การข่าวกรองทางไซเบอร์

พ.ศ.๒๕๖๖

โดย

กองปฏิบัติการไซเบอร์

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

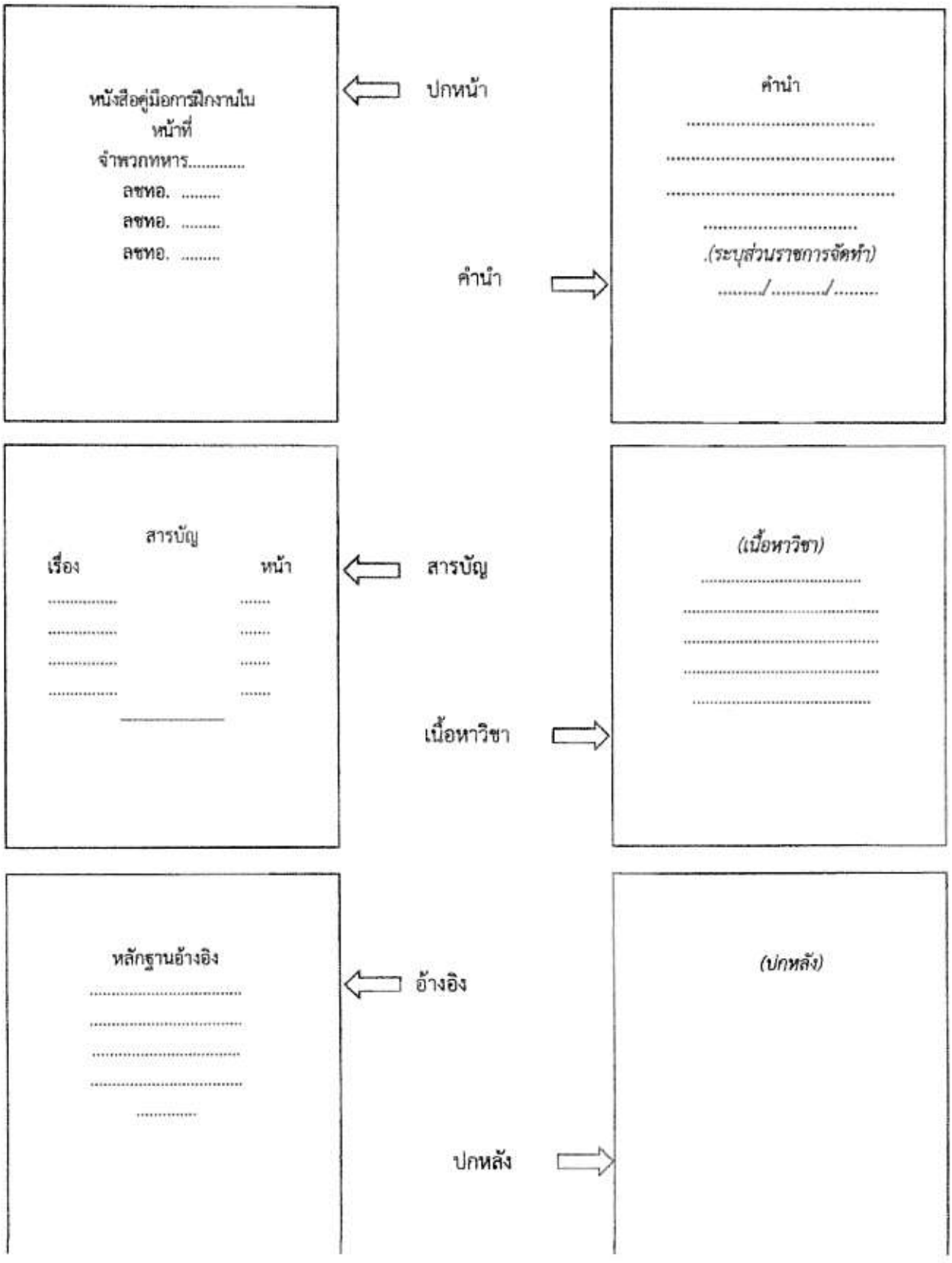
๓๕.๖ ป่วยจนมีเวลาการฝึกไม่เพียงพอตามข้อ ๓๕.๕

๓๕.๗ ขาดการทดสอบความรู้ภาคปฏิบัติตามระยะเวลาที่กำหนด โดยมีเหตุผลอันสมควร

ข้อ ๓๖ การลา ...

ผนวก ๗ ประกอบระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓

หนังสือคู่มือการฝึกงานในหน้าที่



คู่มือการฝึกงานในหน้าที่
จำพวกทหารไซเบอร์

ลชทอ.๒๘๑๓๐

ลชทอ.๒๘๑๕๐

ลชทอ.๒๘๑๗๐

กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

คำนำ

คู่มือการฝึกงานในหน้าที่วิชาการข่าวกรองไซเบอร์ จัดทำขึ้นเพื่อประกอบการฝึกความชำนาญตามมาตรฐานการฝึกความชำนาญ (มฝช.) ของสายวิทยาการไซเบอร์ เนื้อหาความรู้ของคู่มือเล่มนี้กล่าวถึงการข่าวกรองไซเบอร์ ได้แก่ ความรู้เบื้องต้นทางข่าวกรอง ข่าวกรองทางทหาร และข่าวกรองไซเบอร์ เพื่อให้ผู้เข้ารับการฝึกงานในหน้าที่ มีความรู้ความเข้าใจและทักษะในการนำไปปฏิบัติงานในสายวิทยาการไซเบอร์ และสามารถนำองค์ความรู้ที่ได้รับ ไปประยุกต์เพื่อให้เกิดความปลอดภัยสูงสุดต่อผู้ปฏิบัติงานระบบคอมพิวเตอร์ และระบบสารสนเทศของกองทัพอากาศ

หวังเป็นอย่างยิ่งว่าคู่มือเล่มนี้ จะเป็นประโยชน์ต่อผู้เข้ารับการฝึกงานในหน้าที่และขอขอบคุณเจ้าหน้าที่ทุกท่านที่มีส่วนในการจัดทำคู่มือเล่มนี้จนเสร็จสมบูรณ์

กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

๒๘ สิงหาคม ๒๕๖๖

สารบัญ

หน้า

สารบัญภาพ

บทที่ ๑ ความรู้เบื้องต้นทางข่าวกรอง

การนำเทคโนโลยีสารสนเทศมาใช้ทางด้านการทหารอย่างแพร่หลาย ทำให้กองทัพต้องปรับเปลี่ยนรูปแบบในการทำสงครามแบบใหม่ หรือที่เรียกว่ายุคการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางซึ่งเป็นยุคที่จำเป็นต้องใช้เทคโนโลยีสารสนเทศและการสื่อสาร เข้ามาเป็นองค์ประกอบที่สำคัญ ในการขับเคลื่อนปฏิบัติการทางทหาร เช่น ระบบบัญชาการและควบคุม ระบบเชื่อมโยงข้อมูลทางยุทธวิธี ระบบป้องกันภัยทางอากาศระบบอาวุธยุทโธปกรณ์ และระบบส่งกำลังบำรุง เป็นต้นการใช้ประโยชน์จากเทคโนโลยีสารสนเทศจะช่วยเพิ่มประสิทธิภาพในการปฏิบัติการ อย่างไรก็ตามระบบต่าง ๆ เหล่านี้มีความเสี่ยงสูงที่จะเป็นเป้าหมายของการถูกโจมตีผ่านทางไซเบอร์สเปซ (Cyberspace) จนปัจจุบันได้เกิดการทำสงครามรูปแบบใหม่ที่เรียกว่า สงครามไซเบอร์ (Cyber Warfare) ซึ่งเป็นการปฏิบัติการสงครามที่เกิดขึ้นในโลกไซเบอร์แต่ส่งผลกระทบในโลกจริง

ไซเบอร์สเปซ (Cyberspace) กลายเป็นศัพท์ใหม่ที่ได้รับการยอมรับในสังคมโลกอย่างรวดเร็ว และเป็นสิ่งที่จำเป็นต้องเกี่ยวข้องอย่างหลีกเลี่ยงไม่ได้ ไซเบอร์สเปซ หมายถึง เครือข่ายอินเทอร์เน็ตที่เป็นโครงสร้างพื้นฐานหลัก และมีคอมพิวเตอร์รวมถึงอุปกรณ์ทุกอย่างเชื่อมต่อเข้ากับระบบเครือข่ายอินเทอร์เน็ตและระบบเครือข่ายย่อยขององค์กร โดยรวมถึงเครือข่ายย่อยส่วนบุคคลและไม่จำเป็นต้องเป็นเครื่องคอมพิวเตอร์ ซึ่งรวมอุปกรณ์ที่เชื่อมต่อกับอินเตอร์เน็ต (Internet of Things: IoT) เช่น กล้องวงจรปิด อุปกรณ์ไฟฟ้าที่ใช้ในครัวเรือน เป็นต้น ดังนั้นข้อมูลจำนวนมหาศาลจึงเดินทางไปในมิติไซเบอร์เพื่อตอบสนองความสะดวกสบาย รวดเร็ว การแลกเปลี่ยนข้อมูลข่าวสาร การลดความซับซ้อนของการทำงานและการใช้บริการข้อมูลต่าง ๆ

ปริมาณการใช้งานรวมถึงจำนวนผู้ใช้ที่เพิ่มขึ้น กลับเปิดโอกาสให้กับกลุ่มมิจฉาชีพ ที่มุ่งแสวงหาผลประโยชน์จากการก่ออาชญากรรมทางไซเบอร์ (Hacker) เพิ่มขึ้นด้วยเช่นกัน จากที่กล่าวมานั้นคือภัยคุกคามทางไซเบอร์ (Cyber Threat) ซึ่งมีความสำคัญในยุคปัจจุบัน เพราะมีแนวโน้มความรุนแรงที่ส่งผลกระทบต่อชีวิตและทรัพย์สินมากขึ้นตามลำดับอย่างหลีกเลี่ยงไม่ได้ นอกจากนี้ยังส่งผลกระทบต่อระบบโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure) ได้แก่ กลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เช่น กลุ่มความมั่นคง และบริการภาครัฐ กลุ่มการเงิน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภคและกลุ่มสาธารณสุขเป็นต้น ส่งผลกระทบต่อความมั่นคงปลอดภัยของประเทศ ในภาพรวม จะเห็นได้ว่าภัยคุกคามทางไซเบอร์เป็นภัยคุกคามรูปแบบใหม่ ที่เน้นกระทำต่อ ระบบอินเทอร์เน็ต และระบบเครือข่ายคอมพิวเตอร์ ทำให้ประชาคมโลกเริ่มตื่นตัวและตระหนักถึงภัยคุกคามดังกล่าว

ก่อนที่จะเข้าถึงเรื่องการพัฒนาศักยภาพในการปฏิบัติการเครือข่ายนั้นจำเป็นที่ต้องเข้าใจคำจำกัดความ ศัพท์ที่เกี่ยวข้อง ซึ่งกระทรวงกลาโหมสหรัฐฯ ได้กำหนดคำจำกัดความเหล่านี้ไว้ในเอกสารร่วม Joint Publication 3 - 13 โดยศัพท์ที่สำคัญ เช่น สงครามไซเบอร์ (Cyber warfare) หมายถึง การปฏิบัติการ ทางทหารที่ใช้ไซเบอร์สเปซเป็นสมรภูมิการรบ ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมที่ข้อมูลดิจิตอลสามารถสื่อสารผ่านได้ ซึ่งรวมถึงเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม ระบบคอมพิวเตอร์ โปรเซสเซอร์และคอนโทลเลอร์ และการปฏิบัติการไซเบอร์ (Cyber operation) หมายถึง การปฏิบัติการทางทหารภายในไซเบอร์สเปซ เป็นต้น อย่างไรก็ตาม

เนื่องจากความหมายของคำว่า “การปฏิบัติการไซเบอร์” อาจมีความหมายไม่สื่อความเข้าใจมากนัก ดังนั้น สำหรับคู่มือเล่มนี้ผู้เขียนจะขอใช้คำว่า “การปฏิบัติการสงครามไซเบอร์” ในความหมายเดียวกันกับคำว่า “การปฏิบัติการไซเบอร์”

ตัวอย่างกรณีของไวรัสสตักซ์เน็ต (Stuxnet) เป็นไวรัสโทรจันที่ถูกสร้างขึ้นเพื่อเป็นอาวุธไซเบอร์ชนิดสามารถทำลายโรงงานผลิตอาวุธนิวเคลียร์ของประเทศอิหร่านได้ (จากตัวอย่างกรณีนี้และอีกหลาย ๆ เหตุการณ์ทำให้หลายประเทศได้เห็นความสำคัญ และเริ่มกระบวนการพัฒนาอาวุธไซเบอร์เพื่อใช้โจมตีเป้าหมายทางทหารบางประเภท ดังนั้นกองทัพจึงมีความจำเป็นอย่างยิ่งที่ต้องเตรียมการในการป้องกันการโจมตีจากไซเบอร์สเปซ (Cyberspace) และในขณะเดียวกันจำเป็นที่ต้องพัฒนาศักยภาพ ความพร้อมในการปฏิบัติการสงครามไซเบอร์ ซึ่งจะเป็นการทวีกำลังทางทหารในการต่อสู้ในสงครามรูปแบบใหม่ที่จะเกิดขึ้นอย่างแน่นอนในอนาคตอันใกล้)

