ความรู้พื้นฐาน
สำหรับปฏิบัติการทางไซเบอร์
พ.ศ.๒๕๖๖

โดย
กองการฝึกและพัฒนาทางไซเบอร์
ศูนย์ไซเบอร์กองทัพอากาศ

บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๒๔๖๗)

ที่ กห ๐๖๐๙.๓/ ๑๒๒๕ **วันที่** ๑๙ ก.ย.๖๖

เรื่อง ส่งคู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เสนอ ศชบ.ทอ.

๑. ตามอนุมัติ จก.ทสส.ทอ.เมื่อ ๑๓ ก.ย.๖๖ ท้ายหนังสือ สนผ.ทสส.ทอ.ที่ กห ๐๖๐๙.๓(๒)/๒๐๓ ลง ๑๒ ก.ย.๖๖ ให้ใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึกความชำนาญของจำพวกทหารไซเบอร์ นั้น

๒. ทสส.ทอ.จึงขอส่งคู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ เพื่อใช้ในการฝึกความชำนาญของจำพวกทหารไซเบอร์ รายละเอียดตามแนบ

จึงเสนอมาเพื่อดำเนินการต่อไป

พล.อ.ต.

ผอ.สนผ.ทสส.ทอ.ทำการแทน

จก.ทสส.ทอ.

บันทึกข้อความ

ส่วนราชการ สนผ.ทสส.ทอ.(กนผ.โทร.๒-๑๐๕๖)

ที่ กห ๐๖๐๙.๓(๒)/ ๒๐๓ **วันที่** ๑๒ ก.ย.๖๖

เรื่อง ขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เรียน จก.ทสส.ทอ.

๑. ตามหนังสือ ศชบ.ทอ.ที่ กห ๐๖๕๐.๑/๗๔๖ ลง ๒๘ ส.ค.๖๖ ขอให้พิจารณาตำราของหลักสูตรสายวิทยาการไซเบอร์ นั้น

๒. สนผ.ทสส.ทอ.ตรวจสอบแล้ว มีข้อมูล ดังนี้

๒.๑ ระเบียบ ทอ.ว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓ และฉบับแก้ไขเพิ่มเติม ข้อ ๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่าทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แนบท้ายระเบียบนี้ (แนบ ๑)

๒.๒ ทสส.ทอ.เป็นหน่วยรับผิดชอบสายวิทยาการสารสนเทศและสงครามอิเล็กทรอนิกส์และสายวิทยาการไซเบอร์ ได้จัดทำคู่มือการฝึกงานในหน้าที่ เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญการปฏิบัติงานในสายวิทยาการไซเบอร์ จำนวน ๕ วิชา (แนบ ๒) ประกอบด้วย

๒.๒.๑ วิชา การป้องปรามทางไซเบอร์
๒.๒.๒ วิชา การป้องกันทางไซเบอร์
๒.๒.๓ วิชา การข่าวกรองทางไซเบอร์
๒.๒.๔ วิชา การพิสูจน์หลักฐานทางดิจิทัล
๒.๒.๕ วิชา ความรู้พื้นฐานสำหรับปฏิบัติการทางไซเบอร์

๓. สนผ.ฯ พิจารณาแล้ว เพื่อให้การดำเนินการฝึกงานในหน้าที่ของสายวิทยาการไซเบอร์เป็นไปด้วยความเรียบร้อย จึงขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึกความชำนาญของจำพวกทหารไซเบอร์ต่อไป

จึงเรียนมาเพื่ออนุมัติตามข้อ ๓

พล.อ.ต.
ผอ.สนผ.ทสส.ทอ.

- อนุมัติตามข้อ ๓

พล.อ.ท.
จก.ทสส.ทอ.
๑๙ ก.ย.๖๖

ทสส.ทอ.
เลขรับ ๕๕๔๐
วันที่ ๒๔ ส.ค. ๒๕๖๖
เวลา ๑๓๔๘

บันทึกข้อความ

ส่วนราชการ ศชบ.ทอ.(นกพ.ฯ โทร.๒-๒๗๑๒)

ที่ กห ๐๖๕๐.๑/ ๗๔๖ วันที่ ๒๔ ส.ค.๖๖

เรื่อง ขอให้พิจารณาตำราของหลักสูตรสายวิทยาการไซเบอร์

สนผ.ทสส.ทอ.
เลขรับ ๒๗๗๑
วันที่ ๒๔ ส.ค.๖๖
เวลา ๑๓๕๗

เสนอ ทสส.ทอ.

สนผ-๖
๒๔ ส.ค. ๒๕๖๖

๑. ตามหนังสือ ทสส.ทอ.ที่ กห ๐๖๐๙.๓/๑๐๘๙ ลง ๙ ส.ค.๖๖ ให้ ศชบ.ทอ.ปรับปรุงเนื้อหาตำราของหลักสูตรสายวิทยาการไซเบอร์จำนวน ๕ วิชา นั้น

๒. ศชบ.ทอ.ตรวจสอบและพิจารณาแก้ไขเนื้อหา รายละเอียดตามความเหมาะสม ร่วมกับ ร.อ.หญิง สุธิดา บทสันเทียะ นมฐ.ผมทส.กนผ.สนผ.ทสส.ทอ.แล้วเมื่อวันที่ ๒๓ ส.ค.๖๖ ดังมี รายละเอียดตามแนบ

จึงเสนอมาเพื่อพิจารณาดำเนินการให้ต่อไป

พล.อ.ต.
ผอ.ศชบ.ทอ.

กนผ.สนผ.ทสส.ทอ.
เลขรับ ๒๑๐๕
วันที่ ๒๘ ส.ค. ๖๖
เวลา ๑๓๕๗

ทราบแล้ว
- รอง ผอ.กนผ.สนผ.ทสส.ทอ.ทราบ
- ผสส.๑ ดำเนินการในส่วนที่เกี่ยวข้อง

น.อ.
ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ทราบแล้ว

น.อ.
รอง ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ทราบแล้ว

น.อ.
รอง ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ระเบียบกองทัพอากาศ
ว่าด้วยการฝึกงานในหน้าที่
พ.ศ.๒๕๖๓

โดยที่เป็นการสมควรปรับปรุงแก้ไขแนวทางปฏิบัติเกี่ยวกับการฝึกงานในหน้าที่ของกองทัพอากาศ ให้เป็นไปด้วยความเรียบร้อย จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๕๔

บรรดาระเบียบและคำสั่งอื่นใด ในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

๔.๑ "การฝึกงานในหน้าที่" หมายความว่า การให้นายทหารประทวนเข้ารับการฝึกงานตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญให้สูงขึ้น ตามลักษณะความชำนาญทหารอากาศของเหล่าทหารหรือจำพวกทหาร โดยใช้ตามมาตรฐานการฝึกความชำนาญ และหนังสือคู่มือการฝึกงานในหน้าที่เป็นแนวทางการฝึก

๔.๒ "การฝึก" หมายความว่า การฝึกงานในหน้าที่

๔.๓ "นายทหารฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตร ที่แต่งตั้งขึ้นให้มีหน้าที่รับผิดชอบ และดำเนินการ ควบคุม กำกับ ดูแล เกี่ยวกับการฝึกงานในหน้าที่ของหน่วยขึ้นตรงกองทัพอากาศ ให้ใช้คำย่อว่า "นฝน."

๔.๔ "ผู้ช่วยนายทหารฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตรจำพวกทหารกำลังพลที่แต่งตั้งขึ้น ให้มีหน้าที่ช่วยเหลือนายทหารฝึกงานในหน้าที่ ให้ใช้คำย่อว่า "ผช.นฝน."

๔.๕ "เจ้าหน้าที่ฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตร หรือนายทหารประทวน หรือลูกจ้างที่แต่งตั้งขึ้น ให้มีหน้าที่ด้านธุรการเกี่ยวกับการฝึกงานในหน้าที่ ให้ใช้คำย่อว่า "จนท.ฝน."

๔.๖ "ผู้ควบคุมการฝึก" หมายความว่า นายทหารสัญญาบัตรที่เป็นเหล่าหรือจำพวกทหารเดียวกันกับผู้รับการฝึกที่แต่งตั้งขึ้น ให้มีหน้าที่ดำเนินการ ควบคุม กำกับ ดูแลการฝึกงานในหน้าที่ภาคปฏิบัติประจำปีให้เป็นไปตามมาตรฐานการฝึกความชำนาญ

๔.๗ "ผู้ช่วยผู้ควบคุมการฝึก" หมายความว่า นายทหารสัญญาบัตรที่แต่งตั้งขึ้นให้มีหน้าที่ช่วยเหลือผู้ควบคุมการฝึก

๔.๘ "ครูฝึก"...

๓๑.๑๘.๒.๒ ระดับ ๕๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ไม่เกินร้อยละ ๘๐ ของจำนวนชั่วโมงรวมในระดับ ๗๐

๓๑.๑๘.๒.๓ ระดับ ๗๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ตรงกับความมุ่งหมายเฉพาะและวัตถุประสงค์การเรียนรู้ในระดับ ๗๐

๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่าทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แนบท้ายระเบียบนี้

หมวด ๖
การควบคุมกำกับดูแล

ข้อ ๓๒ หน่วยฝึกจะต้องดำเนินการฝึกตามระยะเวลาที่กำหนดไว้ในวงรอบการฝึก

ข้อ ๓๓ ผู้รับการฝึก จะต้องทำการฝึกครบทุกหัวข้อวิชา หรือหมวดวิชาที่เป็นวิชาหลักของจำพวกทหารตามที่กำหนดในมาตรฐานการฝึกความชำนาญ

ข้อ ๓๔ เมื่อผู้รับการฝึกย้ายสังกัด ในระหว่างการฝึกภาคปฏิบัติ หรือรอการทดสอบภาควิชาการ ให้ส่วนราชการต้นสังกัดเดิมแจ้งให้ส่วนราชการต้นสังกัดใหม่ทราบถึงสถานภาพการฝึกที่ผ่านมา และเรื่องที่จะต้องดำเนินการต่อไป พร้อมกับส่งประวัติการฝึก กับมาตรฐานการฝึกความชำนาญไปยังส่วนราชการต้นสังกัดใหม่ โดยส่วนราชการต้นสังกัดใหม่จะต้องแต่งตั้งผู้รับผิดชอบในขั้นตอนที่ยังเหลืออยู่ เพื่อดำเนินการฝึกต่อไปให้ครบตามหัวข้อที่กำหนดไว้ หากจะให้ทำการฝึกที่ส่วนราชการเดิมต่อไป ให้ประสานตกลงกันแล้วแจ้งการเปลี่ยนแปลงให้ กรมกำลังพลทหารอากาศทราบ เพื่อแก้ไขเปลี่ยนแปลงหลักฐานการควบคุมการฝึกงานในหน้าที่ให้ถูกต้อง

ข้อ ๓๕ ผู้ที่ไม่สามารถทำการฝึกได้ครบตามที่กำหนด และอยู่ในกรณีที่จะต้องพ้นจากการฝึก ให้ส่วนราชการต้นสังกัดรายงานพร้อมหลักฐานประกอบให้กรมกำลังพลทหารอากาศ ดำเนินการนำเรียนขออนุมัติผู้บัญชาการทหารอากาศ หากจะเข้ารับการฝึกในปีต่อไปจะต้องเริ่มดำเนินการใหม่ ซึ่งการพ้นจากการฝึกจะต้องอยู่ในกรณี ดังนี้

๓๕.๑ ลาออก ให้ออก ปลดออก

๓๕.๒ ต้องหาคดีอาญา ยกเว้นความผิดลหุโทษ หรือความผิดตามกฎหมายอื่นที่มีอัตราโทษไม่สูงกว่าความผิดลหุโทษ

๓๕.๓ ย้าย โอน ไปสังกัดนอกกองทัพอากาศ

๓๕.๔ มีราชการจำเป็นเร่งด่วนและสำคัญ

๓๕.๕ มีเวลาการฝึกภาคปฏิบัติไม่ถึงร้อยละ ๘๕ ของเวลาการฝึกทั้งหมด โดยมีเหตุผลอันสมควร

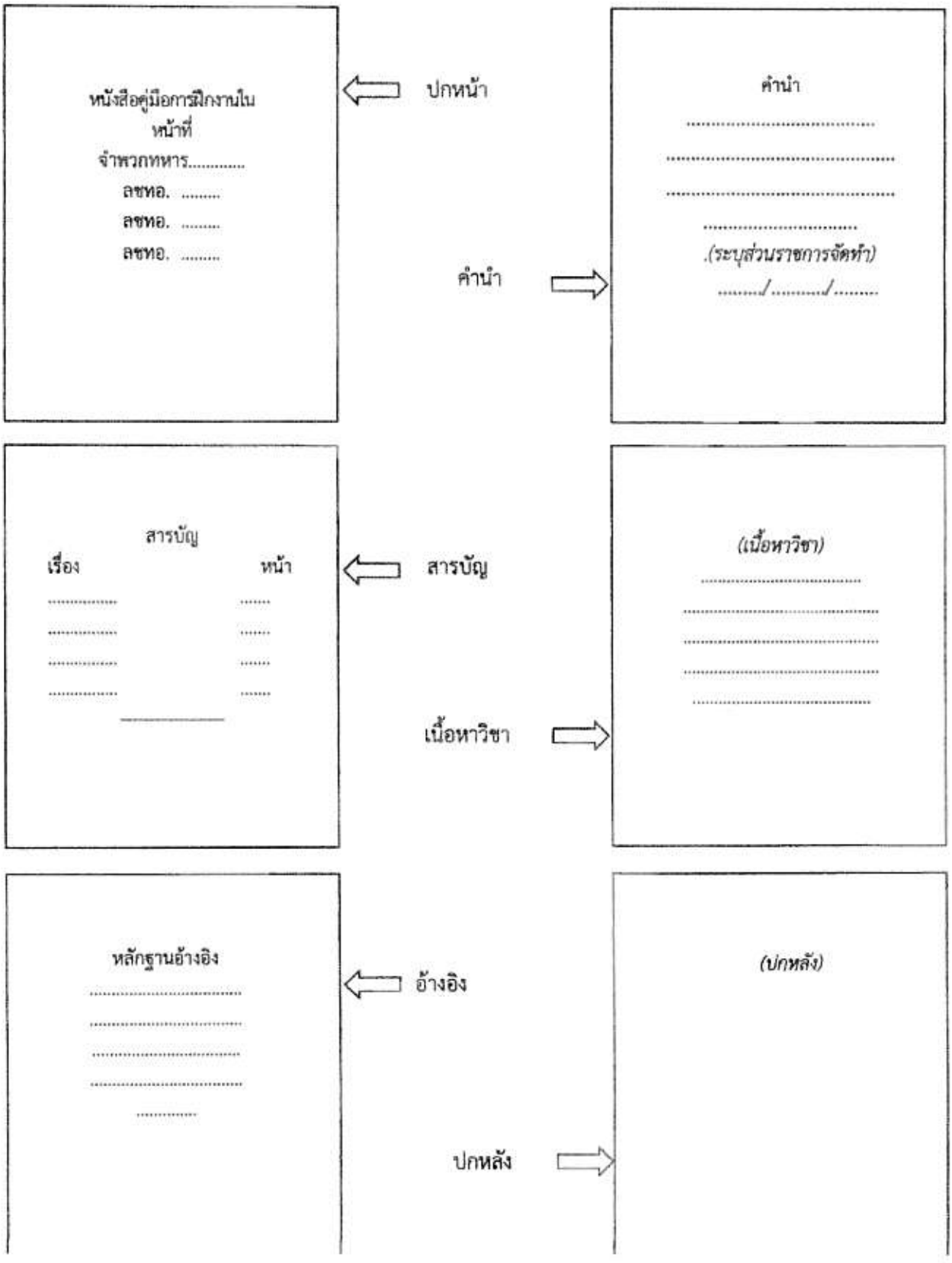
๓๕.๖ ป่วยจนมีเวลาการฝึกไม่เพียงพอตามข้อ ๓๕.๕

๓๕.๗ ขาดการทดสอบความรู้ภาคปฏิบัติตามระยะเวลาที่กำหนด โดยมีเหตุผลอันสมควร

ข้อ ๓๖ การลา ...

ผนวก ๗ ประกอบระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓

หนังสือคู่มือการฝึกงานในหน้าที่



คู่มือการฝึกงานในหน้าที่
จำพวกทหารไซเบอร์

ลชทอ.๒๘๑๓๐

ลชทอ.๒๘๑๕๐

ลชทอ.๒๘๑๗๐

กองการฝึกและพัฒนาทางไซเบอร์
ศูนย์ไซเบอร์กองทัพอากาศ

คำนำ

คู่มือการฝึกงานในหน้าที่วิชาการปฏิบัติการทางไซเบอร์ จัดทำขึ้นเพื่อประกอบการฝึกความชำนาญตามมาตรฐานการฝึกความชำนาญ (มฝช.) ของสายวิทยาการไซเบอร์ โดยเนื้อความรู้ของคู่มือกล่าวถึงความรู้พื้นฐานด้านการปฏิบัติการทางไซเบอร์ การปฏิบัติการในมิติไซเบอร์ของกองทัพอากาศ การจัดหน่วยปฏิบัติด้านไซเบอร์ในการเตรียมกำลัง/ใช้กำลัง รวมถึงงานด้านการฝึกและพัฒนาทางไซเบอร์ เพื่อให้ผู้ที่ศึกษามีความรู้ ความเข้าใจในการปฏิบัติงานในสายวิทยาการไซเบอร์

หวังเป็นอย่างยิ่งว่าคู่มือเล่มนี้ จะเป็นประโยชน์ต่อผู้เข้ารับการฝึกงานในหน้าที่และขอขอบคุณเจ้าหน้าที่ทุกท่านที่มีส่วนในการจัดทำคู่มือเล่มนี้จนเสร็จสมบูรณ์

กองการฝึกและพัฒนาทางไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

๒๘ สิงหาคม ๒๕๖๖

สารบัญ

	หน้า
คำนำ	ก
สารบัญ	ข
สารบัญภาพ	ค
บทที่ ๑ ความรู้พื้นฐานสำหรับปฏิบัติการทางไซเบอร์	
๑.๑ ความหมาย และขอบเขตของไซเบอร์	๑
๑.๒ ประเภทของการปฏิบัติการในมิติไซเบอร์	๑
๑.๓ หน่วยงานที่เกี่ยวข้องในมิติไซเบอร์	๑
๑.๔ ประเภทของภัยคุกคามไซเบอร์	๒
บทที่ ๒ การปฏิบัติการในมิติไซเบอร์ของกองทัพอากาศ	
๒.๑ ยุทธศาสตร์ที่เกี่ยวข้องด้านไซเบอร์	๙
๒.๒ หลักนิยมที่เกี่ยวข้องด้านไซเบอร์	๑๓
๒.๓ แนวความคิดการปฏิบัติการในมิติไซเบอร์กองทัพอากาศ/การปฏิบัติการที่มีเครือข่ายเป็นศูนย์กลาง (NCO)	๑๗
๒.๔ ระบบสารสนเทศและเครือข่ายกองทัพอากาศ และทรัพย์สินทางไซเบอร์	๒๐
๒.๕ กฎหมาย ระเบียบ และการกำหนดมาตรฐานทางไซเบอร์	๒๑
บทที่ ๓ การจัดหน่วยปฏิบัติด้านไซเบอร์ในการเตรียมกำลัง/ใช้กำลัง	
๓.๑ ภารกิจและโครงสร้างการจัดศูนย์ไซเบอร์กองทัพอากาศ และหน่วยเกี่ยวข้อง	๒๗
๓.๒ ภารกิจและโครงสร้างการจัดศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ	๓๑
บทที่ ๔ การฝึกและพัฒนาด้านไซเบอร์	
๔.๑ งานด้านการฝึก	๓๓
๔.๒ งานด้านการพัฒนาระบบ	๓๗
เอกสารอ้างอิง	๓๘

สารบัญภาพ

		หน้า
ภาพที่ ๑.๑	ภัยคุกคามทางไซเบอร์โดยอาศัยช่องโหว่หรือจุดอ่อนของความมั่นคงปลอดภัย ส่งผลให้เกิดความเสียหายต่อระบบสารสนเทศ	๒
ภาพที่ ๑.๒	ตัวอย่างการเข้ารหัส (Encryption)	๓
ภาพที่ ๑.๓	ภาพแสดงช่วงเวลาการเกิด Zero-day Attack และการออกโปรแกรมปิดช่องโหว่	๗
ภาพที่ ๒.๑	ทิศทางการพัฒนามิติไซเบอร์ (Cyber Domain) ของกองทัพอากาศ ตามยุทธศาสตร์กองทัพอากาศ ๒๐ ปี ฉบับปรับปรุง (พ.ศ.๒๕๖๑ – ๒๕๘๐) ฉบับปรับปรุง พ.ศ. ๒๕๖๓	๑๑
ภาพที่ ๒.๒	ภาพแสดงการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations: NCO)	๑๙
ภาพที่ ๒.๓	ภาพแสดงวงจร ๕ ฟังก์ชันหลักของ NIST Framework	๒๔
ภาพที่ ๓.๑	โครงสร้างหน่วยขึ้นตรงศูนย์ไซเบอร์กองทัพอากาศ	๒๘
ภาพที่ ๓.๒	โครงสร้างกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ	๒๘
ภาพที่ ๓.๓	โครงสร้างหน่วยขึ้นตรงกรมข่าวทหารอากาศ	๒๙
ภาพที่ ๓.๔	โครงสร้างหน่วยขึ้นตรงกรมสื่อสารทหารอากาศ	๓๐
ภาพที่ ๓.๕	โครงสร้างหน่วยขึ้นตรงศูนย์ซอฟต์แวร์กองทัพอากาศ	๓๐
ภาพที่ ๓.๖	โครงสร้างหน่วยขึ้นตรงกองบัญชาการควบคุมการปฏิบัติทางอากาศ	๓๑
ภาพที่ ๓.๗	โครงสร้างของศูนย์ยุทธการไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ	๓๑
ภาพที่ ๔.๑	เว็บไซต์ https://overthewire.org/wargames/	๓๕
ภาพที่ ๔.๒	เว็บไซต์ https://www.root-me.org/en/Challenges	๓๕
ภาพที่ ๔.๓	เว็บไซต์ https://portswigger.net/web-security/all-labs	๓๕
ภาพที่ ๔.๔	เว็บไซต์ https://cryptohack.org/ และ https://cryptopals.com/	๓๖
ภาพที่ ๔.๕	เว็บไซต์ https://www.hackthebox.com/	๓๖
ภาพที่ ๔.๖	เว็บไซต์ https://www.vulnhub.com/	๓๖
ภาพที่ ๔.๗	เว็บไซต์ https://www.nccgroup.com/	๓๗
ภาพที่ ๔.๘	เว็บไซต์ https://github.com/vulhub/vulhub	๓๗

