีเซียม สารโปรแตสเซียม การลุกไหม้จากเชื้อเพลิงประเภทนี้มีโอกาสเกิดขึ้นได้น้อยครั้ง เนื่องจากหน่วยงานที่ครอบครองสารเคมีเหล่านี้จะต้องควบคุมดูแลอย่างดี

๘.๓ ทำป้ายแสดงคุณสมบัติเครื่องดับเพลิงที่ใช้กับเชื้อเพลิงแต่ละประเภทให้ชัดเจน ป้ายนี้ให้ติดควบคู่กับถังดับเพลิง เพื่อให้เป็นที่ทราบโดยทั่วถึง เพราะหากใช้เครื่องดับเพลิงที่มีน้ำยาไม่เหมาะสมกับเชื้อเพลิงแล้ว อาจจะกลายเป็นการเสริมให้เพลิงไหม้ขยายวงกว้างยิ่งขึ้น

๘.๔ อาคารและสิ่งก่อสร้างที่มีความสูงเกินกว่า ๒ ชั้นขึ้นไปควรมีทางหนีไฟ พร้อมแผนผังเส้นทางหนีไฟ ป้ายแจ้งทางหนีไฟ (Exit Sign) และป้ายแสดงสัญลักษณ์เกี่ยวกับการป้องกันเพลิงไหม้ สำหรับทางหนีไฟต้องมั่นตรวจตราให้อยู่ในสภาพพร้อมใช้งาน ไม่มีสิ่งของ พัสดุครุภัณฑ์เหลือใช้ หรือวัสดุใดๆ วางขวางเส้นทางหนีไฟต้องแข็งแรงปลอดภัย หากพบส่วนที่ชำรุดต้องรีบซ่อมบำรุงให้สภาพสมบูรณ์ตามเดิม

๘.๕ เอกสารหรือวัสดุโดยทั่วไปหรือที่รอทำลาย ครุภัณฑ์ชำรุดหลายประเภทมีความเป็นเชื้อเพลิง ดังนั้น เมื่อยังไม่มีความจำเป็นต้องใช้หรือรอเวลาจำหน่าย ต้องจัดเก็บให้เรียบร้อยและอย่าให้อยู่ใกล้สิ่งที่ลุกไหม้ได้ เพราะในกรณีที่จะเกิดการลอบวางเพลิงหรือโดยประมาทเลินเล่อขึ้นแล้ว สิ่งเหล่านั้นจะกลายเป็นเชื้อเพลิงขยายความรุนแรงของอัคคีภัยได้ทันที เช่น เพลิงไหม้ที่มีเหตุมาจากการจุดธูป ยากันยุงไว้ใกล้กองกระดาษเอกสาร เป็นต้น

๘.๖ สำหรับหน่วยงานที่มีความสำคัญ ควรติดตั้งระบบเตือนภัยอัตโนมัติ เช่น ระบบป้องกันเพลิงอัตโนมัติ (Fire Alarm System) เครื่องตรวจจับควันไฟ (Smoke Detector) เครื่อง

ฉีดน้ำอัตโนมัติ (Sprinkle) เป็นต้น แต่ระบบเหล่านี้มีราคาสูง ต้องคอยตรวจตราและบำรุงรักษาให้มีความสมบูรณ์พร้อมใช้งานตลอดเวลา

๙. ระบบปรับอากาศภายในอาคารและเครื่องปรับอากาศ

วัตถุประสงค์ ป้องกันมิให้มีการใช้ระบบปรับอากาศสร้างความเสียหายภายในหน่วยงาน

๙.๑ ห้องควบคุมระบบปรับอากาศควรอยู่ในพื้นที่ควบคุมเช่นเดียวกับห้องควบคุมระบบไฟฟ้า ซึ่งบุคคลภายนอกไม่สามารถเข้าถึงได้ เนื่องจากห้องควบคุมนี้นับเป็นจุดอ่อนสำหรับการก่อวินาศกรรมหรือการก่อการร้ายทางชีวภาพ ได้แก่ การปล่อยก๊าซพิษให้ฟุ้งกระจายผ่านทางระบบถ่ายเทอากาศ การแพร่กระจายเ ชื้อโรค เช่น สปอร์เชื้อแอนแทรกซ์ เป็นต้น

๙.๒ ที่ตั้งส่วนประกอบของเครื่องปรับอากาศ เช่น คอมเพรสเซอร์ ควรติดตั้งในที่ปลอดภัยและควรกำหนดระยะเวลาการตรวจตรา ดูแล ยกเว้นในภาวะที่อาจเกิดการโจมตีจากฝ่ายตรงข้าม ควรดูแลให้เข้มงวดขึ้น เพราะการทำให้คอมเพรสเซอร์เสียหาย เพื่อใช้การซ่อมบำรุงเป็นข้ออ้างเข้ามา เพื่อกระทำการร้าย อย่างเช่น การลอบวางระเบิด เนื่องจากน้ำยาปรับความเย็นที่บรรจุอยู่ในเครื่องปรับอากาศ เมื่อผสมกับน้ำตาลทราย จะเกิดการระเบิดขึ้นได้

๙.๓ ในกรณีที่หน่วยงานของรัฐพิจารณาเห็นถึงความจำเป็นหรือมีโอกาสเสี่ยงที่อาจเกิดภัยอันตรายจากระบบปรับอากาศ ให้พิจารณาติดตั้งอุปกรณ์ปรับอากาศอื่นๆ ที่ช่วยเพิ่มประสิทธิภาพการรักษาความปลอดภัย แต่ทั้งนี้ต้องมีงบประมาณเพียงพอสำหรับดำเนินการ เช่น ติดตั้งระบบบำบัดอากาศเสียหรือฝุ่นควันในที่ทำการที่เป็นอาคารทึบหรืออยู่ในชั้นใต้ดิน เพราะในกรณีที่มีการปล่อยก๊าซหรือควันพิษขึ้น ระบบนี้จะช่วยดูดก๊าซหรือควันพิษออกไปจากพื้นที่ได้บางส่วน ซึ่งช่วยบรรเทาเหตุและลดความเสียหายที่จะเกิดลงได้บ้าง

๑๐. ที่ตั้งและลักษณะของอาคารและสิ่งก่อสร้าง

วัตถุประสงค์ เพื่อกำหนดมาตรการและวางระเบียบปฏิบัติให้เหมาะสมและเกิดประสิทธิภาพมากที่สุด

๑๐.๑ ที่ตั้งอยู่ใกล้สิ่งก่อสร้างที่อาจเป็นภัยอันตราย เช่น อยู่ใกล้สถานีจำหน่ายก๊าซหรือน้ำมันเชื้อเพลิง คลังเก็บสินค้า เคมีภัณฑ์ หรือโรงงานผลิตปุ๋ยวิทยาศาสตร์ ในทางกลับกันหากอาคารและสิ่งก่อสร้างที่จัดเก็บสารอันตรายของหน่วยงานตั้งอยู่ในทำเลที่ไม่เหมาะสม ก็อาจก่อให้เกิดภัยอันตรายได้เช่นกัน เช่น สถานีจ่ายน้ำมันของหน่วยงานตั้งใกล้กำแพง ถือเป็นจุดอ่อนของหน่วยงานนั้น เพราะง่ายต่อการโจมตีจากภายนอก

๑๐.๒ ความคงทน แข็งแรงของโครงสร้างอาคารหรือสิ่งก่อสร้าง เช่น สร้างจากคอนกรีตเสริมเหล็ก ก่ออิฐถือปูน กระเบื้องกระดาษ หรือวัสดุเทียมไม้ เป็นต้น ความแตกต่างของ

วัสดุก่อ สร้างเป็นส่วนสำคัญอีกส่วนหนึ่งที่ต้องคำนึงถึงในการวางมาตรการการรักษาความปลอดภัยสถานที่ เพราะหากโครงสร้างอาคารหรือสิ่งก่อสร้างไม่แข็งแรงเพียงพอ ก็จำเป็นต้องวางมาตรการเสริมเฉพาะส่วนที่เป็นจุดอ่อนของอาคารหรือสิ่งก่อสร้างนั้น เช่น หลังคาโกดังเก็บวัสดุครุภัณฑ์สร้างด้วยสังกะสี ควรขึงตาข่ายเหล็กปิดใต้โครงหลังคากันผู้บุกรุก เพราะสามารถตัดสังกะสีในส่วนของหลังคาเข้ามา เพื่อขโมยหรือทำลายสิ่งของภายในได้

๑๐.๓ ประตู หน้าต่าง และกลอนตามห้องต่างๆ ภายในอาคารหรือสิ่งก่อสร้างต้องแข็งแรง ทนทานต่อการงัดแงะทำลาย หากต้องการให้มีความปลอดภัยมากยิ่งขึ้นให้เพิ่มเหล็กดัดอีกชั้น ประตูห้องที่จัดเก็บสิ่งที่เป็นความลับต้องติดกุญแจปิดล็อกให้แน่นหนา ประตูห้องประชุมลับเป็นประตู ๒ ชั้น เพื่อป้องกันการแอบฟัง

๑๑. เครื่องมือ อุปกรณ์เสริมประสิทธิภาพการรักษาความปลอดภัยสถานที่

วัตถุประสงค์

- เสริมประสิทธิภาพการรักษาความปลอดภัยสถานที่

- ช่วยผ่อนภาระของเจ้าหน้าที่รักษาความปลอดภัยหรือยามรักษาการณ์ ในกรณีจำนวนเจ้าหน้าที่ไม่เพียงพอกับภารกิจ เครื่องมือ อุปกรณ์เหล่านี้สามารถแบ่งลักษณะการใช้งานสำหรับส่วนภายในอาคารและภายนอกอาคาร ได้แก่

๑๑.๑ ระบบกล้องโทรทัศน์วงจรปิด (Close Circuit Television System-CCTV) ใช้ในการตรวจตราความเคลื่อนไหวหรือเฝ้าสังเกตในพื้นที่ต่างๆ ทั้งภายในและภายนอกอาคาร เพื่อป้องกันการบุกรุก และช่วยลดภาระการเดินตรวจตราพื้นที่ของเจ้าหน้าที่รักษาความปลอดภัยและยามรักษาการณ์

๑๑.๒ ระบบควบคุมการเข้า-ออกอัตโนมัติ (Access Control System) โดยใช้บัตรแสดงตน (ID Card) สำหรับระบุฐานะของผู้ที่เข้ามาปฏิบัติหน้าที่ และควบคุมการผ่านเข้า-ออกในพื้นที่ควบคุม

๑๑.๓ ระบบสัญญาณป้องกันขโมย หรือสัญญาณเตือนภัยต่างๆ (Security Alarm System)

๑๑.๔ เครื่องตรวจสอบบุคคล พัสดุ สิ่งของที่นำเข้ามาในพื้นที่ เพื่อป้องกันการซ่อนพรางวัตถุระเบิดหรืออาวุธที่เข้ามาในพื้นที่ เช่น เครื่องเอ็กซ์-เรย์ประเภทต่างๆ เครื่องตรวจโลหะ (Metal Detector) สำหรับตรวจสัมภาระสิ่งของ

๑๑.๕ เครื่องตรวจสอบยานพาหนะ ใช้ตรวจหาวัตถุต้องสงสัยหรือป้องกันการซ่อนพรางวัตถุระเบิด เช่น ระบบตรวจใต้ท้องรถยนต์ (Under Venicle System) กระจกตรวจใต้ท้องรถยนต์ (Search Tool)

แนวคิดเกี่ยวกับการรักษาความปลอดภัยแห่งชาติ

การรักษาความปลอดภัยแห่งชาติ ตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ข้อ ๔ หมายความว่า มาตรการและการดำเนินการที่กำหนดเพื่อพิทักษ์รักษาและคุ้มครองป้องกันสิ่งที่เป็นความลับของทางราชการ ตลอดจนหน่วยงานของรัฐ เจ้าหน้าที่ของรัฐ และทรัพย์สินมีค่าของแผ่นดิน ให้พ้นจากการรั่วไหล การจารกรรม การก่อวินาศกรรม การบ่อนทำลาย การก่อการร้าย การกระทำที่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ และการกระทำอื่นใดที่เป็นการเปิดเผยสิ่งที่เป็นความลับของทางราชการ

เดชน์ จรูญเรืองฤทธิ์ (๒๕๔๙, หน้า ๗๐-๗๒) ได้อธิบายคำว่า “การรักษาความปลอดภัย” หรือ “ความปลอดภัย” หรือ “ความมั่นคง” ว่ามีการแปลมาจากคำภาษาอังกฤษคำเดียวกัน คือ“Security” และได้ถูกนำไปใช้ในหลายเรื่องหลายระดับ ทำให้มีความหมาย มีขอบเขตที่จะต้องมีการพิจารณา และ/หรือมีมาตรการที่จะนำไปใช้ในการปฏิบัติในรายละเอียดต่างๆ กันไปเฉพาะเรื่องเฉพาะระดับ โดยวัตถุประสงค์หลักของการรักษาความปลอดภัยมี ๒ ประการ คือ เพื่อลดโอกาสที่จะเกิดภัยหรือลดการเสี่ยงภัยในเหลือน้อยที่สุด และเพื่อบรรเทาความเสียหาย หากเกิดขึ้น (เดชน์ จรูญเรืองฤทธิ์ ๒๕๔๙, หน้า ๒๐๐)

มาตรการการรักษาความปลอดภัย ซึ่งถือเป็นเครื่องมือที่จะนำไปใช้ในการปฏิบัติเพื่อให้บรรลุวัตถุประสงค์หลักของการรักษาความปลอดภัย ประกอบด้วย ๓ ประเภท คือ

๑. การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal Security) คือ “มาตรการที่กำหนดขึ้นสำหรับใช้ปฏิบัติต่อข้าราชการ หรือผู้ที่ได้รับความไว้วางใจให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือให้ปฏิบัติหน้าที่ราชการที่สำคัญ เพื่อให้เป็นที่เชื่อแน่ว่าต้องเป็นผู้ที่ไม่เป็นภัยต่อความมั่นคงของประเทศชาติ” (เดชน์ จรูญเรืองฤทธิ์, ๒๕๔๙, หน้า ๒๑๖)

๒. การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ (Classified Information Security) คือ “มาตรการที่กำหนดขึ้นสำหรับปฏิบัติต่อเอกสารลับ เพื่อป้องกันไม่ให้ผู้ไม่มีอำนาจหน้าที่ได้ล่วงรู้ หรือเข้าถึงข้อมูลข่าวสารลับนั้น” (เดชน์ จรูญเรืองฤทธิ์, ๒๕๔๙, หน้า ๒๔๘)

๓. การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Physical Security) คือ “มาตรการที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยที่สงวน อาคาร และสถานที่ของส่วนราชการ ตลอดจนวัสดุอุปกรณ์ เจ้าหน้าที่ และเอกสารในอาคารสถานที่ดังกล่าวให้พ้นจากการโจรกรรม การจารกรรม การก่อนวินาศกรรม และก่อการร้าย หรือเหตุอื่นใด อันอาจจะทำให้เสียสมรรถภาพในการปฏิบัติภารกิจของส่วนราชาการได้” ซึ่งถ้ากล่าวโดยสรุป โดยไม่เน้นที่ส่วนราชการแต่เพียงอย่างเดียว การ

รักษาความปลอดภัยสถานที่ คือ การป้องการอาคาร สถานที่ ทรัพย์สิน ตลอดจนบุคคลในสถานที่ให้พ้นจากภัย (เดชน์ จรูญเรืองฤทธิ์, ๒๕๔๔, หน้า ๓๑๓)

ทั้งนี้ ในการกำหนดมาตรการการรักษาความปลอดภัย และการดำเนินการให้เกิดประสิทธิภาพ จะต้องคำนึงถึงหลักการรักษาความปลอดภัย ภัยคุกคาม ความเสี่ยงและโอกาสที่อาจจะเกิดขึ้นประกอบกัน เพื่อให้มาตรการครอบคลุมและสามารถป้องกันภัยคุกคามและรักษาไว้ซึ่งผลประโยชน์ของชาติ

หลักการรักษาความปลอดภัย คือ ข้อกำหนดที่จะนำไปใช้ในการพิจารณาวางมาตรการและพิจารณาดำเนินการ เพื่อพิทักษ์รักษาและคุ้มครองป้องกัน สิ่งที่เป็นความลับของทางราชการ เจ้าหน้าที่ของรัฐ หน่วยงานของรัฐ และทรัพย์สินอันมีค่าของแผ่นดิน ให้พ้นจากการรั่วไหล การจารกรรม การก่อวินาศกรรม การบ่อนทำลาย และการกระทำอื่นใดที่ส่งผลกระทบ หรือเสียหายต่อผลประโยชน์ของชาติ หรือเป็นภัยต่อความมั่นคงแห่งชาติ หลักการรักษาความปลอดภัย อาจจำแนกออกได้ดังนี้

๑. หลักผลประโยชน์สำคัญของชาติ (National Interests)
๒. หลักความมุ่งหมาย (Purpose)
๓. หลักความรับผิดชอบ (Responsibility)
๔. หลักการประสานงาน (Coordination)
๕. หลักการอ่อนตัว (Flexibility)
๖. หลักความจำเป็น (Necessity)
๗. หลักการลดอันตราย (Reduced Risk)
๘. หลักประสิทธิภาพ (Efficiency)
๙. กฎที่พึงระลึกในการรักษาความปลอดภัย (Security Consideration)

๑. หลักผลประโยชน์สำคัญของชาติ (National Interests)

ผลประโยชน์สำคัญของชาติตามความหมายโดยทั่วไป ก็คือ ความต้องการอันจำเป็นของชาติ เพื่อ “ความอยู่รอด” ตามระบอบการปกครองของประเทศนั้นๆ หรือที่นิยมเรียกกันในปัจจุบันว่า “ความมั่นคงแห่งชาติ” ซึ่งครอบคลุมถึงความมั่นคงแห่งสถาบันทางการเมือง เศรษฐกิจ สังคม และการทหารทั้งปวงของประเทศ ดังนั้นทุกชาติทุกประเทศจึงหวงแหนและยึดถือผลประโยชน์สำคัญของชาติตนเหนือสิ่งอื่นใด

การพิจารณาวางมาตรการและดำเนินการรักษาความปลอดภัย มีจุดประสงค์สำคัญเพื่อความมั่นคงแห่งชาติ แม้ว่าจะกระทบกระเทือนต่อสิทธิและผลประโยชน์ส่วนบุคคล หรือของบาง

กลุ่มบางเหล่า หรืออาจจะขัดผลประโยชน์ของชาติอื่นก็ตาม จะต้องยึดถือผลประโยชน์สำคัญของชาติเป็นหลัก

๒. หลักความมุ่งหมาย (Purpose)

จะต้องพิจารณาว่ามีความมุ่งหมายที่จะป้องกันเป้าหมายอะไร จากภัยอันใด ด้วยมาตรการอย่างไร แล้วควบคุมสอดส่องในขั้นต่อไปด้วยว่าการดำเนินมาตรการต่างๆ นั้น มีจุดอ่อนอย่างไรหรือไม่ หากมีจะต้องมีการปรับปรุงแก้ไขอย่างไร จึงจะบรรลุความมุ่งหมายนั้นให้จงได้

๒.๑ เป้าหมายของการรักษาความปลอดภัย ได้แก่

๒.๑.๑ สิ่งที่เป็นความลับของทางราชการ ซึ่งส่วนใหญ่เป็นเอกสาร

๒.๑.๒ อาคารและสถานที่ของทางราชการ

๒.๑.๓ บุคคลที่มีสิทธิเข้าถึงความลับหรือปฏิบัติหน้าที่บางอย่างของทางราชการ

๒.๒ ภัยคุกคาม

๒.๒.๑ ภัยคุกคาม กล่าวโดยทั่วไปในระดับชาติ ประกอบด้วยภัยคุกคามทางการเมือง เศรษฐกิจ สังคมจิตวิทยา และการทหาร ที่มีต่อความมั่นคงของชาติ

๒.๒.๒ ในส่วนที่เกี่ยวกับการรักษาความปลอดภัยโดยเฉพาะ แยกได้เป็นภัยอันกระทำในทางลบ ๓ ลักษณะ คือการจารกรรม ซึ่งกระทำต่อเป้าหมายสิ่งที่เป็นความลับ การก่อวินาศกรรม ซึ่งกระทำต่อเป้าหมายสถานที่ และการบ่อนทำลาย ซึ่งกระทำต่อเป้าหมายจิตใจของบุคคล

๒.๓ มาตรการรักษาความปลอดภัย แบ่งออกเป็น ๓ ประเภท เพื่อให้สอดคล้องกับเป้าหมาย คือ

๒.๓.๑ การรักษาความปลอดภัยเกี่ยวกับบุคคล กำหนดขึ้นเพื่อให้เป็นที่มั่นใจว่าผู้ที่จะมีสิทธิเข้าถึงความลับ หรือปฏิบัติหน้าที่ที่สำคัญบางอย่างของทางราชการได้นั้น ต้องเป็นผู้ที่ไม่เป็นภัยต่อความมั่นคงของชาติ

๒.๓.๒ การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ กำหนดขึ้นสำหรับปฏิบัติต่อข้อมูลข่าวสารลับ เพื่อป้องกันไม่ให้ผู้ไม่มีอำนาจหน้าที่ล่วงรู้หรือเข้าถึงข้อมูลข่าวสารนั้น

๒.๓.๓ การรักษาความปลอดภัยเกี่ยวกับสถานที่ กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่อาคารและสถานที่ตลอดจนวัสดุ อุปกรณ์ เจ้าหน้าที่ และข้อมูลข่าวสารในอาคารสถานที่ดังกล่าว

๒.๔ จุดอ่อนของมาตรการ

๒.๔.๑ มาตรการการรักษาความปลอดภัยต่าง ๆ ของระเบียบที่เกี่ยวกับการรักษาความปลอดภัย ได้กำหนดขึ้นโดยอาศัยประสบการณ์ของผู้มีหน้าที่รับผิดชอบเป็นแนวทาง ฝ่ายตรงข้ามย่อมจะคิดหาช่องทางและวิธีการใหม่ๆ เพื่อหลุดพ้นหรือหลบหลีกมาตรการการรักษาความปลอดภัยเหล่านี้

๒.๔.๒ การละเมินการรักษาความปลอดภัย อาจเกิดจากความประมาทเลินเล่อหรือความบกพร่องในการปฏิบัติหน้าที่เช่น ความไม่รอบคอบ และความไม่เอาใจใส่ เป็นต้น

๒.๕ การควบคุม

๒.๕.๑ กระทำด้วยการสอดส่องดูแลและตรวจสอบ มาตรการการรักษาความปลอดภัยที่นำมาใช้อยู่เสมอ

๒.๕.๒ วิเคราะห์หลักฐานในการปฏิบัติและข้อบกพร่องที่ได้มีมาแล้ว และวางแผนในการตรวจสอบและทดสอบ

๒.๕.๓ ดำเนินการตรวจสอบและทดสอบ มาตรการการรักษาความปลอดภัยตามแผน

๒.๕.๔ รายงานผลการตรวจสอบและทดสอบ โดยชี้ให้เห็นอุปสรรคและปัญหาข้อบกพร่องของมาตรการป้องกันที่ใช้อยู่ อันก่อนให้เกิดการละเมิดการรักษาความปลอดภัย และเสนอการปรับปรุงแก้ไขหรือวางมาตรการขึ้นใหม่

๒.๖ การปรับปรุง

๒.๖.๑ การปรับปรุงแก้ไขมาตรการให้มีประสิทธิภาพและทันสมัย เป็นสิ่งจำเป็นโดยอาศัยหลักการต่างๆ เข้าพิจารณาประกอบการปรับปรุงแก้ไขมาตรการ เพื่อให้บรรลุความมุ่งหมายให้จงได้

๒.๖.๒ เจ้าหน้าที่ที่มีจิตสำนึกในการรักษาความปลอดภัยอยู่ตลอดเวลา ย่อมนำหลักการมาประยุกต์ในทางปฏิบัติจนสามารถแก้ไขปัญหาไปได้เสมอ

๓. หลักความรับผิดชอบ (Responsibility)

เพื่อให้การรักษาความปลอดภัย บรรลุตามหลักผลประโยชน์สำคัญของชาติและหลักความมุ่งหมาย การพิจารณาวางมาตรการและดำเนินการในเรื่องการรักษาความปลอดภัยใดๆ ก็ตาม จำเป็นต้องมีการกำหนดความรับผิดชอบให้แน่นอนทุกระดับ ความรับผิดชอบในเรื่องการรักษาความปลอดภัย แบ่งออกเป็น ๓ ระดับ คือ

๓.๑ ระดับชาติ สำนักงานสภาความมั่นคงแห่งชาติ เป็นส่วนราชการที่รับผิดชอบในนโยบายเกี่ยวกับการรักษาความปลอดภัยในระดับชาติ โดยมีสำนักข่าวกรองแห่งชาติ สำนัก

นายกรัฐมนตรี เป็นองค์การรักษาความปลอดภัยฝ่ายพลเรือน ศูนย์รักษาความปลอดภัยกองทัพไทย เป็นองค์การรักษาความปลอดภัยฝ่ายทหาร และกองบัญชาการตำรวจสันติบาล สำนักงานตำรวจแห่งชาติ เป็นองค์การรักษาความปลอดภัยฝ่ายตำรวจ รับผิดชอบในการกำกับดูแลและให้การสนับสนุนหน่วยงานของรัฐ เพื่อให้ระบบการรักษาความปลอดภัยของชาติได้ผลสมบูรณ์อยู่เสมอ

๓.๒ ระดับส่วนราชการ หัวหน้าส่วนราชการมีอำนาจหน้าที่และความรับผิดชอบในเรื่องการรักษาความปลอดภัย ทั้งปวงของส่วนราชการของตน รวมทั้งแต่งตั้งเจ้าหน้าที่รักษาความปลอดภัย เช่น เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย และนายทะเบียนข้อมูลข่าวสารลับ เป็นต้น สำหรับหน่วยงานของรัฐในระดับต่ำกว่ากรมหรือเทียบเท่าลงมา อาจพิจารณาแต่งตั้งเจ้าหน้าที่รักษาความปลอดภัยต่าง ๆ ขึ้นได้ตามความจำเป็น

๓.๓ ระดับบุคคล เจ้าหน้าที่ของรัฐทุกคน ไม่ว่าจะเป็นเจ้าหน้าที่รักษาความปลอดภัยหรือไม่ก็ตามจะต้องรับผิดชอบในการรักษาความปลอดภัยต่อหน่วยงานของรัฐที่ตนสังกัดตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ และตามภารกิจหรือหน้าที่ที่ได้รับมอบหมาย โดยมีจิตสำนึกในการรักษาความปลอดภัยอยู่ตลอดเวลา

๔. หลักการประสานงาน (Coordination)

เพื่อให้งานด้านการรักษาความปลอดภัย ที่มีส่วนราชการหรือเจ้าหน้าที่หลายฝ่ายรับผิดชอบ หรือปฏิบัติร่วมกันหรือเกี่ยวข้องกัน สามารถดำเนินไปได้อย่างสอดคล้องกันทุกระดับและมีประสิทธิภาพ ส่วนราชการและ/หรือบุคคลที่เกี่ยวข้องจำเป็นต้องประสานการปฏิบัติ รวมทั้งประสานมาตรการที่ใช้อยู่ตลอดเวลา กล่าวคือ

๔.๑ มีการประสานงาน ระหว่างองค์การรักษาความปลอดภัยฝ่ายพลเรือน องค์การรักษาความปลอดภัยฝ่ายทหาร และองค์การรักษาความปลอดภัยฝ่ายตำรวจ

๔.๒ มีการประสานงาน ระหว่างองค์การรักษาความปลอดภัยกับส่วนราชการต่างๆ

๔.๓ มีการประสานงาน ในด้านการรักษาความปลอดภัยระหว่างส่วนราชการต่างๆ ในเรื่องที่เกี่ยวข้องซึ่งกันและกัน หรือในภารกิจที่ต้องรับผิดชอบร่วมกัน

๔.๔ มีการประสานงาน ระหว่างเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยกับเจ้าหน้าที่อื่นๆ ในส่วนราชการเดียวกัน

๔.๕ มีการประสานมาตรการ โดยคำนึงถึงภัยคุกคามหลายด้านประกอบกัน เช่น ในการรักษาความปลอดภัยเกี่ยวกับสถานที่ จะต้องคำนึงถึงภัยคุกคามหลายอย่าง ทั้งภัยคุกคามตามธรรมชาติ และภัยคุกคามที่เกิดจากการกระทำของมนุษย์ทั้งทางลับและเปิดเผย

๔.๖ มีการประสานมาตรการในทางป้องกัน และในทางปราบปรามประกอบกัน

๔.๗ มีการประสานมาตรการและช่องทางติดต่อสื่อสาร ในการกำหนดแผนปฏิบัติ

๕. หลักการอ่อนตัว (Flexibility)

การใช้มาตรการการรักษาความปลอดภัย ย่อมมีปัจจัยหลายอย่างเข้ามาเกี่ยวข้อง เช่น กำลังคนที่จะปฏิบัติงาน เครื่องมือเครื่องใช้ สิ่งอำนวยความสะดวก สภาวะแวดล้อม ฯลฯ ซึ่งปัจจัยเหล่านี้ แต่ละส่วนราชการมีความพร้อมไม่เท่าเทียมกัน ทำให้ไม่สามารถปฏิบัติตามระเบียบได้โดยครบถ้วน อย่างไรก็ดี เมื่อเกิดปัญหาอุปสรรคและข้อบกพร่องในการปฏิบัติ ตามระเบียบการรักษาความปลอดภัย จะต้องศึกษาและทำความเข้าใจหลักการต่าง ๆ อย่างถี่ถ้วน และปฏิบัติงานโดยยึดถือหลักการดังกล่าว รวมทั้งรู้จักประยุกต์วิธีปฏิบัติในรายละเอียด ให้เหมาะสมกับสภาวะแวดล้อม ตลอดจนสถานการณ์ที่เผชิญหน้าอยู่ ย่อมจะสามารถแก้ปัญหาอุปสรรคและข้อบกพร่อง ทำให้การรักษาความปลอดภัยได้ผลสมบูรณ์ ตามความมุ่งหมายของหน่วยงานของรัฐนั้นๆ ได้

๕.๑ มาตรการการรักษาความปลอดภัย ที่นำมาใช้ จะต้องพิจารณาถึงความสมดุลระหว่างมาตรการในการรักษาความปลอดภัย กับประสิทธิภาพในการปฏิบัติงานของแต่ละหน่วยงานด้วย เพราะการวางมาตรการเข้มงวดเกินสมควร ย่อมกลายเป็นอุปสรรคขัดขวางการปฏิบัติภารกิจของหน่วยงานของรัฐนั้นได้ แต่ก็มิได้หมายความว่าจะยอมปล่อยให้มาตรการ การรักษาความปลอดภัยหละหลวมหรือละเลยต่อการปฏิบัติ อันจะเป็นช่องทางให้เกิดจุดอ่อนในการรักษาความปลอดภัยขึ้นได้

๕.๒ การใช้มาตรการ ควรให้สอดคล้องกับลำดับความสำคัญของแต่ละหน่วยงานของรัฐ และความสำคัญของแต่ละเป้าหมายในหน่วยงาน

๕.๓ การวางมาตรการการรักษาความปลอดภัย ควรดัดแปลงให้เหมาะสมกับสถานการณ์และสภาวะแวดล้อมที่เปลี่ยนแปลงไป แต่จะต้องให้เป็นตามระเบียบแบบแผนและหลักวิชา มิใช่ปรับเปลี่ยนโดยพลการ และต้องเป็นการปรับเปลี่ยนในรายละเอียด มิใช่เปลี่ยนในหลักการ

๖. หลักความจำเป็น (Necessity)

๖.๑ คือการจำกัดให้ทราบเท่าที่จำเป็น ซึ่งหมายถึงการให้สิทธิเข้าถึงสิ่งที่เป็นความลับของทางราชการแก่บุคคลผู้ที่จำเป็นต้องทราบ เพื่อให้สามารถปฏิบัติภารกิจให้ลุล่วงไปได้

๖.๒ ผู้ไม่มีหน้าที่หรือมิได้รับคำสั่งหรือมิได้รับการมอบหมายที่ถูกต้อง จะอ้างฐานะตำแหน่งหรืออิทธิพลใดๆ เพื่อเข้าถึงความลับของทางราชการมิได้เป็นอันขาด

๗. หลักการลดอันตราย (Reduced Risk)

๗.๑ หมายถึงการโยกย้ายข้าราชการหรือบุคคล ที่มีพฤติการณ์อันเป็นภัยหรือไม่น่าไว้วางใจ ออกไปจากตำแหน่งหน้าที่ที่สำคัญโดยเร็ว เพราะถ้าให้คงอยู่ในหน้าที่ต่อไป อาจก่อให้เกิดความเสียหายหรือเสี่ยงต่อการรักษาความปลอดภัย

๗.๒ การกำจัดข้อบกพร่องหรือสิ่งที่ล่อแหลม หรืออาจก่อให้เกิดอันตราย หรือความเสียหายแก่มาตรการการรักษาความปลอดภัยให้หมดสิ้นไป

๘. หลักประสิทธิภาพ (Efficiency)

๘.๑ หมายถึงความพยายามที่จะดำรงไว้ ซึ่งประสิทธิภาพของมาตรการการรักษาความปลอดภัยทั้งปวง ให้อยู่ในลักษณะถาวรและสม่ำเสมอด้วยการอบรม ตลอดจนการปลูกฝังหรือกระตุ้นจิตสำนึกในการรักษาความปลอดภัยอยู่ตลอดเวลา หากสามารถปลูกฝังบุคคลทุกคนในส่วนราชการให้มีจิตสำนึกในเรื่องการรักษาความปลอดภัยได้ ย่อมเป็นความสำเร็จอย่างสูง

๘.๒ จะต้องอบรมชี้แจงเกี่ยวกับระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ แก่บุคคลทุกคนที่มีหน้าที่ได้ทราบ หรือได้ดำเนินการหรือได้เก็บรักษาสิ่งที่เป็นความลับของทางราชการให้เข้าใจและปฏิบัติตามระเบียบโดยเคร่งครัด โดยชี้แจงให้เห็นถึงความจำเป็นของการรักษาความปลอดภัย และจะต้องจัดให้มีการอบรมเพิ่มเติมตามเหมาะสม

๙. กฎที่พึงระลึกในการรักษาความปลอดภัย (Security Consideration)

๙.๑ ไม่มีมาตรการการรักษาความปลอดภัยใดๆ ที่จะมีประสิทธิภาพอันถาวรและประกันภัยผลได้โดยครบถ้วนจากความพยายามของฝ่ายตรงข้าม เพราะการรักษาความปลอดภัยเป็นมาตรการเชิงรับ แต่ความพยายามของฝ่ายตรงข้ามเป็นมาตรการเชิงรุก

๙.๒ การกำหนดมาตรการป้องกันแต่เพียงประการเดียว ไม่อาจเพียงพอที่จะประกันได้ว่า สิ่งที่เป็นความลับของทางราชการจะมีความปลอดภัยโดยสิ้นเชิง หากการวางมาตรการพิทักษ์รักษามิได้กระทำควบคู่กับมาตรการอื่นๆ ด้วย

๙.๓ ความเข้มแข็งของมาตรการการรักษาความปลอดภัยใดๆ พิจารณาได้จากจุดอ่อนที่สุดของมาตรการนั้นเอง การรักษาความปลอดภัยที่ดีจะต้องมีจุดอ่อนน้อยที่สุด

๙.๔ มาตรการการรักษาความปลอดภัยทั้งปวง จะต้องได้รับการสอดส่องดูแลและตรวจสอบอยู่เสมอ การสอดส่องเป็นประจำจะทำให้สามารถตรวจพบว่า จุดอ่อนอยู่ที่ใด และควรแก้ไขอย่างไร

๙.๕ มาตรการการรักษาความปลอดภัย จะต้องสอดคล้องกับความต้องการทางธุรการ และการดำเนินภารกิจประจำของส่วนราชการอื่นและไม่เป็นอุปสรรคต่อการบริหารงาน

๙.๖ การรักษาความปลอดภัยจะมีประสิทธิผลเพิ่มขึ้นก็ต่อเมื่อมีการประสานงานและประสานการปฏิบัติ การซักซ้อมกันระหว่างบรรดามาตรการทั้งหลายตั้งแต่ระยะวางแผน

๙.๗ สิ่งที่เป็นความลับของราชการที่มีผู้เข้าถึงมากเพียงใด ย่อมเสี่ยงต่อการรั่วไหลมากขึ้นเพียงนั้น

๔.๘ เจ้าหน้าที่รักษาความปลอดภัยจะต้องมีจิตสำนึกในการระแวงภัยตลอดเวลา

๔.๙ การจำกัดให้ทราบเท่าที่จำเป็น เป็นหัวใจของการรักษาความปลอดภัย

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒

ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ลงประกาศในราชกิจจานุเบกษาเมื่อวันที่ ๑๓ มีนาคม ๒๕๕๒ และมีผลบังคับใช้แทนระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ ตั้งแต่วันที่ ๑๑ มิถุนายน ๒๕๕๒ เนื่องจากระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ บังคับใช้มาเป็นเวลานาน บทบัญญัติบางเรื่องอาจไม่สอดคล้องกับสถานการณ์ปัจจุบัน ประกอบกับการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับเพื่อป้องกันข้อมูลข่าวสารลับของทางราชการมิให้รั่วไหล ได้กำหนดให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ กำหนดขึ้นเพื่อเป็นแนวทางการปฏิบัติ เกี่ยวกับการรักษาความปลอดภัยแก่หน่วยงานของรัฐ ให้เป็นไปในแนวทางเดียวกัน โดยมีจุดมุ่งหมายเพื่อ

๑. ให้มีความรู้ความเข้าใจในเรื่องการรักษาความปลอดภัย และเห็นถึงความจำเป็นที่ต้องกำหนดมาตรการการรักษาความปลอดภัย

๒. ดำเนินการและถือปฏิบัติตามระเบียบเกี่ยวกับการรักษาความปลอดภัยที่กำหนดไว้ ทั้งนี้รวมถึงการปรับแนวทางปฏิบัติให้เหมาะสมกับสำคัญ หน้าที่ความรับผิดชอบ สถานการณ์ สภาวะแวดล้อม และงบประมาณของหน่วยงานของรัฐนั้นๆ

๓. ควบคุม กำกับ และดูแลมาตรการการรักษาความปลอดภัย ตลอดจนทบทวนปรับปรุงให้เหมาะสมกับสถานการณ์อย่างมีประสิทธิภาพอยู่เสมอ เพื่อหยุดยั้งภัยอันตราย หรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อชีวิตและทรัพย์สินภายในหน่วยงานของรัฐได้

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ กำหนดให้มีการดำเนินการการรักษาความปลอดภัยเกี่ยวกับบุคคล การรักษาความปลอดภัยเกี่ยวกับสถานที่ การรักษาความปลอดภัยในการประชุมลับ และการดำเนินการเมื่อเกิดเหตุละเมิดการรักษาความปลอดภัย โดยที่ระเบียบได้กำหนดให้มีคณะกรรมการนโยบายรักษาความปลอดภัยแห่งชาติ จำนวน ๒๔ คน มีรัฐมนตรีที่นายกรัฐมนตรีมอบหมาย เป็นประธานกรรมการ และเลขาธิการสภาความมั่นคงแห่งชาติ เป็นกรรมการและเลขานุการ โดยมีผู้อำนวยการสำนักข่าวกรองแห่งชาติ

ผู้บัญชาการศูนย์รักษาความปลอดภัย และผู้บัญชาการตำรวจสันติบาล เป็นกรรมการและผู้ช่วยเลขานุการ (ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ ฉบับที่ ๒ พ.ศ.๒๕๕๔, หน้า ๑-๒)

การรักษาความปลอดภัยเกี่ยวกับบุคคล

การรักษาความปลอดภัยเกี่ยวกับบุคคล เป็นมาตรการที่กำหนดขึ้นสำหรับใช้ปฏิบัติต่อผู้ที่อยู่ระหว่างรอบรรจุ หรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ หรือผู้ที่จะได้รับความไว้วางใจเข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือให้ปฏิบัติหน้าที่ราชการที่สำคัญ เพื่อเลือกเฟ้นและตรวจสอบให้ได้ผู้ที่มีคุณสมบัติเหมาะสม ให้เป็นที่เชื่อแน่ว่าต้องเป็นผู้ที่ไม่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติหรือมอบหมายให้มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล ดังนี้

๑. ดำเนินการตรวจสอบประวัติและพฤติกรรมบุคคล

๑.๑ ผู้ที่อยู่ระหว่างรอบรรจุหรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ

๑.๒ ผู้ที่เป็นลูกจ้างทดลองปฏิบัติงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน

๑.๓ เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ และผู้ที่ขอกลับเขารับราชการใหม่

๑.๔ เจ้าหน้าที่ของรัฐ หรือบุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งสำคัญของหน่วยงาน หรือเกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการ ทรัพย์สินมีค่าของแผ่นดิน

๑.๕ ผู้ได้รับทุนการศึกษาทั้งในประเทศหรือต่างประเทศแล้ว มีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐเมื่อสำเร็จการศึกษา

๑.๖ บุคคลภายนอกที่เข้ามาปฏิบัติงานให้หน่วยงานของรัฐ

๑.๗ กรณีตรวจพลบุคคล ที่มีพฤติการณ์หรือปรากฏข่าวสารที่น่าจะเป็นภัย ต่อความมั่นคงและผลประโยชน์แห่งรัฐ หรือบุคคลที่เกี่ยวข้องกับชั้นความลับของทางราชการ หัวหน้าหน่วยงานของรัฐอาจขอให้องค์การรักษาความปลอดภัยตรวจสอบเพิ่มเติมได้

๒. หน่วยงานของรัฐ ต้องจัดให้มีการรับรองความไว้วางในบุคคล ที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการ โดยมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร และต้องผ่านการตรวจสอบประวัติและพฤติการณ์

๓. เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหน่วยงานของรัฐ ต้องบันทึกชื่อบุคคลที่ได้รับการรับรองความไว้วางใจไว้ในทะเบียนความไว้วางใจของหน่วยงาน

๔. หัวหน้าหน่วยงานของรัฐ ต้องจัดให้มีการอบรมชี้แจงเกี่ยวกับระเบียบการรักษาความปลอดภัยแก่บุคคลที่ได้รับการบรรจุใหม่ ผู้ที่ไม่เคยได้รับการอบรมหรือผู้ที่จะได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับความลับของทางราชการ รวมถึงการให้ความรู้ในวิทยาการด้านต่างๆ และต้องอบรมทบทวนตามระยะเวลาที่เหมาะสม เพื่อกระตุ้นจิตสำนึกในและวินัยในด้านการรักษาความปลอดภัย

บุคคลเป็นปัจจัยที่สำคัญที่สุด ในการปฏิบัติตามมาตรการรักษาความปลอดภัย ทุกด้านให้สำเร็จและมีประสิทธิภาพ อย่างไรก็ดี บุคคลอาจเป็นต้นเหตุที่ก่อให้เกิดความเสียหาย ต่อระบบการรักษาความปลอดภัยได้เช่นกัน ดังนั้นการรักษาความปลอดภัยเกี่ยวกับบุคคลจึงกำหนดขึ้น เพื่อคัดกรอง ตรวจสอบบุคคลที่จะเข้าปฏิบัติงานให้กับหน่วยงานของรัฐ เพื่อให้ได้ผู้ที่มีคุณสมบัติเหมาะสม และมีความประพฤติที่ไม่เสียหาย หรือเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

๑. การตรวจสอบประวัติและพฤติการณ์บุคคล บุคคลที่ต้องได้รับการตรวจสอบประวัติและพฤติการณ์ คือ ผู้ได้รับการบรรจุเป็นเจ้าหน้าที่ใหม่ของรัฐ เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ ผู้ที่ขอกลับเข้ารับราชการใหม่ ผู้ที่ได้รับทุนการศึกษาของหน่วยงานของรัฐ ที่มีข้อผูกพันว่าจะได้รับการบรรจุเข้าทำงานในหน่วยงานของรัฐนั้น ๆ บุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน่วยงานของรัฐ เช่น พนักงานที่จัดจ้างจากบริษัทภายนอก บุคคลที่ได้รับการแต่งตั้งให้ดำรงตำแหน่งสำคัญ ตามความเหมาะสมของภารกิจในหน่วยงานของรัฐ บุคคลที่มีพฤติการณ์หรือปรากฏข่าวสาร หรือติดต่อกับบุคคลหรือองค์กรที่อาจเป็นภัยต่อความมั่นคงของประเทศ เจ้าหน้าที่ของรัฐที่เข้าถึงเรื่องลับที่สุด ลับมาก หรือการรหัส โดยหน่วยงานของรัฐนั้นๆ ดำเนินการตรวจสอบเองได้ โดยขอคำแนะนำจากองค์การรักษาความปลอดภัย เพื่อให้ได้บุคคลที่มีคุณสมบัติครบถ้วน ตรงตามวัตถุประสงค์ของหน่วยงาน และตามกฎหมายหรือระเบียบข้อบังคับ สำหรับแนวทางการตรวจสอบประวัติและพฤติการณ์บุคคล มีดังนี้

๑.๑ การตรวจสอบเบื้องต้น

๑.๑.๑ การตรวจสอบบุคคลที่อยู่ระหว่างรอบรรจุหรือแต่งตั้ง เป็นเจ้าหน้าที่ของรัฐผู้ที่เป็นลูกจ้างทดลองปฏิบัติงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ ผู้ที่พ้นจากภารกิจ หรือตำแหน่งหน้าที่แล้ว แต่ต้องกลับเข้าทำงานที่เกี่ยวข้องกับชั้นความลับของทางราชการ ผู้ที่ขอกลับเข้ารับราชการใหม่เจ้าหน้าที่ของรัฐหรือบุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งสำคัญของหน่วยงาน หรือเกี่ยวข้องกับส่สิงที่เป็นความลับของทางราชการ หรือทรัพย์สินมีค่าของแผ่นดิน ผู้ได้รับทุนการศึกษาทั้งในประเทศหรือต่างประเทศ แล้วมีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐ เมื่อสำเร็จการศึกษาและบุคคลภายนอกที่เข้ามาปฏิบัติงานให้หน่วยงานของรัฐ