ตัวอย่าง ภัยคุกคามทางไซเบอร์ที่โจมตีโครงสร้างพื้นฐานสำคัญในระดับโลก ที่เพิ่งเกิดขึ้นคือ บริษัท Colonial Pipeline ฝั่งตะวันออกของสหรัฐอเมริกาโดนโจมตีด้วยโปรแกรมประสงค์ร้าย เรียกค่าไถ่ (Ransomware) โดยยึดข้อมูลเกือบ ๑๐๐ กิกะไบต์ เป็นประกัน ทำให้ระบบการขนส่งน้ำมันผ่านท่อลำเลียงล่ม ต้องปิดทำการและกลับมาใช้การขนส่งสำรอง ซึ่งหาก Hacker มุ่งทำลายระบบการขนส่งน้ำมันอาจทำให้เกิดอันตรายต่อชีวิตพนักงานของบริษัท Colonial Pipeline และประชาชนบริเวณโดยรอบได้

ในระดับประเทศ โรงพยาบาลสระบุรีได้ตกเป็นเป้าหมายของการโจรกรรมข้อมูลด้วยโปรแกรมประสงค์ร้ายเรียกค่าไถ่ ทำให้แพทย์และพยาบาลทำงานล่าช้าลงเนื่องจากไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้ โดยทางโรงพยาบาลสระบุรีได้ออกมาประกาศผู้ใช้บริการโรงพยาบาลทุกคนทราบว่าระบบคอมพิวเตอร์ของโรงพยาบาลกำลังถูกเข้ารหัสข้อมูลทำให้ไม่สามารถเข้าถึงข้อมูลผู้ป่วยที่อยู่ในเซิร์ฟเวอร์ได้ ซึ่งข้อมูลถูกเข้ารหัสนั้นล้วนเป็นข้อมูลผู้ป่วยในระบบซึ่งเป็นข้อมูลที่จำเป็นต่อการรักษาและวินิจฉัยโรคเป็นอย่างมาก ซึ่งในเหตุการณ์นี้อาจทำให้มีผู้เสียชีวิตได้ เนื่องจากความล่าช้าในการรักษาในกองทัพอากาศ ศูนย์ข้อมูลคอมพิวเตอร์ สอ.ทอ. ถูกแฮ็กเกอร์โจมตีระบบฐานข้อมูลควบคุมบริหารจัดการบัญชี ทำให้ข้อมูล Username/Password ทอ.รั่วไหล และถูกเรียกค่าไถ่ ส่งผลกระทบต่อการปฏิบัติงานด้วยระบบเทคโนโลยีสารสนเทศของกองทัพอากาศ

บทที่ ๒ ข่าวกรองทางทหาร

๒.๑ ข่าวกรองทางทหาร (Military Intelligence)

เป็นสาขาวิชาทางการทหารที่ใช้วิธีการรวบรวมและวิเคราะห์ข้อมูลเพื่อให้คำแนะนำและทิศทางสำหรับช่วยผู้บังคับบัญชาในการตัดสินใจ จุดมุ่งหมายนี้ทำได้โดยให้การประเมินข้อมูลจากพิสัยของแหล่งที่มาตรงตามข้อกำหนดภารกิจของผู้บังคับบัญชา หรือตอบสนองต่อหัวข้อในฐานะส่วนหนึ่งของการปฏิบัติการหรือการวางแผนการทัพ เพื่อให้การวิเคราะห์ ข้อกำหนดข้อมูลของผู้บังคับบัญชาจะได้รับการระบุ เป็นอันดับแรก ซึ่งจะถูกรวมเข้ากับการรวบรวม การวิเคราะห์ และการเผยแพร่ข่าวกรอง พื้นที่ของการศึกษาอาจรวมถึงสภาพแวดล้อมในการปฏิบัติการ ศัตรู กองกำลังที่เป็นมิตร และเป็นกลาง ประชาชนพลเรือนในพื้นที่ปฏิบัติการรบ และพื้นที่อื่น ๆ ที่น่าสนใจในวงกว้าง กิจกรรมข่าวกรองนั้นดำเนินการ ในทุกระดับตั้งแต่ยุทธวิธีไปจนถึงยุทธศาสตร์ ในยามสงบ ช่วงเวลาของการเปลี่ยนแปลงสู่สงคราม และในช่วงสงครามรัฐบาลส่วนใหญ่รักษาความสามารถในการข่าวกรองทางทหารเพื่อจัดหากำลังพลด้านการวิเคราะห์และการรวบรวมข้อมูล รวมถึงความสามารถด้านข่าวกรองทางการทหารและพลเรือนทำงานร่วมกันเพื่อแจ้งคลื่นความถี่ของกิจกรรมทางการเมืองและการทหาร ทั้งนี้กำลังพลที่ปฏิบัติหน้าที่ด้านข่าวกรองอาจได้รับการคัดเลือกสำหรับความสามารถ ในการวิเคราะห์และข่าวกรองส่วนบุคคล ก่อนที่จะได้รับ การฝึกอย่างเป็นทางการ

การปฏิบัติการข่าวกรองดำเนินไปตามลำดับขั้นของกิจกรรมทางการเมืองและการทหาร ข่าวกรองทางทหาร (Military Intelligence) เป็นข่าวกรองสำหรับนำมาใช้ในการวางแผนการปฏิบัติการตามแผนนโยบาย โครงการ และกำหนดการทางทหาร ซึ่งอาจแบ่งออกได้เป็น (ข่าวกรองทางการรบหรือข่าวกรองทางยุทธวิธี) และ ข่าวกรองทางยุทธศาสตร์ คือ ความรู้เกี่ยวกับลมฟ้าอากาศ และลักษณะทางภูมิศาสตร์ของข้าศึก ที่ใช้ในการวางแผนและการปฏิบัติการ และ ข่าวกรองทางการรบ คือ ข่าวกรองที่ได้มาจากการดำเนินกรรมวิธี ต่อข่าวสารลมฟ้าอากาศข้าศึก ที่ได้รับจากเจ้าหน้าที่รวบรวมข่าวสารของทั้งหน่วยเหนือ หน่วยรอง หน่วยข้างเคียง และแหล่งข่าวอื่น ๆ ซึ่งเป็น ความรู้เกี่ยวกับพื้นฐานในการกำหนดนโยบายและแผนการทางทหารของต่างชาติ ชาติใดชาติหนึ่ง หรือหลาย ๆ ชาติโดยมุ่งพิจารณาถึงวัตถุประสงค์ของชาติ การวางแผน และวิธีการปฏิบัติเพื่อให้บรรลุวัตถุประสงค์ ทั้งนี้ความมุ่งหมายในการใช้ข่าวกรองทางการรบ (ได้แก่ ข้อสรุปเกี่ยวกับพื้นที่ปฏิบัติการขีดความสามารถ จุดล่อแหลม และหนทางปฏิบัติของข้าศึก) ก็เพื่อลดผลกระทบต่าง ๆ ที่จะมีต่อการบรรลุภารกิจของเราให้เหลือน้อยที่สุดเท่าที่จะเป็นไปได้ ผู้บังคับบัญชาใช้ข่าวกรองทางการรบในการกำหนดข้อตกลงใจที่จะใช้ปัจจัยอำนาจกำลังรบของตนได้อย่างเหมาะสม เพื่อบรรลุภารกิจของหน่วย และกำหนดมาตรการรักษาความปลอดภัยให้แก่หน่วยได้

๒.๒ ข่าวกรองทางยุทธศาสตร์

ความต้องการข่าวกรองทางยุทธศาสตร์ ได้แก่ ขีดความสามารถ จุดล่อแหลม และหนทางปฏิบัติที่น่าจะเป็นของชาติอื่นทั้งที่เป็นศัตรู พันธมิตร และชาติที่เป็นกลาง ข่าวกรองทางยุทธศาสตร์เกี่ยวข้องกับประเด็นกว้าง ๆ เช่น เศรษฐศาสตร์ การประเมินทางการเมือง ความสามารถทางการทหาร และเจตนารมณ์ของต่างประเทศ เป็นต้น ข่าวกรองดังกล่าวอาจมีหลักเกณฑ์ เทคนิค ยุทธวิธีการทูต หรือสังคมวิทยา เป็นต้น

ข่าวกรองทางยุทธศาสตร์ได้รับการนิยามอย่างเป็นทางการในฐานะ “ข่าวกรองที่จำเป็นสำหรับการจัดตั้งนโยบายและแผนทางทหารในระดับชาติและระดับนานาชาติ” และสอดคล้องกับการสงครามระดับยุทธศาสตร์ ซึ่งได้รับการนิยามอย่างเป็นทางการในฐานะ “ระดับของการสงครามที่ประเทศหนึ่งซึ่งมักจะเป็นสมาชิกของกลุ่มประเทศต่าง ๆ กำหนดวัตถุประสงค์ด้านความมั่นคงทางยุทธศาสตร์ระดับชาติ หรือระดับนานาชาติ (พันธมิตรหรือการร่วมมือกัน) จากนั้นพัฒนาและใช้ทรัพยากรระดับชาติเพื่อให้บรรลุวัตถุประสงค์เหล่านั้น”

๒.๒.๑ การรวบรวมข่าวสารทางยุทธศาสตร์ สำหรับนำมาดำเนินกรรมวิธีและผลิตเป็นข่าวกรองทางยุทธศาสตร์นั้น อาจกล่าวโดยสรุปได้ว่า วิธีการรวบรวมข่าวสารทางยุทธศาสตร์จะแบ่งเป็น ๒ วิธีการดังนี้

๒.๒.๑.๑ การรวบรวมข่าวสารจากแหล่งข่าวเปิด เป็นการรวบรวมข่าวสารจากแหล่งข่าวต่าง ๆ ซึ่งมิได้มีการพิทักษ์รักษาข่าวสารตามมาตรการรักษาความปลอดภัย และไม่ต้องใช้เทคนิค หรือวิธีการที่ยุ่งยากสลับซับซ้อนในการรวบรวม แต่อาจใช้วิธีการปกติธรรมดา เช่น รวบรวมข่าวสารจากเอกสาร วารสาร สิ่งพิมพ์ เอกสารวิจัยของสถาบันการศึกษาและหน่วยงานต่าง ๆ รายงานทางการศึกษา และทางวิชาการ หนังสือรุ่นหรือทำเนียบรุ่นของผู้เข้ารับการศึกษา หรือเข้าร่วมในกิจกรรมต่าง ๆ เป็นต้น

๒.๒.๑.๒ การรวบรวมข่าวสารโดยการปฏิบัติการลับ เป็นการรวบรวมข่าวสารซึ่งต้องใช้ผู้ชำนาญพิเศษ โดยใช้เทคนิคหรือวิธีการที่สลับซับซ้อน และใช้เครื่องมือหรืออุปกรณ์พิเศษต่าง ๆ ประการสำคัญจะเน้นหนักในเรื่องของการรักษาความปลอดภัยในการปฏิบัติการอย่าง เข้มงวดมี ๒ วิธีการ ดังนี้

๒.๒.๑.๒ (๑) การจัดตั้งข่ายงานข่าวลับ คือ ข่าวกรองที่กำหนดขึ้นตามหน้าที่ การปฏิบัติการและความมุ่งหมายในการนำไปใช้ ซึ่งข่าวกรองชนิดต่าง ๆ

๒.๒.๑.๒ (๒) การใช้เครื่องมือสื่อสารและอิเล็กทรอนิกส์ ซึ่งเรียกรวมกันว่า “ข่าวกรองทางการสื่อสาร” (Signal Intelligence : SIGINT)

บทที่ ๓ ข่าวกรองไซเบอร์

ในการปฏิบัติการไซเบอร์มีความสำคัญอย่างยิ่งต่อการปฏิบัติการทางทหารในปัจจุบัน เมื่อกล่าวถึงรูปแบบการปฏิบัติการไซเบอร์ มักจะกล่าวอ้างถึงการปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operation : CNO) ซึ่งเป็นขีดความสามารถหลักของการปฏิบัติการข้อมูลข่าวสาร (Information Operation : IO) การปฏิบัติการเครือข่ายคอมพิวเตอร์แบ่งออกเป็น ๓ รูปแบบ คือ

