แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพบก

โดย

พลตรี นิพัฒน์ เล็กฉลาด
ผู้อำนวยศูนย์ไซเบอร์กองทัพบก
กองทัพบก

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕
ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ – ๒๕๖๖

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก” ลักษณะวิชา การทหาร ของ พลตรี นิพัฒน์ เล็กฉลาด เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕ ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ – ๒๕๖๖

พลโท

(ชาติชาย ชัยเกษม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก

ลักษณะวิชา การทหาร

ผู้วิจัย พลตรี นิพัฒน์ เล็กฉลาด **หลักสูตร** วปอ. **รุ่นที่** ๖๕

กองทัพบกในฐานะหน่วยงานด้านความมั่นคงของประเทศ มีภารกิจสำคัญในการป้องกันภัยคุกคามในทุกรูปแบบ ปัจจุบันขั้นตอนการรวบรวมข้อมูล การจัดเก็บข้อมูล และการดำเนินกรรมวิธีข้อมูลด้านการข่าวกรองและข่าวสารต่าง ๆ ยังขาดการบูรณาการร่วมกัน เนื่องจากกองทัพบกยังไม่มีกระบวนการแลกเปลี่ยนข้อมูลข่าวกรองจากแหล่งข่าวเปิด ที่เรียกว่า Open-Source Intelligence หรือ OSINT ร่วมกับหน่วยงานรัฐทั้งในประเทศและต่างประเทศ งานวิจัยฉบับนี้ มีวัตถุประสงค์ ๑. เพื่อศึกษาและวิเคราะห์กระบวนการข่าวกรองแบบเปิด (OSINT) ในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อนำไปสู่การปฏิบัติจริง และ ๒. เพื่อจัดทำข้อเสนอแนะแนวทางการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก ว่าด้วยการข่าวกรองแบบเปิด โดยผู้วิจัยได้ทำการคัดเลือกผู้ทรงคุณวุฒิ จำนวน ๖ ท่าน โดยใช้วิธีการวิจัย ๒ วิธี คือ ๑. การวิจัยเอกสาร และ ๒. การวิจัยเชิงคุณภาพ จากผลการวิจัย พบว่า ประเทศสหรัฐฯ มีความเป็นรูปธรรมมากที่สุดในฐานะเป็นต้นแบบของงาน OSINT ทั่วโลก ส่วนประเทศไทยยังไม่มีการกล่าวถึงกรอบการพัฒนาระบบการข่าวกรองแบบเปิดที่ชัดเจน โดยผลการวิเคราะห์อธิบายได้ว่า กระบวนการข่าวกรองแบบเปิด (OSINT Process) เป็นส่วนหนึ่งของวงรอบข่าวกรอง (Intelligence Cycle) และมีขั้นตอนที่คล้ายกัน นอกจากนี้ จำเป็นต้องพิจารณาตามแนวคิด ๓ เสาหลักของความมั่นคงปลอดภัยไซเบอร์ ได้แก่ บุคลากร กระบวนการ และเทคโนโลยี การวิจัยครั้งนี้ มีข้อเสนอแนะแนวทางการพัฒนาระบบข่าวกรองแบบเปิด ประกอบด้วย ๑. ข้อเสนอแนะเชิงนโยบาย โดยจัดทำเกณฑ์การประเมินขีดความสามารถด้านไซเบอร์ สำหรับ OSINT แบ่งได้ ๕ ระดับ ๒. ข้อเสนอแนะเชิงกลยุทธ์ และ ๓. ข้อเสนอแนะเชิงปฏิบัติ โดยได้การออกแบบ ๔ แนวทางในการพัฒนาฯ คือ แนวทางที่ ๑ ประยุกต์ใช้ Pure OSINT แนวทางที่ ๒ ประยุกต์ใช้ Open source ร่วมกับซื้อโปรแกรมแบบเสียค่าบริการประเภท Enterprise/ Premium แนวทางที่ ๓ ประยุกต์ใช้ Pure OSINT ร่วมกับการพัฒนาระบบฯ ขึ้นใช้เอง และแนวทางที่ ๔ จัดหาซอฟต์แวร์เชิงพาณิชย์ (Commercial Software) อย่างไรก็ตาม ยังต้องตระหนักถึงการรักษาความปลอดภัยในการปฏิบัติการ และจริยธรรมไซเบอร์ด้วย

Abstract

Title Guidelines on the Development of the Open-Source Intelligence (OSINT) in Support of Cybersecurity of the Royal Thai Army.

Field Military

Name Major General Nipat Lekchalard **Course** NDC **Class** 65

The Royal Thai Army (RTA), as the agency mainly responsible for national security, has a major duty in preventing threats. At present, the procedures for collecting information and any operations concerning intelligence and information still lack mutual integration since the RTA does not have any established procedures to exchange information and intelligence from the open source or Open-Source Intelligence (OSINT) in collaboration with the government agencies, both domestic and abroad. Therefore, the objectives of this research shall be as follows: 1. to study and analyze OSINT in determining cybersecurity policy with the aim of actual practice and 2. to propose recommendations regarding the guidelines on establishing the RTA's cybersecurity of OSINT. The research has employed two research methods: 1. document research and 2. qualitative research. According to the results, the United States has the most concrete model of OSINT compared to other countries. In contrast, Thailand has not set any clear OSINT framework. In addition, the OSINT process is a part of the Intelligence Cycle and has similar procedures. Besides, the concept of 3 major cybersecurity pillars, personnel, procedures and technology, must be considered. This research has proposed guidelines on the development of OSINT, which consist of 1. policy recommendations by establishing the criteria for cyber competency assessment for OSINT, which shall be divided into 5 levels, 2. strategic recommendations and 3. practical recommendations. There are 4 development guidelines as follows: the first guideline is to apply Pure OSINT, the second guideline is to apply Open Source, coupled with the purchase of paid programs with Enterprise/Premium type, the third guideline is to apply Pure OSINT with system development and the fourth guideline is to procure the Commercial Software. Nonetheless, this shall also consider an awareness of operational security and cyber ethics.

คำนำ

เอกสารวิจัย เรื่อง แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก จัดทำขึ้นโดยได้แรงบันดาลใจจากประสบการณ์การทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) และได้สังเกตว่า กองทัพบกยังไม่มีกระบวนการแลกเปลี่ยนข้อมูลข่าวกรองจากแหล่งข่าวเปิด ที่เรียกว่า Open-Source Intelligence หรือ OSINT ร่วมกับหน่วยงานรัฐทั้งในประเทศและต่างประเทศ ผู้วิจัยจึงเห็นว่า การศึกษาวิจัยนี้จะสามารถเสนอแนวทางการพัฒนาระบบข่าวกรองแบบเปิด ของกองทัพบก เพื่อนำไปสู่การปฏิบัติจริงทั้งในการแก้ปัญหาทางไซเบอร์ในระยะสั้น และระยะยาว รวมถึงสามารถประยุกต์ใช้ข้อมูลจากแหล่งข่าวแบบเปิด (OSINT) เป็นเครื่องมือในการวางแผน ตรวจสอบ และวิเคราะห์สถานการณ์ต่าง ๆ เพื่อรับมือกับภัยคุกคามรูปแบบใหม่ที่จะส่งผลกระทบต่อความมั่นคงของชาติต่อไป

พลตรี
(นิพัฒน์ เล็กฉลาด)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๕
ผู้วิจัย

กิตติกรรมประกาศ

ในนามของผู้วิจัย ขอขอบพระคุณคณะกรรมการและที่ปรึกษางานวิจัยที่ได้กรุณาให้คำแนะนำ และข้อคิดเห็นทางวิชาการที่เป็นประโยชน์อย่างยิ่งในการใช้เป็นกรอบแนวทางในการจัดทำเอกสารวิจัยส่วนบุคคลฉบับนี้ ให้มีความสมบูรณ์ นอกจากนี้ ผู้วิจัยขอขอบพระคุณท่านผู้ทรงคุณวุฒิทุกท่าน และคณาจารย์วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ที่มีส่วนในการสนับสนุนสำคัญในระหว่างการจัดทำเอกสารวิชาการฉบับนี้ ผู้วิจัยขอขอบคุณเจ้าหน้าที่ของวิทยาลัยป้องกันราชอาณาจักรทุกท่าน ที่ให้ความอนุเคราะห์เอื้อเฟื้อสถานที่ และทรัพยากรที่จำเป็นแก่การจัดทำเอกสาร รวมทั้ง การให้ความช่วยเหลือในการให้คำแนะนำรูปแบบและการตรวจทานเอกสารต้นฉบับให้มีความสมบูรณ์มาก และหวังเป็นอย่างยิ่งว่า งานวิจัยฉบับนี้ จะได้รับการนำไปปฏิบัติอย่างเป็นรูปธรรมในประเทศของเรา เพื่อให้เกิดผลสำเร็จเป็นประโยชน์ต่อประเทศชาติบ้านเมืองต่อไปในอนาคตอันใกล้นี้

พลตรี
(นิพัฒน์ เล็กฉลาด)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๕
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันปัญหาการสู้รบโดยใช้กำลังทางทหารระหว่างประเทศลดลง แต่การเผชิญภัยคุกคามรูปแบบใหม่กลับเพิ่มขึ้น ซึ่งส่งผลกระทบต่อความมั่นคงทั้งระดับประเทศและทุกมิติในสังคม ทำให้กำลังอำนาจทหารมีภารกิจอื่น ๆ ทั้งการพัฒนาประเทศและช่วยเหลือประชาชน โดยสภาความมั่นคงแห่งชาติ (สมช.) ได้กำหนด “ภัยคุกคามต่อความมั่นคงของชาติ” ไว้ ๒ ทาง คือ ๑) ภัยคุกคามจากภายใน ซึ่งเป็นปัญหาทางด้านการเมืองภายในประเทศ ได้แก่ ปัญหาเศรษฐกิจ ปัญหาพื้นที่ด้อยพัฒนา ปัญหาชายแดน ปัญหาทางด้านสังคมและจิตวิทยา ปัญหาทรัพยากรและสิ่งแวดล้อม และ ๒) ภัยคุกคามจากภายนอก ได้แก่ ปัญหาความขัดแย้งของสังคมโลก ปัญหากลุ่มประเทศมุสลิม ปัญหาความสัมพันธ์กับประเทศเพื่อนบ้าน เป็นต้น นอกจากนี้ สมช. ได้กำหนดประเภทของภัยคุกคามรูปแบบใหม่ (Non-Traditional Threat) ไว้ ๙ ประเภท โดยเมื่อพิจารณาแล้วมีประเด็นที่เกี่ยวข้องกับภารกิจของกองทัพบก (ทบ.) อยู่ ๔ เรื่อง ได้แก่ ประเด็นที่ ๑ ความมั่นคงในพื้นที่ ๓ จังหวัดชายแดนภาคใต้ เป็นปัญหาความมั่นคงทั้งการก่อเหตุของกลุ่มแนวร่วมการจัดกิจกรรมเชิงสัญลักษณ์และการสร้างวาทกรรม ในแถลงการณ์ต่าง ๆ เพื่อให้บรรลุเป้าหมาย ขณะที่การสนับสนุนกลุ่มเคลื่อนไหว และการลงพื้นที่เพื่อพบปะกับองค์กรภาคประชาสังคม เจ้าหน้าที่ฝ่ายความมั่นคง และผู้เกี่ยวข้องกับการก่อเหตุ เพื่อรับทราบข้อมูลและสถานการณ์ในพื้นที่ขององค์กรต่างชาติจะเอื้อต่อการเคลื่อนไหวของกลุ่มก่อความไม่สงบ และทำให้ความมั่นคงในพื้นที่จังหวัดชายแดนภาคใต้ยังคงยืดเยื้อ ประเด็นที่ ๒ การก่อการร้ายและอาชญากรรมข้ามชาติ การที่กลุ่มก่อการร้าย เช่น กลุ่ม Al Qaeda และกลุ่ม Islamic State (IS) ยังมีความเคลื่อนไหวและรักษาอุดมการณ์อย่างเหนียวแน่น โดยมีปัจจัยสนับสนุนการก่อเหตุจากความขัดแย้งทางการเมือง ศาสนา ชาติพันธุ์ รวมถึงความขัดแย้งตามภูมิภาคต่างๆ ทำให้การก่อการร้าย รวมถึงอาชญากรรมทางไซเบอร์ (Cybercrime) ประเด็นที่ ๓ แรงงานต่างด้าวและผู้หลบหนีเข้าเมือง โดยผู้หลบหนีเข้าเมืองส่วนใหญ่มาจากประเทศเพื่อนบ้านที่มีแนวชายแดนติดกับไทยรวมถึงประเทศใกล้เคียง ในอนาคตประเทศไทยจะยังประสบปัญหาแรงงานต่างด้าวและผู้หลบหนีเข้าเมืองจากปัจจัยต่าง ๆ เช่น ความต้องการแรงงาน ขบวนการค้ามนุษย์ การลักลอบนำคนเข้าเมือง ความต้องการใช้ไทยเป็นทางผ่านไปประเทศที่สาม เป็นต้น และประเด็นที่ ๔ ยาเสพติด ได้แพร่ระบาดอย่างรวดเร็วผ่านช่องทางออนไลน์ และการขนส่งทางพัสดุ โดยไม่จำกัดพื้นที่ ส่วนการที่สามเหลี่ยมทองคำเป็นแหล่งผลิตยาเสพติดที่สำคัญของโลก ทำให้ไทยประสบปัญหาทั้งการเป็นตลาดและทางผ่านลำเลียงยาเสพติดไปยังประเทศที่สาม เช่น ไอซ์ เฮโรอีน กัญชา เป็นต้น

จากสถานการณ์ดังกล่าว พบว่า กองทัพบก (ทบ.) ในฐานะหน่วยงานด้านความมั่นคงของประเทศ จึงมีภารกิจสำคัญในการป้องกันภัยคุกคามรูปแบบใหม่ ซึ่งจากการประเมินสภาพแวดล้อม ปัญหาและอุปสรรคขององค์กรเบื้องต้น พบว่า ขั้นตอนการรวบรวมข้อมูล การจัดเก็บข้อมูล และการดำเนินกรรมวิธีข้อมูลด้านการข่าวกรองและข่าวสารต่าง ๆ ภายในกองทัพบก ยังขาดการบูรณาการการใช้งานข้อมูลข่าวกรองร่วมกัน (Silo-Based) เนื่องจาก ทบ. ยังไม่มีการกำหนดหรือประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy) ด้านข้อมูลที่ชัดเจน รวมถึง ทบ. ยังไม่มีกระบวนการแลกเปลี่ยนข้อมูลข่าวกรองแบบเปิด (Open-Source Intelligence: OSINT) กับหน่วยงานภาครัฐทั้งในประเทศและต่างประเทศอย่างเป็นทางการ นอกจากนี้ พบว่า ประเทศไทยยังขาดการกำหนดแนวทางการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่เป็นรูปธรรม ประกอบกับยังไม่มีแนวทางในการแลกเปลี่ยนข้อมูลข่าวกรองแบบเปิด (OSINT) ระหว่างหน่วยงานด้านความมั่นคง และภาคเอกชน รวมถึงหน่วยงานต่างประเทศ

ดังนั้น จึงเป็นที่มาของงานวิจัยฉบับนี้ ที่มุ่งศึกษาค้นคว้าหาแนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก รวมถึงการประยุกต์ใช้การข่าวกรองแบบเปิดเป็นเครื่องมือในการวางแผน ตรวจสอบ และวิเคราะห์สถานการณ์ต่าง ๆ เพื่อรับมือกับภัยคุกคามรูปแบบใหม่ที่จะส่งผลกระทบต่อความมั่นคงของชาติ

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาและวิเคราะห์กระบวนการข่าวกรองแบบเปิด (Open-Source Intelligence: OSINT) ในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อนำไปสู่การปฏิบัติจริงทั้งในการแก้ปัญหาทางไซเบอร์ในระยะสั้น และระยะยาว

๒. เพื่อจัดทำข้อเสนอแนะแนวทางการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก ว่าด้วยการข่าวกรองแบบเปิด

ขอบเขตของการวิจัย

๑. ขอบเขตด้านเนื้อหา

การวิจัยนี้เน้นการวิจัยเฉพาะเรื่องการข่าวกรองแบบเปิด กระบวนการแลกเปลี่ยนข้อมูลข่าวกรองแบบเปิดระหว่างหน่วยงานภาครัฐภายในประเทศและต่างประเทศ ที่มีผลกระทบต่อความมั่นคงของชาติ