บทที่ ๑ ความรู้พื้นฐานสำหรับปฏิบัติการทางไซเบอร์

๑.๑ ความหมาย และขอบเขตของไซเบอร์

ไซเบอร์ หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

๑.๒ ประเภทของการปฏิบัติการในมิติไซเบอร์

การปฏิบัติการในมิติไซเบอร์ แบ่งการปฏิบัติการที่สำคัญออกเป็น ๒ ด้าน คือ การปฏิบัติการไซเบอร์เชิงรุก (Offensive Cyber Operations) และการปฏิบัติการไซเบอร์เชิงรับ (Defensive Cyber Operations) โดยมีฝ่ายต่าง ๆ ที่เกี่ยวข้องกับการปฏิบัติการคือ ฝ่ายการข่าว ฝ่ายสื่อสารฝ่ายยุทธการ ฝ่ายกำลังพล ฝ่ายส่งกำลังบำรุง โดยมีรายละเอียดของแต่ละการปฏิบัติการดังนี้

๑.๒.๑ การปฏิบัติการไซเบอร์เชิงรุก (Offensive Cyber Operations) มีวิธีปฏิบัติประกอบด้วยการหลอกหลวงฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามหยุดให้บริการทางไซเบอร์ การทำลายหรือรบกวนระบบต่าง ๆ และการเจาะระบบฝ่ายตรงข้าม

๑.๒.๑ การปฏิบัติการไซเบอร์เชิงรับ (Defensive Cyber Operations) มีวิธีปฏิบัติประกอบด้วย การปกป้องระบบ การทำให้ระบบสามารถระบุตัวตนผู้ใช้งานได้ การกู้คืนหรือการฟื้นคืนระบบ การค้นหาและปิดช่องโหว่ระบบ การปฏิบัติตามข้อกำหนดหรือมาตรฐานทางไซเบอร์ การบำรุงรักษาระบบ รวมถึงการปฏิบัติตามข้อกำหนดต่าง ๆ ทางกฎหมายหรือข้อบังคับทางไซเบอร์

๑.๓ หน่วยงานที่เกี่ยวข้องในมิติไซเบอร์

๑.๓.๑ หน่วยงานที่เกี่ยวข้องด้านไซเบอร์ระดับประเทศ

๑.๓.๑.๑ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (Ministry of Digital Economy and Society : MDES)

๑.๓.๑.๒ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (National Cyber Security Agency: NCSA)

๑.๓.๑.๓ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) (Thailand Computer Emergency Response Team : ThaiCERT) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

๑.๓.๑.๔ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

๑.๓.๑.๕ สถาบันเทคโนโลยีป้องกันประเทศ (Defence Technology Institute : DTI)

๑.๓.๑.๖ ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหมกระทรวงกลาโหม

๑.๓.๑.๗ ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย

๑.๓.๑.๘ ศูนย์ไซเบอร์กองทัพบก

๑.๓.๑.๙ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สำนักงานตำรวจแห่งชาติ

๑.๓.๑.๑๐ ศูนย์ไซเบอร์ กรมการสื่อสารและเทคโนโลยีสารสนเทศกองทัพเรือ

๑.๓.๑.๑๑ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๑.๓.๒ หน่วยงานที่เกี่ยวข้องด้านไซเบอร์ภายในศูนย์ไซเบอร์กองทัพอากาศ

๑.๓.๒.๑ กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

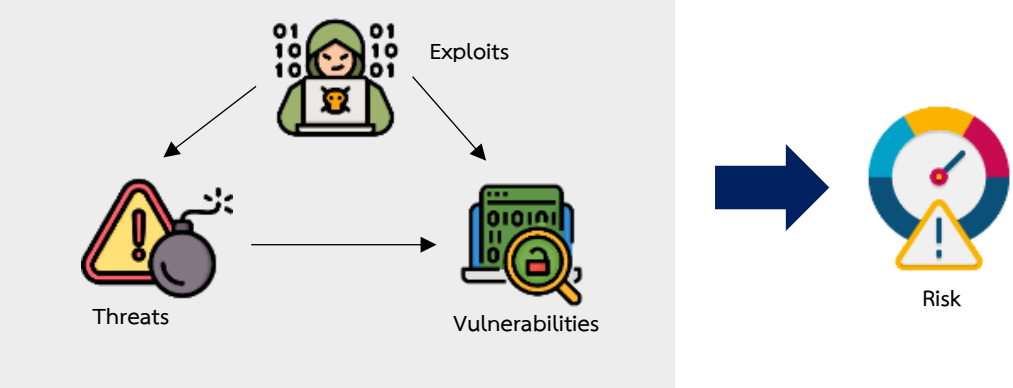
๑.๓.๒.๒ กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

๑.๓.๒.๓ กองการฝึกและพัฒนาทางไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

๑.๓.๓ ศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ

๑.๔ ประเภทของภัยคุกคามไซเบอร์

ภัยคุกคามไซเบอร์ (Threat) คือ เหตุการณ์ที่ไม่พึงประสงค์ให้เกิดขึ้น ซึ่งส่งผลกระทบและสร้างความเสียหายต่อระบบสารสนเทศภายในองค์กร โดยอาศัยช่องโหว่ (Vulnerability) คือจุดอ่อนของระบบความมั่นคงปลอดภัยที่พบในระบบคอมพิวเตอร์และระบบเครือข่าย ทั้งในซอฟต์แวร์และฮาร์ดแวร์ โดยอาจเกิดจากธรรมชาติหรือบุคคล โดยผู้ไม่ประสงค์ดีจะใช้ประโยชน์จากช่องโหว่ เพื่อทำการเจาะระบบ (Exploit)



ภาพที่ ๑.๑ ภัยคุกคามทางไซเบอร์โดยอาศัยช่องโหว่หรือจุดอ่อนของความมั่นคงปลอดภัย ส่งผลให้เกิดความเสียหายต่อระบบสารสนเทศ

๑.๔.๑ การคุกคามและการโจมตีภายในองค์กร (Internal Threats) เกิดจากบุคคล หรือกลุ่มคนภายในองค์กรที่มีความพยายามเข้าถึง การปรับเปลี่ยนดัดแปลง การทำลายข้อมูลและสารสนเทศโดยไม่ได้รับอนุญาตรวมถึงการขโมยข้อมูลที่เป็นความลับขององค์กร โดยมีตัวอย่างดังนี้

๑.๔.๑.๑ การลบข้อมูลที่สำคัญขององค์กร สามารถป้องกันภัยคุกคามได้โดย กำหนดสิทธิ์ในการเข้าถึงข้อมูลความรับผิดชอบของงานตามสิทธิ์การเข้าถึงของผู้ใช้

๑.๔.๑.๒ การเผยแพร่ข้อมูลที่เป็นความลับขององค์กร สามารถป้องกันภัยคุกคามได้โดย ติดตั้งโปรแกรมเพื่อตรวจจับการส่งต่อหรือการนำข้อมูลออก

๑.๔.๑.๓ การเปลี่ยนแปลงการตั้งค่า และรหัสผ่านของบัญชีผู้ใช้ระดับสูง สามารถป้องกันภัยคุกคามได้โดยวิธีพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)

๑.๔.๑.๔ การใช้อีเมลขององค์กรไปในทางที่ไม่เหมาะสม สามารถป้องกันภัยคุกคามได้โดยจัดทำระเบียบปฏิบัติและประกาศใช้นโยบาย และกำหนดบทลงโทษ

ภาพที่ ๑.๒ ตัวอย่างการเข้ารหัส (Encryption)

๑.๔.๒ การคุกคามและการโจมตีภายนอกองค์กร (External Threats) เกิดจากบุคคลหรือองค์กรที่อยู่ภายนอกที่ไม่ได้รับสิทธิ์ในการเข้าถึงข้อมูลและสารสนเทศขององค์กร โดยโจมตีผ่านทางช่องโหว่ระบบความปลอดภัยของเครือข่าย เช่น อินเทอร์เน็ต และไฟร์วอลล์ เป็นต้น โดยมีตัวอย่างการโจมตีจากภายนอกองค์กร ดังนี้

๑.๔.๒.๑ การโจมตีด้วยมัลแวร์ เป็นการสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมีวัตถุประสงค์เพื่อการโจรกรรมข้อมูล คำว่ามัลแวร์ เป็นคำที่ครอบคลุมถึงไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ และซอฟต์แวร์อื่น ๆ ที่เป็นอันตรายต่อระบบคอมพิวเตอร์ ซึ่งเรียกโดยรวมว่า ซอฟต์แวร์ไม่ประสงค์ดี หรือ ซอฟต์แวร์ที่ไม่พึงประสงค์ (Malicious Software) มัลแวร์ส่วนมากจะแพร่กระจายผ่านทางอีเมล การใช้สื่อบันทึกข้อมูลร่วมกัน เช่น แฟลชไดร์ฟ (Flashdrive) การดาวน์โหลดโปรแกรมต่าง ๆ จากอินเทอร์เน็ต และการคลิกลิงก์ที่ไม่รู้จักแหล่งที่มา เป็นต้น โดยมีหลายประเภท ดังนี้

๑.๔.๒.๑ (๑) ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นแอพลิเคชันหรือชุดคำสั่ง (Code) ขนาดเล็กที่ถูกออกแบบขึ้นมาเพื่อสร้างความเสียหายให้กับคอมพิวเตอร์ ความสามารถของไวรัสคอมพิวเตอร์คือ การจำลองตัวเอง โดยการแนบตัวสำเนาไวรัสในชุดคำสั่ง (Code) ของแอปพลิเคชั่น (Application) โดยไวรัสคอมพิวเตอร์บางชนิดจะสร้างความเสียหายให้กับคอมพิวเตอร์ทันทีเมื่อชุดคำสั่ง (Code) ถูกเรียกใช้งาน แต่บางชนิดจะฝังตัวอยู่ในโปรแกรมเฉย ๆ จะเริ่มทำงานก็ต่อเมื่อเข้าเงื่อนไขที่ผู้โจมตีเขียนไว้

๑.๔.๒.๑ (๒) หนอนคอมพิวเตอร์ (Computer Worm) เป็นแอพลิเคชันขนาดเล็กที่ทำงานได้ด้วยตนเอง (Stand-alone) ที่ถูกออกแบบขึ้นมาให้แพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่งผ่านระบบเครือข่ายของตัวเอง

๑.๔.๒.๑ (๓) วิศวกรรมสังคม (Social Engineering) เป็นการหลอกลวงหรือล่อลวง ครอบคลุมถึงการหลอกลวงทางไซเบอร์ เป็นจิตวิทยาทางสังคมโดยมุ่งเป้าไปที่ตัวบุคคลอาศัยทักษะการสื่อสารของผู้ที่ไม่ประสงค์ดี ไม่ว่าเป็นทางโทรศัพท์ หรืออีเมล เพื่อให้เหยื่อที่เป็นเป้าหมายเปิดเผยข้อมูลส่วนตัว เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน และเลขบัตรเครดิต เป็นต้น

๑.๔.๒.๑ (๔) การขโมยข้อมูลตัวตน (Identity Theft) เป็นการที่ผู้ไม่ประสงค์ดีได้นำข้อมูลและรูปภาพของบุคคลนั้นไปใช้โดยไม่ได้รับอนุญาต เพื่อหาผลประโยชน์และสร้างความเสียหาย ทำให้บุคคลนั้นโดนลดความน่าเชื่อถือในสังคม สาเหตุหนึ่งที่ผู้ไม่ประสงค์ดีนั้นสามารถขโมยข้อมูลตัวตนไปได้ คือ การเปิดเผยข้อมูลตัวตนลงบนสื่อสังคมออนไลน์มากเกินไป

๑.๔.๒.๑ (๕) การหลอกลวงแบบฟิชชิง (Phishing) เป็นการหลอกลวงของผู้ไม่ประสงค์ดีผ่านทางอีเมล หรือเว็บไซต์ที่คล้ายกับของจริง เพื่อให้เหยื่อเป้าหมายกรอกข้อมูลส่วนตัวลงเว็บไซต์ โดยส่วนใหญ่เป็นข้อมูลเกี่ยวกับการทำธุรกรรมกับธนาคาร หรือที่เกี่ยวข้องกับการใช้ข้อมูลส่วนตัว

๑.๔.๒.๒ รูปแบบของการโจมตีแอปพลิเคชัน

๑.๔.๒.๒ (๑) การโจมตีในรูปแบบ DoS (Denial-of-Service) การโจมตีเพื่อทำให้ระบบไม่สามารถให้บริการได้ สามารถเกิดขึ้นได้ในหลายรูปแบบ แต่โดยทั่วไปจะเป็นการโจมตีเพื่อทำให้ระบบไม่พร้อมใช้งาน (Availability) การโจมตีแบบ DoS จะทำให้บริการหรือทรัพยากรระบบมีประสิทธิภาพลดลง และจะทำให้ระบบไม่สามารถให้บริการได้ในที่สุด โดยอาจรวมถึงการโจมตีเครื่องแม่ข่ายจากศูนย์คอมพิวเตอร์ แต่โดยทั่วไปการโจมตีแบบ DoS จะหมายถึงการโจมตีระบบเครือข่ายและซอฟต์แวร์ โดยวิธีการป้องกันการโจมตีในรูปแบบ DoS (Denial-of-Service) จะทำการสร้างหลุมเพื่อทำการกรองข้อมูลและอนุญาตให้เส้นทางที่มีสิทธิ์ผ่านและปิดกั้นหน่วยข้อมูลขาเข้าต่อหมายเลขพอร์ต รวมถึงใช้ระบบตรวจจับการบุกรุก เพื่อตรวจจับและป้องกันการโจมตี

๑.๔.๒.๒ (๒) การโจมตีในรูปแบบ DDoS (Distributed DoS) การโจมตีในรูปแบบ DDoS มีลักษณะคล้ายคลึงกับ DoS ซึ่งต่างกันที่ปริมาณข้อมูลที่ใช้ในการโจมตีจะสูงกว่ามาก ผู้ไม่ประสงค์ดีจะใช้เทคนิค Flooding และใช้เครื่องคอมพิวเตอร์ที่ตนเองยึดครองมาได้ (Compromised) จากการขโมย หรือที่เรียกว่า ซอมบี้ โจมตีไปยังเป้าหมายพร้อม ๆ กัน โดยสั่งการผ่าน Command and Control (C2) และในที่สุดระบบก็จะไม่สามารถให้บริการได้ โดยการโจมตีแบบ DDoS มักจะเกิดขึ้นในช่วงเวลาสั้น ๆ แต่ผลกระทบที่เกิดขึ้นอาจสร้างความเสียหายให้กับองค์กรได้อย่างรุนแรง เนื่องจากจะทำให้สูญเสียความน่าเชื่อถือ หรือความมั่นใจในการใช้บริการ

การป้องกันการโจมตีในรูปแบบ DDoS (Distributed DoS) อาจพิจารณาใช้ Content Delivery Network (CDN) หรือเครือข่ายคอมพิวเตอร์แม่ข่ายขนาดใหญ่ที่กระจายตัวกันอยู่ทั่วโลก ซึ่งเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้ จะเชื่อมต่อกันผ่านอินเทอร์เน็ต

เพื่อทำหน้าที่ในการส่งข้อมูลให้ไปถึงผู้รับปลายทางให้เร็วที่สุด รวมทั้งเพิ่มประสิทธิภาพในการเข้าถึงข้อมูลเหล่านั้นได้ตลอดเวลา

๑.๔.๒.๒ (๓) การโจมตีในรูปแบบ Man-in-the-Middle (MitM) เป็นการโจมตีโดยแทรกเป็นคนกลาง คือการที่ผู้ไม่ประสงค์ดีแทรกตนเองไปอยู่ตรงกลางระหว่างการสื่อสารของอุปกรณ์คอมพิวเตอร์ หรือบุคคล แล้วทำหน้าที่เป็นเสมือนตัวกลางในการรับส่งข้อมูล โดยที่ผู้ใช้งานไม่สามารถทราบว่ามีผู้ไม่ประสงค์ดีเป็นผู้รับและส่งสารต่อกับคู่สนทนาตัวเองอยู่ ทำให้ผู้ไม่ประสงค์ดีสามารถใช้รูปแบบการโจมตีในลักษณะนี้ในการดักจับหรือเปลี่ยนแปลงข้อมูลทั้งสองฝั่งได้ โดยการโจมตีในรูปแบบนี้ถูกนำมาประยุกต์ใช้กับการโจมตี MitM ในระบบเครือข่ายไร้สาย ทำให้ผู้ไม่ประสงค์ดีสามารถแทรกแซงการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ และอุปกรณ์ Wireless Access Point เพื่อเข้าถึง ปลอมแปลง หรือแก้ไขข้อมูลที่รับส่งระหว่างเครื่องคอมพิวเตอร์ทั้งสองเครื่องนั้น

การป้องกันการโจมตีแบบ Main-in-the-Middle (MitM) จะใช้วิธีการเข้ารหัส ถึงแม้ว่าผู้โจมตีจะสามารถเข้าถึงข้อมูลได้ แต่ผู้โจมตีจะไม่สามารถตีความข้อมูลได้ รวมถึงการพิสูจน์ตัวตนด้วยข้อความแฮช (Hash) เพราะโค้ดจะสามารถระบุข้อมูลที่ถูกบิดเบือนได้

๑.๔.๒.๒ (๔) การโจมตีในรูปแบบ Buffer Overflow เป็นการโจมตีในส่วนของพื้นที่ในหน่วยความจำ โดยทั่วไปแล้วในการพัฒนาโปรแกรมจะมีการจองพื้นที่ในหน่วยความจำ เพื่อใช้เก็บข้อมูลชั่วคราวซึ่งเรียกว่า Buffer ซึ่งมีขนาดจำกัด หากไม่มีการตรวจสอบขนาดของข้อมูลที่จะนำมาจัดเก็บในหน่วยความจำ ก็จะทำให้เกิดการเก็บข้อมูลที่ใหญ่เกินกว่าความจุของ Buffer และข้อมูลเหล่านั้นจะล้นออกจากหน่วยความจำ สภาวะนี้เรียกว่า Buffer Overflow โดยข้อมูลที่ล้นออกมานั้น จะไปทับกับข้อมูลส่วนอื่น ๆ ในหน่วยความจำ เช่น ชุดคำสั่ง (Code) ของโปรแกรมที่กำลังทำงานอยู่ เป็นต้น ซึ่งทำให้โปรแกรมเกิดการทำงานที่ผิดพลาด หรือไม่สามารถทำงานต่อได้ โดยผู้ไม่ประสงค์ดีจะทำการสร้างข้อมูลที่มีขนาดใหญ่เกินกว่าความจุของ Buffer โดยภายในจะบรรจุชุดคำสั่งที่ไม่ประสงค์ดีไว้ เมื่อโปรแกรมโหลดข้อมูลดังกล่าวเข้าไปในหน่วยความจำและเกิดการล้นของข้อมูล (Data Overflow) นั้น ก็จะไปทับกับส่วนที่เป็นชุดคำสั่งของโปรแกรมที่กำลังทำงานอยู่ ทำให้ชุดคำสั่งที่ไม่ประสงค์ดีถูกนำเข้าไปประมวลผลแทน ซึ่งเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อจะตกอยู่ภายใต้การควบคุมของผู้ไม่ประสงค์ดีในที่สุด

๑.๔.๒.๒ (๕) การโจมตีในรูปแบบ Injection เป็นการโจมตีโดยที่ผู้ไม่ประสงค์ดีใช้คำสั่งแก้ไข หรือลบข้อมูลในฐานข้อมูล โดยทั่วไปจะใช้ภาษา SQL ซึ่งเรียกว่า SQL Injection ซึ่งอาจรวมไปถึงภาษา XML หรือ LDAP Protocol นอกจากนี้ยังมีการโจมตีในรูปแบบ Command Injection โดยผู้ไม่ประสงค์ดีจะแก้ไขคำสั่งใน Command Line และเข้าถึงสิทธิ์ที่สูงขึ้นของระบบได้ ซึ่งสามารถป้องกันได้โดยใช้ Prepared Statement หรือ Store Procedure โดยเป็นการแยกคำสั่งประมวลผลออกจากกัน รวมถึงการตรวจสอบการนำเข้าข้อมูล (Input Validation) เป็นวิธีการที่ใช้ในการตรวจสอบข้อมูลที่ได้รับมาก่อนส่งไปประมวลผลจริง และการทำ Encoding หรือ Sanitization ซึ่งหากข้อมูลที่

รับมาจากภายนอกได้รับการ Encoding หรือ Sanitization ก่อนนำมาประมวลผล ข้อมูลดังกล่าวจะถูกทำให้อยู่ในรูปแบบที่ระบบนำไปประมวลผลได้โดยไม่อันตราย

๑.๔.๒.๒ (๖) การโจมตีในรูปแบบ Cross-Site Scripting and Request Forgery หรือ XSS เป็นการโจมตีโดยเกิดจากช่องโหว่ของแอพพลิเคชั่น ที่ไม่มีการคัดกรองและตรวจสอบข้อมูลที่ได้รับจากผู้ใช้งานว่าเป็นข้อมูลที่เชื่อถือได้หรือไม่ ทำให้ผู้ไม่ประสงค์ดีสามารถสอดแทรกคำสั่งต่างๆ ที่ไม่ประสงค์ดีเข้าไป เมื่อผู้ใช้งานเรียกหน้าเว็บแอพลิเคชันนั้น ๆ ก็อาจถูกขโมยข้อมูลสำคัญไปได้ ซึ่งผู้ไม่ประสงค์ดีอาจจะนำไปใช้ในการสวมรอย และเข้าสู่ระบบเสมือนว่าเป็นผู้ใช้งานตัวจริง ซึ่งการโจมตีในรูปแบบนี้อาจจะไม่เป็นอันตรายต่อเว็บแอปพลเคชันโดยตรงแต่จะส่งผลกระทบต่อผู้ใช้งานได้

๑.๔.๒.๒ (๗) การโจมตีในรูปแบบ Cross-Site Request Forgery หรือ CSRF มักจะใช้ตัวตน และสิทธิ์ของเหยื่อที่มีบนเว็บไซต์ เพื่อปลอมตัวเป็นเหยื่อ และกระทำการใด ๆ ที่ไม่ประสงค์ดี โดยใช้ Cookies ที่เกิดจากการพิสูจน์ตัวตนที่สำเร็จแล้วของเหยื่อ และถูกเก็บไว้ในเว็บบราวเซอร์ ซึ่งการป้องกัน CSRF สามารถทำได้หลายวิธีตั้งแต่การกำหนดเวลาในการพิสูจน์ตัวตนเป็นระยะ ไปจนถึงการกำหนดเวลาให้ Cookies หมดอายุ การเปลี่ยนการใช้ Cookies เป็นการใช้ Session Token ที่ถูกสร้างขึ้นแบบ Dynamic แทน