๑.๑.๒ วิธีการตรวจสอบเบื้องต้น ให้มีการปฏิบัติดังนี้

๑.๑.๒.๑ จัดพิมพ์ชื่อรายชื่อบุคคลที่จะต้องตรวจสอบ หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด ที่อยู่ ชื่อ-สกุลของบิดา/มารดา ส่งกองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ เพื่อตรวจสอบข้อมูลด้านอาชญากรรม

๑.๑.๒.๒ ให้บุคคลที่จะต้องตรวจสอบ ไปพิมพ์ลายนิ้วมือที่สถานีตำรวจ ท้องที่ที่บุคคลผู้นั้นมีภูมิลำเนาอยู่ การจัดพิมพ์ลายนิ้วมือนั้น เพื่อส่งให้สำนักงานตำรวจแห่งชาติ ดำเนินการตรวจสอบประวัติอาชญากรรม และพฤติการณ์อื่นที่สถานีตำรวจท้องที่นั้นๆ บันทึกเก็บไว้

๑.๑.๒.๓ หน่วยงานของรัฐให้ผู้ถูกตรวจสอบกรอกแบบประวัติบุคคล ให้ครบถ้วน และอยู่ภายใต้การดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ประจำหน่วยงานของรัฐหรือเจ้าหน้าที่ผู้รับผิดชอบ จัดส่งให้องค์การรักษาความปลอดภัยเพื่อตรวจสอบข้อมูลด้านความมั่นคง

๑.๒ การตรวจสอบโดยละเอียด

๑.๒.๑ การตรวจสอบบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการชั้นลับที่สุด ลับมาก หรือการรหัส บุคคลที่มีพฤติการณ์ หรือปรากฏข่าวสาร หรือติดต่อกับบุคคลหรือองค์การทั้งภายในและภายนอกประเทศ ที่จะเป็นภัย หรือเสี่ยงต่อความมั่นคงและผลประโยชน์แห่งรัฐบุคคลที่จะได้รับมอบหมายให้ทำหน้าที่ หรือแต่งตั้งให้ดำรงตำแหน่งสำคัญในหน่วยงานของรัฐต้องได้รับการตรวจสอบโดยละเอียด

๑.๒.๒ วิธีการตรวจสอบโดยละเอียด

๑.๒.๒.๑ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนด ในประกาศสำนักนายกรัฐมนตรี

๑.๒.๒.๒ การตรวจสอบโดยละเอียด อาจขอให้องค์การรักษาความปลอดภัยดำเนินการให้ โดยปฏิบัติตามหลักเกณฑ์ที่องค์การรักษาความปลอดภัยกำหนด

๑.๒.๒.๓ กรณีขอให้องค์การรักษาความปลอดภัยตรวจสอบประวัติและพฤติการณ์บุคคล ให้หน่วยงานของรัฐส่งหนังสือนำพร้อมแบบประวัติบุคคล ของบุคคลที่จะต้องตรวจสอบโดยระบุวัตถุประสงค์ในการตรวจสอบ ในกรณีที่เคยผ่านการตรวจสอบประวัติและพฤติการณ์มาแล้ว ให้ระบุชื่อหน่วยงานที่เคยดำเนินการตรวจสอบประวัติและพฤติการณ์ด้วย

๑.๓ ในระหว่างที่รอฟังผลการตรวจสอบประวัติและพฤติการณ์บุคคล ถ้าจำเป็นต้องรีบบรรจุหรือจ้างบุคคลเข้าปฏิบัติงาน ก็ให้บรรจุหรือจ้างก่อนได้ โดยมีเงื่อนไขว่า ถ้าผล

การตรวจสอบปรากฏว่า ผู้นั้นมีความประพฤติหรือมีประวัติและพฤติการณ์ไม่เหมาะสม ให้หน่วยงานของรัฐสั่งเลิกบรรจุหรือเลิกจ้างได้

๑.๔ ถึงแม้ว่าหัวหน้าหน่วยงานของรัฐ จัดให้มีการตรวจสอบประวัติและพฤติการณ์ของผู้ใต้บังคับบัญชาแล้วนั้น เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพอยู่เสมอ หากพบว่าเจ้าหน้าที่ของรัฐผู้ใด มีพฤติการณ์ที่น่าสงสัย หรือมีการกระทำ อันก่อนให้เกิดความไม่น่าไว้วางใจ ซึ่งอาจเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ ให้ย้ายผู้นั้น ออกจากตำแหน่งหน้าที่นั้นโดยเร็วและพิจารณาดำเนินการต่อไป โดยให้รายงานองค์การรักษาความปลอดภัยทราบหรือขอให้ตรวจสอบประวัติพฤติการณ์ใหม่

๒. การรับรองความไว้วางใจบุคคล เพื่อให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ หัวหน้าหน่วยงานของรัฐเป็นผู้พิจารณารับรองความไว้วางใจ ให้เจ้าหน้าที่ของรัฐ หรือบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือปฏิบัติหน้าที่สำคัญ โดยให้ปฏิบัติดังนี้

๒.๑ บุคคลที่ได้รับการรับรองความไว้วางใจ ต้องผ่านการตรวจสอบประวัติและพฤติการณ์ โดยได้รับการอนุมัติจากหัวหน้าหน่วยงานของรัฐ และให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยบันทึกในแบบการรับรองความไว้วางใจ

๒.๒ บุคคลใดที่ได้รับการรับรองความไว้วางใจ ต้องผ่านการอบรม หรือชี้แจงในเรื่องการรักษาความปลอดภัย เพื่อให้สามารถปฏิบัติหน้าที่ที่ได้รับมอบหมายให้ถูกต้อง และมีจิตสำนึกในการรักษาความปลอดภัย

๒.๓ บุคคลที่ได้รับความไว้วางใจ จะต้องลงนามในบันทึกรับรองการรักษาความลับเมื่อเข้ารับตำแหน่งหน้าที่ และเมื่อพ้นตำแหน่งหน้าที่ให้ลงนามในบันทึกรับรองการรักษาความลับเพื่อสัญญาว่าจะรักษาความลับของทางราชการ และไม่นำไปเปิดเผยให้ผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ การรับรองความไว้วางใจบุคคลให้เข้าถึงความลับชั้นต่างๆ หรือหน้าที่สำคัญไม่มีข้อจำกัดในเรื่องตำแหน่ง ระดับ ยศ แต่อย่างใด กรณีเกิดความจำเป็นหัวหน้าหน่วยงานของรัฐพิจารณาเห็นว่าบุคคลผู้นั้นมีความเหมาะสม โดยดำเนินกรรมวิธีการรับรองความไว้วางใจตามที่ระเบียบกำหนดไว้

๒.๔ เมื่อมีความจำเป็นเร่งด่วน หัวหน้าหน่วยงานของรัฐอาจรับรองความไว้วางใจบุคคล ก่อนทราบผลการตรวจสอบประวัติและพฤติการณ์ ในกรณีดังนี้

๒.๔.๑ บุคคลที่มีความจำเป็นต้องรีบบรรจุหรือว่าจ้าง

๒.๔.๒ บุคคลปฏิบัติหน้าที่เฉพาะภารกิจ เป็นการชั่วคราว ที่เกี่ยวกับความลับของทางราชการ

๓. การทะเบียนความไว้วางใจ

เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหน่วยงานของรัฐ จะต้องลงทะเบียนความไว้วางใจ ของเจ้าหน้าที่ในหน่วยงานของตนที่ได้รับความไว้วางใจ โดยยึดถือใบรับรองความไว้วางใจ เป็นหลักฐาน และมีการตรวจสอบข้อมูลให้ถูกต้องตามความเป็นจริงอยู่เสมอ เมื่อพบบุคคลใดมีพฤติการณ์ที่น่าสงสัย ต้องตรวจสอบประวัติและพฤติการณ์ เพิ่มเติม หากปรากฏพฤติการณ์เป็นที่ไม่น่าไว้วางใจ ให้ยกเลิกหรือลดระดับความไว้วางใจพร้อมบันทึกการเปลี่ยนแปลงในทะเบียนความไว้วางใจทุกครั้ง

กรณีที่พ้นตำแหน่งหรือหน้าที่ ที่เกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการในชั้นลับที่สุด ลับมาก และลับ ต้องคัดชื่อบุคคลนั้นออกจากทะเบียนความไว้วางใจด้วย และให้บุคคลนั้นส่งคืนข้อมูลข่าวสารและหลักฐานต่างๆ ในความรับผิดชอบทั้งหมด และเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยประจำหน่วยงานของรัฐ ต้องชี้แจงให้ทราบถึงความรับผิดชอบในการรักษาความลับของทางราชการ พร้อมกับให้บุคคลนั้นลงลายมือชื่อ ในบันทึกรับรองการรักษาความลับเมื่อพ้นตำแหน่งหรือหน้าที่ไว้เป็นหลักฐาน

๔. การอบรมเรื่องการรักษาความปลอดภัย การมีจิตสำนึกและวินัยในการรักษาความปลอดภัย มีความสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยในหน่วยงานของรัฐ ดังนั้นหน่วยงานของรัฐ จึงควรจัดให้มีการปฏิบัติดังนี้

๔.๑ หน้าหน้าหน่วยงานของรัฐ ต้องจัดให้มีการอบรมชี้แจงระเบียบ เกี่ยวกับการรักษาความปลอดภัยแก่เจ้าหน้าที่ของรัฐ บุคคลที่จะปฏิบัติหน้าที่เกี่ยวข้องกับความลับของทางราชการและบุคคลที่ต้องเข้ามาปฏิบัติงานในพื้นที่ควบคุม ให้มีความรู้ความเข้าใจเกี่ยวกับเรื่องการรักษาความปลอดภัย

๔.๒ ต้องมีการอบรม ทบทวนเกี่ยวกับการรักษาความปลอดภัย และเพิ่มเติมวิทยาการใหม่ตามห้วงเวลาที่เหมาะสม เพื่อกระตุ้นจิตสำนึกและวินัยในการรักษาความปลอดภัย

๔.๓ หน่วยงานของรัฐอาจประสานขอความร่วมมือ และคำแนะนำในการจัดอบรมให้ความรู้จากองค์การรักษาความปลอดภัยได้

การรักษาความปลอดภัยเกี่ยวกับสถานที่

การรักษาความปลอดภัยเกี่ยวกับสถานที่ กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่สงวน อาคารและสถานที่ของหน่วยงานของรัฐ ตลอดจนวัสดุอุปกรณ์ เจ้าหน้าที่ของรัฐ และข้อมูลข่าวสารในอาคารสถานที่ดังกล่าว ให้พ้นจากการโจรกรรม การจารกรรม การก่อวินาศกรรม การก่อการร้าย หรือเหตุอื่นใด อันอาจทำให้เสียสมรรถภาพในการปฏิบัติภารกิจของหน่วยงานซึ่งจะส่งผลให้เกิดความเสียหายต่อหน่วยงานของรัฐและการบริหารราชการแผ่นดิน

หน่วยงานของรัฐต้องดำเนินการสำรวจ ตรวจสอบ และจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ การกำหนดมาตรการการรักษาความปลอดภัย เกี่ยวกับสถานที่ ให้ดำเนินการดังนี้

๑. หน่วยงานของรัฐต้องกำหนดพื้นที่รักษาความปลอดภัยตามความเหมาะสม กำหนดขอบเขตที่แน่ชัดว่าพื้นที่ใดเป็นพื้นที่ควบคุมหรือพื้นที่หวงห้าม เพื่อควบคุมการเข้า-ออกของบุคคลและยานพาหนะ

๒. วางระบบป้องกันทางวัตถุเพื่อเป็นเครื่องหน่วงเหนี่ยว กีดขวาง ป้องกันบุคคลหรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัย เช่น รั้ว เครื่องกีดขวาง ช่องทางเข้า-ออก รวมถึงระบบการให้แสงสว่างในยามวิกาล

๓. การควบคุมบุคคลและยานพาหนะ

๓.๑ การควบคุมบุคคล เพื่อตรวจสอบให้ทราบว่าเป็นบุคคลที่ได้รับอนุญาตให้ผ่านพื้นที่ โดยจัดทำบัตรผ่าน บัตรแสดงตน และบันทึกหลักฐานการผ่านเข้า-ออก นั้น

๓.๒ การควบคุมยานพาหนะ เพื่อให้ทราบว่ายานพาหนะใด ได้รับอนุญาตให้ผ่านเข้าในบริเวณพื้นที่ได้ และยังรวมถึงการควบคุมบุคคลและสิ่งของต่าง ๆ บนยานพาหนะด้วย

๔. ระบบรักษาการณ์ หน่วยงานของรัฐต้องจัดให้มีเจ้าหน้าที่รักษาความปลอดภัยประจำวัน เจ้าหน้าที่ยามรักษาการณ์ ฯลฯ วางระบบการติดต่อสื่อสารและสัญญาณแจ้งภัย สำหรับตรวจและเตือนให้ทราบเมื่อมีภัย รวมถึงการติดตั้งอุปกรณ์เสริมมาตรการการรักษาความปลอดภัยทางเครื่องมือเครื่องใช้อิเล็กทรอนิกส์หรืออื่นๆ เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น

๕. ระบบป้องกันและระงับอัคคีภัย หัวหน้าหน่วยงานของรัฐต้องจัดให้มีมาตรการป้องกันและระงับอัคคีภัยที่มีประสิทธิภาพอาคารสถานที่ ทรัพย์สินมีค่าของแผ่นดินและความลับของทางราชการ รวมถึงบุคคลสำคัญของหน่วยงาน อาจเป็นเป้าหมายของการโจรกรรม การจารกรรม การก่อวินาศกรรม และการก่อการร้ายได้ ดังนั้นจึงจำเป็นต้องวางมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ เพื่อพิทักษ์รักษาบุคคลและทรัพย์สินของทางราชาการให้ปลอดภัย หรือขัดขวาง หน่วงเหนี่ยวการดำเนินการของฝ่ายตรงข้ามมิให้สัมฤทธิ์ผล หรือมีผลเสียหายต่อหน่วยงานน้อยที่สุด และยังต้องประสานสอดคล้องกับมาตรการป้องกันภัยทางธรรมชาติ รวมถึงอุบัติภัยด้วย ดังนั้นหน่วยงานของรัฐต้องกำหนดแผนการรักษาความปลอดภัย เกี่ยวกับสถานที่ของหน่วยงานตนเอง โดยสำรวจการรักษาความปลอดภัยเกี่ยวกับสถานที่ของหน่วยงานก่อน จากนั้นจึงนำผลจากการสำรวจเป็นข้อมูลพื้นฐานประกอบในการกำหนดแผน ซึ่งแผนดังกล่าวนี้ เป็นเรื่องที่ต้องปฏิบัติเป็นกิจวัตร หน่วยงานเจ้าของแผนจึงต้องพิจารณาปรับปรุง แก้ไขแผนให้มีประสิทธิภาพ

อยู่ตลอดเวลา การกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ ต้องคำนึงถึงหลักการดังนี้

๑. การกำหนดพื้นที่ที่มีการรักษาความปลอดภัย เพื่อเป็นการป้องกันผู้ไม่มีอำนาจหน้าที่ หรือผู้ไม่ประสงค์ดี เข้าไปในพื้นที่ โดยดำเนินการดังนี้ ต้องมีการเฝ้าตรวจ ผู้ที่จะเข้ามาในพื้นที่ ต้องมีการพิสูจน์ทราบว่าผู้ที่จะเข้ามาเป็นใคร มีวัตถุประสงค์ใด มีสิทธิ มีอำนาจหน้าที่หรือไม่ เป็นภัยหรือไม่ ต้องมีการขัดขวาง หากผู้ที่จะเข้ามาในพื้นที่เป็นผู้ที่ไม่มีอำนาจหน้าที่หรืออาจเป็นภัยได้ พื้นที่หรือบริเวณของส่วนราชการต่างๆ ควรกำหนดขอบเขตให้ชัดเจน ว่าพื้นที่ใดควรได้รับการรักษาความปลอดภัยเป็นพิเศษ โดยแบ่งพื้นที่ ดังนี้

๑.๑ พื้นที่ควบคุม คือพื้นที่โดยรวมของหน่วยงาน อยู่ภายในขอบเขตของพื้นที่มีการรักษาความปลอดภัยทั้งหมด ต้องมีระเบียบการควบคุมบุคคล และยานพาหนะ เพื่อช่วยกลั่นกรองในชั้นหนึ่งก่อน มาตรการที่ใช้ควบคุมการผ่านเข้า-ออก เช่น การออกบัตรผ่าน และ/หรือ บันทึกการผ่านเข้า-ออกของบุคคลและยานพาหนะ

๑.๒ พื้นที่หวงห้าม คือพื้นที่ที่มีการพิทักษ์รักษาสิ่งที่เป็นความลับต่างๆ ตลอดจนบุคคลสำคัญ ทรัพย์สินของทางราชการ ซึ่งแบ่งพื้นที่หวงห้ามออกเป็นดังนี้

๑.๒.๑ “เขตหวงห้ามเฉพาะ” คือ พื้นที่ซึ่งมีความลับ และบุคคลสำคัญ ต้องมีการตรวจสอบบุคคลที่เข้าถึงอย่างเข้มงวด

๑.๒.๒ “เขตหวงห้ามเด็ดขาด” คือ พื้นที่ซึ่งมีความลับ และบุคคลที่สำคัญยิ่งบุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเด็ดขาด” ต้องได้รับการไว้วางใจตามชั้นความลับที่เหมาะสม และมาตรการเสริมเพิ่มเติม เช่น บัตรผ่านเข้า-ออก จะต้องใช้เฉพาะการผ่านเพียงครั้งเดียว และมีการบันทึกการเข้า-ออก ทุกครั้ง

๒. การวางระบบป้องกันทางด้านวัตถุเป็นมาตรการหน่วงเหนี่ยว จำกัด ขัดขวางการรุกล้ำ หรือป้องปราม เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยมีโอกาสตรวจสอบ พิสูจน์ทราบ และขัดขวาง หากมีการบุกรุก การป้องกันทางวัตถุอาจประกอบด้วย

๒.๑ เครื่องกีดขวางโดยรอบ แบ่งได้เป็น

๒.๑.๑ เครื่องกีดขวางตามธรรมชาติ เช่น แม่น้ำ ลำคลอง เป็นต้น อาจพิจารณาดัดแปลง หรือปรับปรุงให้ใช้ประโยชน์เป็นเครื่องกีดขวางได้

๒.๑.๒ เครื่องกีดขวางที่ประดิษฐ์ขึ้น เช่น รั้ว เครื่องกีดขวางบริเวณช่องทางเข้า-ออก ดัดแปลง แผงกั้นล้อเลื่อน และแขนกั้นยานพาหนะ เป็นต้น

๒.๒ การให้แสงสว่าง เพื่อให้มาตรการรักษาความปลอดภัยสถานที่มีประสิทธิภาพ เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่างๆ โดยชัดเจนในเวลามืด จะได้มองเห็นผู้ที่บุกรุกเข้ามานานาสถานที่

๓. ระบบการติดต่อสื่อสารและสัญญาณแจ้งภัย จะช่วยให้การติดต่ออำนวยการควบคุมสถานการณ์ ตลอดจนรายงานผลการดำเนินการ เป็นไปได้อย่างรวดเร็วทันต่อเหตุการณ์ และมีประสิทธิภาพระบบการติดต่อสื่อสาร เช่น โทรศัพท์ วิทยุสื่อสาร เป็นต้น ต้องสามารถติดต่อเจ้าหน้าที่ผู้บังคับบัญชา เพื่อรายงานเหตุการณ์ รวมทั้งติดต่อหน่วยงานอื่น เพื่อระงับยับยั้ง และบรรเทาเหตุที่เกิดขึ้น ระบบสัญญาณแจ้งภัย เช่น เครื่องมือทางอิเล็กทรอนิกส์ ไฟฟ้า เครื่องกล เป็นต้น ที่ทำให้เกิดสัญญาณเมื่อมีผู้บุกรุก หรือเกิดเหตุอื่นๆ เช่น สัญญาณจับควันและสัญญาณจับคลื่นความร้อน เป็นต้น

๔. การควบคุมบุคคลและยานพาหนะ เป็นภารกิจหลักของการรักษาความปลอดภัยสถานที่ ผู้รับผิดชอบต้องการตรวจสอบบุคคล และยานพาหนะอย่างละเอียด รอบคอบ ถี่ถ้วน เพื่อให้แน่ใจว่าผู้ที่ผ่านเข้ามาในพื้นที่มีสิทธิที่จะผ่านเข้ามา และไม่ก่อเหตุละเมินการรักษาความปลอดภัย

๔.๑ การควบคุมบุคคล บัตรผ่านและป้ายแสดงตน เป็นหลักฐานแสดงสถานะต่อเจ้าหน้าที่รักษาการณ์ขณะผ่านจุดตรวจ หรือช่องทาง เข้า-ออก ทั้งนี้ถือเป็นการแสดงว่ามีสิทธิในการผ่าน เข้า-ออก และการเข้าถึงพื้นที่ที่การรักษาความปลอดภัยได้

๔.๑.๑ บัตรผ่าน คือบัตรที่หน่วยงานของรัฐออกให้สำหรับบุคคล และยานพาหนะของผู้ที่ปฏิบัติงานอยู่ในพื้นที่นั้น และบุคคลภายนอกที่ต้องเข้ามาติดต่อเป็นการชั่วคราว โดยให้เจ้าหน้าที่รักษาการณ์ทำการบันทึกหลักฐาน ตรวจสอบ และมอบบัตรผ่าน ให้ใช้ในการผ่านเข้า-ออกในแต่ละครั้ง

๔.๑.๒ ป้ายแสดงตน คือ หลักฐานใช้ควบคุมบุคคล ใช้สำหรับบุคคลทั้งภายในและภายนอก เพื่อแสดงสถานะในการเข้าในพื้นที่ที่มีการรักษาความปลอดภัย ป้ายแสดงตนต้องแสดงไว้ให้เห็นเด่นชันตลอดเวลาที่อยู่ในพื้นที่

๔.๑.๓ บันทึกหลักฐานการผ่านเข้า-ออก เป็นมาตรการควบคุมเสริมจากการใช้บัตรผ่าน หรือบัตรแสดงตน โดยจัดให้มีเจ้าหน้าที่บันทึกหลักฐาน สำหรับบุคคลที่ผ่านเข้า-ออก ในพื้นที่ที่มีการรักษาความปลอดภัย โดยให้มีการจดบันทึกรายละเอียด เช่นกัน ส่วนบุคคลภายนอกในกรณีผู้มาประชุม ติดต่อราชการ หรือพบปะเจ้าหน้าที่ของหน่วยงาน โดยให้มีรายละเอียด เช่น ชื่อ ที่อยู่ของผู้ที่ผ่านเข้า-ออก หน่วยงานที่สังกัด วัน เวลา ที่ผ่านเข้า-ออก ชื่อผู้ที่มาติดต่อ เหตุผลในการผ่านเข้า-ออกพื้นที่

๔.๒ การควบคุมยานพาหนะ หมายรวมถึง การควบคุมทั้งบุคคล และสิ่งของต่าง ๆ บนยานพาหนะด้วย ยานพาหนะที่ได้รับการอนุญาตให้ผ่านเข้าไปในพื้นที่ ควรกำหนดเส้นทางและที่จอดรถทั้งของเจ้าหน้าที่ภายในและบุคคลภายนอกให้ชัดเจน การบันทึกหลักฐานยานพาหนะที่ เข้า-ออก ควรมีรายละเอียดดังต่อไปนี้

๔.๒.๑ วัน เวลา ที่ยานพาหนะผ่าน เข้า-ออก

๔.๒.๒ ชื่อผู้ขับ และชื่อผู้โดยสาร

๔.๒.๓ ประเภท ชนิด สี เลขทะเบียนยานพาหนะ

๔.๒.๔ ลักษณะและจำนวนสิ่งของบนยานพาหนะนั้น

๔.๒.๕ วัตถุประสงค์การเข้าพื้นที่ควบคุม

๕. ระบบการรักษาการณ์

๕.๑ ระบบการรักษาการณ์ คือ การจัดและกำหนดเจ้าหน้ารักษาความปลอดภัย เจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน นายตรวจเวร เจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ ปฏิบัติหน้าที่รักษาความปลอดภัย สถานที่ตามห้วงระยะเวลาที่กำหนด และให้รู้จักการใช้เครื่องมืออุปกรณ์ที่เสริมประสิทธิภาพในการปฏิบัติงาน ตลอดจนสนใจข่าวสารที่อาจส่งผลกระทบเป็นภัยต่อหน่วยงาน

๕.๒ กำลังและขีดความสามารถของเจ้าหน้าที่รักษาการณ์ และหรือยามรักษาการณ์เพียงพอกับการปฏิบัติหน้าที่ ตามความสำคัญของสถานที่ของราชการนั้นๆ หรือไม่ มีการแก้ไขทดแทน หรือปรับปรุงจุดอ่อนเกี่ยวกับเรื่องนี้ด้วยวิธีใด มีการประสานแผนการรักษาความปลอดภัยกับส่วนราชการอื่นที่เกี่ยวข้อหรือไม่

๕.๓ ต้องมีการคัดเลือก ตรวจสอบประวัติและพฤติการณ์ เพื่อสรรหาตัวบุคคลที่ทำหน้าที่เจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ โดยพิจารณาจากคุณสมบัติด้านคุณธรรม จริยธรรม และสมรรถนะทางร่างกาย

๕.๔ ต้องมีการกำกับดูแล โดยเจ้าหน้าที่รักษาความปลอดภัยของหน่วยงานนั้นๆ ด้วยวิธีการดังต่อไปนี้

๕.๔.๑ การกำกับดูแลโดยบุคคล หมายถึงการตรวจสอบการปฏิบัติงาน โดยหัวหน้าเจ้าหน้าที่รักษาการณ์ตามลำดับชั้น การตรวจจะทำตั้งแต่ก่อนเริ่มปฏิบัติหน้าที่ ตรวจสภาพทั่วไปของเครื่องมือ อุปกรณ์ อาวุธ ทบทวนคำสั่งและระเบียบของสถานที่นั้น ตรวจตามระยะเวลาระหว่างการปฏิบัติหน้าที่ เพื่อดูความพร้อม ความเคร่งครัด ความตื่นตัวในการปฏิบัติหน้าที่

๕.๔.๒ การกำกับดูแลโดยเครื่องมือ เป็นการใช้เครื่องมือ หรือวิธีการที่เสมือนบังคับให้เจ้าหน้าที่รักษาการณ์ ต้องปฏิบัติตามระยะเวลาที่ทำหน้าที่ เครื่องมือและวิธีการมีดังนี้

๕.๔.๒.๑ บันทึกการปฏิบัติ โดยใช้แบบฟอร์มรายงานการปฏิบัติให้เจ้าหน้าที่รักษาการณ์เป็นผู้ลงบันทึก ตามจุด และเวลาที่กำหนดไว้

๕.๔.๒.๒ ตรวจสอบการปฏิบัติงาน โดยเครื่องมือสื่อสาร เช่น วิทยุสื่อสาร โทรศัพท์ และสัญญาณอื่น ๆ ที่สามารถสื่อความหมายได้ โดยหัวหน้าเจ้าหน้าที่รักษาการณ์ หรือเจ้าหน้าที่รักษาความปลอดภัยของหน่วยงานเป็นผู้ตรวจสอบ

๕.๕ ต้องมีการฝึกอบรมและพัฒนาเจ้าหน้าที่รักษาการณ์ หรือยามรักษาการณ์เพื่อให้การปฏิบัติหน้าที่มีประสิทธิภาพ ให้ตระหนักถึงภยันตรายที่อาจเกิดขึ้นแก่หน่วยงาน สร้างจิตสำนึกในการรักษาความปลอดภัย ฝึก ทบทวน การใช้เครื่องมือ อาวุธ อุปกรณ์ต่างๆ ตลอดจนทดสอบความสามารถ วินัยในการปฏิบัติหน้าที่

๖. การป้องกันและระงับอัคคีภัย หัวหน้าส่วนราชการต้องกำหนดแผนป้องกันและระงับอัคคีภัย โดยเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงาน เป็นผู้กำหนดรายละเอียดและกำกับดูแล ให้เป็นไปตามกฎหมายเกี่ยวกับการป้องกันและระงับอัคคีภัย ในแต่ละหน่วยงานพิจารณาดังนี้

๖.๑ เจ้าหน้าที่ดับเพลิง ควรกำหนดตัวบุคคล และหน้าที่ความรับผิดชอบให้ชัดเจน

๖.๑.๑ ในเวลาราชการ ให้แบ่งกลุ่มเจ้าหน้าที่รับผิดชอบด้านต่าง ๆ เช่น กลุ่มที่ทำหน้าที่ดับเพลิง กลุ่มที่ทำหน้าที่ขนย้ายเอกสารและวัสดุอุปกรณ์ต่าง ๆ กลุ่มที่ทำหน้าที่ค้นหาตรวจตราผู้ที่หลงเหลือในอาคาร เป็นต้น

๖.๑.๒ นอกเวลาราชาการ เป็นหน้าที่ของ เจ้าหน้าที่รักษาความปลอดภัยและเจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ประจำวันที่หน่วยงานกำหนดขึ้นเป็นผู้รับผิดชอบ

๖.๒ การจัดเตรียมอุปกรณ์ในการดับเพลิง

๖.๒.๑ สัญญาณแจ้งเหตุเพลิงไหม้

๖.๒.๒ เครื่องมือดับเพลิงชั้นต้น เช่น น้ำ ทราย ถัง เชือก ขวาน เป็นต้น อุปกรณ์ถังเคมีดับเพลิงที่เหมาะสมกับเพลิงไหม้ทุกประเภท

๖.๒.๓ ตำแหน่งที่ติดตั้งควรอยู่ในตำแหน่งที่มองเห็นได้ชัดเจน และสามารถนำไปใช้ได้สะดวก

๖.๒.๔ ตรวจสอบอุปกรณ์ทุกชนิดให้อยู่ในสภาพที่ใช้งานได้

๖.๒.๕ หมายเลขโทรศัพท์ของหน่วยงานดับเพลิงที่ติดต่อได้สะดวกรวดเร็ว

๖.๓ การฝึกอบรมเรื่องการดับเพลิง ให้จัดทำแผนป้องกันและระงับอัคคีภัย เส้นทางหนีไฟ และอบรมให้เจ้าหน้าที่ทุกคนในหน่วยงาน ระมัดระวังป้องกันการเกิดอัคคีภัย ฝึกซ้อมให้มีความรู้ ความชำนาญ ในการดับเพลิงเบื้องต้น การหนีไฟตามแผน โดยเจ้าหน้าที่ควรมีความรู้ในเรื่องต่างๆ ดังนี้

๖.๓.๑ ประเภทของเพลิง เช่น จากวัสดุธรรมดา น้ำมัน วัตถุเคมี และกระแสไฟฟ้าลัดวงจร เป็นต้น

๖.๓.๒ เครื่องมืออุปกรณ์ที่ใช้ในการดับเพลิง ตำแหน่งที่ตั้งวิธีการใช้

๖.๓.๓ การติดต่อสื่อสาร แจ้งเหตุ แผนผังอาคาร เส้นทางเคลื่อนย้าย เส้นทางหนีไฟ

๖.๓.๔ หมายเลขโทรศัพท์หน่วยดับเพลิง

๗. อุปกรณ์เสริมมาตรการรักษาความปลอดภัย การติดตั้งอุปกรณ์เสริมมาตรการรักษาความปลอดภัย หน่วยงานของรัฐควรพิจารณาตามความเหมาะสม เช่น ระบบกล้องโทรทัศน์วงจรปิด ซึ่งควรมีผู้รับผิดชอบในการควบคุม เฝ้าดู และตรวจสอบให้อยู่ในสภาพใช้งานได้ตลอดเวลา เป็นต้น

การรักษาความปลอดภัยในการประชุมลับ

หัวหน้าหน่วยงานของรัฐ ต้องจัดให้มีมาตรการการรักษาความปลอดภัย ในการประชุมลับ โดยกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับบุคคล ข้อมูลข่าวสารลับ และสถานที่ เพื่อพิทักษ์รักษาสิ่งที่เป็นความลับของทางราชการการ ที่ปรากฏในการประชุมลับ ไม่ให้มีการรั่วไหล ถูกจารกรรม รบกวน หรือขัดขวาง การประชุม รวมทั้งคุ้มครองบุคคลและสถานที่ที่เกี่ยวข้องกับการประชุมลับนั้น จากการก่อวินาศกรรม ทั้งนี้ให้นำมาตรฐานของการรักษาความปลอดภัยแต่ละเรื่องมาปรับใช้โดยอนุโลม

การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยในการประชุมลับ

๑. หัวหน้าหน่วยงานของรัฐเจ้าของเรื่องที่จะมีการประชุมลับ เป็นผู้รับผิดชอบการรักษาความปลอดภัยเกี่ยวกับการประชุมลับนั้น หรืออาจมอบหมายให้บุคคลที่เหมาะสมเป็นผู้ดำเนินการแทนได้ โดยแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับและนายทะเบียนข้อมูลข่าวสารลับ รวมทั้งแจ้งให้ผู้เข้าร่วมการประชุมและผู้มีหน้าที่เกี่ยวข้องทุกฝ่ายทราบ

๒. กรณีการประชุมลับหลายหน่วยงาน ต้องกำหนดหน่วยงานเจ้าภาพรับผิดชอบและแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ หัวหน้าที่ประสานงานใน

เรื่อง การรักษาความปลอดภัย กับเจ้าหน้าที่รักษาความปลอดภัยในการประชุมลับของแต่ละหน่วยงาน ซึ่งจะต้องวางมาตรการการรักษาความปลอดภัยเฉพาะในฝ่ายตน ให้สอดคล้องกับมาตรการการรักษาความปลอดภัยในการประชุมลับ

๓. การรักษาความปลอดภัยในการประชุมลับต้องคำนึงถึงหลักการดังต่อไปนี้

๓.๑ บุคคลที่เกี่ยวข้องกับการประชุมลับ ต้องผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล พร้อมทั้งได้รับความไว้วางใจให้เข้าถึงความลับในการประชุมนั้น และการปฏิบัติงานให้อยู่ในความควบคุม ของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับนั้น สำหรับผู้ที่ไม่มีอำนาจหน้าที่ ต้องไม่ได้รับทราบหรือครอบครองสิ่งที่เป็นความลับของทางราชการในการประชุม

๓.๒ ห้ามนำเครื่องมือสื่อสาร วัสดุอุปกรณ์ หรือเครื่องบันทึกภาพหรือเสียงเข้าไปในสถานที่ประชุมและต้องไม่นำเครื่องมือ วัสดุอุปกรณ์ หรือข้อมูลข่าวสารใด ๆ ออกนอกสถานที่ประชุมนั้น

๔. การรักษาความปลอดภัยในการประชุมลับ ให้หน่วยงานของรัฐพิจารณาดำเนินการดังต่อไปนี้

๔.๑ กำหนดพื้นที่ที่มีการรักษาความปลอดภัยประกอบด้วยสิ่งดังต่อไปนี้

๔.๑.๑ กำหนดอาณาเขตที่ใช้ในการประชุมลับ ที่ทำการของผู้เข้าประชุมลับ และสถานที่ที่ใช้เก็บรักษาสิ่งที่เป็นความลับของทางราชการ และจัดให้มีมาตรการการรักษาความปลอดภัยตามความจำเป็นและเหมาะสมไว้ล่วงหน้าก่อนเปิดการประชุมลับ

๔.๑.๒ กำหนดให้มีบัตรผ่านหรือป้ายแสดงตน สำหรับใช้ควบคุมบุคคลหลักเกณฑ์และวิธีปฏิบัติ ในการกำหนดพื้นที่ที่มีการรักษาความปลอดภัย ในการประชุมลับตามวรรคหนึ่ง ให้ดำเนินการตามมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่

๔.๒ ดำเนินการรักษาความปลอดภัย เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับต้องดำเนินการดังต่อไปนี้

๔.๒.๑ ตรวจตราและตรวจสอบทางเทคนิคตลอดในพื้นที่ ที่กำหนดให้มีการรักษาความปลอดภัยทั้งหมด อย่างละเอียดก่อนวันเปิดประชุมลับและระหว่างการประชุมลับ

๔.๒.๒ ในกรณีที่การประชุมลับนั้น มีความสำคัญมาก หน่วยของรัฐอาจขอความช่วยเหลือจากองค์การรักษาความปลอดภัย หลังจากที่องค์การรักษาความปลอดภัยตรวจสอบแล้วให้ส่งมอบความรับผิดชอบในพื้นที่นั้น เป็นลายลักษณ์อักษรแก่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ หรือผู้แทนหน่วยงานนั้น

การปฏิบัติต่อสิ่งที่เป็นความลับของทางราชการ การควบคุม ดูแลการประชุมลับการทำลายข้อมูลข่าวสารลับที่ไม่ใช้แล้ว ให้อยู่ในความดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับและนายทะเบียนข้อมูลข่าวสารลับ

๔.๓ ประสานงานการรักษาความปลอดภัย กรณีการประชุมลับหลายหน่วยงาน ต้องกำหนดหน่วยงานเจ้าภาพผิดชอบ และแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ โดยผู้เข้าประชุมแต่ละฝ่าย จำเป็นต้องวางมาตรการการรักษาความปลอดภัยเฉพาะในฝ่ายตน ซึ่งการวางมาตรการดังกล่าว ต้องสอดคล้องกับมาตรการการรักษาความปลอดภัย ในการประชุมลับ ทั้งนี้เจ้าหน้าที่รักษาความปลอดภัยการประชุมลับ ทำหน้าที่ประสานงานในเรื่องการรักษาความปลอดภัยกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ

๔.๔ กำหนดวิธีปฏิบัติต่อผู้มาติดต่อ หลักเกณฑ์การปฏิบัติต่อผู้มาติดต่อในการประชุมลับ ให้ดำเนินการตามมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยผู้ติดต่อกับผู้เข้าร่วมประชุมลับ ต้องเป็นบุคคลที่ได้รับอนุญาตให้ผ่านเข้าพื้นที่ที่มีการรักษาความปลอดภัยพื้นที่ควบคุม หรือพื้นที่หวงห้าม และกำหนดให้มีบัตรผ่านหรือป้ายแสดงตน สำหรับใช้ควบคุมบุคคล รวมทั้งจัดให้มีการบันทึกหลักฐานสำหรับผู้มาติดต่อ ทั้งนี้ จัดให้มีสถานที่พักรอสำหรับผู้มาติดต่อ

๔.๕ แถลงข่าวต่อสื่อมวลชน กรณีจำเป็นต้องมีการแถลงข่าวเกี่ยวกับการประชุมลับให้ผู้รับผิดชอบจัดประชุมดำเนินการดังต่อไปนี้

๔.๕.๑ จัดสถานที่ที่ใช้แถลงข่าวขึ้นโดยเฉพาะ และควรอยู่นอกพื้นที่ที่มีการรักษาความปลอดภัยในการประชุมลับ

๔.๕.๒ กำหนดให้ผู้แถลงข่าว หัวข้อที่จะนำแถลง และข้อมูลข่าวสารที่จะเผยแพร่ต้องได้รับอนุมัติจากที่ประชุมลับก่อน หรือในกรณีที่ที่ประชุมลับมอบหมายให้มีผู้แถลงข่าวหลายคน ผู้แถลงข่าวแต่ละคนต้องแถลงเฉพาะเรื่องที่ตนได้รับอนุมัติจากที่ประชุมลับเท่านั้น

๔.๕.๓ ควบคุมให้การแถลงข่าวหรือการเผยแพร่ข้อมูลข่าวสาร และผู้เข้ารับฟังเป็นไปด้วยความเหมาะสม

๔.๖ บรรยายหรือบรรยายสรุปเรื่องที่เป็นความลับ ในกรณีที่เป็นการบรรยายหรือการบรรยายสรุปเรื่องที่เป็นความลับ นอกจากจะต้องปฏิบัติตามมาตรการในการรักษาความปลอดภัยในการประชุมลับแล้ว ให้ดำเนินการดังต่อไปนี้

๔.๖.๑ กำหนดชั้นความลับของการบรรยายหรือการบรรยายสรุป โดยถือตามชั้นความลับที่สูงสุดในข้อมูลข่าวสาร หรือสิ่งที่ใช้ประกอบการบรรยายหรือการบรรยายสรุป

นั้นๆ จัดสถานที่ที่ใช้แถลงข่าวขึ้นโดยเฉพาะ และควรอยู่นอกพื้นที่ที่มีการรักษาความปลอดภัยในการประชุมลับ

๔.๖.๒ กำหนดให้ผู้เข้าร่วมฟังทุกคน ต้องได้รับความไว้วางใจในเข้าถึงชั้นความลับของการบรรยาย หรือการบรรยายสรุปนั้น

๔.๖.๓ เมื่อเริ่มและสิ้นสุดการบรรยายหรือการบรรยายสรุป ผู้บรรยายต้องแจ้งให้ผู้เข้ารับฟังรับทราบชั้นความลับของการบรรยาย และเน้นย้ำให้ดำเนินการรักษาความปลอดภัยต่อสิ่งที่ได้รับฟังจากการบรรยายหรือการบรรยายสรุปนั้น

การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

หัวหน้าหน่วยงานของรัฐต้องกำหนดแนวทางปฏิบัติ เมื่อเกิดการละเมิดการรักษาความปลอดภัย เพื่อลดระดับความเสียหายกรณีเกิดการละเมิด ฝ่าฝืน หรือละเลยไม่ปฏิบัติตามมาตรการการรักษาความปลอดภัยที่กำหนดไว้ จะโดยเจตนาหรือไม่ก็ตาม อันเป็นเหตุให้ความลับของทางราชการรั่วไหล หรือเป็นเหตุให้เจ้าหน้าที่ของรัฐ วัสดุอุปกรณ์ ทรัพย์สินของรัฐ ได้รับความเสียหายและป้องกันไม่ให้เกิดซ้ำ ค้นหาข้อบกพร่องหรือสาเหตุเพื่อนำมาปรับปรุงแก้ไขมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้น โดยมีแนวทางปฏิบัติเมื่อเกิดเหตุการณ์ดังนี้

๑. ให้เจ้าหน้าที่ของรัฐผู้พบเห็นหรือทราบ หรือสงสัยว่าจะมีหรือมีการละเมิดมาตรการการรักษาความปลอดภัย รีบดำเนินการเบื้องต้นเพื่อลดความเสียหายให้เหลือน้อยที่สุดและรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบหรือแจ้งเจ้าของเรื่องเดิมทราบโดยเร็วที่สุด

๒. ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือเจ้าหน้าที่ผู้รับผิดชอบดำเนินการดังต่อไปนี้

๒.๑ สำรวจและตรวจสอบความเสียหาย อันเกิดจากการละเมิดมาตรการการรักษาความปลอดภัย

๒.๒ ดำเนินการเพื่อป้องกันหรือลดความเสียหายให้เหลือน้อยที่สุด

๒.๓ สำรวจตรวจสอบและค้นหาสาเหตุแห่งการละเมิดมาตรการการรักษาความปลอดภัย ตลอดจนจุดอ่อนและข้อบกพร่องต่างๆ

๒.๔ ดำเนินการแก้ไขมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้นเพื่อป้องกันมิให้มีการละเมิดมาตรการการรักษาความปลอดภัยเกิดขึ้นอีก

๒.๕ รายงานรายละเอียดเกี่ยวกับการละเมิดมาตรการการรักษาความปลอดภัย ต่อผู้บังคับบัญชาตามลำดับชั้น หากมีข้อมูลข่าวสารลับสูญหายให้รายงานและบันทึกลงในทะเบียนควบคุมข้อมูลข่าวสารลับด้วย

๒.๖ หากปรากฏหลักฐานหรือข้อสงสัยว่าเกิดการจารกรรม หรือการก่อวินาศกรรม ให้รายงานและขออนุมัติผู้บังคับบัญชาตามลำดับชั้น เพื่อแจ้งเรื่องให้เจ้าหน้าที่ผู้มีอำนาจหน้าที่ในด้านการสืบสวนดำเนินการต่อไป

๓. เมื่อได้ดำเนินการตามข้อ

๓.๑ แจ้งให้หน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิม หรือเจ้าของสถานที่หรือผู้ที่เกี่ยวข้องทันที

๓.๒ สอบสวนเพื่อให้ทราบว่า ผู้ใดเป็นผู้ละเมิดและผู้ใดเป็นผู้รับผิดชอบต่อการละเมิดนั้น

๓.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนั้นเกิดขึ้นซ้ำอีก

๓.๔ พิจารณาดำเนินการลงโทษตามกฎหมาย ต่อผู้ละเมิดมาตรการการรักษาความปลอดภัย หรือผู้จะละเมิด และผู้รับผิดชอบต่อการละเมิดนั้น

๔. ให้หน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิมหรือผู้ที่เกี่ยวข้อง ดำเนินการดังต่อไปนี้

๔.๑ พิจารณาว่าสมควรลดหรือยกเลิกชั้นความลับ ของสิ่งที่เป็นความลับของทางราชการนั้นหรือไม่

๔.๒ ขจัดความเสียหายอันเกิดจากการละเมิดมาตรการการรักษาความปลอดภัย ที่จะมีต่อความมั่นคงและผลประโยชน์แห่งรัฐ ในการนี้อาจต้องเปลี่ยนนโยบายและแผนพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นสมควร

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ นับเป็นกฎหมายที่ไม่ได้กำหนดขึ้น โดยตรงเกี่ยวกับการรักษาความปลอดภัยแห่งชาติ แต่มีความสำคัญอย่างยิ่งในการถือปฏิบัติ และสนับสนุนให้การรักษาความมั่นคงปลอดภัย และผลประโยชน์แห่งรัฐดำรงอยู่ได้ในปัจจุบัน นอกจากนี้ ยังเป็นกฎหมายอีกฉบับที่มีการกำหนดบทลงโทษต่อผู้กระทำผิดหรือละเมิดและมีผลกับทุกภาคส่วนตั้งแต่ภาคประชาชน ภาคเอกชน ตลอดจนภาครัฐ สรุปสาระสำคัญเกี่ยวกับฐานความผิดดังนี้