๒. ขอบเขตด้านประชากร

กลุ่มเป้าหมายที่จะดำเนินการศึกษา คือ กลุ่มผู้บริหารระดับสูง ผู้ทรงคุณวุฒิที่มีประสบการณ์การทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือนักวิชาการที่มีบทบาทในการกำหนดนโยบายในระดับประเทศ เพื่อขอทราบความคิดเห็นเชิงนโยบายเกี่ยวกับการกำหนดยุทธศาสตร์ ว่าด้วยการข่าวกรองแบบเปิด พร้อมคำแนะนำในการแลกเปลี่ยนข้อมูลข่าวกรองแบบเปิดระหว่างหน่วยงานของประเทศไทย เพื่อนำมาประกอบในการอภิปรายผล

๓. ขอบเขตด้านเวลา

เริ่มการศึกษาวิจัยตั้งแต่วันที่ ๑ พฤศจิกายน พ.ศ. ๒๕๖๕ จนถึงวันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๖

วิธีดำเนินการวิจัย

งานวิจัยเรื่อง แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพบก ผู้วิจัยใช้ระเบียบวิธีในการศึกษาเชิงคุณภาพ (Qualitative Research) เพื่อศึกษา วิเคราะห์ กระบวนการ รูปแบบ และลักษณะของการข่าวกรองแบบเปิดของประเทศไทยและต่างประเทศ รวมถึงปัจจัยที่เกี่ยวข้องอื่น ๆ ที่มีผลต่อการกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ โดยจะทำการเก็บข้อมูลจากการศึกษาเอกสาร (Document Study) ร่วมด้วย โดยมีรายละเอียดดังนี้

๑. การรวบรวมข้อมูล

๑.๑ เครื่องมือในการเก็บข้อมูล

๑.๑.๑ การศึกษาเชิงคุณภาพ (Qualitative Research)

เพื่อเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ (Key informants) ได้แก่ ผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ และนักวิชาการ ที่มีประสบการณ์การทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือมีหน้าที่รับผิดชอบในการกำหนดนโยบายและมาตรการต่างๆ ของประเทศไทย เพื่อแลกเปลี่ยนความคิดเห็นแบบเป็นทางการ (Structured interview or formal interview) เกี่ยวกับประเด็นที่กำลังศึกษา

๑.๑.๒ การศึกษาเอกสาร (Document Study)

มีการศึกษาเอกสารในการเก็บข้อมูล เพื่อใช้เป็นข้อมูลทุติยภูมิประกอบการวิเคราะห์ เช่น ยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑-๒๕๘๐) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และงานวิจัยอื่น ๆ ที่เกี่ยวข้อง เป็นต้น

๑.๒ ประชากรและกลุ่มตัวอย่าง

ประชากรที่เป็นกลุ่มเป้าหมายในการศึกษาครั้งนี้ ประกอบด้วย ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ หรือผู้ทรงคุณวุฒิของกองทัพบก และนักวิชาการ ซึ่งผู้วิจัยได้ทำการเลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) จำนวน ๖ ท่าน

๒. การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลที่ได้จากการศึกษา เมื่อรวบรวมข้อมูลจากการศึกษาเชิงคุณภาพ (Qualitative Research) และการศึกษาเอกสาร (Document Study) เป็นที่เรียบร้อยแล้ว จากนั้นจะทำการตรวจดูความครบถ้วนสมบูรณ์ของข้อมูล โดยนำมาวิเคราะห์ตามกรอบแนวคิดในการศึกษา

๓. การนำเสนอข้อมูล

นำเสนอข้อมูลและสรุปผลการศึกษาโดยใช้รูปแบบการพรรณนานำมาอธิบายเชื่อมโยงกับกรอบแนวคิดและงานวิจัยที่เกี่ยวข้อง และนำเสนอแนวคิดใหม่ ๆ ที่ได้จากการวิจัย

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบถึงกระบวนการข่าวกรองแบบเปิด (Open-Source Intelligence: OSINT) ซึ่งจะช่วยให้มีทิศทางในการดำเนินด้านการข่าวกรองแบบเปิด ของประเทศไทย

๒. ได้ข้อเสนอแนะในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก ว่าด้วยการข่าวกรองแบบเปิด และโครงสร้างของหน่วยงานที่รับผิดชอบหลัก

คำจำกัดความ

การข่าวกรองแบบเปิด หมายถึง การรวบรวมและวิเคราะห์ข้อมูลที่รวบรวมจากแหล่งสาธารณะ หรือแหล่งเปิด หรือแหล่งเปิดบนอินเตอร์เน็ต และโซเชียลมีเดีย ส่วนใหญ่ให้บริการฟรีและมีประสิทธิภาพมาก ดังนั้น OSINT จึงถูกนำมาใช้ในขั้นตอนการสำรวจเพื่อวางแผนการป้องกันการโจมตีทางไซเบอร์ เช่น การโจมตีแบบฟิชชิง (Phishing) วิศวกรรมสังคม (Social Engineering) เป็นต้น

บทที่ ๒
การทบทวนวรรณกรรม และงานวิจัยที่เกี่ยวข้อง

งานวิจัย เรื่อง “แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก” ผู้ศึกษาได้ทำการศึกษาตามแนวคิดทฤษฎีและทบทวนวรรณกรรม รวมทั้งงานวิจัยอื่น ๆ ที่เกี่ยวข้อง เพื่อกำหนดกรอบแนวคิดที่จะใช้ในการศึกษา ดังนี้

๑. แนวคิดเกี่ยวกับภัยคุกคาม

๒. แนวคิดและทฤษฎีเกี่ยวกับการข่าวกรอง

๓. กระบวนการข่าวกรองแบบเปิด

๔. นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยข่าวกรองแบบเปิดของต่างประเทศ

๕. แนวคิดและทฤษฎีในการพัฒนาระบบข่าวกรองแบบเปิด

๖. งานวิจัยที่เกี่ยวข้อง

๗. กรอบแนวคิดของการวิจัย

๘. สรุป

แนวคิดเกี่ยวกับภัยคุกคาม

ความหมายของภัยคุกคาม

ได้มีผู้ให้ความหมายเกี่ยวกับภัยคุกคามไว้หลากหลาย ดังนี้

พจนานุกรมอิเล็กทรอนิกส์ ฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๔๒ (ออนไลน์) ให้ความหมายของคำว่า คุกคาม หมายถึง การแสดงอำนาจด้วยกิริยาหรือวาจาให้หวาดกลัว ทำให้หวาดกลัว ได้แก่ ภัยคุกคาม

เจษฎา มีบุญถือ (๒๕๕๓ : ๒๗) ได้นิยามคำว่า ภัยคุกคาม คือ การกระทำอันจะเป็นอันตราย หรือสั่นคลอนต่อความมั่นคงของชาติในทุก ๆ ด้าน

วิทยาลัยป้องกันราชอาณาจักร (ออนไลน์) นิยามว่า ภัยคุกคาม (Threat) พฤติการณ์ที่คาดคะเนได้ว่าจะก่อให้เกิดความเสียหาย มีผลให้ฝ่ายที่ถูกคุกคามต้องกระทำหรือละเว้นการกระทำอย่างใดอย่างหนึ่ง ภัยคุกคามจะมีความสำคัญเพียงใด ย่อมขึ้นอยู่กับความนึกคิดของทั้งผู้คุกคาม และผู้ถูกคุกคาม ความนึกคิดดังกล่าวขึ้นอยู่กับความรู้สึกว่า ผู้คุกคามมีเครื่องมือพอ หรือมีศักย์กำลังอำนาจพอที่ดำเนินการให้บังเกิดผลตามที่ต้องการจะคุกคามได้หรือไม่ ขึ้นอยู่ที่เจตนาในการพิจารณาภัยคุกคามนั้น ความยากอยู่ที่การหยั่งเจตนาของประเทศที่คุกคาม กล่าวคือ แม้ประเทศที่คุกคามจะมีเครื่องมือที่จะใช้ดำเนินการ แต่ก็หากที่จะรู้ได้ว่าจะใช้เครื่องมือที่มีอยู่หรือไม่ ฉะนั้น บางครั้งจึงต้องอาศัยการศึกษาทางประวัติศาสตร์ และศึกษาลักษณะของผู้นำหรืออิทธิพลในการกำหนดนโยบายของ

ประเทศนั้น ๆ ซึ่งภัยคุกคามแบบดั้งเดิม (Traditional Threat) กล่าวโดยรวมแล้วภัยคุกคามแบบดั้งเดิมจะมีความหมายครอบคลุมถึง ภัยคุกคามจากการใช้กำลังทหารเข้าทำการรบ และยังรวมไปถึงการบ่อนทำลาย ก่อวินาศกรรม จารกรรม ที่มีการกระทำในลักษณะรัฐต่อรัฐ

สรุปความหมายของภัยคุกคาม คือ การแสดงอำนาจด้วยกิริยาหรือวาจาให้หวาดกลัว และทำให้หวาดกลัว โดยพฤติการณ์ที่คาดคะเนได้ว่าจะก่อให้เกิดความเสียหาย มีผลให้ฝ่ายที่ถูกคุกคามต้องกระทำหรือละเว้นการกระทำอย่างใดอย่างหนึ่ง รวมไปถึงการกระทำอันจะเป็นอันตรายหรือสั่นคลอนต่อความมั่นคงของชาติในทุก ๆ ด้าน

ความหมายของภัยคุกคามรูปแบบใหม่

ก่อนที่จะกล่าวถึง “ภัยคุกคามรูปแบบใหม่” หรือคำในภาษาอังกฤษว่า “Non-Traditional Threat” นั้น สิ่งที่ต้องทำความเข้าใจก่อนคือ ภัยคุกคามแบบดั้งเดิม (Traditional Threat) หรือภัยคุกคามตามแบบ (Conventional threats) ซึ่งกล่าวโดยรวมแล้วภัยคุกคามแบบดั้งเดิมจะมีความหมายครอบคลุมถึงภัยคุกคามจากการใช้กำลังทหารเข้าทำการรบ และยังรวมไปถึงการบ่อนทำลาย ก่อวินาศกรรม จารกรรม ที่มีการกระทำในลักษณะรัฐต่อรัฐ ดังเช่นในยุคสงครามเย็นที่สหรัฐอเมริกาและสหภาพโซเวียตต่างมีสถานะที่เป็นภัยคุกคามต่อกัน ทำให้ต่างฝ่ายต่างสะสมอาวุธนิวเคลียร์จนถึงขึ้นสามารถทำลายล้างโลกใบนี้ได้ สำหรับประเทศไทยตั้งแต่มีสถานะเป็นรัฐชาติ (Nation-State) ได้มีหลายครั้งที่ประเทศไทยได้เผชิญกับภัยคุกคามแบบดั้งเดิมที่มีผลกระทบต่อความมั่นคงแห่งชาติ กล่าวได้ว่า “ความมั่นคงของชาติ” มีความหมายเดียวกับ “ความมั่นคงของรัฐ” โดยที่รัฐ (State) ประกอบด้วย องค์ประกอบสำคัญ ๔ ประการ ได้แก่ ประชาชน ดินแดน รัฐบาล และอำนาจอธิปไตย หากองค์ประกอบใดไม่เข้มแข็งเพียงพอชาติก็จะขาดความมั่นคง

ปัจจุบันสถานการณ์ทั้งภายในและต่างประเทศมีการเปลี่ยนแปลงรวดเร็ว ซับซ้อน และไม่แน่นอนมากขึ้น ซึ่งยากต่อการคาดการณ์สถานการณ์ดังกล่าวทำให้ภัยคุกคามในปัจจุบันแตกต่างไปจากเดิม โดยประเทศต่างๆ รวมถึงไทยจะเผชิญภัยคุกคามทั้งรูปแบบใหม่และภัยคุกคามรูปแบบเดิมในลักษณะ Hybrid Threats และต่างจะได้รับผลกระทบจากภัยคุกคามที่เกิดขึ้นจากความเชื่อมโยงระหว่างกัน ส่วนความสูญเสียและความเสียหายแตกต่างกันไปตามกำลังอำนาจ และความพร้อมในการรับมือและจัดการของแต่ละประเทศ โดยได้มีผู้ให้ความหมายเกี่ยวกับภัยคุกคามรูปแบบใหม่ไว้หลากหลาย ดังนี้

สภาความมั่นคงแห่งชาติ ได้กำหนดภัยคุกคามต่อความมั่นคงของชาติไว้กว้าง ๆ ๒ ทาง คือ ภัยคุกคามจากภายใน เป็นปัญหาทางด้านการเมืองภายในประเทศ ได้แก่ ปัญหาเศรษฐกิจ ปัญหาพื้นที่ด้อยพัฒนา ปัญหาชายแดน ปัญหาทางด้านสังคมและจิตวิทยา และปัญหาทรัพยากรและสิ่งแวดล้อม ในขณะที่ภัยคุกคามจากภายนอก ได้แก่ ปัญหาความขัดแย้งของสังคมโลก ปัญหากลุ่มประเทศมุสลิม ปัญหาความสัมพันธ์กับประเทศเพื่อนบ้าน เป็นต้น ซึ่งพลังอำนาจของชาติที่แข็งแกร่งจะเป็นขีดความสามารถทำให้ประเทศชาติมีความมั่นคงผ่านพ้นจากภัยคุกคามได้

อภิเชษฐ์ ซื่อสัตย์ (๒๕๖๑, หน้า ๒๑) กล่าวไว้ว่า ลักษณะของภัยคุกคามรูปแบบใหม่จะมีความสลับซับซ้อน และเกี่ยวข้องกับหลายหน่วยงาน ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน โดยเฉพาะอย่างยิ่งภัยคุกคามที่มีลักษณะเป็นภัยข้ามชาติ ซึ่งจะมีความเกี่ยวพันเชื่อมโยงกับประเทศหรือภูมิภาคอื่น ๆ ทั้งที่เป็นรัฐชาติ และไม่มีสถานะเป็นรัฐ (Non-state Actor) เช่น ภัยคุกคามจาก

การก่อการร้าย อาชญากรรมข้ามชาติ และการค้ายาเสพติด รวมทั้งการก่อความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ เป็นต้น

สรุปความหมายของของภัยคุกคามรูปแบบใหม่ คือ ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศโดยตรงทั้งทางเศรษฐกิจ สังคมจิตวิทยา และการทหาร ในลักษณะที่ภัยคุกคามได้ทวีความรุนแรงเพิ่มขึ้นตามลำดับจากปัจจัยบวกของกระแสโลกาภิวัตน์ ที่มีการเปิดเสรีการค้า การเงิน การลงทุน ความก้าวหน้าทางการสื่อสารและเทคโนโลยีสารสนเทศ ตลอดจนผู้คนมีการย้ายถิ่นฐานระหว่างประเทศมากยิ่งขึ้น

นอกจากนี้ คณะที่ปรึกษาด้านการข่าวกรอง (๒๕๖๔, หน้า ๑๓) ได้อธิบายไว้ว่า สภาความมั่นคงแห่งชาติ (สมช.) ได้กำหนดประเภทของภัยคุกคามรูปแบบใหม่ไว้ ๙ ประเภท ได้แก่

๑. ความแตกแยกทางความคิดของคนในสังคม เป็นผลจากทัศนะที่แตกต่างกับรัฐบาลของกลุ่มเห็นต่างจากรัฐในประเด็นต่าง ๆ เช่น การเมือง สิ่งแวดล้อม สิทธิมนุษยชน นอกจากนั้น ช่องว่างทางความคิดระหว่างวัย (Generation Gap) มีแนวโน้มจะเป็นปัญหาในสังคมไทยมากขึ้น จากการมีความแตกต่างทางความคิด ความเชื่อ ลักษณะนิสัย และแนวทางการทำงาน ซึ่งทำให้เอื้อต่อการสร้างความไม่เข้าใจ และความขัดแย้งระหว่างกัน และเป็นประเด็นอ่อนไหวที่อาจบานปลายเป็นอีกปัญหาทางสังคม

๒. ความไม่เชื่อมั่นต่อระบบและสถาบันการเมือง การเปลี่ยนแปลงทางการเมืองบ่อยครั้ง การขาดเสถียรภาพทางการเมือง การขาดประสิทธิภาพในการบริหารจัดการของรัฐบาล การพัวพันกับการทุจริตของรัฐบาล ตลอดจนการใช้ระบบอุปถัมภ์ในแวดวงการเมือง มีผลให้ประชาชนขาดความเชื่อมั่นต่อระบบและสถาบันการเมือง แม้สนับสนุนระบอบประชาธิปไตย ซึ่งความรู้สึกไม่ไว้วางใจดังกล่าวเป็นปัจจัยสำคัญที่บั่นทอนความมั่นคงทางการเมือง และยังคงเป็นภัยคุกคามหลักต่อระบบการเมือง