๑.๔.๒.๒ (๘) การโจมตีในรูปแบบ ARP Poisoning เป็นการโจมตีในรูปแบบหนึ่งที่เกิดขึ้นในระบบเครือข่าย ไม่ว่าเป็นเครือข่ายแบบไร้สายหรือเป็นแบบมีสายโดยปกติ ซึ่งอาศัยช่องโหว่ของ ARP Protocol หรือ Address Resolution Protocol ซึ่งมีความปลอดภัยต่ำ การโจมตีในรูปแบบ ARP Poisoning คือการปลอมแปลง MAC Address ของข้อมูลที่ส่งมาเพื่อหลอกให้เข้าใจว่าข้อมูลดังกล่าวถูกส่งมาจากต้นทางที่ถูกต้อง เมื่อมีการหลอกได้สำเร็จก็จะสามารถส่งข้อมูลเข้าไปในระบบเครือข่ายได้เรื่อย ๆ ซึ่งจะทำให้เกิดการโจมตีในลักษณะ DoS ตามมา นอกจากนั้นก็จะทำให้เกิดการโจมตีในรูปแบบ Man-in-the-Middle อีกด้วย ปัจจุบันการโจมตีในรูปแบบ ARP Poisoning มักเป็นไปได้ยากขึ้นเนื่องจากสามารถตรวจจับได้ง่ายโดยเทคโนโลยีรักษาความมั่นคงปลอดภัยต่าง ๆ เช่น Host Based, Network Based และ IDS เป็นต้น

๑.๔.๒.๒ (๙) การโจมตีในรูปแบบ DNS Poisoning เป็นการโจมตีโดยผู้ไม่ประสงค์ดีสามารถหลอกลวงคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่จัดการข้อมูลของชื่อโดเมน (Domain Name System: DNS) ให้เชื่อว่าข้อมูล Domain Record ปลอมนั้น เป็นข้อมูลที่ถูกต้อง และเป็นข้อมูลจริง โดยข้อมูลปลอมจะอยู่ใน Cache ระยะหนึ่ง และจะทำให้ผู้ไม่ประสงค์ดีสามารถเขียนการตอบกลับ DNS ของที่อยู่ IP Address ใหม่ ซึ่งทำให้ผู้ใช้งานที่เข้าใช้งานเว็บไซต์ด้วย Domain Name นั้น จะดาวน์โหลดไวรัสคอมพิวเตอร์ หรือหนอนคอมพิวเตอร์ แทนที่จะดาวน์โหลดเนื้อหาที่ตนต้องการ ซึ่งการโจมตีในรูปแบบนี้ถูกนำไปประยุกต์ใช้กับการโจมตีที่เรียกว่า Pharming Attack ซึ่งเป็นการโจมตีเพื่อหลอกให้ผู้ใช้งานจำนวนมากเข้าเว็บไซต์ปลอมเพื่อหลอกขโมยข้อมูลหรือแอบติดตั้งมัลแวร์ในเครื่องผู้ใช้งาน

๑.๔.๒.๒ (๑๐) Hijacking คือการโจมตีที่เกี่ยวข้องกับการดักขโมยองค์ประกอบใด ๆ ของระบบ เช่น Domain Name เป็นต้น รวมถึงการเข้าไปยึดครองทรัพยากรของผู้อื่น เช่น การโจมตีในรูปแบบ Click Jacking โดยการหลอกหลวงให้ผู้ใช้งานหลงเชื่อ คลิกปุ่มที่ผู้ไม่ประสงค์ดีได้จัดเตรียมไว้ เป็นต้น

๑.๔.๒.๒ (๑๑) Domain Hijacking เป็นการเปลี่ยนข้อมูลการขึ้นทะเบียน Domain Name โดยไม่ได้รับอนุญาตจากการลักลอบขโมยชื่อบัญชีผู้ใช้งานและรหัสผ่านจากเจ้าของ Domain หรือผู้ไม่ประสงค์ดีเข้าไปแก้ไขการตั้งค่า Domain ในเว็บโฮสติ้ง และนำเอา Domain ไปหลอกลวงผู้เข้าเยี่ยมชมเว็บไซต์ เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล โดยอาจทำให้เกิดการสูญเสียทางการเงินและภาพลักษณ์ชื่อเสียง ตลอดจนอาจเกิดการละเมิดกฎหมายได้

๑.๔.๒.๒ (๑๒) Man-in-the-Browser (MitB) คือ การโจมตีที่เกิดจาก Trojan ที่ฝังตัวอยู่ใน Browser คอยดักจับและแก้ไขหน้าเว็บไซต์ หรือข้อมูลที่มีการรับส่ง โดยที่ผู้ใช้หรือผู้ให้บริหารไม่ทราบว่าข้อมูลได้ถูกแก้ไข ซึ่งโดยส่วนใหญ่แล้วมักจะมีเป้าหมายไปยังเว็บไซต์ของสถาบันการเงิน เช่น เว็บไซต์ของธนาคาร เป็นต้น การโจมตีแบบ MitB สามารถดักจับข้อมูลได้ทุกประเภท ไม่ว่าเว็บไซต์นั้นจะเข้ารหัสด้วยโปรโตคอล SSL หรือ TLS ก็ตาม เนื่องจากโทรจันที่ฝังอยู่ในเว็บ Browser จะใช้วิธีดักจับข้อมูลที่ถูกนำเข้าทาง Browser โดยตรง เช่น ชื่อผู้ใช้งาน หรือรหัสผ่าน เป็นต้น ก่อนที่บราวเซอร์จะนำข้อมูลเหล่านั้นไปเข้ารหัส และส่งไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อประมวลผลต่อไป

๑.๔.๒.๒ (๑๓) Zero-Day Exploits การโจมตีในรูปแบบ Zero-Day มักเกิดขึ้นกับช่องโหว่ที่ถูกค้นพบโดยผู้ไม่ประสงค์ดี โดยที่ผู้ผลิตซอฟต์แวร์ยังไม่ทราบว่าซอฟต์แวร์ของตนมีช่องโหว่ หรือบางกรณีอาจจะเกิดขึ้นโดยที่ผู้ผลิตซอฟต์แวร์รู้ดีว่าผลิตภัณฑ์ของตนมีช่องโหว่แต่ยังไม่สามารถพัฒนาโปรแกรมปิดช่องโหว่ (Patch) ได้ โดยผู้ไม่ประสงค์ดีจะพัฒนาโปรแกรมที่ใช้ในการเจาะระบบออกมา เรียกว่า Zero-Day Exploit ซึ่งในบางครั้งจะมีการแจกจ่ายไปยังผู้ไม่ประสงค์ดีรายอื่น ๆ เพื่อนำไปโจมตีระบบ หรืออาจเก็บไว้เพื่อจำหน่ายเพื่อใช้เป็นเครื่องมือในการโจมตีเป้าหมายที่เฉพาะเจาะจงต่อไป

ภาพที่ ๑.๓ ภาพแสดงช่วงเวลาการเกิด Zero-day Attack และการออกโปรแกรมปิดช่องโหว่

๑.๔.๒.๒ (๑๔) Replay Attacks คือ การโจมตีที่เกิดขึ้นเมื่อมีการดักจับข้อมูลในเครือข่าย และเข้าไปแก้ไขข้อมูลเช่น การดักจับชื่อผู้ใช้งาน รหัสผ่าน หรือดักรับ Certificate และนำไปใช้ต่อในการยืนยันและพิสูจน์ตัวตนเพื่อเข้าสู่ระบบ เป็นต้น ดังตัวอย่าง โปรโตคอลการตรวจสอบสิทธิ์ Kerberos ผู้ไม่ประสงค์ดีใช้ Certificate ที่ดักรับมาได้ ใช้ในการยืนยันตัวตนซ้ำแล้วซ้ำเล่าเมื่อต้องการเข้าสู่ระบบ หากโจมตีสำเร็จ ผู้ไม่ประสงค์ดีจะได้รับสิทธิ์เช่นเดียวกับ Certificate นั้น ๆ ได้รับ ตราบใดที่ Certificate นั้นยังไม่หมดอายุ

๑.๔.๒.๒ (๑๕) Mac and IP Spoofing Attacks เป็นการโจมตีโดยการปลอมตัวเป็นผู้อื่นเพื่อเข้าถึงทรัพยากรที่ต้องการ เช่น การสร้างหน้า Login เข้าสู่ระบบปลอมเพื่อหลอกให้ผู้ใช้งานกรอกชื่อผู้ใช้งานและรหัสผ่าน รวมไปถึงการโจมตีโดยเทคนิค ARP Spoofing ซึ่งที่เป็นเทคนิคปลอมแปลง Mac Address และเทคนิค IP Spoofing ที่หลอกลวงให้เชื่อว่าข้อมูลที่ส่งมาเป็นข้อมูลที่มาจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ต้นทางจริงที่น่าเชื่อถือ

บทที่ ๒ การปฏิบัติการในมิติไซเบอร์ของกองทัพอากาศ

๒.๑ ยุทธศาสตร์ที่เกี่ยวข้องด้านไซเบอร์

๒.๑.๑ ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๕๘

ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๕๘ เป็นกรอบแนวทางในการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหม ทั้งในด้านการเตรียมและใช้ศักยภาพด้านไซเบอร์เพื่อสนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหมและเตรียมความพร้อมรองรับการมอบหมายหน้าที่จากรัฐบาลให้เป็นหน่วยงานในการจัดการภัยคุกคามทางไซเบอร์ที่มีความรุนแรงระดับชาติเมื่อถึงเงื่อนไขที่กำหนด โดยกำหนดประเด็นยุทธศาสตร์ไว้ ๓ ประเด็น ดังนี้

๒.๑.๑.๑ การมีเสรีภาพในการใช้ไซเบอร์ให้เกิดประโยชน์ (การป้องกัน) กล่าวคือ มีเสรีภาพในการใช้ไซเบอร์ให้เกิดประโยชน์ ปลอดภัย และต่อเนื่อง เพื่อเพิ่มมิติให้กับการปฏิบัติภารกิจ และจัดการปัจจัยแวดล้อมที่เอื้ออำนวยต่อการใช้ไซเบอร์อย่างได้เปรียบไม่ให้เป็นจุดอ่อนหรือจุดล่อแหลมต่อการปฏิบัติภารกิจตลอดจนมีเอกภาพในการเตรียม และใช้ศักยภาพด้านไซเบอร์ในลักษณะรวมการควบคุมแยกการปฏิบัติ โดยหมายถึง การที่กระทรวงกลาโหมมีขีดความสามารถในการใช้ศักยภาพด้านไซเบอร์เป็นเครื่องมือเสริมการปฏิบัติภารกิจในพื้นที่การรบทางบก ทะเล และอากาศ โดยเป็นเครื่องมือหลักของการปฏิบัติในพื้นที่การรบด้านไซเบอร์ได้อย่างมีประสิทธิภาพ ปลอดภัย และต่อเนื่อง ไม่เป็นอุปสรรคหรือข้อจำกัดที่มีผลลดทอนประสิทธิภาพและประสิทธิผลของการปฏิบัติภารกิจ โดยเฉพาะที่มีผลต่อระบบบัญชาการและควบคุม

๒.๑.๑.๒ การจำกัดเสรีภาพการใช้ไซเบอร์ของฝ่ายตรงข้าม (การป้องปราม) กล่าวคือ จำกัดเสรีภาพการใช้ไซเบอร์ของฝ่ายตรงข้าม และขยายผลจากจุดอ่อนหรือจุดล่อแหลมของฝ่ายตรงข้ามเพื่อให้เกิดผลสนับสนุนหรือนำไปสู่ภาวะและ/หรือเงื่อนไขที่ต้องการ โดยหมายถึง การที่กระทรวงกลาโหมมีขีดความสามารถในการใช้ศักยภาพด้านไซเบอร์ เพื่อจำกัดเสรีตลอดจนประสิทธิภาพ ความถูกต้องครบถ้วน และความลับของการใช้ไซเบอร์ของฝ่ายตรงข้าม โดยใช้ประโยชน์จากจุดอ่อนหรือจุดล่อแหลมทางไซเบอร์ของฝ่ายตรงข้ามที่มีอยู่เดิมและที่สร้างขึ้นโดยฝ่ายเรา รวมทั้งมีการใช้การปฏิบัติการทางไซเบอร์ เพื่อให้เกิดประโยชน์ในด้านการข่าวกรองเพื่อสนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหม และการดำเนินการด้านข่าวกรองไซเบอร์ร่วมกับการปฏิบัติการอื่นเพื่อวัตถุประสงค์ทางทหาร

๒.๑.๑.๓ การสนับสนุนการใช้ศักยภาพไซเบอร์ระดับชาติ (การผนึกกำลัง) กล่าวคือ สนับสนุนการใช้ศักยภาพทางไซเบอร์ระดับชาติ มีความพร้อมเป็นหน่วยงานชั้นนำในการจัดการภัยคุกคามทางไซเบอร์ระดับชาติเมื่อได้รับมอบหมายจากรัฐบาลหรือเมื่อถึงเงื่อนไขที่กำหนดรวมทั้งแสวงประโยชน์จากความร่วมมือระดับนานาชาติและรักษาสมดุลของความสัมพันธ์ให้เห็นผลอย่างเป็นรูปธรรม โดยหมายถึง การที่กระทรวงกลาโหมมีขีดความสามารถในการใช้ศักยภาพด้านไซเบอร์ในการเตรียมความพร้อมและดำเนินการร่วมกับหน่วยงานที่เกี่ยวข้อง ในการจัดการภัยคุกคามทางไซเบอร์ระดับชาติ ในฐานะเป็นเครื่องมือหนึ่งของรัฐบาล รวมทั้งความพร้อมเป็นหน่วยงานในการดำเนินการจัดการกับภัยคุกคามทางไซเบอร์ระดับชาติ เมื่อได้รับการสั่งการและสนับสนุนจากรัฐบาล

และสร้างความร่วมมือด้านการป้องกันไซเบอร์ร่วมกับนานาชาติตลอดจนชาติมหาอำนาจ พร้อมทั้งแสวงประโยชน์จากความสัมพันธ์นั้นให้เกิดผลเป็นรูปธรรม

๒.๑.๒ ยุทธศาสตร์ทหารด้านไซเบอร์ กองทัพไทย พ.ศ.๒๕๕๘ กองทัพไทยจัดทำยุทธศาสตร์ทหารด้านไซเบอร์เป็นกรอบแนวทางในการดำเนินการด้านไซเบอร์ของกองทัพไทย ทั้งในด้านการเตรียมและใช้ศักยภาพด้านไซเบอร์ เพื่อให้สามารถบรรลุวัตถุประสงค์ทางทหารที่ตั้งไว้ โดยกำหนดประเด็นยุทธศาสตร์ไว้ ๓ ประเด็น ดังนี้

๒.๑.๒.๑ การป้องกันเชิงรุก เป็นยุทธศาสตร์ที่ว่าด้วยการใช้พลังอำนาจทางไซเบอร์ทั้งปวงของกองทัพไทย เพื่อการปฏิบัติการในมิติทางไซเบอร์ต่อฝ่ายตรงข้าม ทั้งที่กระทำโดยรัฐ สนับสนุนโดยรัฐ และการกระทำที่มิได้ดำเนินการโดยรัฐ ตลอดจนการปฏิบัติการในมิติทางไซเบอร์ต่อกลุ่มหรือบุคคลใดที่อาจเป็นภัยคุกคามทางไซเบอร์ โดยมีความมุ่งหมายในการลดทอน ขัดขวาง ระงับ ยับยั้ง ในเชิงรุก การตอบโต้อย่างรวดเร็วกรณีถูกโจมตีทางไซเบอร์ รวมถึงการป้องปรามทางไซเบอร์ ทั้งนี้ เพื่อการสร้างความได้เปรียบต่อฝ่ายตรงข้ามตั้งแต่สภาวะปกติ และสร้างความตระหนักรู้ทางไซเบอร์ที่จะนำไปสู่การตัดสินใจของระดับผู้บังคับบัญชาให้เท่าทันต่อสถานการณ์

๒.๑.๒.๒ การผนึกกำลังป้องกันประเทศ เป็นยุทธศาสตร์ที่ว่าด้วยการสร้างความร่วมมือและบูรณาการขีดความสามารถในการปฏิบัติการในมิติทางไซเบอร์ของทุกภาคส่วนภายในประเทศเข้าด้วยกันอย่างเป็นระบบ ด้วยการมีแผนรองรับตั้งแต่สภาวะปกติ เพื่อแก้ไขข้อจำกัดและชดเชยอำนาจกำลังรบของกองทัพไทยด้านการปฏิบัติการในมิติทางไซเบอร์ที่มีอยู่อย่างจำกัด เพื่อให้สามารถปฏิบัติหน้าที่ในการป้องกันประเทศได้อย่างมีประสิทธิภาพ โดยจะต้องมีการเตรียมการและดำเนินการอย่างต่อเนื่องตลอดเวลา ทั้งในยามปกติและยามสงคราม อีกทั้งยังรวมถึงการใช้พลังอำนาจทางไซเบอร์ทั้งปวงของกองทัพไทย ในการสนับสนุนการบริหารประเทศของภาครัฐบาลด้านการรักษาความมั่นคงภายในและการรักษาความสงบเรียบร้อยภายในประเทศในทุกมิติ เพื่อให้เกิดความมีเสถียรภาพและความมั่นคงของประเทศโดยรวม

๒.๑.๒.๓ การสร้างความร่วมมือด้านความมั่นคง เป็นยุทธศาสตร์ที่ว่าด้วยการใช้พลังอำนาจทางไซเบอร์ของกองทัพไทย ในการเสริมสร้างความร่วมมือกับประเทศสมาชิกอาเซียนและมิตรประเทศอื่น ทั้งในระดับภูมิภาคและในระดับโลกโดยมุ่งเน้นไปที่การสร้างความร่วมมือ เพื่อเป็นการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ การสร้างบรรยากาศความเป็นมิตรเพื่อลดเงื่อนไขที่จะนำไปสู่ความขัดแย้ง และการควบคุมมิให้ความขัดแย้ง ขยายวงกว้างจนไม่สามารถควบคุมได้ หรือยุติความขัดแย้งได้อย่างสันติวิธี เพื่อสนับสนุนรัฐบาลในการสร้างความร่วมมือระหว่างประเทศ ทั้งในระดับทวิภาคีและระดับพหุภาคี

๒.๑.๓ ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี ฉบับปรับปรุง (พ.ศ.๒๕๖๑ – ๒๕๘๐) ฉบับปรับปรุง พ.ศ.๒๕๖๓

มุ่งเน้นการพัฒนากองทัพอากาศในทุกด้านอย่างเป็นระบบ ให้สอดคล้องกับการพัฒนาด้านความมั่นคงของชาติ และการพัฒนาศักยภาพทางทหารตามยุทธศาสตร์และนโยบายที่เกี่ยวข้อง เพื่อให้กองทัพอากาศมีขีดความสามารถที่เพียงพอและเหมาะสมในการปฏิบัติภารกิจที่ได้รับมอบหมายได้อย่างมีประสิทธิภาพ โดยกองทัพอากาศ แบ่งทิศทางการพัฒนาออกเป็น ๓ มิติสำคัญ คือ มิติทางอากาศ มิติไซเบอร์ มิติอวกาศ มุ่งพัฒนาให้เกิดความต่อเนื่องและส่งต่อในแต่ละระยะ ทั้งนี้