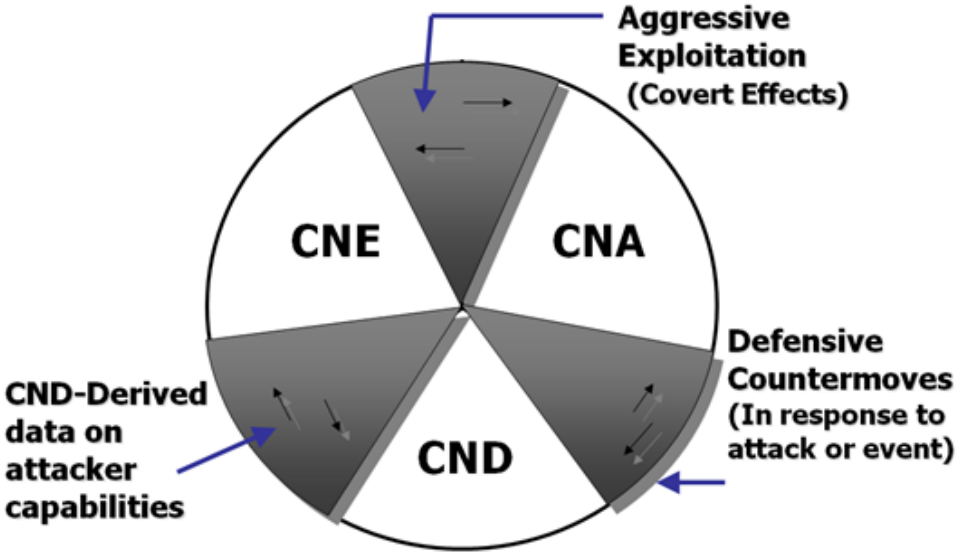
การปฏิบัติการใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์ (Computer Network Exploration : CNE)

การปฏิบัติการโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack : CNA)

การปฏิบัติการป้องกันเครือข่ายคอมพิวเตอร์ (Computer Network Defense : CND)

การปฏิบัติการทั้งสามรูปแบบล้วนแต่มีความจำเป็น และสำคัญต่อความสำเร็จของการปฏิบัติการทางทหารในยุคปัจจุบัน เนื่องจากการปฏิบัติการในรูปแบบใหม่ที่ใช้เครือข่ายเป็นศูนย์กลาง

การพัฒนาศักยภาพในการปฏิบัติการสงครามไซเบอร์ควรเริ่มต้นพัฒนาในส่วนของการปฏิบัติการป้องกันเครือข่ายคอมพิวเตอร์ก่อน เพื่อป้องกันการถูกโจมตีผ่านทางไซเบอร์สเปซต่อระบบต่าง ๆ ที่ใช้ในการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง หลังจากนั้นจึงพัฒนาศักยภาพในการปฏิบัติการใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์ซึ่งหมายถึงปฏิบัติการด้านการข่าว และสุดท้ายจึงเริ่มพัฒนาศักยภาพในการปฏิบัติการโจมตีเครือข่ายคอมพิวเตอร์ ซึ่งศักยภาพด้านนี้จะใช้สำหรับการโจมตีระบบของฝ่ายตรงกันข้ามนอกจากนี้ความรู้เกี่ยวกับเทคนิคและยุทธวิธีในการโจมตียังเป็นข้อมูลหรือความรู้ที่เป็นประโยชน์สำหรับการป้องกันการโจมตีจากฝ่ายตรงกันข้ามได้อย่างมีประสิทธิภาพ



ภาพที่ ๑ CNO components

รูปแบบการปฏิบัติการสงครามไซเบอร์นั้น สามารถจำแนกออกได้เป็น ๓ ประเภทหลัก คือ

การปฏิบัติการใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์ (CNE)

การปฏิบัติการโจมตีเครือข่ายคอมพิวเตอร์ (CNA)

การปฏิบัติการป้องกันเครือข่ายคอมพิวเตอร์ (CND) หรือการป้องกันตนเอง

ทั้ง ๓ ประเภทคือการปฏิบัติการข่าว การปฏิบัติการในเชิงรุก และการป้องกันตนเอง ในการพัฒนาศักยภาพความพร้อม ในการปฏิบัติการสงครามไซเบอร์นั้น แบ่งออกเป็น ๓ ด้าน คือ บุคลากรหรือนักรบไซเบอร์ (Cyberwarrior) อาวุธยุทโธปกรณ์หรืออาวุธไซเบอร์ (Cyberweapon) และการจัดหน่วย (Cyber Unit) ซึ่งจากการศึกษา วรรณกรรมพบว่าเครื่องมือหรืออาวุธไซเบอร์ ส่วนใหญ่สามารถค้นหาและดาวน์โหลดได้จากอินเทอร์เน็ต แต่ก็มีอาวุธไซเบอร์บางประเภทที่ต้องอาศัยการจัดซื้อจากผู้เชี่ยวชาญหรือการสนับสนุนการวิจัยและพัฒนา เช่น ไวรัสสตักซ์เน็ต เป็นต้นทั้งนี้ส่วนที่สำคัญคือการพัฒนาศักยภาพความพร้อมของกำลังพลหรือนักรบไซเบอร์ ซึ่งจากวรรณกรรมนั้นนักรบไซเบอร์ต้องมีการพัฒนา ผ่านการฝึกอบรมอย่างเข้มข้น และควรผ่านการทดสอบเพื่อให้ได้การใบรับรอง (Certificate) ซึ่งขึ้นอยู่กับตำแหน่งและความรับผิดชอบ และสุดท้ายควรมีหน่วยรับผิดชอบเกี่ยวกับการควบคุมสั่งการและประสานการปฏิบัติเพื่อให้เกิดประสิทธิภาพสูงสุด

นอกจากนี้การวิจัยยังพบว่าการปฏิบัติการสงครามไซเบอร์เป็นทั้งส่วนสนับสนุนการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง และเป็นส่วนที่เสริมหรือทวีกำลัง (Force Multiplier) เนื่องจากการปฏิบัติการสงครามไซเบอร์ในเชิงรุกเป็นอีกทางเลือกหนึ่งในการโจมตีเป้าหมายทางทหาร โดยเฉพาะเป้าหมายที่ใช้ระบบคอมพิวเตอร์และเครือข่าย และบางกรณีการโจมตีทางไซเบอร์อาจเป็นหนทางเลือกที่ดีกว่าเนื่องจากไม่ต้องส่งทหารเข้าไปเสี่ยงกับการบาดเจ็บหรือเสียชีวิตในสมรภูมิ หรือบางทีการโจมตีทางไซเบอร์อาจมีต้นทุนหรือค่าใช้จ่ายที่ต่ำกว่าการโจมตีด้วยระเบิดหรืออาวุธยุทโธปกรณ์แบบอื่น ๆยกตัวอย่างเช่น การโจมตีระบบบัญชาการและควบคุม อาจแค่ส่งไวรัสคอมพิวเตอร์เข้าไปในระบบจนทำให้ระบบใช้การไม่ได้ ก็ได้ผลเหมือนกับการส่งเครื่องบินเข้าไปทิ้งระเบิดดาต้าเซ็นเตอร์ของระบบบัญชาการและควบคุม เป็นต้น

แนวทางในการพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ซึ่งมีความจำเป็นที่จะต้องเตรียมการให้พร้อมในองค์ประกอบที่มีความสำคัญ ๓ ด้าน คือ บุคลากร เทคโนโลยีและการจัดการองค์กร (People Process Technology : PPT) เมื่อพิจารณาถึงการเตรียมความพร้อมด้านบุคลากรหรือนักรบไซเบอร์ จะต้องทำให้มั่นใจว่านักรบไซเบอร์มีขีดความสามารถที่พร้อมในการปฏิบัติการสงครามไซเบอร์ โดยเริ่มตั้งแต่การศึกษาและฝึกอบรมอย่างเป็นระบบ โดยพิจารณาจัดให้มีการศึกษาเป็นระดับจากความรู้พื้นฐานที่ต้องมี ทักษะในการปฏิบัติการ และประสบการณ์สำหรับนักรบไซเบอร์ที่พร้อมรบ ส่วนด้านการฝึกจำเป็นที่จะต้องให้นักรบไซเบอร์ได้เกิดทักษะในการปฏิบัติงานสูงสุด จากการใช้สภาพแวดล้อม อาวุธยุทโธปกรณ์ ที่สมจริงมากที่สุด ผ่านกระบวนการในการประเมินผลการปฏิบัติการนำผลมาวิเคราะห์เพื่อการพัฒนาให้เกิดยุทธวิธีที่มีประสิทธิภาพสูงสุด

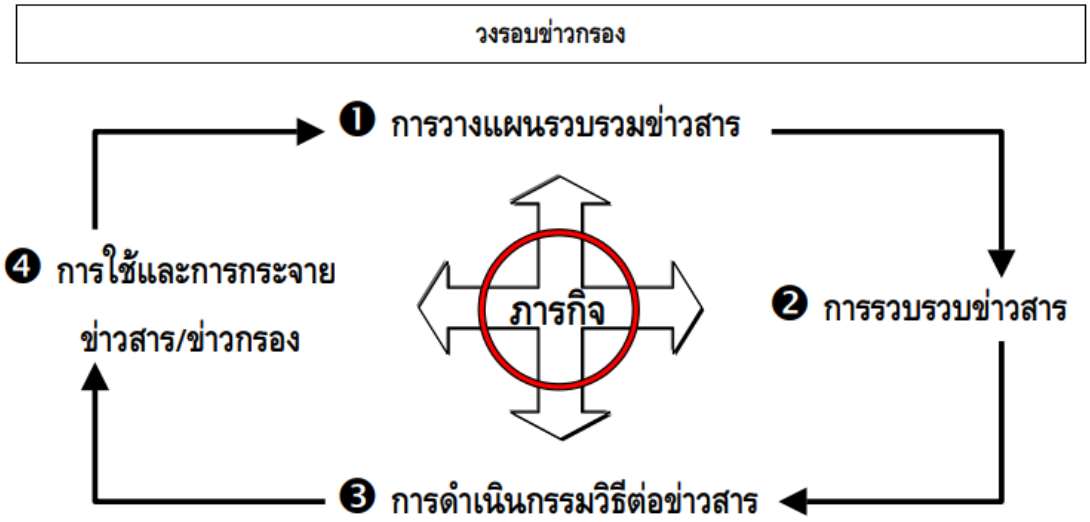
๓.๑ วงรอบข่าวกรองทางไซเบอร์

วงรอบข่าวกรอง คือ การอำนวยการ การรวบรวม การประมวลผล การวิเคราะห์ การเผยแพร่ใช้ประโยชน์ และการเสนอแนะ อ้างอิงจาก The Intelligence Process งานข่าวกรองไซเบอร์ (Cyber Intelligence) มีการปฏิบัติเช่นเดียวกับงานข่าวกรองในมิติอื่น ๆ โดยมีรูปแบบและวงรอบข่าวกรอง

กล่าวคือ การอำนวยการ การรวบรวม การประมวลผล การวิเคราะห์ การเผยแพร่ ใช้ประโยชน์ และการเสนอแนะ ซึ่งหน้าที่และขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ คือ การระบุถึงภัยคุกคามและหนทางปฏิบัติของฝ่ายตรงข้าม การจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์และการจัดทำเป้าหมายทางไซเบอร์เพื่อสนับสนุนการปฏิบัติการ

ไซเบอร์เชิงป้องปรามและการเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment: IPCE) ตัวอย่างการดำเนินการคือการจัดทำแฟ้มบัญชีเป้าหมายทางไซเบอร์เพื่อสนับสนุนข้อมูลในทำเนียบกำลังรบของประเทศตรงข้าม

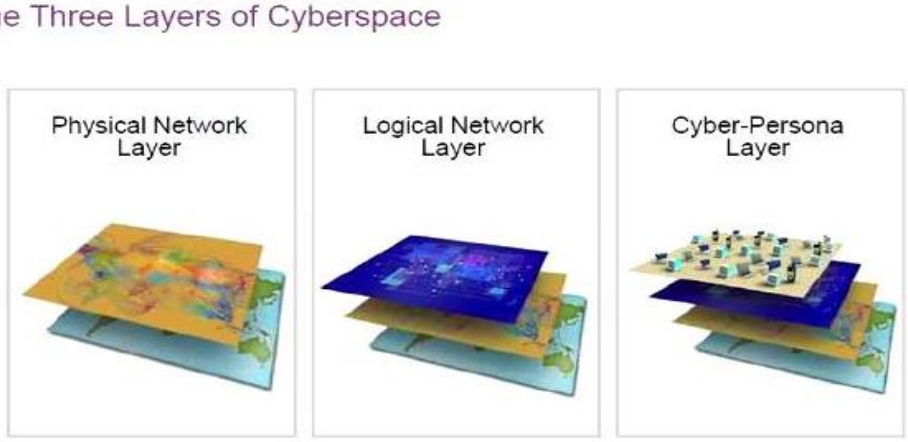
งานข่าวกรองไซเบอร์ (Cyber Intelligence) ถือเป็นกลไกหลักที่มีบทบาทสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วย ซึ่งแนวความคิดในการปฏิบัติด้านการข่าวในมิติของไซเบอร์นั้นเป็นการดำเนินวงรอบข่าวกรอง เช่นเดียวกันกับการปฏิบัติการด้านการข่าวในมิติอื่น ๆ โดยจะต้องดำเนินการทั้งในระดับยุทธวิธี ระดับยุทธการ และระดับยุทธศาสตร์ และจะต้องคัดสรรกำลังพลที่มีความรู้ทั้งในด้านการข่าวและการปฏิบัติการไซเบอร์มาปฏิบัติภารกิจดังกล่าว ซึ่งถือเป็นเรื่องที่ยากลำบาก