๓. การขาดสมดุลของการจัดการทรัพยากรธรรมชาติและสิ่งแวดล้อม ความสูญเสียทั้งชีวิตและทรัพย์สินของประชาชนที่เกิดขึ้นแทบทุกครั้งที่เกิดภัยธรรมชาติ เช่น ภัยแล้ง ไฟป่า อุทกภัย ดินโคลนถล่ม มลพิษทางอากาศ สะท้อนถึงความสำคัญของการบริหารจัดการสิ่งแวดล้อมและทรัพยากรธรรมชาติเพื่อลดผลกระทบจากปัญหาสิ่งแวดล้อมที่เป็นผลจากการเปลี่ยนแปลงสภาพแวดล้อมทางธรรมชาติทั้งที่มีสาเหตุตามธรรมชาติและการกระทำของมนุษย์โดยภัยพิบัติทางธรรมชาติขนาดใหญ่มีแนวโน้มจะเป็นภัยคุกคามต่อความมั่นคงของรัฐและมนุษย์มากขึ้น ทั้งระดับความรุนแรงและความเสียหาย

๔. ภัยพิบัติจากการเปลี่ยนแปลงของสภาพแวดล้อมทางธรรมชาติและโรคระบาดโรคอุบัติใหม่ และโรคระบาดที่กลับมาแพร่ระบาดใหม่ มีแนวโน้มจะเป็นปัญหามากขึ้นและเชื่อมโยงกับการเปลี่ยนแปลงสภาพภูมิอากาศ เช่น สภาพอากาศที่อุ่นหรือร้อนขึ้นทำให้มีเชื้อโรคและพาหะนำเชื้อโรคแพร่กระจายได้มากขึ้น รวมถึง การสูญเสียถิ่นที่อยู่อาศัยของสัตว์ เนื่องจากความต้องการใช้ประโยชน์จากสัตว์ เช่น การค้า หรือการบุกรุกพื้นที่ป่า ทำให้มีความเสี่ยงที่จะเกิดการแพร่ระบาดของเชื้อโรคจากสัตว์สู่คน และเป็นการเพิ่มการระบาดของโรคอย่างมีนัยสำคัญ

๕. ความมั่นคงในพื้นที่ ๓ จังหวัดชายแดนภาคใต้ จะเป็นปัญหาความมั่นคง ทั้งการก่อเหตุของกลุ่มแนวร่วม การจัดกิจกรรมเชิงสัญลักษณ์และการสร้างวาทกรรม ในแถลงการณ์ต่าง ๆ

เพื่อให้บรรลุเป้าหมาย ขณะที่การสนับสนุนกลุ่มเคลื่อนไหว และการลงพื้นที่เพื่อพบปะกับองค์กรภาคประชาสังคม เจ้าหน้าที่ฝ่ายความมั่นคง และผู้เกี่ยวข้องกับการก่อเหตุ เพื่อรับทราบข้อมูลและสถานการณ์ในพื้นที่ขององค์กรต่างชาติและนานาประเทศจะเอื้อต่อการเคลื่อนไหวของกลุ่มก่อความไม่สงบ และทำให้ความมั่นคงในพื้นที่จังหวัดชายแดนภาคใต้ยังคงยืดเยื้อ

๖. การก่อการร้ายและอาชญากรรมข้ามชาติ การที่กลุ่มก่อการร้าย เช่น กลุ่ม Al Qaeda และกลุ่ม Islamic State (IS) ซึ่งเป็นกลุ่มก่อการร้ายระหว่างประเทศที่สำคัญ ยังมีความเคลื่อนไหวและรักษาอุดมการณ์อย่างเหนียวแน่น โดยมีปัจจัยสนับสนุนการก่อเหตุจากความขัดแย้งทางการเมือง ศาสนา ชาติพันธุ์รวมถึงความขัดแย้งตามภูมิภาคต่างๆ ทำให้การก่อการร้าย ยังเป็นปัญหาความมั่นคงระดับโลกและประเทศต่อไป ทั้งการก่อเหตุการเผยแพร่แนวคิด และการชักชวนผู้สนับสนุนให้เข้าร่วมกลุ่ม และต้องอาศัยความร่วมมือระหว่างประเทศในการแก้ไขปัญหาที่เป็นภัยคุกคามร่วมกัน นอกจากนี้ อาชญากรรมข้ามชาติจะเป็นปัญหาที่มีความซับซ้อนและเชื่อมโยงระหว่างประเทศมากขึ้นจากความก้าวหน้าของเทคโนโลยีการสื่อสารสมัยใหม่ ซึ่งกลุ่มอาชญากรรมนำมาใช้ในการกระทำความผิด รวมทั้งสร้างเครือข่ายเชื่อมโยงกับกลุ่มหรือบุคคลในท้องถิ่น โดยอาชญากรรมข้ามชาติที่จะสร้างปัญหาให้ประเทศต่างๆ ที่สำคัญ ได้แก่ การค้ายาเสพติด การลักลอบผลิตและจัดหาเอกสารปลอม การลักลอบค้าอาวุธและสัตว์ป่า การลักลอบตัดไม้หวงห้าม อาชญากรรมทางคอมพิวเตอร์การพนันออนไลน์ การฉ้อโกงข้ามชาติและการฟอกเงิน รวมถึงการลักลอบนำคนเข้าเมืองและค้ามนุษย์

๗. แรงงานต่างด้าวและผู้หลบหนีเข้าเมือง จะยังเป็นปัญหาความมั่นคงสำคัญของไทย แม้แรงงานต่างด้าวมีส่วนสำคัญที่ช่วยแก้ไขปัญหาการขาดแคลนแรงงานของไทย เฉพาะอย่างยิ่งงานประเภทที่แรงงานไทยไม่นิยมทำ ผู้หลบหนีเข้าเมืองส่วนใหญ่มาจากประเทศเพื่อนบ้านที่มีแนวชายแดนติดกับไทยรวมถึงประเทศใกล้เคียง เช่น จีน เนื่องจากประสบปัญหาภายในประเทศทั้งด้านการเมือง เศรษฐกิจ และสังคม ในอนาคตไทยจะยังประสบปัญหาแรงงานต่างด้าวและผู้หลบหนีเข้าเมืองจากปัจจัยภายในของไทย เช่น ความต้องการแรงงาน การเข้าไปเกี่ยวข้องกับขบวนการค้ามนุษย์ และลักลอบนำคนเข้าเมือง และปัจจัยภายนอก เช่น ความต้องการเข้ามาหางานและต้องการสภาพความเป็นอยู่ที่ดีกว่าของแรงงานต่างด้าว การตกเป็นเหยื่อการค้ามนุษย์ และความต้องการใช้ไทยเป็นทางผ่านไปประเทศที่สาม

๘. ยาเสพติด จะแพร่ระบาดได้ง่ายและเร็วขึ้นผ่านช่องทางออนไลน์และการขนส่งทางพัสดุ โดยไม่จำกัดพื้นที่ ส่วนการที่สามเหลี่ยมทองคำเป็นแหล่งผลิตยาเสพติดที่สำคัญของโลก ทำให้ไทยประสบปัญหาทั้งการเป็นตลาดและทางผ่านลำเลียงยาเสพติดไปยังประเทศที่สาม โดยเฉพาะไอซ์ เฮโรอีน และกัญชา มีความร่วมมือกับประเทศเพื่อนบ้านในการสกัดกั้นยาเสพติดและเคมีภัณฑ์ตามแนวชายแดนก็ตาม สำหรับยาเสพติดที่มีการแพร่ระบาดมากที่สุดในไทย คือ ยาบ้า รองลงมา คือ ไอซ์ และกัญชา ส่วนคีตามีนเริ่มเป็นที่นิยมและมีการแพร่ระบาดในกลุ่มนักเที่ยวกลางคืน

๙. ความยากจน เนื่องจากปัญหานี้เป็นภัยที่ฝังรากลึกอยู่ในสังคมไทยมาช้านาน และเป็นเรื่องที่เกี่ยวกับมนุษย์โดยตรง แต่ด้วยตัวปัญหาที่มีความสลับซับซ้อนหลายมิติ ซึ่งน่าจะเกินอำนาจบังคับกฎหมายเพื่อแก้ปัญหาตามพระราชบัญญัติความมั่นคงฯ

แนวคิดและทฤษฎีเกี่ยวกับการข่าวกรอง

ความหมายของข่าวกรอง

ได้มีผู้ให้ความหมายเกี่ยวกับ “ข่าวกรอง” ไว้หลากหลาย ดังนี้

พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. ๒๕๖๒ ได้ระบุคำจำกัดความของ “การข่าวกรอง” ไว้ว่า หมายถึง การดำเนินการเพื่อให้ทราบถึงความมุ่งหมาย กำลังความสามารถและความเคลื่อนไหว รวมทั้งวิถีทางของบุคคล กลุ่มบุคคล หรือองค์การใด ทั้งภายในประเทศและต่างประเทศที่อาจกระทำการอันเป็นพฤติการณ์เป็นภัยคุกคาม ทั้งนี้ เพื่อรักษาความมั่นคงหรือประโยชน์แห่งรัฐ และให้รัฐบาลนำมาประกอบการพิจารณาในการกำหนดนโยบายแห่งชาติ

โรงเรียนเสนาธิการทหารบก กรมยุทธศึกษาทหารบก ได้นิยามความหมายของ “ข่าวกรอง” ไว้ว่า เป็นผลอันเกิดมาจากการรวบรวมการประเมินค่าการวิเคราะห์การสนธิ และการตีความข่าวสารทั้งมวลที่ได้มา ซึ่งเกี่ยวข้องกับลักษณะอย่างหนึ่งหรือหลายประการของต่างคติ หรือของพื้นที่ปฏิบัติการต่างๆ ซึ่งมีความสำคัญ โดยตรงหรือน่าจะมีความสำคัญในการพัฒนาและกำหนดการปฏิบัติการ การกำหนดแผนการยุทธ์ การกำหนดยุทธศาสตร์ชาติ นโยบายของชาติ ยุทธศาสตร์ป้องกันประเทศและยุทธศาสตร์ทหาร

เจตน์พงศ์ โชคสวัสดิ์วรกุล (๒๕๕๓) ได้อธิบายความหมายของ “ข่าวกรอง” ไว้ว่า เป็นผลิตผลที่ได้จากการนำข้อมูลข่าวสาร ซึ่งหมายถึง ปรากฏการณ์ต่าง ๆ ที่เกิดขึ้นมา ผ่านกรรมวิธีทางการข่าว อันมีขั้นตอนต่าง ๆ เช่น รวบรวม วิเคราะห์ ประสานงาน แปลความหมาย ตลอดจนการนำไปใช้ประโยชน์ เพื่อเพิ่มคุณค่าให้กับข้อมูลข่าวสารที่ได้รับให้สามารถใช้ประโยชน์ ตอบสนองความต้องการใช้ข้อมูลของผู้บริหารได้อย่างตรงจุด นำไปสู่ความได้เปรียบเหนือฝ่ายตรงข้าม ซึ่งที่ผ่านมามักใช้กันในหน่วยงานราชการโดยเฉพาะอย่างยิ่งหน่วยงานทางทหาร โดยมีจุดประสงค์เพื่อความมั่นคงปลอดภัยของชาติ แต่ในปัจจุบันได้ถูกนำมาประยุกต์ใช้ในหน่วยงานเอกชนและภาคธุรกิจด้วย

ทวี แจ่มจำรัส (๒๕๕๙) ได้อธิบายความหมายของ “ข่าวกรอง” ไว้ว่า ซุนวู ปราชญ์ทางด้านการทหารผู้เขียนตำราพิชัยสงครามของจีนในอดีตเคยกล่าวไว้ว่า “ถ้ารู้เขารู้เรา รบร้อยครั้งชนะร้อยครั้ง” คำกล่าวเช่นนี้สามารถนำไปใช้ได้ในทุกวงการไม่จำกัด เฉพาะวงการทหารเท่านั้น เพราะฉะนั้น งานการข่าวจึงเป็นเครื่องมือสำคัญที่ทำให้ทุกคนสามารถปฏิบัติภารกิจของหน่วยงานและตนเองสำเร็จ ถ้าขาดงานการข่าวแล้วภารกิจทุกอย่างจะล้มเหลว หรือไม่ประสบผลสำเร็จตามที่มุ่งหวังไว้ จึงขอนำเสนอความรู้เกี่ยวกับงานการข่าวของทหารซึ่งสามารถนำไปประยุกต์ใช้ได้ทั้งองค์กรและยุคคลของสังคมทุกภาคส่วนตามสถานการณ์ที่แตกต่างกันได้อย่างมีประสิทธิภาพ

ศูนย์กิจการอวกาศ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ได้อธิบายความหมายของ “การข่าวกรอง” ไว้ว่า เป็นการรวบรวมข่าวสารเพื่อใช้ในวัตถุประสงค์ด้านการทหาร ซึ่งต้องทำทั้งในยามปกติ และยามเกิดความขัดแย้ง ซึ่งเกี่ยวข้องกับการหาข่าวซึ่งมีวิธีการและอุปกรณ์ที่หลากหลาย ทั้งจากภาคพื้น ในทะเล หรือภาคอากาศ หากปราศจากการข่าวกรอง การปฏิบัติทางทหารจะไม่ประสบความสำเร็จ เนื่องจากก่อนการปฏิบัติใดจำเป็นจะต้องมีข่าวสารรายละเอียดเกี่ยวกับยุทธวิธี ยุทโธปกรณ์ และแนวทางการใช้งานของข้าศึก ตลอดจนที่ตั้งและจำนวน ซึ่งข้อมูลข่าวสารนี้จะถูกนำไปทำเป็นทำเนียบกำลังรบอิเล็กทรอนิกส์ในพื้นที่ (Electronic Order of Battle:

EOB) และฐานข้อมูลด้านอิเล็กทรอนิกส์ (Electronic Database) ตลอดจนใช้เป็นปัจจัยในการตัดสินตกลงใจของผู้บังคับบัญชาในการบัญชาการ และควบคุม (Command and Control Warfare: C2W) อีกด้วย

สรุปความหมายของข่าวกรอง กล่าวคือ ข่าวกรอง (Intelligence) หมายถึง ผลิตผลที่ได้จากการนำข้อมูลข่าวสาร (Information) ซึ่งหมายถึงปรากฏการณ์ต่าง ๆ ที่เกิดขึ้นมา ผ่านกรรมวิธีทางการข่าว ได้แก่ รวบรวม วิเคราะห์ ประสานงาน แปลความหมาย และการนำไปใช้ประโยชน์ เพื่อเพิ่มคุณค่าให้กับข้อมูลข่าวสารที่ได้รับให้สามารถใช้ประโยชน์ ตอบสนองความต้องการใช้ข้อมูลของผู้บังคับบัญชาได้อย่างตรงจุด นำไปสู่ความได้เปรียบเหนือฝ่ายตรงข้าม ซึ่งที่ผ่านมามักใช้กันในหน่วยงานราชการ โดยเฉพาะอย่างยิ่งหน่วยงานทางทหาร โดยมีจุดประสงค์เพื่อความมั่นคงปลอดภัยของชาติ ซึ่งปัจจุบันได้ถูกนำมาประยุกต์ใช้ในหน่วยงานเอกชนและภาคธุรกิจด้วย

ความหมายของข่าวกรองแบบเปิด

ได้มีผู้ให้ความหมายเกี่ยวกับ “ข่าวกรองแบบเปิด (OSINT)” ไว้หลากหลาย ดังนี้

คำว่า โอเพนซอร์ส (open source) ภายใน OSINT ไม่ได้หมายถึงการเคลื่อนไหวของซอฟต์แวร์โอเพ่นซอร์ส แม้ว่าเครื่องมือ OSINT จำนวนมากจะเป็นโอเพ่นซอร์สก็ตาม แต่เป็นการอธิบายถึงลักษณะสาธารณะของข้อมูลที่กำลังวิเคราะห์

Office of Science and Technology Cooperation (OTSC) ได้นิยามความหมายของ “ข่าวกรองแบบเปิด” ไว้ว่า ข่าวกรองทางแหล่งข้อมูลเปิด (OSINT) เป็นข่าวกรองที่ได้จากสิ่งที่อยู่ใกล้ตัว สามารถมองเห็น หรือได้ยินทุกวัน ได้แก่ อินเทอร์เน็ต ช่องทางมีเดียต่าง ๆ เช่น วิทยุ โทรทัศน์ หรือหนังสือพิมพ์ ช่องทางบทความวิชาการ ช่องทาง รูปถ่าย และช่องทางข้อมูลภาพถ่ายเชิงพื้นที่ เป็นต้น