ทิศทางการพัฒนาด้านมิติไซเบอร์ (Cyber Domain) ซึ่งมีรายละเอียด ดังนี้

ทิศทางการพัฒนามิติไซเบอร์ (Cyber Domain)			
๒๕๖๓-๒๕๖๕	**๒๕๖๖-๒๕๗๐**	**๒๕๗๑-๒๕๗๕**	**๒๕๗๖-๒๕๘๐**
✣ กำหนดสมรรถนะหลักและทักษะของกำลังพล/นักรบไซเบอร์ ✣ กำหนดจรรยาบรรณของกำลังพล/นักรบไซเบอร์ (Cyber Worrior Code of Conduct) ✣ สนับสนุนการพัฒนาซอฟต์แวร์ของกองทัพอากาศให้มีมาตรฐานด้านความมั่นคงปลอดภัย ✣ เสริมสร้างขีดความสามารถระบบเฝ้าระวังและตรวจจับภัยคุกคามด้านไซเบอร์ ✣ พัฒนาระบบข่าวกรองทางไซเบอร์ (Cyber Intelligence System) เพื่อการปฏิบัติงานด้านยุทธการ ✣ ริเริ่มการทดสอบการปฏิบัติการไซเบอร์ ตลอดจนการฝึกร่วม (Bilateral exercise) และ Multi-lateral exercise กับมิตรประเทศ ✣ พัฒนารูปแบบการฝึกจำลองยุทธ์ และรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์อย่างต่อเนื่อง ✣ ริเริ่มการประยุกต์ใช้เทคโนโลยี AI ในการปฏิบัติการมิติไซเบอร์ของกองทัพอากาศ ✣ สร้างความร่วมมือกับหน่วยงานที่มีศักยภาพในประเทศและอุตสาหกรรมป้องกันประเทศของไทย เพื่อการพัฒนางานในมิติไซเบอร์ของกองทัพอากาศ ตามแนวทางการจัดหาพร้อมการพัฒนา (P&D)	✣ เตรียมกำลังพล/นักรบไซเบอร์ตั้งแต่ต้นน้ำ โดยพัฒนาให้มีสมรรถนะหลักและทักษะตามที่กองทัพอากาศกำหนด ทั้งในเชิงปริมาณและคุณภาพ ✣ ปลูกฝังจรรยาบรรณให้กับกำลังพล/นักรบไซเบอร์ โดยต้องมีคุณธรรมและจริยธรรมในการปฏิบัติภารกิจ ✣ สร้างเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber security Culture) ในหน่วยงานหลัก ✣ ดำรงมาตรฐานด้านความมั่นคงปลอดภัยซอฟท์แวร์ของกองทัพอากาศ ✣ เสริมสร้างขีดความสามารถและความพร้อมของชุดปฏิบัติการไซเบอร์เพื่อแก้ไขสถานการณ์วิกฤตตามพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ✣ สร้างความเข้มแข็งให้กับระบบข่าวกรองทางไซเบอร์ (Cyber Intelligence System) เพื่อการปฏิบัติงานด้านยุทธการ ✣ ดำรงการฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสมและส่งเสริมการบูรณาการเข้ากับการปฏิบัติการในมิติทางอากาศ และมิติอวกาศ ✣ ทดสอบและใช้งานเทคโนโลยี AI ในการปฏิบัติการมิติไซเบอร์ของกองทัพอากาศ ✣ สร้างความร่วมมือกับสถาบันการศึกษา สถาบันวิจัยและอุตสาหกรรมป้องกันประเทศของไทยในการวิจัยและพัฒนามิติไซเบอร์ของกองทัพอากาศ	✣ พัฒนาระบบคัดสรรและสร้างกำลังพล/นักรบไซเบอร์ และปลูกฝังจรรยาบรรณตั้งแต่ต้นน้ำ เพื่อให้เกิดความยั่งยืน ✣ ดำรงวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber security Culture) ในทุกหน่วยงาน ✣ กำหนดให้ทุกซอฟต์แวร์ของกองทัพอากาศต้องมีมาตรฐานความมั่นคงปลอดภัย ✣ ดำรงความพร้อมของชุดปฏิบัติการไซเบอร์เพื่อแก้ไขสถานการณ์วิกฤตตามพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ✣ ดำรงการฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสมและส่งเสริมการบูรณาการเข้ากับการปฏิบัติการในมิติทางอากาศ และมิติอวกาศ ✣ ทบทวนและประเมินผลหน่วยงานด้านไซเบอร์ และเสนอแนะแนวทางการพัฒนาหน่วยงาน ✣ ปรับปรุงการใช้งานเทคโนโลยี AI ในการปฏิบัติการมิติไซเบอร์ของกองทัพอากาศ ✣ พัฒนาเครื่องมือและอุปกรณ์ในมิติไซเบอร์ โดยความร่วมมือระหว่างกองทัพอากาศและอุตสาหกรรมป้องกันประเทศของไทย ตามแนวทางการจัดหาพร้อมการพัฒนา (P&D)	✣ เสริมสร้างขีดความสามารถกำลังพล/นักรบไซเบอร์ เพื่อรองรับพลวัตรการเปลี่ยนแปลงในมิติไซเบอร์ ✣ ดำรงวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber security Culture) ของกองทัพอากาศทั้งระบบ ✣ ปฏิบัติการในมิติไซเบอร์อย่างเต็มรูปแบบ และยกระดับขีดความสามารถตามความจำเป็น ✣ ดำรงความเป็นมืออาชีพของชุดปฏิบัติการไซเบอร์ เพื่อแก้ไขสถานการณ์วิกฤตตามพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ✣ ใช้งานเทคโนโลยี AI ในการปฏิบัติการมิติไซเบอร์ของกองทัพอากาศอย่างเต็มรูปแบบ ✣ ดำรงขีดความสามารถของระบบต่าง ๆ ในกองทัพอากาศให้มีความสามารถคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) ✣ ประเมินผลการพัฒนาเครื่องมือและอุปกรณ์ในมิติไซเบอร์ ซึ่งเกิดจากความร่วมมือระหว่างกองทัพอากาศและอุตสาหกรรมป้องกันประเทศของไทย

ภาพที่ ๒.๑ ทิศทางการพัฒนามิติไซเบอร์ (Cyber Domain) ของกองทัพอากาศ ตามยุทธศาสตร์กองทัพอากาศ ๒๐ ปี ฉบับปรับปรุง (พ.ศ.๒๕๖๑ – ๒๕๘๐) ฉบับปรับปรุง พ.ศ. ๒๕๖๓

โดยทิศทางในการพัฒนามิติด้านไซเบอร์ดังกล่าวเกี่ยวข้องกับประเด็นยุทธศาสตร์ ต่อไปนี้

ยุทธศาสตร์ที่ ๒ เสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศและรักษาผลประโยชน์แห่งชาติ เป้าหมายของยุทธศาสตร์คือ

กองทัพอากาศมีสมรรถนะและความพร้อมในการป้องกันประเทศ และรักษาผลประโยชน์แห่งชาติอย่างมีประสิทธิภาพ โดยศูนย์ไซเบอร์กองทัพอากาศ

กองทัพอากาศผนึกกำลังร่วมกับเหล่าทัพและหน่วยงานด้านความมั่นคงในการป้องกันประเทศ และรักษาผลประโยชน์ของชาติอย่างมีประสิทธิภาพ

ประเทศไทยมีเกียรติภูมิ และความร่วมมือกับมิตรประเทศ ได้รับการยอมรับในระดับสากล รวมทั้งรักษาดุลยภาพระหว่างประเทศ

สำหรับยุทธศาสตร์ที่เกี่ยวข้องในภารกิจของศูนย์ไซเบอร์กองทัพอากาศตามกลยุทธ์ ดังนี้

๒.๑.๓.๑ กลยุทธ์ที่ ๒.๑ เสริมสร้างขีดความสามารถการบัญชาการและควบคุม (C2) โดยมีวัตถุประสงค์เพื่อการหยั่งรู้การแบบเบ็ดเสร็จ (Total Situation Awareness) มีขีดความสามารถและความพร้อมตลอด ๒๔ ชั่วโมง อันเป็นเครื่องมือสำหรับผู้บังคับบัญชาในการควบคุม โดยมีเป้าหมายการพัฒนาให้มีขีดความสามารถในการบัญชาการและควบคุมหลายมิติ (Multi-Domain Command and Control : MDC2) บนพื้นฐานของการพึ่งพาตนเอง โดยศูนย์ไซเบอร์กองทัพอากาศมีส่วนเกี่ยวข้องในการเตรียมข้อมูลด้านไซเบอร์เพื่อนำไปใช้ในระบบการจัดการข้อมูลด้านยุทธการและด้านการสนับสนุนยุทธการของระบบบัญชาการและควบคุม แบบบูรณาการ

๒.๑.๓.๒ กลยุทธ์ที่ ๒.๒ เสริมสร้างขีดความสามารถระบบตรวจจับ (Sensor) โดยมีวัตถุประสงค์เพื่อพัฒนาระบบตรวจจับ (Sensor) ที่สามารถรวบรวมข้อมูลข่าวสารในรูปแบบดิจิทัลที่มีความถูกต้อง ครบถ้วน และทันเวลา อีกทั้งสามารถบูรณาการข้อมูลข่าสารทั้งหมดให้อยู่ในรูปแบบข้อมูลข่าวสารที่ชาญฉลาด (Smart Information) รวมถึงกระบวนการ (Process) ในการผลิตข้อมูลข่าวสารให้ตรงกับความต้องการของผู้ใช้งาน เพื่อประโยชน์ในการรบและที่มิใช่การรบ ทั้งนี้ต้องสามารถรองรับการบูรณาการร่วมกับระบบตรวจจับ (Sensor) ของกองบัญชาการกองทัพไทย เหล่าทัพและหน่วยงานอื่นที่เกี่ยวข้อง ภายใต้มาตรฐานการรักษาความปลอดภัยของกองทัพอากาศ โดยศูนย์ไซเบอร์กองทัพอากาศจะต้องปรับปรุงขีดความสามารถระบบตรวจจับ (Sensor) ในมิติไซเบอร์ให้รองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ต้องมีความพร้อมและสามารถเชื่อมต่อกับเครือข่ายเดิมและเครือข่ายใหม่ของกองทัพอากาศได้อย่างมีประสิทธิภาพ

๒.๑.๓.๓ กลยุทธ์ที่ ๒.๓ เสริมสร้างขีดความสามารถผู้ปฏิบัติ/หน่วยปฏิบัติ (Shooter) โดยมีวัตถุประสงค์เพื่อให้ผู้ปฏิบัติ/หน่วยปฏิบัติ (Shooter) มีความชาญฉลาด (Smart Platform) มีขีดความสามารถในการปฏิบัติการรบและที่มิใช่การรบ โดยใช้เทคโนโลยีที่ทันสมัยมีอำนาจการทำลาย (Fire Power) มีความแม่นยำ (Precision) มีความสามารถในการปฏิบัติภารกิจจากระยะไกล (Stand-off) และ/หรือเกินระยะสายตา (Beyond Visual Range) มีระบบป้องกันตนเอง รองรับการใช้งานอาวุธสมรรถนะสูงที่ทันสมัย สามารถบูรณาการและเชื่อมโยงข้อมูลรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ของกองทัพอากาศ โดยศูนย์ไซเบอร์กองทัพอากาศมีหน้าที่ในการพัฒนาขีดความสามารถทางไซเบอร์ (Cyber Capability) ในการป้องกันติดตาม เฝ้าระวัง แจ้งเตือน และวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response)

ตลอดจนการป้องปรามด้วยการทำลาย ยับยั้ง รวมทั้งลดทอนขีดความสามารถของ ฝ่ายตรงข้าม และผู้ที่มีส่วนเกี่ยวข้อง

๒.๑.๓.๔ กลยุทธ์ที่ ๒.๗ เสริมสร้างขีดความสามารถด้านการข่าวและความร่วมมือด้านความมั่นคง มีวัตถุประสงค์เพื่อเพิ่มประสิทธิภาพงานด้านการข่าวกรองการต่อต้านข่าวกรองและวิเทศสัมพันธ์ ให้สามารถแจ้งเตือนล่วงหน้าได้อย่างครบถ้วน ถูกต้อง ปลอดภัย และทันต่อสถานการณ์ ตรงตามความต้องการของผู้ใช้ และสามารถสนับสนุนการพัฒนาระบบงานข่าวกรองแห่งชาติแบบบูรณาการอย่างมีประสิทธิภาพ เพื่อรองรับการพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ อีกทั้ง เพื่อเสริมสร้างความสัมพันธ์และความร่วมมือในประชาคมอาเซียนรวมถึงความสัมพันธ์ทางทหารที่ดีระหว่างกองทัพอากาศไทยกับกองทัพอากาศประเทศเพื่อนบ้านและมิตรประเทศ โดยศูนย์ไซเบอร์กองทัพอากาศมีหน้าที่รับผิดชอบพัฒนาระบบข่าวกรองกองทัพอากาศ ให้สามารถสนับสนุนการปฏิบัติการทางไซเบอร์ รวมถึงสนับสนุนการพัฒนาระบบงานข่าวกรองแห่งชาติแบบบูรณาการอย่างมีประสิทธิภาพ

๒.๒ หลักนิยมที่เกี่ยวข้องด้านไซเบอร์

๒.๒.๑ หลักนิยมกองทัพอากาศ พ.ศ.๒๕๖๒ โดยนิยามของหลักนิยมคือหลักการมูลฐานที่มีรากฐานมาจากประสบการณ์ หรือหลักเกณฑ์ที่คิดค้นขึ้นมา และได้รับการพิจารณามาอย่างถ่องแท้แล้วนำมาสั่งสอนจนเป็นที่ยอมรับจากผู้ร่วมงานร่วมอาชีพ สำหรับทางทหารจะได้มาจากบทเรียนและปฏิบัติการที่กระทำอยู่เป็นประจำที่ได้ผลจนเป็นที่ยอมรับว่าเป็นสิ่งที่ควรปฏิบัติ เป็นศูนย์รวมแห่งความเชื่อในการทำศึก ถือกำเนิดมาจากการหลอมรวมกันของหลักการพื้นฐานและความคิดสร้างสรรค์สิ่งใหม่ ๆ ที่เกี่ยวกับการใช้อำนาจกำลังรบ หรือ การใช้อาวุธให้มีประสิทธิภาพมากที่สุดในทุกโอกาสที่ปฏิบัติการต่อข้าศึก เพื่อให้ได้ชัยชนะ เพื่อผลสำเร็จของการปฏิบัติการตามภารกิจที่ได้รับมอบหมาย โดยวัตถุประสงค์ของหลักนิยมการปฏิบัติการไซเบอร์แบ่งออกเป็น ๔ ด้าน ได้แก่ การป้องกันในมิติไซเบอร์ (Cyberspace Defense) การข่าวกรองการลาดตระเวน และการเฝ้าตรวจในมิติไซเบอร์ (Cyberspace Intelligence, Surveillance and Reconnaissance) การเตรียมสภาวะแวดล้อมในการปฏิบัติการในมิติไซเบอร์ (Cyberspace Operational Preparation of the Environment) และการป้องปรามในมิติไซเบอร์ (Cyberspace Offense) ดังนี้

๒.๒.๑.๑ การป้องกันในมิติไซเบอร์ (Cyberspace Defense) การป้องกันในมิติไซเบอร์เป็นการปฏิบัติการไซเบอร์ เพื่อดำรงการใช้งานระบบเครือข่ายสารสนเทศของกองทัพอากาศทั้งระบบสารสนเทศเพื่อการยุทธ์ (Combat Information System: CIS) และระบบสารสนเทศเพื่อการสนับสนุน (Support Information System: SIS) ด้วยการใช้ขีดความสามารถทางไซเบอร์เชิงป้องกัน โดยหน่วยงานด้านไซเบอร์จะรับผิดชอบกำกับดูแลเรื่องการป้องกันระบบเครือข่ายสารสนเทศในภาพรวม ร่วมกับผู้รับผิดชอบของแต่ละระบบสารสนเทศ ซึ่งจะเป็นผู้ดำเนินการป้องกันตามมาตรการที่กำหนด

๒.๒.๑.๒ การข่าวกรอง การลาดตระเวน และการเฝ้าตรวจในมิติไซเบอร์ (Cyberspace Intelligence, Surveillance and Reconnaissance: Cyberspace ISR) การข่าวกรอง กาลาดตระเวน และการเฝ้าตรวจในมิติไซเบอร์เป็นการปฏิบัติการไซเบอร์ เพื่อรวบรวมข้อมูลข่าวกรองที่มีความสำคัญหรือจำเป็นต่อการปฏิบัติการไซเบอร์ทั้งเชิงป้องกันและเชิงป้องปราม รวมทั้งการปฏิบัติการทางทหารของ

กองทัพอากาศในมิติอื่น ๆ โดยปฏิบัติการเหล่านี้ต้องมีความสอดประสาน (Synchronization) กับระบบการวางแผนและการปฏิบัติการทางทหาร สามารถสนับสนุนได้ทั้งการปฏิบัติการในปัจจุบันและในอนาคต ทั้งนี้ปฏิบัติการ Cyber ISR จะมุ่งเป้าไปที่ข้อมูลข่าวกรองในระดับยุทธการและระดับยุทธวิธี เพื่อเชื่อมโยงข้อมูลของฝ่ายตรงข้ามที่ได้จากปฏิบัติการในมิติไซเบอร์ไปสู่การวางแผนทางทหาร ปฏิบัติการ Cyber ISR จะปฏิบัติโดยหน่วยงานด้านไซเบอร์ของกองทัพอากาศ ภายใต้ความร่วมมือกับหน่วยข้อมูลข่าวกรองอื่นที่เกี่ยวข้อง เพื่อการกระจายและแลกเปลี่ยนข้อมูลข่าวกรองร่วม

๒.๒.๑.๓ การเตรียมสภาวะแวดล้อมในการปฏิบัติการในมิติไซเบอร์ (Cyberspace Operational Preparation of the Environment : Cyberspace OPE) การเตรียมสภาวะแวดล้อมในการปฏิบัติการในมิติไซเบอร์เป็นการปฏิบัติการไซเบอร์ เพื่อสร้างสภาวะความพร้อมสำหรับการปฏิบัติการทางทหารในมิติไซเบอร์และมิติอื่น ๆ ด้วยการปฏิบัติการไซเบอร์เชิงป้องกันเพื่อดำรงขีดความสามารถการปฏิบัติการในมิติไซเบอร์ของฝ่ายเรา รวมทั้งปฏิบัติการไซเบอร์เชิงป้องปรามเพื่อการขัดขวาง ทำลาย หรือควบคุมการใช้งานในมิติไซเบอร์ของฝ่ายตรงข้าม ภายใต้การสร้างสภาวะการปฏิบัติการที่ปลอดภัย ด้วยการลบร่องรอยหรือกลบเกลื่อนบิดเบือนร่องรอยของการปฏิบัติการ ให้ยากแก่การสืบย้อนกลับมาถึงแหล่งปฏิบัติการหรือผู้ปฏิบัติการ เพื่อให้เกิดสภาวะแวดล้อมที่เกื้อกูลต่อการปฏิบัติการทางทหารในทุกมิติ ในห้วงเวลาและสถานที่ที่ต้องการ

๒.๒.๑.๔ การป้องปรามในมิติไซเบอร์ (Cyberspace Offense) การป้องปรามในมิติไซเบอร์เป็นปฏิบัติการไซเบอร์ที่แสวงประโยชน์จากช่องโหว่ทางไซเบอร์เพื่อเจาะระบบ (Exploitation) และสร้างผลกระทบในเชิงสร้างความเสียหายหรือเข้าควบคุม ต่อระบบเป้าหมายทั้งในระดับเครือข่ายเชิงกายภาพ (Physical Network Layer) ระดับเครือข่ายเชิงตรรกะ (Logical Network Layer) และระดับเครือข่ายเชิงบุคคล/หน่วยงาน (Cyber-Persona Layer) ดังนี้

๒.๒.๑.๔ (๑) การปฏิเสธการใช้งาน (Deny) มีวัตถุประสงค์เพื่อสร้างผลกระทบให้เกิดขึ้นต่อความพร้อมใช้งานระบบเป้าหมายของฝ่ายตรงข้ามในระดับที่ต้องการในห้วงเวลาที่ต้องการ เป็นการลด ขัดขวาง ทำลายขีดความสามารถในการใช้ทรัพยากรทางไซเบอร์ด้านการทหารของฝ่ายตรงข้าม แบ่งออกเป็น ๓ ระดับ ดังนี้

- ระดับลดขีดความสามารถ (Degrade) เป็นลักษณะของการพยายามลดขีดความสามารถในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมายให้ไปอยู่ในระดับที่ต้องการโดยระบุเป็นค่าเปอร์เซ็นต์เป้าหมายของขีดความสามารถ (Percentage of Capacity) โดยระดับของการลดขีดความสามารถจะต้องกำหนดให้ชัดเจน และหากมีความต้องการระบุห้วงเวลา ให้กำหนดห้วงเวลาด้วย

- ระดับขัดขวางขีดความสามารถ (Disrupt) เป็นลักษณะของการพยายามทำลายขีดความสามารถทั้งมวลในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมายแบบชั่วคราวเฉพาะระหว่างห้วงเวลาที่ต้องการ โดยระบุเวลาเริ่มและเวลาสิ้นสุด ทั้งนี้การขัดขวางขีดความสามารถอาจพิจารณาเป็นรูปแบบของการลดขีดความสามารถ (Degrade) ที่กำหนดระดับของการลดขีดความสามารถเท่ากับ ๑๐๐ เปอร์เซ็นต์ได้

- ระดับทำลายขีดความสามารถ (Destroy) เป็นลักษณะของการพยายามทำลายขีดความสามารถทั้งมวลในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมายแบบถาวร (กำหนดให้ค่าเปอร์เซ็นต์เป้าหมายของขีดความสามารถและห้วงเวลาที่ต้องการมีค่าสูงสุด)

๒.๒.๑.๔ (๒) การเข้าควบคุม (Manipulate) เป็นการเข้าควบคุมหรือเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศ ตลอดจนระบบเครือข่าย ระบบสารสนเทศของเป้าหมายให้เป็นไปตามเจตนารมณ์ วัตถุประสงค์และการสั่งการ ของผู้บังคับบัญชาฝ่ายเรา

๒.๒.๑.๔ (๓) การเตรียมความพร้อม แบ่งได้ตามสถานการณ์ ดังนี้

- ความพร้อมของกำลังรบในภาวะปกติ ได้แก่ ผู้ทดสอบการเจาะระบบ (Pen-Tester) ทำหน้าที่ในการทดสอบเจาะระบบสารสนเทศของกองทัพอากาศ พร้อมทั้งให้คำแนะนำหรือทำการแก้ไขปรับปรุงช่องโหว่ทางไซเบอร์ที่ตรวจพบ ให้มีความปลอดภัยจากการถูกโจมตีทางไซเบอร์

- ความพร้อมของกำลังรบในภาวะไม่ปกติ ได้แก่ ชุดป้องปรามทางไซเบอร์ (Cyber Warriors) ทำหน้าที่ในการปฏิบัติการไซเบอร์เพื่อโจมตีต่อเป้าหมายทางไซเบอร์ทันทีที่ได้รับการสั่งการจากผู้บัญชาการศูนย์ปฏิบัติการกองทัพอากาศ รวมทั้งให้การสนับสนุนการปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวกรองและการปฏิบัติการข่าวสารของกองทัพอากาศ

๒.๒.๑.๕ การปฏิบัติการไซเบอร์ (Cyber Operations) การปฏิบัติการไซเบอร์ของกองทัพอากาศเป็นการปฏิบัติภายใต้การบัญชาการและการควบคุมของกองทัพอากาศ ซึ่งต้องมีการปฏิบัติที่สอดคล้องกับมิติทางอากาศ (Air Domain) และมิติอวกาศ (Space Domain) เพื่อให้เกิดการทวีกำลังกองทัพอากาศ (Force Multiplier) อย่างเป็นรูปธรรม อนึ่ง การปฏิบัติการไซเบอร์ของกองทัพอากาศ เป็นการปฏิบัติการเพื่อการรักษาความลับของข้อมูล (Confidentiality) ซึ่งหมายถึงการรับประกันถึงความปลอดภัยของข้อมูลในระบบว่าผู้ที่ไม่มีส่วนเกี่ยวข้องหรือไม่มีสิทธิ์จะไม่สามารถเข้าถึงเนื้อหาของข้อมูลได้ ควบคู่ไปกับการรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) ซึ่งหมายถึงการยืนยันถึงความถูกต้องครบถ้วนของข้อมูลที่มีการรับส่งในระบบว่าจะไม่ถูกเปลี่ยนแปลงหรือแก้ไข ตลอดจนการดำรงความพร้อมใช้งานของระบบ และข้อมูลสารสนเทศ (Availability) ซึ่งหมายถึงการรับประกันความพร้อมในการใช้งานอุปกรณ์เครือข่ายสารสนเทศและการสื่อสาร รวมทั้งความพร้อมในการใช้งานข้อมูลและบริการประเภทต่าง ๆ ในระบบ ทุกครั้งที่มีความต้องการใช้งาน โดยปฏิบัติการไซเบอร์ของกองทัพอากาศประกอบด้วย ปฏิบัติการหลักทางไซเบอร์ และปฏิบัติการสนับสนุนทางไซเบอร์ ดังนี้