ภาพที่ ๒ วงรอบข่าวกรอง

Joint Publication 1 - 13 (R) Cyberspace Operations (5 Feb 2013) ได้กล่าวถึงกระบวนงานข่าวกรองไซเบอร์ ซึ่งมีส่วนสำคัญในการสนับสนุนการปฏิบัติการทางไซเบอร์ทั้งเชิงรับและเชิงรุก และเป็นการดำเนินการร่วมกันทั้งหน่วยข่าวในระดับกลาโหม และหน่วยข่าวระดับชาติทั้งภาครัฐและเอกชน เนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและรวดเร็วกว่าภัยคุกคามทางทหารซึ่งเป็นภัยคุกคามในรูปแบบเดิม ดังนั้นข่าวกรองที่ได้รับจากหลายภาคส่วนจะช่วยในการวิเคราะห์ระบุสิ่งบอกเหตุ เพื่อทำให้ทราบถึงหนทางการปฏิบัติทางไซเบอร์ของฝ่ายตรงข้าม สำหรับการปฏิบัติการด้านการข่าวในมิติของไซเบอร์นั้น เป็นการดำเนินตามวงรอบข่าวกรอง เช่นเดียวกันกับการปฏิบัติการด้านการข่าวในมิติอื่น ๆ การปฏิบัติการข่าวสาร (Information Operations) เรียกย่อ ๆ ว่า Info Ops หรือ IO ซึ่งมาจากการให้คำจำกัดความแตกต่างกันไป ซึ่งมักจะเกิดจากความเข้าใจเอาเองของผู้ปฏิบัติ เช่น ความเข้าใจว่าหมายถึงการปฏิบัติการจิตวิทยา (Psychological Operation) การโฆษณาชวนเชื่อ (Propaganda) การวิเทศสัมพันธ์ทางสื่อมวลชน (Media Relations) หรือการลวงทางทหาร (Deception) เป็นต้น ซึ่งจะดำเนินการทั้งในระดับยุทธวิธี ระดับยุทธการ และระดับยุทธศาสตร์ รวมทั้งการเตรียมสภาพแวดล้อมพื้นที่

ปฏิบัติการทางไซเบอร์เพื่อใช้ในการวางแผนสำหรับการปฏิบัติการไซเบอร์ สำหรับการปฏิบัติการข่าวในมิติทางไซเบอร์จะดำเนินการในทุกระดับชั้น ของมิติทางไซเบอร์ ประกอบด้วย Physical Network Layer, Logical Network Layer และ Cyber-Persona Layer



ภาพที่ ๓ การแบ่งระดับชั้นต่าง ๆ ในมิติไซเบอร์

ที่มา : Joint Publication 3-13 Cyberspace Operations, Online, 2018

กระบวนการวงรอบข่าวกรองในการปฏิบัติการไซเบอร์ ประกอบด้วย

๓.๑.๑ การวางแผนรวบรวมข่าวสาร

๓.๑.๒ การรวบรวมข่าวสาร รวมทั้งการปฏิบัติการเฝ้าตรวจและการลาดตระเวน

๓.๑.๓ กระบวนการประมวลผลข้อมูลและแสวงหาประโยชน์

๓.๑.๔ การวิเคราะห์ข้อมูลและดาเนินกรรมวิธีผลิตข่าวกรอง

๓.๑.๕ การกระจายข่าวกรอง

๓.๑.๖ การประเมินผลคุณภาพและประสิทธิภาพของข่าวกรอง

๓.๒ การประมาณการสถานการณ์ทางไซเบอร์

ในระดับยุทธการ ข่าวกรองไซเบอร์เชิงเทคนิค (Cyber Threat Intelligence : CTI) ใช้ระบุเทคนิค ยุทธวิธี หรืออาวุธทางไซเบอร์ของฝ่ายตรงข้าม ได้แก่ ข้อมูลภัยคุกคาม ไซเบอร์ รวมทั้งขีดความสามารถ (Capabilitiy) โดยนำมาจัดทำเป็นแฟ้มเป้าหมายทางไซเบอร์ (Cyber Threat Target Folder) เพื่อเตรียมการปฏิบัติการไซเบอร์เชิงรุก ส่วนการปฏิบัติการเชิงรับจะให้ความสนใจกับภัยคุกคามไซเบอร์เพื่อเตรียมการระวังป้องกัน เนื่องจากภัยคุกคามไซเบอร์ ซึ่งไม่มีขอบเขตทางภูมิศาสตร์จะเป็นใครก็ได้ทั่วทุกมุมโลก ไม่จำเป็นต้องมีประเด็นขัดแย้งหรือมีพรมแดน ติดกับประเทศไทย เช่น กรณีการปล่อยมัลแวร์เรียกค่าไถ่ WannaCry โดยเกาหลีเหนือ ในส่วนกองทัพอากาศก็ได้รับผลกระทบทั้งที่ไม่ใช่เป้าหมายที่เกาหลีเหนือจะโจมตี เป็นต้น ดังนั้นการป้องกันภัยคุกคามที่เกิดขึ้นจึงเริ่มต้นจากการหาข่าวผู้กระทำภัยคุกคามไซเบอร์ (ATTACK/APT/Malicious) ทั่วโลก ทั้งที่มีรัฐชาติสนับสนุนหรือ กลุ่มองค์กรอิสระ โดยติดตามข่าวสารจาก APT (Advanced Persistent Threat Groups) ที่วิเคราะห์โดยบริษัทด้านการป้องกันภัยคุกคามทางไซเบอร์ขั้นสูง FireEye โดยนำข่าวสารที่ได้มาวิเคราะห์และพิสูจน์ทราบเจตนารมณ์ ขีดความสามารถ รูปแบบการโจมตีของ Threat Actors กลุ่มต่าง ๆ พร้อมกับการสำรวจตนเอง (Self Assessment) เพื่อป้องกันช่องโหว่ของระบบที่อาจถูกโจมตี หรือได้รับผลกระทบจากการโจมตีเหล่านั้น

ภัยคุกคามด้านไซเบอร์นั้นได้ทวีความรุนแรงขึ้นทุกวัน ผู้ก่อการร้ายอาจใช้ประโยชน์จากอาวุธไซเบอร์ ในการก่อวินาศกรรม โดยอาจมุ่งเป้าไปที่การทำลายที่มีผลกระทบในวงกว้าง ได้แก่ การทำให้ระบบโครงข่ายกระแสไฟฟ้าขัดข้อง การโจมตีระบบโครงข่ายสื่อสาร หรือแม้กระทั่งการโจมตีระบบต่าง ๆ ที่ใช้ในด้านการทหาร ก็อาจสามารถเกิดขึ้นได้เช่นกัน และที่สูงขึ้นมาอีกขั้นคือบางประเทศได้พัฒนาศักยภาพในการทำสงครามไซเบอร์ เพื่อให้เป็นการปฏิบัติการที่ควบคู่ไปกับการทำสงครามตามแบบ การปฏิบัติการสงครามไซเบอร์เป็นการทวีกำลัง ทางทหารในการต่อสู้แบบเบ็ดเสร็จกับข้าศึก

กองทัพส่วนใหญ่มียุทธศาสตร์ที่จะปรับเปลี่ยนไปใช้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ซึ่งหัวใจที่สำคัญคือการใช้เทคโนโลยีสารสนเทศและการสื่อสาร แม้เทคโนโลยีจะช่วยทำให้การปฏิบัติการ มีประสิทธิภาพแต่ก็มีช่องโหว่หรือจุดอ่อนที่อาจเป็นช่องทางทำให้ฝ่ายตรงกันข้ามใช้ประโยชน์ได้หรือใช้ทำลายศักยภาพด้านนี้ ดังนั้นรูปแบบการทำสงครามในยุคที่ใช้เครือข่ายเป็นศูนย์กลางนั้นจำเป็นต้องมีการป้องกัน และรักษาความปลอดภัยในระบบต่าง ๆ ที่ใช้ในการปฏิบัติการด้วย และจำเป็นที่ต้องมีศักยภาพในการที่จะทำลายฝ่ายตรงกันข้ามด้วยอาวุธไซเบอร์ได้ด้วย

๓.๓ ระบบสารสนเทศด้านข่าวกรองไซเบอร์

๓.๓.๑ การปฏิบัติการลาดตระเวนทางไซเบอร์ (Cyber ISR)

การปฏิบัติการที่ใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์ หมายถึง การปฏิบัติการเพื่อให้ได้มาซึ่งข้อมูลข่าวสารผ่านเครือข่ายคอมพิวเตอร์ เพื่อค้นหารวบรวมข้อมูลจากระบบเป้าหมายหรือเครือข่ายและระบบของฝ่ายตรงกันข้าม หรืออีกนัยหนึ่งก็คือการปฏิบัติการข่าวบนเครือข่ายคอมพิวเตอร์ ซึ่งเป็นปฏิบัติการที่เกิดขึ้นเป็นประจำบนมิติไซเบอร์ แต่การโจมตีระบบของฝ่ายตรงข้ามนั้นยังไม่มีให้เห็นมากนัก การปฏิบัติการข่าวบนเครือข่ายคอมพิวเตอร์เป็นภารกิจที่ต้องปฏิบัติเป็นประจำ และเป็นสิ่งที่ทำได้ง่ายกว่าบนโลกทางกายภาพ การที่เก็บข้อมูลโดยเฉพาะข้อมูลที่มีชั้นความลับบนระบบคอมพิวเตอร์ ถึงแม้ระบบดังกล่าวอาจจะไม่เชื่อมต่อโดยตรงกับอินเทอร์เน็ต แต่ก็อาจมีช่องทางหรือช่องโหว่ที่แฮกเกอร์อาจเจาะเข้ามาเอาข้อมูลเหล่านี้ได้ ข้อมูลที่ได้จากการปฏิบัติการ CNE นี้อาจถูกใช้ประโยชน์เพื่อเป็นข้อมูลสำหรับการวางแผนโจมตีระบบเป้าหมายได้ในอนาคต หรืออาจเป็นข้อมูลในการวางแผนสำหรับการป้องกันระบบของฝ่ายเราได้

การระบุเป้าหมายหรือการพิสูจน์ทราบตัวตนของแหล่งที่มาของการโจมตีนั้นอาจไม่ใช่เรื่องง่ายบนมิติไซเบอร์ เช่น การโจมตีแบบ (Distributed Denial of Service : DDoS) ที่มีแหล่งที่มาจากประเทศจีนนั้น ไม่ได้หมายความว่ารัฐบาลประเทศจีนอยู่เบื้องหลังเหตุการณ์ดังกล่าว เนื่องจากผู้โจมตีนั้นอาจใช้ประโยชน์จากคอมพิวเตอร์ในประเทศจีนที่มีช่องโหว่และใช้เป็นฐานในการโจมตีระบบอื่นก็เป็นได้ เป็นต้น ดังนั้นการที่จะวิเคราะห์ตัวตนที่แท้จริงของศัตรูนั้นอาจจะต้องวิเคราะห์เป้าหมาย แหล่งที่มา ผู้โจมตี และผู้ให้การสนับสนุนกิจกรรมที่ถูกมอนิเตอร์เหล่านั้น

การปฏิบัติการลาดตระเวนทางไซเบอร์ (Cyber ISR) แบ่งออกเป็น ๓ ประเภท ดังนี้

๓.๓.๑.๑ การข่าวจากแหล่งเปิด (Open Source Intelligence : OSINT)

การข่าวจากแหล่งเปิดเป็นการปฏิบัติการเพื่อให้ได้มาซึ่งข้อมูลข่าวสาร ที่เป็นประโยชน์ โดยจะไม่ทำให้ส่งผลกระทบหรือทำให้ระบบเป้าหมายรับรู้ถึงการถูกมอนิเตอร์อยู่ รูปแบบการปฏิบัติการข่าวแบบ OSINT มีเทคนิค เช่น การเก็บรวบรวมข้อมูลจากระบบสาธารณะไม่ว่าจะเป็นเว็บไซต์หรือสื่อสังคมออนไลน์ (Facebook twitterและYouTube) การวิเคราะห์ข้อมูลที่เกี่ยวข้องกับหน้าที่การ

งาน ได้แก่ ตำแหน่งหน้าที่ ความรับผิดชอบหน่วยงาน การวิเคราะห์ข้อมูลเกี่ยวกับ (Domain Name System : DNS) การแฮ็กค์กูเกิล ข้อมูลที่ได้จากเว็บไซต์และการเก็บรวบรวมข้อมูล metadata จากไฟล์เอกสารประเภทต่าง ๆ เป็นต้น

ในขณะที่ค้นหาข้อมูลนั้นก็จำเป็นที่ต้องปกปิดข้อมูลหรือทำให้ฝ่ายตรงกันข้าม ไม่รู้ว่าเรากำลังปฏิบัติการนี้อยู่ ซึ่งก็สามารถทำได้โดยการใช้ระบบสาธารณะทั่วไป เช่น ระบบ Web-Based เป็นต้น Whois เป็นเครื่องมือสำหรับการค้นหาข้อมูลเบื้องต้นเกี่ยวกับเป้าหมาย เป็นต้น