๑. การลักลอบเข้าระบบคอมพิวเตอร์ โดยไม่รับอนุญาต

๒. นำวิธีการเข้าระบบคอมพิวเตอร์ของผู้อื่นไปเปิดเผย

๓. ลักลอบเข้าถึงข้อมูลส่วนบุคคลที่จัดเก็บไว้ในระบบคอมพิวเตอร์ของผู้อื่น

๔. ดักจับข้อมูลที่ถูกส่งหากันผ่านเครือข่ายคอมพิวเตอร์ของบุคคลอื่น

๕. ปรับเปลี่ยน แก้ไขข้อมูลในระบบคอมพิวเตอร์ของบุคคลอื่น

๖. ก่อกวนระบบคอมพิวเตอร์ของบุคคลอื่น ด้วยโปรแกรมประสงค์ร้าย เช่น Virus Trojan Worm เป็นต้น

๗. จัดส่งข้อมูลที่ผู้รับไม่ต้องการ จนสร้างความไม่พอใจให้กับบุคคลอื่น

๘. ปรับเปลี่ยน แก้ไข ทำลาย ก่อกวนระบบสาธารณูปโภค หรือระบบจราจร

๙. สร้างโปรแกรมหรือซอฟต์แวร์ เพื่อสนับสนุนการะละเมิดระบบหรือรบกวนเครือข่ายคอมพิวเตอร์ของผู้อื่น ทั้งในระดับองค์กรและส่วนบุคคล

๑๐. เผยแพร่ส่งต่อภาพอนาจาร ให้ข้อมูลที่เป็นเท็จ หรือท้าทายอำนาจรัฐ

๑๑. บุคคลหรือนิติบุคคลที่เป็นผู้ให้บริการ รับทราบ ไม่ระงับยับยั้ง แก้ไข ละเลย

๑๒. ตัดต่อ เปลี่ยนแปลง และเผยแพร่ภาพที่ทำให้ผู้อื่นเสียหาย

๑๓. กระทำความผิดตามข้างต้นกับเว็บไซต์ที่มีสังกัดอยู่ภายนอกประเทศ

๑๔. บุคคลต่างด้าว บุคคลที่มิได้มีสัญชาติไทยกระทำความผิด ต้องรับผิดตามฐานแห่งโทษเช่นกัน ทั้งนี้ ต้องพิจารณาเกี่ยวกับสภาพนอกอาณาเขต และข้อตกลงเกี่ยวกับกฎหมายระหว่างประเทศเป็นกรณี

ทฤษฎีภัยคุกคามและภัยคุกคามรูปแบบใหม่

ภัยคุกคามแบบดั้งเดิม (Traditional Threat) หมายถึง ภัยคุกคามจากการใช้กำลังทหารเข้าทำการรบและยังรวมไปถึงการบ่อนทำลาย การก่อวินาศกรรม การจารกรรม ที่มีการกระทำในลักษณะรัฐต่อรัฐ เช่น สถานการณ์ การสะสมกำลังรบระหว่างสหรัฐอเมริกากับสหภาพโซเวียตในยุคสงครามเย็น ขณะที่ในส่วนของประเทศไทย ภัยคุกคามที่ผ่านมา เช่น ภัยคุกคามจากลัทธิล่าอาณานิคมอังกฤษ-ฝรั่งเศส ในรัชสมัยรัชกาลที่ ๓ ถึงรัชกาลที่ ๕ รวมถึงภัยคุกคามจากลัทธิทหารของญี่ปุ่นในช่วงสงครามโลกครั้งที่ ๒

หลังจากสงครามเย็นยุติลง โลกเข้าสู่กระแสโลกาภิวัตน์ (Globalization) ความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศนำไปสู่โลกไร้พรมแดน เป็นที่มาของภัยคุกคามรูปแบบใหม่ (Non-Tradition Threat) ซึ่งจะกล่าวถึงภัยคุกคามที่ไม่ใช่ทางทหารและไม่มีรูปแบบการกระทำในลักษณะรัฐ เช่น ปัญหาภัยธรรมชาติ อาชญากรรมข้ามชาติ การก่อการร้าย การค้ามนุษย์ สงคราม

ไซเบอร์ และอาวุธชีวภาพ เป็นต้น ทั้งนี้ในสถานการณ์ปัจจุบันเป็นเรื่องยากที่จะกำหนดขอบเขตและคำนิยามของภัยคุกคามรูปแบบใหม่ได้อย่างชัดเจน

ดังนั้นสามารถสรุปได้ว่าลักษณะของภัยคุกคามในยุคปัจจุบันสามารถแบ่งออกได้ ๓ ประเภท ได้แก่

๑. ภัยคุกคามทางทหาร คือ การสงครามในทุกรูปแบบที่ต้องใช้กำลังทหารและกึ่งทหารเข้าทำการรบ ด้วยวิธีการรบตามแบบ (Conventional Warfare) และการสงครามพิเศษ (Special Warfare)

๒. ภัยคุกคามที่ไม่ใช่ทหาร คือ รูปแบบของภัยคุกคามที่ไม่ใช่ทหาร ซึ่งต้องใช้พลังอำนาจของชาติในทุกด้านเพื่อรักษาความมั่นคงของรัฐ ให้รอดพ้นจากภัยคุกคามทุกรูปแบบตั้งแต่ในยามปกติ ได้แก่ ด้านการก่อการร้าย ด้านเศรษฐกิจ ด้านพลังงาน ด้านอาชญากรรมข้ามชาติ และด้านเทคโนโลยี

๓. ภัยคุกคามที่เป็นสาธารณะภัยขนาดใหญ่และภัยพิบัติธรรมชาติ คือ ภัยที่เกิดขึ้นโดยอุบัติเหตุ หรือโดยบังเอิญ ทั้งที่เกิดขึ้นโดยธรรมชาติ หรือโดยน้ำมือมนุษย์ ที่ทำให้เกิดความ เสียหายโดยรวมต่อระบบสาธารณูปโภคพื้นฐานต่างๆ ของสังคม ทำให้หยุดชะงักหรือถูกตัดขาดเป็นเวลานาน เช่น โรงไฟฟ้าพลังงานนิวคลียร์ระเบิด โรคซาร์ระบาด หรือสึนามิ เป็นต้น

เทคโนโลยีการรักษาความปลอดภัย

ในปัจจุบันเทคโนโลยีระบบรักษาความปลอดภัย (Security SystemTechnology) นั้นเป็นอีกระบบหนึ่งที่ได้รับความนิยมมากไม่ว่าเป็นกลุ่มสำนักงานสถานที่ราชการที่พักอาศัยในคอนโดมิเนียมหรือหมู่บ้านจัดสรร โรงพยาบาล โรงเรียนมหาวิทยาลัย โรงงาน หรือแม้แต่พื้นที่สาธารณะ เช่น รถไฟฟ้าและรถไฟใต้ดินทั้งนี้คงเป็นเพราะลักษณะการใช้งานของระบบรักษาความปลอดภัยนั้นสามารถเชื่อมต่อเข้ากับเครือข่ายคอมพิวเตอร์อันทันสมัย ซึ่งจากคุณสมบัติเด่นๆ ดังกล่าวทำให้ระบบรักษาความปลอดภัยได้รับความไว้วางใจจากหน่วยงานต่างๆ ให้สอดส่องดูแลความเรียบร้อยทดแทนการเสียค่าใช้จ่ายในการจ้างพนักงานเพื่อมาเดินตรวจตรา ซึ่งทำให้มีความรู้สึกเสมือนมีคนดูแลความปลอดภัยตลอด ๒๔ ชั่วโมง

ประโยชน์ที่ได้รับอย่างเห็นได้ชัดของระบบรักษาความปลอดภัยนั้น มีอยู่หลายประการด้วยกัน อาทิเช่น

๑. ป้องกันอันตรายต่อชีวิตหรือบุคคลในพื้นที่

๒. ป้องกันความเสียหาย สูญหาย ให้กับทรัพย์สินและของมีค่า

๓. ป้องกันการบุกรุกเข้ามาในพื้นที่ที่ต้องการควบคุม

๔. เฝ้าระวังเหตุร้ายที่อาจเกิดขึ้นในพื้นที่

๕. ตรวจจับผู้ต้องสงสัยหรือผู้กระทำความผิด

ดังนั้นระบบรักษาความปลอดภัยที่ดีจึงควรจะต้องตอบสนองความต้องการของผู้ใช้งานได้เป็นอย่างดี โดยมีการออกแบบให้ครอบคลุมพื้นที่ใช้งาน เลือกใช้อุปกรณ์ที่ได้มาตรฐานเหมาะสมกันสภาวะของการใช้งานและพื้นที่ที่ใช้งาน จะต้องมีระบบการจัดการและบริหารข้อมูลที่มีประสิทธิภาพ สะดวกในการใช้งานและสะดวกในการบำรุงรักษาระบบระบบที่เกี่ยวข้องกับงานเทคโนโลยีรักษาความปลอดภัยในปัจจุบัน อาทิ

๑. ระบบกล้องโทรทัศน์วงจรปิด (CCTV/IP System)

๒. ระบบควบคุมการเข้า - ออกภายในสถานที่ (Access Control System)

๓. ระบบเสียงประกาศ (Public Address System)

๔. ระบบแจ้งเตือนการบุกรุก (Inrusion System) เพื่อการตรวจสอบและป้องกัน (Detection and Prevention)

๕. ระบบป้องกันอัคคีภัย (Fire Alarm System)

๖. ระบบ Prism Skylabs ซึ่งหมายถึงใส่สมองเข้าไปให้กับกล้องวงจรปิด เพื่อใช้ในการคิดวิเคราะห์และประมวลผลต่อยอดจากเรื่องรักษาความปลอดภัยไปสู่เรื่องอื่นๆ

๗. ระบบจัดการความปลอดภัยแบบบูรณาการสำหรับชุมชนเมือง (City Surveillance Solution)

งานวิจัยและวรรณกรรมที่เกี่ยวข้อง

งานวิจัยและวรรณกรรมที่เกี่ยวข้องในการวิจัยนี้มีดังต่อไปนี้

วัชราภรณ์ พิมพา และคณะ (๒๕๔๘)ได้ศึกษาวิจัยเรื่อง การพัฒนาระบบการรักษาความปลอดภัยโดยการประยุกต์ใช้เทคโนโลยีสารสนเทศภูมิศาสตร์ของค่ายสมเด็จพระเอกาทศรถ จังหวัดพิษณุโลก โดยมีวัตถุประสงค์เพื่อสร้างระบบการจัดการฐานข้อมูล และสร้างมุมมองของสารสนเทศภูมิศาสตร์ที่มีส่วนแสดงแผนที่ค่ายสมเด็จพระเอกาทศรถซึ่งสามารถนำไปใช้ประโยชน์ในการวางระบบการรักษาความปลอดภัยภายในค่ายทหาร ได้อย่างถูกต้อง รวดเร็วและมี

ประสิทธิภาพ รวมทั้งเพื่อเป็นต้นแบบของระบบการรักษาความปลอดภัยภายในค่ายทหารอื่นๆ วิธีการดำเนินงานเริ่มจากการศึกษา วิเคราะห์ปัญหา ออกแบบ พัฒนา ทดสอบ และประเมินผลของระบบงาน ระบบนี้ถูกพัฒนาโดยใช้โปรแกรมในรูปแบบของ Web Application โดยใช้ Apache เป็น Web Server ใช้ ArcIMS เป็น Internet Map Server และใช้ภาษา JSP และ PHP ในการติดต่อกับฐานข้อมูล MySQL ผ่านทาง Web Browser ผลจากการศึกษาวิจัยพบว่าผู้ใช้งานและผู้บริหารมีระดับความพึงพอใจอยู่ในระดับดีระบบนี้สามารถสนับสนุนการปฏิบัติงานทางด้านการรักษาความปลอดภัยภายในค่ายทหารได้เป็นอย่างดีและมีประสิทธิภาพ

ชัยเสฏฐ์ พรหมศรี (๒๕๕๔)ได้เขียนรายงานการวิจัย เรื่อง “การพัฒนารูปแบบจิตสำนึกทางด้านการรักษาความปลอดภัยและแผนการฝึกอบรมพัฒนาสำหรับองค์การรักษาความปลอดภัย : กรณีศึกษาของสำนักข่าวกรองแห่งชาติ พ.ศ.๒๕๕๓”โดยพบว่า จิตสำนึกทางด้านการรักษาความปลอดภัย หมายถึง “ความรู้สึกนึกคิดของแต่ละบุคคลที่มีต่อความสำคัญทางด้านการรักษาความปลอดภัยที่ครอบคลุมเรื่องบุคคล ข้อมูลข่าวสาร สถานที่ ถูกสั่งสมมาจากการถ่ายทอดการเรียนรู้ การฝึกอบรม และประสบการณ์ เพื่อดำเนินการในการป้องกันหรือรับมือจากสถานการณ์ที่เป็นภยันตรายได้โดยอัตโนมัติ โดยไม่ต้องมีใครมาบังคับ”เพราะการที่บุคคลใดจะแสดงออกซึ่งจิตที่ระแวดระวังภยันตรายที่อาจเกิดขึ้นและส่งผลกระทบต่อการรักษาความปลอดภัยได้นั้น บุคคลนั้นต้องมีความรู้ ความเข้าใจ และเห็นถึงความสำคัญและผลลัพธ์ของการขาดการรักษาความปลอดภัยเป็นอย่างดี ซึ่งองค์ประกอบที่สำคัญของการสร้างจิตสำนึกทางด้านการรักษาความปลอดภัยมีองค์ประกอบที่สำคัญ ๑๐ องค์ประกอบ ได้แก่

๑. การจัดกิจกรรมที่เกี่ยวข้องกับการรักษาความปลอดภัย (Security Activity) ทั้งภายในองค์กรและโดยความร่วมมือกับหน่วยงานภายนอก เพื่อกระตุ้นบุคลากรให้เห็นถึงความสำคัญของการรักษาความปลอดภัยอย่างสม่ำเสมอ

๒. การสร้างความรู้เกี่ยวกับการรักษาความปลอดภัย (Knowledge Development) โดยการให้ความรู้ความเข้าใจและความชัดเจน และแนวทางปฏิบัติงานทางด้านการรักษาความปลอดภัย รวมทั้งการปลูกฝังค่านิยม การถ่ายทอดประสบการณ์ แนวปฏิบัติที่พึงปรารถนาจากผู้บังคับบัญชาและจากรุ่นพี่สู่รุ่นน้องภายในหน่วยงาน

๓. บทบาทผู้นำต่อการพัฒนาจิตสำนึกในการรักษาความปลอดภัย (Leader Roles) โดยผู้นำหรือผู้บริหารทุกระดับขององค์กรแสดงตนเป็นแบบอย่างและให้การเอาใจใส่ในการพัฒนาจิตสำนึกทางด้านการรักษาความปลอดภัย รวมทั้งกำหนดนโยบายและแนวทางปฏิบัติที่ชัดเจนต่อการพัฒนาจิตสำนึกทางด้านการรักษาความปลอดภัย

๔. การสร้างความผูกพันเพื่อการอยู่ร่วมกันของบุคลากรในองค์กร (Commitment) เพราะเมื่อใดที่บุคลากรมีความผูกพัน ย่อมมีความรู้สึกหวงแหนในชีวิตและทรัพย์สินขององค์กร มีความระแวดระวังภยันตรายที่อาจเกิดขึ้นแก่องค์กร

๕. การประเมินผลการปฏิบัติ (Performance Appraisal) เพื่อเป็นการติดตามผลการปฏิบัติงานของบุคลากรและทำการประเมินพฤติกรรมที่สะท้อนให้เห็นถึงจิตสำนึกทางด้านการรักษาความปลอดภัยเพื่อนำไปสู่การพัฒนาและปรับปรุงอย่างต่อเนื่อง

๖. การประชาสัมพันธ์เพื่อสร้างจิตสำนึกทางด้านการรักษาความปลอดภัย (Public Relations) โดยการจัดทำคำขวัญและป้ายเตือนที่แสดงให้เห็นความสำคัญของการมีจิตสำนึกทางด้านการรักษาความปลอดภัยติดตามบริเวณต่างๆ ในองค์กร เพื่อให้บุคลากรไม่ลืมที่จะปฏิบัติและพยายามเตือนตนเองอยู่เสมอว่าต้องปฏิบัติตนอย่างไร

๗. การปรับปรุงสภาพแวดล้อมในการทำงาน (EnvironmentalImprovement) ให้เหมาะสมกับมาตรการการรักษาความปลอดภัย ช่วยกระตุ้นการสร้างจิตสำนึกทางด้านการรักษาความปลอดภัยได้

๘. การนำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ (Information Technology SystemImplementation) โดยการเผยแพร่ข้อมูลข่าวสารและกรณีศึกษาที่เกี่ยวข้องกับการรักษาความปลอดภัยผ่านระบบอินทราเน็ตหรืออินเตอร์เน็ต เพื่อช่วยกระตุ้นการพัฒนาจิตสำนึกด้านการรักษาความปลอดภัยของบุคลากร

๙. การสร้างสถานการณ์จำลองที่เป็นวิกฤต (CrisisSimulation) ได้แก่ สถานการณ์จำลองด้านการก่อวินาศกรรม การจลาจลหรือการโจรกรรม และการซักซ้อมแนวทางปฏิบัติตนในยามวิกฤตหรือเมื่อเผชิญภัย สามารถช่วยกระตุ้นการสร้างจิตสำนึกด้านการรักษาความปลอดภัยของบุคลากรได้

๑๐. การสร้างแรงจูงใจแก่บุคลากรเพื่อการสร้างจิตสำนึก (Motivation) ซึ่งถือเป็นหัวใจสำคัญของงานด้านการรักษาความปลอดภัยเนื่องจากการทำให้บุคลากรรู้สึกว่าตนเองมีคุณค่าต่อองค์กร เป็นแนวทางที่สำคัญที่ช่วยลดแรงจูงใจในการประพฤติปฏิบัติตนอันนำไปสู่ปัญหาทางด้านการรักษาความปลอดภัย

นิวัติ เนียมพลอย (๒๐๑๒) ได้กล่าวโดยสรุปตามรายงานของ Joint Publication 3-13.3, Operations Security, 4 January 2012 ว่าในสงครามยุคใหม่ นักการทหารพยายามคิดหาวิธีในการเอาชนะข้าศึกโดยการเข้าไปสร้างข้อจำกัดในการใช้ข้อมูลข่าวสารของฝ่ายข้าศึกการรักษาความปลอดภัยในการปฏิบัติการ (Operation Security : OPSEC) โดยการปฏิบัติการทางทหารด้านต่างๆ หลายรูปแบบ เช่น การสงครามด้านบัญชาการและควบคุม (Command and Control Warfare :

C2W) การปฏิบัติการข่าวสาร (Information Operations : IO) และได้รับผลกระทบต่อมาตรการรักษาความปลอดภัยอื่นๆ ได้แก่ มาตรการรักษาความปลอดภัยการติดต่อสื่อสาร (Communication Security: COMSEC), มาตรการต่อต้านข่าวกรอง (Counter-Intelligence) มาตรการรักษาความปลอดภัยข้อมูลข่าวสาร (Information Security : INFOSEC) การรักษาความปลอดภัยสัญญาณ (Signal Security : SIGSEC) และการรักษาความปลอดภัยการรับ-ส่งสัญญาณ (Transmission Security : TRANSEC) การรักษาความปลอดภัยในการปฏิบัติการนั้นเป็นมาตรการหรือวิธีการอย่างเป็นระบบที่ใช้ในการระบุ (identify) ควบคุม (Control) และป้องกัน (Protect) หลักฐานทั่วไปที่ไม่ระบุชั้นความลับที่เกี่ยวข้องหรือเชื่อมต่อกับการปฏิบัติการหรือกิจกรรมต่างๆ ที่สำคัญหรือละเอียดอ่อน ซึ่งแตกต่างกับมาตรการรักษาความปลอดภัยทั่วไปที่เน้นในการรักษาความปลอดภัยเฉพาะข้อมูลข่าวสารที่มีชั้นความลับกระบวนการสำหรับการรักษาความปลอดภัยในการปฏิบัติการจะปฏิบัติควบคู่กับขั้นตอนในการวางแผนร่วมเพื่อนำเสนอข้อมูลที่ต้องการในการระบุไว้ในเอกสารหรือคำสั่งส่วนการรักษาความปลอดภัยในการปฏิบัติการ (OPSEC Section) โดยจะประสานงานอย่างใกล้ชิดกับการวางแผนการปฏิบัติการข้อมูลข่าวสาร (IO) กระบวนการรักษาความปลอดภัยในการปฏิบัติการ (OPSEC Process) ประกอบด้วย ๕ ขั้นตอน ได้แก่ ๑) การระบุข้อมูลวิกฤต (Identification of Critical Information) ๒) การวิเคราะห์ภัยคุกคาม (Analysis of Threats) ๓) การวิเคราะห์จุดอ่อน (Analysis of Vulnerabilities) ๔) การประเมินความเสี่ยง (Assessment of Risk) และ ๕) การประยุกต์ใช้มาตรการการปฏิบัติรักษาความปลอดภัยที่เหมาะสม (Application of Appropriate Operations Security Measures)

ส่วนปัจจัยในการรักษาความปลอดภัยในการปฏิบัติการ (OPSEC Factors) ที่ต้องพิจารณาในการดำเนินตามแผนรักษาความปลอดภัยในการปฏิบัติการ มีดังต่อไปนี้

๑) ผู้บังคับบัญชา มีบทบาทสำคัญหลักในการวางแผน คำแนะนำในการวางแผนควรมาจาก คำแนะนำในการปฏิบัติการข่าวสาร (IO) ของผู้บังคับบัญชา เพื่อให้มั่นใจว่า การรักษาความปลอดภัยในการปฏิบัติการจะถูนำไปพิจารณาในการพัฒนาหนทางปฏิบัติ (COA) ของฝ่ายเรา

๒) กลุ่มวางแผนยุทธการ (J-3 Operations Planners) มีหน้าที่วางแผนการรักษาความปลอดภัยในการปฏิบัติการ (เนื่องจาก OPSEC เป็นงานด้านยุทธการ ไม่ใช่งานด้านการรักษาความปลอดภัย) โดยได้รับความช่วยเหลือจากนายทหาร Program OPSEC และฝ่ายเสนาธิการอื่นๆ ที่เกี่ยวข้อง การสนับสนุนด้านข่าวกรองเป็นสิ่งสำคัญในการพิจารณาภัยคุกคามต่อการปฏิบัติการของฝ่ายเรา การประเมินจุดอ่อนของฝ่ายเรา การพิจารณาขีดความสามารถของข้าศึก และการพยากรณ์แนวทางการปฏิบัติต่างๆ ของข้าศึก

๓) กองกำลังร่วมผสม ควรจัดตั้งชุดปฏิบัติการข่าวสาร (IO) อย่างเต็มรูปแบบ ฝ่ายเสนาธิการร่วม (รวมถึงชุดปฏิบัติการข่าวสาร) พัฒนาและเผยแพร่คำแนะนำและแผนการปฏิบัติด้านข้อมูลข่าวสารที่มีรายระเอียดในการวางแผนและการดำเนินการไปยังหน่วยรอง หน่วยสนับสนุนและหน่วยเกี่ยวข้อง นายทหาร Program OPSEC มีบทบาทสำคัญในชุดปฏิบัติการข่าวสาร (IO) ในการประสานงานด้านการบังคับบัญชาในพื้นที่การรบ หรือกิจกรรมด้านการรักษาความปลอดภัยในการปฏิบัติการ รวมทั้งระบบติดต่อสื่อสาร และการเฝ้าฟังการรักษาความปลอดภัยของการติดต่อสื่อสาร

๔) การวางแผน ต้องมุ่งเน้นไปที่การระบุ และการป้องกันข้อมูลวิกฤต เนื่องจากการปฏิเสธข้อมูลการปฏิบัติการ หรือกิจกรรมทั้งหมดของฝ่ายเรานั้นไม่คุ้มค่าในการดำเนินการ หรือเป็นสิ่งที่ไปไม่ได้

๕) วัตถุประสงค์สำคัญสูงสุดของการรักษาความปลอดภัยในการปฏิบัติการ คือการเพิ่มประสิทธิภาพของภารกิจ โดยการป้องกันไม่ให้ฝ่ายข้าศึกล่วงรู้ความตั้งใจ หรือขีดความสามารถของฝ่ายเรา การรักษาความปลอดภัยในการปฏิบัติการจะช่วยลดความสูญเสียต่อกำลังฝ่ายเรา และเพิ่มโอกาสในการบรรลุเป้าหมายของภารกิจ

๖) การรักษาความปลอดภัยในการปฏิบัติการ เป็นปัจจัยที่ถูกพิจารณาระหว่างการพัฒนาและเลือกหนทางปฏิบัติ (COA) ของฝ่ายเรา หนทางทางปฏิบัติที่แตกต่างกันจะสร้างตัวบ่งชี้ในจำนวนที่ไม่เท่ากัน และมีความยาก-ง่ายไม่เท่ากันในการจัดการกับตัวบ่งชี้โดยการใช้มาตรการรักษาความปลอดภัยในการปฏิบัติการ ขึ้นอยู่กับความสำคัญในการรักษาความปลอดภัยของการบรรลุภารกิจ

๗) การวางแผนรักษาความปลอดภัยในการปฏิบัติการ เป็นกระบวนการที่ต้องทำอย่างต่อเนื่องระหว่างปฏิบัติการในทุกขั้นตอน ความสำเร็จหรือความล้มเหลวของมาตรการรักษาความปลอดภัยนี้จะถูกนำมาประเมินค่าบนพื้นฐานของประสิทธิภาพของมาตรการต่างๆ และแผนการปฏิบัติที่ได้รับการปรับปรุงแล้ว โดยมีแหล่งหลักในการให้ข้อมูล ได้แก่ องค์กรด้านข่าวกรองและต่อต้านข่าวกรองของฝ่ายเรา การติดตามการรักษาความปลอดภัยการติดต่อสื่อสาร (Communication Security : COMSEC) และ การประเมินการรักษาความปลอดภัยในการปฏิบัติการ

๘) นายทหารกิจการพลเรือน มีส่วนร่วมในการวางแผนการรักษาความปลอดภัยในการปฏิบัติการ โดยการประเมินผลกระทบเชิงลบที่เป็นไปได้ของสื่อมวลชน และข้อมูลบนสื่อสิ่งพิมพ์ต่างๆ มาตรการรักษาความปลอดภัยและกฎพื้นฐานของการกิจการพลเรือนในการลดผลกระทบนั้น นายทหารกิจการพลเรือนต้องทำให้มั่นใจว่า การรวมการ การอนุญาต การเผยแพร่ของสื่อมวลชน และอำนาจในการถ่ายทอดสัญญาณภาพต่างๆ (ทั้งโดยวิธีผ่านทางระบบอินเตอร์เน็ต

และช่องทางการสื่อสารอื่นๆ) อยู่ภายใต้มาตรการรักษาความปลอดภัยในการปฏิบัติการ และอยู่ในการติดตามของนายทหารกิจการพลเรือน

๙) การรักษาความปลอดภัยในการปฏิบัติการ จะพิจารณาถึงการรวม การประสานงาน การขจัดข้อขัดแย้ง และการประสานสอดคล้องของกิจกรรมทางข้อมูลนานาชาติภายในพื้นที่ปฏิบัติการร่วมของกองกำลังร่วมผสม

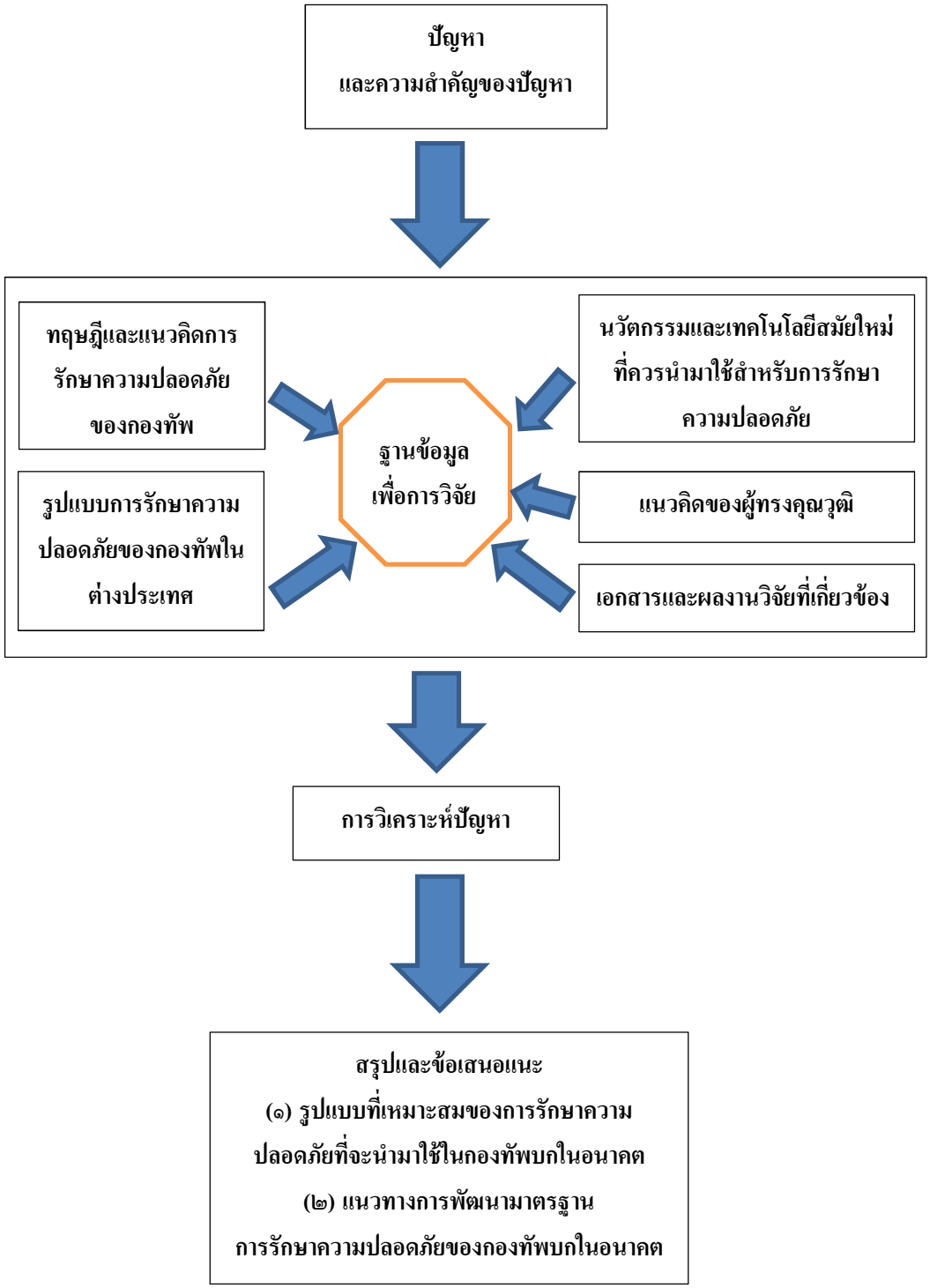
๑๐) การสิ้นสุดของมาตรการรักษาความปลอดภัยในการปฏิบัติ ควรระบุไว้ในแผนการรักษาความปลอดภัย เพื่อป้องกันฝ่ายข้าศึกจากการพัฒนามาตรการต่อต้าน ซึ่งควรมีข้อแนะนำวิธีในการป้องกันเป้าหมายของปฏิบัติการที่เกิดขึ้นก่อนหน้านี้และผลประโยชน์ของฝ่ายที่สาม จากการล่วงรู้ข้อมูลวิกฤตของฝ่ายข้าศึกจากผลการปฏิบัติที่ผ่านมาในอดีต

ดังนั้นจึงเป็นสิ่งจำเป็นที่ทหารต้องทำความเข้าใจและสามารถนำทฤษฎีการรักษาความปลอดภัยในการปฏิบัติการไปประยุกต์ใช้ในการปฏิบัติงานทั้งในภาวะปกติและภาวะสงครามได้ การรักษาความปลอดภัยในการปฏิบัติการจึงเป็นกระบวนการในการระบุข้อมูลข่าวสารวิกฤติใดที่ฝ่ายเราสามารถล่วงรู้มาจากฝ่ายข้าศึก แล้วนำมาตีความให้เกิดประโยชน์ต่อฝ่ายเราตลอดจนนำไปสู่การเลือกใช้มาตรการที่เหมาะสมในการปฏิบัติจนสามารถกำจัด หรือลดทอนขีดความสามารถของข้าศึกในการค้นหาข้อมูลข่าวสารวิกฤตของฝ่ายเราได้

กรอบความคิดของการวิจัย

จากข้อมูลที่กล่าวมาข้างต้นสามารถยืนยันได้ว่าควรมีการศึกษาวิจัยเกี่ยวกับแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต ทั้งนี้เพื่อนำข้อมูลการวิจัยไปใช้เป็นข้อมูลสำคัญในการสร้างรูปแบบที่เหมาะสมกับการรักษาความปลอดภัยของกองทัพบกไทย รวมถึงเพื่อสร้างความมั่นคงให้กับกองทัพไทยและหน่วยงานทางด้านความมั่นคงอื่นๆ ดังนั้นเพื่อให้สามารถนำเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคตได้อย่างมีประสิทธิภาพและมีประสิทธิผล ผู้วิจัยจึงได้กำหนดกรอบความคิดของการวิจัย (Conceptual Framework) ดังแผนภาพที่ ๒ - ๑

แผนภาพที่ ๒ - ๑ กรอบความคิดของการวิจัย



สรุป

การวิจัยเพื่อหาแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต โดยมีเอกสารและงานวิจัยที่เกี่ยวข้อง ได้แก่ รูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน รูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ งานวิจัยและวรรณกรรมที่เกี่ยวข้องเพื่อนำไปสร้างกรอบความคิดของการวิจัย

บทนี้นำเสนอข้อมูลเบื้องต้นรวมถึงบทวิเคราะห์จากการศึกษาและค้นคว้าเอกสารเกี่ยวกับความเป็นมาของการรักษาความปลอดภัยเกี่ยวกับสถานที่ มาตรการการรักษาความปลอดภัยสถานที่แนวคิดเกี่ยวกับการรักษาความปลอดภัยแห่งชาติ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ทฤษฎีภัยคุกคามและภัยคุกคามรูปแบบใหม่ เทคโนโลยีการรักษาความปลอดภัยงานวิจัยและวรรณกรรมที่เกี่ยวข้องเอกสารทางวิชาการ เอกสารทางราชการของหน่วยงานที่เกี่ยวข้อง บทความวิชาการต่างๆ การสำรวจข้อมูลเชิงพื้นที่ รวมทั้งเอกสารประกอบการบรรยายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลที่มีความหลากหลายเพื่อนำมาประกอบการดำเนินการวิจัยเชิงคุณภาพเพื่อหาแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคตต่อไป บทต่อไปจะนำเสนอเกี่ยวกับรูปแบบการรักษาความปลอดภัยของประเทศสหรัฐอเมริกา รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคเอเชีย และรูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคอื่นๆ โดยจะนำเสนอตามลำดับต่อไป

บทที่ ๓
รูปแบบการรักษาความปลอดภัยในต่างประเทศ

บทนี้จะเป็นการศึกษาเปรียบเทียบรูปแบบการรักษาความปลอดภัยในประเด็นต่างๆ ดังต่อไปนี้

๑. รูปแบบการรักษาความปลอดภัยของประเทศสหรัฐอเมริกา
๒. รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคเอเชีย
๓. รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคอื่นๆ
๔. เปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ
๕. สรุป

รูปแบบการรักษาความปลอดภัยของประเทศสหรัฐอเมริกา

รูปแบบการรักษาความปลอดภัยของประเทศสหรัฐอเมริกาซึ่งถือได้ว่าเป็นประเทศต้นแบบของกองทัพยุคใหม่ แต่อย่างไรก็ตามระบบการรักษาความปลอดภัยและเทคโนโลยีบางอย่างนั้นถูกปกปิดเนื่องด้วยเหตุผลทางความปลอดภัยจากการศึกษาเอกสาร ข้อมูลและงานวิจัยที่เกี่ยวข้องผู้วิจัยพบว่าการรักษาความปลอดภัยของประเทศสหรัฐอเมริกา มีการกำหนดเป็นนโยบาย โดย Military Police : Security of Unclassified Army Property ซึ่งกำหนดเป็นความปลอดภัยขั้นต่ำ และหากเป็นสถานที่ที่มีความต้องการความปลอดภัยสูงมาก สามารถดำเนินการเพิ่มเติมได้เองตามนโยบายของแต่ละชั้นความลับที่ได้รับมอบหมายจากผู้บังคับบัญชาได้ โดย US Military Police มีการแบ่งออกเป็นการรักษาความปลอดภัยสำหรับสถานที่ ทรัพย์สิน บุคคล และยานพาหนะ อย่างไรก็ตามงานวิจัยชิ้นนี้มุ่งเน้นการศึกษาความปลอดภัยด้านสถานที่ที่เหมาะสมในอนาคต ผู้วิจัยจึงขอสรุปข้อตกลงเบื้องต้นโดยแบ่งตามรูปแบบการรักษาความปลอดภัยตามระดับของ Security of Unclassified Army Property (Military Police, 1993) ดังนี้

๑. มาตรการการป้องกันทางกายภาพขั้นตอนการรักษาความปลอดภัยและการต่อต้านการก่อการร้ายสำหรับประเภทของทรัพย์สินที่กำหนดไว้ที่สถานที่ปฏิบัติงานนอกชายฝั่งของกองทัพสหรัฐอเมริกาหรือสถานที่ต่างๆ มีการแบ่งหมวดหมู่ตามระดับความเสี่ยงที่กำหนดโดยใช้ขั้นตอนการวิเคราะห์ความเสี่ยงในนโยบาย DA Pam ๑๕๐-๕๑ โดยแบ่งเป็น ๓ ระดับขึ้นอยู่กับการ

ประเมินและการวิเคราะห์ของผู้เกี่ยวข้องที่ได้รับมอบหมายจากผู้บังคับบัญชา หากระดับความเสี่ยงเป็นขั้นต่ำ การป้องกันและการรักษาความปลอดภัยจะถือว่าเป็นขั้นต่ำเช่นกัน การป้องกันร่างกายและการรักษาความปลอดภัยมาตรการต่างๆ จะขึ้นอยู่กับการประเมินสถานการณ์และการวิเคราะห์ความเสี่ยง

๒. มาตรการรักษาความปลอดภัยขั้นต่ำที่จำเป็นสำหรับการดำเนินการต่อประเภทของทรัพย์สิน แม้ว่าประเภทของทรัพย์สินของกองทัพเหล่านี้ไม่จำเป็นต้องมีการวิเคราะห์ความเสี่ยงโดยใช้ DA Pam ๑๙๐-๕๑ ควรใช้หลักการวิเคราะห์ความเสี่ยงและพิจารณาปัจจัยเสี่ยงผู้บังคับบัญชามามาร่วมด้วย

๓. มาตรการรักษาความปลอดภัยที่ต้องใช้รั้วรอบที่ตั้ง กำหนดให้มีความสูง (๖ หรือ ๗ ฟุต) และมีความสามารถในการป้องกันที่ดีหรือมีคุณสมบัติอื่นๆ จะขึ้นอยู่กับการตัดสินของผู้บังคับบัญชาการติดตั้ง และต้องดำเนินการติดตั้งตามคำแนะนำที่พบได้ใน Field Manual (FM) ๑๙-๓๐ เว้นแต่เป็นไปตามข้อกำหนดของกองกำลังวิศวกรสหรัฐอเมริกาเลขที่ ๔๐-๑๖-๐๘, Type FE

๔. หากมีข้อโต้แย้งหรือไม่สามารถดำเนินการได้ตามมาตรฐานต่างๆ ที่กำหนดให้ทำหนังสือระบุเป็นลายลักษณ์อักษร พร้อมระบุมาตรการทดแทน โดยหนังสือจะถูกส่งไปตามลำดับชั้นบังคับบัญชาจาก MACOM ไปยัง HQDA (DAMO-ODL-S) เพื่ออนุมัติต่อไป

รูปแบบการรักษาความปลอดภัยแบ่งตามทรัพย์สินที่ถูกเก็บในแต่ละสถานที่และระดับความเสี่ยงตามข้อกำหนดของ Security of Unclassified Army Property

๑. สถานที่เก็บอากาศยานและชิ้นส่วนของกองทัพ (Aircraft and Components at Army Aviation Facilities)

๑.๑ ความเสี่ยงระดับ ๑

๑.๑.๑ สถานที่เก็บอากาศยานของกองทัพ จะต้องผ่านการรับรองด้านความปลอดภัยจากผู้ผลิตหรือผู้ได้รับใบอนุญาตด้านความปลอดภัย และชิ้นส่วนอุปกรณ์ต่างๆ จะต้องมีการรักษาความปลอดภัยโดยต้องล็อคประตูเสมอเมื่อไม่ใช้งาน อากาศยานที่อยู่ระหว่างการซ่อมบำรุงรักษา จะต้องมีเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้นที่ได้รับอนุญาตให้เข้าส่วนการซ่อมบำรุง

๑.๑.๒ สถานที่เก็บอากาศยานของกองทัพ จะต้องมีการควบคุมกุญแจสำหรับตู้นิรภัยที่เก็บกุญแจอากาศยานอุปกรณ์หรือตัวจุดระเบิดเครื่องยนต์โดยต้องมีการควบคุม ด้วยการใช้เจ้าหน้าที่เฝ้าระวัง ระบบเทคโนโลยีและการลาดตระเวน กุญแจอากาศยานจะไม่ถูกนำมาเก็บรักษาส่วนบุคคล และทำซ้ำเด็ดขาด

๑.๑.๓ หากอากาศยานยังไม่ได้ใช้งาน ชิ้นส่วน อุปกรณ์ของอากาศยาน เครื่องบิน และอุปกรณ์ของนักบินรวมถึงลูกเรือจะถูกเก็บไว้ในโรงเก็บอากาศยาน หรือโครงสร้าง

อื่นๆ ที่ปลอดภัยที่สุด ถ้าไม่มีพื้นที่เก็บสัมภาระเพียงพออุปกรณ์นี้อาจจัดเก็บไว้ ณ สถานที่ที่อยู่ใกล้กับสถานที่เก็บอากาศยานของกองทัพ

๑.๑.๔ เมื่อสถานที่เก็บอากาศยานของกองทัพ ไม่ได้ทำการจอดเครื่องบินหรืออากาศยาน จะต้องมีการเตรียมพร้อมการใช้งานไว้เสมอ พร้อมคงการรักษาความปลอดภัยไว้ตลอดเวลา

๑.๒ ความเสี่ยงระดับ ๒

๑.๒.๑ มาตรการทั้งหมดที่จำเป็นสำหรับความเสี่ยงระดับ ๑ จะต้องดำเนินการ

๑.๒.๒ สถานที่เก็บอากาศยานจะได้รับการคุ้มครองโดยรั้วรอบขอบชิดพร้อมเจ้าหน้าที่รักษาความปลอดภัย

๑.๓ ความเสี่ยงระดับ ๓

๑.๓.๑ มาตรการทั้งหมดสำหรับความเสี่ยงระดับ ๑ และ ๒ จะต้องดำเนินการ

๑.๓.๒ สถานที่เก็บอากาศยานจะต้องมีแสงสว่างในเวลากลางคืนทั้งภายในและภายนอกเพื่อให้เจ้าหน้าที่รักษาความปลอดภัยสามารถตรวจจับผู้บุกรุกได้

๑.๓.๓ ควรเพิ่มเจ้าหน้าที่รักษาความปลอดภัยทั้งระยะไกลและระยะใกล้รอบ พื้นที่สถานที่เก็บอากาศยาน

๒. สถานที่เก็บอากาศยานและชิ้นส่วนของกองทัพ ที่ไม่อยู่ในสถานที่ของกองทัพ (Aircraft and componentsnot at Army aviation facilities) สถานที่เก็บอากาศยานและชิ้นส่วนของกองทัพ ที่ไม่อยู่ในสถานที่ของกองทัพจะมีการปฏิบัติตามข้อกำหนดด้านความรับผิดชอบของทรัพย์สินที่ระบุไว้ในหัวข้อสถานที่เก็บอากาศยานและชิ้นส่วนของกองทัพ (Aircraft and Components at Army Aviation Facilities) ตามข้อบังคับมาตรการป้องกันทางกายภาพความเสี่ยงระดับ ๑ และต้องดำเนินการดังต่อไปนี้

๒.๑ การจอดอากาศยาน จะต้องจอดที่สนามบินของรัฐบาลหรือสนามบินพลเรือนที่มีการรักษาความปลอดภัยตามมาตราฐานสากล หากสนามบินดังกล่าวไม่มีการรักษาความปลอดภัยตามมาตรฐานและนักบินหรือลูกเรือไม่สามารถอยู่กับอากาศยานได้ จะต้องแจ้งผู้บัญชาการทราบ โดยอาจใช้สถานที่ที่เป็นหน่วยความมั่นคงอื่นๆ ในท้องถิ่นเป็นสถานที่จอดเครื่องบินได้ แต่นักบินหรือลูกเรือจะต้องทำการเฝ้าระวังตลอดระยะเวลาจอด

๒.๒ เครื่องบินจะต้องได้รับการตรวจสอบอย่างละเอียดอย่างน้อยหนึ่งครั้งต่อวันโดยนักบินหรือลูกเรือ เพื่อป้องกันการดัดแปลง การก่อวินาศกรรมและความเสียหาย

๓. สถานที่เก็บยานพาหนะ ชิ้นส่วน ส่วนประกอบและระบบอาวุธ (Vehicles and Carriage–Mounted/Towed Weapons Systems and Components)

๓.๑ ความเสี่ยงระดับ ๑

๓.๑.๑ สถานที่เก็บยานพาหนะที่ออกแบบเพื่อการพาณิชย์ จะต้องทำการเปิดล็อคประตูสถานที่ รวมถึงล็อครถตามรูปแบบที่ผู้ผลิตกำหนด

๓.๑.๒ สถานที่เก็บยานพาหนะทางยุทธวิธีและยานพาหนะชุด M880 จะต้องทำการตรึงด้วยโซ่และกุญแจที่ได้รับอนุมัติ ชิ้นส่วน อาทิยางสำรองและถังน้ำมันเชื้อเพลิงควรได้รับการรับรองความปลอดภัยด้วยอุปกรณ์ล็อคที่ได้มาตรฐานของผู้ผลิต หรือใช้กุญแจคล้องที่ให้มาพร้อมกับยานพาหนะ ทั้งนี้ต้องปฏิบัติตามมาตรการด้านความปลอดภัยอื่นๆ ที่กำหนดรวมถึงกฎระเบียบปฏิบัติที่บังคับใช้อยู่