สรุปความหมายของ “ข่าวกรองแบบเปิด” กล่าวคือ เป็นส่วนหนึ่งในวิธีการสืบสวนสอบสวน ด้วยการรวบรวม และวิเคราะห์ข้อมูลที่รวบรวมจากแหล่งสาธารณะ หรือแหล่งเปิดบนอินเตอร์เน็ต และโซเชียลมีเดีย ส่วนใหญ่ให้บริการฟรีและมีประสิทธิภาพมาก ดังนั้น OSINT จึงถูกนำมาใช้ในขั้นตอนการสำรวจ เพื่อวางแผนการโจมตีทางไซเบอร์ เช่น การโจมตีแบบฟิชชิง (Phishing) วิศวกรรมสังคม (Social Engineering) เป็นต้น

ประเภทของข่าวกรอง

จากหลักนิยมการข่าวกรองของกองทัพบก พ.ศ.๒๕๔๑ ยังได้แบ่งประเภทของข่าวกรองออกเป็น ๓ ประเภท คือ ข่าวกรองแห่งชาติ ข่าวกรองทางทหาร และข่าวกรองประเภทอื่น ๆ สามารถอธิบายได้ดังนี้

๑. ข่าวกรองแห่งชาติ เป็นข่าวกรองในระดับ กระทรวง ทบวง กรม ตั้งแต่หนึ่งหน่วยขึ้นไป เพื่อใช้ในการรักษาผลประโยชน์และความมั่นคงของชาติ ประกอบด้วย

๑.๑ ข่าวกรองกิจกรรมภายใน เป็นข่าวที่นำไปใช้ประโยชน์ในด้านการบริหารการปกครอง การพัฒนาประเทศ รวมทั้งการบริการสวัสดิการของรัฐ ซึ่งเป็นกิจการภายในประเทศ

๑.๒ ข่าวกรองการรักษาความมั่นคงปลอดภัย เป็นข่าวกรองที่ใช้ประโยชน์ในการปฏิบัติการเพื่อเสถียรภาพ การป้องกัน และปราบปรามการก่อความไม่สงบ

๑.๓ ข่าวกรองการต่างประเทศ เป็นข่าวกรองที่ใช้ประโยชน์ในการกำหนดนโยบายและการดำเนินความสัมพันธ์กับต่างประเทศ รวมทั้งการเตรียมการป้องกันประเทศ และการทำสงคราม

๒. ข่าวกรองทางทหาร เป็นข่าวกรองสำหรับการวางแผนการปฏิบัติการตามนโยบายและการกำหนดการทางทหาร ประกอบด้วย

๒.๑ ข่าวกรองทางยุทธศาสตร์ (Strategic Intelligence) คือ ความรู้พื้นฐานเกี่ยวกับศักยภาพในการกำหนดนโยบายและแผนการทางทหารของชาติใดชาติหนึ่ง เพื่อให้บรรลุวัตถุประสงค์ตามความต้องการ เช่น ขีดความสามารถ จุดล่อแหลม และหนทางปฏิบัติที่น่าจะเป็นไปได้ของต่างชาติที่สามารถเป็นได้ทั้งมิตร กลาง และศัตรู

๒.๒ ข่าวกรองทางยุทธวิถี (Tactical Intelligence) หรือที่เรียกว่า ข่าวกรองทางการรบ คือ ความรู้เกี่ยวกับฝ่ายตรงข้ามที่ได้มาจากกรรมวิธีข่าวสารของฝ่ายตรงข้าม ที่มีองค์ประกอบทั้งภูมิประเทศที่ได้รับมาจากเจ้าหน้าที่รวบรวมข่าวสารตามที่ผู้บังคับบัญชาต้องการในการวางแผนและการปฏิบัติการทางยุทธวิธี ซึ่งข่าวกรองทางรบจะให้ข่าวสารและข้อสรุปที่เกี่ยวกับพื้นที่ปฏิบัติการ ขีดความสามารถจุดล่อแหลมและหนทางปฏิบัติของฝ่ายตรงข้าม

๓ ข่าวกรองประเภทอื่นๆ เป็นข่าวกรองที่กำหนดขึ้นตามหน้าที่ การปฏิบัติการและความมุ่งหมายในการนำไปใช้ ซึ่งข่าวกรองชนิดต่าง ๆ อาจจะเป็นทั้งส่วนประกอบทั้งข่าวกรองแห่งชาติ และข่าวกรองยุทธวิถีได้

แหล่งข่าวกรอง

แหล่งข่าวกรอง (Intelligence Source) เป็นหนทางหรือระบบที่ใช้เพื่อสังเกตรับรู้บันทึกหรือได้มาซึ่งข้อมูลของสภาพการณ์ สถานการณ์ หรือเหตุการณ์ ซึ่งจากการที่ผู้วิจัยได้ศึกษาและทบทวนสามารถสรุปแหล่งข่าวกรองออกเป็น ๘ ประเภท ดังนี้

๑. HUMINT (Human Intelligence) คือ การรวบรวมข้อมูลด้วยบุคคล เช่น สายลับ ตำรวจ ทหาร เจ้าหน้าที่ด้านการทูต ข้าราชการท้องถิ่น สื่อมวลชน นักเคลื่อนไหวเอ็นจีโอ นักการเมือง เป็นต้น ซึ่งบุคคลเหล่านี้ สามารถรวบรวมข้อมูลได้ด้วยการลงพื้นที่ สังเกตการณ์ เก็บภาพถ่ายในพื้นที่และพูดคุยกับคนในพื้นที่

๒. GEOINT (Geospatial Intelligence) คือ การรวบรวมข้อมูลภาพถ่ายทางอากาศและภาพถ่ายดาวเทียม เพื่อสำรวจลักษณะภูมิประเทศ และแผนที่ของพื้นที่ต่าง ๆ โดยที่การใช้ Google Map ถือเป็นการรวบรวมข้อมูลแผนที่ และข้อมูลที่อยู่ ซึ่งสามารถเข้าถึงได้อย่างสะดวกง่ายดาย

๓. MASINT (Measurement and signature intelligence) คือ การค้นหาแหล่งพลังงาน สัญญาณ และวัตถุ โดยใช้เทคโนโลยีระบบเรดาห์หรือระบบเซ็นเซอร์ ในการค้นหาตรวจจับวัตถุหรือแหล่งพลังงานต่าง ๆ เช่น เส้นทางขีปนาวุธ วิถีกระสุนปืนใหญ่ แหล่งกัมมันตภาพรังสีนิวเคลียร์ แหล่งคลื่นแม่เหล็กไฟฟ้า แหล่งคลื่นสัญญาณวิทยุ แหล่งสารเคมี แหล่งเชื้อโรค เป็นต้น

๔. OSINT (Open-source Intelligence) คือ การรวบรวมข้อมูลจากแหล่งข้อมูลที่มีการเปิดเผยต่อสาธารณะอยู่แล้ว ทั้งห้องสมุด หนังสือ หนังสือพิมพ์ และอินเตอร์เน็ต โดยเฉพาะอินเตอร์เน็ตที่สามารถเข้าถึงข้อมูลได้อย่างมหาศาล เช่น เว็บไซต์ Google สามารถช่วยค้นหาข้อมูลได้

อย่างสะดวก หลากหลาย และแม่นยำ ทั้งการพิมพ์ค้นหาข้อมูลในหน้าหลักของ Google การค้นหารูป การค้นหาวิดีโอ การค้นหาข่าวสารหรือลิงค์เว็บไซต์สำนักข่าว และการค้นหาตำแหน่งที่ตั้งใน Google Maps ทั้งนี้ การค้นหาตำแหน่งที่ตั้งใน Google Maps ก็สามารถช่วยสืบค้นและช่วยวิเคราะห์ความเชื่อมโยงของข้อมูลดิบต่าง ๆ ได้เป็นอย่างดี ซึ่งการทราบแหล่งถิ่นที่อยู่อาจทำให้ทราบถึงขอบเขตของร่องรอยข้อเท็จจริงเกี่ยวกับชีวิตประจำวันขององค์กรได้ นอกจากนี้ แพลตฟอร์มโซเชียลมีเดียทั้ง Facebook, Twitter, YouTube รวมถึงเว็บไซต์สำนักข่าวต่าง ๆ ก็เป็นแหล่งข้อมูลเปิดที่ทุกคนสามารถเข้าถึงได้อย่างแม่นยำเช่นกัน

๕. SIGINT (Signals Intelligence) คือ การรวบรวมข้อมูลด้วยการดักสัญญาณที่ถูกป้องกันด้วยรหัส Encryption และรวบรวมข้อมูลการสนทนา หรือที่เรียกว่า COMINT (Communications intelligence) ไม่ว่าจะเป็นการสนทนาผ่านโทรศัพท์ บทสนทนาในอินเตอร์เน็ต หรือบทสนทนาในวิทยุ ส่วนการดูข้อความการสนทนาในโซเชียลมีเดีย และข้อความแชทในแอปพลิเคชันต่าง ๆ ก็ถือว่าเป็น COMINT ด้วยเช่นกัน เช่น การจับภาพคอมเม้นต์โต้ตอบกันใน Facebook, การจับภาพทวีตข้อความโต้ตอบกันไปมา Twitter และการแค็ปภาพข้อความแชทในกลุ่ม Line ซึ่งทุกการกระทำทุกการสนทนาทั้งหมดในโลกออนไลน์ นอกจากจะนำมาเป็นข้อมูล COMINT ได้แล้ว ยังเป็นข้อมูลรอยเท้า หรือ digital footprint ที่สามารถสืบค้นย้อนหลังได้

๖. TECHINT (Technical Intelligence) คือ การรวบรวมและวิเคราะห์ข้อมูล ผ่านรายละเอียดเครื่องมือเทคโนโลยีของศัตรูหรือคู่แข่ง เช่น อุปกรณ์สื่อสาร โปรแกรม แอปพลิเคชัน ยานพาหนะขนส่ง อาวุธยุทโธปกรณ์ เป็นต้น

๗. CYBINT (Cyber Intelligence) คือ การรวบรวมข้อมูลจากไซเบอร์สเปซหรือโลกไซเบอร์ ด้วยการเก็บข้อมูลการสื่อสารในอินเตอร์เน็ต ซึ่ง CYBINT ถือได้ว่าเป็นซับเซ็ต (Subset) ของ SIGINT (Signals intelligence) COMINT (Communications intelligence) และ OSINT (Open-source intelligence)

๘. FININT (Financial Intelligence) คือ การรวบรวมข้อมูลธุรกรรมการเงิน เพื่อค้นหาการเลี่ยงภาษี การฟอกเงิน การสืบสวนคดีอาชญากรรม และการสืบเส้นทางการเงินกลุ่มบุคคลหรือองค์กรที่ก่อความไม่สงบหรือเป็นภัยต่อความมั่นคง

วงรอบข่าวกรอง

ได้มีผู้ศึกษาและวิจัยเกี่ยวกับ “วงรอบข่าวกรอง” ไว้หลากหลาย ดังนี้

โรงเรียนเสนาธิการทหารบก กรมยุทธศึกษาทหารบก อธิบายไว้ว่า “วงรอบ” หมายถึง ลำดับ ชุด หรือติดต่อกัน หรือเป็นตอน ๆ ของเหตุการณ์ หรือการปฏิบัติการต่าง ๆ ที่มีขึ้นให้เป็นไปอย่างสม่ำเสมอ และการปฏิบัติการนี้ก็จะย้อนกลับมาเริ่มต้น ณ จุดที่เริ่มต้นใหม่นี้อยู่ตลอดเวลา ดังนั้น จากคำจำกัดความของคำว่า “วงรอบการดำเนินงานข่าวกรอง” อาจจะกล่าวอีกนัยหนึ่ง คือ “กรรมวิธีในการจัดตั้งและปฏิบัติให้บรรลุความมุ่งหมายของข่าวกรอง” หรือ “การผลิตข่าวกรอง” นั่นเอง

ฉัตรพงศ์ ฉัตราคม (๒๕๕๓) อธิบายไว้ว่า วงรอบข่าวกรอง (Intelligence Cycle) ประกอบด้วย ๔ ขั้นตอน ได้แก่ ความต้องการข่าวสาร (Requirement) การรวบรวม (Collection) การดำเนินกรรมวิธี (Processing) และการวิเคราะห์ (Analysis) หากแต่ในกระบวนการผลิตข่าวกรอง

รูปแบบเดิมนั้น ถือว่าข่าวจากแหล่งเปิด (Open sources) อยู่ในขั้นตอนของการรวบรวม รายละเอียดดังต่อไปนี้

ขั้นตอนที่ ๑ ความต้องการข่าวสาร (Requirement) - OSINT ไม่ได้จำกัดอยู่เฉพาะข่าวที่เป็นเรื่องเกี่ยวกับความลับของประเทศฝ่ายตรงข้ามหรือศัตรูเพียงอย่างเดียว เพราะ OSINT สามารถจะสนองตอบความต้องการข่าวสารของผู้บังคับบัญชา หรือผู้ใช้ข่าวได้กว้างขึ้น ทั้งในแง่ของปัญหาความเดือดร้อนหรือความต้องการของประชาชนที่มีต่อรัฐบาล บทบาทของกลไกภาครัฐที่ปฏิบัติงานสนองต่อนโยบายรัฐบาล โอกาสและปัจจัยเสี่ยงด้านการค้า/การลงทุน หรือกล่าวได้ว่ารัฐบาล หรือผู้กำหนดนโยบายสามารถใช้หน่วยข่าวกรองให้รวบรวมและเสนอรายงานได้ทั้งในเรื่องความมั่นคงของชาติและความมั่งคั่งของชาติ ในลักษณะของการทำงานคู่ขนานไปกับหน่วยงานหลัก

ขั้นตอนที่ ๒ การรวบรวม (Collection) - หลักสำคัญในการรวบรวมของ OSINT คือ Knowing who Knows หรือการที่หน่วยข่าวกรองจะต้องตอบคำถาม/คำขอของรัฐบาล หรือผู้ใช้ข่าวโดยต้องรู้ว่าใครคือผู้เชี่ยวชาญที่รู้เรื่องราวหรือเหตุการณ์ที่ดีที่สุด ซึ่งวิธีนี้ค่อนข้างจะแตกต่างจากการข่าวกรองที่เน้น All-Sources Intelligence ที่มักจะดูที่ฐานข้อมูลข่าวสารที่หน่วยมีอยู่ว่าสามารถตอบคำถามได้หรือไม่ รวมทั้งการใช้ HUMINT หรือ SIGINT เป็นช่องทางสำคัญในการรวบรวมข่าวสาร โดยค่อนข้างให้ความสนใจน้อยมากกับแหล่งข้อมูลเปิด โดยเฉพาะอย่างยิ่งเอกสารวิจัยหรือบทความทางวิชาการ รวมถึงการไม่ให้ความสำคัญในการติดตามหรือศึกษาผลงานของนักวิชาการในสาขาต่าง ๆ โดยเฉพาะสาขาด้านความมั่นคง ปัจจัยสำคัญที่ทำให้ OSINT จะกลายเป็นเครื่องมือสำคัญของงานข่าวกรอง คือ สภาพแวดล้อมด้านความมั่นคงของโลกที่เปลี่ยนแปลงอย่างรวดเร็ว เพราะหลังสงครามเย็นยุติลง สภาพการเผชิญหน้าทางทหารระหว่างประเทศหรือกลุ่มประเทศต่าง ๆ แทบไม่ปรากฏ ประเทศส่วนใหญ่มุ่งเน้นการสร้างความสัมพันธ์ทางการทูต ขณะที่กฎหมายระหว่างประเทศและกฎหมายภายในประเทศของทุกประเทศให้ความสำคัญกับสิทธิมนุษยชนมาก ส่งผลให้เป้าหมายของงานด้านการข่าวกรองในส่วนที่จะต้องใช้ HUMINT ไม่ชัดเจน ขณะที่การดักรับการติดต่อสื่อสารต่างๆ และการดักฟังเป็นเครื่องมือ SIGINT ก็ไม่สามารถนำมาใช้ได้ภายในประเทศ เพราะผิดกฎหมาย ด้วยเหตุนี้ OSINT จึงกลายเป็นเครื่องมือที่เข้ามาเติมหรือช่วยลดจุดอ่อนของงานข่าวกรองเดิม โดยได้มีการนำเอาความทันสมัยของเทคโนโลยีสารสนเทศมาประยุกต์ใช้กับงานจนเต็มประสิทธิภาพ