ส่วนการใช้เครื่องมือสำหรับมอนิเตอร์เครือข่ายในขั้นตอน OSINT นั้นต้องทำด้วยความระมัดระวัง เช่น Passive Network Sniffer ซึ่งเครื่องมือเหล่านี้ถึงแม้ว่าจะไม่ทำให้มีผลกระทบกับข้อมูลที่ส่งผ่านเครือข่าย แต่ก็มีความจำเป็น ที่ต้องเชื่อมต่อทางกายภาพเข้ากับเครือข่าย อย่างไรก็ตามปัจจุบันมีเครื่องมือในการมอนิเตอร์เครือข่ายมากมายที่สามารถแท็พสายสัญญาณโดยที่ไม่ต้องตัดสายหรือทำให้เสียหายทางกายภาพ แม้สายสัญญาณนั้นจะเป็นสายใยแก้วนำแสงก็ตาม ปัจจุบันมีเครื่องมือราคาถูกที่สามารถใช้ดักอ่านข้อมูลจากแสงที่หลุดออกมาจากแจ็กเก็ตของคอร์ของสายไฟเบอร์นั้นได้ และยิ่งในกรณีระบบเครือข่ายแบบไร้สายหรือไวร์เลสแลน (Wireless LAN) ยิ่งเป็นการง่ายเพราะคลื่นนั้นจะแพร่กระจายอยู่บริเวณโดยรอบ เพียงแต่ต้องระมัดระวังว่าจะไม่ไปรบกวนคลื่นเหล่านั้น โดยหลักที่สำคัญคือต้องลดโอกาสที่ฝ่ายตรงกันข้ามรู้ว่าฝ่ายเรากำลังทำอะไรอยู่

๓.๓.๑.๒ การลาดตระเวน (Reconnaissance)

การลาดตระเวน เป็นขั้นตอนต่อไปที่ใช้สำหรับถอดข้อมูลออกมาจากเป้าหมาย แต่ก็ยังคงความเป็นแบบ Passive เมื่อเทียบกับเป้าหมาย ยกตัวอย่างเช่น การแฮ็กเราเตอร์ที่เป็นทางผ่านข้อมูลของระบบเป้าหมาย หลังจากนั้นก็ทำให้เส้นทางข้อมูลอื่นของเป้าหมายใช้ไม่ได้ ทำให้ระบบเป้าหมายนั้นต้องมาใช้เส้นทางข้อมูลที่ต้องผ่านเราเตอร์ที่เราได้ทำการแฮ็กไว้แล้ว ทำให้เราสามารถมอนิเตอร์ทราฟฟิกข้อมูลที่ระบบเป้าหมายส่งเข้าออกได้ซึ่งเป็นข้อมูลเบื้องต้นเกี่ยวกับเป้าหมาย ในการที่จะตัดสินใจทำอย่างอื่นต่อไป ข้อมูลเบื้องต้นนี้ จะช่วยในการเลือกใช้เครื่องมือที่เหมาะสมสำหรับการโจมตีต่อไป การเก็บข้อมูลเบื้องต้นอาจเป็นการสแกนจากอินเทอร์เน็ตโดยที่ ไม่มีข้อมูลใด ๆ เลยเกี่ยวกับเป้าหมาย การสแกนจากเครือข่ายภายใน และท้ายสุดการสแกนจากเครือข่ายที่ไว้วางใจพร้อมทั้งให้สิทธิ์เต็มรูปแบบ โดยการสแกนจากหลาย ๆ ตำแหน่งนี้จะช่วยให้ทราบถึงช่องโหว่ได้จากการปฏิบัติในขั้นตอนนี้จำเป็นที่ต้องใช้เครื่องมือที่หลากหลาย เช่น เครื่องมือที่ใช้สำหรับการเจาะระบบเพื่อควบคุมระบบเครือข่าย, Port Scanner, Vulnerability Analysis Tools, Operating System Fingerprint Tool, Banner Grabbing Tools และ Utility Tools เป็นต้น

อย่างไรมีก็ตามโอกาสที่ข้อมูลเกี่ยวกับระบบฝ่ายเราอาจหลุดออกไปหรือฝ่ายตรงกันข้ามอาจรู้ได้ว่ามีการปฏิบัติการของฝ่ายเราอยู่ ดังนั้นเพื่อป้องกันการที่ฝ่ายตรงกันข้ามจะรู้ว่าเรากำลังทำก็อาจใช้เครื่องมือสำหรับปกปิดแหล่งที่มา โดยการใช้หลายระบบจากหลายแหล่ง เพราะถ้าฝ่ายตรงข้ามรู้ก็อาจโจมตีกลับหรือบล็อกแหล่งที่มาที่โดนจับได้

๓.๓.๑.๓ การเฝ้าตรวจ (Surveillance)

การเฝ้าตรวจซึ่งแตกต่างจากการลาดตระเวน คือการลาดตระเวนนั้นจะเป็นการเฝ้าสังเกตเฉพาะช่วงเวลาใดเวลาหนึ่งเท่านั้น ในขณะที่การเฝ้าตรวจนั้นจะหมายถึงการเฝ้าสังเกตตลอดเวลา ดังนั้นเครื่องมือที่ใช้ในช่วงการลาดตะเวนนั้นก็สามารถใช้ในช่วงนี้ได้เช่นกัน อย่างไรก็ตามการเฝ้าตรวจตลอดเวลานั้นเป็นการเพิ่มความเสี่ยงหรือโอกาสที่จะถูกตรวจจับได้มากขึ้น

การที่จะทำการสแกนแบบไม่รู้ข้อมูลเกี่ยวกับเป้าหมายมาก่อน โดยการสแกนแบบทั้งเครือข่ายนั้น ก็เพื่อให้ทราบว่าเครื่องเป้าหมายนั้นเปิดใช้งานอยู่หรือไม่ โดยปกติจะนิยมใช้การปิง (ICMP Ping) การทดสอบเป้าหมายด้วยการปิงนั้นจะช่วยลดเวลาในการสแกน เนื่องจาก ถ้าหมายเลขไอพีใดไม่ตอบกลับการปิงก็จะไม่ทำการทดสอบอื่น ๆ ต่อกับหมายเลขไอพีนั้น แต่ถ้าไม่ได้เลือกที่จะใช้การปิงทุก ๆ หมายเลขไอพีที่ระบุหรืออยู่ในช่วง ที่กำหนดก็จะถูกทดสอบทั้งหมด แต่ปัญหาที่มักพบเป็นประจำคือการปิงนั้นอาจถูกกรองออกโดยไฟร์วอลล์ หรือเราเตอร์เพื่อป้องกันการค้นพบระบบนั้น และอีกอย่างหนึ่งที่ต้องระวังคือการปิงเป้าหมายแบบทั้งเครือข่ายนั้นอาจถูกจับได้ง่าย เนื่องจากไฟร์วอลล์ (Intrusion Detection System : IDS) อาจตรวจจับได้และเก็บล็อกเกี่ยวกับการปิงนั้นหรืออาจรายงานในทันทีให้ผู้เกี่ยวข้องรับทราบ ดังนั้นการปิงนั้นจะเหมาะสำหรับการสแกนจากเครื่องที่อยู่ในเครือข่ายเดียวกันกับเป้าหมายหรือถ้าทราบว่าไม่มีไฟร์วอลล์ขวางระหว่างระบบเป้าหมายและเครื่องที่สแกน หรืออีกวิธีหนึ่งในการหลบไฟร์วอลล์ก็อาจโดยการใช้การ Telnet ไปยังพอร์ตที่คาดว่าจะเปิด เช่น พอร์ต ๘๐, ๒๕ และ ๒๑ เป็นต้น โดยถ้าระบบใดตอบกลับก็แสดงว่าเครื่องเป้าหมายนั้นเปิดอยู่

เมื่อค้นพบเป้าหมายแล้วขั้นตอนต่อไปคือการค้นหาพอร์ตที่เปิดให้บริการซึ่งทำได้โดยการสแกนพอร์ต ดูเผิน ๆ แล้วการสแกนพอร์ตนั้นเป็นเรื่องธรรมดาหรือง่าย แต่ในความเป็นจริงแล้วเป็นเรื่องที่ค่อนข้างซับซ้อน ยกตัวอย่างเช่น ถ้าพอร์ตนั้นไม่ได้เปิดใช้งานระบบก็จะตอบกลับว่าพอร์ตนั้นไม่ได้เปิด แต่ถ้าเป็นการทดสอบผ่านไฟร์วอลล์ ไฟร์วอลล์ก็อาจจะไม่ส่งข้อความใด ๆ เลย

ข้อมูลที่ต้องมีการแลกเปลี่ยนเมื่อสแกนพอร์ตคือ การซ่อนตัว ความเร็ว และความแม่นยำ สิ่งที่เป็นสาเหตุให้มีการแลกเปลี่ยนกันคือ ประเภทของการสแกนไทม์เอาต์ (Timeout) และพอร์ตอะไรที่จะสแกน ประเภทของการสแกนที่นิยมมากที่สุดคือการสแกนแบบ Connect และ SYN แต่ละอย่างนั้นจะมีข้อแตกต่างเมื่อใช้บิวต์อินสแกนของเนสซัสและใช้ NMAP โดยบิวต์อินสแกนเนอร์นั้นมีค่ากำหนดไม่มากนักแต่ก็ใช้การได้ดี ส่วน NMAP นั้นมีค่าเลือกมากและบางครั้งก็เหมาะสำหรับการสแกนในบางสภาวะแวดล้อม ทั้งนี้ การสแกนแบบ Connect เป็นวิธีที่ง่ายกว่า เพราะมันจะพยายามเชื่อมต่อไปยังพอร์ตที่กำหนดให้จนสำเร็จ และการสแกนแบบนี้ มีโอกาสน้อยมากที่จะทำให้ระบบล่มเนื่องจากเมื่อเชื่อมต่อได้สำเร็จแล้วก็จะทำการยกเลิกการเชื่อมต่อนั้น จึงไม่ใช่วิธีที่อาจถูกจับได้ง่าย และเป็นวิธีที่เร็ว

การสแกนแบบ SYN นั้นค่อนข้างจะปลอดจากการถูกจับได้และยากที่จะป้องกันได้เนื่องจากเป็นการเชื่อมต่อแบบไม่สมบูรณ์ โดยการสแกนแบบนี้จะส่งแพ็กเก็ตเพื่อร้องขอการเชื่อมต่อไปยังพอร์ต แต่จะไม่ยอมทำการแฮนด์เชค (TCP Handshake) ให้สมบูรณ์ หรือไม่ส่งแพ็กเก็ต ACK กลับไปให้เป้าหมาย ทำให้พอร์ตนั้น เปิดรอจนกว่าเวลาไทม์เอาต์หมดเอง วิธีนี้จะใช้การได้ดีกับการสแกนตรง ๆ และการสแกนผ่านไฟร์วอลล์ และที่บอกว่าการสแกนแบบนี้นั้น จึงมีโอกาสที่จะถูกจับได้น้อยเพราะการสแกนแบบนี้จะดูเหมือนว่าเป็นการพยายาม เชื่อมต่อที่ล้มเหลว ดังนั้นก็จะไม่มีการแจ้งเตือนใน IDS หรือไฟร์วอลล์ แต่ถ้ามีการเก็บล็อกอย่างละเอียด เหตุการณ์นี้อาจถูกบันทึกไว้ในล็อกไฟล์ แต่ก็เป็นการยากที่จะวิเคราะห์และสรุปได้ว่าเป็นการโจมตีระบบ

ที่ผ่านมาได้กล่าวถึงแต่การสแกนพอร์ตของ TCP การสแกนพอร์ตของ UDP ก็ทำได้เช่นกัน แต่ช่องโหว่ของ UDP นั้นมีน้อยกว่า และการสแกนพอร์ตของ UDP นั้นจะค่อนข้างยุ่งยากกว่าและใช้เวลามากกว่า ดังนั้นโดยส่วนใหญ่จะไม่ค่อยนิยมสแกน UDP พอร์ต

อีกประเด็นหนึ่งที่สำคัญคือตำแหน่งที่วางสแกนเนอร์ เช่น ถ้าต้องการสแกนเครื่องอินเทอร์เน็ตเซิร์ฟเวอร์ เช่น เว็บเมล์ หรือ DNS ควรสแกนเครื่องเหล่านี้ตรง ๆ โดยที่ไม่มีไฟร์วอลล์กั้น

และถ้าต้องการสแกนเครือข่ายภายในก็ควรวางสแกนเนอร์ไว้ในเครือข่าย และอย่าลืมสแกนไฟร์วอลล์หรืออุปกรณ์ในระบบการรักษาความปลอดภัยด้วย เป็นต้น