๓.๑.๓ สถานที่เก็บยานพาหนะทางการรบอื่นๆ อาทิ M๑๐๐๘, ๑๐๐๙, และ ๑๐๑๐ series รวมถึงยานพาหนะเพื่อขนส่ง (CUCV) จะต้องทำการตรึงด้วยโซ่และกุญแจที่ได้รับอนุมัติ และยานพาหนะดังกล่าวจะต้องถูกจัดเก็บไว้ในสถานที่ที่มีโครงสร้างแข็งแรงปลอดภัย

๓.๑.๔ สถานที่จัดเก็บอุปกรณ์วัสดุ อะไหล่ และยานพาหนะอื่น ๆ ของกองทัพที่ไม่สามารถดำเนินการตามการรักษาความปลอดภัยตามที่ระบุไว้ในข้อ (๓.๑.๑) ถึง (๓.๑.๓) ข้างต้นควรมีกลไกการล็อคหรือควบคุมการเข้าถึงแบบอื่น โดยอุปกรณ์ วัสดุ อะไหล่ และยานพาหนะดังกล่าวจะต้องถูกจัดเก็บไว้ในสถานที่ที่มีโครงสร้างแข็งแรงปลอดภัย

๓.๑.๕ สถานที่เก็บยานพาหนะของกองทัพ จะต้องมีการควบคุมกุญแจหรือมีตู้นิรภัยที่เก็บกุญแจ อุปกรณ์หรือระบบอาวุธ โดยต้องมีการควบคุม ด้วยการใช้เจ้าหน้าที่เฝ้าระวังระบบเทคโนโลยีและการลาดตระเวน กุญแจจะไม่ถูกนำมาเก็บรักษาส่วนบุคคล และทำซ้ำเด็ดขาด

๓.๑.๖ สถานที่เก็บยานพาหนะจะต้องติดเครื่องหมายข้อความดังนี้ “Off Limits To Unauthorized Personnel” ณ บริเวณทางเข้า

๓.๒ ความเสี่ยงระดับ ๒

๓.๒.๑ มาตรการทั้งหมดที่จำเป็นสำหรับความเสี่ยงระดับ ๑ จะต้องดำเนินการ

๓.๒.๒ สถานที่เก็บอากาศยานจะต้องมีแสงสว่างในเวลากลางคืนทั้งภายในและภายนอกเพื่อให้เจ้าหน้าที่รักษาความปลอดภัยสามารถตรวจจับผู้บุกรุกได้

๓.๒.๓ ควรเพิ่มเจ้าหน้าที่รักษาความปลอดภัยทั้งระยะไกลและระยะใกล้รอบ พื้นที่สถานที่เก็บอากาศยาน

๓.๓ ความเสี่ยงระดับ ๓

๓.๓.๑ มาตรการทั้งหมดสำหรับความเสี่ยงระดับ ๑ และ ๒ จะต้องดำเนินการ

๓.๓.๒ จะต้องมีการสร้างแท่นยึดพื้นไว้สำหรับรถเทรลเลอร์ รถกึ่งพ่วง และอุปกรณ์พ่วงอื่นๆ หรือใช้สายเคเบิลเพื่อยึดอุปกรณ์ดังกล่าว

๓.๓.๓ ยานพาหนะที่เสี่ยงต่อการลักขโมยการยักยอกหรือความเสียหายจะถูกเก็บไว้ในโรงจอดรถที่ปลอดภัย

๔. สถานที่เก็บอุปกรณ์สื่อสารอุปกรณ์อิเล็กทรอนิกส์และอุปกรณ์ตรวจการณ์กลางคืน (Communications and Electronics Equipment and Night Vision Devices)

๔.๑ ความเสี่ยงระดับ ๑

๔.๑.๑ อุปกรณ์ต่างๆ จะต้องจัดให้มีระบบป้องกันตามแบบคู่มือของอุปกรณ์ รวมถึงให้คำนึงถึงสภาพแวดล้อมด้วย

๔.๑.๑.๑ อาคารสถานที่เก็บอุปกรณ์จะต้องถูกล็อก และต้องแยกจากสถานที่เก็บยานพาหนะ และต้องได้รับการป้องกัน โดยมีรั้วรอบขอบชิด

๔.๑.๑.๒ ต้องมีการสร้างกรงเหล็กและทำการล็อกให้แน่นหนาเพื่อเก็บอุปกรณ์ให้ปลอดภัย

๔.๑.๒.๓ ต้องมีการยึดอุปกรณ์หรือที่เก็บกับโครงสร้างอาคารที่จัดเก็บ

๔.๑.๒.๔ ติดตั้งอุปกรณ์อย่างแน่นหนา และทำการเฝ้าระวังอย่างต่อเนื่อง

๔.๑.๒ สิ่งของที่ไม่สามารถนำมาเก็บในอาคารจะต้องได้รับการป้องกันโดยอุปกรณ์ลวดหนามหรืออุปสรรคอื่นๆ

๔.๑.๓ จะต้องติดเครื่องหมายข้อความดังนี้ “Off Limits To Unauthorized Personnel” ณ บริเวณทางเข้า

๔.๑.๔ อุปกรณ์ต่างๆ จะต้องเก็บอยู่ภายในและห่างจากภายนอกให้มากที่สุด

๔.๑.๕ อุปกรณ์การสื่อสารทางยุทธวิธีที่อยู่บนยานพาหนะจะต้องยึดกับยานพาหนะอย่างแน่นหนา

๔.๒ ความเสี่ยงระดับ ๒

๔.๒.๑ มาตรการทั้งหมดที่จำเป็นสำหรับความเสี่ยงระดับ ๑ จะต้องดำเนินการ

๔.๒.๒ การเข้าถึงกุญแจและสถานที่ต้องอยู่ภายใต้การควบคุมทางทหาร

๔.๓ ความเสี่ยงระดับ ๓

๔.๓.๑ มาตรการทั้งหมดสำหรับความเสี่ยงระดับ ๑ และ ๒ จะต้องดำเนินการ

๔.๓.๒ จะต้องมีแสงสว่างในเวลากลางคืนทั้งภายในและภายนอกเพื่อให้เจ้าหน้าที่รักษาความปลอดภัยสามารถตรวจจับผู้บุกรุกได้

๔.๓.๓ ควรเพิ่มเจ้าหน้าที่รักษาความปลอดภัยทั้งระยะไกลและระยะใกล้รอบพื้นที่

๕. สถานที่เก็บวัสดุวิศวกรรมและพื้นที่จัดเก็บวัสดุก่อสร้าง (Facility Engineering Supply and Construction Material Storage Areas)

๕.๑ ความเสี่ยงระดับ ๑

๕.๑.๑ อาคารที่จัดเก็บวัสดุสิ้นเปลืองและวัสดุก่อสร้างจะต้องเป็นไปตามข้อกำหนดของกองทัพ

๕.๑.๒ พื้นที่จัดเก็บด้านนอกจะล้อมรอบด้วยรั้วรอบขอบชิด

๕.๑.๓ วัสดุสิ้นเปลืองที่ไม่จำเป็นหรือหมดอายุจะถูกเก็บไว้ให้น้อยที่สุด

๕.๑.๔ จะต้องติดเครื่องหมายข้อความดังนี้ “Off Limits To Unauthorized Personnel” ณ บริเวณทางเข้า

๕.๒ ความเสี่ยงระดับ ๒

๕.๒.๑ มาตรการทั้งหมดที่จำเป็นสำหรับความเสี่ยงระดับ ๑ จะต้องดำเนินการ

๕.๒.๒ ชิ้นส่วนที่สามารถถอดออกได้ ต้องแยกออกจากวัสดุสิ้นเปลืองและวัสดุก่อสร้างอื่นๆ และเก็บไว้ในอาคารที่แยกออกและมีการควบคุมการเข้าถึง

๕.๒.๓ สถานที่จะต้องมีแสงสว่างในเวลากลางคืน

๕.๓ ความเสี่ยงระดับ ๓

๕.๓.๑ มาตรการทั้งหมดสำหรับความเสี่ยงระดับ ๑ และ ๒ จะต้องดำเนินการ

๕.๓.๒ จะต้องมีแสงสว่างในเวลากลางคืนทั้งภายในและภายนอกเพื่อให้เจ้าหน้าที่รักษาความปลอดภัยสามารถตรวจจับผู้บุกรุกได้

๕.๓.๓ อาคารจัดเก็บข้อมูลจะต้องมีการปิดผนึกอย่างเต็มที่

๕.๓.๔ ต้องมีสิ่งขีดขวางความสูงมากกว่า ๑ ฟุตและควรเพิ่มเจ้าหน้าที่รักษาความปลอดภัยทั้งระยะไกลและระยะใกล้รอบๆ พื้นที่

๖. ศูนย์ฝึกอบรมและอุปกรณ์ที่เกี่ยวข้อง (Audiovisual Equipment, Training Devices, and Subcaliber Devices at Training and Audiovisual Support Centers (TASCs)

๖.๑ ความเสี่ยงระดับ ๑

๖.๑.๑ การเข้าถึงอาคารจะต้องมีการใช้คีย์การ์ด กุญแจและมีการควบคุม

๖.๑.๒ อุปกรณ์ที่มีมูลค่าสูงจะต้องถูกจัดเก็บแยกออกและมีการป้องกัน

๖.๒ ความเสี่ยงระดับ ๒

๖.๒.๑ มาตรการทั้งหมดที่จำเป็นสำหรับความเสี่ยงระดับ ๑ จะต้องดำเนินการ

๖.๒.๒ ต้องมีการจัดสร้างจุดตรวจสอบ ซึ่งติดกับทางเข้าออก

๖.๒.๓ การเข้าถึงพื้นที่จัดเก็บอุปกรณ์จะ จำกัด เฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น

๖.๒.๔ ต้องมีการจัดทำบัญชีทรัพย์สินสำหรับอุปกรณ์ทั้งหมดพร้อมการสำรองข้อมูล

๖.๓ ความเสี่ยงระดับ ๓

๖.๓.๑ มาตรการทั้งหมดสำหรับความเสี่ยงระดับ ๑ และ ๒ จะต้องดำเนินการ

๖.๓.๒ ต้องจัดให้มีเจ้าหน้าที่ลาดตระเวนอย่างน้อยหนึ่งครั้งทุกๆ ๒ ชั่วโมง ตลอด ๒๔ ชั่วโมง

๗. บุคลากรที่มีความสำคัญและมีความเสี่ยงสูง (Mission–Critical and High–Risk Personnel)

๗.๑ ความเสี่ยงระดับ ๑ การเข้าถึงพื้นที่ที่มีบุคลากรที่ความสำคัญ หรือมีความเสี่ยงสูง จะต้องมีการควบคุม

๗.๒ ความเสี่ยงระดับ ๒ แม้บุคลากรที่ความสำคัญ หรือมีความเสี่ยงสูงไม่อยู่ในพื้นที่หรือสถานที่แล้วยังคงต้องมีการควบคุมสถานที่อย่างต่อเนื่อง

๗.๓ ความเสี่ยงระดับ ๓

๗.๓.๑ การเข้าถึงสถานที่ทั้งหมดจะถูกควบคุมตลอดเวลา

๗.๓.๒ การเข้าถึงพื้นที่โดยรอบจะต้องได้รับการควบคุม แม้บุคลากรที่ความสำคัญ หรือมีความเสี่ยงสูงไม่อยู่ในพื้นที่

๗.๓.๓ บุคคลที่ไม่มีส่วนเกี่ยวข้อง จะไม่ได้รับอนุญาตให้เข้าใกล้พื้นที่ และต้องมีการค้นหาตรวจสอบอาวุธและวัตถุระเบิด

รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคเอเชีย

รูปแบบการป้องกันความปลอดภัยในประเทศไทยและภูมิภาคเอเชีย

ปัจจุบันและแนวโน้มในอนาคต ภัยคุกคาม นับวันจะทวีความเข้มข้นและความรุนแรงมากขึ้นตามลำดับ ทั้งนี้เป็นผลมาจากความเจริญก้าวหน้าด้านการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร องค์กรหลายแห่งกำลังถูกคุกคามอย่างต่อเนื่อง ซึ่งมีผลกระทบต่อภูมิภาคเอเชียตะวันออกเฉียงใต้ ซึ่งประเทศในเอเชียหลายๆ ประเทศได้ไปศึกษาและจัดตั้งศูนย์ข้อมูลความปลอดภัยตามรูปแบบต่างๆ ได้แก่ การพัฒนาตามหลักสากลของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย (Policy) การจัดการองค์กร (Organization) และเทคโนโลยี (Technology) เพื่อบริหารความเสี่ยงไซเบอร์ (Cyber Risk Management) ที่มีผลกระทบกับหน่วยงานได้อย่างเหมาะสม โดยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัย เพื่อนำมาใช้ในการดำเนินการร่วมกัน ประกอบด้วย

๑. หน้าที่งาน(Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยในระดับภาพรวม จำแนกเป็น ๕ Functions (IPDRR : Identify, Protect, Detect, Respond, Recover)

๒. กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัย องค์กรอาทิ การจัดการทรัพย์สิน การควบคุมการเข้าถึง

๓. กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และ/หรือกิจกรรมในการบริหารจัดการ

๔. ข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติ ที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม

กองทัพบกไทย ได้เล็งเห็นความสำคัญในด้านการรักษาความมั่งคงปลอดภัย เช่นกัน จึงได้อนุมัติหลักการให้จัดตั้ง ศูนย์ไซเบอร์กองทัพบก (Army Cyber Centre) ขึ้น โดยจะเริ่มทดลองปฏิบัติงานตั้งแต่ ๑ ตุลาคม ๒๕๕๗ นี้เป็นต้นไป นับเป็นความท้าทายของกองทัพในการดำเนินการด้านต่างๆท่ามกลางสถานการณ์ทางการเมืองที่อ่อนไหว และภายใต้การจับตามมองของนานาประเทศ โดยเฉพาะประเทศกลุ่มสมาชิกอาเซียน ดังนั้นการกำหนดกรอบความคิดในการปฏิบัติงาน (Framework) เพื่อสร้างหลักประกันความสำเร็จในการดำเนินการ จึงเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่ง ทั้งนี้เพื่อใช้เป็นแนวทางการปฏิบัติงาน Guide Line ของเจ้าหน้าที่ศูนย์ความปลอดภัยกองทัพบก เจ้าหน้าที่อื่นๆ ที่เกี่ยวข้อง รวมถึงการสร้างความสำนึก ความตระหนัก และ

สร้างความรู้เข้าใจของกำลังพลทุกระดับชั้น โดยในชั้นต้นกรอบแนวทางการปฏิบัติงานของศูนย์ความปลอดภัยกองทัพบก ยังคงยึดถือการดำเนินงานตามหลักหน้าที่พื้นฐานของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทั้ง ๕ ประการ (IPDRR : Identify, Protect, Detect, Respond, Recover) ดังนี้

๑. **การระบุ (Identify)** เป็นการศึกษาสภาพแวดล้อม ทำความเข้าใจบริบท ทรัพยากรและกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยต่างๆ โดยเริ่มต้นจากการบริหารจัดการทรัพย์สิน (Asset Management : AM) การดำเนินการตรวจสอบสภาพแวดล้อม (Environmental Scanning : ES) การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย (Risk Assessment : RA) การประเมินช่องโหว่ของระบบ (Vulnerability Assessment : VA) การประกันความเสี่ยงด้านสารสนเทศ (Information Assurance : IA) การทดสอบเจาะระบบ (Penetration Testing : Pen-Test) และการกำหนดกลยุทธ์บริหารจัดการความเสี่ยง (Risk Management Strategy : RMS) เป็นต้น

๒. **การป้องกัน (Protect)** เป็นการดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อ จำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยต่างๆ โดยกำหนดมาตรการควบคุมการเข้าถึง (Access Control) การยืนยันและรับรองตัวบุคคล (Authentic) การสร้างความสำนึกความตระหนักและการฝึกอบรม (Awareness and Training) และมาตรการด้านความมั่นคงปลอดภัยต่างๆ ทั้งกระบวนการ และวิธีปฏิบัติ ตลอดจนเทคโนโลยีการรักษาความปลอดภัยต่างๆ เช่น ระบบตรวจหาการบุกรุก (Intrusion Detection System : IDS) ระบบป้องกันการบุกรุก (Intrusion Protection System : IPS)

๓. **การตรวจจับ (Detect)** เป็นการตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวัง หรือตรวจติดตามอย่างต่อเนื่อง โดยการเฝ้าระวัง สืบค้นตรวจสอบ วิเคราะห์ข้อมูลและพฤติการณ์ต่างๆ (Monitoring and Analysis) ที่ส่งผลกระทบหรือเป็นภัยต่อระบบสารสนเทศ จาก ห้องปฏิบัติการความมั่นคงปลอดภัยภายใน (Cyber Security Operations Center : CSOC) รวมถึงการตรวจสอบระบบสารสนเทศ (IT Audit) และหลักฐานทางดิจิตอลโดยกระบวนการทางวิทยาศาสตร์ (Digital Forensics) เพื่อดำเนินการทางกฎหมายต่อไป

๔. **การตอบสนอง (Respond)** เป็นการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง โดยจัดชุดปฏิบัติการฉุกเฉินด้านภายใน (Cyber Emergency Response Team : CERT) เพื่อทำหน้าที่ช่วยเหลือผู้ใช้งานที่ประสบปัญหาการคุกคามในเบื้องต้น การประสานการใช้งานระบบสำรอง (Backup System) คอยประสานการปฏิบัติกับหน่วยงานที่เกี่ยวข้อง

ควบคุมจำกัดขอบเขตและลดผลกระทบที่เกิดขึ้น (Mitigation) ตลอดจนควบคุมพยานหลักฐานต่างๆ เพื่อรอการพิสูจน์ต่อไป นอกจากนี้ยังมีชุดปฏิบัติการเชิงรุก (Cyber Warrior) เพื่อทำหน้าที่ปฏิบัติการภารกิจต่อเป้าหมายที่เป็นภัยคุกคามทั้งด้านภายในองค์กรและการปฏิบัติการข่าวสาร (Information Operations : IO) บนไซเบอร์ในกรณีที่มีความจำเป็น

๕. การคืนสภาพ (Recover) เป็นการดำเนินการกู้คืนสภาพระบบสารสนเทศที่ได้รับความเสียหายจากการถูกคุกคามด้านทรัพย์สินภายในองค์กรทั้ง ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และระบบฐานข้อมูลสารสนเทศ เพื่อรองรับการดำเนินงานอย่างต่อเนื่อง รวมถึงการจัดทำแผนการกู้คืนสภาพทั้งด้านขีดความสามารถ และการบริการให้ได้ตามเวลาที่กำหนด โดยจัดชุดปฏิบัติการกู้คืนระบบ (System Recovery Team : SRT) ดำเนินการตามขั้นตอนการกู้คืนสภาพ เพื่อให้ระบบกลับคืนสภาพสามารถใช้การได้ตามปกติ

การดำเนินงานต่างๆ ดังกล่าว นับเป็นความท้าทายด้านความรู้ ความสามารถของคนในกองทัพ เพราะเป็นเรื่องใหม่ที่องค์กรต่างๆ ทั่วโลกต่างให้ความสำคัญ โดยเฉพาะกองทัพบก ซึ่งได้มีนโยบายและกำลังเปิดแคมเปญ Kick off ออกไป โดยมีคุณลักษณะของงานประเภทสาขาต่างๆ ที่ต้องใช้ความรู้ ความสามารถ และประสบการณ์เฉพาะด้าน ที่แตกต่างและเหนือกว่าประเภทของงานสาขาด้านเทคโนโลยีสารสนเทศ (Information Technology : IT) ปกติ ซึ่งจะต้องมีการกำหนดหมายเลขความชำนาญการทางทหาร (ชกท.) ขึ้นมาเป็นพิเศษ เพื่อรองรับคุณสมบัติด้านคุณวุฒิตามสาขาวิชาชีพ และตามตำแหน่งหน้าที่การงาน รวมถึงการพิจารณากำหนดค่าตอบแทนวิชาชีพ ตามความเหมาะสมในสาขาต่างๆ เช่นเดียวกับ หมอ พยาบาลที่ปฏิบัติงานในตำแหน่งโดยไม่ต้องจำกัดชั้นยศ ทั้งนี้เพื่อให้เกิดประสิทธิภาพในการ ปฏิบัติงาน สร้างแรงจูงใจ และเสริมสร้างขวัญกำลังใจของเจ้าหน้าที่ในการทำงาน ไม่เกิดภาวะสมองไหล เนื่องจากบุคลากรดังกล่าว ยังเป็นที่ขาดแคลนและมีความต้องการสูงจากหน่วยงานภายนอก และองค์กรธุรการเอกชนต่างๆ ซึ่งสามารถยื่นข้อเสนอเงินเดือนและค่าตอบแทนได้สูงกว่ากองทัพ สำหรับคุณลักษณะของงานประเภทสาขาต่างๆ ที่ต้องใช้ความรู้ ความสามารถ และประสบการณ์เฉพาะด้านเป็นพิเศษ ในด้านองค์กรอาทิเช่น

๑. การบริหารจัดการทรัพย์สิน (Asset Management : AM)

๒. การตรวจสอบสภาพแวดล้อมภัยคุกคามองค์กร (Environmental Scanning : ES)

๓. การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย (Risk Assessment : RA)

๔. การประเมินช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment : VA)

๕. การประกันความเสี่ยงด้านสารสนเทศ (Information Assurance : IA)

๖. การปฏิบัติการทดสอบเจาะระบบสารสนเทศ (Penetration Testing : Pen-Test)

๗. การบริหารจัดการความเสี่ยงระบบสารสนเทศ (Risk Management : RM)

๘. การกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

๙. การยืนยันและรับรองตัวบุคคลด้านสารสนเทศ (Authentic)

๑๐. การสร้างความสำนึกความตระหนักและการฝึกอบรม (Awareness and Training)

๑๑. การตรวจหาการบุกรุก (Intrusion Detection : ID)

๑๒. การป้องกันการบุกรุก (Intrusion Protection : IP)

๑๓. การเฝ้าระวัง ตรวจสอบ และวิเคราะห์องค์กร (Monitoring and Analysis)

๑๔. การปฏิบัติการความมั่นคงปลอดภัยองค์กร (Security Operations)

๑๕. การตรวจสอบระบบสารสนเทศ (IT Audit)

๑๖. การตรวจพิสูจน์หลักฐานทางดิจิตอล (Digital Forensics)

๑๗. การปฏิบัติการฉุกเฉินด้านองค์กร (Cyber Emergency Response; CER)

๑๘. การปฏิบัติการกู้คืนระบบ (System Recovery : SR)

๑๙. การปฏิบัติการไซเบอร์เชิงรุก (Cyber Warrior)

๒๐. การปฏิบัติการข่าวสาร (Information Operations : IO) บนไซเบอร์

ประเภทงานต่างๆ ที่กล่าวมานี้ ปัจจุบันมีสถาบันการศึกษา หน่วยงาน องค์กรภาครัฐและเอกชน ทั้งภายในและภายนอกประเทศ ได้เปิดหลักสูตรการศึกษาระดับปริญญาตรีถึงปริญญาเอก สำหรับสถาบันการศึกษา และองค์กรในประเทศไทยที่เปิดสอน อาทิเช่น MUT, MU, AIT, CSAT, ASIC, NECTEC, NSTDA, KSC, ITPC, etc.

ปัจจัยการปฏิบัติงานด้านไซเบอร์ของกองทัพจะทำให้เกิดประสิทธิภาพ ประสิทธิผล นอกเหนือจากองค์กร (Organization) ระบบการทำงาน(Function) บุคลากร (Human Resource) องค์ความรู้ (Knowledge) และแรงจูงใจ (Incentive) แล้ว สิ่งที่สำคัญอีกประการ คือ ข้อกฎหมาย (Law) เนื่องจากการปฏิบัติงานด้านองค์กรมักจะมีความล่อแหลม และเกี่ยวพันกับข้อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รักษากฎหมาย โดยเนื้อหาสาระของกฎหมายส่วนใหญ่มุ่งเน้นไปในด้านอาชญากรรมคอมพิวเตอร์ (Computer Crime) แต่การปฏิบัติงานของกองทัพจะมุ่งเน้นไปในงานไซเบอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ ดังนั้นกองทัพควรจะพิจารณาออกกฎหมายพิเศษที่เกี่ยวข้องกับความมั่นคงของชาติด้านองค์กรเพื่อให้อำนาจ หน้าที่ และเป็นเกราะคุ้มกันเจ้าหน้าที่ของหน่วยงานไซเบอร์ของกองทัพ ที่มีการจัดตั้งหน่วยทั้งระดับกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ในการปฏิบัติงานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของชาติ (National Cyber Security) ทำนองเดียวกับ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) ก็จะมี

กฎหมายความมั่นคง เช่น พรบ. การรักษาความมั่นคงภายในราชอาณาจักร ใช้เป็นเครื่องมือทางกฎหมาย เป็นต้น

สำหรับ กรอบการปฏิบัติงานไซเบอร์ในด้านการรักษาความมั่นคงของชาติ เบื้องต้นในระหว่างที่ยังไม่มีกฎหมายมารองรับ จะเน้นไปในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร โดยจะเริ่มต้นการดำเนินการสำรวจตรวจสอบทรัพย์สินอุปกรณ์ต่างๆ ที่เกี่ยวข้องกับองค์กร เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบฐานข้อมูล รวมถึงระบบคอมพิวเตอร์ที่เชื่อมโยงกับอาวุธยุทโธปกรณ์ ระบบควบคุมอาวุธยิง ระบบค้นหาและติดตามเป้าหมาย ระบบลาดตระเวนและเฝ้าตรวจ ฯลฯ การดำเนินการตรวจสอบสภาพแวดล้อมภัยคุกคามองค์กรโดยเฉพาะการโจมตี การบุกรุก และการใช้โปรแกรมไวรัส และมัลแวร์ การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย โดยเฉพาะเครือข่ายอินเตอร์เน็ตและเครือข่ายไร้ การประเมินช่องโหว่ของระบบสารสนเทศ ทั้งอุปกรณ์เครือข่าย Hub Switching Ports อุปกรณ์คอมพิวเตอร์ โปรแกรมระบบงาน และระบบฐานข้อมูลต่างๆ การประกันความเสี่ยงด้านสารสนเทศ โดยเฉพาะอุปกรณ์คอมพิวเตอร์ โปรแกรมระบบงาน และระบบฐานข้อมูลต่างๆ เพื่อให้เกิดความต่อเนื่องในการใช้งาน การปฏิบัติการทดสอบเจาะระบบสารสนเทศ เป็นการฝึกปฏิบัติการ (Workshop) ภายในห้องปฏิบัติการองค์กร (Cyber War Room) ที่กำลังพัฒนาปรับปรุงจากห้องฝึกอบรมคอมพิวเตอร์เดิมขึ้นมาใหม่ เพื่อรองรับการฝึก การทดสอบ และการปฏิบัติงานจริง การบริหารจัดการความเสี่ยงระบบสารสนเทศ ในกรณีที่เกิดการโจมตีองค์กรเกิดความเสียหาย หรือเกิดปัญหาข้อขัดข้องต่างๆ โดยการจัดทำแผนฉุกเฉิน และการกำหนดกลยุทธ์บริหารจัดการความเสี่ยง การกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ เพื่อควบคุมสิทธิการใช้งานระบบสารสนเทศ และการเข้าถึงข้อมูลในระดับต่างๆ ของผู้ที่มีสิทธิ์ รวมถึงการป้องกันการเข้าใช้งานจากบุคคลที่ไม่มีสิทธิ์ การยืนยันรับรองตัวบุคคลด้านสารสนเทศ เพื่อยืนยันรับรองตัวตนและความถูกต้องของบุคคลที่มีสิทธิ์เข้าใช้งาน และเก็บบันทึกไว้สำหรับการตรวจสอบ การสร้างความสำนึกความตระหนักและการฝึกอบรม เป็นการดำเนินการรณรงค์ ชี้แจง ทำความเข้าใจ ปลูกฝังจิตสำนึก สร้างความตระหนัก รวมถึงการฝึกอบรมความรู้ความเข้าใจในกฎ ระเบียบ ข้อบังคับ และแนวทางการปฏิบัติต่างๆ รวมถึงการสร้างภาคีประชาคมเครือข่ายไซเบอร์กองทัพบก (Army Cyber Communities) ซึ่งได้ดำเนินการไปแล้วทั้ง ๔ พื้นที่กองทัพภาค การดำเนินการเฝ้าระวังตรวจสอบ วิเคราะห์องค์กรและข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง การเตรียมการปรับปรุงห้องปฏิบัติการความมั่นคงปลอดภัยองค์กร (Cyber Security Operations Center : CSOC) เพื่อใช้เป็นศูนย์ปฏิบัติการฯ ในการดูแลรักษาความมั่นคงปลอดภัยองค์กรโดยเฉพาะระบบคอมพิวเตอร์ของหน่วยต่างๆ ทั้งกองทัพบก การตรวจสอบระบบสารสนเทศ เป็นกระบวนการตรวจสอบภายในด้านสารสนเทศ

เช่นเดียวกับ การตรวจสอบภายในด้านการเงินและงบประมาณ การตรวจพิสูจน์หลักฐานทางดิจิตอล เป็นกระบวนการทางกฎหมาย ซึ่งจำเป็นจะต้องใช้ความชำนาญการเป็นพิเศษ เพื่อใช้เป็นหลักฐานในการดำเนินการทางกฎหมายต่อไป การปฏิบัติการฉุกเฉินด้านองค์กรในกรณีที่มีการคุกคามด้านองค์กรจะมีชุดปฏิบัติการฉุกเฉินด้านไซเบอร์ของกองทัพบก (Army CERT) เข้าไปปฏิบัติการในพื้นที่ที่เกิดเหตุ โดยชุดปฏิบัติการดังกล่าวจะประสานความร่วมมือในการปฏิบัติการกับระดับชาติ (Thai CERT) ระดับกระทรวงกลาโหม และระดับเหล่าทัพ ในกรณีที่เกิดความเสียหายต่อระบบสารสนเทศ จะมีชุดการปฏิบัติการกู้คืนระบบ (System Recovery Team : SRT) เข้าไปดำเนินการปฏิบัติการกู้คืนระบบ เพื่อให้สามารถกับมาใช้งานได้ตามปกติ

สำหรับการดำเนินการปฏิบัติการข่าวสารบนไซเบอร์จะเป็นการใช้ประโยชน์จากไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร ในกรณีการใช้ข่าวสารและสื่อไซเบอร์เพื่อเผยแพร่โจมตีให้ร้ายสถาบันพระมหากษัตริย์และกองทัพ การโจมตีให้ร้ายหรือบิดเบือนข้อเท็จจริงที่มีผลกระทบต่อความมั่นคงของชาติ การเผยแพร่ ยั่วยุ ปลุกปั่นให้เกิดความแตกแยกเกลียดชังของคนในสังคม การเผยแพร่หรือบิดเบือนข้อเท็จจริงที่มีผลกระทบต่อการรักษาความสงบเรียบร้อย การเผยแพร่ข้อมูลข่าวสารที่มีผลกระทบต่อการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ และการเผยแพร่ข้อมูลข่าวสารที่มีผลกระทบต่อความสัมพันธ์ระหว่างประเทศโดยเฉพาะประเทศเพื่อนบ้าน เป็นต้น โดยดำเนินการเฝ้าระวัง ค้นหา ติดตาม ตรวจสอบ ความเคลื่อนไหวข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง ตามที่กล่าวมาแล้วเพื่อรวบรวม สังเคราะห์ วิเคราะห์ และพิสูจน์ทราบความเคลื่อนไหวข้อมูลข่าวสาร จากกลุ่มบุคคล และเครือข่ายต่างๆ ในโลกไซเบอร์ เพื่อเป็นหลักฐานในการดำเนินการทางกฎหมาย หรือกำหนดมาตรการในการปฏิบัติการข่าวสารในด้านอื่นๆ เช่น การตอบโต้ข่าวสาร การบิดเบือนข้อมูล การสร้างความสับสน การลดกระแสและลดความน่าเชื่อถือของข่าวสาร ตลอดจนการกำหนดเป็นเป้าหมายในการปฏิบัติการเชิงรุกเมื่อจำเป็นต่อไป

การจัดตั้งศูนย์ไซเบอร์กองทัพบกระดับประเทศในหลายประเทศ

ภายใต้หลักการบริหารงานเชิงกลยุทธ์ ๔ ประการ (POLE) คือ การวางแผนงาน (**P**lanning) การจัดการองค์กร (**O**rganizing) การนำไปสู่การปฏิบัติ (**L**eading) และการประเมินผล (**E**valuating) โดยได้จัดการระดมความคิด (Brain Storming) ในการจัดทำแผนที่การทำงาน (Road Map) และกรอบตารางการปฏิบัติงาน (Time Frame) การดำเนินการปรับปรุงโครงสร้างองค์กร (Reorganization) และที่ตั้งสำนักงานศูนย์ไซเบอร์กองทัพบก การปรับเปลี่ยนระบบกระบวนการทำงานใหม่ (Reengineering) เพื่อให้เกิดประสิทธิภาพ และประสิทธิผลในการทำงานขององค์กร โดยเน้นผลสัมฤทธิ์ (Outcome) และได้เริ่มทดลองปฏิบัติงานขั้นต้นเป็นการภายในมาตั้งแต่กันยายน ๒๕๕๗ เช่น การสำรวจตรวจสอบทรัพย์สินที่เกี่ยวข้องกับไซเบอร์ (Asset

Management) การตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์ (Environmental Scanning) การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ (Risk Assessment) การประเมินช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) การปลูกฝังสร้างเสริมความสำนึก ความตระหนัก และการฝึกอบรม (Awareness and Training) การสร้างภาคีประชาคมเครือข่ายไซเบอร์กองทัพบก (Army Cyber Communities) การเฝ้าระวัง ตรวจสอบ วิเคราะห์องค์กรและข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง การปรับปรุงห้องปฏิบัติการความมั่นคงปลอดภัยองค์กร (CSOC) เป็นต้น โดยอาศัยเครื่องมืออุปกรณ์ที่มีอยู่เดิม ซอฟต์แวร์ Open source และแสวงหาความร่วมมือจากหน่วยงานภายนอก โดยมีผลการปฏิบัติงานที่ผ่านมา ดังนี้

๑. การสำรวจตรวจสอบทรัพย์สินที่เกี่ยวข้องกับองค์กร(Asset Management) เพื่อจัดทำบัญชีคุมสถานภาพสิ่งอุปกรณ์ การจำหน่ายสิ่งอุปกรณ์ที่ชำรุดใช้การไม่ได้ และการนำอุปกรณ์ที่ไม่ใช้งานไปใช้เป็นเครื่องมือในการปฏิบัติงานเบื้องต้นของ ศูนย์ไซเบอร์ของกองทัพบก

๒. การตรวจสอบสภาพแวดล้อมภัยคุกคามองค์กร (Environmental Scanning) เป็นการใช้เครื่องมือตรวจสอบ ป้องกันระบบ Network และ Application โดยสามารถตรวจสอบและดักจับความเคลื่อนไหวของภัยคุกคามไซเบอร์ในระบบเครือข่ายคอมพิวเตอร์ได้ตั้งแต่ระดับ Physical Layer (Layer ๑)ไปจนถึงระดับ Application Layer (Layer ๗) ตั้งแต่แหล่งที่มาของต้นทางไปยังอุปกรณ์คอมพิวเตอร์ปลายทางภายในระบบเครือข่าย โดยเฉพาะโปรแกรม BotNet, Trojan Horse, Backdoor, Virus และ Malware รวมถึงเส้นทางการจราจรบนเครือข่าย (Network Traffic) ที่ผิดปกติเพื่อแจ้งให้หน่วยที่เกี่ยวข้องทราบ และดำเนินการต่อไป

๓. การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่งคงปลอดภัยองค์กร (Risk Assessment) เป็นการประเมินตนเองด้านความเสี่ยงในการรักษาความมั่งคงปลอดภัยไซเบอร์ของกองทัพบก ผ่านระบบ online ของ ACIS Professional Center เพื่อวิเคราะห์ ภาพจำลองความพร้อม และความไม่พร้อมในด้านต่างๆ ของกองทัพบก ซึ่งควรจะต้องเร่งดำเนินการพัฒนาปรับปรุงแก้ไขจุดอ่อนดังกล่าวต่อไปในอนาคต

๔. การประเมินช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) เป็นการใช้เครื่องมือตรวจสอบช่องโหว่ระบบสารสนเทศ ด้วยซอฟต์แวร์ Open source เพื่อตรวจสอบและวิเคราะห์ช่องโหว่ของพอร์ตต่างๆ บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) รวมถึงการบุกรุก โจมตีผ่านช่องโหว่ดังกล่าว เพื่อแจ้งให้หน่วยที่เกี่ยวข้องทราบ และดำเนินการต่อไป

๕. การปลูกฝังสร้างเสริมความสำนึก ความตระหนักและการฝึกอบรม (Awareness and Training) เป็นการจัดชุดนิเทศไซเบอร์เคลื่อนที่ไปชี้แจงระเบียบคำสั่ง ด้านการรักษาความปลอดภัยสารสนเทศ การสร้างความตระหนัก ความสำนึก และความระมัดระวังในการใช้งาน

เทคโนโลยีสารสนเทศและการสื่อสาร โดยได้ดำเนินการไปแล้วในพื้นที่ทั้ง ๔ กองทัพภาค รวมถึงการเข้ารับฝึกอบรมฯ จากสถาบันและองค์กรต่างๆ ตามแนวทางการพัฒนาความร่วมมือจากหน่วยงานภายนอก ทั้งภาครัฐและเอกชน เพื่อพัฒนาขีดความสามารถของบุคลากรศูนย์ไซเบอร์ของกองทัพบก

๖. การสร้างภาคีประชาคมเครือข่ายไซเบอร์กองทัพบก (Army Cyber Communities) เป็นการจัดตั้งประชาคมเครือข่ายไซเบอร์ของกำลังพลในกองทัพบก โดยแสวงประโยชน์จากการดำเนินงานของชุดนิเทศไซเบอร์เคลื่อนที่ ซึ่งลงไปปฏิบัติงานในพื้นที่หน่วยทหารทั้ง ๔ กองทัพภาค

๗. การปรับปรุงห้องปฏิบัติการความมั่นคงปลอดภัยองค์กร (CSOC) เพื่อใช้เป็นศูนย์ปฏิบัติการฯ ในการดูแลรักษาความมั่นคงปลอดภัยองค์กร โดยดำเนินการขออนุมัติโครงการปรับปรุงห้องฝึกอบรมศูนย์เทคโนโลยีทางทหาร เพื่อใช้เป็นห้องปฏิบัติการองค์กร (War Room) ในขั้นต้น และโครงการปรับปรุงระบบการรักษาความมั่นคงปลอดภัยเครือข่ายภายใน

๘. การดำเนินการเฝ้าระวัง ติดตาม ตรวจสอบ วิเคราะห์องค์กรและข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง เพื่อสนับสนุนการปฏิบัติการข่าวสารของกองทัพบก โดยดำเนินการเฝ้าระวัง สืบค้น ติดตามตรวจสอบ แหล่งที่มาของข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง อย่างต่อเนื่องตลอดเวลา และรายงานให้หน่วยงานที่เกี่ยวข้องทราบเพื่อดำเนินการต่อไป

๙. การดำเนินการพัฒนาบุคลากร โดยจัดกำลังพลเข้ารับการศึกษาอบรมหลักสูตรต่างๆ ด้านไซเบอร์ จาก มหาวิทยาลัยมหิดล อำเภอศาลายา จังหวัดนครปฐม จำนวนหลายหลักสูตร การเดินทางไปร่วมสัมมนาและศึกษาดูงานด้านไซเบอร์ ณ ประเทศสิงคโปร์ สืบเนื่องมาจากการแสวงหาความร่วมมือจากหน่วยงานภายนอก โดยไม่ใช้งบประมาณจากทางราชการ

สำหรับแผนการดำเนินงานในขั้นทดลองปฏิบัติงานของ ศูนย์ไซเบอร์กองทัพบก จะมีความต่อเนื่องจากการดำเนินงานที่ผ่านมา ซึ่งจะมีความพร้อม ความน่าสนใจ และความเข้มข้นเพิ่มขึ้นตามลำดับ โดยเฉพาะอย่างยิ่งด้านการพัฒนาบุคลากร เพื่อรองรับภารกิจที่ท้าทายความรู้ความสามารถของกำลังพลในกองทัพบก โดยจะมีการประกันความเสี่ยงด้านสารสนเทศ (Information Assurance : IA) การทดสอบเจาะระบบสารสนเทศ (Penetration Testing : Pen-Test) การบริหารจัดการความเสี่ยงระบบสารสนเทศ (Risk Management : RM) การกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) การยืนยันและรับรองตัวบุคคลด้านสารสนเทศ (Authentic) การตรวจหาการบุกรุก (Intrusion Detection : ID) การป้องกันการบุกรุก (Intrusion Protection : IP) การเฝ้าระวัง ตรวจสอบ และวิเคราะห์ไซเบอร์ (Cyber Monitoring and Analysis) การปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operations) การตรวจสอบ

ระบบสารสนเทศ (IT Audit) การตรวจพิสูจน์หลักฐานทางดิจิตอล (Digital Forensics) การปฏิบัติการฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Team : CERT) การปฏิบัติการกู้คืนระบบ (System Recovery : SR) การปฏิบัติการไซเบอร์เชิงรุก (Cyber Warrior) และการปฏิบัติการข่าวสาร (Information Operations : IO) บนไซเบอร์ ซึ่งหลาย งานที่กล่าวมา จำเป็นต้องอาศัยอุปกรณ์เครื่องมือที่จะได้มาจาก โครงการปรับปรุงระบบการรักษาความมั่นคงปลอดภัยเครือข่ายภายใน

นอกเหนือจากแผนการดำเนินงานที่กล่าวมาแล้วข้างต้น ซึ่งจะอยู่ในกรอบแนวทางการปฏิบัติการด้านไซเบอร์ของกองทัพบกทั้ง ๓ ขั้น คือ ขั้นที่ ๑ การจัดการทรัพยากรเพื่อการปฏิบัติการด้านไซเบอร์ขั้นที่ ๒ การเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยองค์กรมาตรการเชิงรับ และขั้นที่ ๓ การเสริมสร้างขีดความสามารถการปฏิบัติการองค์กรมาตรการเชิงรุก โดยห้วงระยะเวลาในแต่ละขั้นอาจจะปรับลดจำนวนปีให้เร็วขึ้น เนื่องจากความพร้อมในการเตรียมการ และการพัฒนาขีดความสามารถของกำลังพล ซึ่งแสวงหาความร่วมมือจากองค์กรต่างๆ แต่สิ่งที่น่าสนใจและควรติดตามการดำเนินงานของศูนย์ไซเบอร์กองทัพบกเป็นอย่างยิ่ง คือ การกำหนดมาตรฐานการปฏิบัติงานเบื้องต้นของกองทัพบก โดยได้รับการรับรองจากสถาบันด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ที่มีชื่อเสียงภายในประเทศ ในการออกใบรับรองมาตรฐานการปฏิบัติงานด้านการรักษาความมั่งคงปลอดภัยองค์กร (Cyber Security Certificate) และการจัดการแข่งขันทักษะด้านการรักษาความมั่นคงปลอดภัยและการปฏิบัติการไซเบอร์ (Army Cyber Security & Operations Contest ๒๐๑๕) ในปี ๒๕๕๘ ซึ่งจะได้วางแผนดำเนินการแข่งขันฯ เป็นปีแรกและปีต่อๆ ไปอย่างต่อเนื่อง เพื่อตรวจสอบขีดความสามารถของกำลังพลของกองทัพบก และบุคคลทั่วไป รวมถึงการพัฒนาทักษะเพื่อเสริมสร้างขีดความสามารถการปฏิบัติการองค์กรทั้งมาตรการเชิงรับและเชิงรุกต่อไป

การดำเนินการจัดตั้งศูนย์ไซเบอร์กองทัพบก ตามที่กล่าวมาข้างต้น จะเห็นได้ว่าเป็นการดำเนินการภายใต้กรอบกฎหมาย ตามหลักการและมาตรฐานสากล สอดรับกับนโยบายของรัฐบาล ทั้งนี้เพื่อเป็นการเตรียมความพร้อมของกองทัพและประเทศชาติ ในการรับมือกับภัยคุกคามที่กำลังเป็นภัยคุกคามไปทั่วทุกมุมโลกรวมถึงภัยคุกคามในอนาคต โดยกองทัพบกจะเปิดกว้างให้กับประชาชนและองค์กรทุกภาคส่วนเข้ามามีส่วนร่วมในด้านการพัฒนาความพร้อมด้านไซเบอร์ร่วมกัน เพื่อเสริมสร้างให้ประเทศไทยมีศักยภาพ และมีความแข็งแกร่งในด้านการรักษาความมั่นคงปลอดภัยในภูมิภาค

รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคอื่นๆ

รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคอื่นๆ ซึ่งหากนับภูมิภาคที่สำคัญในโลกโดยตัดเอเชียและอเมริกาเหนือไปเนื่องจากได้ดำเนินการสรุปให้ไว้ในหัวข้ออื่นแล้วนั้น จะคงเหลือภูมิภาคอเมริกาเหนือ ยุโรป โอเชียเนีย และแอฟริกา ซึ่งถือได้ว่ามีหลากหลายทางเชื่อชาติ ศาสนา ประเทศและหลากหลายแนวคิด ขึ้นกับการแบ่งประเภทการรักษาความปลอดภัยของแต่ละประเทศและองค์กร อย่างไรก็ตามประเทศชั้นนำของภูมิภาคต่างๆ ต่างยึดรูปแบบการดำเนินการทางการทหารสมัยใหม่ตามรูปแบบของกองทัพสหรัฐอเมริกา แต่ได้มีการปรับเปลี่ยนและสั่งสมความรู้เป็นระยะเวลานานจนกระทั้งได้รูปแบบที่เหมาะสมของประเทศตนเองรวมถึงศักยภาพและกำลังพลของตนเองด้วยเช่นกัน จากการศึกษาเอกสาร ข้อมูลและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยพบว่าการรักษาความปลอดภัยส่วนมากมีการแบ่งออกเป็นการรักษาความปลอดภัยสำหรับสถานที่ ทรัพย์สินบุคคล และยานพหนะอย่างไรก็ตามงานวิจัยชิ้นนี้มุ่งเน้นการศึกษาความปลอดภัยด้านสถานที่ที่เหมาะสมในอนาคต ผู้วิจัยจึงขอสรุปโดยแบ่งตามรูปแบบอุปกรณ์การรักษาความปลอดภัยและแบ่งตามความสำคัญจของพื้นที่ได้ ๔ ระดับดังนี้