ขั้นตอนที่ ๓ การดำเนินกรรมวิธี (Processing) - การดำเนินกรรมวิธีของ OSINT มีมาตรฐานค่อนข้างดี เมื่อเทียบกับการข่าวกรองแบบอื่น ๆ กล่าวคือ มีการจัดระบบฐานข้อมูลของหน่วยงานที่นักวิเคราะห์สามารถสืบค้นได้ง่าย โดยมีการแบ่งแยกชัดเจนระหว่างฝ่ายที่ทำหน้าที่รวบรวมกับฝ่ายวิเคราะห์ และฝ่ายเจ้าหน้าที่เทคนิคอย่างชัดเจน นอกจากนี้ ในประเทศมหาอำนาจหลายประเทศ เช่น สหรัฐอเมริกา อังกฤษ ยังมีการใช้ซอฟต์แวร์สำหรับใช้ช่วยสนับสนุนการเข้าถึงแหล่งข้อมูลข่าวสาร การนำข้อมูลข่าวสารที่ได้ไปรวบรวมและจัดเก็บอย่างเป็นระบบและ ซอฟต์แวร์ใช้ช่วยแปลข้อมูลข่าวสารที่เป็นภาษาต่างประเทศต่าง ๆ ซึ่งได้มาจากแหล่งข่าวทุกแหล่งที่รวบรวมได้ อย่างไรก็ตาม การประมวลข้อมูลข่าวสารทั่วไป ยังต้องใช้คนเป็นผู้ดำเนินการ หลักการดำเนินการจะเหมือนกับการดำเนินกรรมวิธีในการผลิตข่าวกรองทั่วไป ได้แก่ การนำเอาข้อมูลข่าวสารที่รวบรวมได้มาปะติดปะต่อประมวลเป็นเรื่องราวหรือเหตุการณ์ ซึ่งต้องอาศัยความละเอียดรอบคอบ และความรอบรู้ของผู้ปฏิบัติงานเป็นสำคัญ เพราะจะต้องเริ่มตั้งแต่การประเมินความน่าเชื่อถือของข่าวสารแต่

ละชิ้น โดยแยกข่าวที่ไม่เป็นประโยชน์หรือขาดความน่าเชื่อถือออก ต้องสามารถดึงเรื่องที่สำคัญออกมาจากข่าวสารจำนวนมาก และสามารถเชื่อมโยงเรื่องราวหรือเหตุการณ์จากข่าวสารแต่ละชิ้นที่ได้แยกแยะไว้แล้วเพื่อประมวลออกมาเป็นภาพใหญ่ แต่ในระบบงานของ OSINT จะยุ่งยากมากกว่า เพราะต้องรับผิดชอบกับข้อมูลข่าวสารจำนวนมหาศาล

ขั้นตอนที่ ๔ การวิเคราะห์ (Analysis) - จุดแข็งของ OSINT คือ เน้นการแสวงประโยชน์ผลงานวิเคราะห์ของผู้เชี่ยวชาญหรือนักวิชาการที่มีความรู้ในเชิงลึก หรือการแสวงประโยชน์จากผลการประชุมสัมมนาของหน่วยงานต่าง ๆ ทั้งภาครัฐและภาคเอกชนซึ่ง รวมทั้งอาจใช้การสัมภาษณ์หรือซักถามจากนักวิเคราะห์หรือผู้เชี่ยวชาญในเรื่องนั้น ๆ OSINT จึงเปรียบเสมือนการนำความรู้ที่แท้จริงของผู้รู้มาต่อยอดเป็นรายงาน อย่างไรก็ตาม จุดอ่อนของ OSINT คือ ในการจัดทำรายงานข่าวกรองบางเรื่องนักวิเคราะห์อาจตามไม่ทันความคิดของบรรดานักวิชาการ และนักวิเคราะห์อาจมีอคติต่อเรื่องราวหรือเหตุการณ์หรือต่อนักวิชาการที่วิเคราะห์เหตุการณ์นั้นไว้

หลักนิยมการปฏิบัติการร่วมกองทัพไทย พ.ศ. ๒๕๕๐ ด้านข่าวกรองร่วม อธิบายไว้ว่า วงรอบข่าวกรอง (Intelligence Cycle) ประกอบด้วย กระบวนการ ๔ ขั้นตอน คือ การวางแผน (Planning) การรวบรวมข่าวสาร (Collection) การดำเนินกรรมวิธีข่าวสาร (Processing) และการใช้และการกระจายข่าวสาร/ข่าวกรอง (Dissemination) รายละเอียดดังต่อไปนี้

ขั้นตอนที่ ๑ การวางแผน (Planning) ขั้นการอำนวยการรวบรวมข่าวสารผ่านการรวบรวมข่าวสารตามภารกิจของหน่วย และสถานการณ์ข้าศึกจะต้องจัดทำขึ้น จากแผนดังกล่าวจะส่งคำสั่งและคำขอการรวบรวมคำสั่งต่าง ๆ แผนการรวบรวมข่าวสาร เพื่อแสดงให้เห็นถึงความเกี่ยวข้องกับภารกิจและความต้องการข่าวกรองอื่น ๆ และให้เห็นถึงกรรมวิธีแสดงความคิดเห็นอย่างมีเหตุผล ซึ่งงานข่าวกรองจะใช้ผลิตคำสั่งและคำขออันเฉพาะเจาะจง ที่จะส่งไปให้เจ้าหน้าที่รวบรวมข่าวสารต่าง ๆ ลำดับงานในการวางแผนและการดำเนินการรวบรวมข่าวสารต่อไป

ขั้นตอนที่ ๒ การรวบรวมข่าวสาร (Collection) หลังจากที่พิจารณาเลือกเจ้าหน้าที่รวบรวมข่าวสารตามขีดความสามารถ นายทหารฝ่ายข่าวกรองจะกำกับดูแลการดำเนินการรวบรวมข่าวสารเพื่อตรวจสอบคำสั่งและคำแนะนำต่าง ๆ โดยจะมีการติดต่ออย่างใกล้ชิดกับผู้บังคับหน่วยตลอดจนเจ้าหน้าที่รวบรวมข่าวสารที่เกี่ยวข้อง การติดต่อเช่นนี้จะช่วยให้ทราบข่าวสารที่ล่าสุดและทำให้สามารถพิจารณาแผนการรวบรวมข่าวสารได้อย่างต่อเนื่องซึ่งอาจจำเป็นจะต้องมีการปรับปรุงไปตามสถานการณ์ข้าศึกที่เปลี่ยนแปลงไป เจ้าหน้าที่รวบรวมข่าวสารต่าง ๆ จะได้รับข่าวสารที่มีปริมาณมากกว่าเพื่อนำไปใช้ประโยชน์ในการผลิตข่าวกรอง และสภาพข่าวกรองก็จะมีลักษณะที่ซับซ้อนจนอาจตีความผิดพลาดนอกจากจะนำเอาข่าวสารและข่าวกรองที่ได้รวบรวมมาแล้วนั้นนำมาสนธิเข้าด้วยกันอย่างเหมาะสมให้มีความหมายเป็นอันหนึ่งอันเดียวกัน

ขั้นตอนที่ ๓ การดำเนินกรรมวิธีข่าวสาร (Processing) กระทำเพื่อเปลี่ยนข่าวสารให้เป็นข่าวกรอง การดำเนินกรรมวิธีจะประกอบด้วยการปฏิบัติ ๓ ประการ ได้แก่

๑. การบันทึก เป็นกรรมวิธีของฝ่ายการข่าวที่ได้รับนั้นสามารถนำไปใช้ประโยชน์ เพื่ออ้างอิงได้ในอนาคต โดยข่าวสารนั้นต้องได้รับการจัดระเบียบอย่างเหมาะสมเพื่อนำไป

ใช้ได้ทันเวลาเครื่องมือที่สำคัญในการบันทึกข่าวสาร ได้แก่ บันทึกประจำวัน (Journal) แผนที่สถานการณ์ (Situation Map) เอกสารแยกเรื่องข่าวกรอง (Intelligence Workbook) และแฟ้มข่าวกรอง (Intelligence Files)

๒. การประเมินค่า เป็นตรวจสอบข่าวเพื่อกาหนดค่าของข่าวกรอง อีกทั้งยังเป็นขั้นตอนเพื่อ หาความเกี่ยวข้องของข่าวสาร ความน่าเชื่อถือของแหล่งข่าว และความถูกต้องแน่นอนของข่าว ประกอบด้วย ความเกี่ยวข้องของข่าวสาร ความเชื่อถือได้ของแหล่งข่าว และความแน่นอน โดยข่าวสารขึ้นอยู่กับความจริง

๓. การตีความการบันทึก ประกอบด้วย ๓ ขั้น ดังต่อไปนี้

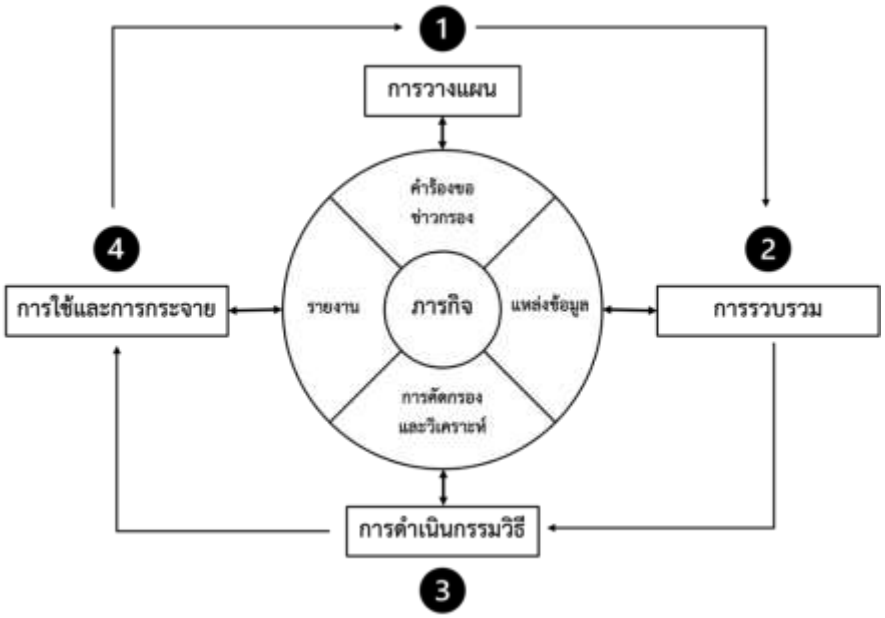
๓.๑ การวิเคราะห์ เป็นการกลั่นกรองการแยกข่าวสารที่ได้ประเมินค่าแล้วนำมาพิจารณาส่วนที่สำคัญของข่าวสารที่เกี่ยวข้องกับภารกิจ และการปฏิบัติต่าง ๆ โดยการวิเคราะห์จำเป็นต้องใช้การวินิจฉัยที่ดี และความรู้ความเข้าใจในภารกิจหรือพื้นที่ปฏิบัติเป็นอย่างดี

๓.๒ การสนธิกรรม เป็นการรวมส่วนต่าง ๆ ที่ถูกแยกออกแล้วเพื่อการเห็นภาพที่เป็นไปได้ และการสมมติฐานเกี่ยวกับการปฏิบัติของฝ่ายตรงข้ามหรืออิทธิพลในพื้นที่ปฏิบัติการที่มีต่อภารกิจของหน่วย การสนธิกรรมจะใช้เวลามากหรือน้อย ขึ้นอยู่กับจานวนของข้อมูลข่าวสาร และประสิทธิภาพของผู้วิเคราะห์ข้อมูล

๓.๓ การอนุมาน หมายถึง การพิจารณาเหตุผลจาก สมมติฐานที่ได้กำหนดขึ้น จากนั้นทดสอบและพิจารณาถึงความเป็นไปได้จากการที่ได้นามาสนธิกรรม ซึ่งเป็นขั้นสุดท้ายของการตีความข่าวสารที่จะกาหนดขึ้นเพื่อทราบถึงความหมายที่เกี่ยวข้อง เช่น สถานการณ์หรือพื้นที่ปฏิบัติการ ซึ่งคาตอบที่ได้รับจะเป็นข้อสรุปที่มีประโยชน์ในการกาหนดทิศทางปฏิบัติของฝ่ายตรงข้าม

ขั้นตอนที่ ๔ การใช้และการกระจายข่าวสาร/ข่าวกรอง (Dissemination) เมื่อข้อมูลผ่านการวิเคราะห์และตรวจสอบความน่าเชื่อถือแล้ว หลังจากนั้น การรายงานข้อมูลที่ได้แก่ ผู้บังคับบัญชา หรือผู้ที่มีอำนาจในการใช้ข่าวกรองที่มีหลักเกณฑ์ทั้งสามประการ คือ ทันเวลาเหมาะสม และความปลอดภัยนั้น ถ้าหากข้อมูลดังกล่าวนั้นเกี่ยวข้องกับส่วนราชการ หรือองค์กรอื่นที่สามารถนำข้อมูลไปใช้ประโยชน์ได้

แผนภาพที่ ๒ – ๑ วงรอบข่าวกรอง (Intelligence Cycle) ตามหลักนิยมของกองทัพไทย



ที่มา: หลักนิยมการปฏิบัติการร่วมกองทัพไทย พ.ศ. ๒๕๕๐ ด้านข่าวกรองร่วม

จากหลักนิยม Joint Publication 2-0, Joint Intelligence อธิบายไว้ว่า กระบวนการข่าวกรองร่วมเป็นพื้นฐานสำหรับคำศัพท์และกระบวนการข่าวกรองทั่วไป ประกอบด้วยการปฏิบัติการข่าวกรอง ๕ ขั้นตอนที่สัมพันธ์กัน ดำเนินการโดยเจ้าหน้าที่ข่าวกรองและหน่วยงานต่าง ๆ ที่เกี่ยวข้อง เพื่อจุดประสงค์ในการจัดหาข่าวกรองที่เกี่ยวข้องและทันท่วงที ให้กับผู้บังคับบัญชาและผู้มีอำนาจตัดสินใจระดับชาติ โดยการปฏิบัติการข่าวกรอง ๕ ขั้นตอนหลัก รายละเอียดดังต่อไปนี้

ขั้นตอนที่ ๑ กำหนดทิศทางและการวางแผน (Planning and Directing) การใช้ตัวอย่างที่ระดับยุทธศาสตร์หรือระดับกลยุทธ์ เช่น ความต้องการข่าวกรองจะถูกกำหนดโดยผู้ตัดสินใจเพื่อให้บรรลุวัตถุประสงค์ที่ต้องการบรรลุ ใน NATO ผู้บัญชาการใช้ข้อกำหนด บางครั้งเรียกว่า “Essential Elements of Intelligence (EEIs)” เพื่อเริ่มต้นวงจรข่าวกรอง ในขณะที่ข้อกำหนดของสหรัฐอเมริกาสามารถออกได้จากทำเนียบขาว หรือรัฐสภา

ขั้นตอนที่ ๒ การรวบรวมข่าวสาร (Collection) เพื่อตอบสนองต่อข้อกำหนด เจ้าหน้าที่ข่าวกรองพัฒนาแผนการรวบรวมข่าวกรองโดยใช้แหล่งข้อมูลและวิธีการที่มีอยู่ และแสวงหาข่าวกรองจากหน่วยงานอื่น ๆ การรวบรวมข่าวสาร ประกอบด้วย ข้อมูลจากสาขาการรวบรวมข่าวกรองต่าง ๆ เช่น HUMINT (ข่าวกรองของมนุษย์), IMINT (ข่าวกรองด้านภาพ), ELINT (ข่าวกรองอิเล็กทรอนิกส์), SIGINT (ข่าวกรองสัญญาณ), OSINT (ข้อมูลข่าวกรองแบบเปิด) เป็นต้น

ขั้นตอนที่ ๓ การประมวลผลและแสวงประโยชน์ (Processing & Exploitation) หมายถึง การคัดสรรและจัดระเบียบข้อมูลดิบ (Raw Data) โดยวิธีการต่าง ๆ เช่น การตีความ (Interpret) การแปลความหมาย (Translate) ให้มีความเหมาะสมต่อการนำไปใช้ประโยชน์ในกระบวนการต่อไป กล่าวคือ เป็นการแปลงข้อมูลดิบ (Convert) ให้แบ่งเป็นข่าวสาร (Information) เพื่อเตรียมพร้อมสำหรับการแสวงประโยชน์

ขั้นตอนที่ ๔ การวิเคราะห์และการผลิตข่าวกรอง (Analysis and Production) การวิเคราะห์กำหนดความสำคัญและความหมายของการประมวลผลหน่วยสืบราชการลับ บูรณาการโดย

การรวมชิ้นส่วนของข้อมูลที่แตกต่างกัน เพื่อระบุข้อมูลหลักประกันและรูปแบบ จากนั้นตีความความสำคัญของความรู้ที่พัฒนาขึ้นใหม่

ขั้นตอนที่ ๕ กระจายข่าวกรอง (Dissemination and Integration) เป็นขั้นตอนที่ทำให้การวางแผนรวบรวมข่าวสารอย่างมีเหตุผล โดยการกระจายข่าวกรองไปขังผู้ใช้ประ โซชน์หรือผู้ที่ต้องการข่าวสาร ซึ่งจะนำไปใช้ในการตัดสินใจในด้านต่างๆ ซึ่งจะนำไปสู่การกำหนดความต้องการข่าวสารในวงรอบข่าวกรองใหม่อีกครั้ง

แผนภาพที่ ๒ – ๒ วงรอบข่าวกรอง (Intelligence Cycle)

ที่มา: Joint Publication 2-0, Joint Intelligence. (2013).

