ร่างรายละเอียดตัวชี้วัดตามคำรับรองการปฏิบัติราชการของ กองบัญชาการกองทัพไทย
ประจำปีงบประมาณ พ.ศ.๒๕๖๕

ตัวชี้วัดที่ ๓ : ผลการประเมินสถานะความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ ของ บก.ทท.

๑. น้ำหนัก : ร้อยละ ๒๐

๒. หลักการ เหตุผล ความจำเป็น ในการกำหนดตัวชี้วัด :

กองบัญชาการกองทัพไทย (บก.ทท.) โดยศูนย์ไซเบอร์ทหาร (ศซบ.ทหาร) ในฐานะหน่วยงานหลักที่รับผิดชอบในการ ๑) การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ บก.ทท. ๒) การบูรณาการการปฏิบัติการร่วมทางไซเบอร์ของกองทัพไทย ๓) เป็นหน่วยงานกลางหลักสูตร/การฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ และ ๔) สามารถปฏิบัติการในมิติทางไซเบอร์เพื่อสนับสนุนรัฐบาลและประเทศได้ (ตาม พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในระดับสถานการณ์วิกฤติ) ซึ่ง บก.ทท. จะต้องมีความพร้อมในการปฏิบัติการทางไซเบอร์ทั้งในสภาวะปกติ (การรักษาความมั่นคงปลอดภัยทางไซเบอร์ : Cyber Security) ในระดับ บก.ทท. และในสภาวะไม่ปกติ (สงครามไซเบอร์ : Cyber Warfare) ในระดับ ทท. ซึ่งเชื่อมโยงและสอดคล้องกับยุทธศาสตร์ชาติ แผนแม่บทภายใต้ประเด็นยุทธศาสตร์ชาติด้านความมั่นคง ตลอดจนแผนระดับ ๒ และแผนระดับ ๓ อื่นๆ ที่เกี่ยวข้อง โดยสรุป บก.ทท. มีการดำเนินการพัฒนาขีดความสามารถและศักยภาพด้านไซเบอร์เพื่อเตรียมความพร้อมในการปฏิบัติการทางไซเบอร์อย่างต่อเนื่องและเป็นระบบทั้ง ๓ ระดับ คือ ระดับ บก.ทท. (การรักษาความมั่นคงปลอดภัยทางไซเบอร์) ระดับ ทท. (ปฏิบัติการร่วมทางไซเบอร์) และระดับประเทศ (ปฏิบัติการสนับสนุน) ทั้งนี้ การดำเนินการดังกล่าว บก.ทท. มีการวิเคราะห์วางแผน กำกับดูแล การติดตามประเมินผล และการบริหารจัดการทรัพยากรทางทหารทั้งมวล โดยมุ่งหมายให้ บก.ทท. มีการพัฒนาและยกระดับของขีดความความสามารถและศักยภาพความพร้อมทางไซเบอร์ที่สามารถพึ่งพาตนเองได้อย่างยั่งยืนในอนาคต โดยมีความพร้อมในการปฏิบัติการในมิติทางไซเบอร์ในทุกระดับ โดยเฉพาะในการติดตาม ป้องกัน แก้ไข และรับมือกับปัญหาความมั่นคงทุกมิติทุกรูปแบบและทุกระดับแบบบูรณาการ (ปัญหาความมั่นคงของประเทศในภาพรวมด้านไซเบอร์ลดลงอย่างมีนัยสำคัญ) โดยดำเนินการภายใต้กรอบแนวคิดการประเมินความพร้อม (RTARF Readiness Assessment Framework) ของ บก.ทท. ในมิติทางไซเบอร์ทั้งเชิงรับและเชิงรุก ในด้านการป้องกันประเทศและความมั่งคงของรัฐ ผ่านระบบการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Center Operations : NCO) ของกองทัพไทยสามารถวัดและประเมินผลสถานะความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ บก.ทท. ด้วยองค์ประกอบ ๓ ด้าน ได้แก่ ด้านกำลังพล ด้านยุทโธปกรณ์ และ ด้านระบบ