ระดับที่ ๑ ที่รั้วและพื้นที่ทางเข้าสถานที่

ระดับที่ ๒ จากรั้วจนถึงอาคารและห้องรับรอง

ระดับที่ ๓ ภายในห้องรับรอง

ระดับที่ ๔ จุดที่ต้องการความปลอดภัยสูง อาทิห้องภายในอาคารที่เก็บทรัพย์สิน หรือเอกสารข้อมูลที่สำคัญ (Restrict Zone) บริเวณห้ามเข้า (Forbidding Zone) พื้นที่เก็บหรือฐานยิงจรวดบรรจุระเบิด

ระดับที่ ๑ ที่รั้วและพื้นที่ทางเข้าสถานที่

บริเวณรั้ว และทางเข้า สำหรับสถานที่ที่ต้องการควบคุมความปลอดภัยสูงกว่าทั่วๆ ไป (ถ้าสำคัญน้อยกว่าก็สามารถลดระดับความเข้มลงได้) และต้องมีการกำหนดการลาดตระเวนทั้งภายนอกและภายในการระเบียบของกองทัพแต่ละประเทศ โดยความถี่ในการลาดตระเวนจะขึ้นอยู่กับสภาวะและสถานการณ์

๑. สำหรับบุคคล ทางเข้าอาคารควรมีหลังคา คนผ่านเข้ามาในอาคาร เข้ามาติดต่อ กับห้อง รปภ. หรือพนักงานรักษาความปลอดภัยจากนั้น กำหนดให้ผ่านเข้าทางเข้าที่มีแขนกั้นแบบ ๓ ขา (Tripod Turnstile) หรือแบบกั้นแบบแผ่นกั้น (Butterfly Turnstile) หรือที่กั้นแบบอื่นๆ ในลักษณ์เดียวกัน โดยจะยอมให้ผ่านได้เมื่อใช้บัตรเจ้าหน้าที่ทาบบนเครื่องทาบบัตร (Card Scanner) หรือเครื่องแสกนใบหน้า (Facial Scanner)หรือ ใช้เครื่องสแกนลายนิ้วมือ (Finger Scanner) โดยส่วนผู้

มาเยี่ยม (บุคคลภายนอก) จะต้องมีระบบการถ่ายภาพ เก็บข้อมูลและการยืนยันตัวตน แล้วจึงผ่านเครื่องกั้นผ่านเข้าไปยังห้องรับรองเพื่อตรวจสัมภาระ และเมื่อผ่านขั้นตอนนี้จึงจะมี รปภ. นำทางไปหรือไม่นำทางไปแล้วแต่ความสำคัญของสถานที่

๒. สำหรับยานพาหนะ โดยสถานที่ต้องการความปลอดภัยสูง ต้องมีที่จอดยานพหานะ นอกรั้วกั้นต่างหากแต่หากหลีกเลียงไม่ได้ต้องจอดภายในสถานที่ (รั้ว) ก็ควรมีแขนกั้นรถยนต์และจักรยานยนต์โดยมีห้องทำงานของ รปภ.คอยควบคุมโดยที่รถบุคคลภายใน และรถพนักงานจะต้องมีบัตรติดหน้ากระจก ซึ่งจะมีคลื่นวิทยุหรือระบบอื่นๆ ส่วนรถของผู้มาเยี่ยม (บุคคลภายนอก) จะต้องมีการจัดให้มีที่จอดเฉพาะและผู้มาเยี่ยมต้องผ่านอาคาร รปภ. เพื่อบันทึกภาพ แลกบัตรและตรวจยานพาหนะขั้นต้นก่อน

๓. สำหรับผู้บุกรุกคือปีนรั้วข้ามเข้ามา หรือออกไป ควรจะใช้รั้วไฟแรงสูงกันไว้อีกชั้นถ้าจำเป็น หรือจะใช้เครื่องตรวจจับด้วยคลื่นแสงอินฟาเรดที่มองไม่เห็นแสง แล้วมีสัญญาณดังที่ห้อง รปภ. หรือผู้เกี่ยงข้อง

สรุปอุปกรณ์รักษาความปลอดภัยสำหรับทางเข้าบุคคล

๑. กล้องวงจรปิดเพื่อเพื่อดูและเก็บบันทึกวีดีโอ

๒. บัตรพนักงานและบัตรผู้มาเยี่ยม

๓. กล้องถ่ายรูป

๔. เครื่องกั้นแขนกั้น

๕. เครื่องอ่านบัตร (Card Scanner)

๖. เครื่องสแกนลายนิ้วมือ (Finger Scanner)

๗. เครื่องแสกนใบหน้า (Facial Scanner)

สรุปอุปกรณ์รักษาความปลอดภัยสำหรับ ทางเข้ายานพาหนะ

๑. กล้องวงจรปิด

๒. แขนกั้นรถยนต์

๓. เครื่องทาบบัตร/เครื่องอ่านบัตรระยะไกล

ระดับที่ ๒ บริเวณพื้นที่รั้ว จนถึงห้องรับรอง

บริเวณพื้นที่รั้ว จนถึงห้องรับรอง ควรมีถนนหรือทางเดินและสำหรับอาคารที่สำคัญให้มีเซนเซอร์แบบแม่เหล็กติดที่หน้าต่าง หรือทางออกฉุกเฉิน เนื่องจากหากมีผู้บุกรุกมางัดหน้าต่างประตูฉุกเฉิน ระบบแจ้งเตือน (Alarm System) จะมีสัญญาณดังที่ห้อง รปภ. หรือที่ผู้เกี่ยงข้อง โดยรอบควรมีกล้องวงจรปิดที่คลอบคลุมเห็นพื้นที่ตามกำแพงอาคารโดยรอบ กล้องวงจรปิดอาจจะ

เป็นกล้องสปีดโดม (Speed Dome Camera) สำหรับแขวนนอกอาคาร หรือกล้องแบบ Auto Tracking (Auto Tracking Speed Dome Camera)

สรุปอุปกรณ์รักษาความปลอดภัยสำหรับใช้บริเวณพื้นที่รั้ว จนถึงห้องรับรอง

๑. ระบบแจ้งเตือน (Alarm System)

๒. เซ็นเซอร์แม่เหล็ก (Magnetic Sensor)

๓. กล้องวงจรปิดแบบภายนอกอาคาร Auto Trading Speed Dome Camera

๔. PTZ Speed Dome Camera

๕. Box Camera with Housing

๖. Guard Tour

ระดับที่ ๓ พื้นที่ภายในห้องรับรอง

ควรมีการใช้ระบบเครื่องทาบ เมื่อเขาไปในห้องรับรองแล้วติดต่อกับโอเปอเรเตอร์เพื่อขอให้พนักงานที่ต้องการติดต่อลงมาคุยในห้องดังกล่าวและมีระบบยืนยันการเข้าพบเพื่อจะได้นำไปแสดงต่อ รปภ. ถ้าสถานที่มีความปลอดภัยสูงก็ให้พนักงานเดินไปส่งให้พ้นอาคาร รปภ.

สรุปอุปกรณ์รักษาความปลอดภัยสำหรับใช้ พื้นที่ภายในห้องรับรอง

๑. เครื่องสแกนบัตรหน้าประตู

๒. โฟโต้สวิทซ์

๓. กล้องวงจรปิด

ระดับที่ ๔ จุดที่ต้องการความปลอดภัยสูง

ควรจะมีกำหนดนโยบายว่าบุคคลใดบ้างที่สามารถเข้าได้กำหนดว่าบุคคลใดบ้างที่สามารถเข้าได้ที่ละคนหรือมากกว่า ประตูทางเข้าควรมีเครื่องสแกนดวงตา หรือ สแกนใบหน้าหรือสแกนลายนิ้วมือ ตามแต่จะเลือกใช้ตามความสำคัญ กล้องวงจรปิดทั้งนอกห้องและในห้อง ระบบแจ้งเตือนป้องกันหน้าต่างและประตูห้องถ้าเปิดออกโดยไม่ถูกวิธีการ ตอนขาออกจากห้อง ต้องผ่านเครื่องสแกนลายนิ้วมือพร้อมกัน โดยทั้งหมดนี้ให้ขึ้นอยู่กับนโยบายและความสำคัญของแต่ละสถานที่นั้นๆ (องค์การรักษาความมั่นคงฝ่ายพลเรือน, ๒๕๖๐)

ดังนั้นสามารถสรุปได้ว่ารูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคอื่นๆ ล้วนมีแนวคิดและโครงสร้างพื้นฐานที่ใกล้เคียงกัน แต่อาจจะแตกต่างกันบ้างในส่วนของอุปกรณ์และเทคโนโลยีที่เกี่ยวข้องบ้างตามแต่กรณี

เปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ

จากการวิเคราะห์รูปแบบการรักษาความปลอดภัยของประเทศต่างๆ ดังที่ได้กล่าวไว้ในหัวข้อที่ผ่านมาสามารถสรุปเปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ ดังตารางที่ ๓ - ๑ ต่อไปนี้

ตารางที่ ๓ - ๑ เปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ

รูปแบบการรักษาความปลอดภัย	ด้านระบบ/โครงสร้างหรือมาตรการ	ด้านการแบ่งระดับและขั้นตอน	ด้านอุปกรณ์เครื่องมือที่ใช้
ประเทศสหรัฐอเมริกา	- มาตรการการป้องกันทางกายภาพขั้นตอนการรักษาความปลอดภัยและการต่อต้านการก่อการร้าย - มาตรการรักษาความปลอดภัยขั้นต่ำที่จำเป็นสำหรับการดำเนินการต่อประเภทของทรัพย์สิน - มาตรการรักษาความปลอดภัยที่ต้องใช้รั้วรอบที่ตั้ง	๑. สถานที่เก็บอากาศยานและชิ้นส่วนของกองทัพ ๒. สถานที่เก็บอากาศยานและชิ้นส่วนของกองทัพ ที่ไม่อยู่ในสถานที่ของกองทัพ ๓. สถานที่เก็บยานพาหนะ ชิ้นส่วนส่วนประกอบและระบบอาวุธ ๔. สถานที่เก็บอุปกรณ์สื่อสาร อุปกรณ์อิเล็กทรอนิกส์และอุปกรณ์ตรวจการณ์กลางคืน ๕. สถานที่เก็บวัสดุวิศวกรรมและพื้นที่จัดเก็บวัสดุก่อสร้าง ๖. ศูนย์ฝึกอบรมและอุปกรณ์ที่เกี่ยวข้อง	ระบบเครือข่ายคอมพิวเตอร์ และเทคโนโลยีสารสนเทศและอื่นๆ

ตารางที่ ๓ - ๑ เปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ (ต่อ)

รูปแบบการรักษาความปลอดภัย	**ด้านระบบ/โครงสร้างหรือมาตรการ**	**ด้านการแบ่งระดับและขั้นตอน**	**ด้านอุปกรณ์เครื่องมือที่ใช้**
ประเทศสหรัฐอเมริกา		การแบ่งระดับออกเป็น ความเสี่ยงระดับ ๑ ความเสี่ยงระดับ ๒ ความเสี่ยงระดับ ๓	
ประเทศในภูมิภาคเอเชีย	๑. หน้าที่งาน (Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยในระดับภาพรวม จำแนกเป็น ๕ Functions (IPDRR: Identify, Protect, Detect, Respond, Recover) ๒. กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยองค์กร อาทิ การจัดการทรัพย์สิน การควบคุมการเข้าถึง ๓. กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค	๑. การระบุ (Identify) ๒. การป้องกัน (Protect) ๓. การตรวจจับ (Detect) ๔. การตอบสนอง (Respond) ๕. การคืนสภาพ (Recover) ภายใต้หลักการบริหารงานเชิงกลยุทธ์ ๔ ประการ (POLE) คือ การวางแผนงาน (**P**lanning) การจัดการองค์กร (**O**rganizing) การนำไปสู่การปฏิบัติ (**L**eading) และการประเมินผล (**E**valuating)โดยได้จัดการระดมความคิด (Brain Storming) ในการจัดทำแผนที่การทำงาน	ระบบเครือข่ายคอมพิวเตอร์ และเทคโนโลยีสารสนเทศ และอื่นๆ

ตารางที่ ๓ - ๑ เปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ (ต่อ)

รูปแบบการรักษาความปลอดภัย	ด้านระบบ/โครงสร้างหรือมาตรการ	ด้านการแบ่งระดับและขั้นตอน	ด้านอุปกรณ์เครื่องมือที่ใช้
ประเทศในภูมิภาคเอเชีย	และ/หรือกิจกรรมในการบริหารจัดการ ๔.ข้อมูลอ้างอิง Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทางและแนวปฏิบัติ ที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม	(Road Map) และกรอบตารางการปฏิบัติงาน (Time Frame) การดำเนินการปรับปรุงโครงสร้างองค์กร (Reorganization)	
ประเทศในภูมิภาคอื่นๆ	การรักษาความปลอดภัยส่วนมากมีการแบ่งออกเป็น ๑. การรักษาความปลอดภัยสำหรับสถานที่ ทรัพย์สิน บุคคล ๒. การรักษาความปลอดภัยสำหรับยานพาหนะ	การรักษาความปลอดภัยและแบ่งตามความสำคัญของพื้นที่ได้ ๔ ระดับ ดังนี้ ระดับที่ ๑ ที่รั้วและพื้นที่ทางเข้าสถานที่ ระดับที่ ๒ จากรั้วจนถึงอาคารและห้องรับรอง ระดับที่ ๓ ภายในห้องรับรอง ระดับที่ ๔ จุดที่ต้องการความปลอดภัยสูง อาทิห้องภายในอาคารที่เก็บทรัพย์สินหรือเอกสารข้อมูลที่สำคัญ (Restrict Zone)	ระบบเครือข่ายคอมพิวเตอร์ และเทคโนโลยีสารสนเทศและอื่นๆ ได้แก่ อุปกรณ์รักษาความปลอดภัยสำหรับทางเข้าบุคคล - กล้องวงจรปิดเพื่อเพื่อดูและเก็บบันทึกวีดีโอ - บัตรพนักงานและบัตรผู้มาเยี่ยม - กล้องถ่ายรูป - เครื่องกั้นแขนกั้น

ตารางที่ ๓ - ๑ เปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ (ต่อ)

รูปแบบการรักษาความปลอดภัย	ด้านระบบ/โครงสร้างหรือมาตรการ	ด้านการแบ่งระดับและขั้นตอน	ด้านอุปกรณ์เครื่องมือที่ใช้
ประเทศในภูมิภาคอื่นๆ		บริเวณห้ามเข้า (Forbidding Zone)พื้นที่เก็บ หรือฐานยิงจรวด บรรจุ ระเบิด	- เครื่องอ่านบัตร (Card Scanner) - เครื่องสแกนลายนิ้วมือ (Finger Scanner) - เครื่องแสกนใบหน้า (Facial Scanner) อุปกรณ์รักษาความปลอดภัยสำหรับทางเข้ายานพาหนะ - กล้องวงจรปิด - แขนกั้นรถยนต์ - เครื่องทาบบัตร/เครื่องอ่านบัตรระยะไกล

สรุป

จากการศึกษารูปแบบการรักษาความปลอดภัยของประเทศต่างๆ รวมถึงการเปรียบเทียบรูปแบบการรักษาความปลอดภัยดังที่กล่าวไว้ในตารางที่ ๓ - ๑ สามารถนำมาสรุปผลการวิเคราะห์ข้อมูลได้ดังต่อไปนี้

๑. รูปแบบการรักษาความปลอดภัยของประเทศสหรัฐอเมริกา

การรักษาความปลอดภัยของประเทศสหรัฐอเมริกา มีการกำหนดเป็นนโยบาย โดย Military Police: Security of Unclassified Army Property ซึ่งกำหนดเป็นความปลอดภัยขั้นต่ำและหากเป็นสถานที่ที่มีความต้องการความปลอดภัยสูงมาก สามารถดำเนินการเพิ่มเติมได้เองตาม

นโยบายของแต่ละชั้นความลับที่ได้รับมอบหมายจากผู้บังคับบัญชาได้ โดย US Military Police มีการแบ่งออกเป็นการรักษาความปลอดภัยสำหรับสถานที่ ทรัพย์สิน บุคคล และยานพหนะ อย่างไรก็ตามงานวิจัยชิ้นนี้มุ่งเน้นการศึกษาความปลอดภัยด้านสถานที่ที่เหมาะสมในอนาคต ซึ่งสรุปข้อตกลงเบื้องต้นโดยแบ่งตามรูปแบบการรักษาความปลอดภัยตามระดับของ Security of Unclassified Army Property ดังนี้

๑.๑ มาตรการการป้องกันทางกายภาพขั้นตอนการรักษาความปลอดภัยและการต่อต้านการก่อการร้ายสำหรับประเภทของทรัพย์สิน

๑.๒ มาตรการรักษาความปลอดภัยขั้นต่ำที่จำเป็นสำหรับการดำเนินการต่อประเภทของทรัพย์สิน แม้ว่าประเภทของทรัพย์สินของกองทัพเหล่านี้ไม่จำเป็นต้องมีการวิเคราะห์ความเสี่ยงโดยใช้ DA Pam ๑๙๐-๕๑

๑.๓ มาตรการรักษาความปลอดภัยที่ต้องใช้รั้วรอบที่ตั้ง กำหนดให้มีความสูง (๖ หรือ ๗ ฟุต) และมีความสามารถในการป้องกันที่ดีหรือมีคุณสมบัติอื่นๆจะขึ้นอยู่กับการตัดสินของผู้บังคับบัญชาการติดตั้ง และต้องดำเนินการติดตั้งตามคำแนะนำที่พบได้ใน Field Manual (FM) ๑๙-๓๐ เว้นแต่เป็นไปตามข้อกำหนดของกองกำลังวิศวกรสหรัฐอเมริกาเลขที่ ๔๐-๑๖-๐๘, Type FE

๑.๔ หากมีข้อโต้แย้งหรือไม่สามารเนินการได้ตามมาตรฐานต่างๆ ที่กำหนดให้ทำหนังสือระบุเป็นลายลักษณ์อักษร พร้อมระบุมาตรการทดแทน

๒. รูปแบบการป้องกันความปลอดภัยในประเทศไทยและภูมิภาคเอเชีย

การพัฒนาตามหลักสากลของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย (Policy) การจัดการองค์กร (Organization) และเทคโนโลยี (Technology) เพื่อบริหารความเสี่ยง (Risk Management) ที่มีผลกระทบกับหน่วยงานได้อย่างเหมาะสม โดยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัย เพื่อนำมาใช้ในการดำเนินการร่วมกัน ประกอบด้วย

๒.๑ หน้าที่งาน(Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยในระดับภาพรวม จำแนกเป็น ๕ ฟังก์ชั่น (IPDRR : Identify, Protect, Detect, Respond, Recover)

๒.๒ กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยองค์กร อาทิ การจัดการทรัพย์สินและการควบคุมการเข้าถึง

๒.๓ กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และ/หรือกิจกรรมในการบริหารจัดการ

๒.๔ ข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติ ที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม

๓. รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคอื่นๆ

ภูมิภาคอเมริกาเหนือ ยุโรป โอเชียเนีย และแอฟริกา ซึ่งถือได้ว่ามีหลากหลายทางเชื่อชาติ ศาสนา ประเทศและหลากหลายแนวคิด ขึ้นกับการแบ่งประเภทการรักษาความปลอดภัยของแต่ละประเทศและองค์กร อย่างไรก็ตามประเทศชั้นนำของภูมิภาคต่างๆ ต่างยึดรูปแบบการดำเนินการทางการทหารสมัยใหม่ตามรูปแบบของกองทัพสหรัฐอเมริกา ความปลอดภัยด้านสถานที่ที่เหมาะสมในอนาคต ผู้วิจัยจึงขอสรุปโดยแบ่งตามรูปแบบอุปกรณ์การรักษาความปลอดภัยและแบ่งตามความสำคัญของพื้นที่ได้ ๔ ระดับ ระดับที่ ๑ ที่รั้วและพื้นที่ทางเข้าสถานที่ ระดับที่ ๒ จากรั้วจนถึงอาคารและห้องรับรอง ระดับที่ ๓ ภายในห้องรับรอง ระดับที่ ๔ จุดที่ต้องการความปลอดภัยสูง อาทิห้องภายในอาคารที่เก็บทรัพย์สิน หรือเอกสารข้อมูลที่สำคัญ (Restrict Zone) บริเวณห้ามเข้า (Forbidding Zone) พื้นที่เก็บหรือฐานยิงจรวดบรรจุระเบิด

บทนี้ได้นำเสนอข้อมูลเกี่ยวกับรูปแบบการรักษาความปลอดภัยทั้งของประเทศสหรัฐอเมริกา ประเทศในภูมิภาคเอเชีย ประเทศในภูมิภาคอื่นๆ และได้เปรียบเทียบรูปแบบการรักษาความปลอดภัยของประเทศต่างๆ บทต่อไปจะนำข้อมูลที่ได้ไปออกแบบเป็นเครื่องมือวิจัยที่จะนำไปใช้ในการวิเคราะห์เพื่อหาแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต โดยจะเสนอเป็นลำดับต่อไป

บทที่ ๔
แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัย ของกองทัพบกในอนาคต

บทนี้นำเสนอประเด็นสำคัญที่ได้จากการวิจัยประกอบด้วย

๑. การวิเคราะห์แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

๒. รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

๓. สรุป

ประเทศไทยมีการพัฒนาไปอย่างรวดเร็วโดยเฉพาะในยุคประเทศไทย ๔.๐ รวมถึงการเข้าสู่ประชาคมอาเซียน แต่อย่างไรก็ตามการพัฒนาประเทศยังคงเป็นการกระตุ้นให้สภาพความเป็นเมืองขยายตัวออกไปทั่วประเทศ ขณะเดียวกันภัยคุกคามที่หลากหลายและซับซ้อนทั้งจากสถานการณ์ภายในและภายนอกประเทศต่างก็ส่งผลถึงประเทศไทยมากขึ้น ทำให้หน่วยงานต่างๆ ของไทย รวมถึงหน่วยงานทางความมั่นคง โดยเฉพาะกองทัพที่มีหน้าที่รับผิดชอบด้านนี้โดยตรงควรจะต้องเข้าใจรูปแบบและแนวทางการรักษาความปลอดภัยอย่างจริงจัง เนื่องจากเป็นวิธีการหนึ่งในการป้องกันภัยคุกคามให้กับประชาชน อีกทั้งยังเป็นการเสริมสร้างความมั่นคง และรักษาผลประโยชน์ของชาติอีกด้วย สำหรับมาตรการการรักษาความปลอดภัยในประเทศไทยได้มีการดำเนินการตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ซึ่งเน้นไปที่ ๑) การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal Security) และ ๒) การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Physical Security) ซึ่งคลอบคลุมการรักษาความปลอดภัยได้เป็นอย่างดี แต่อย่างไรก็ตามเมื่อสถานการณ์ทางการเมืองของประเทศไทยและโลกมีการเปลี่ยนแปลงอยู่เสมอ รวมถึงเทคโนโลยีที่มีความทันสมัยมากขึ้น ทำให้การรักษาความปลอดภัยต้องมีการปรับปรุงเพื่อรองรับการรักษาความปลอดภัยในอนาคต ทำให้ผู้วิจัยได้ดำเนินการพัฒนาและวิจัยแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต เพื่อเป็นข้อเสนอแนะในการปรับปรุงระเบียบและมาตรฐานที่เกี่ยวข้อง จึงได้ดำเนินการวิจัยเชิงคุณภาพโดยการศึกษาทฤษฎีและแนวคิด รวมถึงเทคโนโลยีที่เกี่ยวข้อง พร้อมทั้งตรวจสอบแนวทางการรักษาความปลอดภัยของกองทัพบกในอนาคตโดยการสัมมนาอิงผู้เชี่ยวชาญ โดยอาศัยความรู้ ความเชี่ยวชาญ และ

ประสบการณ์ของผู้วิจัย ร่วมกับความเห็นของผู้ทรงคุณวุฒิในด้านการรักษาความปลอดภัยที่มีประสิทธิภาพ เพื่อยืนยันแนวทาง แสดงความคิดเห็น และให้ข้อเสนอแนะ จากนั้นนำผลการตรวจสอบไปปรับปรุงแนวทางที่สมบูรณ์และนำเสนอผลในงานวิจัยต่อไป

การวิเคราะห์แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

ผู้วิจัยได้ดำเนินการศึกษาเอกสาร รายงาน งานวิจัยที่เกี่ยวข้อง รายงานการวิจัย และบทความวิชาการ จากนั้นได้ทำการออกแบบเครื่องมือวิจัยและทดสอบการใช้เครื่องมือเชิงคุณภาพโดยผู้เชี่ยวชาญ และดำเนินการรวบรวมข้อมูลเชิงลึกตามกระบวนการวิจัยเชิงคุณภาพโดยการสัมภาษณ์แบบเชิงลึกผู้ที่มีหน้าที่เกี่ยวข้องกับการรักษาความปลอดภัยในกองทัพ จำนวน ๔ ท่าน ดังนี้

๑. พลตรีวัฒนะ พลจันทร์ ผู้ช่วยผู้บัญชาการ ศูนย์รักษาความปลอดภัย กองบัญชาการกองทัพไทย

๒. พันเอกชัยรัตน์ จ่างแก้ว รองผู้บัญชาการ โรงเรียนข่าวทหารบก

๓. พันเอกหญิง ดร.นพมาศสิริ วงศ์บา สำนักงานวิจัยและพัฒนาการทางทหาร กองทัพบก

๔. นายศรายุทธ ทองกูล นักการข่าวเชี่ยวชาญ สำนักข่าวกรองแห่งชาติ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

และดำเนินการสัมภาษณ์แบบเชิงลึกผู้เชี่ยวชาญด้านนวัตกรรมการรักษาความปลอดภัย จำนวน ๓ ท่าน ดังนี้

๑. ดร.เศรษฐชัย ชัยสนิท คณบดี วิทยาเขตชลบุรี คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

๒. ผศ.ดร.พงษ์ศักดิ์ ผกามาศ สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก

๓. ผศ.ดร.ชัยวัฒน์ ประสงค์สร้าง คณะศิลปศาสตร์ มหาวิทยาลัยเทคโลยีราชมงคลรัตนโกสินทร์

จากนั้นได้ดำเนินการสรุปข้อเสนอแนะจากผู้เชี่ยวชาญทั้ง ๗ ท่าน โดยสามารถสรุปเป็นข้อเสนอแนะแนวทางการรักษาความปลอดภัยของกองทัพในอนาคตได้ดังนี้

๑. ข้อเสนอแนะด้านมาตรการการรักษาความปลอดภัย

๑.๑ มาตรการการรักษาความปลอดภัยด้านบุคคล

๑.๑.๑ ควรมีการตรวจสอบข้อมูลประวัติบุคคลก่อนเข้าปฏิบัติงานอย่างละเอียดและดำเนินการอย่างต่อเนื่อง

๑.๑.๒ ควรมีการตรวจสอบข้อมูลประวัติผู้ใกล้ชิดบุคคลที่ปฏิบัติหน้าที่รักษาความปลอดภัย

๑.๑.๓ เจ้าหน้าที่ที่เกี่ยวข้องควรได้รับการอบรมด้านการรักษาความปลอดภัยอย่างต่อเนื่องทั้งบุคลากรใหม่และผู้ปฏิบัติงานเดิม โดยต้องดำเนินการอบรมให้คลอบคลุมทุกมิติทั้งด้านบุคคล ด้านข้อมูลข่าวสาร และด้านสถานที่

๑.๑.๔ ควรมีระบบการตรวจสอบอย่างเข้มงวดและมีการหมุนเวียนบุคคลดูแล มิใช้ให้ดูแลคนเดียวตลอด เพื่อความมั่นคงปลอดภัย

๑.๑.๕ ควรมีการตั้งคณะกรรมการ โดยมีฝ่ายต่างๆ ที่เกี่ยวข้องเข้าร่วมเพื่อกำหนดรูปแบบและประเมินความเสี่ยง

๑.๒ มาตรการการรักษาความปลอดภัยด้านข้อมูลข่าวสาร

๑.๒.๑ ควรมีระเบียบข้อมูลข่าวสาร โดยกำหนดให้มีผู้ปฏิบัติหน้าที่รับผิดชอบโดยตรง

๑.๒.๒ ควรมีการตั้งคณะกรรมการดูแลชั้นความลับต่างๆ แต่ละชั้น เช่น ชั้นความลับมากและชั้นความลับที่สุด เป็นต้น

๑.๒.๓ ควรมีกระบวนการทางเทคโนโลยีที่มีระบบรักษาความปลอดภัยเพิ่มเติม

๑.๒.๔ ควรมีการกำหนดชั้นความลับที่ชัดเจนและมีการสร้างความเข้าใจกับผู้ปฏิบัติงาน

๑.๒.๕ ควรมีการตั้งคณะกรรมการเพื่อวิเคราะห์สถานการณ์ ข่าวสาร บุคคล และสถานที่

๑.๓ มาตรการการรักษาความปลอดภัยด้านสถานที่

๑.๓.๑ ควรจัดให้มีการตรวจับและจัดให้มีการรักษาความปลอดภัยช่องทางเข้าออก

๑.๓.๒ ควรมีการตรวจสิ่งของผู้เข้าออกสถานที่สำคัญและควรมีการนำเทคโนโลยีมาใช่ร่วมด้วย

๑.๓.๓ ควรมีระเบียบการรักษาความปลอดภัยสถานที่โดยเฉพาะ

๑.๓.๔ ควรมีการจัดพื้นที่ห่วงห้ามและกำหนดสิทธ์ที่ชัดเจน

๑.๓.๕ ควรมีการวางมาตรการที่เหมาะสมของแต่ละสถานที่ โดยควรนำข้อเสนอแนะจากผู้เชี่ยวชาญ มีการวิเคราะห์หาจุดอ่อนและควรมีการเพิ่มแสงสว่างในพื้นที่มุมอับต่างๆ

๑.๓.๖ ควรมีการบันทึกบุคคลที่ทำการนัด รวมทั้งมีบุคคลดูแลตลอดเวลา

๑.๓.๗ ควรมีกล้องวงจรปิดเป็นจุดต่างๆโดยจัดเป็นมาตรการเสริม

๑.๓.๘ ควรมีการใช้ฐานข้อมูลที่สามารถตรวจสอบประวัติบุคคลได้ร่วมกันและมีการปรับปรุงให้ทันสมัยตอลดเวลา

๒. ข้อเสนอแนะด้านโครงสร้างและรูปแบบการรักษาความปลอดภัยของหน่วยงาน

๒.๑ ควรมีการดำเนินการโดยใช้โครงสร้างตามสายบังคับบัญชาและมีการมอบหมายหน้าที่การดูแลตามลำดับชั้นและกระจายอำนาจอย่างเหมาะสม

๒.๒ ควรมีการแต่งตั้งคณะกรรมการเฉพาะเพื่อดูแลความปลอดภัยในแต่ละหน่วยงานต่างๆภายใน

๒.๓ ควรมีการดำเนินงานให้มีเครือข่ายการรักษาความปลอดภัยกับหน่วยงานภายนอกและมีการเซ็น MOU ร่วมกับหน่วยงานต่างๆ ภายนอก เพื่อช่วยเหลือทางด้านความปลอดภัยระหว่างหน่วยงาน

๒.๔ ควรมีการสร้างความเข้าใจถึงระเบียบและการรักษาความปลอดภัยให้กับบุคลากรในหน่วยงานทุกระดับชั้นยศ ร่วมถึงสร้างความเข้าใจให้กับชุมชนโดยรอบและประชาชนผู้รับบริการที่มาติดต่อหน่วยงาน

๒.๕ กองทัพควรกำหนดโครงสร้างการบริหารและการจัดการรักษาความปลอดภัยไว้อย่างชัดเจน สำหรับเครื่องมือที่จะนำมาใช้ในการรักษาความปลอดภัย ต้องคำนึงถึงความทันสมัย เหมาะสมกับภารกิจทั้งฮาร์ดแวร์และซอฟแวร์ที่จะนำมาทำเป็นระบบรักษาความปลอดภัยอัตโนมัติที่สามารถป้องกัน ตรวจจับ และหน่วงภัยคุกคามนั้นได้

๓. ข้อเสนอแนะด้านภัยคุกคามใดที่ส่งผลกระทบต่อการรักษาความปลอดภัย

๓.๑ ภัยคุกคามจากธรรมชาติ เช่น ฟ้าผ่าและน้ำท่วม

๓.๒ เป็นภัยคุกคามที่มาจากมนุษย์ และจากความก้าวหน้าของวิทยาศาสตร์และเทคโนโลยี

๓.๓ การบุกรุกของผู้ก่อการร้าย การโจมตีสถานที่ทั้งทางบกและทางอากาศ และการโจมตีทางไซเบอร์ เป็นต้น

๓.๔ ภัยคุกคามโดยมนุษย์เข้ามาอย่างเปิดเผย เช่น ม็อบและฝูงชน

๓.๕ ภัยคุกคามมาอย่างลับๆ โดยอาจแอบเข้ามาที่ผ่านมาจากบุคคลภายใน

๓.๖ ภัยคุกคามทางไซเบอร์ การเจาะระบบทางคอมพิวเตอร์และเครือข่ายต่างๆ

๔. ข้อเสนอแนะเรื่องการเปลี่ยนแปลงด้านการเมืองและสังคมที่ส่งผลกระทบต่อการรักษาความปลอดภัย

๔.๑ ควรมีแผนเผชิญเหตุและมีแผน After Action Review โดยมีการปรับปรุงแผนนี้อย่างต่อเนื่อง

๔.๒ ควรมีระบบปฏิบัติงานเปิดและปฏิบัติงานปิดและมีการตั้งคำสั่งแต่งตั้งผู้บัญชาการดูแลเพื่อป้องกันเหตุต่างๆ อย่างเป็นระบบ

๔.๓ ควรมีการจัดทำแผนเผชิญเหตุรองรับในเหตุการณ์ต่างๆ อย่างเป็นรูปธรรม

๔.๔ ควรมีระบบและการดำเนินการการติดต่อสื่อสารร่วมกับหน่วยงานภายนอกอย่างเป็นระบบและปลอดภัย

๔.๕ การเปลี่ยนแปลงด้านสังคมและการเมืองส่งผลกระทบต่อการรักษาความปลอดภัย โดยหน่วยงานทางความมั่นคง ต้องพิจารณาเป็นพิเศษ เนื่องจากอาจมีผลกระทบต่อระบบรักษาความปลอดภัยได้มากกว่าการเปลี่ยนแปลงด้านอื่นๆ เนื่องจากต้องมีบุคคลจากหลายภาคส่วนเข้ามาเกี่ยวข้องอาทิ กลุ่มการเมือง กลุ่มเศรษฐกิจ ซึ่งความคิด แนวคิดและวัตถุประสงค์ของแต่ละกลุ่มมีหลากหลายและแตกต่าง ดังนั้นระบบการรักษาความปลอดภัยย่อมมีปลกระทบอย่างยิ่งเพราะจะต้องตรวจสอบทั้งด้านข้อมูล พฤติกรรม การประเมินสถานการณ์ เป็นต้น ซึ่งการเปลี่ยนแปลในสังคมยุคนี้มีความแตกต่างจากยุคก่อนอย่างมาก ดังนั้นการรักษาความปลอดภัยจึงเป็นเครื่องมือที่สำคัญ ต้องมีการปรับปรุงและคอยเฝ้าระวังอยู่เสมอ

๔.๖ การเปลี่ยนแปลงทางด้านการเมือง เศรษฐกิจ และสังคม อาจส่งผลกระทบต่อระบบรักษาความปลอดภัยในด้านต่างๆ เช่น การเปลี่ยนแปลงนโยบายของรัฐบาล ความมั่นคงด้านเศรษฐกิจชาติ และการตรวจสอบจากภาคประชาชนต่องบประมาณการใช้จ่ายด้านความมั่นคงปลอดภัย เป็นต้น

๕. ข้อเสนอแนะด้านนวัตกรรมและเทคโนโลยีที่ใช้ในด้านการรักษาความปลอดภัยและแนวโน้มในอนาคต

๕.๑ เทคโนโลยีที่เหมาะสมสำหรับการรักษาความปลอดภัย ได้แก่ เทคโนโลยีสมัยใหม่ที่สามารถเข้ากันได้กับการรักษาความปลอดภัยวิธีปกติ โดยจะต้องเป็นระบบที่มีการวางโครงสร้างที่ชัดเจน มีศักยภาพในการตรวจตราหรือเตือนภัยอย่างรวดเร็วและแม่นยำ มีความสามารถตอบสนองต่อสถานการณ์เฉพาะหน้าได้เร็วกว่าความสามารถของมนุษย์ มีการติดตั้ง

และทดสอบการใช้งานจริง ตลอดจนสามารถปรับปรุงและพัฒนาให้ระบบการรักษาความปลอดภัยมีสมรรถนะที่ดีขึ้นตามการเปลี่ยนแปลงของเทคโนโลยีที่รวดเร็ว

๕.๒ โครงสร้างต้องประกอบไปด้วยระบบหลักทั้งทางด้านฮาร์ดแวร์และซอฟท์แวร์ โดยมีการผสมผสานกับรูปแบบการรักษาความปลอดภัยวิธีปกติ รวมถึงมีการเชื่อมโยงข้อมูลความปลอดภัยอัตโนมัติ (Auto-Synchronize) เพื่อให้สามารถนำมาใช้ในการตรวจสอบ กำกับติดตาม และป้องกันเหตุอันไม่พึงประสงค์กรณีต่างๆ หรือภัยคุกคามที่สามารถมีได้ตลอดเวลา

๕.๓ ควรใช้นวัตกรรมและเทคโนโลยีแบบผสมผสาน (Hybrid) ที่สามารถเชื่อมโยงข้อมูลแบบ Real Time

๕.๔ ควรเป็นระบบป้องกันภัยอิเล็กทรอนิกส์และบนเครือข่ายที่ทำงานแบบบูรณาการเป็นระบบหนึ่งเดียวกัน ซึ่งสามารถทำให้หน่วยงานหรือองค์กรต่างๆสามารถป้องกัน ตรวจจับ ตรวจสอบ และจัดการกับอันตราย เหตุฉุกเฉิน และภัยคุกคามได้แบบ Real Time โดยไม่ต้องพึ่งพนักงานเพิ่มเติม

๕.๕ ควรเป็นระบบที่สามารถจับตาดูเหตุการณ์จากระบบเตือนภัยและกล้องวงจรปิด โดยสามารถส่งข้อมูลไปยังผู้ที่เกี่ยวข้องผ่านโทรศัพท์มือถือหรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ

๕.๖ ควรเป็นระบบสนับสนุนการปฏิบัติงานด้านการรักษาความปลอดภัยที่สามารถบันทึกเหตุการณ์ในสถานการณ์ต่างๆ ได้รวมถึงการเรียกดูย้อนหลังหากต้องการหรือจำเป็น

๕.๗ ควรมีอุปกรณ์ประเภท High Security เข้ามาช่วยเสริมสร้างความปลอดภัยให้กับตัวอาคาร ทั้งภายในและภายนอกอาคารเพื่อป้องกันภัยคุกคามในรูปแบบต่างๆที่อาจเกิดขึ้น

๕.๘ ควรเป็นระบบอัจฉริยะ (Smart Security) ที่มีระบบติดต่อสื่อสารรวดเร็ว มีการเก็บรักษาข้อมูลด้วยเทคโนโลยี Cloud และต้องมีการ Update อุปกรณ์ให้ทันสมัยตามช่วงระยะเวลาเพื่อก่อให้เกิด Safety Zone อย่างมั่นคง

๕.๙ ควรเป็นรูปแบบที่มีโครงสร้างอย่างง่าย (Simple) และเข้ากันได้กับรูปแบบการรักษาความปลอดภัยวิธีปกติเป็นอย่างดี

๕.๑๐ ควรมีนวัตกรรมและเทคโนโลยีที่สามารถตรวจจับอันตราย ระบุหาแหล่งที่มา และจัดการกับภัยคุกคามได้อย่างทันทีและอัตโนมัติ โดยไม่ต้องรอให้ใครคอยกดปุ่มสั่งการ

๕.๑๑ ควรมีนวัตกรรมและเทคโนโลยีที่มีการเชื่อมต่อ Firewall แบบ Next Generation โดยสามารถติดต่อสื่อสาร Real Time แบบต่อเนื่อง

๕.๑๒ ควรมีระบบที่สามารถรองรับภัยคุกคามรูปแบบใหม่รวมถึงภัยแฝงในยุคสงคราม Cyberspace ที่มีรูปแบบการโจมตีที่ระบุที่มาไม่ได้

๕.๑๓ ควรมีระบบอัจฉริยะที่สามารถระบุตัวบุคคลหรือยานพาหนะที่เข้ามาในพื้นที่ผ่านระบบคอมพิวเตอร์และสามารถตัดสินใจได้ว่าบุคคลหรือยานพาหนะนั้นเป็นภัยคุกคามหรือไม่

๕.๑๔ ควรมีระบบที่สามารถประยุกต์ใช้งานด้านอื่นในสถานการณ์ปกติ เช่น การเตือนอัคคีภัยและการเตือนภัยพิบัติจากธรรมชาติที่อาจก่อให้เกิดความเสียหายต่อสถานที่ได้

๕.๑๕ ควรมีกองทัพอาจจะต้องมีการใช้อากาศยานแบบไร้คนขับหรือโดรนเพื่อบินตรวจตรารักษาความปลอดภัยจากมุมสูงที่มีแนวโน้มนำไปสู่การเปลี่ยนรูปแบบและวิธีการรักษาความปลอดภัยในอนาคตไปโดยสิ้นเชิง

๕.๑๖ นโยบายกองทัพควรมีศูนย์ควบคุมระบบกลาง (Convergence Command Center) ที่สามารถเชื่อมต่อกับหน่วยงานความมั่นคงอื่นเพื่อเฝ้าระวังต่อภัยคุกคามต่างๆ ทุกรูปแบบ

๕.๑๗ ผู้บังคับบัญชาสามารถเข้าถึง ตรวจสอบและตัดสินใจได้ง่ายเมื่อเกิดปัญหาฉุกเฉิน

๕.๑๘ เครื่องมือควรประกอบด้วยอุปกรณ์ที่ทันสมัยทั้งทางด้านฮาร์แวร์และซอฟท์แวร์ อาทิเช่น

๕.๑๘.๑ ระบบสัญญาณเตือนภัยเชื่อมต่อกับกล้องวงจรปิดที่รองรับทั้งภาษาไทยและภาษาอังกฤษตลอด ๒๔ ชั่วโมง

๕.๑๘.๒ ระบบ Access Control แบบ Multifunction ซึ่งสามารถควบคุมและบันทึกการเข้า-ออกจากงานได้

๕.๑๘.๓ เครื่องตรวจจับโลหะ (หรือเครื่องตรวจแบบสุ่ม)

๕.๑๘.๔ ระบบจัดการการเข้า-ออกสำหรับผู้มาติดต่องานจากหน่วยงานภายนอก

๕.๑๘.๕ ระบบอัจฉริยะกล้องวงจรปิด CCTV แบบเคลื่อนที่และแบบติดตั้งอยู่กับที่ที่สามารถเตือนภัย ติดตาม และค้นหา รวมถึงซอฟท์แวร์ที่ช่วยในการจดจำ

๕.๑๘.๖ เครื่องตรวจจับการเคลื่อนไหวแบบอินฟาเรดที่สามารถทำงานได้ทั้งภายในอาคารและภายนอกอาคาร

๕.๑๘.๗ ระบบการ Backup ข้อมูลไว้ที่ต่างๆกับหน่วยงานที่น่าเชื่อถือ และระบบออนไลน์ที่ปลอดภัย

๕.๑๘.๘ ระบบ Access Control แบบหลายหลายแบบ เช่น ใช้บัตร ใช้ใบหน้า และใช้นิ้วตรวจสอบ

รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

การหารูปแบบที่เหมาะสมของการรักษาความปลอดภัยจะดำเนินการตรวจสอบแนวทางโดยการสัมมนาอิงผู้เชี่ยวชาญ จำนวน ๕ ท่าน ดังนี้

๑. พลโท อดิศรย์ โครพ ผู้ทรงคุณวุฒิพิเศษกองทัพบก

๒. ดร. ธ ธง พวงสุวรรณ ที่ปรึกษาด้านนวัตกรรมและเทคโนโลยี มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

๓. พันเอกธีระพงษ์ ปานเจริญ หัวหน้าแผนกรักษาความปลอดภัยกอง ๗ ศูนย์รักษาความปลอดภัย กองบัญชาการกองทัพไทย

๔. ดร.ประชา ตันเสนีย์ สมาคมผู้ตรวจสอบแห่งประเทศไทย

๕. นางสาวธัญลักษณ์ กริดาคม นักการข่าวชำนาญการ หัวหน้าฝ่ายรักษาความปลอดภัย สำนักข่าวกรองแห่งชาติ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

อย่างไรก็ตามหลังจากที่ได้ดำเนินการสัมมนาอิงผู้เชี่ยวชาญโดยใช้ข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก สามารถสรุปได้รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคตดังแผนภาพที่ ๔ - ๑ ต่อไปนี้

แผนภาพที่ ๔ - ๑รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

จากแผนภาพสามารถสรุปผลการวิเคราะห์รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคตจากผู้เชี่ยวชาญและการสัมมนาอิงผู้เชี่ยวชาญ พบว่าประกอบด้วย ๖ องค์ประกอบคือ ๑) นโยบายด้านความปลอดภัย ๒) การกำหนดแนวปฏิบัติ โครงสร้างและรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง ๓) นวัตกรรมและเทคโนโลยี ๔) กระบวนการสร้างความเข้าใจกับประชาชนและเจ้าหน้าที่ และ ๕) การบริหารและการประเมินความเสี่ยง ซึ่งสามารถสรุปได้ดังนี้