ทั้งนี้ เวลาในการสแกนนั้นอาจเป็นสาเหตุหนึ่งที่อาจทำให้ถูกจับได้ กล่าวคือ ยิ่งถ้าใช้เวลาในการสแกนมากก็ยิ่งทำให้โอกาสที่จะถูกจับได้มากขึ้น แต่ข้อดีของการสแกนที่ใช้เวลานานก็จะได้ผลที่แน่นอนมากขึ้น การสแกนผ่านไฟร์วอลล์หรือเครือข่ายที่ช้าอาจใช้เวลานาน การใช้เวลาน้อยในการสแกนก็อาจพลาดการตอบกลับจากพอร์ตที่ช้าเนื่องจากอาจเป็นเพราะเครือข่ายที่ช้า เวลาที่ใช้ในการสแกนนั้นก็ขึ้นอยู่กับรายละเอียดหรือข้อมูลเพิ่มที่ต้องการ ถ้าระบบมีความสำคัญมากก็ควรให้เวลาเต็มที่เพื่อที่จะค้นหาช่องโหว่หรือจุดอ่อนให้ได้มากที่สุด เพื่อจะได้ไม่เกิดปัญหาหรือเกิดความเสียหายกับระบบในภายหลัง

ผนวก

การปฏิบัติการข่าวกรองไซเบอร์จากหน่วยงานด้านไซเบอร์ของ USAF

กำหนดความต้องการในการป้องกันและรับมือกับภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ คือ การสร้าง ขีดความสามารถข่าวกรองไซเบอร์ ทั้งนี้การที่งานด้านการข่าวกรองไซเบอร์จะสามารถสร้างความตระหนักรู้สถานการณ์ให้แก่ฝ่ายเราทราบก่อนที่ภัยคุกคามต่าง ๆ จะทำการโจมตีนั้น จำเป็นต้องทราบและสามารถระบุสภาพแวดล้อมของการปฏิบัติการให้ได้ก่อน และเมื่อทราบถึงคุณลักษณะสำคัญและผลกระทบของสภาพแวดล้อม การปฏิบัติการที่มีต่อฝ่ายเราแล้ว งานด้านการข่าวจะทราบว่าภัยคุกคามหรือศัตรูของฝ่ายเรานั้น คือใครมีจุดมุ่งหมายอะไร มีขีดความสามารถ และมีหนทางปฏิบัติอย่างไร

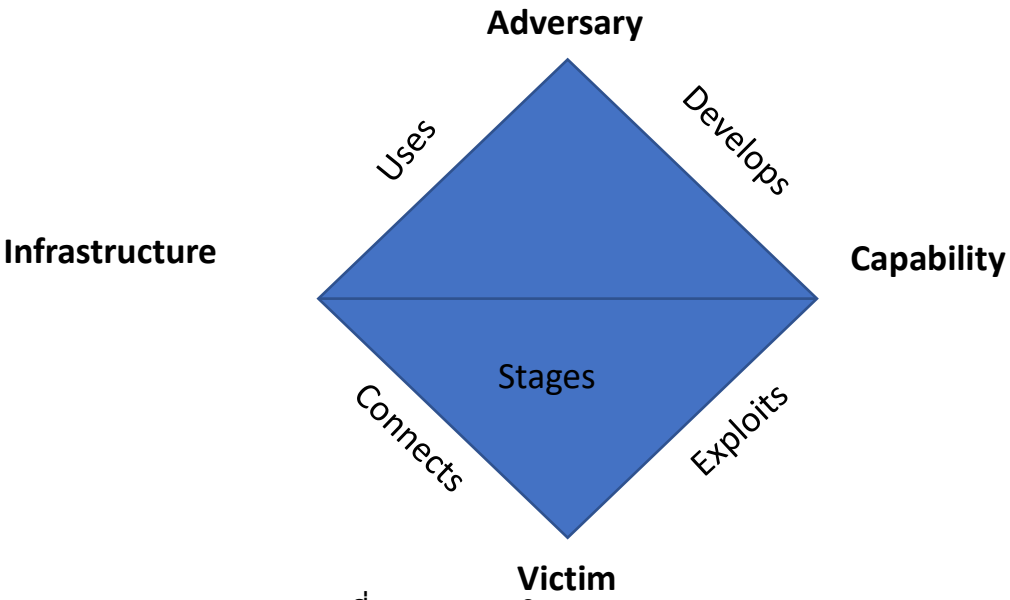
USAF ได้ใช้กรอบแนวคิด ‘Diamond model’ เพื่อช่วยจำแนกสิ่งที่ต้องการและดำเนินการตรวจสอบการเข้าควบคุมเครื่องเป้าหมายของ USAF โดยใช้ข้อมูลการค้นพบเพื่อสร้างข่าวกรองไซเบอร์และใช้ประโยชน์จากข้อมูลดังกล่าวเพื่อช่วยในการสอบสวนต่อไป ‘Diamond model’ เป็นกรอบแนวคิดเพื่อสร้างตัวบ่งชี้

ฝ่ายตรงข้าม – ผู้โจมตี, เป้าหมาย

โครงสร้างพื้นฐาน – คอมพิวเตอร์ โดเมน บัญชี ที่ถูกบุกรุกซึ่งใช้เป็นพร็อกซี ฯลฯ

ขีดความสามารถ – ชุดเครื่องมือ วิธีการ

เหยื่อ – ตัวชี้วัดของการถูกเข้าควบคุมเครื่อง,เป้าหมายสอดคล้องกับดำเนินการเตรียมสภาพแวดล้อมพื้นที่ปฏิบัติการทางไซเบอร์



ภาพที่ ๔ กรอบแนวคิด ‘Diamond model’

ที่มา: United States Air Force Cyberspace Threat Intelligence Process Overview

- การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE)
- ติดตาม ประเมินสถานการณ์ ระบุถึงภัยคุกคาม และแจ้งเตือนฝ่ายให้เราทราบ (การสร้างความตระหนักรู้สถานการณ์ (Situation Awareness : SA)
- รวบรวมข้อมูลข่าวสารและเหตุการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำมาจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงบุคคลหรือกลุ่มบุคคลที่เฝ้าระวังทั้งภายในและภายนอกประเทศ
- จัดเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation Of The Cyber Environment : IPCE) ซึ่งประกอบด้วย ๔ ขั้นตอน ดังนี้

๑. การระบุสภาพแวดล้อมของการปฏิบัติการ (Determine The Operational Environment)

๒. การระบุถึงสิ่งที่ส่งผลกระทบต่อสภาพแวดล้อมของการปฏิบัติการ (Determine Influences On The Environment)

๓. การระบุตัวภัยคุกคาม (Determine The Threat Actors)

๔. การระบุถึงแผนการหรือหนทางปฏิบัติของภัยคุกคาม (Determine The Threat Scenarios)

- การวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้ามหรือภัยคุกคาม เพื่อใช้สำหรับการวางแผนการปฏิบัติการไซเบอร์
- จัดทำเป้าหมายทางไซเบอร์ เมื่อจำเป็นต้องใช้มาตรการตอบโต้เชิงรุกต่อฝ่ายตรงข้ามหรือภัยคุกคาม

การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ เป็นกระบวนการวิเคราะห์อย่างต่อเนื่อง และเป็นระบบมุ่งเน้นการศึกษาและทำความเข้าใจกับสภาพแวดล้อม ของพื้นที่ปฏิบัติการในมิติทางไซเบอร์ ระบุถึงขีดความสามารถและหนทางปฏิบัติของฝ่ายตรงข้าม โดยมีลักษณะสภาพแวดล้อมที่แตกต่างจากพื้นที่ปฏิบัติการอื่น ๆ นอกจากนี้การรวบรวมข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ หรือการรวบรวมและแบ่งปันข่าวกรองภัยคุกคามไซเบอร์ ถือเป็นอีกกระบวนการหนึ่งที่จะทำให้การจัดทำฐานข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ประสบผลสำเร็จ

ผลงานวิจัยที่เกี่ยวข้อง

นาย Jay Mcallister ได้ทำการศึกษาเรื่องการประยุกต์กระบวนการคิดเชิงวิพากษ์ เพื่อนำมาใช้กับ งานข่าวกรองไซเบอร์ สรุปว่านักวิเคราะห์ในทุกระดับควรอุทิศเวลาให้กับการพัฒนาวิธีการคิด โดยการลงลึกไปถึงกระบวนการทำงานของจิตใจมนุษย์ เพื่อปรับปรุงทักษะการวิเคราะห์ ซึ่งผู้วิจัยพบว่า หลักวิธีเช่นนี้ไม่ต่างกับการวิเคราะห์ข่าวกรองชนิดอื่น ๆ

นาย Robert M. Lee ทำการศึกษางานข่าวกรองไซเบอร์เพื่อบรรยายในหลักสูตรบัณฑิตศึกษา ด้านความมั่นคงและปลอดภัยทางไซเบอร์ สรุปว่าขั้นตอนแรกในการเข้าใจงานข่าวกรองไซเบอร์ คือ การเข้าใจวงรอบข่าวกรองทั้งในด้านยุทธวิธี เทคนิค และขั้นตอนการปฏิบัติ ซึ่งการดำเนินการข่าวกรองประเภทต่าง ๆ มีอยู่นานก่อนที่จะเกิดงานข่าวกรองไซเบอร์ โดยเฉพาะด้านการตัดสินตกลงใจทางทหารที่ ผู้บังคับบัญชา ต้องการทราบเจตนารมณ์ของฝ่ายตรงข้ามเพื่อเลือกยุทธศาสตร์

ที่ดีกว่าในสนามรบหรือ เตรียมตัวให้พร้อมสำหรับการโจมตี รวมถึงการป้องกันอย่างเหมาะสม เพราะฉะนั้นการเริ่มศึกษาข่าวกรองไซเบอร์สามารถเริ่มได้จากการศึกษาแนวทางข่าวกรองทหาร

เครือข่าย Intelligence and National Security Alliance ระบุว่า ข่าวกรองไซเบอร์ คือ การประเมินขีดความสามารถ เจตนารมณ์ และกิจกรรมของข้าศึก ในห้วงมิติทางไซเบอร์ (Cyber Domain) เพื่อสนับสนุนการแจ้งเตือน การโจมตี และการป้องกันภัยคุกคาม ซึ่งเป็นผลผลิตที่ได้จากการดำเนิน วงรอบข่าวกรองโดยมีขีดความสามารถที่จำเป็น ได้แก่

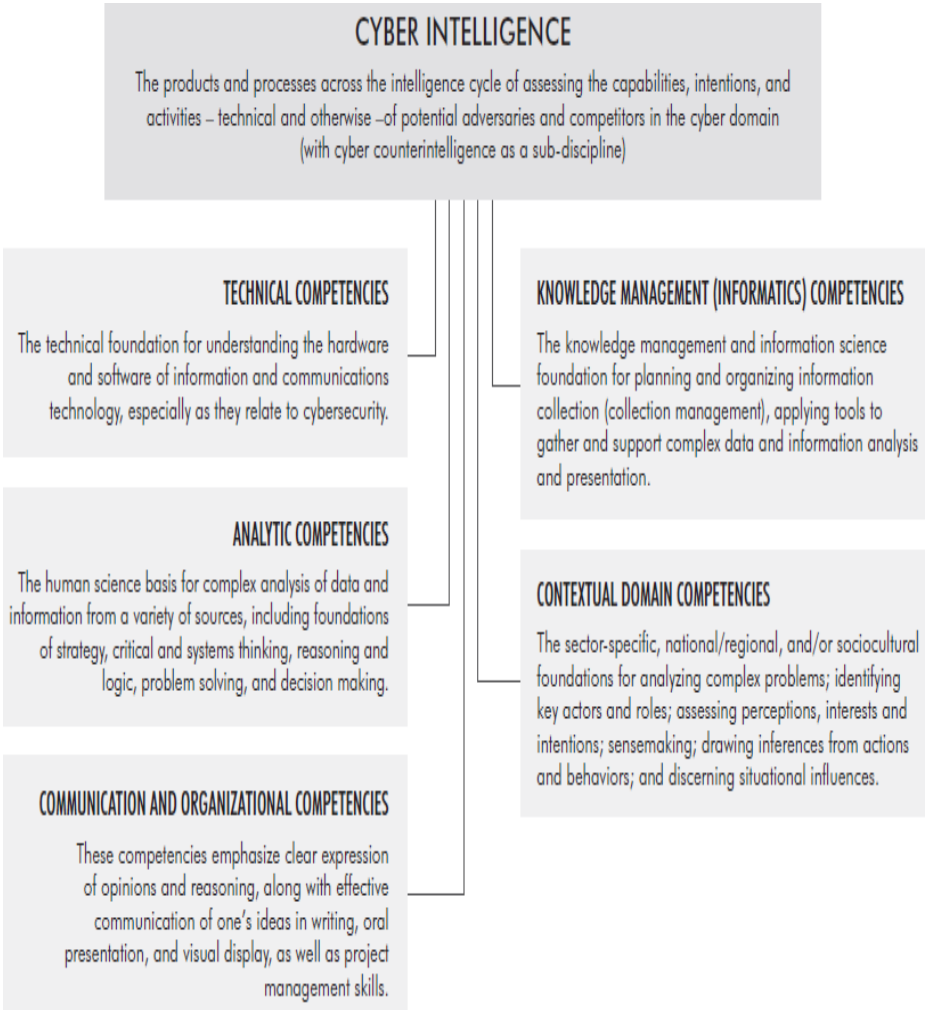
๑. ความเข้าใจในเรื่องของระบบฮาร์ดแวร์ ซอฟต์แวร์ ระบบสารสนเทศและการสื่อสาร