๓. ความเชื่อมโยง : นโยบายที่สำคัญ

แผน ได้แก่

๑.๑ แผนระดับ ๑ : ยุทธศาสตร์ชาติ (พ.ศ.๒๕๖๑ - ๒๕๘๐) : ยุทธศาสตร์ที่ ๑ ด้านความมั่นคง

๑.๒ แผนระดับ ๒

๑.๒.๑ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ : ประเด็นด้านความมั่นคง แผนงานย่อยการพัฒนาศักยภาพของประเทศ

๑.๒.๒ แผนการปฏิรูปประเทศ

๑.๒.๓ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ : ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน

๑.๒.๔ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ พ.ศ.๒๕๖๒ – ๒๕๖๕

๑.๒.๕ แผนแม่บทเฉพาะกิจภายใต้ยุทธศาสตร์ชาติ อันเป็นผลกระทบมาจากสถานการณ์ Covid-๑๙

๑.๓ แผนระดับ ๓

๑.๓.๑ แผนปฏิบัติการด้านการปกป้องอธิปไตยและการรักษาผลประโยชน์ของชาติ ระยะที่ ๑ (พ.ศ.๒๕๖๓ – ๒๕๖๕) ทท.

๑.๓.๒ แผนปฏิบัติการด้านการพัฒนาศักยภาพของประเทศด้านความมั่นคง ระยะที่ ๑ (พ.ศ.๒๕๖๓ - ๒๕๖๕)

๑.๔ กฎหมายสำคัญ/แผน/นโยบายอื่น ๆ ที่เกี่ยวข้อง

๑.๔.๑ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๑.๔.๒ นโยบาย รมว.กห. (ด้านไซเบอร์) / นโยบาย ผบ.ทสส. (ด้านไซเบอร์)

๑.๔.๓ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. พ.ศ.๒๕๖๔

๑.๔.๔ (ร่าง) แผนปฏิบัติการด้านการปกป้องอธิปไตยและผลประโยชน์ของชาติ (ด้านไซเบอร์) ทท. ซึ่งปรับปรุงจากยุทธศาสตร์ทหารด้านสงครามไซเบอร์ ทท. พ.ศ.๒๕๕๘

๑.๔.๕ (ร่าง) หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ ทท. พ.ศ... (ฉบับปรับปรุง) ซึ่งปรับปรุงจากหลักนิยมการปฏิบัติการร่วมทางไซเบอร์ ทท. พ.ศ.๒๕๕๘

๑.๔.๖ (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์ บก.ทท. พ.ศ...

องค์ประกอบ ได้แก่

องค์ประกอบที่ ๑ (Function Base)

องค์ประกอบที่ ๔ (Innovation Base)

องค์ประกอบที่ ๕ (Potential Base)

๔. เป้าประสงค์ :

๔.๑ บก.ทท. มีความมั่นคงปลอดภัยทางไซเบอร์

๔.๒ บูรณาการการปฏิบัติการร่วมทางไซเบอร์ ทท.

๔.๓ พัฒนาศักยภาพและเพิ่มมีขีดความสามารถ บก.ทท. และ ทท. ให้มีความพร้อมในการปฏิบัติการในมิติทางไซเบอร์ เพื่อสนับสนุนรัฐบาลและประเทศ ตามบทบาทและอำนาจหน้าที่ที่กฎหมายกำหนด

๕. คำอธิบายตัวชี้วัด :

๕.๑ ขั้นตอนการดำเนินการ

เป็นการวัดความสำเร็จของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยสะท้อนสถานะความพร้อมด้วยองค์ประกอบ ๓ ด้าน ได้แก่ ด้านกำลังพล ด้านยุทโธปกรณ์ และ ด้านระบบ