กระบวนการข่าวกรองแบบเปิด

ในห้วง ๑๐ กว่าปีที่ผ่านมา หน่วยข่าวกรองชั้นนำของโลก โดยเฉพาะสำนักงานข่าวกรองกลางของสหรัฐอเมริกา (CIA) ได้ให้ความสำคัญกับกระบวนการผลิตข่าวกรองจากแหล่งเปิด (OSINT) เป็นอย่างมาก เพราะสามารถลดภารกิจของการปฏิบัติการลับ (Secret Operation) ซึ่งมีความเสี่ยงและสิ้นเปลืองค่าใช้จ่ายสูงลงได้มาก อีกทั้ง ยังสามารถช่วยหาข่าวในส่วนที่การใช้วิธีการปฏิบัติการลับไม่สามารถแสวงหามาได้ โดยสหรัฐอเมริกาได้จัดตั้งหน่วยงานที่ทำหน้าที่หาข่าวและผลิตรายงานข่าวกรองจากแหล่งเปิดชื่อ Foreign Broadcast Information Service (FBIS) เพื่อรวบรวมข่าวสารที่เกิดขึ้น ทั่วโลกนำมาใช้จัดทำรายงานข่าวกรอง จนปัจจุบันการผลิตข่าวกรองจากแหล่งเปิด ของ FBIS ได้เข้ามามีบทบาทสำคัญอย่างมากในการผลิตรายงานข่าวกรอง เพื่อสนองตอบความต้องการของรัฐบาลและหน่วยงานด้านความมั่นคงของสหรัฐอเมริกา ซึ่งแนวความคิดดังกล่าวได้แพร่ขยายไปอย่างรวดเร็วในประเทศต่าง ๆ ทั้งในยุโรปและเอเชีย

จากผลการศึกษาของ ฉัตรพงศ์ ฉัตราคม (๒๕๕๓) อธิบายไว้ว่า สำหรับประเทศไทยนั้น การผลิตข่าวกรองจากแหล่งเปิดไม่ใช่เรื่องใหม่ เพราะแหล่งเปิดเป็นองค์ประกอบสำคัญของการผลิตข่าวกรอง โดยอยู่ในขั้นตอนของการรวบรวม (Collection) ซึ่งจะอาศัยข่าวสารจากแหล่งเปิดประมาณร้อยละ ๘๕-๙๐ ของข่าวสารทั้งหมด และจะอาศัยข่าวที่ได้จากการปฏิบัติการลับประมาณ

ร้อยละ ๑๐-๑๕ เพื่อจัดทำรายงานข่าวกรอง อย่างไรก็ตาม การศึกษา วิจัย และพัฒนาด้านของการผลิตข่าวกรองจากแหล่งเปิด (OSINT) ของประเทศไทย ยังนับว่ามีน้อยมากเมื่อเปรียบเทียบกับองค์การข่าวกรองชั้นนำของโลก ซึ่งสาเหตุสำคัญเป็นผลเนื่องจากข้อจำกัดด้านความรู้ เพราะความรู้ด้านข่าวกรองมักจำกัดอยู่เฉพาะในหน่วยงานด้านการข่าวกรองของรัฐ ขณะที่สถาบันการศึกษาของประเทศไทยยังขาดองค์ความรู้ (Knowledge) และบุคลากร (People) ด้านนี้อย่างมากเช่นกัน นอกจากนี้ การพึ่งพาองค์ความรู้ (KM) จากหน่วยข่าวกรองของต่างประเทศก็กระทำได้ยากลำบาก จากการที่หน่วยงานด้านการข่าวกรองของต่างประเทศยังถือว่างานด้านการข่าวกรองเป็นความลับของประเทศ การเผยแพร่ความรู้ให้กับประเทศต่างๆ ที่เป็นพันธมิตร แม้จะมีอยู่บ้างแต่ก็เป็นการถ่ายทอดอย่างจำกัด

เครื่องมือของข่าวกรองแบบเปิด

การวิเคราะห์ข้อมูลเป็นปัจจัยสำคัญในการรักษาความมั่นคงปลอดภัยของประเทศและในเชิงพาณิชย์ ดังนั้น การนำ OSINT มาใช้เป็นเครื่องมืออย่างแพร่หลายจึงสะท้อนถึงความก้าวหน้าของการข่าวกรองในวงกว้าง ปัจจุบันเครื่องมือสำหรับการรวบรวมข้อมูลมีให้สำหรับผู้ใช้ส่วนตัว ไม่ใช่โดเมนเฉพาะของรัฐบาลและหน่วยงานบังคับใช้กฎหมาย ดังนั้น OSINT ได้กลายเป็นศูนย์กลางในการรับมือกับความท้าทายที่เด่นชัดของยุคดิจิทัล ผู้วิจัยได้ศึกษาและสามารถสรุปตัวอย่างเครื่องมือ OSINT ที่เป็นที่นิยมในปัจจุบัน รายละเอียดดังนี้

๑. Lampyre เป็นแอปพลิเคชันระดับพรีเมียมที่สร้างขึ้นสำหรับ OSINT โดยเฉพาะ เป็นประโยชน์อย่างยิ่งสำหรับการตรวจสอบวิเคราะห์สถานะ ข้อมูลภัยคุกคามทางไซเบอร์ การสืบสวนอาชญากรรม และการวิเคราะห์ทางการเงิน สามารถติดตั้งบนคอมพิวเตอร์ของคุณหรือเรียกใช้ออนไลน์ได้ โดยจะวิเคราะห์แหล่งข้อมูลที่อัปเดตตามปกติมากกว่า ๑๐๐ รายการโดยอัตโนมัติ ซึ่งสามารถเข้าถึงได้ผ่านแอปพลิเคชันบน PC หรือการเรียก API หากจำเป็นผ่านบริการ SaaS Lighthouse ซึ่งต้องชำระเงินต่อคำขอ API มีคุณสมบัติดังนี้

๑.๑ การประมวลผลอาร์เรย์ข้อมูลขนาดใหญ่ในลักษณะที่สะดวก

๑.๒ ตัดข้อมูลทางสถิติที่ง่ายต่อการใช้งานและประเมินผล

๑.๓ การสร้างกราฟการเชื่อมต่อจำนวนมากและซ้อนสิ่งที่ค้นพบทั้งหมดบนแผนที่และมาตราส่วนเวลา

๑.๔ ประโยชน์ของการประหยัดเวลาในงานวิเคราะห์

๒. Maltego เป็นเครื่องมือสำหรับระบบปฏิบัติการอัจฉริยะและนิติคอมพิวเตอร์ (Digital Forensics) ช่วยให้สามารถวิเคราะห์ลิงก์ได้อย่างมีประสิทธิภาพผ่านการทำเหมืองข้อมูลแบบโต้ตอบด้วยภาพที่สมบูรณ์ดำเนินการตรวจสอบการเชื่อมโยงระหว่างข้อมูลจากแหล่งอินเทอร์เน็ตต่างๆ สามารถค้นหาข้อมูลที่เปิดเผยต่อสาธารณะและเปิดเผยความเชื่อมโยงระหว่างบุคคลและองค์กร มีคุณสมบัติดังนี้

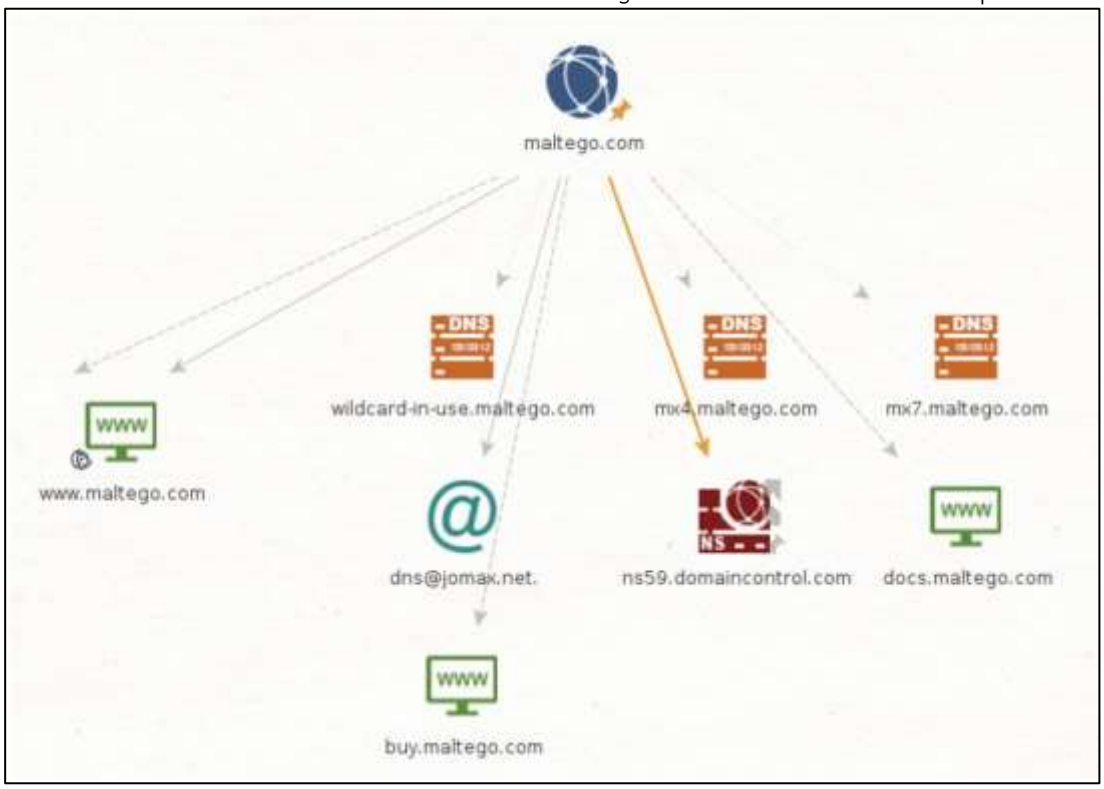
๒.๑ เป็นเทคโนโลยีที่วิเคราะห์ รวบรวม และเชื่อมโยงข้อมูลเพื่อการสืบสวน

๒.๒ รวบรวมข้อมูลจากแหล่งสาธารณะที่หลากหลายได้อย่างง่ายดาย

๒.๓ Interface ที่ใช้งานง่ายจะเชื่อมโยงและรวมข้อมูลในกราฟโดยอัตโนมัติ

๒.๔ ทำการสืบค้นข้อมูลและใช้การวิเคราะห์ลิงก์เพื่อเปิดเผยความเชื่อมโยงระหว่างแหล่งที่มา

แผนภาพที่ ๒ – ๓ ตัวอย่างการแสดงผลลัพธ์ของ Maltego ในการค้นหา Network Footprint



ที่มา: https://www.maltego.com/

๓. Recon-ng เป็นการสอดแนมเว็บบน Python และ OSINT Framework สามารถทำให้กระบวนการได้มาซึ่งความรู้เป็นไปโดยอัตโนมัติโดยการค้นคว้าเนื้อหาโอเพนซอร์ซบนอินเทอร์เน็ต (Information Gathering) อย่างกว้างขวางและรวดเร็ว ยูทิลิตีนี้มีอินเทอร์เฟซบรรทัดคำสั่งแบบโต้ตอบตามโมดูล ส่วนประกอบอิสระของมันรวมถึงการลาดตระเวน การรายงาน การนำเข้า การแสวงประโยชน์ และการค้นพบ มีคุณสมบัติดังนี้

๓.๑ เป็นชุดโมดูลการรวบรวมข้อมูลที่ครอบคลุม มีโมดูลหลากหลายที่สามารถใช้รวบรวมข้อมูลได้

๓.๒ เป็นหนึ่งในเครื่องมือพื้นฐานและมีประโยชน์ที่สุดสำหรับการลาดตระเวน

๓.๓ ทำงานของเว็บแอปพลิเคชัน/เครื่องสแกนเว็บไซต์

๓.๔ Interface ค่อนข้างคล้ายกับ metasploitable1 และ metasploitable2 ทำให้ใช้งานง่ายมาก

๓.๕ ใช้เพื่อรวบรวมข้อมูลและประเมินช่องโหว่ของเว็บแอปพลิเคชัน

๓.๖ ใช้เครื่องมือค้นหา Shodan เพื่อสแกนอุปกรณ์ IoT

๔. SpiderFoot เป็นโปรแกรมสำรวจโอเพนซอร์ซฟรี มักเรียกว่าการพิมพ์ลายนิ้วมือกับคอลเลกชัน OSINT ที่สำคัญที่สุด สามารถส่งคำถามไปยังแหล่งข้อมูลสาธารณะมากกว่า ๑๐๐ แห่ง และรวบรวมข้อมูลเกี่ยวกับที่อยู่ IP ชื่อโดเมน เว็บเซิร์ฟเวอร์ ที่อยู่อีเมล และข้อมูลอื่นๆ มีคุณสมบัติดังนี้

๔.๑ ซอร์สโค้ดสามารถเข้าถึงได้ฟรีสำหรับทุกคนในการสนับสนุนและปรับปรุง

๔.๒ มันถูกเขียนขึ้นอย่างสวยงามเกี่ยวกับโค้ด ทำให้ผู้ใช้สามารถสำรวจ ทำความเข้าใจ และทำความเข้าใจคุณลักษณะต่างๆ ของโค้ดได้ดียิ่งขึ้น

๔.๓ ผู้ใช้สามารถกำหนดเป้าหมายและเลือกจากโมดูลมากกว่า ๑๐๐ โมดูลที่รองรับ SpiderFoot ในการรวบรวมข้อมูลและสร้างโปรไฟล์

๔.๔ ไม่จำเป็นต้องติดตั้งหรือตั้งค่าเพิ่มเติมใดๆ เมื่อลงทะเบียนแล้ว

๔.๕ มีให้ใช้งานบนระบบปฏิบัติการ Linux และ Windows รวมถึงในรุ่นคลาวด์

๕. StalkFace เป็นเครื่องมือที่ยอดเยี่ยมในการตรวจสอบหรือ “สะกดรอย” โปรไฟล์ Facebook คุณยังสามารถดึงโพสต์ที่แสดงความคิดเห็นหรือถูกใจโดยผู้ใช้ได้อีกด้วย ใช้ประโยชน์จากการสืบค้นเพื่อดำเนินการค้นหาขั้นสูงที่ Facebook ไม่อนุญาตให้เราดูโดยใช้การค้นหามาตรฐานตรงกันข้ามกับชื่อที่แนะนำ โปรดใช้ชื่อนี้เพื่อจุดประสงค์ทางจริยธรรมเท่านั้น มีคุณสมบัติดังนี้

๕.๑ เมื่อป้อน URL ของ Facebook หรือ URL รูปภาพของ Facebook จะปรากฏภาพถ่าย, ภาพถ่ายที่ถูกแท็ก, เรื่องราวที่ชอบ, รูปที่ชอบ, รูปภาพแสดงความคิดเห็น และเพจถูกใจ

๖. OSINT Framework นำเสนอข้อมูลในรูปแบบของแผนที่ความคิดเชิงโต้ตอบบนเว็บที่จัดระเบียบข้อมูลอย่างสวยงาม เป็นที่นิยมในหมู่ผู้ทดสอบการเจาะระบบและนักวิจัยด้านความปลอดภัยในโลกไซเบอร์ที่ค้นหาเครื่องมือสำหรับการรวบรวมข้อมูล และการสำรวจบางพื้นที่ Framework นี้ สามารถสำรวจเครื่องมือ OSINT ต่าง ๆ ที่จัดหมวดหมู่ได้ มีคุณสมบัติดังนี้