๒.๒.๑.๕ (๑) การปฏิบัติการหลักทางไซเบอร์ เป็นการปฏิบัติการที่ใช้ขีดความสามารถทางไซเบอร์ทั้งมวล เพื่อให้บรรลุวัตถุประสงค์ในมิติไซเบอร์ กำหนดกิจเฉพาะสำคัญดังนี้

- การปฏิบัติการไซเบอร์เชิงป้องกัน (Defensive Cyber Operations : DCO) เป็นปฏิบัติการเพื่อการป้องกันทางไซเบอร์ มีขั้นตอนการปฏิบัติตามวงรอบการ

ป้องกันทางไซเบอร์ (Defense Cycle) จำนวน ๔ ขั้นตอนคือ การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (React) และการฟื้นฟู (Recovery)

- การปฏิบัติการไซเบอร์เชิงป้องปราม (Offensive Cyber Operations: OCO) เป็นปฏิบัติการเพื่อการโจมตีทางไซเบอร์ มีขั้นตอนการปฏิบัติตามวงรอบการโจมตีทางไซเบอร์ (Attack Cycle) จำนวน ๕ ขั้นตอน คือ การรวบรวมข้อมูลเป้าหมาย (Information Gathering) การตรวจสอบหาช่องโหว่ของระบบ (Vulnerability Identification) การปฏิบัติการโจมตี (Attack) การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access) และการลบร่องรอยการโจมตี (Covering Tracks)

- การปฏิบัติการข่าวกรองทางไซเบอร์ (Cyber Intelligence: CI) เป็นการปฏิบัติการเพื่อรวบรวมข้อมูลข่าวกรองทางไซเบอร์ด้วยวิธีต่าง ๆ เช่น การรวบรวมข้อมูลข่าวกรองจากแหล่งเปิด (Open-Source Intelligence: OSINT) จากข่าวกรองทางบุคคล (Human Intelligence: HUMINT) จากข่าวกรองทางสัญญาณ (Signal Intelligence: SIGINT) จากข่าวกรองทางภาพ (Image Intelligence: IMINT) และจากข่าวกรองทางภูมิสารสนเทศเชิงพื้นที่ (Geospatial Intelligence: GEOINT) เป็นต้น โดยมีวัตถุประสงค์เพื่อรวบรวมและวิเคราะห์แนวโน้มเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ และ การปฏิบัติการต่อต้านข่าวกรองทางไซเบอร์ เป็นการปฏิบัติการเพื่อป้องกัน ระงับยับยั้ง และลดทอนประสิทธิภาพการปฏิบัติการข่าวกรองทางไซเบอร์ ของฝ่ายตรงข้ามที่กระทำต่อฝ่ายเรา

๒.๒.๑.๕ (๒) การปฏิบัติการสนับสนุนทางไซเบอร์ เป็นการปฏิบัติการที่ใช้ขีดความสามารถด้านไซเบอร์ในการสนับสนุนภารกิจอื่น ๆ เพื่อเอื้ออำนวยให้ภารกิจนั้นสามารถดำเนินการได้อย่างมีประสิทธิภาพกำหนดกิจเฉพาะสำคัญ ดังนี้

- การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร (Military Intelligence Support: MIS) เป็นการปฏิบัติการข่าวกรองทางไซเบอร์ และการปฏิบัติการต่อต้านข่าวกรองทางไซเบอร์ ด้วยอุปกรณ์/วิธีทางไซเบอร์ วิธีวิศวกรรมสังคม (Social Engineering) และวิธีอื่น ๆ เพื่อให้ได้มาซึ่งข้อมูลข่าวสารที่จำเป็นสำหรับการสนับสนุนการปฏิบัติการทางทหารในมิติอื่น ๆ พร้อมทั้งป้องกัน ระงับยับยั้ง และลดทอนประสิทธิภาพการปฏิบัติการข่าวกรองทางไซเบอร์ ของฝ่ายตรงข้ามที่กระทำต่อฝ่ายเราโดยต้องมีความสอดประสาน (Synchronization) ระหว่างการปฏิบัติการทางทหารในมิติไซเบอร์และการปฏิบัติการทางทหารในมิติอื่น ๆ ภายใต้แผนการรบ เพื่อให้บรรลุวัตถุประสงค์ทางทหารตามที่ต้องการ ดังนั้น การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร จะต้องมีความสัมพันธ์เชิงร่วมมือกับการปฏิบัติการข่าวกรองของกรมข่าวทหารอากาศ ในลักษณะให้การสนับสนุนซึ่งกันและกันทั้งในยามปกติและยามเกิดความขัดแย้ง

- การปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร (Information Operations Support: IO Support) เป็นการปฏิบัติการไซเบอร์เชิงป้องกัน (DCO) การปฏิบัติการไซเบอร์เชิงป้องปราม (OCO) และการปฏิบัติการข่าวกรองทางไซเบอร์ การปฏิบัติการต่อต้านการข่าวกรองทางไซเบอร์ เพื่อสนับสนุนการดำรงขีดความสามารถในการปฏิบัติการข่าวสาร ในการสร้างสภาวะที่ได้เปรียบเชิงข่าวสารต่อฝ่ายตรงข้าม เช่น การสนับสนุนการปฏิบัติการลวงทางทหาร (Military Deception: MILDEC) การรักษาความปลอดภัย

ในการปฏิบัติการ (Operations Security: OPSEC) การประกันข่าวสาร(Information Assurance: IA) และการต่อต้านข่าวกรอง เป็นต้น

๒.๓ แนวความคิดการปฏิบัติการในมิติไซเบอร์กองทัพอากาศ/การปฏิบัติการที่มีเครือข่ายเป็นศูนย์กลาง (NCO)

๒.๓.๑ แนวความคิดการปฏิบัติการในมิติไซเบอร์กองทัพอากาศ มีวัตถุประสงค์เพื่อรวบรวมข้อมูล ศึกษาวิเคราะห์ความต้องการ และกำหนดแนวความคิดการปฏิบัติให้ตอบสนองความต้องการทางยุทธการได้อย่างมีประสิทธิภาพ เพื่อเป็นกรอบแนวทางในการจัดทำแผนแม่บทในมิติไซเบอร์และแนวทางการพัฒนาในมิติไซเบอร์ให้มีความสอดคล้องและเป็นไปในทิศทางเดียวกัน ตลอดจนเสริมสร้างความเข้าใจให้กับกำลังพล และหน่วยเกี่ยวข้องของกองทัพอากาศทุกระดับ ทำให้เกิดการบูรณาการร่วมกันอย่างมีประสิทธิภาพและคุ้มค่า โดยแนวความคิดการปฏิบัติการไซเบอร์แบ่งแนวความคิดออกเป็นแนวความคิด ดังนี้

๒.๓.๑.๑ แนวความคิดการเตรียมกำลัง มุ่งเน้นการพัฒนากำลังพลให้มีความรู้ ทักษะและประสบการณ์จนกระทั่งมีความเชี่ยวชาญในการปฏิบัติการทางไซเบอร์ทุกรูปแบบ ด้วยการส่งเข้าศึกษาในสถาบันด้านไซเบอร์ จัดการฝึกทดสอบและแข่งขันด้านไซเบอร์ จัดเข้าฝึกร่วม/ผสมในภารกิจต่าง ๆ ของกองทัพ นอกจากนั้นยังมุ่งเน้นการพัฒนาอุปกรณ์ เครื่องมือที่จะนำมาใช้ในการปฏิบัติการให้มีความทันสมัย ใช้ร่วมกับเทคโนโลยีปัจจุบันได้อย่างมีประสิทธิภาพ พร้อมกับการจัดทำและปรับปรุงระเบียบคู่มือการปฏิบัติต่าง ๆ ให้ทันสมัยได้มาตรฐาน แบ่งออกเป็น ๓ ด้าน ดังนี้

๒.๓.๑.๑ (๑) ด้านนโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง เพื่อให้เป็นกรอบในการปฏิบัติ ทำให้การปฏิบัติเป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ

๒.๓.๑.๑ (๒) ด้านอุปกรณ์ เครื่องมือ และเทคโนโลยี จัดให้มีอุปกรณ์เครื่องมือ โดยมีเทคโนโลยีที่ทันสมัย เพื่อการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์และสารสนเทศของกองทัพอากาศ สำหรับการปฏิบัติการในมิติไซเบอร์เชิงป้องกันและการปฏิบัติการในมิติไซเบอร์เชิงป้องปราม ให้มีความทันสมัย ครอบคลุม และเพียงพอต่อความต้องการใช้งานเพื่อการรักษาความปลอดภัยระบบสารสนเทศด้านยุทธการและด้านการสนับสนุนของกองทัพอากาศ พร้อมทั้งสามารถให้การสนับสนุนแก่หน่วยงานที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

๒.๓.๑.๑ (๓) ด้านกำลังพล เป็นการเตรียมความพร้อมด้านกำลังพลของกองทัพอากาศ สำหรับการปฏิบัติการในมิติไซเบอร์เชิงป้องกัน และปฏิบัติการในมิติไซเบอร์เชิงป้องปราม

๒.๓.๑.๒ แนวความคิดการใช้กำลังในมิติไซเบอร์ เป็นการเสนอแนะแนวทางการใช้กำลังสำหรับการปฏิบัติการเชิงป้องกันเป็นหลัก เพื่อปกป้องระบบสารสนเทศทั้งมวลของกองทัพอากาศให้มีความปลอดภัย และให้พร้อมใช้งานอยู่เสมอ พร้อมทั้งแนวทางการใช้กำลังสำหรับการปฏิบัติการเชิงป้องปราม เพื่อตอบสนองต่อวัตถุประสงค์ทางทหารที่ต้องการ แบ่งออกเป็น ๕ ประเภท ดังนี้

๒.๓.๑.๒ (๑) การปฏิบัติการเชิงป้องกันและป้องปราม แบ่งออกเป็นการปฏิบัติการป้องกันเชิงรุก (Proactive Defense Operations) และการปฏิบัติการป้องกันเชิงรับ

(Passive Defense Operations) เพื่อป้องกันและตอบสนองต่อภัยคุกคามทุกรูปแบบ ได้แก่ การบุกรุก การโจมตี การทำลาย และการจารกรรมข้อมูลทั้งจากภายนอกและภายในระบบเครือข่ายของกองทัพอากาศ

๒.๓.๑.๒ (๒) การปฏิบัติการเพื่อรักษาความปลอดภัยระบบเครือข่ายสารสนเทศที่เชื่อมต่อกับเครือข่ายของกองทัพอากาศ มุ่งเน้นไปที่การรักษาความมั่นคงปลอดภัยระบบสารสนเทศด้านยุทธการ (CIS) และระบบสารสนเทศด้านการสนับสนุน (SIS) ของกองทัพอากาศ

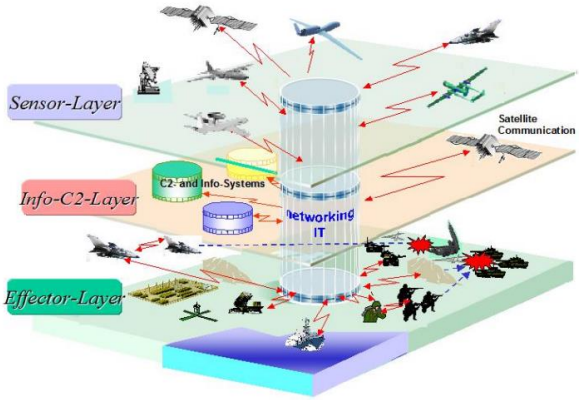
๒.๓.๑.๒ (๓) การปฏิบัติการเพื่อการใช้งานระบบสารสนเทศประจำวัน โดยทั่วไปแล้วกำลังพลกองทัพอากาศใช้งานด้านไซเบอร์ส่วนใหญ่จะเป็นลักษณะของการใช้งานระบบสารสนเทศประจำวัน เช่น การรับส่งอีเมล การเข้าชมเว็บไซต์ การติดต่อสื่อสารผ่านแอปพลิเคชันแบบออนไลน์การใช้งานอินเทอร์เน็ตประกอบการทำงาน และการปฏิบัติงานที่เกี่ยวกับเอกสารอิเล็กทรอนิกส์ผ่านมิติไซเบอร์ เป็นต้น ซึ่งผู้ใช้งานทั่วไปไม่ได้รับสิทธิในการเชื่อมต่อกับระบบสำคัญหรือไม่ได้รับสิทธิการใช้งานในระดับผู้ดูแลระบบ แต่การใช้งานระบบสารสนเทศประจำวันในลักษณะนี้มีโอกาสก่อให้เกิดช่องโหว่ที่ผู้ไม่ประสงค์ดีสามารถใช้ในการเข้าถึงและโจมตีระบบเครือข่ายของกองทัพอากาศได้

๒.๓.๑.๒ (๔) การปฏิบัติการเพื่อสนับสนุนการปฏิบัติการข่าวกรอง การปฏิบัติการข่าวกรองของกองทัพอากาศ เป็นการปฏิบัติของกรมข่าวทหารอากาศเพื่อสนับสนุนแผนและการปฏิบัติการใช้กำลังทางอากาศในมิติทางกายภาพ โดยมีวิธีต่าง ๆ เช่น ข่าวกรองทางบุคคล (Human Intelligence: HUMINT) ข่าวกรองทางสัญญาณ (Signals Intelligence: SIGINT) และข่าวกรองทางภาพ (Imagery Intelligence: IMINT) เป็นต้น

๒.๓.๑.๒ (๕) การปฏิบัติการเพื่อสนับสนุนการปฏิบัติการข่าวสาร โดยให้ความสำคัญกับระบบสารสนเทศด้านยุทธการเป็นหลัก และระบบสารสนเทศด้านการสนับสนุนเป็นรองการปฏิบัติการในมิติไซเบอร์ สามารถใช้ในการสนับสนุนการดำรงขีดความสามารถในการปฏิบัติการข่าวสาร เพื่อสร้างสภาวะที่ได้เปรียบต่อฝ่ายตรงข้าม โดยสนับสนุนการปฏิบัติการลวงทางทหาร การรักษาความปลอดภัยในการปฏิบัติการ (Operations Security: OPSEC) การประกันข่าวสาร (Information Assurance: IA) และการปฏิบัติการต่อต้านข่าวกรอง

๒.๓.๒ การปฏิบัติการที่มีเครือข่ายเป็นศูนย์กลาง (NCO) การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) เป็นการปฏิบัติการทางทหารด้วยเทคโนโลยีที่มีความทันสมัย ประกอบไปด้วย ๖ องค์ประกอบ ได้แก่ การบัญชาการและควบคุม (Command and Control: C2) ระบบตรวจจับ (Sensor) ผู้ปฏิบัติและหน่วยปฏิบัติ (Shooter) ระบบเครือข่าย (Network) การสนับสนุนและบริการ (Support and Service) บุคลากรและพฤติกรรมการปฏิบัติงาน (Human and Behavior) ซึ่งสามารถแสวงหาข้อมูลข่าวสารแบบเบ็ดเสร็จ และบูรณาการส่งไปยังระบบบัญชาการและควบคุมก่อให้เกิดการตัดสินตกลงใจของผู้บังคับบัญชาแบบชาญฉลาด และมอบคำสั่งการไปยังหน่วยรบให้ปฏิบัติภารกิจ ถูกที่ ถูกเวลา และถูกเป้าหมาย โดยการใช้เครือข่ายเป็นศูนย์กลางในการแลกเปลี่ยนและรับส่งข้อมูลจากทุกภาคส่วนทำให้ฝ่ายเราสามารถสร้างความได้เปรียบด้านข้อมูลข่าวสาร (Information Advantage) สามารถรวบรวมข้อมูลข่าวสารที่มีความเป็นเลิศ (Information Superiority) และนำข้อมูลข่าวสารมาวิเคราะห์เป็นข่าวกรองได้อย่างบูรณาการและเป็นรูปธรรม

ทำให้ผู้ที่มีอำนาจตัดสินตกลงใจ สามารถรับรู้ในสถานการณ์ วิเคราะห์สถานการณ์ ทำความเข้าใจกับสถานการณ์ และตัดสินใจใช้กำลังได้อย่างชาญฉลาด



ภาพที่ ๒.๒ ภาพแสดงการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations: NCO)

การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations: NCO) เป็นแนวคิดที่ถูกพัฒนาขึ้นเพื่อตอบสนองทฤษฎีการสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare: NCW) เป็นการประยุกต์ใช้ความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสาร สนับสนุนให้เกิดการแลกเปลี่ยนข้อมูลระหว่าง Sensor Layer, Info-C2 Layer และ Effector Layer โดยใช้เครือข่ายเป็นศูนย์กลาง ทั้งภายในและระหว่างหน่วยทหารทั้งระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ เพื่อให้ข้อมูล ข่าวสาร ภาพสถานการณ์ และคำสั่งผ่านการสื่อสารได้อย่างถูกต้อง รวดเร็ว แม่นยำและทั่วถึงทำให้ผู้บังคับบัญชาสามารถตัดสินสั่งการไปยังผู้ปฏิบัติได้อย่างถูกตอง และทันต่อสถานการณ อันจะก่อให้เกิดความได้เปรียบในการทำสงคราม ซึ่งความได้เปรียบที่กล่าวมานั้น เกิดจากความกาวหน้าในเทคโนโลยีเครื่องมือสื่อสารต่าง ๆ รวมทั้งความก้าวหน้าของเทคโนโลยีเครือข่ายที่ทำให้การเชื่อมต่อ และการสื่อสารระหว่างชั้นต่าง ๆ เป็นไปอย่างมีประสิทธิภาพ รวมทั้งก่อให้เกิดความเหนือกว่าในด้านการบัญชาการและควบคุมต่อข้าศึก

โดยแนวความคิดในการเตรียมการใช้กำลังด้านไซเบอร์ ด้านอุปกรณ์ เครื่องมือ และเทคโนโลยีกำหนดให้ จัดให้มีระบบตรวจพิสูจน์ตัวตนของผู้ใช้งานแบบหลายองค์ประกอบ (Multi-Factor User Authentication) ซึ่งใช้ในการพิสูจน์เพื่อยืนยันตัวตนของผู้ใช้งานในการเข้าใช้งานระบบสารสนเทศ โดยเฉพาะระบบสารสนเทศด้านยุทธการที่ติดตั้งในอาคารปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCOC) ด้วยการใช้ปัจจัยพิสูจน์ยืนยันอื่นเพิ่มเติมจากรหัสผ่าน (Password) ปกติ เช่น การใช้อุปกรณ์โทเค็น (Token) และการใช้ปัจจัยทางกายภาพของบุคคล (Biometric) เป็นต้น ประกอบในการพิสูจน์ยืนยันตัวตนผู้ใช้งาน ทั้งนี้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ซึ่งต้องมีความสอดประสาน (Synchronization) ระหว่างการปฏิบัติการทางทหารในมิติไซเบอร์และการปฏิบัติการใช้กำลังทางอากาศภายใต้แผนการรบ เพื่อให้บรรลุวัตถุประสงค์ทางทหารตามที่ต้องการ ดังนั้น การปฏิบัติการข้อมูลข่าวกรองในมิติไซเบอร์จึงต้องมีความสัมพันธ์เชิงร่วมมือกับการปฏิบัติการข้อมูลข่าวกรองของกรมข่าวทหารอากาศ ในลักษณะให้การสนับสนุนซึ่งกันและกัน ทั้งในยามปกติและยามเกิดความขัดแย้ง โดยมีหน่วยเกี่ยวข้องดังนี้

กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ ให้การสนับสนุนการได้มาซึ่งข้อมูลข่าวสารที่มีความสำคัญและเป็นประโยชน์หรือมีความจำเป็นต่อการวางแผน และการปฏิบัติการทางทหารในมิติทางกายภาพ ด้วยการใช้ขีดความสามารถทางไซเบอร์ (อุปกรณ์ เครื่องมือ และวิธีการทางไซเบอร์) ในการเก็บรวบรวมเพื่อส่งให้สำนักข่าวกรอง กรมข่าวทหารอากาศ นำไปวิเคราะห์ใช้งาน

สำนักข่าวกรอง กรมข่าวทหารอากาศ ให้การสนับสนุนการได้มาซึ่งข้อมูลข่าวสารที่มีความสำคัญและเป็นประโยชน์หรือมีความจำเป็นต่อการวางแผนและการปฏิบัติการทางทหารในมิติไซเบอร์ด้วยการใช้ขีดความสามารถทางการข่าวกรอง (เช่น HUMINT, SIGINT และ IMINT เป็นต้น) ในการเก็บรวบรวมเพื่อส่งให้กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ นำไปวิเคราะห์และใช้งาน

๒.๓.๒.๑ ความสัมพันธ์ระหว่างการปฏิบัติงานในมิติไซเบอร์ กับการปฏิบัติการที่มีเครือข่ายเป็นศูนย์กลาง โดยในส่วนของมิติไซเบอร์ มีรายละเอียด ดังนี้

๒.๓.๒.๑ (๑) Sensor ทางไซเบอร์ มีศูนย์ปฏิบัติการทางไซเบอร์ (Cyber Security Operations Center: CSOC) ศูนย์ไซเบอร์กองทัพอากาศ ใช้เครื่องมือที่ใช้เฝ้าระวังเหตุและป้องกันภัยทางไซเบอร์ เพื่อเฝ้าระวังป้องกันภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดภายในระบบเครือข่าย และอุปกรณ์ในส่วนเกี่ยวข้องทางไซเบอร์ โดยมีแผนกเฝ้าระวังและตรวจจับ และแผนกตอบสนองภัยคุกคาม กองรักษาความมั่นคงปลอดภัยไซเบอร์รับผิดชอบ

๒.๓.๒.๑ (๒) Info - C2 ทางไซเบอร์ มีกรมข่าวทหารอากาศรับผิดชอบ โดยใช้ขีดความสามารถทางการข่าวกรอง (HUINT, SIGINT และ IMINT) ทำงานบูรณาการร่วมกับการข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligent: CTI) ของศูนย์ไซเบอร์กองทัพอากาศ เพื่อใช้วิเคราะห์และให้ผู้บังคับบัญชาของศูนย์ยุทธการ/ศูนย์ปฏิบัติการกองทัพอากาศ พิจารณา เพื่อวางแผนและดำเนินการทางด้านยุทธการทางไซเบอร์ต่อไป โดยมีกองปฏิบัติการไซเบอร์รับผิดชอบ

๒.๓.๒.๑ (๓) Effector-Layer ทางไซเบอร์ มีกองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ รับผิดชอบให้การปฏิบัติการด้านการยับยั้งภัยคุกคามทางไซเบอร์บูรณาการกับหน่วยที่เกี่ยวข้อง เช่น กองบัญชาการควบคุมการปฏิบัติทางอากาศ, กรมข่าวทหารอากาศ, ศูนย์คอมพิวเตอร์ กรมสื่อสารทหารอากาศ และกองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ปฏิบัติการทางยุทธการทางไซเบอร์ เป็นต้น