๑. ด้านกำลังพล : มิติเชิงคุณภาพ น้ำหนักร้อยละ ๓๐

ร้อยละอัตรากำลังพลที่บรรจุในตำแหน่งด้านไซเบอร์ของ บก.ทท. ที่มีใบ Certificate สากลด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือสำเร็จหลักสูตรปรับพื้นฐานบุคลากรทางไซเบอร์

วิธีการประเมินผลความสำเร็จ

$$\text{สูตร ร้อยละของ .... } = \frac{\text{จำนวนผู้สำเร็จหลักสูตรฯ และ/หรือมีใบ Certificate}}{\text{อัตรากำลังพลที่บรรจุในตำแหน่งด้านไซเบอร์ของ บก.ทท. (ณ ๓๐ ก.ย.๖๔ อัตราบรรจุ จำนวน ๖๔ นาย)}} \times ๑๐๐$$

หมายเหตุ

๑. การนับจำนวนผู้มีใบ Certificate หรือผู้ที่สำเร็จหลักสูตรปรับพื้นฐานบุคลากรทางไซเบอร์ จำนวนรวมทั้งสิ้น ๖๔ อัตรา โดยนับจากกำลังพลของ ศซบ.ทหาร เฉพาะผู้ที่ปฏิบัติหน้าที่หรือบรรจุในตำแหน่งอัตราของ

๑.๑ กองยุทธการและการข่าว (กยข.ฯ) อัตรา อฉก. ๒๓ บรรจุจริง ๑๕ นำมาคิดคำนวณได้ ๑๓ อัตรา (หัก ๒ อัตรา คือ ประจำกอง ๑ อัตรา และเสมียนกอง ๑ อัตรา)

๑.๒ กองวิทยาการ (กวก.ฯ) อัตรา อฉก ๒๗ บรรจุจริง ๑๕ นำมาคิดคำนวณได้ ๑๓ อัตรา (หัก ๒ อัตรา คือ ประจำกอง ๑ อัตรา และเสมียนกอง ๑ อัตรา)

๑.๓ กองปฏิบัติการ (กปก.ฯ) อัตรา อฉก ๓๐ บรรจุจริง ๒๒ นำมาคิดคำนวณได้ ๒๐ อัตรา (หัก ๒ อัตรา คือ ประจำกอง ๑ อัตรา และเสมียนกอง ๑ อัตรา)

๑.๔ กองรักษาความปลอดภัย (กรภ.ฯ) อัตรา อฉก ๓๕ บรรจุจริง ๒๐ นำมาคิดคำนวณได้ ๑๘ อัตรา (หัก ๒ อัตรา คือ ประจำกอง ๑ อัตรา และเสมียนกอง ๑ อัตรา)

๒. ด้านยุทโธปกรณ์ : มิติเชิงคุณภาพ น้ำหนักร้อยละ ๓๐

ร้อยละของยุทโธปกรณ์สนับสนุนการปฏิบัติงานด้านไซเบอร์ ซึ่งปฏิบัติงานรองรับ ๖ ส่วนงาน

ส่วนควบคุมบังคับบัญชา Command & Control	ส่วนข่าวกรองทางไซเบอร์ CTI	ส่วนเฝ้าระวังภัยคุกคามทางไซเบอร์ CSM
ส่วนรับมือเหตุการณ์ IR	ส่วนพิสูจน์หลักฐานทางดิจิทัล Digital Forensics	ส่วนตรวจสอบและประเมินผล Audit & SA

วิธีการประเมินผลความสำเร็จ

$$\text{สูตร ร้อยละของ .... } = \frac{\text{จำนวนยุทโธปกรณ์ที่มีพร้อมใช้งาน}}{\text{จำนวนยุทโธปกรณ์สนับสนุนการปฏิบัติงานด้านไซเบอร์เพื่อรองรับ ๖ ส่วนงาน}} \times ๑๐๐$$