๒. ทักษะการคิดวิเคราะห์

๓. การนำเสนอ รายงาน ให้ความเห็นที่เป็นเหตุเป็นผล

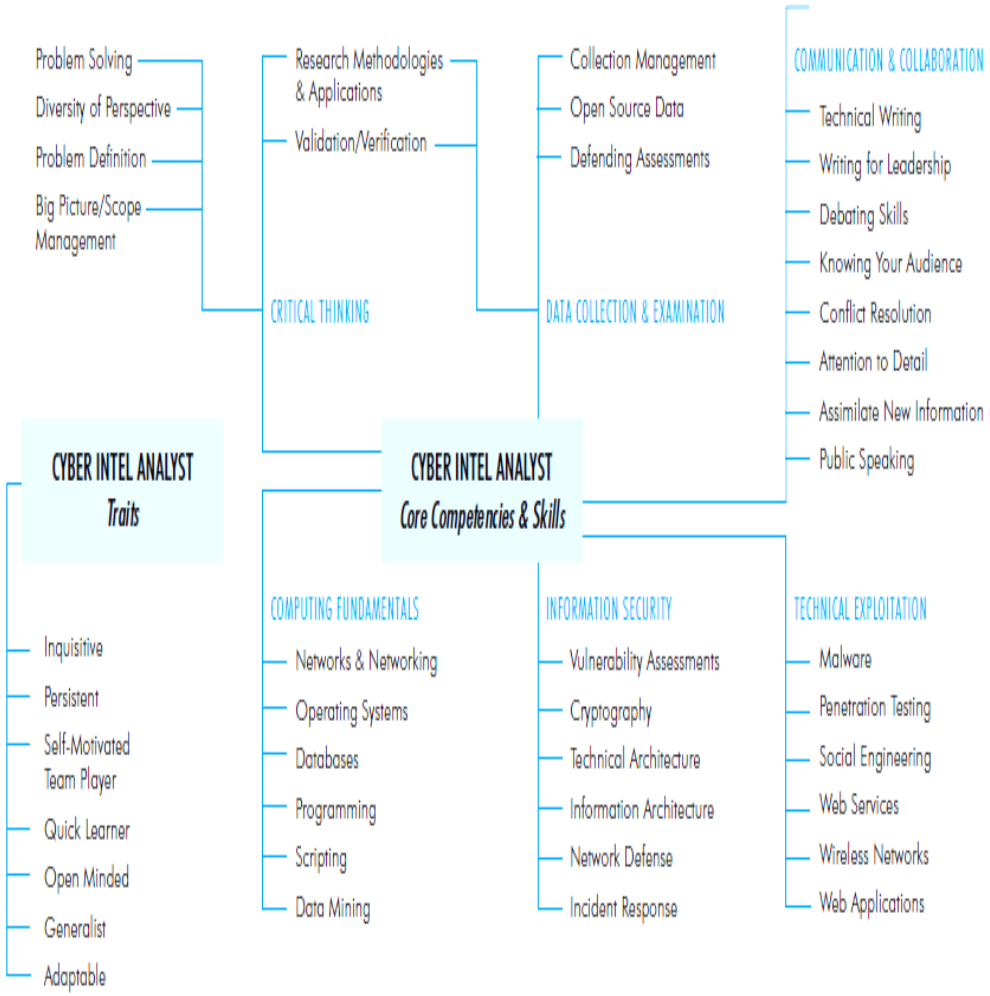
๔. การบริหารจัดการวางแผนรวบรวมข้อมูลข่าวกรอง

๕. ความเข้าใจในภารกิจ และบริบทของหน่วยงาน เช่น ผู้แสดงหลักและกลุ่มผลประโยชน์ เป็นต้น



ภาพที่ ๕ ขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์

ที่มา : CTI –EU | Bonding EU Cyber Threat Intelligence ENISA, Online, 2017



ภาพที่ ๖ ขีดความสามารถและทักษะที่จำเป็นของนักวิเคราะห์ข่าวกรองทางไซเบอร์
ที่มา : Information Security Education Carnegie Mellon University, Online, 2017

หลักนิยมการปฏิบัติการไซเบอร์ของกองทัพอากาศ ประกอบกับแนวทางข่าวกรองไซเบอร์ในกองทัพอากาศปัจจุบัน

แนวคิดการปฏิบัติการไซเบอร์ ทอ.

ปฏิบัติการไซเบอร์เชิงรับ ระวังป้องกันและตรวจจับการบุกรุก สืบค้นจุดอ่อนและช่องโหว่ในระบบไซเบอร์ของฝ่ายเรา รวมทั้งการสำรองและกู้คืนระบบกรณีถูกโจมตีทางไซเบอร์จากฝ่ายตรงข้าม

ปฏิบัติการไซเบอร์เชิงรุก เพื่อดักรับข้อมูลการใช้งานทางไซเบอร์ การก่อกวนระบบคอมพิวเตอร์ จำกัดเสรีภาพในการใช้งาน และทำให้เครื่องคอมพิวเตอร์แม่ข่ายปฏิเสธการให้บริการหรือหยุดการทำงาน รวมถึงสามารถ จารกรรมข้อมูลของฝ่ายตรงข้ามได้ในระดับหนึ่ง โดยระวังป้องกันและรักษาความปลอดภัยระบบสารสนเทศของหน่วยและระบบ ให้ปฏิบัติตามระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๖๕ หรือฉบับที่มีผลบังคับใช้อย่างเคร่งครัด

ปฏิบัติการข่าวกรองไซเบอร์ มีเป้าหมายเพื่อ วางแผน รวบรวม วิเคราะห์ ข่าวกรองเพื่อสนับสนุน การปฏิบัติการทั้งเชิงรุกและเชิงรับเพื่อให้ประสบความสำเร็จในการปฏิบัติการเชิงรับ

การปฏิบัติการข่าวกรองไซเบอร์ในกองทัพอากาศในปัจจุบัน ประกอบด้วย

- เรื่องของภัยคุกคาม (Threat) สามารถระบุและตรวจสอบได้ว่าภัยคุกคามคือใคร ทราบถึงขีดความสามรถ และหนทางปฏิบัติของภัยคุกคาม
- การรวบรวมข่าวสาร (Collection) เมื่อเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (IPCE) แล้วจะทำให้ทราบว่ายังขาดข้อมูลข่าวสาร/ข่าวกรองใดที่กระทบต่อการวิเคราะห์ภัยคุกคาม และทำให้สามารถรวบรวมข้อมูลข่าวสาร/ข่าวกรองในพื้นที่ปฏิบัติการได้อย่างเหมาะสม
- การกำหนดเป้าหมาย (Targeting) เมื่อทราบถึงคุณลักษณะสำคัญของสภาพแวดล้อมการปฏิบัติการและภัยคุกคามแล้ว จะทำให้การกำหนดเป้าหมายเพื่อตอบโต้ภัยคุกคามที่ทำการโจมตี ฝ่ายเรานั้น ทำได้ง่ายขึ้น และตรงตามเจตนารมณ์ของผู้บังคับบัญชา

การดำเนินงานด้านข่าวกรองไซเบอร์ของกองทัพอากาศในปัจจุบันจะเป็นการประสานความร่วมมือระหว่างกรมข่าวทหารอากาศ และศูนย์ไซเบอร์กองทัพอากาศ โดยกรมข่าวทหารอากาศมีหน้าที่ติดตามสถานการณ์ภัยคุกคามไซเบอร์ในระดับยุทธศาสตร์ และส่งข้อมูลให้ศูนย์ไซเบอร์กองทัพอากาศดำเนินการ ข่าวกรองไซเบอร์

วิเคราะห์ข่าวกรองไซเบอร์ในกองทัพอากาศในปัจจุบันเพื่อหาแนวทางที่เหมาะสมสำหรับการพัฒนา ขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ

จากการวิเคราะห์ข้อมูลพบว่าข่าวกรองไซเบอร์ (Cyber Intelligence) เป็นกลไกสำคัญโดยงานข่าวกรองไซเบอร์ แบ่งออกเป็น ๓ ระดับ คือ ข่าวกรองยุทธศาสตร์ ข่าวกรองยุทธการ และข่าวกรองยุทธวิธี และต้องใช้บุคลากร ที่เชี่ยวชาญทั้งในด้านงานข่าวกรองและด้านการปฏิบัติการไซเบอร์ ทั้งนี้ การดำเนินงานข่าวกรองไซเบอร์ของกองทัพอากาศในปัจจุบัน ยังไม่มีหลักนิยมหรือแนวความคิดในการปฏิบัติที่ชัดเจน การดำเนินงานจึงเป็น ลักษณะของการประสานความร่วมมือแลกเปลี่ยนหรือสนับสนุนข้อมูล ระหว่างหน่วยงานด้านการข่าวกับหน่วยไซเบอร์เป็นหลัก โดยหน่วยข่าวส่วนใหญ่จะสนับสนุนข้อมูลข่าวกรองยุทธศาสตร์เพื่อแจ้งเตือนให้ทราบถึงสถานการณ์หรือเบื้องหลังเหตุการณ์การโจมตีทางไซเบอร์ ส่วนหน่วยไซเบอร์จะเป็นผู้ดำเนินการข่าวกรองยุทธการ และข่าวกรองยุทธวิธีเอง เนื่องจากมีความเชี่ยวชาญด้านเทคโนโลยีที่ใช้ในการรวบรวมข่าวสารและการวิเคราะห์ ภัยคุกคามไซเบอร์

- เพื่อช่วยในการระบุแหล่งที่มา ทำให้หาแหล่งที่มาจากการเชื่อมต่อกับเครือข่ายภายนอกและตรวจสอบช่องโหว่โครงสร้างพื้นฐานวิกฤตของ ทอ. เพื่อปรับปรุงกระบวนการป้องกันภัยคุกคามทางไซเบอร์
- กำหนดขอบเขต/กำหนดการตอบสนองภัยคุกคาม
- จัดเก็บข้อมูลในระบบจัดเก็บข้อมูลด้านการข่าวกรองด้านการปฏิบัติการในมิติไซเบอร์ของข้าศึก
- จัดทำบัญชีเป้าหมายทางไซเบอร์ โดยเฉพาะเป้าหมายภายในระบบโครงสร้างพื้นฐานวิกฤต และเป้าหมาย ที่มีความอ่อนไหว หรือมีความสำคัญทางยุทธศาสตร์ของฝ่ายตรงข้าม
- ส่งข่าวกรองทางไซเบอร์ให้ส่วนปฏิบัติการตอบโต้เพื่อให้บรรลุเป้าหมายตามคำสั่งที่ได้รับ

คำนิยามศัพท์

คำจำกัดความด้านไซเบอร์

เพื่อให้เกิดความเข้าใจในแนวทางที่สอดคล้องกัน และเพื่อความสะดวกในการอ้างอิงสำหรับการศึกษาและใช้เป็นกรอบในการดำเนินการด้านสงครามไซเบอร์ของ ทอ. จึงได้กำหนดคำจำกัดความหรือคำนิยามศัพท์ด้านไซเบอร์ ดังนี้

๑. การกระทำโดยรัฐ (State Actor) หมายถึง การปฏิบัติในมิติไซเบอร์ใบลักษณะที่เป็นภัยคุกคาม โดยมีรัฐให้การสนับสนุนหรือสั่งการ

๒. การกระทำที่มิได้ดำเนินการโดยรัฐ (Non-state Actor) หมายถึง การปฏิบัติในลักษณะที่เป็น ภัยคุกคาม โดยปราศจากการสนับสนุนหรือสั่งการจากรัฐ

๓. การตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Audit) หมายถึง การตรวจสอบการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยไม่กำหนดวิธีการหรือขั้นตอนที่จะดำเนินการตรวจสอบ เพื่อให้ได้ผลการตรวจสอบตามความเป็นจริง

๔. การโจมตีทางไซเบอร์ (Cyber Attack) หมายถึง การโจมตีต่อฝ่ายตรงข้ามโดยมีวัตถุประสงค์เพื่อขัดขวาง (Disrupt) ทำลาย (Destroy) หรือควบคุม (Control) การใช้งานมิติไซเบอร์ของฝ่ายตรงข้าม รวมถึงการทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลของฝ่ายตรงข้ามด้วย

๕. การทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการให้บริการ (Distributed Denial of Service : DDoS) หมายถึง การขัดขวางหรือก่อกวนระบบเครือข่ายหรือ Server จนทำให้ทรัพยากรของเครื่องเป้าหมายที่ถูกโจมตีหมดไป หรือเครือข่ายนั้น ๆ ไม่สามารถทำงานได้ตามปกติ

๖. การรับรองความสามารถด้านไซเบอร์ทางทหาร (Cyber Defense Certification) หมายถึง ระบบการพัฒนาขีดความสามารถของนักรบไซเบอร์ ประกอบด้วยการทดสอบความสามารถทางไซเบอร์ด้านทฤษฎีและปฏิบัติ ซึ่งจำเป็นต่อการปฏิบัติงานในมิติไซเบอร์ โดยแบ่งเป็นระดับที่แตกต่างกันตามขอบเขตความรับผิดชอบและลักษณะงาน เพื่อให้กระทรวงกลาโหมมีนักรบไซเบอร์ที่เพียงพอทั้งในเชิงปริมาณและเชิงคุณภาพ ตามมาตรฐานของกระทรวงกลาโหม