๒.๔ ระบบสารสนเทศและเครือข่ายกองทัพอากาศ และทรัพย์สินทางไซเบอร์

ระบบเครือข่ายคอมพิวเตอร์ที่เป็นโครงสร้างพื้นฐานในเขตที่ตั้งดอนเมือง และนอกที่ตั้งดอนเมือง ระบบโทรคมนาคม และระบบสารสนเทศของกองทัพอากาศ โดยระบบสารสนเทศแบ่งออกเป็น ๒ ส่วน ได้แก่ ระบบสารสนเทศด้านยุทธการ (Combat Information System: CIS) และระบบสารสนเทศด้านการสนับสนุน (Support Information System: SIS) ดังนี้

๒.๔.๑ ระบบเครือข่ายคอมพิวเตอร์ แบ่งออกเป็น ๒ ส่วน ดังนี้

๒.๔.๑.๑ ระบบเครือข่ายคอมพิวเตอร์ระยะไกล (Wide Area Network: WAN)

๒.๔.๑.๒ ระบบเครือข่ายคอมพิวเตอร์ภายใน (Local Area Network: LAN)

๒.๔.๒ ระบบสารสนเทศ แบ่งออกเป็น ๒ ส่วน ตามแผนเฉลิมอากาศ ดังนี้

๒.๔.๒.๑ ระบบสารสนเทศด้านยุทธการ (CIS)

๒.๔.๒.๒ ระบบสารสนเทศด้านการสนับสนุน (SIS)

๒.๔.๓ ทรัพย์สินทางไซเบอร์ แบ่งได้เป็น ๒ ส่วน ดังนี้

๒.๔.๓.๑ ทรัพย์สินประเภทฮาร์ดแวร์ และซอฟต์แวร์ โดยมีทรัพย์สินที่เป็นเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) และเครื่องคอมพิวเตอร์โน้ตบุ๊ก (Notebook) รวมถึงซอฟต์แวร์ที่ใช้ในงานสำนักงานภายในศูนย์ไซเบอร์กองทัพอากาศ

๒.๔.๓.๒ ทรัพย์สินประเภทอุปกรณ์เครือข่าย เป็นทรัพย์สินทางด้านอุปกรณ์เครือข่าย รวมถึงอุปกรณ์ที่ทำหน้าที่ทำหน้าที่ตรวจสอบข้อมูลที่ผ่านเข้า-ออกระบบเครือข่าย ตัวอย่างเช่น คอมพิวเตอร์เซิร์ฟเวอร์ (Server), ไฟร์วอลล์ (Firewall), เร้าเตอร์ (Router) และ Network Switch ที่ใช้ในการสนับสนุนภารกิจของศูนย์ไซเบอร์กองทัพอากาศ เป็นต้น

๒.๕ กฎหมาย ระเบียบ และการกำหนดมาตรฐานทางไซเบอร์

๒.๕.๑ กฎหมาย ระเบียบ ทางไซเบอร์ มีวัตถุประสงค์เพื่อกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญ ต้องมีการจัดเตรียมการและปฏิบัติตามกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสามารถรับมือและลดความเสี่ยงจากภัยคุกคามที่อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ โดยมีรายละเอียด ดังนี้

๒.๕.๑.๑ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ (ฉบับแก้ไขเพิ่มเติม) ทำหน้าที่ เป็นกฎหมายกลางที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ให้มีผลผูกพันและใช้บังคับได้ตามกฎหมายโดยหลักการพื้นฐานของ พ.ร.บ.ธุรกรรมฯ โดยมีหลักการคือ

๒.๕.๑.๑ (๑) หลักความเท่าเทียมกัน (Functional Equivalence) ระหว่างกระดาษ และข้อมูลอิเล็กทรอนิกส์ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ มีผลทางกฎหมายเทียบเท่าการใช้กระดาษ

๒.๕.๑.๑ (๒) หลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality) ที่ไม่ระบุเฉพาะเจาะจงเทคโนโลยีใดเทคโนโลยีหนึ่ง แต่รองรับพัฒนาการของเทคโนโลยีที่จะเกิดขึ้นในอนาคต

๒.๕.๑.๑ (๓) หลักเสรีภาพการแสดงเจตนา (Party Autonomy) ของคู่สัญญา

ทั้งนี้ ภายใต้กฎหมายธุรกรรมฯ ได้มีหลักเกณฑ์รองรับการทำธุรกรรมทางอิเล็กทรอนิกส์ในกระบวนการต่าง ๆ ที่สำคัญ เช่น หากเกิดคดีความฟ้องร้องแล้วมีการขอหลักฐานต้นฉบับกฎหมายจะระบุไว้ว่า ข้อมูลอิเล็กทรอนิกส์ที่เป็นต้นฉบับต้องเป็นอย่างไร หรือในกรณีที่บางหน่วยงานมีข้อบังคับเรื่องการจัดเก็บเอกสารบางประเภทเป็นเวลาหลายปี กฎหมายจะระบุว่า วิธีการจัดเก็บเอกสารอิเล็กทรอนิกส์ที่เป็นที่ยอมรับตามกฎหมายเป็นอย่างไร เป็นต้น โดยแนวทางการใช้กฎหมายเพื่อเสริมกฎหมายอื่นให้ทำแบบอิเล็กทรอนิกส์ได้ โดยไม่แทนที่หรือมีผลไปยกเว้นหรือเปลี่ยนแปลง

เกณฑ์ตามกฎหมายเดิม ดังตัวอย่าง การปรับใช้กับประมวลกฎหมายแพ่งและพาณิชย์ มาตรา ๔๕๖ ได้แก่ สัญญาซื้อขายสังหาริมทรัพย์ราคาตั้งแต่ ๒๐,๐๐๐ บาท ที่กฎหมายกำหนดว่าต้องมี หลักฐานเป็นหนังสือ และ ลงลายมือชื่อฝ่ายที่ต้องรับผิดเป็นสำคัญ ซึ่งสามารถนำ พ.ร.บ.ธุรกรรมฯ มาตรา ๘ เรื่องเอกสารอิเล็กทรอนิกส์ และมาตรา ๙ เรื่องลายมือชื่ออิเล็กทรอนิกส์ มาปรับใช้ได้กับการทำแบบของสัญญาซื้อขายสังหาริมทรัพย์แบบอิเล็กทรอนิกส์ได้ โดยมี โครงสร้างกฎหมาย ดังนี้

หมวด ๑ ธุรกรรมทางอิเล็กทรอนิกส์ รองรับการทำธุรกรรมในรูปแบบข้อมูลอิเล็กทรอนิกส์ในเรื่องต่าง ๆ

หมวด ๒ ลายมือชื่ออิเล็กทรอนิกส์ รองรับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

หมวด ๓ ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รองรับการกำกับดูแลธุรกิจบริการที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ที่สำคัญและมีผลกระทบวงกว้าง

หมวด ๓/๑ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รองรับให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมีกลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้อง เพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและมั่นคงปลอดภัย

หมวด ๔ ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ รองรับการให้บริการภาครัฐด้วยวิธีการทางอิเล็กทรอนิกส์

หมวด ๕ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) รองรับการมีคณะกรรมการเพื่อส่งเสริมและพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ

หมวด ๖ บทกำหนดโทษ

๒.๕.๑.๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ใช้บังคับเกี่ยวกับความผิดเกี่ยวกับคอมพิวเตอร์ ผู้ให้บริการ ครอบคลุมระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และข้อมูลจราจรทางคอมพิวเตอร์

๒.๕.๑.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ เพิ่มเติมจากฉบับ พ.ศ.๒๕๕๐ โดยเกี่ยวข้องกับการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูล การจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด

๒.๕.๑.๔ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ คือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นกฎหมายที่ถูกสร้างมาเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลของทุกคน รวมถึงการจัดเก็บข้อมูลและนำไปใช้โดยไม่ได้แจ้งให้ทราบ และไม่ได้รับความยินยอมจากเจ้าของข้อมูล โดยกฎหมายนี้ได้เริ่มบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ ๑ มิ.ย.๒๕๖๕ เป็นกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ รูปถ่าย บัญชีธนาคาร อีเมล ไอดีไลน์ บัญชีผู้ใช้ของเว็บไซต์ ลายนิ้วมือ และประวัติสุขภาพ เป็นต้น ซึ่งข้อมูลเหล่านี้สามารถระบุถึงตัวเจ้าของข้อมูลนั้นได้ อาจเป็นได้ทั้งข้อมูลในรูปแบบเอกสาร กระดาษ หนังสือ หรือจัดเก็บในรูปแบบอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อให้เจ้าของข้อมูลมีสิทธิในข้อมูลส่วนตัวที่ถูกจัดเก็บไปแล้ว หรือกำลังจะถูกจัดเก็บมากขึ้น เพื่อสร้างความปลอดภัยและเป็นส่วนตัวให้แก่เจ้าของข้อมูล

๒.๕.๑.๕ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ถูกกำหนดขึ้นเพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการ

ป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ โดยกำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐมีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ รวมถึงจะต้องร่วมมือและประสานงานกันกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้ จนทำให้ประชาชนทั่วไปเดือดร้อน

๒.๕.๑.๖ ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ ความมุ่งหมายของระเบียบฯ เพื่อกำหนดหลักการ และมาตรการป้องกันระบบสารสนเทศของกองทัพอากาศเพื่อรักษาไว้ซึ่งคุณสมบัติที่มั่นคงปลอดภัยของระบบสารสนเทศ ได้แก่ การรักษาความลับ (Confidentiality) ความครบถ้วนสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมถึงการรักษาความต่อเนื่องในการดำเนินการให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศของกองทัพอากาศ

๒.๕.๒ การกำหนดมาตรฐานทางไซเบอร์ เป็นการกำหนดแนวทาง หรือหลักการในการป้องกันทรัพย์สินที่เกี่ยวข้องทางไซเบอร์และสารสนเทศให้ปลอดภัยจากภัยคุกคามที่ก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลในระบบสารสนเทศ โดยมีตัวอย่างมาตรฐานทางไซเบอร์ ดังนี้

๒.๕.๒.๑ U.S. DoD Standard เป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของระบบคอมพิวเตอร์เพื่อความมีประสิทธิภาพของอุปกรณ์ตั้งแต่ขั้นตอนแรก คือ กระบวนการประมูลจัดซื้อหรือจัดจ้างสำหรับหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางในการออกแบบ พัฒนาผลิตหรือทดสอบสำหรับผู้ผลิตเทคโนโลยี หรือภาคเอกชน

๒.๕.๒.๒ Information Technology Infrastructure Library (ITIL) เป็นแนวทางปฏิบัติที่ว่าด้วยเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เป็นมาตรฐานด้านความมั่นคงปลอดภัยจากประเทศอังกฤษ The British Office of Government Commerce (OGC) มุ่งเน้นการพัฒนากระบวนการเพื่อรองรับการให้บริการต่อลูกค้าและธุรกิจเป็นหลัก เช่น การออกแบบ การติดตั้ง การกระจาย และการดูแลรักษาและการปรับปรุง เป็นต้น ITIL เป็นแนวทางปฏิบัติที่ดีเยี่ยมในการบริหารจัดการด้าน IT Service โดยแนวทางปฏิบัตินี้เหมาะกับองค์กรไม่ว่าจะขนาดเล็กหรือใหญ่โดยเฉพาะอย่างยิ่งองค์กรที่เน้นเรื่องของการบริการด้าน IT Service

๒.๕.๒.๓ The Federal Information Processing Standards Publication 200 (FIPS PUB 200) กล่าวถึงเรื่องของข้อกำหนดขั้นต่ำสำหรับความต้องการด้านความมั่นคงปลอดภัย ซึ่งเป็นภาคบังคับขององค์กรบริหารจัดการสารสนเทศและระบบสารสนเทศกลางของประเทศสหรัฐอเมริกา ทุกองค์กรที่เป็นหน่วยงานภาครัฐจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยนี้เป็นอย่างน้อย โดยมาตรฐานนี้จะมีการระบุประเภทของระบบสารสนเทศต่าง ๆ และวิธีปฏิบัติที่จำเป็นสำหรับควบคุม เพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศในระบบนั้น ๆ โดยมีเนื้อหาโดยสรุปของมาตรฐาน ได้แก่

๒.๕.๒.๓ (๑) การระบุข้อกำหนดขั้นต่ำ ของระบบประมวลผลสารสนเทศขององค์กรกลางในประเทศสหรัฐอเมริกา

๒.๕.๒.๓ (๒) การจัดทำข้อกำหนดนี้เพื่อสนับสนุนการพัฒนา

๒.๕.๒.๓ (๓) การลงมือปฏิบัติ

๒.๕.๒.๓ (๔) การดำเนินการ เพื่อสร้างความมั่นคงปลอดภัยระบบสารสนเทศ โดยหน่วยงานสามารถคัดเลือกเฉพาะส่วนที่เกี่ยวข้องกับองค์กรของตนมาปฏิบัติตาม มาตรฐานนี้จึงได้มีการจัดทำ แนวทางในการคัดเลือก และกำหนดมาตรการด้านความมั่นคงปลอดภัยที่จำเป็นและเหมาะสมสำหรับระบบประมวลผลสารสนเทศของแต่ละหน่วยงาน

๒.๕.๒.๔ NIST Framework หรือ National Institute for Standards and Technology (NIST) เป็นองค์กรภายในกระทรวงพาณิชย์ของสหรัฐอเมริกาที่มีหน้าที่ส่งเสริมนวัตกรรมและความสามารถในการแข่งขันทางอุตสาหกรรม ส่วนหนึ่งของภารกิจนี้ NIST พัฒนาและเผยแพร่มาตรฐานและแนวทางที่มุ่งปรับปรุงแนวทางปฏิบัติ โดยหัวใจสำคัญของ NIST Framework คือ

๒.๕.๒.๔ (๑) การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)

๒.๕.๒.๔ (๒) การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร (Protect)

๒.๕.๒.๔ (๓) การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ (Detect)

๒.๕.๒.๔ (๔) การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น (Respond)

๒.๕.๒.๔ (๕) การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม (Recovery)

ภาพที่ ๒.๓ ภาพแสดงวงจร ๕ ฟังก์ชันหลักของ NIST Framework

๒.๕.๒.๕ ISO 27001:2013 มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS) โดยมาตรฐานนี้เป็นต้นแบบสำหรับการประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึง

การบริหารจัดการความปลอดภัยมาตรฐาน ISO 27001 ได้ระบุแนวทางการดำเนินงานและการบริหารจัดการที่จะช่วยในการเก็บรักษาข้อมูลทั้งเป็นดิจิตอลและเอกสารของได้อย่างปลอดภัย โดยมีหัวข้อสำคัญในมาตรฐานนี้จำนวน ๑๔ หัวข้อ ดังนี้

๒.๕.๒.๕ (๑) นโยบายความมั่นคงปลอดภัยสารสนเทศ

๒.๕.๒.๕ (๒) โครงสร้างความมั่นคงปลอดภัยสารสนเทศขององคกร

๒.๕.๒.๕ (๓) ความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวของกับพนักงาน

๒.๕.๒.๕ (๔) การบริหารจัดการทรัพย์สิน

๒.๕.๒.๕ (๕) การควบคุมการเขาถึง

๒.๕.๒.๕ (๖) การเข้ารหัสข้อมูล

๒.๕.๒.๕ (๗) ความมั่นคงปลอดภัยสารสนเทศทางกายภาพและสิ่งแวดล่อม

๒.๕.๒.๕ (๘) การรักษาความมั่นคงปลอดภัยสารสนเทศด้านการดำเนินการ

๒.๕.๒.๕ (๙) ความมั่นคงปลอดภัยทางด้านการสื่อสาร

๒.๕.๒.๕ (๑๐) การจัดหา การพัฒนา และการบำรุงรักษาระบบ

๒.๕.๒.๕ (๑๑) ความสัมพันธ์กับผู้ใหบริการภายนอก

๒.๕.๒.๕ (๑๒) การบริหารจัดการเหตุการณความมั่นคงปลอดภัยสนเทศ

๒.๕.๒.๕ (๑๓) ดานความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ

๒.๕.๒.๕ (๑๔) การปฏิบัติตามขอกำหนด

โดยมาตรฐานนี้ได้ถูกจัดทำขึ้นโดยยึดตามแนวคิดของหลักการ PDCA (Plan-Do-Check-Act) เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบ และมีการพัฒนาขึ้นอย่างต่อเนื่อง เริ่มต้นตั้งแต่การจัดตั้ง การนำระบบไปใช้ การดำเนินงาน การติดตามและวัดผล การทบทวน การบำรุงรักษาระบบ และการปรับปรุงพัฒนาระบบให้ดียิ่งขึ้น

๒.๕.๒.๖ Information Technology Baseline Protection Manual (IT BPM) เป็นการรักษาความมั่นคงปลอดภัยระบบอย่างมีมาตรฐาน โดยจะจัดทำเฉพาะระบบสารสนเทศที่มีใช้ในองค์กรทั่วไป อาทิระบบสารสนเทศเกี่ยวกับบุคลากรขององค์กร ระบบสารสนเทศสำหรับสื่อสารด้วยไปรษณีย์อิเล็กทรอนิกส์เป็นต้น ซึ่งเนื้อหา IT BPM ประกอบด้วย

๒.๕.๒.๖ (๑) ระบบต้องมีการบริหารจัดการด้านความมั่นคงปลอดภัยตั้งแต่ขั้นการออกแบบ ประสานงานและติดตามสถานะของความมั่นคงปลอดภัยของระบบที่เกี่ยวกับหน้าที่งานนั้น

๒.๕.๒.๖ (๒) ระบบต้องมีการวิเคราะห์และจัดทำ เป็นเอกสารเกี่ยวกับโครงสร้างที่มีอยู่ของทรัพย์สินที่เป็นเทคโนโลยีสารสนเทศในองค์กร

๒.๕.๒.๖ (๓) ระบบต้องได้รับการประเมินถึงมาตรการและระบบบริหารจัดการด้านความมั่นคงปลอดภัยเดิม ที่ได้จัดทำไว้แล้วนั้น ว่ามีประสิทธิภาพเพียงพอและเหมาะสมแล้วหรือยัง

๒.๕.๒.๖ (๔) องค์กรต่าง ๆ สามารถนำโครงสร้างของเครือข่ายที่มีความมั่นคงปลอดภัย ซึ่งได้ออกแบบไว้เหมาะสมแล้วตามคู่มือนี้มาเป็นแนวทางในการจัดทำเครือข่ายขององค์กร

๒.๕.๒.๖ (๕) ระบบต้องได้รับการดำเนินการปรับปรุงแก้ไขกรณีที่พบว่ามาตรการหรือแนวทางการรักษา ความมั่นคงปลอดภัยเหล่านั้นไม่เพียงพอ หรือมีการดำเนินการบางอย่างที่ยังไม่รัดกุม

๒.๕.๖.๗ Control Objective for Information and related Technology (COBIT) เป็นทั้งแนวคิดและแนวทางการปฏิบัติเพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่าง ๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดีซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของมาตรฐาน COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจแบ่งได้เป็น 4 กระบวนการหลัก ได้แก่

๒.๕.๖.๗ (๑) การวางแผนและการจัดการองค์กร

๒.๕.๖.๗ (๒) การจัดหาและติดตั้ง

๒.๕.๖.๗ (๓) การส่งมอบและบำรุงรักษา

๒.๕.๖.๗ (๔) การติดตามผล

๒.๕.๖.๘ The Committee of Sponsoring of the Treadway Commission (COSO) เป็นกรอบปฏิบัติที่ช่วยส่งเสริมให้การตรวจสอบกิจการภายในองค์กรมีความเที่ยงตรงและโปร่งใส โดยเฉพาะองค์กรทางด้านการเงิน เพื่อให้เกิดความน่าเชื่อถือ ความถูกต้องเป็นไปตามหลักความเป็นจริง โดย COSO มีองค์ประกอบ ๕ องค์ประกอบหลัก ดังนี้

๒.๕.๖.๘ (๑) การควบคุมสภาพแวดล้อม

๒.๕.๖.๘ (๒) การประเมินความเสี่ยง

๒.๕.๖.๘ (๓) การควบคุมการดำเนินงานหรือกิจกรรมต่าง ๆ

๒.๕.๖.๘ (๔) เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๕.๖.๘ (๕) การติดตามผล

บทที่ ๓ การจัดหน่วยปฏิบัติด้านไซเบอร์ในการเตรียมกำลัง/ใช้กำลัง

๓.๑ ภารกิจและโครงสร้างการจัดศูนย์ไซเบอร์กองทัพอากาศ และหน่วยเกี่ยวข้อง

๓.๑.๑ ศูนย์ไซเบอร์กองทัพอากาศ (ศซบ.ทอ.) ก่อตั้งเป็นหน่วยงานเพื่อพลางเมื่อ ๑ เม.ย.๖๒ และได้รับอนุมัติเป็นหน่วยขึ้นตรงกองทัพอากาศเมื่อ ๑ ต.ค.๖๒ เพื่อรองรับหลักนิยมกองทัพอากาศในการปฏิบัติการไซเบอร์

ตามอนุมัติ ผบ.ทอ. เมื่อ ๕ ส.ค.๖๔ ท้ายหนังสือ ยก.ทอ. ที่ กห ๐๖๐๖.๓/๓๕๖ ลง ๓๐ ก.ค.๖๔ เรื่อง การแก้ไขอัตรา ทอ.๕๒ กำหนด อฉก.หมายเลข ๑๑๕๑ ให้ ศูนย์ไซเบอร์กองทัพอากาศ (ศซบ.ทอ.) เป็นส่วนราชการขึ้นตรงกองทัพอากาศ ซึ่งมีภารกิจหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านไซเบอร์ของกองทัพอากาศ มีผู้อำนวยการ ศูนย์ไซเบอร์กองทัพอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