<u>เงื่อนไข</u> กรณีเกิดปัญหาข้อขัดข้องอันเกิดจากปัจจัยภายนอกที่ไม่สามารถควบคุมได้และ/หรือไม่ได้รับการจัดสรรงบประมาณหรือได้รับงบประมาณไม่เพียงพอ จะไม่นำมาพิจารณา

๓. ด้านระบบ : มิติด้านการฝึก คิดเป็นน้ำหนักร้อยละ ๔๐

๓.๑ ร้อยละคะแนนเฉลี่ยของการประเมินผลการฝึกระดับ บก.ทท. น้ำหนักร้อยละ ๑๕

การฝึกในระดับกองบัญชาการกองทัพไทย เรียกว่า การฝึกตามหน้าที่และหลักพื้นฐานการปฏิบัติการทางไซเบอร์ มีวัตถุประสงค์และขั้นตอนการฝึกดังนี้

๑) วัตถุประสงค์การฝึก เพื่อตรวจสอบความรู้ความเข้าใจในการปฏิบัติหน้าที่และขีดความสามารถในการปฏิบัติการทางไซเบอร์.ของผู้ปฏิบัติงานด้านไซเบอร์ของ บก.ทท. ของ หน่วย ศซบ.ทหาร และหน่วยเกี่ยวข้องใน บก.ทท. เพื่อนำผลการประเมินไปทบทวน วิเคราะห์ และปรับปรุงพัฒนาการฝึกในครั้งต่อไปให้มีประสิทธิภาพและประสิทธิผลมากขึ้น

๒) การฝึกในระดับ บก.ทท. แบ่งออกเป็น ๓ ขั้น ดังนี้

๒.๑) ขั้นวางแผนและเตรียมการฝึก ด้วยการจัดทำกำหนดการและเตรียมการที่สำคัญ ได้แก่ การประชุมวางแผนขั้นต้น (IPC) และการประชุมวางแผนขั้นสุดท้าย (FPC) การติดตั้งและเตรียมความพร้อมระบบบริหารจัดการการฝึก การกำหนดโครงสร้างการฝึกของหน่วยงานที่เกี่ยวข้องซึ่งประกอบด้วย กองอำนวยการฝึก ส่วนควบคุมการฝึก และส่วนผู้เข้ารับการฝึก

๒.๒) ขั้นการฝึกเตรียมการ ประกอบด้วย การอบรมวิชาการให้กับผู้เข้ารับการฝึก เพื่อเป็นการสร้างเสริมองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์กับกระบวนการบริหารจัดการภายใน ศซบ.ทหาร และหน่วยเกี่ยวข้อง ตามกรอบแนวคิดในการปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของ บก.ทท. ซึ่งมี ๖ กลุ่มงาน ได้แก่

๒.๒.๑) กลุ่มงานเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ (Network Security Monitoring : NSM)

๒.๒.๒) กลุ่มงานตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incidenst Respond : IR)

๒.๒.๓) กลุ่มงานตรวจพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

๒.๒.๔) กลุ่มงานข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence : CTI)

๒.๒.๕) กลุ่มงานประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Risk Assessment : RA)

๒.๒.๖) กลุ่มงานระบบควบคุมบังคับบัญชา (Command Center : CC)

๒.๓) ขั้นการฝึกจริงในระดับ บก.ทท. เป็นการตรวจสอบและประเมินผลการประสานการปฏิบัติการร่วมกันทั้ง ๖ กลุ่มงานของ ศซบ.ทหาร ซึ่งการฝึกในครั้งนี้จะนำแบบประเมินด้านความมั่นคงปลอดภัยทางไซเบอร์ ๖ กลุ่มงาน (Cyber Security Check List) มาเป็นแบบประเมินขีดความสามารถของกำลังพล เพื่อตรวจสอบให้เกิดความพร้อมในการรับมือและแก้ปัญหาภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อ บก.ทท. ตลอดจนมีการทบทวนบทเรียนที่ได้รับจากการฝึก (AAR)