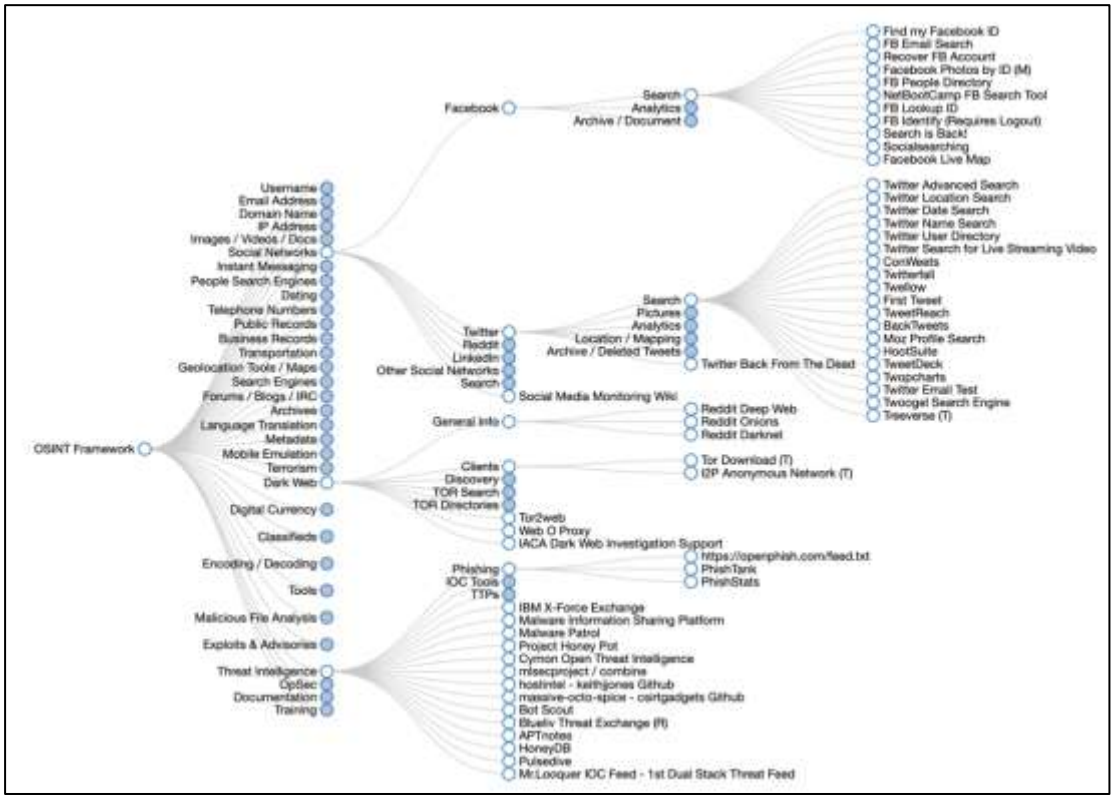
๖.๑ เครื่องมือและเว็บไซต์ที่ใช้กับข้อมูลการสืบค้นนั้นส่วนใหญ่ฟรีหรือไม่มีค่าใช้จ่าย

๖.๒ มีวิธีการที่หลากหลายในการรวบรวมข้อมูลตามเป้าหมายที่กำหนด

๖.๓ OSINT Framework เป็นเฟรมเวิร์กบนเว็บพื้นฐานที่ใช้โดยนักวิจัย และผู้ทดสอบด้านความปลอดภัยเพื่อรวบรวมร่องรอยและข้อมูลดิจิทัล

๖.๔ มันจัดหมวดหมู่แหล่งข่าวกรองและแบ่งออกเป็นวิชาและจุดมุ่งหมาย

แผนภาพที่ ๒ – ๔ ตัวอย่างการแสดงผลลัพธ์ของเครื่องมือ OSINT Framework



ที่มา: https://osintframework.com/

๗. Twitonomy เป็นโปรแกรมวิเคราะห์โซเชียลมีเดียบนเว็บที่ให้ข้อมูลเชิงลึกที่นำไปดำเนินการได้สำหรับองค์กรในกิจกรรมบัญชี Twitter ทั้งหมดของตน อนุญาตให้ผู้ใช้ติดตามการโต้ตอบกับผู้ใช้ Twitter คนอื่น ๆ ผ่านการถูกใจ ทวีต รีทวีต และวิธีการอื่นๆ มีคุณสมบัติดังนี้

๗.๑ นำเสนอข้อมูลประสิทธิภาพ แดชบอร์ด รายงานที่กำหนดค่าได้ และการตรวจสอบการมีส่วนร่วม

๗.๒ เมตริกภาพมีให้สำหรับทวีต รีทวีต กล่าวถึง ตอบกลับ และแฮชแท็ก

๗.๓ องค์กรสามารถใช้รายงานผู้ติดตามเพื่อรับข้อมูลเชิงลึกเกี่ยวกับผู้ติดตามและค้นหารายชื่อผู้ที่ไม่ติดตามพวกเขา

๗.๔ ช่วยให้ทีมสามารถส่งออกและสำรองข้อมูลการกล่าวถึง รีทวีต ทวีต และรายงานไปยังไฟล์ Excel และ PDF

๘. Shodan เป็น Search Engine แรกสำหรับอุปกรณ์เครือข่าย ซึ่งบางครั้งเรียกว่าอุปกรณ์ IoT Shodan จัดทำดัชนีทุกอย่างบนอินเทอร์เน็ต ในขณะที่ Google เพียงแค่จัดทำดัชนีเว็บ สามารถตรวจจับกล้อง เซิร์ฟเวอร์ เราเตอร์ กล้องวงจรปิด สัญญาณไฟจราจร สมาร์ททีวี ตู้เย็น และรถยนต์ที่เชื่อมโยงกับอินเทอร์เน็ต อุปกรณ์ IoT เหล่านี้ไม่สามารถค้นหาได้เสมอไป แต่ Shodan ได้สร้างวิธีการเพื่อค้นหาข้อมูลเกี่ยวกับอุปกรณ์ ซึ่งรวมถึงพอร์ตที่เปิดอยู่และช่องโหว่ต่างๆ เป็นหนึ่งในไม่กี่แห่งที่สามารถระบุตำแหน่งเทคโนโลยีการดำเนินงานที่แพร่หลายในระบบควบคุมอุตสาหกรรม ด้วยเหตุนี้ Shodan จึงเป็นเครื่องมือสำคัญสำหรับการรักษาความปลอดภัยทางไซเบอร์ในอุตสาหกรรม มีคุณสมบัติดังนี้

๘.๑ ช่วยในการตรวจสอบความปลอดภัยของเครือข่ายโดยการติดตามอุปกรณ์ทั้งหมดที่เชื่อมต่อกับเครือข่ายหนึ่งๆ

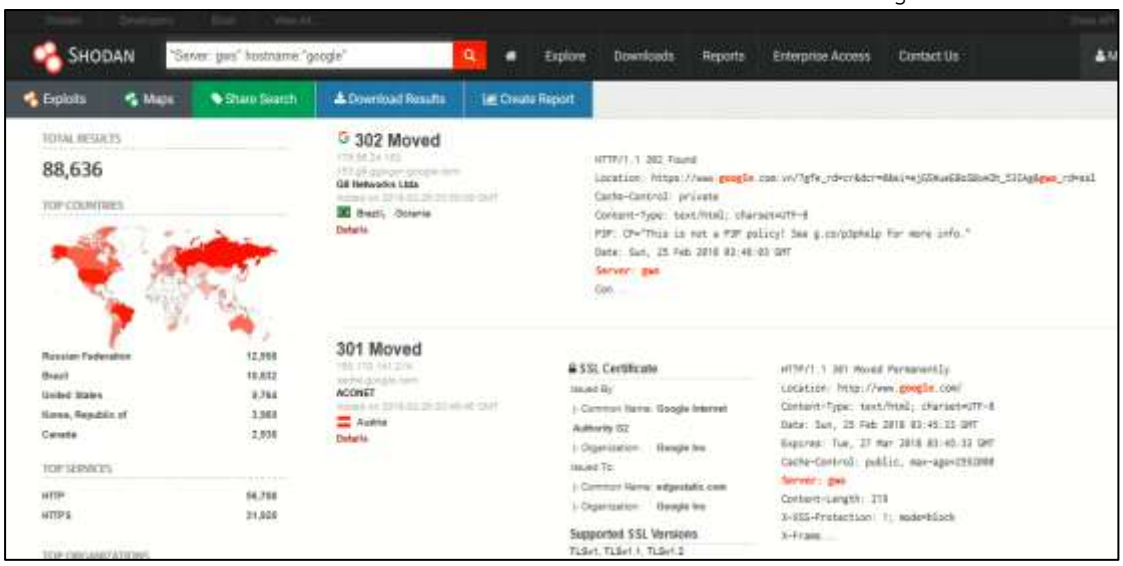
๘.๒ ใช้เพื่อค้นหาอุปกรณ์ IoT รวมถึงผู้ใช้หลัก

๘.๓ ด้วยเซิร์ฟเวอร์ที่มีอยู่ทั่วโลก ระบบจะรวบรวมข้อมูลอินเทอร์เน็ตตลอด ๒๔ ชั่วโมง XNUMX วันต่อสัปดาห์ และนำเสนอข่าวกรองที่ทันสมัยที่สุด

๘.๔ Shodan สร้างความได้เปรียบในการแข่งขันด้วยการดำเนินการตามข้อมูลตลาดเชิงประจักษ์

๘.๕ ช่วยให้สามารถทำงานร่วมกับเทคโนโลยีอื่นๆ ได้

แผนภาพที่ ๒ – ๕ การแสดงผลลัพธ์ของเครื่องมือ Shodan ในการค้นหา “Google Web Server”



ที่มา: https://www.yeahhub.com/shodan-search-examples/

๙. Google Dorks เป็นฐานข้อมูลของข้อความค้นหาของ Google ที่พยายามค้นหาข้อมูลที่เปิดเผยต่อสาธารณะ หรือที่เรียกว่า GHDB (ฐานข้อมูลแฮ็กของ Google) โดยผู้ที่ตกเป็นเหยื่อจะใส่ข้อมูลที่ละเอียดอ่อนบนอินเทอร์เน็ตโดยไม่รู้ตัว เช่น เว็บคอนโซลที่ไม่มีการป้องกัน พอร์ตเปิด Portal การเข้าสู่ระบบ โฟลเดอร์ที่ละเอียดอ่อน กล้องที่เปิดอยู่ ไฟล์ที่มีข้อมูลชื่อผู้ใช้ และอื่น ๆ ที่เปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ต มีคุณสมบัติดังนี้

๙.๑ สามารถใช้ทำแผนที่เครือข่ายได้ เนื่องจาก Simple Dorks ค้นหาโดเมนย่อย

๙.๒ Google Dorks มีบริการสำหรับ Open-Source Network Intelligence Tools และเครื่องมือค้นหาต่าง ๆ

๙.๓ สามารถเจาะลึกเข้าไปในที่เก็บถาวรของเซิร์ฟเวอร์และรับข้อมูลเกี่ยวกับ Argument ต่าง ๆ

๑๐. Metagoofil คือ คอลเล็กชันข้อมูลเมตา recon แบบพาสซีฟฟรีที่ใช้ Python เพื่อดึงข้อมูลจากเอกสารต่าง ๆ เช่น pdf, doc, xls, ppt, ODP เป็นต้น ที่ค้นพบบนเว็บไซต์ของเป้าหมายหรือไซต์สาธารณะอื่น ๆ ยูทิลิตีค้นหาเอกสารโดยใช้ Google จากนั้นดาวน์โหลดไปยังไดรฟ์ในเครื่องและแยกข้อมูลเมตาทั้งหมด จะตรวจสอบข้อมูลเมตาของเอกสารเหล่านี้และรวบรวมข้อมูลจำนวนมาก สามารถระบุตำแหน่งข้อมูลที่ละเอียดอ่อน เช่น ชื่อผู้ใช้ ข้อมูลระบุตัวตนจริง เวอร์ชันซอฟต์แวร์ อีเมล และเส้นทาง/เซิร์ฟเวอร์ มีคุณสมบัติดังนี้

๑๐.๑ สามารถรับรู้ข้อมูลเส้นทางซึ่งช่วยในการทำแผนที่เครือข่าย

๑๐.๒ ค้นหาและดึงข้อมูลจากไฟล์ในเครื่องหรือไฟล์บนเว็บเพจ

๑๐.๓ สามารถโคลนและติดตั้งได้อย่างง่ายดาย โดยใช้เว็บไซต์ GitHub

๑๐.๔ สามารถดึงข้อมูล MAC Address จากเอกสารต่าง ๆ ได้

๑๑. TinEye เป็นเครื่องมือค้นหารูปภาพบนอินเทอร์เน็ตที่ทำงานย้อนกลับ (Image Search Engine) โดยสามารถอัปโหลดรูปถ่ายเพื่อเรียนรู้ว่าพวกเขาถ่ายที่ไหน ใช้ที่ไหน และหากมีเวอร์ชั่นที่เปลี่ยนแปลง เทคโนโลยีการจดจำภาพถูกนำมาใช้แทนคำสำคัญ ข้อมูลเมตา หรือลายน้ำ การศึกษาของ TinEye ระบุว่า จะค้นหาภาพได้อย่างแม่นยำ แม้ว่าจะย่อขนาด ครอบตัด และดัดแปลงก็ตาม มีคุณสมบัติดังนี้

๑๑.๑ ย้อนกลับการค้นหา เพื่อค้นหาว่ารูปภาพมาจากไหนหรือเรียนรู้เพิ่มเติมเกี่ยวกับรูปภาพนั้น

๑๑.๒ ตรวจสอบหรือติดตามลักษณะที่ปรากฏของภาพบนอินเทอร์เน็ต

๑๑.๓ ระบุหน้าเว็บที่ใช้รูปภาพที่คุณสร้างขึ้น

๑๒. Searchcode เป็น Search Engine ที่ไม่ซ้ำแบบใครที่แสวงหาข่าวกรองในรหัสโอเพนซอร์ซ นักพัฒนาสามารถใช้เพื่อค้นหาปัญหาเกี่ยวกับการเข้าถึงข้อมูลที่ละเอียดอ่อนในโค้ด โดยจะทำงานคล้ายกับ Google ยกเว้นว่าแทนที่จะสร้างดัชนีเว็บเซิร์ฟเวอร์ เครื่องมือค้นหาจะค้นหาข้อมูลภายในบรรทัดของโค้ดในแอปที่ใช้งานอยู่หรือในแอปที่กำลังพัฒนา แฮ็กเกอร์สามารถใช้ผลการค้นหาเพื่อค้นหาชื่อผู้ใช้ ช่องโหว่ หรือข้อบกพร่องในโค้ด นอกจากนี้ Searchcode ค้นหาที่เก็บโค้ด เช่น GitHub, Bitbucket, Google Code, GitLab, CodePlex และอื่นๆ คุณยังสามารถกรองภาษาตามชนิดของมันได้ มีคุณสมบัติดังนี้

๑๒.๑ เป็นเครื่องมือค้นหาโค้ดบนเว็บที่ให้บริการฟรี

๑๒.๒ นักพัฒนาสามารถใช้อักขระพิเศษเพื่อค้นหา

๑๒.๓ เป็นไปได้ที่จะกรองโค้ดสำหรับภาษาหรือที่เก็บข้อมูลต่างๆ

๑๒.๔ คุณสามารถใช้ผลการค้นหาเพื่อระบุชื่อผู้ใช้หรือช่องโหว่ในรหัส

จากข้อมูลของ Social Links (๒๕๖๕) ได้นำเสนอ “OSINT Landscape” กล่าวคือ มีทั้งแบบโปรแกรมฟรี (opensource) และแบบโปรแกรมลิขสิทธิ์ (commercial license) โดยความสามารถของแพลตฟอร์มมีหลายระดับและแตกต่างกันออกไป ตั้งแต่การรวบรวมข้อมูลที่เป็นข้อมูลดิบ นำมาวิเคราะห์ และความสามารถแกะรอย หรือคาดการณ์แนวทางการโจมตีในลำดับต่อไป เพื่อเป็นข้อมูลให้เจ้าหน้าที่ปฏิบัติการ และผู้บังคับบัญชาสามารถตัดสินใจได้อย่างทันท่วงที OSINT เป็นอีกเครื่องมือที่ใช้ในการรวมรวมข่าวสารโดยอัตโนมัติที่บูรณาการ มีวัตถุประสงค์เพื่อสกัดกั้นการโจมตีซ้ำ และระบุการเส้นทางการโจมตี และช่วยเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย ซึ่งประกอบด้วยประเภทของเครื่องมือ ดังต่อไปนี้