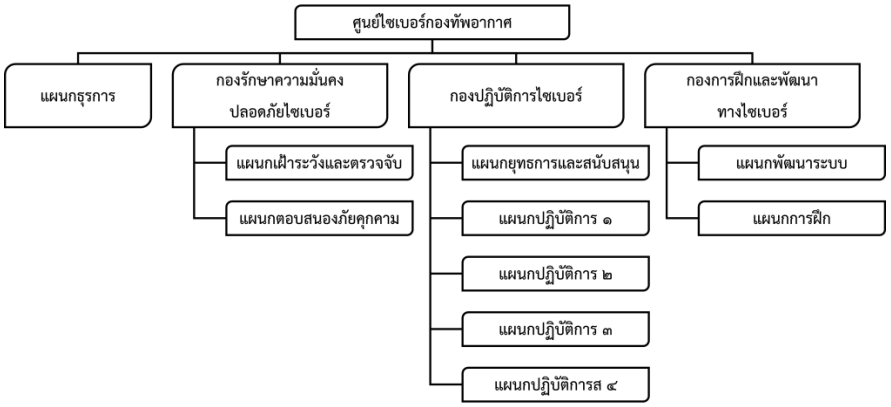
การแบ่งส่วนราชการ ศูนย์ไซเบอร์กองทัพอากาศแบ่งส่วนราชการออกเป็น

๓.๑.๑.๑ แผนกธุรการ มีหน้าที่ดำเนินการเกี่ยวกับธุรการ การสารบรรณ การพัสดุ ตลอดจนดูแลสถานที่และเครื่องมือเครื่องใช้ของศูนย์ไซเบอร์กองทัพอากาศ มีหัวหน้าแผนกธุรการเป็นผู้บังคับบัญชารับผิดชอบ

๓.๑.๑.๒ กองรักษาความมั่นคงปลอดภัยไซเบอร์ มีหน้าที่วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการเกี่ยวกับรักษาความมั่นคงปลอดภัยไซเบอร์ การเฝ้าระวังและตรวจจับ การตอบสนองภัยคุกคามทางไซเบอร์ กู้คืนระบบ และการพิสูจน์หลักฐานทางดิจิทัล มีผู้อำนวยการกอง กองรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ

๓.๑.๑.๓ กองปฏิบัติการไซเบอร์ มีหน้าที่วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการเกี่ยวกับการปฏิบัติการสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ การติดตาม รวบรวม วิเคราะห์ข่าวสารทางไซเบอร์ และการปฏิบัติการข่าวสารมีผู้อำนวยการกอง กองปฏิบัติการไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ

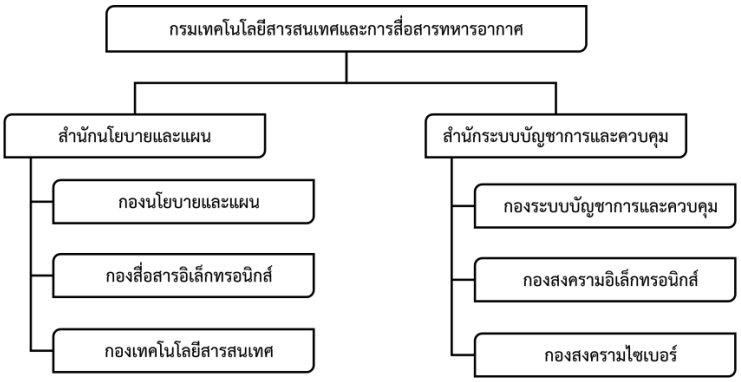
๓.๑.๑.๔ กองการฝึกและพัฒนาทางไซเบอร์ มีหน้าที่วางแผน เตรียมการประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการเกี่ยวกับการศึกษา การฝึกอบรม การวิจัยและพัฒนาด้านไซเบอร์ รวมทั้งให้การสนับสนุนการปฏิบัติการด้านไซเบอร์ มีหัวหน้ากอง กองการฝึกและพัฒนาทางไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ



ภาพที่ ๓.๑ โครงสร้างหน่วยขึ้นตรงศูนย์ไซเบอร์กองทัพอากาศ

๓.๑.๒ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) มีหน้าที่พิจารณาเสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการพัฒนาและดำเนินการด้านระบบบัญชาการและควบคุม ข่าย เครือข่ายเทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์และการสงครามอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผลและตรวจตราการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ มีเจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

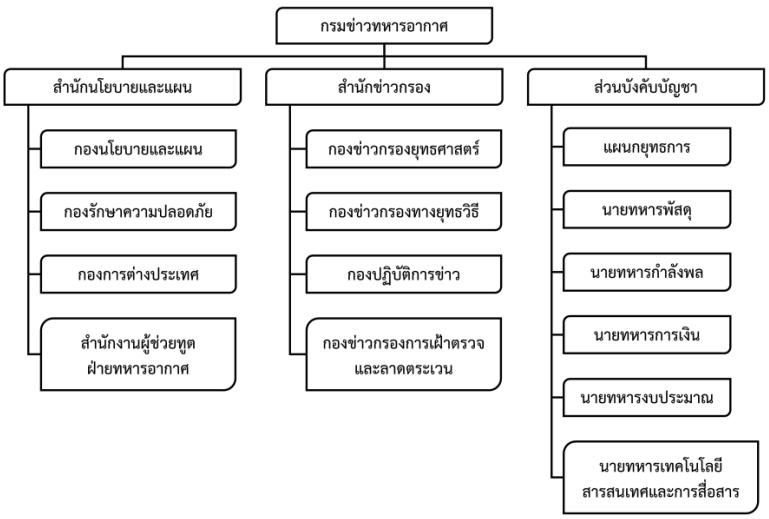
ทสส.ทอ.เป็นหน่วยงานฝ่ายอำนวยการ โดยรับผิดชอบเกี่ยวกับงานเชิงนโยบายด้านเทคโนโลยีสารสนเทศและการสื่อสาร การปฏิบัติการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ โดยมีกองสงครามไซเบอร์เป็นหน่วยงานรับผิดชอบด้านการรักษาความปลอดภัยข้อมูล ระบบสารสนเทศและการสงครามไซเบอร์



ภาพที่ ๓.๒ โครงสร้างกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๓.๑.๓ กรมข่าวทหารอากาศ (ขว.ทอ.) มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการพัฒนาและดำเนินการด้านการข่าวกรอง ต่อต้านข่าวกรอง การรักษาความปลอดภัยกิจการต่างประเทศ กับมีหน้าที่สร้างองค์ความรู้ ควบคุม ประเมินผลและการตรวจตรงกิจการในสายวิทยาการด้านการข่าวและรักษาความปลอดภัย โดยมีเจ้ากรมข่าวทหารอากาศเป็นผู้บังคับบัญชารับผิดชอบ

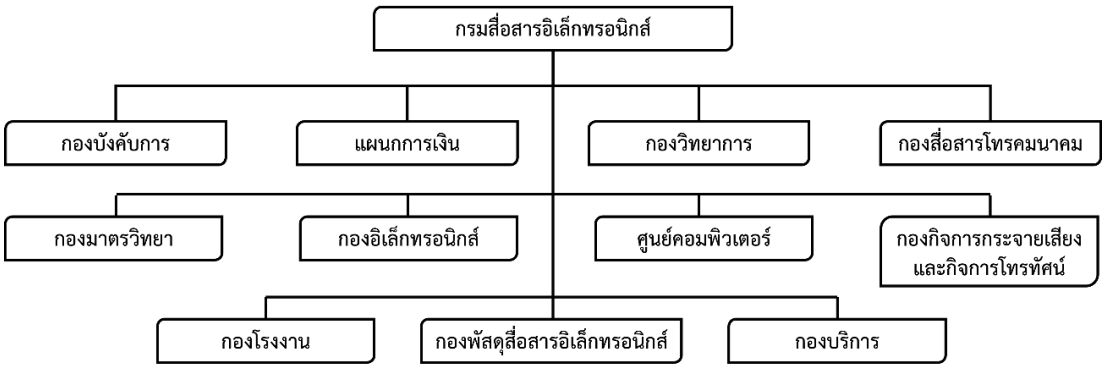
ขว.ทอ.มีหน้าที่ภารกิจด้านการปฏิบัติการข่าวกรองของกองทัพอากาศ เพื่อสนับสนุนแผนและการปฏิบัติการใช้กำลังทางอากาศในมิติกายภาพ โดยมีวิธีต่าง ๆ เช่น ข่าวกรองทางบุคคล (Human Intelligence: HUMINT) ข่าวกรองทางสัญญาณ (Signals Intelligence: SIGINT) และข่าวกรองทางภาพ (Imagery Intelligence: IMINT) โดยหน้าที่เกี่ยวข้องด้านไซเบอร์ในการสนับสนุนข้อมูลข่าวเพื่อยุทธการทางไซเบอร์



ภาพที่ ๓.๓ โครงสร้างหน่วยขึ้นตรงกรมข่าวทหารอากาศ

๓.๑.๔ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.) หน้าที่ วางแผนการปฏิบัติอำนวยการประสานงาน ติดตาม กำกับการ พัฒนา และดำเนินการเกี่ยวกับกิจการสื่อสารอิเล็กทรอนิกส์ กิจการกระจายเสียงและกิจการโทรทัศน์ มาตรวิทยา และการพัสดุสื่อสารอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุมประเมินผล และตรวจตรากิจการในสายวิทยาการสื่อสารอิเล็กทรอนิกส์ มีเจ้ากรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

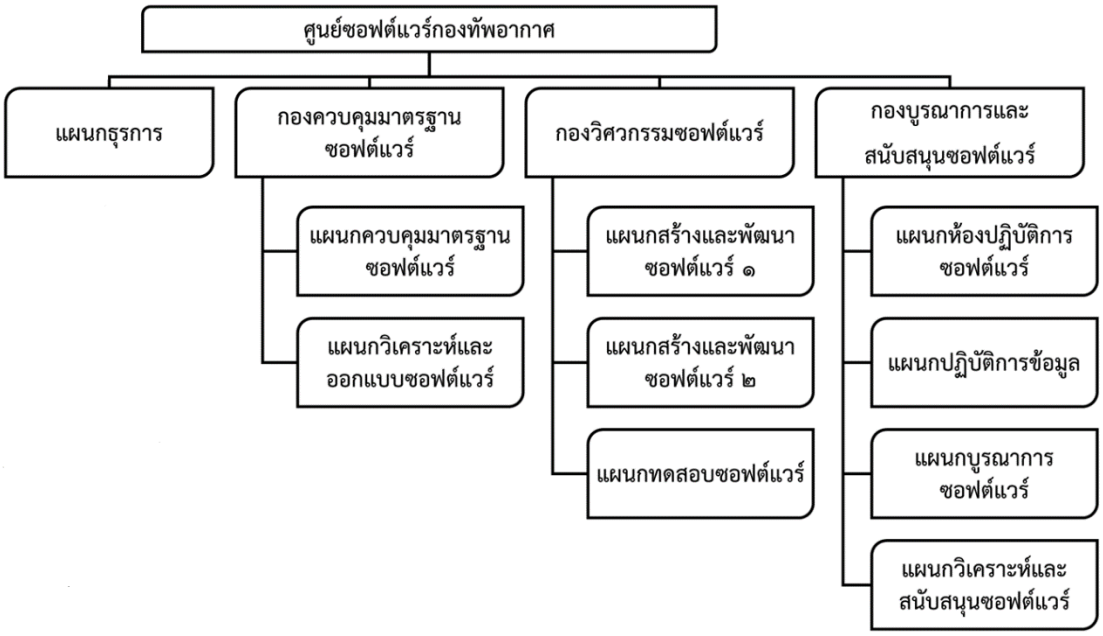
สอ.ทอ.เป็นคลังใหญ่สายสื่อสารอิเล็กทรอนิกส์ ทำหน้าที่ส่งกำลังบำรุงและซ่อมบำรุงระบบอุปกรณ์ที่เกี่ยวกับการปฏิบัติการและควบคุมสถานภาพการใช้งานด้านระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบโทรคมนาคม และการติดต่อสื่อสาร โดยมีศูนย์คอมพิวเตอร์ และกองสื่อสารโทรคมนาคม เป็นหน่วยงานรับผิดชอบ มีหน้าที่รับผิดชอบในการดูแลรักษาอุปกรณ์ และเครือข่ายที่เกี่ยวข้องด้านไซเบอร์ให้มีความพร้อมใช้งาน (Availability) ตลอดเวลา



ภาพที่ ๓.๔ โครงสร้างหน่วยขึ้นตรงกรมสื่อสารทหารอากาศ

๓.๑.๕ ศูนย์ซอฟต์แวร์กองทัพอากาศ (ศซว.ทอ.) มีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านซอฟต์แวร์ของกองทัพอากาศ มีผู้อำนวยการศูนย์ซอฟต์แวร์กองทัพอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

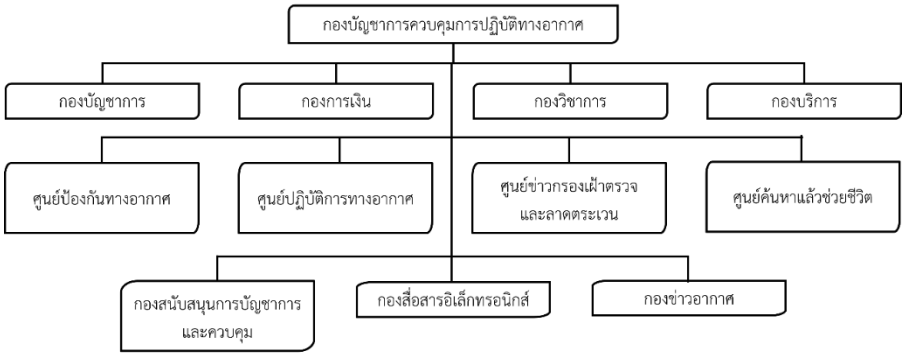
ศซว.ทอ.เป็นหน่วยฝ่ายส่งกำลังบำรุง ดำเนินการพัฒนาซอฟต์แวร์ของกองทัพอากาศให้เป็นไปตามมาตรฐาน ข้อกำหนดเพื่อป้องกันปัญหาภัยคุกคามทางไซเบอร์ในการโจมตีซอฟต์แวร์ที่ไม่ได้มาตรฐาน



ภาพที่ ๓.๕ โครงสร้างหน่วยขึ้นตรงศูนย์ซอฟต์แวร์กองทัพอากาศ

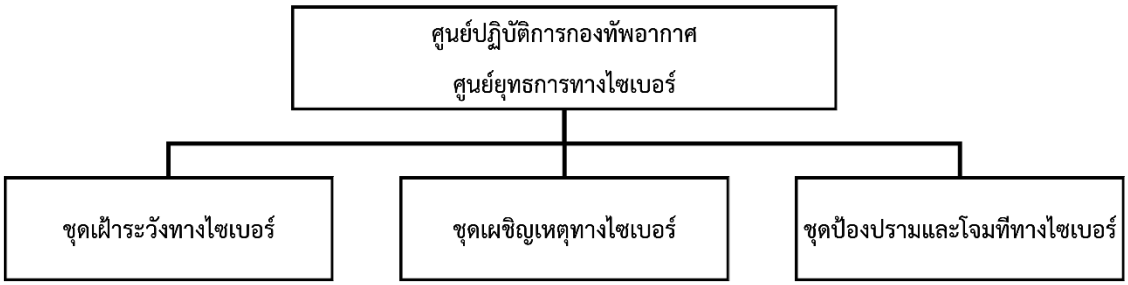
๓.๑.๖ กองบัญชาการควบคุมการปฏิบัติกองทัพอากาศ (คปอ.) มีหน้าที่เตรียมและดำเนินการเกี่ยวกับการบัญชาการและควบคุมการปฏิบัติทางอากาศ ทางอวกาศ และทางไซเบอร์ และดำเนินการด้านการป้องกันทางอากาศ การปฏิบัติการทางอากาศ การค้นหาและช่วยชีวิต การข่าวกรองการเฝ้าตรวจและลาดตระเวน การสนับสนุนการบัญชาการและควบคุม การจราจรทางอากาศ การข่าวอากาศ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตราภิจการในสายวิทยาการที่เกี่ยวข้องในด้านการควบคุมการปฏิบัติทางอากาศ มีผู้บัญชาการกองบัญชาการควบคุมการปฏิบัติทางอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

เป็นหน่วยกำลังรบ ควบคุมการปฏิบัติการทางไซเบอร์ในด้านยุทธการ โดยดำเนินการร่วมกับศูนย์ไซเบอร์กองทัพอากาศในด้านการเตรียมความพร้อมการใช้กำลังให้มีความพร้อม รวมถึงการปฏิบัติการทางไซเบอร์เพื่อตอบสนองวัตถุประสงค์ทางทหารที่ต้องการ



ภาพที่ ๓.๖ โครงสร้างหน่วยขึ้นตรงกองบัญชาการควบคุมการปฏิบัติทางอากาศ

๓.๒ ภารกิจและโครงสร้างการจัดศูนย์ยุทธการทางไซเบอร์ศูนย์ปฏิบัติการกองทัพอากาศ



ภาพที่ ๓.๗ โครงสร้างของศูนย์ยุทธการไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ

๓.๒.๑ ภารกิจ มีประสานงาน สั่งการ และควบคุมการใช้กำลังหน้าที่วางแผน อำนวยการมิติไซเบอร์เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ ด้วยการป้องกันทางไซเบอร์ตลอดจนสามารถลิดลอน หรือจำกัดเสรีภาพในการปฏิบัติการทางไซเบอร์ของฝ่ายตรงข้ามด้วยการโจมตีทางไซเบอร์ และสนับสนุน ภารกิจการป้องกันประเทศด้านไซเบอร์ตามสั่งการของผู้มีอำนาจรับผิดชอบ มีผู้อำนวยการศูนย์ยุทธการทางไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ โดยแบ่งเป็น ๓ ชุด ดังนี้

๓.๒.๑.๑ ชุดเฝ้าระวังทางไซเบอร์ มีหน้าที่ปฏิบัติการในมิติไซเบอร์ เพื่อสนับสนุน ศปก.ทอ.โดยรับผิดชอบการเฝ้าระวังและตรวจจับการบุกรุก/โจมตีระบบสารสนเทศของ ทอ. โดยมีหัวหน้าชุดเฝ้าระวังทางไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ

การแบ่งมอบ

๓.๒.๑.๑ (๑) ทำการเฝ้าระวัง ตรวจจับ วิเคราะห์ และประเมินเหตุการณ์ที่ละเมิดความปลอดภัยของระบบเครือข่าย (Network) ระบบบัญชาการและควบคุม (C2) ระบบตรวจจับ (Sensor) ระบบสารสนเทศในระบบงานของ ศปก.ทอ.และระบบงานอื่นของ ทอ.ตลอด ๒๔ ชม.

๓.๒.๑.๑ (๒) แจ้งเตือน กำหนดมาตรการ และกำกับดูแลระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยต่าง ๆ ในกองทัพอากาศ

๓.๒.๑.๒ ชุดเผชิญเหตุทางไซเบอร์ มีหน้าที่ ปฏิบัติการในมิติไซเบอร์ เพื่อสนับสนุน ศปก.ทอ.โดยรับผิดชอบปฏิบัติการตอบสนองกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ มีหัวหน้าชุดเผชิญเหตุทางไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ

การแบ่งมอบ

๓.๒.๑.๒ (๑) ปฏิบัติการระงับการบุกรุก/โจมตี

๓.๒.๑.๒ (๒) การพิสูจน์หลักฐานทางดิจิทัล

๓.๒.๑.๒ (๓) การฟื้นฟูระบบที่ได้รับผลกระทบให้กลับคืนสู่สภาพปกติพร้อมใช้งาน และปรับปรุงกระบวนการป้องกันให้มีความปลอดภัย

๓.๒.๑.๓ ชุดป้องปรามและโจมตีทางไซเบอร์ มีหน้าที่ ปฏิบัติการในมิติไซเบอร์ เพื่อสนับสนุน ศปก.ทอ.โดยรับผิดชอบปฏิบัติการไซเบอร์ เชิงป้องปรามเพื่อตอบสนองวัตถุประสงค์ทางทหารที่ต้องการ มีหัวหน้าชุดป้องปรามและโจมตีทางไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ

การแบ่งมอบ

๓.๒.๑.๓ (๑) การเตรียมพร้อมในการปฏิบัติตามวงรอบการโจมตีทางไซเบอร์ตามบัญชีแฟ้มเป้าหมายที่ได้รับอนุมัติ

๓.๒.๑.๓ (๒) การปฏิบัติการโจมตีเป้าหมาย เปิดช่องทางลับสำหรับการปฏิบัติครั้งต่อไป และลบร่องรอยการโจมตี

๓.๒.๑.๓ (๓) การตรวจสอบจุดอ่อนและช่องโหว่ในระบบทางไซเบอร์ของฝ่ายเรา พร้อมทั้งประสานให้คำแนะนำการปฏิบัติแก่หน่วยที่เกี่ยวข้อง

บทที่ ๔ การฝึกและพัฒนาด้านไซเบอร์

๔.๑ งานด้านการฝึก

มีแผนกการฝึก กองการฝึกพัฒนาทางไซเบอร์รับผิดชอบ โดยมีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการเกี่ยวกับการศึกษา การฝึกอบรม เพื่อเตรียมความพร้อมในการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ ได้แก่ การวิเคราะห์ข่าวสารทางไซเบอร์ การค้นหา การทดสอบหาช่องโหว่หรือจุดอ่อนของระบบคอมพิวเตอร์ ระบบสารสนเทศ หรือระบบรักษาความปลอดภัยไซเบอร์ การรับมือเหตุการณ์ทางไซเบอร์ การตอบสนองภัยคุกคาม และการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล รวมทั้งให้การสนับสนุนการปฏิบัติการไซเบอร์ด้านอื่น ๆ ที่ได้รับมอบหมาย โดยมีการดำเนินการในการฝึกอบรม ดังนี้

๔.๑.๑ โครงการศึกษาของ ทอ.ประจำปีทั้งใน และต่างประเทศ โครงการศึกษาของ ทอ. เป็นการบรรจุหลักสูตรหรือ/โครงการด้านการศึกษาและฝึกอบรมตามความต้องการ ของ นขต.ทอ. เพื่อขับเคลื่อนความสามารถของกำลังพล ทอ. และตอบสนองภารกิจของ ทอ.โดยมีคณะ คณอก. โครงการศึกษาของ ทอ.ซึ่งมีหน้าที่พิจารณากลั่นกรองและจัดทำโครงการศึกษาของ ทอ. โดย คณอก.ฯ ได้แต่งตั้ง คณะ จนท.จัดทำโครงการศึกษาของ ทอ. ซึ่งมี ผอ.สปพ.กพ.ทอ.เป็น หน.จนท.ทำงาน มีอำนาจหน้าที่พิจารณากลั่นกรองและตรวจสอบโครงการศึกษาของหน่วยที่เสนอ รวมทั้งกำหนดลำดับความสำคัญของโครงการศึกษา โดยต้องมีความสอดคล้องกับยุทธศาสตร์ ทอ., นโยบาย ผบ.ทอ. และระเบียบที่เกี่ยวข้อง โดย ศซบ.ทอ.ได้พิจารณาเสนอโครงการศึกษาเป็นวงรอบทุก ๆ ปีเพื่อพัฒนากำลังพลให้มีความรู้ความสามารถในด้านการปฏิบัติงานไซเบอร์ เพื่อสอดรับกับยุทธศาสตร์ ทอ. และนโยบาย ผบ.ทอ. โดยมีหลักสูตรที่เสนอตามวงรอบ ดังนี้