๒.๔) การผลการฝึก

๒.๔.๑) ศซบ.ทหาร รายงานสรุปผลการฝึกนำเรียน ผบ.ทสส. (ผ่าน ยก.ทหาร)

๒.๔.๒) ศซบ.ทหาร จัดทำรายงานผลการดำเนินการตามวงรอบ ส่ง สปช.ทหาร

วิธีการประเมินผลความสำเร็จ

คณะทำงาน/กรรมการประเมินผลการฝึก ทำการประเมินผลการฝึกตามหัวข้อการประเมิน (Check lists) คิดเป็นคะแนนรวมร้อยละ ๑๐๐ โดยแบ่งออกเป็น ๒ ส่วน คือ

๑. ประเมินผลด้านความพร้อมของจัดการฝึก คิดเป็นคะแนนร้อยละ ๔๐

๒. ประเมินผลด้านการปฏิบัติการทางไซเบอร์ตามภารกิจและบ่งการที่ได้รับ คิดเป็นคะแนนร้อยละ ๖๐

$$\text{สูตร ร้อยละของการประเมินผลการฝึก} = \frac{\text{คะแนนการประเมินด้าน ๑ และ ๒}}{\text{ผลรวมคะแนนประเมินผลการฝึก}} \times ๑๐๐$$

หลักฐานการเชิงประจักษ์ : มีเอกสารหลักฐานประกอบดวย

๑. อนุมัติจัดการฝก

๒. คำสั่งจัดตั้ง กอ.ฝก/คณะกรรมการหรือคณะทำงานประเมินผลการฝึก

๓. ภาพการจัดการฝก

๔. แบบประเมินการฝก/คะแนนประเมินผลการฝก

๕. รายงานสรุปผลการฝก

๓.๒ ร้อยละคะแนนเฉลี่ยของการประเมินผลการฝึกระดับ ทท. น้ำหนักร้อยละ ๑๐

บก.ทท. โดย ศซบ.ทหาร เป็นหน่วยรับผิดชอบดำเนินการจัดการฝึกการปฏิบัติการทางไซเบอร์ในระดับ ทท. เรียกว่า การฝึกการรักษาความมั่นคงปลอดภัยไซเบอร์แบบเป็นหน่วย โดยมีผู้เข้ารับการฝึกจากหน่วยงานต่างๆ จากหน่วยงานด้านไซเบอร์ภายใน กห. และหน่วยงานเกี่ยวข้อง ใน กห. ได้แก่ ศซบ.ทสอ.กห. ศซบ.ทหาร ศซบ.เหล่าทัพ สส.ทหาร ยก.ทหาร ยก.เหล่าทัพ เป็นต้น นอกจากนี้ ยังมีหน่วยงานต่าง ๆ ทั้งภาครัฐและภาคเอกชน นอก กห. ที่เกี่ยวข้อง ตลอดจนหน่วยงานโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Information : CII) ตาม พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ อาจได้รับเชิญให้เข้าร่วมการฝึก หรือร่วมสังเกตการฝึก ได้ เช่น สมช. สกมช. ปอท. สทป. ดศ. สตช. DSI การไฟฟ้า การธนาคาร การนิคมอุตสาหกรรม การธุรกิจประกันภัย การขนส่ง ฯลฯ สำหรับการฝึกในระดับ บก.ทท.