๑. นโยบายด้านความปลอดภัย

รัฐควรกำหนดนโยบายด้านความปลอดภัย รวมถึงมีการกำหนดระเบียบปฏิบัติเพื่อรักษาความปลอดภัยสถานที่ของแต่ละส่วนแต่ละหน่วยงานที่เหมาะสมชัดเจน เนื่องจากหน่วยงานของรัฐย่อมมีความแตกต่างกันไปตามสภาพแวดล้อม ความจำเป็นที่เผชิญอยู่ ดังนั้นเพื่อให้การวางระเบียบปฏิบัติในแต่ละหน่วยงานเป็นไปอย่างเหมาะสม ครอบคลุมสภาพการณ์ และเพื่อให้ผู้ปฏิบัติสามารถปฏิบัติตามได้จริง จึงควรพิจารณาจากตัวชี้วัดดังนี้

๑.๑ ภารกิจ หน้าที่ และความรับผิดชอบของหน่วยงาน

๑.๒ สภาพแวดล้อมและสถานการณ์ที่เผชิญอยู่

๑.๓ จำนวนเจ้าหน้าที่ที่ปฏิบัติงาน และเจ้าหน้าที่รักษาความปลอดภัย

๑.๔ งบประมาณสำหรับการรักษาความปลอดภัยและการสนับสนุนจากผู้บังคับบัญชา

๑.๕ ข่าวสาร สิ่งบอกเหตุ และการแจ้งเตือนภัย

๑.๖ การวิจัยและพัฒนานวัตกรรมและเทคโนโลยี

๑.๗ การติดต่อสื่อสารภายในหน่วยงาน และกับหน่วยงานของรัฐอื่นๆ

๑.๘ รายงานผลการสำรวจหรือการตรวจสอบการรักษาความปลอดภัยที่ได้เคยกระทำมา

อย่างไรก็ตามการดำเนินการด้านป้องกันและแก้ไขปัญหาการก่อการร้ายทุกรูปแบบเป็นอีกปัจจัยที่มีความสำคัญสูงในปัจจุบันจึงเห็นควรให้มีการกำหนดนโยบายและให้ความสำคัญกับปัญหาด้านนี้โดยเฉพาะ โดยมีความจำเป็นต้องสร้างนโยบายที่สามารถลดปัจจัยและเงื่อนไขที่เกื้อกูลต่อการก่อการร้าย การป้องกันมิให้กลุ่มก่อการร้าย บุคคลหรือกลุ่มบุคคลที่สนับสนุนการก่อการร้ายทุกรูปแบบใช้พื้นที่ในอาณาเขตประเทศไทยเป็นพื้นที่พักพิง พื้นที่แสวงหาปัจจัย เพื่อสนับสนุนการก่อการร้าย ตลอดจนเป็นพื้นที่ก่อความรุนแรงหรือกระทำการก่อการร้าย โดยมุ่งเน้นให้เป็นนโยบายระยะยาวและระยะสั้น พร้อมทั้งมีการกำหนดมาตรการเชิงรุกและเชิงรับ รวมถึงการกำหนดแนวปฏิบัติที่ชัดเจน

๒. การกำหนดแนวปฏิบัติ โครงสร้าง และรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง

ควรกำหนดให้มีหน่วยรับผิดชอบในทุกนโยบาย ทั้งหน่วยรับผิดชอบหลักและหน่วย รับผิดชอบร่วม โดยกำหนดให้นโยบายแต่ละเรื่องมีหน่วยงานรับผิดชอบหลักที่เป็นเจ้าภาพบูรณาการนโยบายหนึ่งหน่วยงาน ยกเว้นกรณีที่สาระสำคัญของนโยบายมีลักษณะภารกิจที่แตกต่างกันอย่างชัดเจนให้พิจารณา ตามความเหมาะสม หรือมีการจัดตั้งคณะกรรมการร่วม และกำหนดให้มีหน่วยรับผิดชอบหลักตามแนวนโยบายย่อยทุกข้อ เพื่อสนับสนุนการดำเนินการของเจ้าภาพบูรณาการนโยบาย เนื่องจากสาระสำคัญของนโยบายอาจมีประเด็นดำเนินการที่สำคัญในหลายด้านที่แตกต่างกัน เพื่อให้การขับเคลื่อนนโยบายมีหน่วยรับผิดชอบอย่างครบถ้วนชัดเจนและสามารถนำมาใช้เป็นแนวปฏิบัติและมาตรการการรักษาความปลอดภัยได้

ควรมีการปรับและสร้างศูนย์ป้องกันความปลอดภัยแห่งชาติ ซึ่งมีภารกิจในการให้คำแนะนำด้านการรักษาความปลอดภัยให้กับภาคธุรกิจ ภาคบริการ ภาคอุตสาหกรรม ภาครัฐ และองค์กรต่างๆ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานแห่งชาติ เพื่อลดจุดอ่อนที่อาจจะถูกโจมตีจากภัยคุกคามต่างๆ โดยศูนย์ป้องกันความปลอดภัยดังกล่าวควรปฏิบัติงานร่วมกับหน่วยงานทางความมั่นคงเดิมที่มีอยู่ ทั้งนี้ควรส่งเสริมให้เกิดความร่วมมือระหว่างผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของทุกภาคส่วน นอกจากนี้ควรเป็นส่วนประสานงานหรือสร้างความร่วมมือกับรัฐบาลในภูมิภาคอาเซียนและประเทศอื่นๆ เพื่อแลกเปลี่ยนข่าวสารและความเชี่ยวชาญเฉพาะด้าน นอกจากนี้ควรเป็นผู้กำหนดแผนการรองรับเหตุต่างๆ ตามระดับของสถานการณ์และหน่วยงานที่รับผิดชอบ ทั้งยังเป็นหน่วยงานหลักที่ให้ข่าวสารหรือสื่อสารข้อมูลที่น่าเชื่อถือไปยังประชาชนและหน่วยงานต่างๆ ทราบ

อย่างไรก็ตามเพื่อไม่ให้เกิดความสับสนควรมีการดำเนินการโดยใช้โครงสร้างตามสายบังคับบัญชาและมีการมอบหมายหน้าที่การดูแลตามลำดับชั้นและกระจายอำนาจอย่างเหมาะสม และมีการแต่งตั้งคณะกรรมการเฉพาะเพื่อดูแลความปลอดภัยในแต่ละหน่วยงานต่างๆ ภายใน ควรมีสร้างเครือข่ายการรักษาความปลอดภัยกับประชาชน ชุมชน และหน่วยงานภายนอก เพื่อช่วยเหลือทางด้านความปลอดภัยระหว่างหน่วยงาน ควรสร้างความเข้าใจและความสำคัญของการรักษาความปลอดภัยให้กับนักเรียน นักศึกษาและประชาชน รวมถึงบุคลากรในหน่วยงานต่างๆ ทุกระดับชั้นยศ

นอกจากนี้ควรกำหนดให้กองทัพมีโครงสร้างการบริหารและการจัดการรักษาความปลอดภัยไว้อย่างชัดเจน สำหรับเครื่องมือที่จะนำมาใช้ในการรักษาความปลอดภัยต้องคำนึงถึงความทันสมัย เหมาะสมกับภารกิจทั้งฮาร์ดแวร์และซอฟแวร์ที่จะนำมาทำเป็นระบบรักษาความปลอดภัยอัตโนมัติที่สามารถป้องกัน ตรวจจับ เฝ้าระวัง และหน่วงภัยคุกคามนั้นได้ กรณีที่

สำคัญคืองานด้านข่าวกรองที่มีคุณภาพและแจ้งเตือนภัยล่วงหน้าอย่างมีประสิทธิภาพ ทั้งภัยคุกคามต่อความมั่นคงแห่งชาติและความเคลื่อนไหวที่สนับสนุนการเสริมสร้างความมั่นคงและผลประโยชน์แห่งชาติ การเสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง และหน่วย งานภาครัฐ รวมทั้งหน่วยงานข่าวกรองต่างประเทศ และมีเครือข่ายด้านข้อมูลข่าวสารกับภาคเอกชน ภาคประชาชน และเสริมสร้างพัฒนาขีดความสามารถของระบบงานข่าวกรองอย่างต่อเนื่อง

๓. นวัตกรรมและเทคโนโลยี

ควรส่งเสริมการพัฒนาศักยภาพทางนวัตกรรมและเทคโนโลยี โดยส่งเสริมการวิจัย พัฒนา และจดสิทธิบัตรนวัตกรรมและเทคโนโลยีที่ผลิตโดยคนไทย การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยโดยเน้นการพัฒนาทั้งฮาร์ดแวร์และซอฟแวร์ อาทิ

๓.๑ ระบบสัญญาณเตือนภัยเชื่อมต่อกับกล้องวงจรปิดที่สามารถรองรับหลากหลายภาษา

๓.๒ เครื่องตรวจจับโลหะที่มีประสิทธิภาพและมีราคาที่เหมาะสม

๓.๓ ระบบกล้องวงจรปิด CCTV อัจฉริยะ แบบเคลื่อนที่และแบบติดตั้งอยู่กับที่ที่สามารถเตือนภัย ติดตาม และค้นหา รวมถึงซอฟท์แวร์ที่ช่วยในการจดจำใบหน้าบุคคลที่สามารถเชื่อมต่อกับระบบฐานข้อมูลของหน่วยงานทางความมั่นคงได้

๓.๔ เครื่องตรวจจับการเคลื่อนไหว โดยมีเซ็นเซอร์ที่แม่นยำและสามารถทำงานได้ทั้งภายในอาคารและภายนอกอาคาร

๓.๕ ระบบการสำรองข้อมูลที่น่าเชื่อถือ และระบบการสื่อสารออนไลน์ที่ปลอดภัย

๓.๖ ระบบ Access Control แบบใช้ไบโอเมตทริกซ์ที่สามารถตรวจสอบและเก็บข้อมูลอัตลักษณ์บุคคล รวมถึงการตรวจสอบลักษณะทางกายภาพ (Physiological Biometrics) และการตรวจสอบลักษณะทางพฤติกรรม (Behavioural Biometrics) ได้

นอกจากนี้ควรมีการพัฒนาระบบการบูรณาการเชื่อมโยงระบบฐานข้อมูลภาครัฐ การพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ รวมถึงการใช้ระบบอิเล็กทรอนิกส์ เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานทางความมั่นคง ระบบคลาวด์ทางความมั่นคง ตลอดจนการพัฒนาบุคลากรภาครัฐ องค์กรทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ ความชำนาญทางด้านนวัตกรรมและเทคโนโลยีและการรักษาความปลอดภัย เพื่อให้บุคลากรทุกภาคส่วนที่เกี่ยวข้องมีข้อมูลข่าวสารและความรู้ทางด้านเทคโนโลยีที่ทันสมัย รวมถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการพัฒนาบุคลากรทางด้านการรักษาความปลอดภัย

การปกป้องและป้องกันภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยการบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานต่าง ๆ การประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ บุคลากร องค์กร และผู้เชี่ยวชาญทางด้านการรักษา ความมั่นคงทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างประเทศ การเฝ้าระวังและการพัฒนาระบบป้องกัน การโจมตีระบบสารสนเทศ การพัฒนาความพร้อมต่อสงครามไซเบอร์ การปกป้องโครงสร้างพื้นฐานที่รวมถึงการสำรองข้อมูลที่เหมาะสม

ท้ายที่สุดในประเด็นมาตรฐานการรักษาความปลอดภัยควรมีการพัฒนากฎหมายระเบียบข้อบังคับเพื่อความมั่นคงที่ทันสมัย เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอยู่ตลอดเวลา รวมถึงควรมีการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันการคุกคามทางกายภาพ ทั้งด้านบุคคล ด้านสถานที่ ด้านข่าวสาร รวมถึงอาชญากรรมไซเบอร์ ให้สามารถลดภัยคุกคามหรืออันตรายที่ส่งผลกระทบกับบุคคล ข้อมูล และเทคโนโลยีต่างๆ โดยเฉพาะ ทั้งนี้อาจรวมถึงการเฝ้าระวังภัยคุกคามต่างๆ อย่างมีมาตรฐานอีกด้วย

๔. กระบวนการสร้างความเข้าใจกับประชาชนและเจ้าหน้าที่

ในกระบวนการนี้ควรมีการผนึกกำลังทุกภาคส่วนให้พร้อมเผชิญปัญหาและภัยคุกคามความมั่นคง โดยการเปิดโอกาสให้ทุกภาคส่วนมีส่วนร่วมกำหนดแนวทางการพัฒนาการป้องกันและแก้ปัญหา โดยเฉพาะการเสริมสร้างความมั่นคงของชาติในระดับพื้นที่ให้มีภูมิคุ้มกันอยู่เสมอ มีความพร้อมเผชิญปัญหาและภัยคุกคามความมั่นคง รวมถึงสามารถผนึกกำลังประชาชนหรือกลุ่มพลังมวลชนเพื่อสนับสนุนหน่วยงานทางความมั่นคงของประเทศในการเผชิญกับสถานการณ์ต่างๆ ตลอดจนการส่งเสริมมิติด้านวัฒนธรรมและภูมิปัญญาชุมชน/ท้องถิ่น และการจัดการศึกษาที่สะท้อนถึงความตระหนักในหน้าที่และการมีส่วนร่วมในการรักษาความปลอดภัยแห่งชาติ ในอนาคตก็ควรจะบรรจุอยู่ในหลักสูตรการเรียนการสอนในสถาบันการศึกษาต่างๆ เพื่อให้การรักษาความปลอดภัยของประเทศเป็นวาระแห่งชาติ

จากการวิเคราะห์ผลการวิจัยในองค์ประกอบของรูปแบบระบบรักษาความปลอดภัยที่เหมาะสมดังกล่าวมาข้างต้น ผู้เชี่ยวชาญได้เสนอสมรรถนะและเกณฑ์ในการปฏิบัติงานเพื่อให้กระบวนการรักษาความปลอดภัยมีมาตรฐานในทางปฏิบัติและสามารถเชื่อมโยงกับภารกิจหลักของหน่วยงานไว้ดังตารางที่ ๔ – ๑ ต่อไปนี้

คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

หน่วยสมรรถนะนี้เป็นหน่วยที่เกี่ยวกับทักษะและความรู้ที่จำเป็นในการปฏิบัติตามระเบียบการรักษาความปลอดภัย ซึ่งเกี่ยวข้องกับการระบุสิ่งที่จำเป็นต่อความปลอดภัยและการรักษาความปลอดภัย การปฏิบัติตามมาตรการป้องกันความปลอดภัยและขั้นตอนการรักษาความปลอดภัย การตอบสนองต่อสถานการณ์ฉุกเฉิน และการให้ข้อเสนอแนะในการจัดการเกี่ยวกับมาตรการความปลอดภัยและการรักษาความปลอดภัย

ตารางที่ ๔ - ๑ สมรรถนะย่อยและเกณฑ์ในการปฏิบัติงาน

สมรรถนะย่อย **Element of Competency**	**เกณฑ์ในการปฏิบัติงาน** **Performance Criteria**
๑. ระบุสิ่งที่จำเป็นต่อความปลอดภัยและการรักษาความปลอดภัย	๑.๑ อธิบายกฎหมายความปลอดภัยและข้อกำหนดของการรักษาความปลอดภัย ๑.๒ อธิบายนโยบายและระเบียบวิธีการปฏิบัติงานด้านความปลอดภัยและการรักษาความปลอดภัยขององค์กร ๑.๓ ระบุทรัพยากรที่ใช้สนับสนุนด้านความปลอดภัยและมาตรการรักษาความปลอดภัย ๑.๔ อธิบายผลที่จะเกิดขึ้นจากการไม่ปฏิบัติตามมาตรการความปลอดภัยและขั้นตอนการรักษาความปลอดภัย ๑.๕ ชี้แจงขอบเขตอำนาจหน้าที่และความรับผิดชอบของแต่ละบุคคลในส่วนที่เกี่ยวข้องกับความปลอดภัยและการรักษาความปลอดภัย ๑.๖ ค้นคว้าหาข้อมูลความปลอดภัยและการรักษาความปลอดภัยหรือเหตุการณ์ต่างๆ ที่กำลังเกิดขึ้นและมีผลต่อความปลอดภัย

ตารางที่ ๔ - ๑ สมรรถนะย่อยและเกณฑ์ในการปฏิบัติงาน (ต่อ)

สมรรถนะย่อย **Element of Competency**	**เกณฑ์ในการปฏิบัติงาน** **Performance Criteria**
๒. ปฏิบัติตามมาตรการป้องกันความปลอดภัยและขั้นตอนการรักษาความปลอดภัย	๒.๑ ให้ข้อมูลเกี่ยวกับมาตรการความปลอดภัยและการรักษาความปลอดภัยแก่ผู้อื่น ๒.๒ ติดตามตรวจสอบความปลอดภัยและการรักษาความปลอดภัยตามที่ได้มีการระบุขอบเขตไว้ ๒.๓ ปฏิบัติตามมาตรการรักษาความปลอดภัยและขั้นตอนการปฏิบัติงานในการควบคุมความปลอดภัย ๒.๔ ดำเนินการเพื่อรับมือกับความเสี่ยงที่มีอยู่ในกิจวัตรประจำวันและการละเมิดมาตราการความปลอดภัย ๒.๕ สอบสวนบุคคลผู้ต้องสงสัยและสถานการณ์ที่ผิดปกติต่างๆ ๒.๖ ขอความช่วยเหลือด้านความปลอดภัยหรือขอให้ช่วยรักษาความปลอดภัยจากบุคคลที่เกี่ยวข้อง ๒.๗ รายงานความเสี่ยงที่ร้ายแรง สิ่งที่เป็นอันตราย และการละเมิดมาตรการความปลอดภัย ๒.๘ จัดทำเอกสารต่างๆ ที่เกี่ยวกับความปลอดภัยและการรักษาความปลอดภัย

ตารางที่ ๔ - ๑ สมรรถนะย่อยและเกณฑ์ในการปฏิบัติงาน (ต่อ)

สมรรถนะย่อย **Element of Competency**	**เกณฑ์ในการปฏิบัติงาน** **Performance Criteria**
๓. ตอบสนองต่อสถานการณ์ฉุกเฉิน	๓.๑ ระบุและประเมินสถานการณ์ฉุกเฉิน ๓.๒ ตัดสินใจดำเนินการสิ่งใดสิ่งหนึ่งเพื่อรับมือกับสถานการณ์หรือเหตุการณ์ฉุกเฉินนั้นๆ ๓.๓ ปฏิบัติตามขั้นตอนการรับมือกับเหตุการณ์ฉุกเฉิน ๓.๔ ขอความช่วยเหลือจากบุคคลที่เกี่ยวข้องเพื่อช่วยอำนวยความสะดวกในการรับมือหรือตอบสนองต่อสถานการณ์ฉุกเฉินนั้นๆ ๓.๕ ทำการบันทึกสิ่งที่ได้กระทำลงไปเพื่อรับมือกับสถานการณ์ฉุกเฉิน
๔. ให้ข้อเสนอแนะในการจัดการเกี่ยวกับมาตรการความปลอดภัยและการรักษาความปลอดภัย	๔.๑ ระบุประเด็นที่ต้องให้ความสนใจ ๔.๒ ชี้ประเด็นปัญหาในการจัดการ ๔.๓ แนะนำวิธีหรือมาตรการแก้ไขปัญหาที่ระบุ

ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

๑. ความต้องการด้านทักษะ

ทักษะการสื่อสารความเป็นผู้นำระหว่างบุคคลและทักษะการเจรจาต่อรอง

๒. ความต้องการด้านความรู้

- นโยบายขององค์กรและวิธีการปฏิบัติที่เกี่ยวกับความปลอดภัยและการรักษาความปลอดภัย

- ภาพรวมของกฎหมายที่เกี่ยวข้องกับความปลอดภัยและการรักษาความปลอดภัยของประเทศ

- กฎหมายที่เกี่ยวข้องกับความปลอดภัยขององค์กรท้องถิ่น และกฎหมายที่เกี่ยวข้องกับความปลอดภัยในองค์กร

- ความรู้เกี่ยวกับสาเหตุของการเกิดอุบัติเหตุ การบาดเจ็บ และการละเมิดการรักษาความปลอดภัย

- หลักการของการบริหารความเสี่ยง

- ความรู้เกี่ยวกับหน่วยงานที่ให้บริการช่วยเหลือฉุกเฉินในพื้นที่

๕. การบริหารความเสี่ยงและการประเมินความเสี่ยง

บริบทการเปลี่ยนแปลงที่นำไปสู่ภัยคุกคามรูปแบบใหม่อื่นๆ โดยปัจจุบันถือว่าภัยคุกคามความมั่นคงมีขอบเขตที่กว้างขวาง มีความเชื่อมโยง ซับซ้อน และส่งผลกระทบต่อประชาชนโดยตรงมากยิ่งขึ้น ภัยคุกคามความมั่นคงรูปแบบใหม่ประกอบด้วยภัยที่เกิดจากการเปลี่ยนแปลงที่เชื่อมโยงกับบริบทโลกในมิติต่างๆ ทั้งมิติด้านเศรษฐกิจ สังคม และการเมือง รวมถึงการเปลี่ยนแปลงของสภาพภูมิอากาศของโลก ผลจากการพัฒนาประเทศที่ผ่านมาประกอบกับการใช้ทรัพยากรธรรมชาติโดยขาดความสมดุลได้ส่งผลกระทบต่อความมั่นคงของมนุษย์ ปัญหาความมั่นคงทางอาหาร ปัญหาความเสื่อมโทรมของทรัพยากรธรรมชาติและสิ่งแวดล้อม ปัญหาความขัดแย้งแย่งชิงทรัพยากรที่ส่งผลต่อเนื่องเป็นความขัดแย้งระหว่างประชาชนและความขัดแย้งกับหน่วยงานภาครัฐ นอกจากนี้ประเทศกำลังพัฒนาจะตกเป็นเป้าหมายการโจมตีมากขึ้นเพราะมีความล้าหลังทางเทคโนโลยีและขาดความรู้ในการกำหนดมาตรการป้องกันที่ต้องใช้ผู้ที่มีความชำนาญเฉพาะทาง นอกจากนี้อิทธิพลของสื่อประเภทเครือข่ายสังคมเป็นเครื่องมือสำคัญของประชาชน แต่สื่อดังกล่าวมีโอกาสถูกนำมาใช้ในทางที่ผิด เพื่อโจมตีบ่อนทำลาย หรือบิดเบือนข้อเท็จจริง รวมถึงการแพร่กระจายถ้อยคำที่สร้างความเกลียดชังที่มีฐานมาจากอคติทำให้เกิดความเกลียดชังและปัญหาความแตกแยกภายในประเทศ รวมถึงส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศอีกด้วย จากความเสี่ยงดังกล่าวควรมีการจัดการและประเมินความเสี่ยงที่จะเกิดขึ้นตลอดเวลารวมถึงการจัดการบริหารความเสี่ยงอีกด้วย

การพิจารณามาตรฐานด้านการรักษาความปลอดภัยที่ดีนั้นควรจะมีโครงการหรือกิจกรรมที่เกี่ยวข้องกับมาตรการรักษาความปลอดภัย ทั้งนี้เพื่อให้สามารถพัฒนารูปแบบหรือวิธีการที่จะเผชิญกับภัยคุกคามได้อย่างทันท่วงทีและได้มาตรฐาน โดยเฉพาะอย่างยิ่งการฝึกซ้อมเสมือนจริงและการนำไปสู่การพัฒนารูปแบบหรือวิธีการรักษาความปลอดภัยให้มีประสิทธิภาพและประสิทธิผลเพิ่มขึ้นอย่างต่อเนื่องในอนาคต ตัวอย่างโครงการและกิจกรรมการรักษาความปลอดภัยของกองทัพบกมีดังนี้

๑) โครงการฝึกซ้อมเพื่อป้องกันการก่อการร้าย

หลักการและเหตุผล

หน่วยทหารของกองทัพบกนอกจากมีหน้าที่ปฏิบัติภารกิจหลักตามที่ได้รับมอบหมายจากหน่วยงานต้นสังกัดแล้วยังต้องมีการฝึกซ้อมแผนป้องกันการก่อการร้ายเพื่อให้เกิดความปลอดภัยต่อการปฏิบัติหน้าที่อีกด้วย ดังนั้นจึงจำเป็นอย่างยิ่งที่หน่วยทหารทุกหน่วยต้องมีความเข้าใจในแผนการฝึกซ้อมด้านความปลอดภัย ซึ่งจะช่วยให้ผู้มีส่วนเกี่ยวข้องเกิดการรับรู้และเข้าใจเพื่อนำไปสู่การรักษาความปลอดภัยอย่างเป็นระบบและได้มาตรฐาน

วัตถุประสงค์

๑. เพื่อรักษารูปแบบและพัฒนามาตรฐานการรักษาความปลอดภัยในหน่วยงานสังกัดกองทัพบก

๒. เพื่อฝึกซ้อมกำลังพลและผู้มีส่วนเกี่ยวข้องให้ได้รับรู้และเข้าใจถึงมาตรการเชิงรุกในการรักษาความปลอดภัยสถานที่ราชการ

๓. เพื่อกระตุ้นจิตสำนึกและวินัยในด้านการรักษาความปลอดภัยให้กับกำลังพล

เป้าหมาย

ผู้รับผิดชอบด้านการรักษาความปลอดภัยจัดรูปแบบการฝึกซ้อมเพื่อเผชิญกับภัยการก่อการร้ายหรือการคุกคามที่มิอาจทราบล่วงหน้า โดยดำเนินการตามแผนการรักษาความปลอดภัยและมีรายงานสรุปอย่างเป็นระบบ

ขั้นตอนการดำเนินงาน/กิจกรรม/เวลา

ที่	งาน/กิจกรรม	เวลา	ผู้รับผิดชอบ	หมายเหตุ

แผนการปฏิบัติงาน/กิจกรรม (ระบุย่อยรายละเอียดแต่ละหัวข้อกิจกรรมจากตารางข้างต้น)

ที่	งาน/กิจกรรม	วิธีการ/สถานที่ เวลา	ผู้รับผิดชอบ	หมายเหตุ

งบประมาณและทรัพยากร

งบประมาณและทรัพยากรจากกองทัพบก

การติดตามและประเมินผล

ตัวชี้วัดความสำเร็จ	วิธีวัดและประเมินผล	เครื่องมือวัดและประเมินผล	ผู้รับผิดชอบ

ผลที่คาดว่าจะได้รับ

๑. หน่วยงานของกองทัพบกสามารถรับมือกับภัยการก่อการร้ายหรือภัยคุกคามได้อย่างทันท่วงทีและสามารถรักษาหน่วยงานให้ดำรงอยู่ได้อย่างปลอดภัย

๒. กำลังพลของกองทัพบกและผู้มีส่วนเกี่ยวข้องมีความรู้ความเข้าใจเกี่ยวกับแผนปฏิบัติการรักษาความปลอดภัย และสามารถพัฒนาขีดความสามารถในการปฏิบัติให้มีมาตรฐานมากขึ้น

๓. กำลังพลของกองทัพบกมีวินัยในการปฏิบัติหน้าที่ด้านการรักษาความปลอดภัยและสามารถพัฒนาขีดความสามารถในการปฏิบัติให้มีสมรรถนะสูงขึ้น

๒) โครงการทดสอบระบบการรักษาความปลอดภัย

หลักการและเหตุผล

หน่วยทหารของกองทัพบกนอกจากมีหน้าที่ปฏิบัติภารกิจหลักตามที่ได้รับมอบหมายจากหน่วยงานต้นสังกัดแล้วยังต้องมีการทดสอบระบบการรักษาความปลอดภัยอย่างต่อเนื่อง โดยระบบนี้อาจประกอบไปด้วยโครงสร้างพื้นฐานทั้งทางด้านฮาร์ดแวร์ ซอฟต์แวร์ และกำลังพลที่รับผิดชอบงานด้านความปลอดภัย โครงการนี้อาจดำเนินการควบคู่ไปกับโครงการฝึกซ้อมแผนป้องกันการก่อการร้ายปกติ ดังนั้นจึงจำเป็นอย่างยิ่งที่หน่วยทหารทุกหน่วยต้องมีความรู้ความเข้าใจในการทดสอบระบบรักษาความปลอดภัย ซึ่งจะช่วยให้ระบบรักษาความปลอดภัยสามารถดำเนินการได้อย่างมีประสิทธิภาพอย่างต่อเนื่องตามมาตรฐานความปลอดภัยที่กำหนด

วัตถุประสงค์

๑. เพื่อการทดสอบระบบรักษาความปลอดภัยให้สามารถทำงานได้อย่างมีประสิทธิภาพควบคู่ไปกับแผนฝึกซ้อมการก่อการร้ายปกติในหน่วยงานสังกัดกองทัพบก

๒. เพื่อการพัฒนาระบบและมาตรฐานการรักษาความปลอดภัยให้สามารถรับมือกับเหตุฉุกเฉินหรือสถานการณ์ไม่ปกติ

เป้าหมาย

ผู้รับผิดชอบด้านการรักษาความปลอดภัยจัดรูปแบบการทดสอบระบบรักษาความปลอดภัยเพื่อเผชิญกับภัยการก่อการร้ายหรือการคุกคามที่มิอาจทราบล่วงหน้า ดำเนินการควบคู่กับแผนฝึกซ้อมการรักษาความปลอดภัยปกติและมีรายงานสรุปอย่างเป็นระบบ

ขั้นตอนการดำเนินงาน/กิจกรรม/เวลา

ที่	งาน/กิจกรรม	เวลา	ผู้รับผิดชอบ	หมายเหตุ

แผนการปฏิบัติงาน/กิจกรรม (ระบุย่อยรายละเอียดแต่ละหัวข้อกิจกรรมจากตารางข้างต้น)

ที่	งาน/กิจกรรม	วิธีการ/สถานที่ เวลา	ผู้รับผิดชอบ	หมายเหตุ

งบประมาณและทรัพยากร

งบประมาณและทรัพยากรจากกองทัพบก

การติดตามและประเมินผล

ตัวชี้วัดความสำเร็จ	วิธีวัดและประเมินผล	เครื่องมือวัดและประเมินผล	ผู้รับผิดชอบ

ผลที่คาดว่าจะได้รับ

๑. หน่วยงานของกองทัพบกสามารถทราบถึงขีดความสามารถของระบบรักษาความปลอดภัยและสามารถรับมือกับภัยการก่อการร้ายหรือภัยคุกคามได้อย่างทันท่วงที

๒. กำลังพลของกองทัพบกและผู้มีส่วนเกี่ยวข้องกับงานด้านความปลอดภัยสามารถใช้ประโยชน์จากระบบรักษาความปลอดภัยอย่างเต็มความสามรถ โดยมีความรู้ความเข้าใจเกี่ยวกับการใช้งานและสามารถพัฒนาขีดความสามารถในการรักษาความปลอดภัยให้มีมาตรฐานยิ่งขึ้น

๓) โครงการให้ความรู้ความเข้าใจต่อสงครามไซเบอร์

หลักการและเหตุผล

สงครามไซเบอร์นับเป็นภัยคุกคามรูปแบบใหม่ในระบบคอมพิวเตอร์และเทคโนโลยีสารสนเทศของหน่วยงานทุกหน่วยโดยเฉพาะอย่างยิ่งหน่วยงานทางความมั่นคง การรักษาความปลอดภัยของข้อมูลข่าวสารที่สำคัญของประเทศรวมถึงงานทางความมั่นคงย่อมเป็นหน้าที่ของผู้รับผิดชอบทุกคน ดังนั้นจึงจำเป็นอย่างยิ่งที่หน่วยทหารทุกหน่วยต้องมีความรู้ความเข้าใจในสงครามไซเบอร์ การพัฒนาทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ความชำนาญทางด้านระบบไอซีทีและการรักษาความปลอดภัยทางไซเบอร์ที่ทันสมัย และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ซึ่งจะช่วยให้รักษาความปลอดภัยข้อมูลข่าวสารสำคัญของประเทศเป็นไปอย่างมีประสิทธิภาพ

วัตถุประสงค์

๑. เพื่อเผยแพร่ข้อมูลและรับรู้รูปแบบของสงครามไซเบอร์ที่อาจสร้างความเสียหายด้านข้อมูลของกองทัพ

๒. เพื่อให้เกิดความรู้ความเข้าใจในสงครามไซเบอร์และสามารถดำเนินการตามมาตรการรักษาความปลอดภัยของข้อมูลสำคัญได้

๓. เพื่อการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพเพิ่มขึ้น

เป้าหมาย

ผู้รับผิดชอบด้านการรักษาความปลอดภัยของข้อมูลด้านความมั่นคงสามารถรับรู้รูปแบบของสงครามไซเบอร์ การป้องกันการโจรกรรมข้อมูล การปกป้องโครงสร้างพื้นฐานด้านไอซีที รวมถึงการสร้างความตระหนักรู้ให้กับกำลังพลเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ที่เป็นภัยต่อประเทศชาติ

ขั้นตอนการดำเนินงาน/กิจกรรม/เวลา

ที่	งาน/กิจกรรม	เวลา	ผู้รับผิดชอบ	หมายเหตุ

แผนการปฏิบัติงาน/กิจกรรม (ระบุย่อยรายละเอียดแต่ละหัวข้อกิจกรรมจากตารางข้างต้น)

ที่	งาน/กิจกรรม	วิธีการ/สถานที่ เวลา	ผู้รับผิดชอบ	หมายเหตุ

งบประมาณและทรัพยากร

งบประมาณและทรัพยากรจากกองทัพบก

การติดตามและประเมินผล

ตัวชี้วัดความสำเร็จ	วิธีวัดและประเมินผล	เครื่องมือวัดและประเมินผล	ผู้รับผิดชอบ

ผลที่คาดว่าจะได้รับ

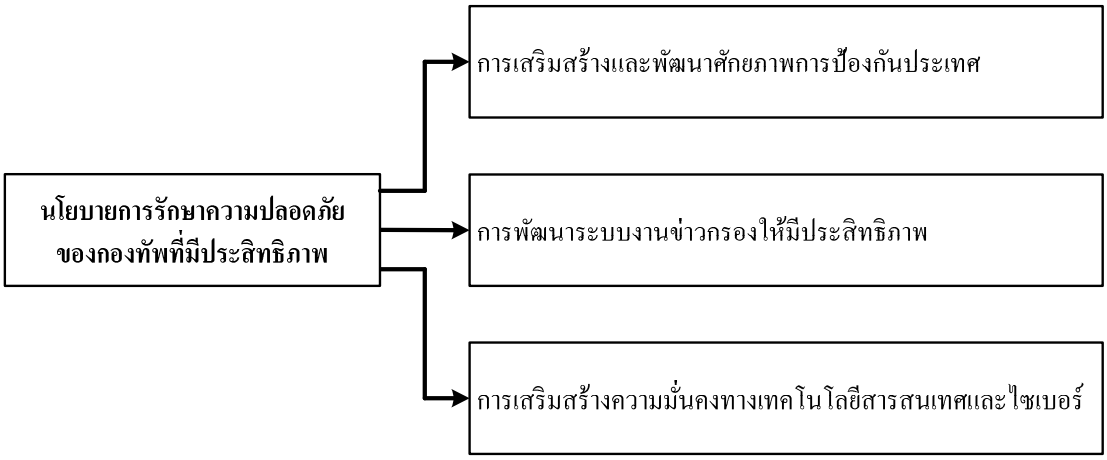
๑. บุคลากรของกองทัพบกสามารถทราบถึงระดับและรูปแบบของสงครามไซเบอร์ที่เป็นภัยต่อความมั่นคงด้านข้อมูลไอซีทีและความลับ รวมถึงสามารถรับมือกับภัยนี้ได้อย่างทันท่วงทีและมีประสิทธิภาพ

๒. ข้อมูลข่าวสารและความลับที่เกี่ยวข้องกับงานทางความมั่นคงได้รับการปกป้องอย่างมีรูปแบบและสามารถพัฒนาขีดความสามารถในการรักษาความปลอดภัยของข้อมูลให้มีมาตรฐานยิ่งขึ้น

๓. เป็นการยกระดับให้กำลังพลตระหนักรู้ถึงการเข้าสู่ระบบฐานข้อมูลสมัยใหม่อย่างปลอดภัย

จากผลการวิจัยสามารถนำเสนอเป็นข้อเสนอแนะเชิงนโยบาย ๓ ประเด็นหลักเพื่อให้เกิดความมั่นคงด้านการรักษาความปลอดภัยที่มีประสิทธิภาพ ซึ่งดังแสดงในแผนภาพที่ ๔ - ๒ ต่อไปนี้

แผนภาพที่ ๔ – ๒ ข้อเสนอแนะเชิงนโยบายการรักษาความปลอดภัยของกองทัพที่มีประสิทธิภาพ



รายละเอียดที่เกี่ยวข้องกับนโยบายมีดังนี้

๑. การเสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ โดยสามารถดำเนินการ ๓ ประเด็นย่อย ได้แก่

๑.๑ การส่งเสริมและพัฒนาวิทยาศาสตร์และเทคโนโลยีการป้องกันประเทศและความมั่นคง โดยพัฒนาระบบอาวุธและระบบการแจ้งเตือนภัยทางทหารให้มีขีดความสามารถในการป้องปรามทางยุทธศาสตร์

๑.๒ การส่งเสริมการศึกษาวิจัยและพัฒนาทางการทหารรวมถึงเสริมสร้างขีดความสามารถด้านอุตสาหกรรมป้องกันประเทศและพลังงานทหาร โดยประสานการวิจัยและความร่วมมือระหว่างหน่วยงานภายในกองทัพกับสถาบันวิจัยและสถาบันการศึกษาด้านเทคโนโลยีของภาครัฐและภาคเอกชนทั้งในประเทศและต่างประเทศ รวมถึงการขยายผลการวิจัยและเสริมสร้างขีดความสามารถด้านอุตสาหกรรมป้องกันประเทศและพลังงานทหารเพื่อการพึ่งพาตนเอง ตลอดจนพัฒนาเทคโนโลยีสารสนเทศเพื่อการสื่อสารทางทหารให้สนับสนุนการป้องกันประเทศ

๑.๓ เสริมสร้างความสัมพันธ์อันดี และความร่วมมือในทุกระดับกับกองทัพประเทศเพื่อนบ้าน กลุ่มอาเซียน และมิตรประเทศ บนพื้นฐานการรักษาผลประโยชน์และการรักษาความปลอดภัยร่วมกัน

๒. การพัฒนาระบบงานข่าวกรองให้มีประสิทธิภาพ โดยสามารถดำเนินการ ๓ ประเด็นย่อย ได้แก่

๒.๑ ดำเนินงานข่าวกรองที่มีคุณภาพและแจ้งเตือนภัยล่วงหน้าอย่างมีประสิทธิภาพทั้งภัยคุกคามต่อความมั่นคงแห่งชาติ และความเคลื่อนไหวที่สนับสนุนการเสริมสร้างความมั่นคงและผลประโยชน์แห่งชาติ

๒.๒ เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง และหน่วยงานภาครัฐ รวมทั้งหน่วยงานข่าวกรองต่างประเทศ และมีเครือข่ายด้านข้อมูลข่าวสารกับภาคเอกชนและประชาชน

๒.๓ เสริมสร้างและพัฒนาขีดความสามารถของระบบงานข่าวกรองอย่างต่อเนื่อง โดยพัฒนาบุคลากรและเพิ่มศักยภาพของเทคโนโลยีระบบฐานข้อมูลและองค์กรด้านการข่าว

๓. การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ โดยสามารถดำเนินการ ๓ ประเด็นย่อย ได้แก่

๓.๑ การปกป้อง ป้องกันภัยคุกคาม และเสริมสร้างความปลอดภัยต่อสงครามไซเบอร์ โดยการบูรณาการจัดการความมั่นคงไซเบอร์ระหว่างหน่วยงานรัฐ การสร้างภาคีเครือข่ายกับภาคเอกชน ภาควิชาการ บุคลากร องค์กร และผู้เชี่ยวชาญ รวมถึงความร่วมมือระหว่างประเทศ การเฝ้าระวังและพัฒนาระบบป้องกันการโจมตี การพัฒนาความพร้อม การปกป้องโครงสร้างพื้นฐานด้านไอซีที การกู้คืนข้อมูล ระบบ/เครือข่ายและพัฒนามาตรฐานความปลอดภัยทุกด้าน

๓.๒ การพัฒนาการบังคับใช้กฎหมาย โดยการพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์และพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ให้สามารถลดภัยคุกคามหรืออันตรายที่ส่งผลกระทบกับบุคคล ข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยเฉพาะที่อยู่ในรูปธุรกรรมทางอิเล็กทรอนิกส์ การละเมิดทรัพย์สินทางปัญญา การโจรกรรมข้อมูล การละเมิดสิทธิเสรีภาพของบุคคล การกรรโชกข้อมูลสารสนเทศ การกระทำผิดตลอดจนการก่อวินาศกรรมหรือทำลายระบบสารสนเทศ รวมถึงการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

๓.๓ การพัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ โดยส่งเสริมการวิจัยพัฒนาและจดสิทธิบัตรที่ผลิตโดยคนไทยเพื่อความมั่นคงปลอดภัยไซเบอร์ การบูรณาการเชื่อมโยงระบบฐานข้อมูลภาครัฐ การพัฒนาและการใช้ระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ระบบคลาวด์ภาครัฐ (G-Cloud) ตลอดจนการพัฒนาทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ความชำนาญทางด้านระบบไอซีทีและการรักษาความปลอดภัยทางไซเบอร์ที่ทันสมัย และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในเชิงปริมาณและคุณภาพอย่างต่อเนื่อง

สรุป

การรักษาความปลอดภัยมีความสำคัญเป็นอย่างยิ่ง ดังนั้นจึงควรส่งเสริมให้ประชาชนเกิดความรู้สึกเป็นส่วนหนึ่งของการรักษาความปลอดภัย อีกทั้งทุกภาคส่วนควรตระหนักถึงความสำคัญของการรักษาความปลอดภัยเช่นกัน โดยมีแนวทางและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพในอนาคตตามที่ผู้เชี่ยวชาญได้ให้ข้อเสนอแนะดังกล่าว อย่างไรก็ตามปัจจัยแห่งความสำเร็จของการรักษาความปลอดภัยนั้นจะต้องคำนึงถึงประเด็นต่างๆ ดังนี้ ๑. รัฐบาลให้ความสำคัญและสนับสนุนการดำเนินนโยบายความมั่นคงปลอดภัยแห่งชาติอย่างต่อเนื่อง โดยให้การสนับสนุนทรัพยากรแก่หน่วยงานที่เกี่ยวข้องในการดำเนินภารกิจที่สอดคล้องกับนโยบายด้านความปลอดภัยแห่งชาติ ตลอดจนสนับสนุนการแก้ไขปัญหาอุปสรรคในการดำเนินงานตามนโยบายโดยเร็วและเหมาะสมกับสถานการณ์ ๒. หน่วยงานที่เกี่ยวข้องต้องมีการเตรียมความพร้อมในการดำเนินนโยบายด้านความปลอดภัยโดยการกำหนดผู้รับผิดชอบทั้งในระดับบริหารและระดับปฏิบัติงานอย่างชัดเจน รวมทั้งจัดทำแผนงานที่สอดคล้องกับนโยบาย มาตรการและแนวทางปฏิบัติด้านความปลอดภัย กำหนดให้มีงบประมาณสนับสนุนและนำไปสู่การปฏิบัติอย่างเป็นระบบและมีประสิทธิภาพ และ ๓. ภาคประชาสังคม ตระหนักและให้การสนับสนุนเพื่อให้สอดคล้องกับบริบทด้านความปลอดภัยที่เปลี่ยนแปลงไป โดยที่อาจเป็นการให้ความรู้และส่งเสริมให้มีหลักสูตรที่เกี่ยวข้องกับความปลอดภัยในสถานศึกษาเพื่อสร้างความเข้าใจและมีร่วมตั้งแต่เยาว์วัย และต้องเปิดโอกาสให้ภาคส่วนอื่นๆ อาทิ ภาควิชาการ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน ได้เข้ามามีส่วนร่วมอย่างใกล้ชิดเป็นหุ้นส่วนเครือข่ายในการขยายผลต่อไป

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

การศึกษาวิจัยเรื่อง “แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต” ซึ่งมีวัตถุประสงค์เพื่อ ๑. ศึกษารูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน ๒. ศึกษารูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ ๓. ศึกษารูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต และ ๔. นำเสนอแนวทางการรักษาความปลอดภัยของกองทัพบกในอนาคต การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพโดยการศึกษาค้นคว้าเชิงเปรียบเทียบและรวบรวมข้อมูลที่เกี่ยวข้องกับรูปแบบการรักษาความปลอดภัยของกองทัพในอดีตจนถึงปัจจุบันและในต่างประเทศ ทั้งนี้เพื่อนำข้อมูลดังกล่าวมากำหนดเป็นรูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพให้มีประสิทธิภาพและนำไปใช้ได้จริง รวมถึงร่างแนวทางการรักษาความปลอดภัยของกองทัพในอนาคตที่สามารถรองรับต่อภัยคุกคามและความท้าทายพร้อมข้อเสนอแนะเชิงนโยบาย กลุ่มเป้าหมาย ได้แก่ ผู้ที่เกี่ยวข้องกับการรักษาความปลอดภัยและความมั่นคงของกองทัพไทย รวมถึงผู้เชี่ยวชาญด้านนวัตกรรมและเทคโนโลยี จำนวน ๑๒ คน ได้มาจากการเลือกแบบเจาะจงโดยอาศัยความสะดวก เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์แบบไม่มีโครงสร้าง การวิเคราะห์และสังเคราะห์ข้อมูลตามหลักการวิจัยเชิงคุณภาพโดยวิธีพรรณนาเชิงวิเคราะห์และตรวจสอบข้อมูลโดยใช้วิธีการสามเส้า