๔.๑.๑.๑ หลักสูตรการปฏิบัติการทางไซเบอร์ ทอ.เป็นหลักสูตรเพื่อให้ผู้เข้ารับการศึกษามีความเข้าใจและมีทักษะในการปฏิบัติการทางไซเบอร์ได้อย่างถูกต้องและมีประสิทธิภาพ รวมทั้งมีเจตคติที่ดีต่อการปฏิบัติการทางไซเบอร์ตามค่านิยมหลักของกองทัพอากาศ และมีความเข้าใจในการปฏิบัติงานด้านไซเบอร์ อีกทั้งยังสามารถนำความรู้ที่ได้รับไปปฏิบัติงานได้อย่างถูกต้อง

๔.๑.๑.๒ โครงการสัมมนาเชิงปฏิบัติการเพื่อรับมือภัยคุกคามไซเบอร์ เป็นการฝึกอบรมเพื่อให้บุคลากรด้านเทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์และด้านไซเบอร์ เกิดความรู้ความเข้าใจในการปฏิบัติงานในมิติไซเบอร์ รวมถึงแนวทางการรับมือภัยคุกคามไซเบอร์ เพื่อนำไปใช้ในการปฏิบัติงานสำหรับการรับมือภัยคุกคามไซเบอร์ของหน่วย

๔.๑.๑.๓ หลักสูตรการอบรมสร้างความตระหนักรู้ด้านไซเบอร์กำลังพล ทอ. เป็นการฝึกอบรมเพื่อเสริมสร้างความตระหนักรู้ไซเบอร์แก่กำลังพล ทอ.โดยมีเนื้อหาเกี่ยวข้องกับการสร้างความตระหนักรู้ด้านไซเบอร์ครอบคลุม ๕ กลุ่ม ได้แก่ การใช้งานสื่อสังคมออนไลน์อย่างปลอดภัย การใช้งานอินเทอร์เน็ตอย่างปลอดภัย การใช้งาน Application Device & Network อย่างปลอดภัย ความรู้พื้นฐานด้านการโจมตีระบบและการรับมือภัยคุกคามทางไซเบอร์ และ กฎหมาย ระเบียบ และนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๔.๑.๑.๔ การฝึกอบรมทบทวนและประเมินผลเพื่อรักษาสถานภาพความชำนาญกำลังพลพร้อมเรียกด้านไซเบอร์ (Cyber On-call List) ของ ทอ. เพื่อให้กำลังพลพร้อมเรียกด้านไซเบอร์ของ ทอ.ได้ทบทวนแนวทางการปฏิบัติสำหรับการรับมือกับภัยคุกคามไซเบอร์ให้เป็นในทิศทางเดียวกันทั้งเชิงรุก และเชิงรับ และมีความพร้อมปฏิบัติการด้านไซเบอร์

๔.๑.๑.๕ การอบรมเชิงปฏิบัติการด้านไซเบอร์ ทอ. WA - ANG 23 เป็นการฝึกเพื่อเสริมสร้าง และเพิ่มพูนความรู้ต่อการดำเนินงานของ ทอ. ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและสงครามไซเบอร์ รวมถึงการพัฒนางานด้านไซเบอร์ของ ทอ. ทั้งด้านนโยบาย กระบวนการ กำลังพล และเทคโนโลยี โดยเฉพาะในระดับผู้ปฏิบัติการ รวมถึงสร้างเครือข่ายประชาคมไซเบอร์ในกลุ่มมิตรประเทศ และสอดรับกับยุทธศาสตร์ไซเบอร์ กห., ทท. และ ทอ. ที่กำหนดไว้

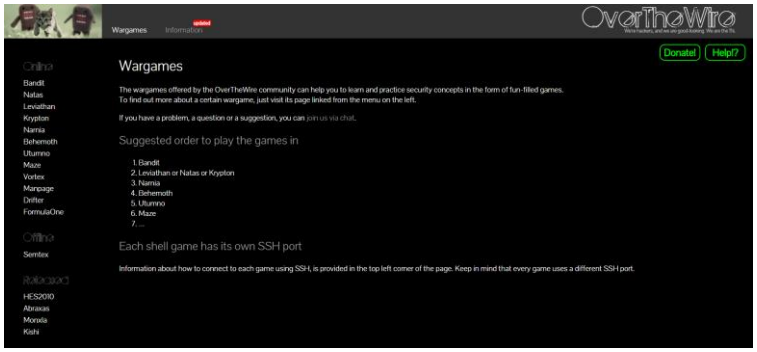
๔.๑.๑.๖ การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (National Cyber Exercise) เป็นการฝึกเพื่อให้บุคคลที่ปฏิบัติงานที่เกี่ยวข้องกับงานด้านไซเบอร์ภัยคุกคามทางไซเบอร์และแนวทางปฏิบัติเพื่อรับมือภัยคุกคามไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (National Cyber Exercise)

๔.๑.๑.๗ Cobra Gold เป็นการฝึกร่วม/ผสมทางการทหารระดับพหุภาคีที่จัดขึ้นเป็นประจำทุกปีในประเทศไทย เริ่มครั้งแรกจากการฝึกทวิภาคีระหว่างประเทศไทยกับสหรัฐอเมริกาเมื่อปี พ.ศ. ๒๕๒๕ ต่อมาได้เปลี่ยนเป็นแบบพหุภาคีโดยมีประเทศอื่น ๆ เข้าร่วม ได้แก่ สิงคโปร์ อินโดนีเซีย มาเลเซีย เกาหลีใต้ และญี่ปุ่น วัตถุประสงค์ของการฝึกคอบร้าโกลด์ คือ ปรับปรุงการทำงานร่วมกัน แลกเปลี่ยนประสบการณ์ และส่งเสริมความสัมพันธ์ระหว่างชาติต่าง ๆ ที่เข้าร่วมในการฝึก นอกจากนี้ยังช่วยส่งเสริมความสงบสุขและความมั่นคงในภูมิภาค การตอบสนองที่รวดเร็วและมีประสิทธิภาพหลังเหตุการณ์คลื่นสึนามิที่เกิดจากแผ่นดินไหวในมหาสมุทรอินเดีย พ.ศ. ๒๕๔๗ ส่วนหนึ่งเป็นผลที่ได้รับจากการฝึกร่วม/ผสมนี้ โดยมีส่วนของการฝึกทางไซเบอร์เข้าร่วมด้วย

๔.๑.๑.๘ โครงการเข้าร่วมการอบรม/การแข่งขันด้านไซเบอร์ทั้งในและต่างประเทศ ผลักดัน
ส่งเสริมให้บุคลากรของกองทัพอากาศ มีใบรับรองความสามารถด้านความปลอดภัยทางไซเบอร์ (Security Certification) พร้อมทั้งสนับสนุนงบประมาณค่าใช้จ่ายในการ เข้าฝึกอบรม เพื่อเตรียมความพร้อมและการสอบ

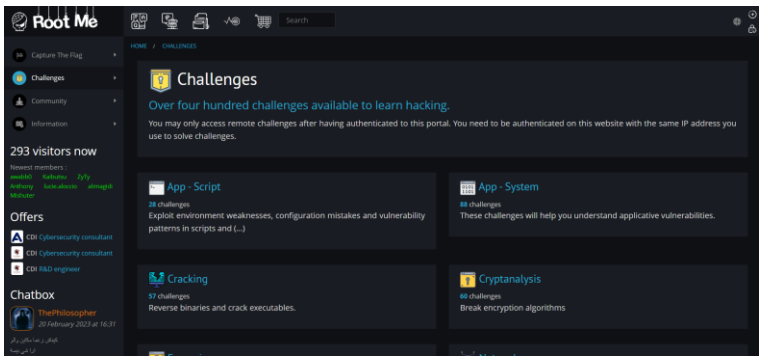
๔.๑.๒ การฝึกปฏิบัติการทางไซเบอร์ เป็นการฝึกเพื่อให้เกิดความรู้ ความเข้าใจ และทักษะในการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่าง ๆ โดยมีรูปแบบที่เรียกว่า เกมส์จำลองสงครามทางไซเบอร์ (Wargame) โดยเป็นโจทย์ไว้เพื่อพัฒนาตนเอง ซึ่งมีตัวอย่างที่นิยม ดังต่อไปนี้

๔.๑.๒.๑ OverTheWire เป็นเว็บไซต์รวม Wargame แบ่งออกเป็นหลายหมวดตั้งแต่ Basic Linux ไปจนถึง Web Exploitation โดยรูปแบบจะเป็น เส้นตรง คือ ต้องผ่านข้อก่อนหน้าถึงจะไปทำข้อต่อไปได้



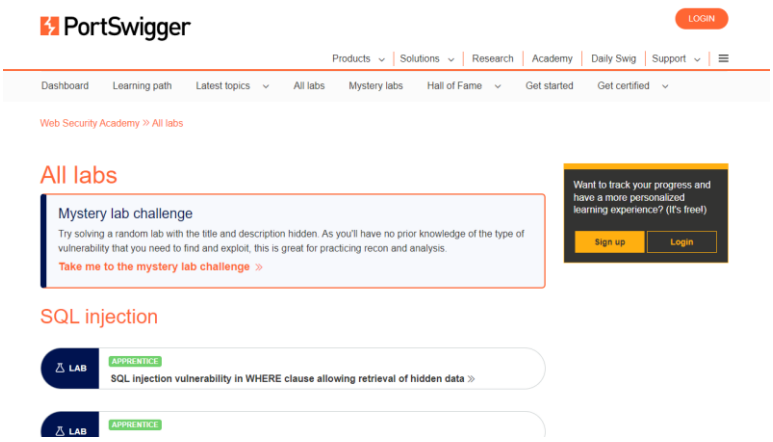
ภาพที่ ๔.๑ เว็บไซต์ https://overthewire.org/wargames/

๔.๑.๒.๒ Root-me.org เป็นเว็บไซต์ที่รวมโจทย์ Cybersecurity ไว้อย่างหลากหลายหมวดหมู่ ในแต่ละข้อมีข้อมูลที่เกี่ยวข้อง พร้อมทั้งข้อแนะนำในการศึกษาเรียนรู้ด้วยตนเอง



ภาพที่ ๔.๒ เว็บไซต์ https://www.root-me.org/en/Challenges

๔.๑.๒.๓ Portswigger Web Security Academy เว็บไซต์ที่ดูแลโดย บริษัท Portswigger ผู้พัฒนาโปรแกรม Burp Suite โดยเนื้อหาจะเกี่ยวกับ Web Exploitation พร้อมมี Lab ที่เกี่ยวข้องกับหัวข้อนั้น ๆ

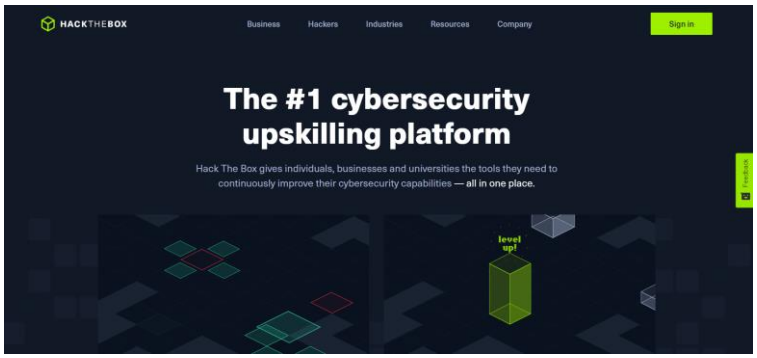


ภาพที่ ๔.๓ เว็บไซต์ https://portswigger.net/web-security/all-labs

๔.๑.๒.๔ CryptoHack และ Cryptopals เป็นเว็บไซต์ Wargame เกี่ยวกับช่องโหว่ต่าง ๆ ของการเข้ารหัสและถอดรหัส

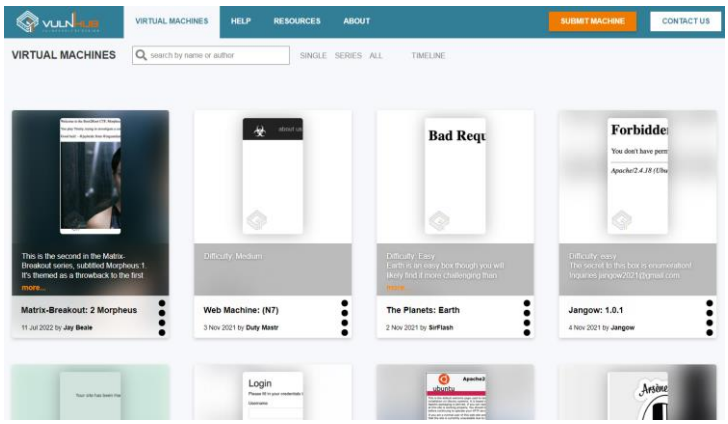
ภาพที่ ๔.๔ เว็บไซต์ https://cryptohack.org/ และ https://cryptopals.com/

๔.๑.๒.๕ Hack The Box เป็นเว็บไซต์รวมโจทย์จำลองการทดสอบเจาะระบบที่มีทั้งระบบปฏิบัติการ Windows และ Linux โดยผู้ใช้งานจะได้เริ่มตั้งแต่การหาช่องโหว่ไปจนถึงการโจมตี



ภาพที่ ๔.๕ เว็บไซต์ https://www.hackthebox.com/

๔.๑.๒.๖ Vulnhub เป็นเว็บไซต์ที่รวบรวมไฟล์โจทย์ซึ่งเป็น Virtual Machine

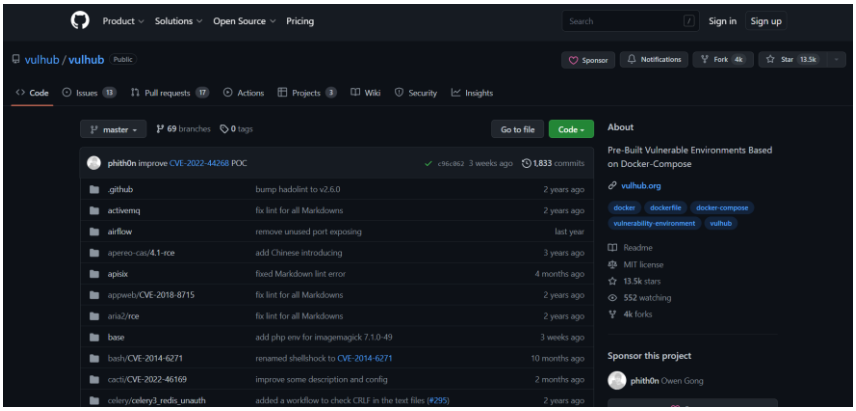


ภาพที่ ๔.๖ เว็บไซต์ https://www.vulnhub.com/

๔.๑.๒.๗ Microcorruption เป็นเว็บไซต์ Wargame ของโจทย์ Cybersecurity เกี่ยวกับการทำ Reverse Engineering ฉบับเริ่มต้น

ภาพที่ ๔.๗ เว็บไซต์ https://www.nccgroup.com/

๔.๑.๒.๘ Vulhub เป็น git repository (พื้นที่เก็บข้อมูลชุดคำสั่ง) ที่รวม docker ของช่องโหว่ที่มี CVE ต่าง ๆ จำนวนมาก สามารถนำมาเปิดเล่นเพื่อทดสอบโจมตีช่องโหว่ ที่เคยมีมาในอดีตได้บนเครื่องของตัวเอง ได้ง่าย ๆ



ภาพที่ ๔.๘ เว็บไซต์ https://github.com/vulhub/vulhub

๔.๒ งานด้านการพัฒนาระบบ

รับผิดชอบโดย แผนกพัฒนาระบบ กองการฝึกและพัฒนาทางไซเบอร์ ศูนย์ไซเบอร์ กองทัพอากาศ มีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการเกี่ยวกับการวิจัยและพัฒนาเครื่องมือด้านไซเบอร์ในการปฏิบัติการสงครามไซเบอร์ ทั้งเชิงรุกและเชิงรับ เพื่อการวิเคราะห์ข่าวสารทางไซเบอร์ การค้นหา การทดสอบหาช่องโหว่หรือจุดอ่อนของระบบคอมพิวเตอร์ ระบบสารสนเทศ หรือระบบรักษาความปลอดภัยไซเบอร์ การรับมือเหตุการณ์ทางไซเบอร์ การตอบสนองภัยคุกคาม และการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล รวมทั้งให้การสนับสนุนด้านการพัฒนาระบบสารสนเทศอื่น ๆ ที่ได้รับมอบหมาย

เอกสารอ้างอิง

กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.) (๒๕๖๒). ตำราวิชาพื้นฐานคอมพิวเตอร์และดิจิตอล พ.ศ.๒๕๖๒.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดส.) (๒๕๖๐). พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒).

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดส.) (๒๕๖๒). พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดส.) (๒๕๖๒). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.

กองทัพอากาศ (ทอ.) (๒๕๕๒). ระเบียบ ทอ.ว่าด้วยการศึกษาภายในประเทศ พ.ศ.๒๕๕๒.

กองทัพอากาศ (ทอ.) (๒๕๕๓). ระเบียบกองทัพอากาศ ว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓.

กองทัพอากาศ (ทอ.) (๒๕๕๓). ระเบียบกองทัพอากาศ ว่าด้วยการศึกษาในต่างประเทศ พ.ศ.๒๕๕๓.

กองทัพอากาศ (ทอ.) (๒๕๕๓). ระเบียบกองทัพอากาศ ว่าด้วยการศึกษาภายในประเทศ พ.ศ.๒๕๕๓.

กองทัพอากาศ (ทอ.) (๒๕๕๖). นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอากาศ.

กองทัพอากาศ (ทอ.) (๒๕๖๑). แนวความคิดในการปฏิบัติการในมิติไซเบอร์ กองทัพอากาศ.

กองทัพอากาศ (ทอ.) (๒๕๖๑). เอกสารประกอบการบรรยาย วิชาการปฏิบัติการที่มีเครือข่ายเป็นศูนย์กลาง (NCO) (ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี).

กองทัพอากาศ (ทอ.) (๒๕๖๒). หลักนิยมกองทัพอากาศ พ.ศ.๒๕๖๒.

กองทัพอากาศ (ทอ.) (๒๕๖๓). ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐)

กองทัพอากาศ (ทอ.) (๒๕๖๓). ระเบียบ ทอ.ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๓.

กองทัพอากาศ (ทอ.) (๒๕๖๓). ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓.

กองทัพอากาศ (ทอ.) (๒๕๖๔). ระเบียบกองทัพอากาศ ว่าด้วยการฝึกงานในหน้าที่ (ฉบับที่ ๒) พ.ศ.๒๕๖๔.

กองทัพอากาศ (ทอ.) (๒๕๖๕). คู่มือจัดทำและบริหารโครงการศึกษาของ ทอ. ประจำปีงบประมาณ ๖๕ - ๖๖.

กองทัพอากาศ (ทอ.) (๒๕๖๕). ระเบียบกองทัพอากาศ ว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ พ.ศ.๒๕๖๕.

กองทัพอากาศ (ทอ.) (๒๕๖๕). ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัย พ.ศ.๒๕๖๕.

Keesler Air Force Base. (2019). Student Text (ST) E3OQR17D1 001A Technical Training : Undergraduate Cyber Training (Phase 1).

Meyers, M. (2018). Com TIA Network+ Certification All-in-One Exam Guide. In M. G. Hill (Ed.), (Seventh Edition ed.).

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) (๒๕๕๙). เอกสารประกอบการบรรยาย วิชาระบบสารสนเทศของกองทัพอากาศ.

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) (๒๕๖๓). แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารกองทัพอากาศ พ.ศ.๒๕๖๓ – ๒๕๗๐.

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) (๒๕๕๙). คู่มือการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารกองทัพอากาศ.

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) (๒๕๕๕). ตำราฝึกงานในหน้าที่จำพวกทหารสารสนเทศและสงครามอิเล็กทรอนิกส์

การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฝผ.) (๒๕๖๓). มาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ กฟผ., 3.

จิระ จิตสุภา, ปรัชญนันท์ นิลสุข และพัลลภ พิริยะสุรวงศ์ (๒๕๕๕). การสังเคราะห์เนื้อหาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศตามมาตรฐานสากล (Synthesis of a Security in International Information Technology Standards). วารสารเทคโนโลยีสารสนเทศ Information Technology Journal, 1.

นิวัติ เนียมพลอย (๒๕๕๙). ความสัมพันธ์ภายในการปฏิบัติการข่าวสาร. Retrieved from https://nniwat.wordpress.com/2016/01/16/ความสัมพันธ์ภายในการปฏ/

จตุชัย แพงจันทร์ (๒๕๕๘). Master in Security 3rd Edition: ไอดีซี พรีเมียร์.

จตุชัย แพงจันทร์ และอนุโชต วุฒิพรพงษ์ (๒๕๕๕). เจาะระบบ Network Edition.

วิรินทร์ เมฆประดิษฐสิน (๒๕๕๙). คัมภีร์ออกแบบติดตั้งอุปกรณ์เครือข่าย Cisco เล่ม 1 New Edition.

ศูนย์ไซเบอร์กองทัพอากาศ (ศซบ.ทอ.) (๒๕๖๕). หลักสูตรปฏิบัติการทางไซเบอร์กองทัพอากาศ (RTAF Cyber Operations Course).

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (๒๕๖๕). หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน (Cybersecurity Foundation Course).

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) (๒๕๖๒). พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) (๒๕๕๙). ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน.

สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ. (๒๕๖๑). ยุทธศาสตร์ชาติ พ.ศ.๒๕๖๑ - ๒๕๘๐.

เอกชัย สิงห์ทอง และเฉลิมขวัญ ศิริพันธุ์ (๒๕๖๓). เอกสารประกอบการบรรยาย วิชา การพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic).

ศิวลีย์ สิริโรจน์บริรักษ์ (๒๕๕๘). การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม Standard Development; Cyber Security of the Ministry of Defence. สถาบันวิชาการป้องกันประเทศ, 6(3).

พิชญะ โมริโมโต. (2020). ยกระดับศักยภาพของทีม IT Security องค์กรด้วยการเล่น CTF. Retrieved from https://www.cyfence.com/article/empower-your-itsecurity-team-with-capture-the-flag/