๑) วัตถุประสงค์การฝึก มีวัตถุประสงค์และขั้นตอนการฝึกดังนี้

๑.๑) เพื่อทดสอบความรู้ความเข้าใจในการปฏิบัติหน้าที่และขีดความสามารถในการปฏิบัติการทางไซเบอร์ของผู้ปฏิบัติงานด้านไซเบอร์ของหน่วยงานด้านไซเบอร์ของ กห. และหน่วยเกี่ยวข้อง

๑.๒) เพื่อทดสอบความพร้อมและขีดความสามารถในการปฏิบัติการร่วมทางไซเบอร์ของ ทท. ในการปฏิบัติการในมิติทางไซเบอร์ ทั้งในสภาวะปกติและในสภาวะสงคราม

๑.๓) เพื่อสร้างเสริมความร่วมมือระหว่างหน่วยงานด้านไซเบอร์ของ ทท. กับหน่วยงานอื่น ๆ ที่เกี่ยวข้องทั้งภายในและภายนอก กห.

๑.๔) เพื่อเตรียมความพร้อมในการปฏิบัติการทางไซเบอร์ในสถานการณ์ระดับวิกฤติของประเทศตามบทบัญญัติของ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๑.๕) เพื่อประเมินผลการฝึกในระดับ ทท. โดยนำผลการประเมินไปทบทวน วิเคราะห์ และปรับปรุงพัฒนาการฝึกในครั้งต่อไปให้มีประสิทธิภาพและประสิทธิผลมากขึ้น

โดยในการฝึก จะเป็นการฝึกการปฏิบัติการทางไซเบอร์ในมิติทางไซเบอร์ เพื่อให้ ทท. มีความพร้อมในการปฏิบัติการทางไซเบอร์ทั้งในสภาวะปกติและสภาวะสงคราม ทั้งเชิงรุกและเชิงรับ โดย ทท. มีขีดความสามารถให้การสนับสนุนรัฐบาลและประเทศได้ รวมทั้งสามารถตรวจสอบและประเมินผลการฝึกได้อย่างเป็นระบบ

๒) การฝึกในระดับ ทท. แบ่งออกเป็น ๓ ขั้น ดังนี้

๒.๑) ขั้นวางแผนและเตรียมการฝึก ด้วยการจัดทำกำหนดการและเตรียมการที่สำคัญ ได้แก่ การประชุมวางแผนขั้นต้น (IPC) และการประชุมวางแผนขั้นสุดท้าย (FPC) การติดตั้งและเตรียมความพร้อมระบบบริหารจัดการการฝึก การกำหนดโครงสร้างการฝึกของหน่วยงานที่เกี่ยวข้องซึ่งประกอบด้วย กองอำนวยการฝึก ส่วนควบคุมการฝึก และส่วนผู้เข้ารับการฝึก

๒.๒) ขั้นการฝึกเตรียมการ ประกอบด้วย การอบรมวิชาการให้กับผู้เข้ารับการฝึก เพื่อเป็นการสร้างเสริมองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์กับกระบวนการบริหารจัดการภายในของหน่วยตนเอง ตามกรอบแนวคิดในการปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ตามมาตรฐานสากล NIST framework ซึ่งมี ๖ กลุ่มงาน ได้แก่

๒.๒.๑) กลุ่มงานเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ (Network Security Monitoring : NSM)

๒.๒.๒) กลุ่มงานตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incidenst Respond : IR)

๒.๒.๓) กลุ่มงานตรวจพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

๒.๒.๔) กลุ่มงานข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence : CTI)

๒.๒.๕) กลุ่มงานประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Risk Assessment : RA)

๒.๒.๖) กลุ่มงานระบบควบคุมบังคับบัญชา (Command Center : CC)