ผลการวิจัยพบว่ารูปแบบการรักษาความปลอดภัยในอดีตจนถึงปัจจุบันได้มีการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยตามระดับความสำคัญหน้าที่ความรับผิดชอบและกำลังงบประมาณของหน่วยงาน เนื่องจากส่วนงานตามโครงสร้างที่ประกอบขึ้นมีระดับความสำคัญต่อหน่วยงานต่างกัน ส่วนรูปแบบการรักษาความปลอดภัยในต่างประเทศล้วนมีความหลากหลายทางเชื่อชาติศาสนาประเทศและแนวคิดโดยขึ้นอยู่กับการแบ่งประเภทการรักษาความปลอดภัยของแต่ละประเทศและองค์กร อย่างไรก็ตามประเทศชั้นนำของภูมิภาคต่างยึดรูปแบบการดำเนินการทางการทหารสมัยใหม่ตามรูปแบบของกองทัพสหรัฐอเมริกาเป็นส่วนใหญ่ รวมถึงมีการปรับปรุงรูปแบบและวิธีการรักษาความปลอดภัยให้เหมาะสมอยู่เสมอ อีกทั้งศักยภาพของ

รูปแบบและวิธีการอาจขึ้นอยู่กับลักษณะภูมิประเทศและสภาพทางเศรษฐกิจของประเทศนั้นด้วย รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพในอนาคตจากการสัมมนาอิงผู้เชี่ยวชาญพบว่าประกอบด้วย ๕ องค์ประกอบ ได้แก่ ๑. นโยบายด้านความปลอดภัย ๒. การกำหนดโครงสร้างแนวปฏิบัติและรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง ๓. นวัตกรรมและเทคโนโลยี ๔. กระบวนการสร้างความเข้าใจกับประชาชนตลอดจนเจ้าหน้าที่ และ ๕. การบริหารและการประเมินความเสี่ยง การรักษาความปลอดภัยของกองทัพให้ได้มาตรฐานถือว่าเป็นเรื่องสำคัญที่ต้องดำเนินการอย่างต่อเนื่องทั้งนี้ก็เพื่อกำหนดขีดความสามารถด้านการรักษาความปลอดภัยของบุคลากรและสถานที่ของหน่วยงานทางราชการให้มีความมั่นคงปลอดภัยมากที่สุด

อภิปรายผลการวิจัย

จากการวิจัยตามขั้นตอนการดำเนินการวิจัยที่กล่าวมาแล้วข้างต้นผู้วิจัยนำข้อมูลทั้งหมดมาสรุปรายงานตามวัตถุประสงค์ของการวิจัยและอภิปรายผลการวิจัยได้ดังต่อไปนี้

๑. รูปแบบการรักษาความปลอดภัยของกองทัพในอดีตจนถึงปัจจุบัน

รูปแบบการรักษาความปลอดภัยในอดีตจนถึงปัจจุบันได้มีการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยตามระดับความสำคัญหน้าที่ความรับผิดชอบและกำลังงบประมาณของหน่วยงาน เนื่องจากส่วนงานต่างๆ ตามโครงสร้างที่ประกอบขึ้นเป็นหน่วยงานของกองทัพแต่ละส่วนมีระดับความสำคัญต่อหน่วยงานต่างกัน ดังนั้นการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยสถานที่ภายในหน่วยงานของกองทัพจึงต้องมีระดับความเข้มงวดต่างกันเพื่อมิให้เกิดบรรยากาศที่กดดันแก่ผู้ปฏิบัติงานในหน่วยงานนั้น อย่างไรก็ตามการรักษาความปลอดภัยโดยเฉพาะสถานที่ทำการทางการทหารที่มีความสำคัญทางความมั่นคงนั้นจำเป็นต้องมีมาตรการป้องกันหรือป้องปรามที่เหมาะสม โดยมุ่งให้มีประสิทธิภาพสูงสุดเท่าที่จะดำเนินการได้และมีความพร้อมต่อการเผชิญกับเหตุร้ายและในโลกยุคดิจิทัลภัยคุกคามและความท้าทายทางความมั่นคงของประเทศมักจะเข้ามาในรูปแบบใหม่ที่มีความซับซ้อนเพิ่มมากขึ้นโดยเฉพาะอย่างยิ่งเมื่อมีการนำเทคโนโลยีสมัยใหม่เข้ามาใช้ในการคุกคามทำให้เกิดการเปลี่ยนแปลงทั้งภาครัฐภาคเอกชนและภาคสังคม ซึ่งจะสร้างความยากลำบากให้กับหน่วยงานที่รับผิดชอบด้านการรักษาความปลอดภัยจึงมีความจำเป็นที่จะนำเทคโนโลยีสมัยใหม่มาใช้ร่วมกับการรักษาความปลอดภัยรูปแบบเดิมเพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยและความมั่นคง โดยการนำเทคโนโลยีที่เหมาะสมและปลอดภัยมาใช้นั้นมีความจำเป็นต้องมีการศึกษาและ

ตรวจสอบอย่างละเอียดเพื่อให้มีความเป็นไปได้และเหมาะสมกับระบบและระเบียบต่างๆ รวมถึงมาตรการในการรักษาความปลอดภัยของกองทัพหรือหน่วยงานทางความมั่นคงอื่นๆ ที่มีคุณลักษณะใกล้เคียงกัน ซึ่งสอดคล้องกับแนวคิดของโรเบิร์ต (Reid Robert N.) ที่กล่าวไว้ว่า การวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยควรเป็นไปเพื่อรองรับตามระดับความสำคัญหน้าที่ความรับผิดชอบและกำลังงบประมาณของหน่วยงาน เนื่องจากส่วนงานต่างๆ ตามโครงสร้างที่ประกอบขึ้นเป็นหน่วยงานของกองทัพแต่ละส่วนมีระดับความสำคัญต่อหน่วยงานต่างกัน ตัวอย่างเช่น ส่วนงานเครื่องมืออุปกรณ์ของหน่วยงานหนึ่งมีความสำคัญมากกว่าส่วนงานระบบคอมพิวเตอร์ ในทางกลับกันสำหรับอีกหน่วยงานส่วนงานระบบคอมพิวเตอร์เป็นส่วนงานที่มีความสำคัญที่สุด เป็นต้น ฉะนั้นการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยสถานที่ภายในหน่วยงานของกองทัพจึงต้องมีระดับความเข้มงวดต่างกันเพื่อมิให้เกิดบรรยากาศที่กดดันแก่ผู้ปฏิบัติงานในหน่วยงานนั้น (Reid Robert N., 2005) ซึ่งรูปแบบการรักษาความปลอดภัยในอดีตจนถึงปัจจุบันได้มีการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยตามระดับความสำคัญหน้าที่ความรับผิดชอบและกำลังงบประมาณของหน่วยงาน เนื่องจากส่วนงานต่างๆ ตามโครงสร้างที่ประกอบขึ้นเป็นหน่วยงานของกองทัพแต่ละส่วนมีระดับความสำคัญต่อหน่วยงานต่างกัน อีกทั้งกองทัพยังมีการเพิ่มศักยภาพด้านการรักษาความปลอดภัยด้วยการฝึกอบรมกำลังพลและผู้ที่เกี่ยวข้องอยู่เสมอ

๒. รูปแบบการรักษาความปลอดภัยของต่างประเทศ

๒.๑ รูปแบบการรักษาความปลอดภัยของประเทศสหรัฐอเมริกา

การรักษาความปลอดภัยของประเทศสหรัฐอเมริกามีการกำหนดเป็นนโยบายโดย Military Police: Security of Unclassified Army Property ซึ่งกำหนดเป็นความปลอดภัยขั้นต่ำและหากเป็นสถานที่ที่มีความต้องการความปลอดภัยสูงมากสามารถดำเนินการเพิ่มเติมได้เองตามนโยบายของแต่ละชั้นความลับที่ได้รับมอบหมายจากผู้บังคับบัญชาได้โดย US Military Police มีการแบ่งออกเป็นการรักษาความปลอดภัยสำหรับสถานที่ทรัพย์สินบุคคลและยานพาหนะอย่างไรก็ตามงานวิจัยชิ้นนี้มุ่งเน้นการศึกษาความปลอดภัยด้านสถานที่ที่เหมาะสมในอนาคตซึ่งสรุปข้อตกลงเบื้องต้นโดยแบ่งตามรูปแบบการรักษาความปลอดภัยตามระดับของ Security of Unclassified Army Property ดังนี้

๒.๑.๑ มาตรการการป้องกันทางกายภาพขั้นตอนการรักษาความปลอดภัยและการต่อต้านการก่อการร้ายสำหรับประเภทของทรัพย์สิน

๒.๑.๒ มาตรการรักษาความปลอดภัยขั้นต่ำที่จำเป็นสำหรับการดำเนินการต่อประเภทของทรัพย์สินแม้ว่าประเภทของทรัพย์สินของกองทัพเหล่านี้ไม่จำเป็นต้องมีการวิเคราะห์ความเสี่ยงโดยใช้ DA Pam ๑๕๐-๕๑

๒.๑.๓ มาตรการรักษาความปลอดภัยที่ต้องใช้รั้วรอบที่ตั้งกำหนดให้มีความสูง (๖ หรือ ๗ ฟุต) และมีความสามารถในการป้องกันที่ดีหรือมีคุณสมบัติอื่นๆ จะขึ้นอยู่กับการตัดสินของผู้บังคับบัญชาการติดตั้งและต้องดำเนินการติดตั้งตามคำแนะนำที่พบได้ใน Field Manual (FM) ๑๕-๓๐ เว้นแต่เป็นไปตามข้อกำหนดของกองกำลังวิศวกรสหรัฐอเมริกาเลขที่ ๔๐-๑๖-๐๘, Type FE

๒.๑.๔ หากมีข้อโต้แย้งหรือไม่สามารถดำเนินการได้ตามมาตรฐานต่างๆ ที่กำหนดให้ทำหนังสือระบุเป็นลายลักษณ์อักษรพร้อมระบุมาตรการทดแทน

จากผลการศึกษาข้างต้นสอดคล้องและเป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ (ฉบับที่ ๒) พ.ศ.๒๕๕๔ ที่ระบุไว้ว่าหน่วยงานที่มีความสำคัญทางความมั่นคงควรใช้มาตรการที่เป็นไปตามมาตรฐานหลักสากล และนำเทคโนโลยีสมัยใหม่มาใช้ร่วมกับการรักษาความปลอดภัยรูปแบบเดิมเพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยและความมั่นคงโดยการนำเทคโนโลยีที่เหมาะสมและปลอดภัยมาใช้นั้นมีความจำเป็น โดยให้ตระหนักถึงภัยคุกคามและผลกระทบต่อความมั่นคงที่มีต่อสถานที่สำคัญ ซึ่งจะสร้างความยากลำบากให้กับหน่วยงานที่รับผิดชอบด้านการรักษาความปลอดภัยจึงมีความจำเป็นที่จะนำเทคโนโลยีสมัยใหม่มาใช้ร่วมกับการรักษาความปลอดภัยรูปแบบเดิม เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยและความมั่นคงโดยการนำเทคโนโลยีที่เหมาะสมและปลอดภัยมาใช้นั้นมีความจำเป็นต้องมีการศึกษาและตรวจสอบอย่างละเอียดเพื่อให้มีความเป็นไปได้และเหมาะสมกับระบบระเบียบรวมถึงมาตรการในการรักษาความปลอดภัยของกองทัพหรือหน่วยงานทางความมั่นคงอื่นๆ ที่มีคุณลักษณะใกล้เคียงกัน ซึ่งในขณะเดียวกันสามารถสรุปและวิเคราะห์เชิงความสอดคล้องกับงานวิจัยต่างๆ ได้ว่า รูปแบบการรักษาความปลอดภัยในหลายภูมิภาคซึ่งมีหลากหลายทางเชื่อชาติศาสนาประเทศและหลากหลายแนวคิดล้วนขึ้นกับการแบ่งประเภทการรักษาความปลอดภัยของแต่ละประเทศและองค์กรอย่างไรก็ตามประเทศชั้นนำของภูมิภาคต่างๆ ต่างยึดรูปแบบการดำเนินการทางการทหารสมัยใหม่ตามรูปแบบของกองทัพสหรัฐอเมริกาเป็นส่วนใหญ่ รวมถึงมีการปรับปรุงรูปแบบและวิธีการรักษาความปลอดภัยด้านสถานที่ให้เหมาะสมในอนาคตอยู่เสมอ ทั้งนี้ศักยภาพของรูปแบบและวิธีการอาจขึ้นอยู่กับลักษณะภูมิประเทศและสภาพทางเศรษฐกิจของประเทศนั้นๆ ด้วย ผลงานวิจัยยังสอดคล้องกับรายงานยุทธศาสตร์โลกเพื่อการสร้างเสริมความปลอดภัยและสุขภาพอนามัยในการทำงาน (Vision Zero : A Global Strategy to Promote Safety and Health at

Workplace) ที่กล่าวว่า ยุทธศาสตร์ Vision Zero เพื่อการบริหารจัดการและสร้างเสริมความปลอดภัยในสถานที่ทำงาน โดยมีกลยุทธ์เชิงป้องกันเพื่อมุ่งไปสู่โลกอนาคตแห่งความปลอดภัย ปราศจากการเสียชีวิตจากการทำงาน และไม่มีอุบัติเหตุที่รุนแรง โรคจากการทำงาน รวมถึงอุบัติเหตุจราจรที่ร้ายแรงเนื่องจากการทำงาน ภายใต้ยุทธศาสตร์ Vision Zero ประกอบด้วยกลยุทธ์ที่กำหนดเป็นกฎเหล็ก (Golden Rules) จำนวน ๗ ข้อ ดังนี้

๑. การเป็นผู้นำและให้คำมั่น (Take Leadership & Commitment) ในการดำเนินงาน โดยผู้บริหารสูงสุดขององค์กรต้องมีบทบาทเป็นผู้นำ มีนโยบายหรือแสดงความมุ่งมั่นที่จะให้ลำดับความสำคัญด้านความปลอดภัยของผู้ปฏิบัติงานทุกระดับ

๒. การบ่งชี้อันตรายและความเสี่ยง (Identify Hazards and Risks) โดยจัดให้มีมาตรการเพื่อสำรวจ ตรวจวัด วิเคราะห์ และประเมินระดับอันตรายหรือความเสี่ยง อย่างเป็นระบบ/เป็นขั้นตอน พร้อมมีการจัดทำรายงานหรือบันทึกข้อมูลอย่างครบถ้วน

๓. การกำหนดเป้าหมายด้านความปลอดภัยและสุขภาพ (Set Targets for Safety & Health) เพื่อให้มีการดำเนินกิจกรรมด้านความปลอดภัยอย่างมีทิศทาง เป็นไปตามวัตถุประสงค์ที่พึงประสงค์ และบรรลุเป้าหมายที่ตั้งไว้ตามกรอบเวลาที่กำหนด

๔. การมีระบบงานที่ปลอดภัยและดีต่อสุขภาพอนามัย (Ensure a Safe & Healthy System) มุ่งเน้นการออกแบบสภาพการทำงานและปัจจัยที่เกี่ยวข้องกับการทำงานภายใต้หลักความปลอดภัยและสุขภาพอนามัย และเหมาะสมกับผู้ปฏิบัติงาน

๕. การใช้เทคโนโลยีที่ปลอดภัยและดีต่อสุขภาพอนามัย (Use Safe & Healthy Technology) เพื่อลดความเสี่ยงของผู้ปฏิบัติงานต่อการได้รับอันตราย โดยอาศัยหลักทางด้านวิศวกรรมเพื่อการป้องกันและควบคุมความเสี่ยงให้มีน้อยที่สุดเท่าที่ปฏิบัติได้

๖. การปรับปรุง/พัฒนาคุณภาพและสมรรถนะ (Improve Qualification & Competency) โดยมีการวางแผน วิเคราะห์ ตรวจสอบ ทบทวน และขับเคลื่อนสู่การปฏิบัติ พร้อมทั้งมีการประเมินผลเพื่อการปรับปรุงหรือพัฒนาอย่างต่อเนื่อง

๗. การลงทุนด้านทรัพยากรมนุษย์ (Invest in People) โดยคนเป็นศูนย์กลางของการพัฒนา จึงต้องมุ่งเน้นการอบรมให้ความรู้ สร้างเสริมจิตสำนึกและทัศนคติที่ถูกต้อง เพื่อให้ปฏิบัติงานด้วยความปลอดภัยและมีสุขภาพอนามัยที่ดี

ทั้งนี้ ยุทธศาสตร์ Vision Zero ได้รับการรับรองและนำไปประยุกต์ใช้ในหลายประเทศ เพื่อมุ่งสู่เป้าหมายในการสร้างวัฒนธรรมเชิงป้องกันด้านความปลอดภัย (Culture of Prevention) ให้เกิดขึ้นอย่างยั่งยืน โดยในที่ประชุมสุดยอดผู้นำชาติมหาอำนาจ (G7 Summit) เมื่อเดือนมิถุนายน ๒๕๕๘ ณ สหพันธ์สาธารณรัฐเยอรมนี ได้มีการประกาศปฏิญญาที่ให้การสนับสนุนการจัดตั้ง

กองทุน Vision Zero ภายใต้ความร่วมมือกับองค์การแรงงานระหว่างประเทศ (ILO) เพื่อส่งเสริมการป้องกันอุบัติเหตุอันตรายและการเสียชีวิตจากการทำงาน และสร้างเสริมสภาพการทำงานที่ปลอดภัยและดีต่อสุขภาพอนามัยในสถานที่ทำงานทุกประเภทกิจการ

ในส่วนของประเทศไทย กรมสวัสดิการและคุ้มครองแรงงาน จะมีการนำยุทธศาสตร์ Vision Zero รวมทั้ง ๗ Golden Rules มาผสมผสานเข้ากับการพัฒนาแผนแม่บทด้านความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงานแห่งชาติ ฉบับที่ ๒ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) ซึ่งอยู่ระหว่างการยกร่างขั้นตอนสุดท้ายก่อนขับเคลื่อนให้มีการประกาศใช้ นอกจากนี้ ยังจะได้นำข้อมูลรายละเอียดเกี่ยวกับแนวปฏิบัติ (Guideline) เพื่อการประยุกต์ใช้ Vision Zero & ๗ Golden Rules ซึ่ง ISSA จัดทำขึ้นมาแปลเป็นภาษาไทย และเผยแพร่สู่กลุ่มเป้าหมายที่เกี่ยวข้องรวมทั้งผลักดันทั้งในระดับนโยบายและการปฏิบัติของสถานประกอบกิจการต่อไป (วิสันติ เลาหอุดมโชค, ๒๕๕๙)

๒.๒ รูปแบบการป้องกันความปลอดภัยในประเทศไทยและภูมิภาคเอเชีย

การพัฒนาตามหลักสากลของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐานซึ่งครอบคลุมทั้งในระดับนโยบาย (Policy) การจัดการองค์กร (Organization) และเทคโนโลยี (Technology) เพื่อบริหารความเสี่ยง (Risk Management) ที่มีผลกระทบกับหน่วยงานได้อย่างเหมาะสมโดยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยเพื่อนำมาใช้ในการดำเนินการร่วมกันประกอบด้วย

๒.๒.๑ หน้าที่งาน(Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยในระดับภาพรวมจำแนกเป็น ๕ Functions (IPDRR : Identify, Protect, Detect, Respond, Recover)

๒.๒.๒ กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยองค์กรอาทิการจัดการทรัพย์สินการควบคุมการเข้าถึง

๒.๒.๓ กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิคและ/หรือกิจกรรมในการบริหารจัดการ

๒.๒.๔ ข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐานแนวทางและแนวปฏิบัติที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม

จากผลการศึกษาข้างต้นสอดคล้องและเป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ (ฉบับที่ ๒) พ.ศ.๒๕๕๔ ที่ระบุไว้ว่าหน่วยงานที่มีความสำคัญ

ทางความมั่นคงควรมีการแบ่งโครงสร้างอย่างชัดเจนตามระบบโครงสร้างพื้นฐานสำคัญและการแบ่งหน้าที่สายบังคับบัญชาตามระเบียบราชการ

๒.๓ รูปแบบการรักษาความปลอดภัยของประเทศในภูมิภาคอื่นๆ

ภูมิภาคอเมริกาเหนือยุโรปโอเชียเนียและแอฟริกาซึ่งถือได้ว่ามีหลากหลายทางเชื่อชาติศาสนาประเทศและหลากหลายแนวคิดขึ้นกับการแบ่งประเภทการรักษาความปลอดภัยของแต่ละประเทศและองค์กร อย่างไรก็ตามประเทศชั้นนำของภูมิภาคต่างๆ ต่างยึดรูปแบบการดำเนินการทางการทหารสมัยใหม่ตามรูปแบบของกองทัพสหรัฐอเมริการวมถึงมีการปรับปรุงรูปแบบและวิธีการรักษาความปลอดภัยด้านสถานที่ให้เหมาะสมในอนาคตอยู่เสมอ ผู้วิจัยจึงขอสรุปโดยแบ่งตามรูปแบบอุปกรณ์การรักษาความปลอดภัยและแบ่งตามความสำคัญของพื้นที่ได้ ๔ ระดับระดับที่ ๑ ที่รั้วและพื้นที่ทางเข้าสถานที่ระดับที่ ๒ จากรั้วจนถึงอาคารและห้องรับรองระดับที่ ๓ ภายในห้องรับรองระดับที่ ๔ จุดที่ต้องการความปลอดภัยสูงอาทิห้องภายในอาคารที่เก็บทรัพย์สินหรือเอกสารข้อมูลที่สำคัญ (Restrict Zone) บริเวณห้ามเข้า (Forbidding Zone) พื้นที่เก็บหรือฐานยิงจรวดบรรจุระเบิด

ซึ่งสอดคล้องกับรายงานของ Joint Publication ๓-๑๓.๓, Operations Security, ๔ มกราคม ๒๕๕๕ ว่าการรักษาความปลอดภัยในการปฏิบัติการ (Operation Security: OPSEC) โดยในการปฏิบัติการทางทหารด้านต่างๆ หลายรูปแบบ เช่น ด้านบัญชาการและควบคุม (Command and Control Warfare : C2W) การปฏิบัติการข่าวสาร (Information Operations : IO) และได้รับผลกระทบต่อมาตรการรักษาความปลอดภัยอื่นๆ ได้แก่ มาตรการรักษาความปลอดภัยการติดต่อสื่อสาร (Communication Security : COMSEC), มาตรการต่อต้านข่าวกรอง (Counter-Intelligence) มาตรการรักษาความปลอดภัยข้อมูลข่าวสาร (Information Security : INFOSEC) การรักษาความปลอดภัยสัญญาณ (Signal Security : SIGSEC) และการรักษาความปลอดภัยการรับ-ส่งสัญญาณ (Transmission Security : TRANSEC) การรักษาความปลอดภัยในการปฏิบัติการนั้นเป็นมาตรการหรือวิธีการอย่างเป็นระบบที่ใช้ในการระบุ (identify) ควบคุม (Control) และป้องกัน (Protect)

๓. รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

ผลการวิเคราะห์รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคตจากการสัมมนาอิงผู้เชี่ยวชาญพบว่าประกอบด้วย ๕ องค์ประกอบสำคัญ ได้แก่ ๑) นโยบายด้านความปลอดภัย ๒) การกำหนดแนวปฏิบัติโครงสร้างและรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง ๓) นวัตกรรมและเทคโนโลยี ๔) กระบวนการสร้างความเข้าใจ

กับประชาชนและเจ้าหน้าที่ และ ๕) การบริหารและการประเมินความเสี่ยง ซึ่งผลการวิเคราะห์รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพในอนาคต ซึ่งมีความหมายดังนี้

๑. นโยบายด้านความปลอดภัย

รัฐควรกำหนดนโยบายด้านความปลอดภัยรวมถึงมีการกำหนดระเบียบปฏิบัติเพื่อรักษาความปลอดภัยสถานที่ของแต่ละส่วนแต่ละหน่วยงานที่เหมาะสมชัดเจน เนื่องจากหน่วยงานของรัฐย่อมมีความแตกต่างกันไปตามสภาพแวดล้อมความจำเป็นที่เผชิญอยู่ ดังนั้นเพื่อให้การวางระเบียบปฏิบัติในแต่ละหน่วยงานเป็นไปอย่างเหมาะสมครอบคลุมสภาพการณ์และเพื่อให้ผู้ปฏิบัติสามารถปฏิบัติตามได้จริงจึงควรพิจารณาจากตัวชี้วัดดังนี้

๑.๑ ภารกิจหน้าที่ความรับผิดชอบของหน่วยงาน

๑.๒ สภาพแวดล้อมและสถานการณ์ที่เผชิญอยู่

๑.๓ จำนวนเจ้าหน้าที่ที่ปฏิบัติงานและเจ้าหน้าที่รักษาความปลอดภัย

๑.๔ งบประมาณสำหรับการรักษาความปลอดภัยและการสนับสนุนจากผู้บังคับบัญชา

๑.๕ ข่าวสารสิ่งบอกเหตุและการแจ้งเตือนภัย

๑.๖ การวิจัยและพัฒนานวัตกรรมและเทคโนโลยี

๑.๗ การติดต่อสื่อสารภายในหน่วยงานและกับหน่วยงานของรัฐอื่นๆ

๑.๘ รายงานผลการสำรวจหรือการตรวจสอบการรักษาความปลอดภัยที่ได้เคยกระทำมา

อย่างไรก็ตามการดำเนินการด้านป้องกันและแก้ไขปัญหาการก่อการร้ายทุกรูปแบบเป็นอีกปัจจัยที่มีความสำคัญสูงในปัจจุบัน จึงเห็นควรให้มีการกำหนดนโยบายและให้ความสำคัญกับปัญหาด้านนี้โดยเฉพาะ โดยมีความจำเป็นต้องสร้างนโยบายที่สามารถลดปัจจัยและเงื่อนไขที่เกื้อกูลต่อการก่อการร้ายการป้องกันมิให้กลุ่มก่อการร้ายบุคคลหรือกลุ่มบุคคลที่สนับสนุนการก่อการร้ายทุกรูปแบบใช้พื้นที่ในอาณาเขตประเทศไทยเป็นพื้นที่พักพิงพื้นที่แสวงหาปัจจัยเพื่อสนับสนุนการก่อการร้ายตลอดจนเป็นพื้นที่ก่อความรุนแรง หรือกระทำการก่อการร้ายโดยมุ่งเน้นให้เป็นนโยบายระยะยาวและระยะสั้นพร้อมทั้งมีการกำหนดมาตรการเชิงรุกและเชิงรับรวมถึงการกำหนดแนวปฏิบัติที่ชัดเจน

๒. การกำหนดแนวปฏิบัติโครงสร้างและรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง

ควรกำหนดให้มีหน่วยรับผิดชอบในทุกนโยบายทั้งหน่วยรับผิดชอบหลักและหน่วยรับผิดชอบร่วม โดยกำหนดให้นโยบายแต่ละเรื่องมีหน่วยงานรับผิดชอบหลักที่เป็นเจ้าภาพบูรณาการนโยบายหนึ่งหน่วยงาน ยกเว้นกรณีที่สาระสำคัญของนโยบายมีลักษณะภารกิจที่แตกต่างกันอย่างชัดเจนให้พิจารณาตามความเหมาะสมหรือมีการจัดตั้งคณะกรรมการร่วมและกำหนดให้มีหน่วยรับผิดชอบหลักตามแนวนโยบายย่อยทุกข้อ เพื่อสนับสนุนการดำเนินการของเจ้าภาพ บูรณาการนโยบายเนื่องจากสาระสำคัญของนโยบายอาจมีประเด็นดำเนินการที่สำคัญในหลายด้านที่แตกต่างกัน ทั้งนี้เพื่อให้การขับเคลื่อนนโยบายมีหน่วยรับผิดชอบอย่างครบถ้วนชัดเจนและสามารถนำมาใช้เป็นแนวปฏิบัติและมาตรการการรักษาความปลอดภัยได้

อีกทั้งควรมีการปรับและสร้างศูนย์ป้องกันความปลอดภัยแห่งชาติซึ่งมีภารกิจในการให้คำแนะนำด้านการรักษาความปลอดภัยให้กับภาคธุรกิจภาคบริการภาคอุตสาหกรรมภาครัฐและองค์กรต่างๆ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานแห่งชาติ เพื่อลดจุดอ่อนที่อาจจะถูกโจมตีจากภัยคุกคามต่างๆ โดยศูนย์ป้องกันความปลอดภัยดังกล่าวควรปฏิบัติงานร่วมกับหน่วยงานทางความมั่นคงเดิมที่มีอยู่ทั้งนี้ควรส่งเสริมให้เกิดความร่วมมือระหว่างผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของทุกภาคส่วน นอกจากนี้ควรเป็นส่วนประสานงานหรือสร้างความร่วมมือกับรัฐบาลในภูมิภาคอาเซียนและประเทศอื่นๆ เพื่อแลกเปลี่ยนข่าวสารและความเชี่ยวชาญเฉพาะด้าน นอกจากนี้ควรเป็นผู้กำหนดแผนการรองรับเหตุต่างๆ ตามระดับของสถานการณ์และหน่วยงานที่รับผิดชอบทั้งยังเป็นหน่วยงานหลักที่ให้ข่าวสารหรือสื่อสารข้อมูลที่น่าเชื่อถือไปยังประชาชนและหน่วยงานต่างๆ ทราบ

อย่างไรก็ตาม เพื่อไม่ให้เกิดความสับสนควรมีการดำเนินการโดยใช้โครงสร้างตามสายบังคับบัญชาและมีการมอบหมายหน้าที่การดูแลตามลำดับชั้นและกระจายอำนาจอย่างเหมาะสม รวมถึงมีการแต่งตั้งคณะกรรมการเฉพาะเพื่อดูแลความปลอดภัยในแต่ละหน่วยงานต่างๆ ภายในควรมีสร้างเครือข่ายการรักษาความปลอดภัยกับประชาชนชุมชนและหน่วยงานภายนอกเพื่อช่วยเหลือทางด้านความปลอดภัย อีกทั้งระหว่างหน่วยงานควรสร้างความเข้าใจและความสำคัญของการรักษาความปลอดภัยให้กับนักเรียนนักศึกษาและประชาชนรวมถึงบุคลากรในหน่วยงานต่างๆ ทุกระดับชั้นยศพร้อมกับกำหนดให้กองทัพมีโครงสร้างการบริหารและการจัดการรักษาความปลอดภัยไว้อย่างชัดเจน สำหรับเครื่องมือที่จะนำมาใช้ในการรักษาความปลอดภัยต้องคำนึงถึงความทันสมัยเหมาะสมกับภารกิจทั้งฮาร์ดแวร์และซอฟแวร์ที่จะนำมาทำเป็นระบบรักษาความปลอดภัยอัตโนมัติที่สามารถป้องกันตรวจจับและหน่วงภัยคุกคามนั้นได้ กรณีที่สำคัญคืองานด้านข่าวกรองที่มีคุณภาพและแจ้งเตือนภัยล่วงหน้าอย่างมีประสิทธิภาพทั้งภัยคุกคามต่อความมั่นคงแห่งชาติและความเคลื่อนไหวที่สนับสนุนการเสริมสร้างความมั่นคงและผลประโยชน์แห่งชาติ การ

เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรองและหน่วยงานภาครัฐรวมทั้งหน่วยงานข่าวกรองต่างประเทศและมีเครือข่ายด้านข้อมูลข่าวสารกับภาคเอกชนภาคประชาชนและเสริมสร้างพัฒนาขีดความสามารถของระบบงานข่าวกรองอย่างต่อเนื่อง ซึ่งผลการวิจัยนี้สอดคล้องกับรายงานการวิจัยของ ชัยเสฏฐ์ พรหมศรี (๒๕๕๓) และ เดชน์ จรูญเรืองฤทธิ์ (๒๕๔๕) อีกด้วย

๓. นวัตกรรมและเทคโนโลยี

ควรส่งเสริมการพัฒนาศักยภาพทางนวัตกรรมและเทคโนโลยีโดยส่งเสริมการวิจัยพัฒนาและจดสิทธิบัตรนวัตกรรมและเทคโนโลยีที่ผลิตโดยคนไทย การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยโดยเน้นทั้งฮาร์แวร์และซอฟแวร์ อาทิ

๓.๑ ระบบสัญญาณเตือนภัยเชื่อมต่อกับกล้องวงจรปิดที่รองรับหลากหลายภาษา

๓.๒ เครื่องตรวจจับโลหะที่มีประสิทธิภาพและมีราคาที่เหมาะสม

๓.๓ ระบบกล้องวงจรปิด CCTV อัจฉริยะแบบเคลื่อนที่และแบบติดตั้งอยู่กับที่ที่สามารถเตือนภัยติดตามและค้นหารวมถึงซอฟท์แวร์ที่ช่วยในการจดจำใบหน้าบุคคลที่สามารถเชื่อมต่อกับระบบฐานข้อมูลของหน่วยงานทางความมั่นคงได้

๓.๔ เครื่องตรวจจับการเคลื่อนไหวโดยมีเซ็นเซอร์ที่แม่นยำและสามารถทำงานได้ทั้งภายในอาคารและภายนอกอาคาร

๓.๕ ระบบการสำรองข้อมูลที่น่าเชื่อถือและระบบการสื่อสารออนไลน์ที่ปลอดภัย

๓.๖ ระบบ Access Control แบบใช้ไบโอเมตทริกซ์ที่สามารถตรวจสอบและเก็บข้อมูลอัตลักษณ์บุคคลรวมถึงการตรวจสอบลักษณะทางกายภาพ (Physiological Biometrics) และการตรวจสอบลักษณะทางพฤติกรรม (Behavioral Biometrics) ได้

นอกจากนี้ควรมีการพัฒนาระบบการบูรณาการเชื่อมโยงระบบฐานข้อมูลภาครัฐการพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ รวมถึงการใช้ระบบอิเล็กทรอนิกส์เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานทางความมั่นคงระบบคลาวด์ทางความมั่นคง ตลอดจนการพัฒนาบุคลากรภาครัฐองค์กรทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ความชำนาญทางด้านนวัตกรรมและเทคโนโลยีและการรักษาความปลอดภัยเพื่อให้บุคลากรทุกภาคส่วนที่เกี่ยวข้องมีข้อมูลข่าวสารและความรู้ทางด้านเทคโนโลยีที่ทันสมัยรวมถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Spagnoletti, Paolo and Resca A., 2008) และการพัฒนาบุคลากรทางด้านการรักษาความปลอดภัย

การปกป้องและป้องกันภัยคุกคามด้านไซเบอร์สงครามไซเบอร์และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศโดยการบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานต่างๆ การประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชนภาควิชาการบุคลากรองค์กรและผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างประเทศ การเฝ้าระวังและการพัฒนาระบบป้องกันการโจมตีระบบสารสนเทศ การพัฒนาความพร้อมต่อสงครามไซเบอร์ การปกป้องโครงสร้างพื้นฐานที่รวมถึงการสำรองข้อมูลที่เหมาะสม นอกจากนี้ควรมีการพัฒนากฎหมายระเบียบข้อบังคับเพื่อความมั่นคงที่ทันสมัยเนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอยู่ตลอดเวลา รวมถึงควรมีการพัฒนาเทคโนโลยี สำหรับงานสืบสวนและป้องกันการคุกคามทางกายภาพทั้งด้านบุคคลด้านสถานที่ด้านข่าวสารรวมถึงอาชญากรรมไซเบอร์ให้สามารถลดภัยคุกคามหรืออันตรายที่ส่งผลกระทบกับบุคคลข้อมูลและเทคโนโลยีต่างๆ โดยเฉพาะ (ISO/IEC 27000:2009 (E), 2009)

๔. กระบวนการสร้างความเข้าใจกับประชาชนและเจ้าหน้าที่

ควรมีการผนึกกำลังทุกภาคส่วนให้พร้อมเผชิญปัญหาและภัยคุกคามความมั่นคงโดยเปิดโอกาสให้ทุกภาคส่วนมีส่วนร่วมกำหนดแนวทางการพัฒนาการป้องกันและแก้ปัญหาโดยเฉพาะ การเสริมสร้างความมั่นคงของชาติในระดับพื้นที่ให้มีภูมิคุ้มกันมีความพร้อมเผชิญปัญหาและภัยคุกคามความมั่นคง รวมถึงสามารถผนึกกำลังประชาชนหรือกลุ่มพลังมวลชนเพื่อสนับสนุนหน่วยงานทางความมั่นคงของประเทศในสถานการณ์ต่างๆ ตลอดจนการส่งเสริมมิติวัฒนธรรมและภูมิปัญญาชุมชน/ท้องถิ่นและการจัดการศึกษาที่สะท้อนถึงความตระหนักในหน้าที่และการมีส่วนร่วมในการรักษาความปลอดภัยโดยควรบรรจุอยู่ในหลักสูตรการเรียนการสอนในสถาบันการศึกษาต่างๆ

ซึ่งรูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพในอนาคตจากการสัมมนาอิงผู้เชี่ยวชาญในหัวข้อที่ผ่านมาพบว่าประกอบด้วย ๕ องค์ประกอบสำคัญ ได้แก่ ๑) นโยบายด้านความปลอดภัย ๒) การกำหนดแนวปฏิบัติโครงสร้างและรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง ๓) นวัตกรรมและเทคโนโลยี ๔) กระบวนการสร้างความเข้าใจกับประชาชนและเจ้าหน้าที่ และ ๕) การบริหารและการประเมินความเสี่ยง

ซึ่งผู้วิจัยได้ศึกษาผลงานวิจัยพบว่ามีความสอดคล้องกับงานวิจัยของวัชราภรณ์ พิมพา และคณะ (๒๕๔๙) และ Baker, Paul R. (2012) ที่กล่าวถึงรูปแบบของการรักษาความปลอดภัยว่าการพัฒนานวัตกรรมและเทคโนโลยีจะช่วยให้รูปแบบการรักษาความปลอดภัยมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น ทั้งนี้จะขึ้นอยู่กับโครงสร้าง ระเบียบ มาตรการ การบริหารจัดการ และการสร้างความเข้าใจกับผู้มีส่วนเกี่ยวข้องด้านความปลอดภัย

ดังนั้นในการกำหนดรูปแบบที่เหมาะสมควรขึ้นอยู่กับนโยบาย การจัดโครงสร้างตามภาระหน้าที่ การกำหนดมาตรการในการปฏิบัติงาน การกำหนดแผนงานตามภารกิจ การสนับสนุนทั้งทางด้านกำลังพลและงบประมาณ ทั้งนี้เพื่อให้การดำเนินงานด้านการรักษาความปลอดภัยมีประสิทธิภาพสูงสุด ผลงานวิจัยสอดคล้องกับนโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘-๒๕๖๔ สำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี (๒๕๕๘) และรายงานการวิจัยของพงษ์ศักดิ์ ฮงประยูร (๒๕๕๘) ที่ระบุถึงมาตรการทางกฎหมายเกี่ยวกับการรักษาความปลอดภัยว่าหน่วยงานทางความมั่นคงจะต้องมีการกำหนดมาตรการทางกฎหมายควบคู่ไปกับการดำเนินตามนโยบายด้านการรักษาความปลอดภัย

๔. แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

เมื่อนำข้อมูลที่ได้จากการวิจัยมาตรวจสอบโดยใช้วิธีการสามเส้าของข้อมูลพบว่าแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคตจะประกอบด้วยส่วนสำคัญดังต่อไปนี้

๔.๑ มาตรการการรักษาความปลอดภัย

๔.๑.๑ มาตรการการรักษาความปลอดภัยด้านบุคคล

๔.๑.๑.๑ ควรมีการตรวจสอบข้อมูลประวัติบุคคลก่อนเข้าปฏิบัติงานอย่างละเอียดและดำเนินการอย่าต่อเนื่อง

๔.๑.๑.๒ ควรมีการตรวจสอบข้อมูลประวัติผู้ใกล้ชิดบุคคลที่ปฏิบัติหน้าที่รักษาความปลอดภัย

๔.๑.๑.๓ เจ้าหน้าที่ที่เกี่ยวข้องควรได้รับการอบรมด้านการรักษาความปลอดภัยอย่างต่อเนื่องทั้งบุคลากรใหม่และผู้ปฏิบัติงานเดิมโดยต้องดำเนินการอบรมให้คลอบคลุมทุกมิติทั้งด้านบุคคลด้านข้อมูลข่าวสารและด้านสถานที่

๔.๑.๑.๔ ควรมีระบบการตรวจสอบอย่างเข้มงวดและมีการหมุนเวียนบุคคลดูแลมิใช้ให้ดูแลคนเดียวตลอดเพื่อความมั่นคงปลอดภัย

๔.๑.๑.๕ ควรมีการตั้งคณะกรรมการโดยมีฝ่ายต่างๆ ที่เกี่ยวข้องเข้าร่วมเพื่อกำหนดรูปแบบและประเมินความเสี่ยง

๔.๑.๒ มาตรการการรักษาความปลอดภัยด้านข้อมูลข่าวสาร

๔.๑.๒.๑ ควรมีระเบียบข้อมูลข่าวสารโดยกำหนดให้มีผู้ปฏิบัติหน้าที่รับผิดชอบโดยตรง

๔.๑.๒.๒ ควรมีการตั้งคณะกรรมการดูแลชั้นความลับต่างๆ แต่ละชั้นเช่นชั้นความลับมากชั้นความลับที่สุดเป็นต้น

๔.๑.๒.๓ ควรมีกระบวนการทางเทคโนโลยีที่มีระบบรักษาความปลอดภัยเพิ่มเติม

๔.๑.๒.๔ ควรมีการกำหนดชั้นความลับที่ชัดเจนและมีการสร้างความเข้าใจกับผู้ปฏิบัติงาน

๔.๑.๒.๕ ควรมีการตั้งคณะกรรมการเพื่อวิเคราะห์สถานการณ์ข่าวสารบุคคลและสถานที่

๔.๑.๓ มาตรการการรักษาความปลอดภัยด้านสถานที่

๔.๑.๓.๑ ควรจัดให้มีการตรวจจับและจัดให้มีการรักษาความปลอดภัยช่องทางเข้าออก

๔.๑.๓.๒ ควรมีการตรวจสิ่งของผู้เข้าออกสถานที่สำคัญและควรมีการนำเทคโนโลยีมาใช่ร่วมด้วย

๔.๑.๓.๓ ควรมีระเบียบหรือการรักษาความปลอดภัยสถานที่ (Security Plan) โดยเฉพาะ

๔.๑.๓.๔ ควรมีการจัดพื้นที่หวงห้าม (Restricted Area) และการกำหนดสิทธิ์ที่ชัดเจน

๔.๑.๓.๕ ควรมีการวางมาตรการที่เหมาะสมของแต่ละสถานที่โดยควรนำข้อเสนอแนะจากผู้เชี่ยวชาญมีการวิเคราะห์หาจุดอ่อนและควรมีการเพิ่มแสงสว่างในพื้นที่มุมอับต่างๆ

๔.๑.๓.๖ ควรมีการบันทึกบุคคลที่ทำการนัดรวมทั้งมีบุคคลดูแลตลอดเวลา

๔.๑.๓.๗ ควรมีกล้องวงจรปิดเป็นจุดต่างๆโดยจัดเป็นมาตรการเสริม

๔.๑.๓.๘ ควรมีการใช้ฐานข้อมูลที่สามารถตรวจสอบประวัติบุคคลได้ร่วมกันและมีการปรับปรุงให้ทันสมัยตลอดเวลา

๔.๑.๓.๙ ควรมีระบบสำรวจและตรวจสอบ (Survey & Inspection) ทางการรักษาความปลอดภัย

นอกจากนี้ยังพบว่าการสร้างระบบการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้มีประสิทธิภาพนั้นอย่างน้อยควรมีรายละเอียดต่างๆ เบื้องต้นดังนี้ ๑) จัดให้มีพื้นที่การรักษาความปลอดภัย (Restricted Area) ๒) ระบบสัญญาณแจ้งเหตุและการสื่อสาร (Alarm & Communication) ๓) การระมัดระวังและการป้องกันทางวัตถุ (Physical Protection) ๔) การควบคุมบุคคลและ

ยานพาหนะ (Personal & Control) ๕) ระบบยามรักษาการณ์ (Guard Force System) และ ๖) ระบบป้องกันและระงับอัคคีภัยและการหนีไฟ (Fire Protection, Fire Fighting &Fire Escape)

๔.๒ โครงสร้างและรูปแบบการรักษาความปลอดภัยของหน่วยงาน

๔.๒.๑ ควรมีการดำเนินการโดยใช้โครงสร้างตามสายบังคับบัญชาและมีการมอบหมายหน้าที่การดูแลตามลำดับชั้นและกระจายอำนาจอย่างเหมาะสม

๔.๒.๒ ควรมีการแต่งตั้งคณะกรรมการเฉพาะเพื่อดูแลความปลอดภัยในแต่ละหน่วยงานต่างๆ ภายใน

๔.๒.๓ ควรมีการดำเนินงานให้มีเครือข่ายการรักษาความปลอดภัยกับหน่วยงานภายนอกและมีการลงนามความร่วมมือกับหน่วยงานต่างๆ ภายนอกเพื่อช่วยเหลือทางด้านความปลอดภัยระหว่างหน่วยงาน

๔.๒.๔ ควรมีการสร้างความเข้าใจถึงระเบียบและการรักษาความปลอดภัยให้กับบุคลากรในหน่วยงานทุกระดับชั้นยศร่วมถึงสร้างความเข้าใจให้กับชุมชนโดยรอบและประชาชนผู้รับบริการที่มาติดต่อหน่วยงาน

๔.๒.๕ กองทัพควรกำหนดโครงสร้างการบริหารและการจัดการรักษาความปลอดภัยไว้อย่างชัดเจน สำหรับเครื่องมือที่จะนำมาใช้ในการรักษาความปลอดภัยต้องคำนึงถึงความทันสมัยเหมาะสมกับภารกิจทั้งฮาร์ดแวร์และซอฟแวร์ที่จะนำมาทำเป็นระบบรักษาความปลอดภัยอัตโนมัติที่สามารถป้องกันตรวจจับและหน่วงภัยคุกคามนั้นได้

๔.๓ นวัตกรรมและเทคโนโลยีที่ใช้ในด้านการรักษาความปลอดภัยและแนวโน้มในอนาคต

๔.๓.๑ เทคโนโลยีที่เหมาะสมสำหรับการรักษาความปลอดภัย ได้แก่ เทคโนโลยีสมัยใหม่ที่สามารถเข้ากันได้กับการรักษาความปลอดภัยวิธีปกติโดยจะต้องเป็นระบบที่มีการวางโครงสร้างที่ชัดเจน มีศักยภาพในการตรวจตราหรือเตือนภัยอย่างรวดเร็ว และแม่นยำมีความสามารถตอบสนองต่อสถานการณ์เฉพาะหน้าได้เร็วกว่าความสามารถของมนุษย์มีการติดตั้งและทดสอบการใช้งานจริง ตลอดจนสามารถปรับปรุงและพัฒนาให้ระบบการรักษาความปลอดภัยมีสมรรถนะที่ดีขึ้นตามการเปลี่ยนแปลงของเทคโนโลยีที่รวดเร็ว