๗. การหลอกลวงทางอินเทอร์เน็ต (Phishing) หมายถึง การล่อลวงทางอินเทอร์เน็ตชนิดหนึ่งที่พยายามหลอกผู้ใช้งาน โดยการสร้างอีเมล หรือหน้าเว็บไซค์ปลอมขึ้นมาเพื่อหวังผลในการให้ผู้ใช้งานเกิดความสับสน และทำธุรกรรมต่าง ๆ บนเว็บไซต์ปลอมที่ถูกสร้างขึ้นนั้น โดยข้อมูลต่าง ๆ ที่ผู้ใช้งานได้กรอกบนหน้าเว็บไซค์ปลอมเหล่านี้ จะถูกดักข้อมูลและบันทึกไว้เพื่อใช้ในการปลอมแปลง และเข้าถึงข้อมูลของผู้เสียหายโดยที่ไม่ได้รับอนุญาต ส่วนการหลอกลวงแบบเจาะจงเป้าหมาย (Spear Phishing) คือ รูปแบบการหลอกลวงของข้อความอีเมลที่เฉพาะเจาะจง ซึ่งอาจดูเสมือนว่านายจ้าง หรือเพื่อนร่วมงานส่งข้อความอีเมลให้คนในองค์กร

๘. การสืบสวนทางไซเบอร์ (Cyber Forensics/Computer Forensics) หมายถึง กระบวนการสกัดข้อมูลข่าวสารจากคอมพิวเตอร์และสื่อบันทึกข้อมูลแบบดิจิทัล เพื่อให้ได้มาซึ่งหลักฐานทางดิจิทัล เพื่อใช้ในการดำเนินคดีด้านอาชญากรรมไซเบอร์

๙. การแสวงประโยชน์จากช่องโหว่ (Exploitation) หมายถึง การนำเทคนิคการปฏิบัติในมิติไซเบอร์ มาดำเนินการกับช่องโหว่ หรือใช้ช่องโหว่เป็นทางผ่าน เพื่อให้เกิดผลตามที่ต้องการ

๑๐. ความตระหนักรู้ทางไซเบอร์ (Cyber Awareness, Cyberspace Domain Awareness) หมายถึง ความเข้าใจอย่างถูกต้องเกี่ยวกับสภาวะแวดล้อมและภัยคุกคามในมิติไซเบอร์ ในห้วงเวลาหนึ่งหรือตามห้วงเวลาที่ต้องการ มีความเกี่ยวข้องตั้งแต่ระดับบุคคล องค์กร ซึ่งสามารถส่งผลกระทบต่อความมั่นคงของชาติหรือผลประโยชน์แห่งชาติ

๑๑. ความพร้อมในการรับมือทางไซเบอร์ (Cyber Resilience) หมายถึง ความสามารถในการรับมือและฟื้นฟูกลับคืนสู่สภาพปกติโดยเร็วที่สุด หลังจากการถูกโจมตีทางไซเบอร์

๑๒. ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง หลักการ มาตรการ กระบวนการ แนวทางปฏิบัติ เพื่อปกป้องมิติไซเบอร์จากการโจมตีทางไซเบอร์ มักใช้ในบริบทด้านพลเรือน

๑๓. โครงสร้างพื้นฐานวิกฤตของ ทอ. (RTAF Critical Infrastructure) หมายถึง ระบบสาธารณูปโภคที่สำคัญยิ่งสำหรับการปฏิบัติในมิติไซเบอร์ หากถูกโจมตีทางไซเบอร์หรือแสวงประโยชน์จาก ช่องโหว่จะเกิดผลเสียหายร้ายแรงต่อความสำเร็จของการปฏิบัติภารกิจของ ทอ.เช่น ระบบควบคุมบังคับบัญชา ระบบฐานข้อมูลข่าวกรอง ระบบสนับสนุนการตัดสินใจทางยุทธศาสตร์ ระบบสื่อสารโทรคมนาคม ระบบสื่อสารทางยุทธวิธี ระบบป้องกันทางอากาศ เป็นต้น

๑๔. โครงสร้างพื้นฐานวิกฤตของชาติ (National Critical Infrastructure) หมายถึง ระบบสาธารณูปโภคที่สำคัญยิ่งของรัฐ ซึ่งใช้ระบบสารสนเทศในการควบคุมการปฏิบัติงาน มักใช้ในการให้บริการประชาชน เช่น ระบบการจ่ายกระแสไฟฟ้า ระบบการบริหารจัดการน้ำ ระบบบริการด้านการเงิน ระบบการให้บริการอินเทอร์เน็ต ระบบการสื่อสารทั้งภาคพื้นดินและดาวเทียม ระบบกิจการวิทยุและโทรทัศน์ ระบบการขนส่งมวลชน ระบบควบคุมการจราจรทางบกและทางอากาศ เป็นต้น

๑๕. ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่อง ซึ่งถูกนำมาใช้เพื่อให้ได้ผลตามที่ต้องการ

๑๖. ไซเบอร์ (Cyber) หมายถึง สิ่งที่เกี่ยวข้องหรือสัมพันธ์กับอินเทอร์เน็ต ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ระบบควบคุมกำกับดูแลและเก็บข้อมูล (Supervisory Control and Data Acquisition : SCADA) ระบบควบคุมการทำงานของอุปกรณ์อิเล็กทรอนิกส์ (Embedded Systems) เป็นต้น

๑๗. นักรบไซเบอร์ (Cyber Warrior) หมายถึง บุคคลหรือกลุ่มบุคคลซึ่งปฏิบัติงานในมิติไซเบอร์ โดยเน้นการปฏิบัติในลักษณะการโจมตีทางไซเบอร์ หรือแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม ประกอบด้วยผู้ปฏิบัติงานด้านนโยบาย/ยุทธศาสตร์ รวมทั้งผู้ปฏิบัติงานเชิงเทคนิค

๑๘. โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูลบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Browser แบ่งออกได้หลากหลายประเภท เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger) ดังนี้

๑๘.๑ ไวรัส (virus) หมายถึง โปรแกรมที่สามารถติดต่อจากอีกไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกัน หรือจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น สามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล

๑๘.๒ เวิร์ม (worm) หมายถึง โปรแกรมที่สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่น ๆ ผ่านทางเครือข่ายเวิร์ม สามารถทำอันตรายให้กับระบบ

๑๘.๓ โทรจัน (Trojan) หมายถึง โปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตราย แต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์หรือทำลายระบบที่ทำงานโดยโปรแกรมนี้ส่วนใหญ่จะถูกแนบมากับจดหมายอิเล็กทรอนิกส์

๑๘.๔ การแอบดักจับข้อมูล (Spyware) หมายถึง โปรแกรมที่ถูกออกแบบมาให้คอยติดตาม บันทึกข้อมูลส่วนบุคคล รายงานข้อมูลการใช้งานของผู้ใช้แต่ละคนบนอินเทอร์เน็ต หรือทำการเปลี่ยนการตั้งค่าของโปรแกรมบราวเซอร์ใหม่ ซึ่งก่อให้เกิดความรำคาญและทำให้ประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ช้าลง

๑๘.๕ คีย์ล๊อกเกอร์ (Key Logger) หมายถึง สปายแวร์ประเภทหนึ่งที่ทำหน้าที่บันทึกข้อมูลการกดแป้นคีย์บอร์ดของผู้ใช้ ข้อมูลที่จัดเก็บจะถูกส่งผ่านอินเทอร์เน็ต เพื่อใช้ก่ออาชญากรรมในรูปแบบต่าง ๆ ได้

๑๙. มิติไซเบอร์ (Cyberspace) หมายถึง มิติที่มีการประยุกต์ใช้หลักการด้านอิเล็กทรอนิกส์และหลักการด้านสเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) ในการจัดเก็บ แก้ไข หรือแลกเปลี่ยนข้อมูลบนโครงสร้างพื้นฐานทางกายภาพ

๑๙.๑ อิเล็กทรอนิกส์ (Electronics) หมายถึง หลักการที่เกี่ยวข้องกับการออกแบบวงจรไฟฟ้า (Circuits) โดยใช้ทรานซิสเตอร์ (Transistors) และไมโครชิป (Microchips) รวมไปถึงหลักการที่เกี่ยวข้องกับพฤติกรรมและการเคลื่อนที่ของอิเล็กตรอนในสารกึ่งตัวนำ (Semiconductor) ตัวนำ (Conductor) สุญญากาศหรือก๊าซ

๑๙.๒ สเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) หมายถึง หลักการที่เกี่ยวข้องกับช่วงหรือแถบคลื่นแม่เหล็กไฟฟ้าซึ่งมีความยาวที่แตกต่างกัน ใช้ในด้านการสื่อสารโทรคมนาคมแบบต่าง ๆ ตามคุณสมบัติของแต่ละช่วงคลื่น

๑๙.๓ การปฏิบัติในมิติไซเบอร์ (Cyberspace Operations) หมายถึง การดำเนินการโดยใช้ขีดความสามารถทางไซเบอร์ในมิติไซเบอร์ เพื่อให้บรรลุวัตถุประสงค์ที่ตั้งไว้

๒๐. ยุทธภัณฑ์ทางไซเบอร์ (Cyber Weapon) หมายถึง ระบบชุดของยุทโธปกรณ์ หรือชุดคำสั่ง ทางคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ซึ่งใช้ในการโจมตีทางไซเบอร์หรือแสวงประโยชน์จากช่องโหว่ ในมิติไซเบอร์ของฝ่ายตรงข้าม

๒๑. สงครามไซเบอร์ (Cyberwarfare) หมายถึง การปฏิบัติในมิติไซเบอร์ซึ่งมีมูลเหตุหรือวัตถุประสงค์ทางการเมืองหรือทางทหาร โดยนำเทคนิคการปฏิบัติในมิติไซเบอร์มาใช้ป้องกัน รวมทั้งโจมตีหรือแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม

๒๒. เหตุคุกคามทางไซเบอร์ (Cyber Incident) หมายถึง เหตุการณ์ (Event) ที่ไม่เป็นไปตามนโยบายหรือมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจบ่งบอกถึงการถูกโจมตีทางไซเบอร์ หรือการถูกแสวงประโยชน์จากช่องโหว่ ได้แก่ ความพยายามเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

(Unauthorized Access) เหตุการณ์ขัดขวางหรือทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ (Disruption or Denial of Service) หรือเหตุการณ์พยายามเปลี่ยนแปลงข้อกำหนดทางเทคนิคของระบบสารสนเทศ เป็นต้น

๒๓. ระบบคลาวด์ภาครัฐ (Government Cloud : G-Cloud) หมายถึง โครงสร้างพื้นฐานบนอินเทอร์เน็ต แบบใช้ทรัพยากรร่วมกัน โดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) หรือ อีจีเอ ให้บริการแก่หน่วยงานภาครัฐด้วยเทคโนโลยี Cloud ซึ่งเก็บทรัพยากรไว้ บนอินเทอร์เน็ตสามารถเรียกใช้งานผ่านเครือข่าย ได้ตลอดเวลาจากระยะไกล ปรับขนาดได้ตามความต้องการของผู้ใช้ มีการจัดสรรทรัพยากร ลดภาระการบริหารจัดการและมีความมั่นคงปลอดภัยสูง

เอกสารอ้างอิง

ภาษาไทย

พลอากาศตรี พงษ์สวัสดิ์ จันทสาร.(๒๕๖๑). “การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร”

สหรัฐฯ ประกาศภาวะฉุกเฉินหลัง บ.ท่อส่งน้ำมันรายใหญ่โดนมัลแวร์เรียกค่าไถ่โจมตี,สืบค้นเมื่อ ๒๕๖๕ https://www.bbc.com/thai/international-57052951

แฮ็กโรงพยาบาล-รีดค่าไถ่ เรียกถึง 6.3 หมื่นล้านบาท, ๑๐ ก.ย. ๒๕๖๓, สืบค้นเมื่อ ๒๕๖๕ https://www.thairath.co.th/news/local/central/1926912

สรุปผลการตรวจสอบเหตุการณ์ข้อมูล Username/Password ทอ.รั่วไหล”(๒๕๖๓).

“หลักนิยมการปฏิบัติการไซเบอร์”(๒๕๖๓).(๒๕๖๐).“36กลยุทธ์ของซุนวูรู้เขารู้เรา”. สามารถเข้าถึงเมื่อ ๒๕๖๔,

“พบเกาหลีเหนืออาจพัวพันเหตุมัลแวร์โจมตีทั่วโลก ” .(๒๕๖๐). สืบค้นเมื่อ ๒๕๖๕, https://www.bbc.com/thai/international-39931940

ภาษาอังกฤษ

“Joint Publication 3-12 cyberspace operations” ,(2018). accessed 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/.

“Joint Publication 2-0 joint intelligence”,(2013).accessed 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

SCOTT JASPER.(2020) “RUSSIAN CYBER OPERATIONS”

“Cyber Security”.accessed 2021, http://www.rdpb.go.th/MediaUploader/File/10166/ CyberSecurity