๒.๓) ขั้นการฝึกจริงในระดับ ทท. เป็นการตรวจสอบและประเมินผลการประสานการปฏิบัติการร่วมกันทั้ง ๖ กลุ่มงานของหน่วยงานด้านไซเบอร์ของ กห. (ศซบ.ทสอ.กห. ศซบ.ทหาร ศซบ.เหล่าทัพ และ สส.ทหาร) และหน่วยงานอื่น ๆ ที่เกี่ยวข้องทั้งภายในและภายนอก กห. ที่เข้าร่วมการฝึก ซึ่งการฝึกในครั้งนี้จะนำแบบประเมินด้านความมั่นคงปลอดภัยทางไซเบอร์ ๖ กลุ่มงาน (Cyber Security Check List) มาเป็นแบบประเมินขีดความสามารถของกำลังพลและหน่วยที่เข้าร่วมการฝึก เพื่อตรวจสอบให้เกิดความพร้อมในการรับมือและแก้ปัญหาภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อ ทท. และประเทศ (หน่วยงานด้าน CII ที่เข้าร่วมการฝึก (ถ้ามี)) ตลอดจนมีการทบทวนบทเรียนที่ได้รับจากการฝึก (AAR)

๒.๔) การรายงานผลการฝึก

๒.๔.๑) ศซบ.ทหาร รายงานสรุปผลการฝึกนำเรียน ผบ.ทสส. (ผ่าน ยก.ทหาร) และสำเนาแจกจ่าย ศซบ.เหล่าทัพ และ ศซบ.ทสอ.กห.

๒.๔.๒) ศซบ.ทหาร จัดทำรายงานผลการดำเนินการตามวงรอบ ส่ง สพร.กห. ผ่าน สปช.ทหาร

วิธีการประเมินผลความสำเร็จ

คณะทำงาน/กรรมการประเมินผลการฝึก ทำการประเมินผลการฝึกตามหัวข้อการประเมิน (Check lists) คิดเป็นคะแนนรวมร้อยละ ๑๐๐ โดยแบ่งออกเป็น ๒ ส่วน คือ

๑. ประเมินผลด้านความพร้อมของจัดการฝึก คิดเป็นคะแนนร้อยละ ๔๐

๒. ประเมินผลด้านการปฏิบัติการทางไซเบอร์ตามภารกิจและบ่งการที่ได้รับ คิดเป็นคะแนนร้อยละ ๖๐

$$\text{สูตร ร้อยละของการประเมินผลการฝึก} = \frac{\text{คะแนนการประเมินด้าน ๑ และ ๒}}{\text{ผลรวมคะแนนประเมินผลการฝึก}} \times ๑๐๐$$

หลักฐานการเชิงประจักษ์ : มีเอกสารหลักฐานประกอบดวย

๑. อนุมัติจัดการฝึก

๒. คำสั่งจัดตั้ง กอ.ฝก/คณะกรรมการหรือคณะทำงานประเมินผลการฝึก

๓. ภาพการจัดการฝึก

๔. แบบประเมินการฝึก/คะแนนประเมินผลการฝึก

๕. รายงานสรุปผลการฝึก

๓.๓ ร้อยละความสำเร็จของการดำเนินการในการรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ของ บก.ทท.
น้ำหนักร้อยละ ๑๕

เป็นการสะท้อนด้านคุณภาพของระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ บก.ทท. มีขีดความสามารถในการตรวจจับภัยคุกคามทางไซเบอร์ บก.ทท. เพิ่มสูงขึ้น (ตรวจจับได้มากขึ้น/ดีขึ้น) ทำให้รู้/ทราบ และสามารถดำเนินการป้องกันและรับมือ แก้ไขปัญหาได้ดีขึ้น/เร็วขึ้น ทำให้ลดภัยคุกคามทางไซเบอร์ของ บก.ทท.

สูตร

$$\text{ร้อยละ} = \frac{\text{จำนวนครั้งของการตรวจจับภัยคุกคามทางไซเบอร์ที่สำคัญที่สามารถแก้ไขปัญหาได้}}{\text{จำนวนทั้งหมดของการตรวจจับภัยคุกคามทางไซเบอร์}} \times ๑๐๐$$