๔.๓.๒ โครงสร้างต้องประกอบไปด้วยระบบหลักทั้งทางด้านฮาร์ดแวร์และซอฟท์แวร์โดยมีการผสมผสานกับรูปแบบการรักษาความปลอดภัยวิธีปกติรวมถึงมีการเชื่อมโยงข้อมูลความปลอดภัยอัตโนมัติ (Auto-Synchronize) เพื่อให้สามารถนำมาใช้ในการตรวจสอบกำกับติดตามและป้องกันเหตุอันไม่พึงประสงค์กรณีต่างๆ หรือภัยคุกคามที่สามารถมีได้ตลอดเวลา

๔.๓.๓ ควรใช้นวัตกรรมและเทคโนโลยีแบบผสมผสาน (Hybrid) ที่สามารถเชื่อมโยงข้อมูลแบบ Real Time

๔.๓.๔ ควรเป็นระบบป้องกันภัยอิเล็กทรอนิกส์และบนเครือข่ายที่ทำงานแบบบูรณาการเป็นระบบหนึ่งเดียวกันซึ่งสามารถทำให้หน่วยงานหรือองค์กรต่างๆ สามารถป้องกันตรวจจับตรวจสอบและจัดการกับอันตรายเหตุฉุกเฉินและภัยคุกคามได้แบบ Real Time โดยไม่ต้องพึ่งพนักงานเพิ่มเติม

๔.๓.๕ ควรเป็นระบบที่สามารถจับตาดูเหตุการณ์จากระบบเตือนภัยและกล้องวงจรปิดโดยสามารถส่งข้อมูลไปยังผู้ที่เกี่ยวข้องผ่านโทรศัพท์มือถือหรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ

๔.๓.๖ ควรเป็นระบบสนับสนุนการปฏิบัติงานด้านการรักษาความปลอดภัยที่สามารถบันทึกเหตุการณ์ในสถานการณ์ต่างๆ ได้รวมถึงการเรียกดูย้อนหลังหากต้องการหรือจำเป็น

๔.๓.๗ ควรมีอุปกรณ์ประเภท High Security เข้ามาช่วยเสริมสร้างความปลอดภัยให้กับตัวอาคารทั้งภายในและภายนอกอาคารเพื่อป้องกันภัยคุกคามในรูปแบบต่างๆ ที่อาจเกิดขึ้น

๔.๓.๘ ควรเป็นระบบอัจฉริยะ (Smart Security) ที่มีระบบติดต่อสื่อสารรวดเร็วมีการเก็บรักษาข้อมูลด้วยเทคโนโลยี Cloud และต้องมีการ Update อุปกรณ์ให้ทันสมัยตามช่วงระยะเวลาเพื่อก่อให้เกิด Safety Zone อย่างมั่นคง

๔.๓.๙ ควรเป็นรูปแบบที่มีโครงสร้างอย่างง่าย (Simple) และเข้ากันได้กับรูปแบบการรักษาความปลอดภัยวิธีปกติเป็นอย่างดี

๔.๓.๑๐ ควรมีนวัตกรรมและเทคโนโลยีที่สามารถตรวจจับอันตรายระบุหาแหล่งที่มาและจัดการกับภัยคุกคามได้อย่างทันทีและอัตโนมัติโดยไม่ต้องรอให้ใครคอยกดปุ่มสั่งการ

๔.๓.๑๑ ควรมีนวัตกรรมและเทคโนโลยีที่มีการเชื่อมต่อ Firewall แบบ Next Generation โดยสามารถติดต่อสื่อสาร Real Time แบบต่อเนื่อง

๔.๓.๑๒ ควรมีระบบที่สามารถรองรับภัยคุกคามรูปแบบใหม่รวมถึงภัยแฝงในยุคสงคราม Cyberspace ที่มีรูปแบบการโจมตีที่ระบุที่มาไม่ได้

๔.๓.๑๓ ควรมีระบบอัจฉริยะที่สามารถระบุตัวบุคคลหรือยานพาหนะที่เข้ามาในพื้นที่ผ่านระบบคอมพิวเตอร์ และสามารถตัดสินใจได้ว่าบุคคลหรือยานพาหนะนั้นเป็นภัยคุกคามหรือไม่

๔.๓.๑๔ ควรมีระบบที่สามารถประยุกต์ใช้งานด้านอื่นในสถานการณ์ปกติ เช่น การเตือนอัคคีภัยและการเตือนภัยพิบัติจากธรรมชาติที่อาจก่อให้เกิดความเสียหายต่อสถานที่ได้

๔.๓.๑๕ กองทัพอาจจะต้องมีการใช้อากาศยานแบบไร้คนขับหรือโดรนเพื่อบินตรวจตรารักษาความปลอดภัยจากมุมสูงที่มีแนวโน้มนำไปสู่การเปลี่ยนรูปแบบและวิธีการรักษาความปลอดภัยในอนาคตไปโดยสิ้นเชิง

๔.๓.๑๖ นโยบายกองทัพควรมีศูนย์ควบคุมระบบกลาง (Convergence Command Center) ที่สามารถเชื่อมต่อกับหน่วยงานความมั่นคงอื่นเพื่อเฝ้าระวังต่อภัยคุกคามต่างๆ ทุกรูปแบบ

๔.๓.๑๗ ผู้บังคับบัญชาสามารถเข้าถึงตรวจสอบและตัดสินใจได้ง่ายเมื่อเกิดเหตุการณ์ฉุกเฉินหรือสถานการณ์ที่เป็นภัยต่อความมั่นคง

๔.๓.๑๘ เครื่องมือควรประกอบด้วยอุปกรณ์ที่ทันสมัยทั้งทางด้านฮาร์ดแวร์และซอฟท์แวร์ อาทิเช่น

๔.๓.๑๘.๑ ระบบสัญญาณเตือนภัยเชื่อมต่อกับกล้องวงจรปิดที่รองรับทั้งภาษาไทยและภาษาอังกฤษตลอด ๒๔ ชั่วโมง

๔.๓.๑๘.๒ ระบบ Access Control แบบ Multifunction ซึ่งสามารถควบคุมและบันทึกการเข้า-ออกจากงานได้

๔.๓.๑๘.๓ เครื่องตรวจจับโลหะ (หรือเครื่องตรวจแบบสุ่ม)

๔.๓.๑๘.๔ ระบบจัดการการเข้า-ออกสำหรับผู้มาติดต่องานจากหน่วยงานภายนอก

๔.๓.๑๘.๕ ระบบอัจฉริยะกล้องวงจรปิด CCTV แบบเคลื่อนที่และแบบติดตั้งอยู่กับที่ที่สามารถเตือนภัยติดตามและค้นหารวมถึงซอฟท์แวร์ที่ช่วยในการจดจำ

๔.๓.๑๘.๖ เครื่องตรวจจับการเคลื่อนไหวแบบอินฟาเรดที่สามารถทำงานได้ทั้งภายในอาคารและภายนอกอาคาร

๔.๓.๑๘.๗ ระบบการ Backup ข้อมูลไว้ที่ต่างๆ กับหน่วยงานที่น่าเชื่อถือและระบบออนไลน์ที่ปลอดภัย

ส่วนแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่จะประกอบด้วยส่วนสำคัญพื้นฐานดังต่อไปนี้

๑. ความมุ่งหมายของแผน หมายถึง การป้องกันการโจรกรรมการจารกรรมและการก่อวินาศกรรม ส่วนการป้องกันการก่อการร้ายการป้องกันการโจมตีด้วยอาวุธหรือการป้องกันสาธารณะภัยจะไม่อยู่ในแผนนี้โดยตรง ซึ่งอาจจะทำเป็นแผนป้องกันเฉพาะก็ได้

๒. พื้นที่ที่มีการรักษาความปลอดภัยหมายถึง การระบุพื้นที่ขององค์กรหรือหน่วยงานแบ่งเป็นขอบเขตมีเครื่องหมายกำหนดเขตหรืออาจจะทำเป็นแผนผังประกอบก็ได้

๓. มาตรการการควบคุม หมายถึง การกำหนดพื้นที่ของการควบคุมบุคคลยานพาหนะวัตถุที่ผ่านเข้า-ออกตลอดจนมาตรการควบคุมความเคลื่อนไหวระหว่างที่อยู่ในพื้นที่

๔. เครื่องช่วยในการรักษาความปลอดภัย เช่น การป้องกันทางวัตถุแสงสว่างรั้วและสัญญาณแจ้งเหตุรวมถึงการติดตั้งกล้องวงจรปิด

๕. หน่วยรักษาการณ์ หมายถึง การวางกำลังการจัดหน่วยรักษาการณ์และคำแนะนำทั่วไป

๖. การปฏิบัติในกรณีฉุกเฉิน หมายถึง การปฏิบัติเมื่อมีเหตุฉุกเฉินต่อบุคคลหรือต่อหน่วยงาน เช่น การก่อวินาศกรรมและการเกิดไฟไหม้ เป็นต้น

๗. คำแนะนำในการประสานงาน หมายถึง การติดต่อประสานงานกับองค์กรหรือส่วนราชการรวมทั้งการประสานงานกับบุคคลภายนอกตามความเหมาะสมและความจำเป็น

กล่าวโดยสรุปแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคตที่มีประสิทธิภาพ (Efficiency) และประสิทธิผล (Effective) ต้องมีองค์ประกอบพื้นฐาน ๔ ประการด้วยกัน ดังนี้ (Fennelly, Lawrence J. 2012)

๑. เครื่องช่วยในการรักษาความปลอดภัยเกี่ยวกับสถานที่ เช่น รั้ว กำแพง เครื่องมือสื่อสารหรือการติดตั้งกล้องวงจรปิด เป็นต้น

๒. ระเบียบคำสั่งหรือแผนในการรักษาความปลอดภัยกำหนดเขตหวงห้าม ระเบียบควบคุมบุคคลและยานพาหนะที่ผ่านเข้า-ออก ระเบียบการตรวจค้นรวมถึงแผนป้องกันและระงับอัคคีภัย เป็นต้น

๓. การอบรมโดยต้องมีการจัดการอบรมแก่บุคคลในหน่วยงานและองค์กรให้มีความรู้ความเข้าใจและปฏิบัติตามระเบียบโดยทั่วกัน

๔. บุคคลหรือเจ้าหน้าที่รักษาความปลอดภัยซึ่งจะต้องมีบุคคลเพื่อควบคุมความเคลื่อนไหวให้เป็นไปตามระบบและใช้เครื่องมือช่วยในการตรวจพิสูจน์และขัดขวางผู้ที่จะทำให้เกิดความเสียหาย ดังนั้นองค์ประกอบที่สำคัญที่สุดในการรักษาความปลอดภัยก็คือเจ้าหน้าที่รักษาความปลอดภัยเพราะองค์ประกอบอื่นหรือเครื่องมือรวมถึงการควบคุมให้เป็นไปตามระเบียบก็ต้องอาศัยคนหรือเจ้าหน้าที่รักษาความปลอดภัยนั่นเอง

ซึ่งผลงานวิจัยสอดคล้องกับข้อเขียนของ Brad Gray (2005) ที่กล่าวถึงมาตรการด้านการรักษาความปลอดภัยที่มีประสิทธิภาพควรมีรูปแบบเป็นวงจรชีวิต (Security Life Cycle) ที่ประกอบด้วยการวางแผน (Planning) เพื่อกำหนดนโยบาย การวิเคราะห์ (Analysis) เพื่อกำหนด

โครงสร้างที่เหมาะสม การออกแบบ (Design) เพื่อกำหนดกลยุทธ์ การนำไปใช้งานจริง (Implementation) เพื่อการนำไปใช้งานให้มีประสิทธิภาพและประสิทธิผล และการสนับสนุน (Support) เพื่อการพัฒนาระบบให้มีสมรรถนะที่ดีขึ้น และ ๓) ภาคประชาสังคมตระหนักและให้การสนับสนุนเพื่อให้สอดคล้องกับบริบทด้านความปลอดภัยที่เปลี่ยนแปลงไปโดยที่อาจเป็นการให้ความรู้และส่งเสริมให้มีหลักสูตรที่เกี่ยวข้องกับความปลอดภัยในสถานศึกษาเพื่อสร้างความเข้าใจและมีส่วนร่วมตั้งแต่เยาว์วัยและต้องเปิดโอกาสให้ภาคส่วนอื่นๆ ได้แก่ ภาควิชาการ ภาคเอกชน ภาคประชาสังคม และภาคประชาชนเข้ามามีส่วนร่วมอย่างใกล้ชิดหรือเป็นหุ้นส่วนเครือข่ายในการขยายผลกระทั่งนำไปสู่การรักษาความปลอดภัยของทุกสรรพสิ่ง (Security of Things) ต่อไป

ข้อเสนอแนะ

แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคตถือว่าเป็นเรื่องสำคัญที่ต้องดำเนินการให้แล้วเสร็จโดยเร็วที่สุด ทั้งนี้ก็เพื่อกำหนดขีดความสามารถด้านการรักษาความปลอดภัยของบุคลากรและสถานที่ของหน่วยงานทางราชการให้มีความมั่นคงปลอดภัย รวมถึงการนำไปใช้เป็นมาตรการที่สามารถเชื่อมโยงกับภารกิจหลักของหน่วยงานนั้นได้อย่างเป็นรูปธรรม ผู้วิจัยมีข้อเสนอแนะที่ได้จากการวิจัยดังนี้

๑. ข้อเสนอแนะเชิงนโยบาย

๑.๑ กองทัพบกควรกำหนดเป้าหมายที่ชัดเจนว่าจะใช้หลักการรักษาความปลอดภัยรูปแบบใด ทั้งนี้อาจจะใช้หลักการสากลร่วมกับการพัฒนานวัตกรรมและเทคโนโลยีสมัยใหม่ในการพิจารณาว่าจะมีองค์ประกอบที่เหมาะสมอย่างไรเพื่อหาข้อสรุปที่ชัดเจนและนำไปสู่การนำไปใช้ต่อไป

๑.๒ กองทัพบกควรศึกษารูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศเพื่อนำมาใช้ในการเปรียบเทียบสมรรถนะร่วมกันเพื่อนำไปใช้ในการปรับปรุงขีดความสามารถในการรักษาความปลอดภัยให้ทัดเทียมกับสากล

๑.๓ กองทัพบกควรมีหน่วยงานด้านการพัฒนานวัตกรรมและเทคโนโลยีการรักษาความปลอดภัยเป็นการเฉพาะเพื่อให้เกิดการออกแบบและพัฒนารูปแบบและกระบวนการรักษาความปลอดภัยอย่างต่อเนื่อง

๑.๔ กองทัพบกควรส่งเสริมให้เกิดการพัฒนานวัตกรรมและเทคโนโลยีด้านการรักษาความปลอดภัยอย่างเป็นรูปธรรม มีการฝึกปฏิบัติการด้านการรักษาความปลอดภัยเป็นระยะๆ เพื่อให้ทันต่อภัยคุกคามด้านต่างๆ ที่อาจจะเกิดขึ้นได้ทั้งในปัจจุบันและอนาคต

๑.๕ กองทัพไทยควรมีการประสานความร่วมมือและแลกเปลี่ยนเรียนรู้ด้านระบบรักษาความปลอดภัยที่เชื่อมโยงกับนโยบายการรักษาความปลอดภัยแห่งชาติ เพื่อให้รูปแบบของการรักษาความปลอดภัยมีมาตรฐานเดียวกันและเป็นการผนึกกำลังกันเพื่อป้องกันการก่อการร้ายสากล

๒. ข้อเสนอแนะในการวิจัยครั้งต่อไป

๒.๑ ควรมีการศึกษาวิจัยการออกแบบและพัฒนาระบบรักษาความปลอดภัยที่เหมาะสมกับหน่วยงานทางความมั่นคงหรือกองทัพอื่น เพื่อให้เกิดความหลากหลายและเกิดประโยชน์ในการพัฒนางานวิจัยมากยิ่งขึ้น

๒.๒ ควรมีการศึกษาวิจัยการพัฒนาขีดความสามารถทางด้านการรักษาความปลอดภัยเพื่อให้ทัดเทียมกับมาตรฐานการรักษาความปลอดภัยสากล และเกิดประโยชน์ในการนำไปใช้แก้ปัญหาด้านความมั่นคงของหน่วยงานที่ขึ้นตรงกับกองทัพไทยต่อไป

๒.๓ ควรมีการศึกษาวิจัยเชิงลึกยุทธศาสตร์การสร้างระบบรักษาความปลอดภัยที่สามารถเชื่อมโยงและเทียบได้กับมาตรฐานสากล

๒.๔ ควรมีการศึกษาวิจัยเชิงลึกถึงแผนงานและมาตรการในการพัฒนาระบบรักษาความปลอดภัยที่เกี่ยวข้องกับนวัตกรรมและเทคโนโลยีสมัยใหม่ เพื่อให้ได้รูปแบบระบบรักษาความปลอดภัยของกองทัพบกไทยและหน่วยงานทางความมั่นคงที่ทันสมัยมากยิ่งขึ้น

๒.๕ ควรมีการศึกษาวิจัยและพัฒนามาตรฐานด้านการรักษาความปลอดภัยที่สามารถเชื่อมโยงนโยบายแห่งรัฐกับหน่วยงานทางความมั่นคง องค์กรต่อต้านการก่อการร้าย ภาคเอกชน ภาคประชาสังคม และภาคประชาชน เพื่อให้ได้รูปแบบของระบบรักษาความปลอดภัยที่มีประสิทธิภาพภายใต้มาตรฐานเดียวกัน

บรรณานุกรม

ภาษาไทย

ชัยเสฏฐ์ พรหมศรี. “รายงานการวิจัยเรื่อง การพัฒนารูปแบบจิตสำนึกทางด้านการรักษาความปลอดภัยและแผนการฝึกอบรมพัฒนาสำหรับองค์การรักษาความปลอดภัย : กรณีศึกษาของสำนักข่าวกรองแห่งชาติ พ.ศ.๒๕๕๓”. ๒๕๕๓.

เดชน์ จรูญเรืองฤทธิ์. ความรู้พื้นฐานเรื่องการรักษาความปลอดภัยสำหรับผู้บริหาร. กรุงเทพมหานคร : จุฬาลงกรณ์มหาวิทยาลัย, ๒๕๔๙.

นิวัติ เนียมพลอย. “รายงานสรุปของ Joint Publication ๓-๑๓.๓”. Operations Security. ๔ มกราคม ๒๐๑๒.

พงษ์ศักดิ์ ฮงประยูร. มาตรการทางกฎหมายเกี่ยวกับการรักษาความปลอดภัยในการบินพลเรือน: ศึกษาองค์การที่ทำหน้าที่รักษาความปลอดภัยในท่าอากาศยาน. กรุงเทพมหานคร : วารสารสังคมศาสตร์วิชาการปีที่ ๘ ฉบับที่ ๓ ๒๕๕๘.

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒. กรุงเทพมหานคร : สำนักนายกรัฐมนตรี, ๒๕๕๒.

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ (ฉบับที่ ๒) พ.ศ.๒๕๕๔. กรุงเทพมหานคร : สำนักนายกรัฐมนตรี, ๒๕๕๔.

วัชราภรณ์ พิมพา และคณะ. “รายงานการวิจัยเรื่อง การพัฒนาระบบการรักษาความปลอดภัยโดยการประยุกต์ใช้เทคโนโลยีสารสนเทศภูมิศาสตร์ของค่ายสมเด็จพระเอกาทศรถ จังหวัดพิษณุโลก”. ๒๕๔๙.

วิสันติ เลาหอุดมโชค. “ยุทธศาสตร์โลกเพื่อการสร้างเสริมความปลอดภัยและสุขภาพอนามัยในการทำงาน (Vision Zero : A Global Strategy to Promote Safety and Health at Workplace)”. ฝ่ายวิชาการและความร่วมมือระหว่างประเทศ กลุ่มงานยุทธศาสตร์ความปลอดภัยฯ กองความปลอดภัยแรงงาน, ๒๕๕๙.

สภาความมั่นคงแห่งชาติ สำนักงาน สำนักนายกรัฐมนตรี. นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘-๒๕๖๔. กรุงเทพมหานคร : สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา พ.ศ.๒๕๕๘, ๒๕๕๘.

องค์การรักษาความมั่นคงฝ่ายพลเรือน http://www.secnia.go.th เข้าถึงเมื่อ วันที่ ๓ กุมภาพันธ์ พ.ศ. ๒๕๖๐.

ภาษาต่างประเทศ

Baker, Paul R. “Security Construction Projects”. In Baker, Paul R. & Benny, Daniel J. The Complete Guide to Physical Security. CRC Press. ISBN 9781420099638, 2012.

Brad Gray. The Role of the Security Analyst in the Systems Development Life Cycle. SANS Institute, 2005.

Bruce Schneier. Beyond Fear : Thinking about Security in an Uncertain World. Copernicus Books, 2012. pp.26-27.

Fennelly, Lawrence J. “Effective Physical Security”. Butterworth-Heinemann. 2012. pp.345-346.

ISO/IEC 27000:2009 (E). “Information Technology - Security Techniques - Information Security Management Systems”. Overview and Vocabulary. ISO/IEC. 2009.

Military Police : Security of Unclassified Army Property, Sensitive and Nonsensitive, USA form https://dmna.ny.gov/foodservice/docs/references/AR_19051_ Security_of_Army_Prop.pdf, 1993.

Patton, MQ. Qualitative Evaluation and Research Methods (2nd Edition). Thousand Oaks, CA : Sage Publications, 2001.

Reid, Robert N. Guards and Guard forces. Facility Manager's Guide to Security : Protecting Your Assets. The Fairmont Press, 2005.

Rothbauer, Paulette. Triangulation. In Given, Lisa (Ed.), The SAGE Encyclopedia of Qualitative Research Methods. CA : Sage Publications, 2008. pp.892-894.

Spagnoletti, Paolo and Resca A. “The duality of Information Security Management: fighting against predictable and unpredictable threats”. Journal of Information System Security 4 (3), 2008. pp.46-62.

ภาคผนวก

ผนวก ก
รายชื่อผู้เชี่ยวชาญ

ผู้เชี่ยวชาญด้านนวัตกรรมการรักษาความปลอดภัย จำนวน ๓ ท่าน

๑. ดร.เศรษฐชัย ชัยสนิท รองคณบดี วิทยาเขตชลบุรี คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

๒. ผศ.ดร.พงษ์ศักดิ์ ผกามาศ สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก

๓. ผศ.ดร.ชัยวัฒน์ ประสงค์สร้าง คณะศิลปศาสตร์ มหาวิทยาลัยเทคโลยีราชมงคลรัตนโกสินทร์

ผู้มีหน้าที่เกี่ยวข้องด้านการรักษาความปลอดภัยในกองทัพ จำนวน ๔ ท่าน

๑. พลตรีวัฒนะ พลจันทร์ ผู้ช่วยผู้บัญชาการ ศูนย์รักษาความปลอดภัย กองบัญชาการกองทัพไทย

๒. พันเอกชัยรัตน์ จ่างแก้ว รองผู้บัญชาการ โรงเรียนข่าวทหารบก

๓. พันเอกหญิง ดร.นพมาศสิริ วงศ์บา สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก

๔. นายศรายุทธ ทองกูล นักการข่าวเชี่ยวชาญ สำนักข่าวกรองแห่งชาติ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

การสัมมนาอิงผู้เชี่ยวชาญ (Focus Group Discussion) จำนวน ๕ ท่าน ดังนี้

๑. พลโท อดิศรย์ โครพ ผู้ทรงคุณวุฒิพิเศษกองทัพบก

๒. ดร. ธ ธง พวงสุวรรณ ที่ปรึกษาด้านนวัตกรรมและเทคโนโลยี มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

๓. พันเอกธีระพงษ์ ปานเจริญ หัวหน้าแผนกรักษาความปลอดภัยกอง ๗ ศูนย์รักษาความปลอดภัย กองบัญชาการกองทัพไทย

๔. ดร.ประชา ตันเสนีย์ สมาคมผู้ตรวจสอบแห่งประเทศไทย

๕. นางสาวธัญลักษณ์ กริดาคม นักการข่าวชำนาญการ หัวหน้าฝ่ายรักษาความปลอดภัย สำนักข่าวกรองแห่งชาติ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

ผนวก ข
เครื่องมือที่ใช้ในการวิจัย

แบบสัมภาษณ์งานวิจัย

เรื่อง แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

กลุ่มเป้าหมาย ผู้ที่มีหน้าที่เกี่ยวข้องกับการรักษาความปลอดภัยในกองทัพ

คำชี้แจง วัตถุประสงค์ของแบบสัมภาษณ์เพื่อนำไปใช้ในการกำหนดร่าง “แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต” โดยแบบสัมภาษณ์จะมีประเด็นสำคัญ ได้แก่

๑. นโยบายการรักษาความปลอดภัยของกองทัพเป็นอย่างไร

๒. มาตรการการรักษาความปลอดภัยของหน่วยงานท่านเป็นอย่างไร

๒.๑ ด้านบุคคล

๒.๒ ด้านข้อมูลข่าวสาร

๒.๓ ด้านสถานที่

๓. โครงสร้างและรูปแบบการรักษาความปลอดภัยของหน่วยงานท่านเป็นอย่างไร

๔. ภัยคุกคามใดที่ส่งผลกระทบต่อการรักษาความปลอดภัยในหน่วยงานของท่าน

๕. มาตรฐานด้านการรักษาความปลอดภัยของหน่วยงานเป็นอย่างไร

๖. การเปลี่ยนแปลงด้านการเมืองและสังคมส่งผลกระทบต่อการรักษาความปลอดภัยอย่างไร

๗. นวัตกรรมและเทคโนโลยีที่ใช้ในด้านการรักษาความปลอดภัยในปัจจุบันและแนวโน้มในอนาคต

๘. ยุคเศรษฐกิจดิจิทัลจะต้องมีนโยบายและมาตรการการรักษาความปลอดภัยอย่างไร

๙. นวัตกรรมและเทคโนโลยีที่เหมาะสมในยุคไทยแลนด์ ๔.๐ ควรเป็นอย่างไร

๑๐. รูปแบบการรักษาความปลอดภัยที่เหมาะสมที่จะนำมาใช้สำหรับกองทัพบกในอนาคต

๑๑. แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคตควรเป็นอย่างไร

จบการสัมภาษณ์

แบบสัมภาษณ์งานวิจัย

เรื่อง แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

กลุ่มเป้าหมาย ผู้เชี่ยวชาญด้านนวัตกรรมการรักษาความปลอดภัย

คำชี้แจง วัตถุประสงค์ของแบบสัมภาษณ์นี้เพื่อนำไปใช้ในการกำหนดร่าง “แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต” โดยแบบสัมภาษณ์จะมีประเด็นสำคัญได้แก่

๑. นโยบายและเทคโนโลยีที่เหมาะสมสำหรับการรักษาความปลอดภัยของกองทัพ

๒. กองทัพควรมีโครงสร้างและเครื่องมือในด้านการรักษาความปลอดภัยอย่างไร

๓. ภัยคุกคามใดที่ส่งผลกระทบต่อระบบรักษาความปลอดภัย

๔. นวัตกรรมและเทคโนโลยีที่เหมาะสมสำหรับการรักษาความปลอดภัยของกองทัพ

๕. การเปลี่ยนแปลงทางด้านการเมือง เศรษฐกิจ และสังคมส่งผลกระทบต่อระบบรักษาความปลอดภัยอย่างไร

๖. รูปแบบของนวัตกรรมและเทคโนโลยีที่เหมาะสมสำหรับการรักษาความปลอดภัยของกองทัพบกในอนาคต

จบการสัมภาษณ์

ประวัติย่อผู้วิจัย

ชื่อ พลตรี วาสิฏฐ์ มณีโชติ

วัน เดือน ปี เกิด ๒๒ ตุลาคม ๒๕๐๓

การศึกษา **หลักสูตรทางทหาร**

- นักเรียนเตรียมทหารรุ่นที่ ๒๑
- นักเรียนนายร้อย จปร.รุ่นที่ ๓๒
- หลักสูตรชั้นนายร้อย เหล่าทหารราบ ศูนย์การทหารราบ
- หลักสูตรชั้นนายพัน เหล่าทหารราบ ศูนย์การทหารราบ
- หลักสูตรเสนาธิการทหารบก (หลักสูตรหลักประจำชุดที่ ๗๓)
  โรงเรียนเสนาธิการทหารบก

หลักสูตรทางพลเรือน

- รัฐประศาสนศาสตรมหาบัณฑิต มหาวิทยาลัยราชภัฏสวนสุนันทา

ประวัติการทำงาน **ณ ที่ตั้งหน่วย**

- ผู้บังคับหมวดปืนเล็ก กองพันทหารราบที่ ๓ กรมทหารราบที่ ๑๙
- รองผู้บังคับกองร้อยอาวุธเบา กองพันทหารราบที่ ๓ กรมทหารราบที่ ๑๙
- ผู้บังคับกองร้อยอาวุธเบา กองพันทหารราบที่ ๓ กรมทหารราบที่ ๑๙
- ผู้ช่วยหัวหน้าฝ่ายยุทธการ กองพลทหารราบที่ ๙
- รองผู้บังคับกองพันทหารราบที่ ๑ กรมทหารราบที่ ๙
- หัวหน้าฝ่ายกำลังพล กองพลทหารราบที่ ๙
- ผู้บังคับกองพันทหารราบที่ ๑ กรมทหารราบที่ ๙
- รองเสนาธิการ กองพลทหารราบที่ ๙
- รองผู้บังคับการกรมสนับสนุน กองพลทหารราบที่ ๙
- รองผู้บังคับการกรมทหารราบที่ ๙
- เสนาธิการกองพลทหารราบที่ ๙
- ผู้บังคับการกรมสนับสนุนกองพลทหารราบที่ ๙
- ผู้บังคับการกรมทหารราบที่ ๒๙
- รองผู้บัญชาการกองพลทหารราบที่ ๙

ราชการสนามชายแดน

- ปฏิบัติงานตามแผนป้องกันประเทศของกองกำลังสุรสีห์ และราชการสนามอื่นๆ รวมระยะเวลา ๑๙ ปี

งานการเมือง

- นักวิชาการประจำคณะกรรมมาธิการการคมนาคม (๒๕๕๘-๒๕๕๙)
- คณะทำงานของที่ปรึกษานายกรัฐมนตรี (พลเอก สกล ชื่นตระกูล ที่ปรึกษานายกรัฐมนตรีด้านความมั่นคง/ผู้แทนพิเศษของรัฐบาล ๒๕๕๙-๒๕๖๐)

ตำแหน่งปัจจุบัน ผู้ทรงคุณวุฒิกองทัพบก

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

ผู้วิจัย พลตรี วาสิฏฐ์ มณีโชติ หลักสูตร วปอ. รุ่นที่ ๕๙

ตำแหน่ง ผู้ทรงคุณวุฒิกองทัพบก

ความเป็นมาและความสำคัญของปัญหา

หลังสิ้นสุดสงครามเย็น โลกได้พัฒนาเข้าสู่ยุคแห่งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วและไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยีได้นำมา ซึ่งการเคลื่อนย้ายอย่างเสรีของผู้คน สินค้าและการบริการได้เพิ่มจำนวนขึ้นในอัตราที่ไม่เคยปรากฏมาก่อน เกิดความเชื่อมโยงอย่างกว้างขวางที่ทำให้บุคคลหรือผู้แสดงบทบาทที่ไม่ใช่รัฐ (Non-state actor) มีอิทธิพลมากขึ้นในการดำเนินกิจกรรมต่างๆ ทั้งในระดับโลก ภูมิภาคหรือภายในรัฐชาติหนึ่งรัฐชาติใด อันส่งผลให้เกิดความท้าทายต่อความเป็นรัฐชาติ รวมถึงองค์การระหว่างประเทศ ประเทศที่พัฒนาแล้วได้ให้ความสนใจกับระบบธรรมาภิบาลในงานด้านความมั่นคง (Security Sector Governance : SSG) ของประเทศต่างๆ

ในส่วนของประเทศไทยก็กำลังเผชิญกับยุคแห่งการเปลี่ยนแปลงที่รวดเร็วมากขึ้น และภายใต้กระแสประชาธิปไตย และสิทธิมนุษยชนของโลกในยุคปัจจุบันนั้น ประเทศไทยได้มีพัฒนาการทางการเมืองอย่างต่อเนื่อง ภายใต้การปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ซึ่งในทศวรรษที่ผ่านมาประชาชนได้มีความตื่นตัวในการมีส่วนร่วมทางการเมืองมากขึ้นและในหลายรูปแบบ อาทิ การจัดตั้งพรรคการเมืองขึ้นใหม่ การจัดตั้งกลุ่มผลประโยชน์และการรวมตัวกันเพื่อเรียกร้องสิทธิประโยชน์และความต้องการของกลุ่มมีจำนวนเพิ่มมากขึ้น ปัญหาการก่อเหตุรุนแรง อาทิ ก็อดอาร์มี่บุกยึดโรงพยาบาลศูนย์ราชบุรี การปล้นปืน (คลังอาวุธ) ของกองพันพัฒนาที่ ๔ และการก่อเหตุรุนแรงในจังหวัดชายแดนภาคใต้ยังคงมีอยู่ และได้นำมาซึ่งความรุนแรงของปัญหาตั้งแต่ พ.ศ. ๒๕๔๗ โดยในห้วงเวลาที่ผ่านมาได้เกิดความสูญเสียทั้งชีวิตประชาชนผู้บริสุทธิ์และเจ้าหน้าที่รัฐ รวมถึงงบประมาณจำนวนมาก ซึ่งยังคงเป็นปัญหาระดับชาติที่ทุกรัฐบาลกำหนดเป็นนโยบายเร่งด่วนในการแก้ไขปัญหาเพื่อความสงบสุขกลับคืนสู่พื้นที่โดยเร็วที่สุด ทั้งนี้จากการดำเนินการของทุกรัฐบาลอย่างจริงจัง ทำให้สถานการณ์ความรุนแรงมีแนวโน้มที่ดีขึ้น การที่ประเทศไทยมีที่ตั้งทางยุทธศาสตร์ที่

สำคัญยิ่ง โดยเป็นพื้นที่ศูนย์กลางของภูมิภาคเอเชียตะวันออกเฉียงใต้ที่สามารถเชื่อมโยงประเทศเพื่อนบ้าน และอยู่ใกล้ประเทศที่มีประชากรโลกมากที่สุด ๒ ลำดับแรก คือ จีน และ อินเดีย จึงได้นำมาซึ่งปัญหาความมั่นคงของไทยที่มีความยุ่งยากสลับซับซ้อนเพิ่มขึ้นในอีกหลายมิติ ไม่ว่าจะเป็นปัญหาการค้ายาเสพติด การค้ามนุษย์ อาชญากรรมคอมพิวเตอร์ การก่อการร้ายสากล และปัญหาการแพร่ระบาดของยาเสพติดภายในประเทศ ซึ่งส่งผลกระทบต่อสภาพสังคมและความมั่นคงในระยะยาว นอกจากนี้ปัญหาสิ่งแวดล้อมและภัยธรรมชาติเป็นอีกปัญหาหนึ่งที่สำคัญของไทยเป็นปัญหาที่เกิดจากความเสื่อมโทรมของธรรมชาติ และภัยพิบัติทางธรรมชาติ (ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒)

ดังนั้นจากปัญหาและการเปลี่ยนแปลงข้างต้นการวางมาตรการและการกำหนดวิธีปฏิบัติเพื่อรักษาความปลอดภัยควรเป็นไปเพื่อรองรับตามระดับความสำคัญ หน้าที่ความรับผิดชอบ และกำลังงบประมาณของหน่วยงาน เนื่องจากส่วนงานต่างๆ ตามโครงสร้างที่ประกอบขึ้นเป็นหน่วยงานของกองทัพแต่ละส่วนมีระดับความสำคัญต่อหน่วยงานต่างกัน อย่างไรก็ตาม จากปัญหาด้านการรักษาความปลอดภัยและความสำคัญของหน่วยงานทางความมั่นคง จึงมีความจำเป็นในการพัฒนามาตรฐานการรักษาความปลอดภัย โดยทำการศึกษาเทคโนโลยีที่ทันสมัยและเหมาะสมมาใช้ในการรักษาความปลอดภัย มาตรฐานการรักษาความปลอดภัยจึงเป็นแนวทางหนึ่งที่เหมาะสมที่สามารถนำมาใช้แก้ปัญหาและสร้างความมั่นคงให้กับความปลอดภัยของหน่วยงานทางความมั่นคงได้เป็นอย่างดี ผู้วิจัยจึงเกิดแนวคิดและความสนใจที่จะศึกษาแนวทางและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยของกองทัพในอนาคต โดยการศึกษาค้นคว้าเพื่อดำเนินการออกแบบ วิเคราะห์ และสังเคราะห์แนวทางและรูปแบบที่เหมาะสมของการรักษาความปลอดภัยของกองทัพ ส่งผลให้เกิดแนวทางมาตรฐานที่สามารถนำไปใช้งานได้จริงและมีความมั่นคงปลอดภัยต่อการรักษาความปลอดภัยของกองทัพ ดังนั้นการจัดทำวิจัยดังกล่าวจึงสามารถแก้ปัญหาและเป็นไปตามนโยบายของประเทศที่จะเปลี่ยนแปลงในอนาคตต่อไป

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษารูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน

๒. เพื่อศึกษารูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ

๓. เพื่อศึกษารูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

๔. เพื่อนำเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

ขอบเขตของการวิจัย

การศึกษาวิจัยครั้งนี้เป็นการศึกษาหาแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต โดยการศึกษา ค้นคว้า รวบรวม ทบทวน วิเคราะห์ และสังเคราะห์ ตามระเบียบวิธีวิจัยเชิงคุณภาพ โดยกำหนดขอบเขตการวิจัยดังนี้

๑. ศึกษาค้นคว้าเชิงเปรียบเทียบแนวคิดและความเป็นมาของรูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน

๒. ศึกษาค้นคว้าเชิงเปรียบเทียบแนวคิดและความเป็นมาของรูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ

๓. ศึกษารวบรวม วิเคราะห์ และสังเคราะห์รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

๔. ศึกษาทบทวนและให้ข้อเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกให้มีประสิทธิภาพมากยิ่งขึ้น และรองรับภัยคุกคามและความท้าทายในอนาคต

วิธีดำเนินการวิจัย

การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research Methodology) โดยมีจุดมุ่งหมายเพื่อนำเสนอแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต โดยมีขั้นตอนการดำเนินการวิจัยตามลำดับดังต่อไปนี้

๑. ศึกษาเอกสาร รายงาน งานวิจัยที่เกี่ยวข้อง รายงานการวิจัย และบทความวิชาการต่างๆ เพื่อสร้างกรอบแนวคิดในการวิจัย

๒. ออกแบบเครื่องมือที่ใช้ในการวิจัยและทดสอบการใช้เครื่องมือเบื้องต้น โดยเครื่องมือที่ใช้ต้องผ่านการตรวจสอบความเที่ยงตรงเชิงเนื้อหาจากผู้เชี่ยวชาญ

๓. เก็บรวบรวมข้อมูลเชิงลึกตามกระบวนการวิจัยเชิงคุณภาพและใช้ตรวจสอบข้อมูลโดยใช้เทคนิควิธีการสามเส้า (Triangulation Technique) (Somarie Holtzhausen, 2001 และ Rothbauer Paulette, 2008) โดยมีข้อมูลปฐมภูมิและทุติยภูมิ ดังนี้

๓.๑ ข้อมูลปฐมภูมิ (Primary) ดำเนินการโดยการสัมภาษณ์แบบเชิงลึกผู้ที่มีหน้าที่เกี่ยวข้องกับการรักษาความปลอดภัยในกองทัพ จำนวน ๔ คน และสัมภาษณ์แบบเชิงลึกผู้เชี่ยวชาญด้านนวัตกรรมการรักษาความปลอดภัย จำนวน ๓ คน

๓.๒ ข้อมูลทุติยภูมิ (Secondary) ได้จากเอกสารที่เกี่ยวข้อง อาทิ กฎหมาย ระเบียบ วารสาร บทความทางวิชาการ รายงานวิจัย และเอกสารสื่อสิ่งพิมพ์อิเล็กทรอนิกส์ทั้งในและต่างประเทศ รวมทั้งผลการสัมมนาและการทบทวนแนวทางด้านการรักษาความปลอดภัยของกองทัพ รวมถึงฝ่ายพลเรือนในแต่ละกระทรวง

๔. การวิเคราะห์และสังเคราะห์ข้อมูลตามหลักการวิจัยเชิงคุณภาพโดยวิธีพรรณนาเชิงวิเคราะห์ (Patton MQ, 2001)

๕. ร่างแนวทาง กำหนดแผนงานหรือมาตรการที่เกี่ยวข้อง และข้อเสนอแนะเชิงนโยบาย

๖. ตรวจสอบแนวทางโดยการสัมมนาอิงผู้เชี่ยวชาญ (Focus Group Discussion) โดยอาศัยความรู้ ความเชี่ยวชาญ และประสบการณ์ของผู้วิจัย ร่วมกับความเห็นของผู้ทรงคุณวุฒิ โดยใช้การสัมภาษณ์แบบไม่มีโครงสร้าง (Unstructured Interview) จากการเลือกผู้เชี่ยวชาญและผู้ทรงคุณวุฒิแบบเจาะจง เพื่อยืนยันแนวทาง (Confirmatory) ในด้านการรักษาความปลอดภัยที่มีประสิทธิภาพ

๗. สรุปและเขียนรายงานการวิจัยฉบับสมบูรณ์

ผลการวิจัย

ผลการวิจัยแนวทางการพัฒนามาตรฐานการรักษาความปลอดภัยของกองทัพบกในอนาคต

๑. รูปแบบการรักษาความปลอดภัยของกองทัพไทยในอดีตจนถึงปัจจุบัน

รูปแบบการรักษาความปลอดภัยในอดีตจนถึงปัจจุบันได้มีการวางมาตรการและการกำหนดวิธีปฏิบัติ เพื่อรักษาความปลอดภัยตามระดับความสำคัญ หน้าที่ความรับผิดชอบ และกำลังงบประมาณของหน่วยงาน เนื่องจากส่วนงานต่างๆ ตามโครงสร้างที่ประกอบขึ้นเป็นหน่วยงานของกองทัพแต่ละส่วนมีระดับความสำคัญต่อหน่วยงานต่างกัน อีกทั้งกองทัพยังมีการเพิ่มศักยภาพด้านการรักษาความปลอดภัยด้วยการฝึกอบรมกำลังพลและผู้ที่เกี่ยวข้องอยู่เสมอ

๒. รูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศ

รูปแบบการรักษาความปลอดภัยในหลายภูมิภาคซึ่งมีหลากหลายทางเชื่อชาติ ศาสนา ประเทศ และหลากหลายแนวคิด ล้วนขึ้นกับการแบ่งประเภทการรักษาความปลอดภัยของแต่ละประเทศและองค์กร อย่างไรก็ตามประเทศชั้นนำของภูมิภาคต่างๆ ต่างยึดรูปแบบการดำเนินการทางการทหารสมัยใหม่ตามรูปแบบของกองทัพสหรัฐอเมริกาเป็นส่วนใหญ่ รวมถึงมีการปรับปรุงรูปแบบและวิธีการรักษาความปลอดภัยด้านสถานที่ให้เหมาะสมในอนาคตอยู่เสมอ ทั้งนี้ศักยภาพของรูปแบบและวิธีการอาจขึ้นอยู่กับลักษณะภูมิประเทศและสภาพทางเศรษฐกิจของประเทศนั้นด้วย

๓. รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคตจากการสัมมนาอิงผู้เชี่ยวชาญในหัวข้อที่ผ่านมาพบว่าประกอบด้วย ๕ องค์ประกอบสำคัญ ได้แก่ ๑) นโยบายด้านความปลอดภัย ๒) การกำหนดแนวปฏิบัติ โครงสร้าง และรูปแบบการรักษาความปลอดภัยของหน่วยงานความมั่นคง ๓) นวัตกรรมและเทคโนโลยี ๔) กระบวนการสร้างความเข้าใจกับประชาชนและเจ้าหน้าที่ และ ๕) การบริหารและการประเมินความเสี่ยง

รูปแบบที่เหมาะสมของการรักษาความปลอดภัยที่จะนำมาใช้ในกองทัพบกในอนาคต

ข้อเสนอแนะ

ข้อเสนอแนะเชิงนโยบาย

๑ กองทัพบกควรกำหนดเป้าหมายที่ชัดเจนว่าจะใช้หลักการรักษาความปลอดภัยรูปแบบใด ทั้งนี้อาจจะใช้หลักการสากลร่วมกับการพัฒนานวัตกรรมและเทคโนโลยีสมัยใหม่ในการพิจารณาว่าจะมีองค์ประกอบที่เหมาะสมอย่างไร เพื่อหาข้อสรุปที่ชัดเจนและนำไปสู่การนำไปใช้ต่อไป

๒ กองทัพบกควรศึกษารูปแบบการรักษาความปลอดภัยของกองทัพในต่างประเทศเพื่อนำมาใช้ในการเปรียบเทียบสมรรถนะร่วมกันเพื่อนำไปใช้ในการปรับปรุงขีดความสามารถในการรักษาความปลอดภัยให้ทัดเทียมกับสากล

๓ กองทัพบกควรมีหน่วยงานด้านการพัฒนานวัตกรรมและเทคโนโลยีการรักษาความปลอดภัยเป็นการเฉพาะเพื่อให้เกิดการออกแบบและพัฒนารูปแบบและกระบวนการรักษาความปลอดภัยอย่างต่อเนื่อง

๔ กองทัพไทยควรส่งเสริมให้เกิดการพัฒนานวัตกรรมและเทคโนโลยีด้านการรักษาความปลอดภัยอย่างเป็นรูปธรรม มีการฝึกปฏิบัติการด้านการรักษาความปลอดภัยเป็นระยะๆ เพื่อให้ทันต่อภัยคุกคามด้านต่างๆ ที่อาจจะเกิดขึ้นได้ทั้งในปัจจุบันและอนาคต