ภัยคุกคามทางไซเบอร์ที่สำคัญ คือ ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและส่งผลกระทบต่อระบบรักษาความมั่นคงปลอดภัยของ บก.ทท. จนไม่สามารถทำงานได้ (ต้องหยุดทำงาน) หรือ ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและส่งผลกระทบต่อระบบงานสารสนเทศของ บก.ทท. จนส่งผลกระทบต่อการใช้งาน เช่น ระบบล่ม ข้อมูลถูกจารกรรม/ทำลาย และได้รับสั่งการจากผู้บังคับบัญชา/หน่วยเหนือสั่งการหรือร้องขอ

๕.๒ ผลผลิต : กองบัญชาการกองทัพไทย มีขีดความสามารถด้านความมั่นคงทางไซเบอร์ ในมิติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทั้งเชิงรับและเชิงรุก ในมิติการป้องกันประเทศ และความมั่งคงของรัฐ รวมถึงทำให้ระบบปฏิบัติการเครือข่ายเป็นศูนย์กลาง (Network Centric Operation : NCO) ของ กองทัพไทยให้มีความปลอดภัย โดยสะท้อนสถานะความพร้อมด้วยองค์ประกอบ ๓ ด้าน ได้แก่ ด้านกำลังพล ด้านยุทโธปกรณ์ และ ด้านระบบ

๕.๓ ผลลัพธ์ : กองบัญชาการกองทัพไทย มีสถานะความพร้อมด้านความมั่นคงทางไซเบอร์ ในการอำนวยการร่วมการป้องกันประเทศ รองรับยุทธศาสตร์ชาติด้านการป้องกันประเทศ ตอบสนองต่อกลยุทธ์ในแผนแม่บทย่อยภายใต้แผนแม่บท และมีความพร้อมในการปฏิบัติตามภารกิจและสามารถสนับสนุนภารกิจของรัฐบาลได้

๖. เกณฑ์การให้คะแนน :

ตัวชี้วัด	เกณฑ์การประเมิน		
	เป้าหมายขั้นต่ำ (๕๐ คะแนน)	เป้าหมายมาตรฐาน (๗๕ คะแนน)	เป้าหมายขั้นสูง (๑๐๐ คะแนน)
ร้อยละของผลการประเมินสถานะความพร้อมด้านความมั่นคงทางไซเบอร์ของ บก.ทท.	๗๐	๗๕	๘๐

ตัวชี้วัดในยุทธศาสตร์ชาติ ประเด็นการพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ **เป้าหมาย “กองทัพและหน่วยงานด้านความมั่นคงมีความพร้อมสูงขึ้นที่จะเผชิญภัยคุกคามทุกรูปแบบทุกมิติและทุกระดับความรุนแรง”** ตัวชี้วัด **“ระดับความพร้อมของกองทัพและหน่วยงานด้านความมั่นคง”** มีค่าเป้าหมายในปี ๒๕๖๕ จะต้องมีความพร้อม ร้อยละ ๘๐

๗. เงื่อนไข : เป็นไปตามเงื่อนไขที่ระบุไว้ในแต่ละด้าน

๘. รายละเอียดข้อมูลพื้นฐาน : (หากเป็นโครงการที่มีแผนดำเนินการหลายปี (Road Map) ให้ระบุแผน และเป้าหมายรายปี ในข้อ ๘.๒ ด้วย)

๘.๑ ผลการดำเนินงานในอดีต

ข้อมูลพื้นฐานประกอบตัวชี้วัด	หน่วยวัด	ผลการดำเนินงานในอดีต ประจำปีงบประมาณ		
		๒๕๖๒	๒๕๖๓	๒๕๖๔

๘.๒ แผนดำเนินการหลายปี (Road Map)

เป้าหมายของแผน..... ห้วงปีงบประมาณ ๒๕๖๑ - ๒๕๖๖	เป้าหมายประจำปีงบประมาณ					
	๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕	๒๕๖๖
แผนปฏิบัติราชการประจำปี ๒๕๖๓ – ๒๕๖๕			ร้อยละ ๗๐	ร้อยละ ๗๕	ร้อยละ ๘๐	