๑. Social media intelligence (SOCMINT)

๒. Chat/Messenger Intelligence

๓. Intelligence Platforms

๔. Image/Video/Text/ Audio intelligence

๕. Dark Web Intelligence

๖. Case Management

๗. Blockchain Analytics

๘. Graph Analysis
๙. Geospatial Intelligence (GEOINT)
๑๐. Threat Intelligence
๑๑. Web Intelligence (WEBINT)
๑๒. Asset Tracking

แผนภาพที่ ๒ – ๖ OSINT Landscape

ที่มา: https://blog.sociallinks.io/osint-landscape/

การแลกเปลี่ยนข้อมูลกลางภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) อธิบายไว้ว่า ในช่วงหลายปีที่ผ่านมารัฐบาลได้พยายามผลักดันให้มีการนำเทคโนโลยีดิจิทัลมาใช้เพื่อพัฒนาระบบการทำงานและการให้บริการภาครัฐที่สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ รวมถึงการตราพระราชบัญญัติ การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ เพื่อกำหนดแนวทางการประยุกต์ใช้เทคโนโลยีดิจิทัลในการบริหารราชการแผ่นดิน ซึ่งเป็นไปตามข้อเสนอแนะของสภาปฏิรูปประเทศแห่งชาติ (สปช.) และสภาขับเคลื่อนการปฏิรูปประเทศ (สปท.) เพื่อยกระดับรัฐบาลไปสู่การเป็น “รัฐบาลแห่งการเชื่อมโยงและเปิดเผย” หรือ “Open and Connected Government”

สพร. จัดทำระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (Government Data Exchange: GDX) ขึ้นเพื่อทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัล และทะเบียนดิจิทัล ระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล ตามที่กำหนดไว้ในพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๑๕

ปัจจุบันมีหน่วยงานที่เชื่อมโยงข้อมูลกับระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) ๑๙๔ หน่วยงาน และในปีงบประมาณ พ.ศ. ๒๕๖๔ ที่ผ่านมา มีการเชื่อมโยงข้อมูลผ่านระบบ GDX กว่า ๓๕.๓ ล้านครั้ง และมีหน่วยงานที่เปิดให้เชื่อมโยงข้อมูลผ่านระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) ๗ หน่วยงาน เช่น กรมการปกครอง กรมพัฒนาธุรกิจการค้า กรมส่งเสริมสหกรณ์ เป็นต้น

ระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) ทำหน้าที่เป็นตัวกลาง (Gateway) ระหว่างระบบดิจิทัลของหน่วยงานผู้ใช้ข้อมูล (Consumer) และหน่วยงานผู้จัดทำและครอบครองข้อมูลดิจิทัล (Producer) โดยขั้นตอนในการเชื่อมโยงข้อมูลผ่านระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) มีดังนี้

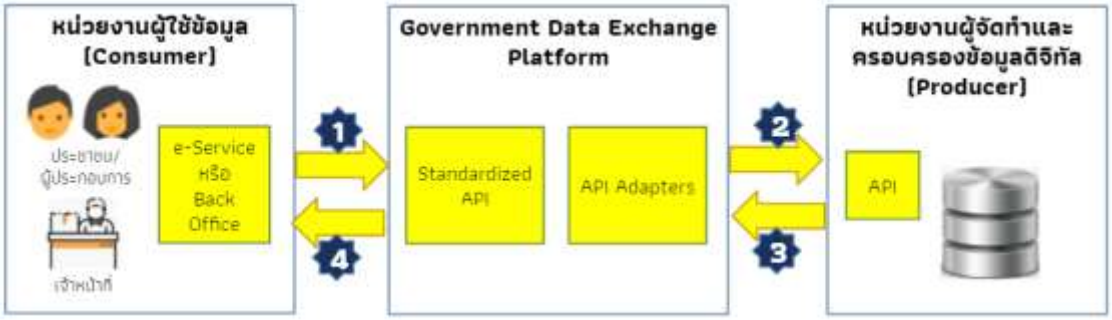
๑. ระบบให้บริการประชาชน (e-Service) หรือระบบสนับสนุนการให้บริการ (Back Office) ของหน่วยงานผู้ใช้ข้อมูล (Consumer) ส่งคำร้องขอข้อมูล (Request) ไปยังระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX)

๒. ระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) ตรวจสอบว่าหน่วยงานผู้ร้องขอข้อมูลได้รับสิทธิ์จากหน่วยงานผู้จัดทำและครอบครองข้อมูลดิจิทัล (Producer) หรือไม่ หากหน่วยงานผู้ร้องขอข้อมูลมีสิทธิ์ดังกล่าว ระบบ GDX จะทำส่งต่อคำร้องขอข้อมูลไปยังหน่วยงานผู้จัดทำและครอบครองข้อมูลดิจิทัล (Producer)

๓. หน่วยงานผู้จัดทำและครอบครองข้อมูลดิจิทัล (Producer) ทำการเรียกข้อมูลตามที่ได้รับร้องขอจากระบบฐานข้อมูลตามคำร้องขอข้อมูลที่ได้รับ และส่งข้อมูลที่เรียกได้ไปยังระบบ GDX

๔. ระบบ GDX ทำการส่งต่อข้อมูลที่ได้รับจากหน่วยงานผู้จัดทำและครอบครองข้อมูลดิจิทัล (Producer) ไปยังระบบให้บริการประชาชน (e-Service) หรือระบบสนับสนุนการให้บริการ (Back Office) ของหน่วยงานผู้ใช้ข้อมูล (Consumer) โดยไม่มีการจัดเก็บข้อมูลที่รับส่งไว้ที่ระบบ GDX แต่อย่างใด

แผนภาพที่ ๒ – ๗ ลักษณะเชิงเทคนิค ของระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX)



ที่มา: สำนักงานพัฒนารัฐบาลดิจิทัล. https://www.dga.or.th/

กล่าวโดยสรุป คือ “Government Data Exchange” เน้นการแลกเปลี่ยนข้อมูลให้บริการประชาชนเป็นหลัก แต่ยังขาดการแลกเปลี่ยนข้อมูลภัยคุกคาม (Threats) ระหว่างหน่วยงานรัฐกับรัฐ หรือในบริบทของหน่วยงานด้านความมั่นคง

การรักษาความมั่นคงปลอดภัยของระบบศูนย์แลกเปลี่ยนข้อมูลกลาง

ปัจจุบันระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) ติดตั้งอยู่บนระบบคลาวด์ที่ให้บริการและบริหารจัดการ โดย สพร. ระบบคลาวด์ภาครัฐมีระดับเสถียรภาพ (SLA) ไม่น้อยกว่าร้อยละ ๙๙.๕ และเป็นระบบที่มีมาตรการป้องกันการโจรกรรมข้อมูลอย่างรัดกุม มีความปลอดภัยสูง และได้รับการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems – ISMS) ทั้งนี้ แอปพลิเคชัน และระบบงานต่าง ๆ ที่เกี่ยวข้อง มีการดำเนินงานต่างๆ ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

นอกจากนี้ ระบบศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐได้รับการพัฒนาขึ้น โดยคำนึงถึงความมั่นคงปลอดภัยต่าง ๆ ดังนี้

๑. การพัฒนาแอปพลิเคชัน ระบบ และแพลตฟอร์มต่าง ๆ ของ สพร. ดำเนินการภายใต้มาตรฐาน ISO/IEC ๙๐๐๑

๒. ก่อนที่จะเปิดแอปพลิเคชัน ระบบและแพลตฟอร์ม เพื่อให้บริการจริง แอปพลิเคชัน ระบบ และแพลตฟอร์มดังกล่าวจะต้องผ่านการทดสอบ ทั้งในด้านคุณสมบัติ (Functional Test) และด้านอื่นๆ (Non-Functional Test) เช่น Performance Test และ Security Test โดยผลการทดสอบต้องแสดงให้เห็นว่าระบบทำงานได้โดยสมบูรณ์ มีระดับความมั่นคงสูง (Highly Available) มีความเสี่ยงด้านความปลอดภัยต่ำ

สพร. ทดสอบความปลอดภัยของแอปพลิเคชันและแพลตฟอร์ม (Security Test) โดยใช้อย่างน้อย ๒ วิธี ดังนี้

๑. Static Application Security Testing (SAST) ซึ่งเป็นการตรวจสอบ Source Code ของแอปพลิเคชัน และแพลตฟอร์มที่เขียนขึ้น ว่าเป็นการเขียนโปรแกรมที่มีความเสี่ยงที่จะถูกโจมตี หรือถูกเจาะโดยผู้ไม่หวังดีมากน้อยเพียงใด

๒. Vulnerability Assessment (VA) เป็นการตรวจสอบแอปพลิเคชันและแพลตฟอร์มที่ติดตั้งแล้วในภาพรวม ว่ามีความเสี่ยงที่จะถูกโจมตีเนื่องจากการตั้งค่า (Settings) ต่าง ๆ หรือโครงสร้างพื้นฐานที่ไม่ปลอดภัยเพียงพอหรือไม่

การคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่หน่วยงานมีข้อมูลดิจิทัลที่เป็นข้อมูลส่วนบุคคล และจะเปิดให้หน่วยงานอื่นเชื่อมโยงข้อมูลดังกล่าวได้ผ่านระบบศูนย์แลกเปลี่ยนข้อมูลกลางนั้น ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หน่วยงานมีสิทธิในการเข้าถึงข้อมูลดิจิทัลถือเป็น “ผู้คุ้มครองข้อมูลส่วนบุคคล (Data Controller)” และ (ตามมาตรา ๒๗) ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๗ ซึ่งครอบคลุมถึง

เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา ๒๔(๔))

เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (มาตรา ๒๔(๕))

ทั้งนี้ ระบบศูนย์แลกเปลี่ยนข้อมูลกลาง ถือเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)” ซึ่ง ดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา ๖) และ สพร. มีการดำเนินการต่างตามที่กำหนดในมาตรา ๔๐ กล่าวคือ

๑. ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับ จากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครอง ข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

๒. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้ง แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๓. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ดังนั้น หน่วยงานที่มีข้อมูลดิจิทัลสามารถกำหนดข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล หรือคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล เพื่อกำหนดให้ สพร. ทำหน้าที่อำนวยความสะดวกในการเชื่อมโยงข้อมูลระหว่างหน่วยงาน โดยจัดทำข้อตกลง/คำสั่งดังกล่าวในรูปแบบสัญญาผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับ สพร. ได้

ความท้าทายสำคัญของกระบวนการแลกเปลี่ยนข้อมูล OSINT

ปัจจุบันหน่วยงานด้านข่าวกรองและความมั่นคงของประเทศไทยมีศักยภาพในการใช้ประโยชน์จากแหล่งเปิด และได้ใช้แหล่งเปิดเป็นองค์ประกอบสำคัญในการผลิตเป็นรายงานข่าวกรองมาเป็นเวลายาวนาน โดยมุ่งเน้นการใช้เครื่องมือด้านการข่าวพิเศษที่เรียกว่า HUMINT และ SIGINT แต่การใช้ประโยชน์จากแหล่งเปิด (OSINT) ของหน่วยข่าวกรองของไทยที่ผ่านมา พบว่า ยังเป็นเพียงการใช้แหล่งเปิดในแง่ของการรวบรวมข้อมูลข่าวสาร เพื่อนำมาใช้ร่วมกับข่าวสารอื่นที่ได้จากการปฏิบัติการพิเศษดังกล่าว โดยมีค่อนข้างน้อยที่ใช้แหล่งเปิดเพียงอย่างเดียวในการผลิตเป็นรายงานข่าวกรอง ที่เป็นเช่นนี้เพราะไม่มั่นใจในความถูกต้องน่าเชื่อถือของข้อมูลข่าวสาร รวมทั้งยังขาดการศึกษาค้นคว้ากระบวนการที่จะนำข่าวเปิดมาใช้เป็นรายงานข่าวกรองอย่างเป็นหลักวิชาการ จากรายงานผลการศึกษาของ McAfee Labs, ๒๐๑๗ ได้สรุปประเด็นความท้าทายสำคัญของกระบวนการแลกเปลี่ยนข้อมูล OSINT ไว้ ๕ ด้าน ดังนี้

๑. ปริมาณ (Volume) หมายถึง เซ็นเซอร์ (Sensor) เครื่องมือการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) และ Machine Learning ก่อให้เกิดปัญหาข้อมูลไร้ประโยชน์เป็นจำนวนมาก ซึ่งส่งผลกระทบต่อการคัดแยก ประมวลผล และดำเนินการเพื่อสร้างข้อมูล OSINT

๒. การตรวจสอบ (Validation) หมายถึง แหล่งที่มาของข้อมูล (Source) ต้องได้รับการตรวจสอบอย่างละเอียด เพื่อให้มั่นใจว่าข้อมูลที่ได้มามีความถูกต้อง ทั้งนี้ หลักการวิเคราะห์ข่าวกรองจากแหล่งเปิดไม่ได้แตกต่างจากหลักการวิเคราะห์ข่าวกรองโดยทั่วไป แต่จะต้องมีความระมัดระวังอย่างมาก เพราะด้วยข้อมูลข่าวสารจำนวนมาก โดยเฉพาะจากอินเทอร์เน็ต (Internet) ท่ามกลางกระแสการสร้าง fake news และการสร้าง false narratives ที่มีมากขึ้นใน ปัจจุบันจึงจำเป็นต้องคัดสรร กลั่นกรอง และตรวจสอบความน่าเชื่อถือของข่าวและแหล่งข่าวนั้นเป็นพิเศษ รวมทั้ง ต้องระมัดระวังเรื่องความคิดที่เป็นอคติ (bias or prejudice) หรือความลำเอียงทางอุดมการณ์ (ideological preference) ของตัวนักวิเคราะห์เอง

๓. คุณภาพ (Quality) หมายถึง ฟิลเตอร์ แท็ก และการขจัดความซ้ำซ้อนของข้อมูลโดยอัตโนมัติ เป็นกระบวนการสำคัญในการรับข้อมูลจากแหล่งที่มาต่าง ๆ

๔. ความรวดเร็ว (Speed) หมายถึง การแลกเปลี่ยนข้อมูลแบบเปิด (OSINT) ที่ได้มาตรฐานช่วยขจัดปัญหาด้านความล่าช้าของการส่งข้อมูลภัยคุกคามหลังจากตรวจจับได้ เข้าสู่ระบบข่าวกรองภัยคุกคามไซเบอร์ (CTI)

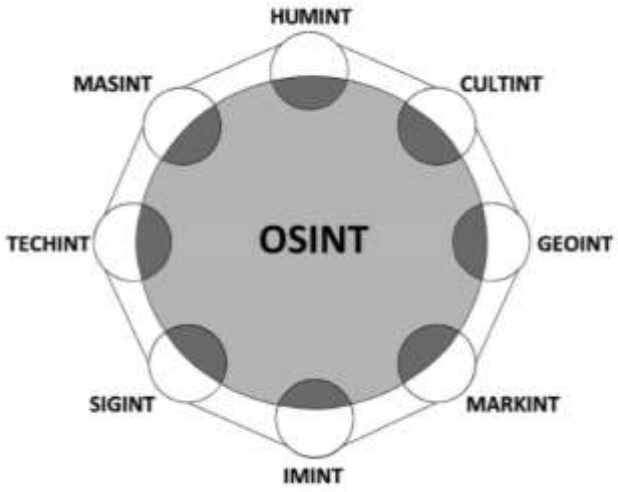
๕. ความสัมพันธ์ (Correlation) หมายถึง การเชื่อมโยงความสัมพันธ์ระหว่างระบบปฏิบัติการ อุปกรณ์ และระบบเครือข่าย รวมไปถึงการคัดแยกเหตุการณ์และการกำหนดขอบเขตในการตอบสนองเป็นสิ่งสำคัญเพื่อให้สามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ

นอกจากนี้ ฉัตรพงศ์ (๒๕๕๓) ได้อธิบายไว้ว่า การผลิตข่าวกรองจากแหล่งเปิด (OSINT) มีองค์ประกอบเดียวกับงานผลิตข่าวกรองทั่วไปที่ใช้อยู่ในปัจจุบัน (All-Sources Intelligence) หากแต่ในกระบวนการผลิตข่าวกรองรูปแบบเดิมนั้นถือว่าข่าวจากแหล่งเปิด (Open Sources) อยู่ในขั้นตอนของการรวบรวม โดยจะนำข่าวสารจากแหล่งเปิดที่ได้ไปรวมกับข่าวสารที่ได้จากการรวบรวมด้วยวิธีการปฏิบัติการลับและการใช้เครื่องมือทางเทคนิคต่าง ๆ เช่น HUMINT และ SIGINT เพื่อนำไปดำเนินกรรมวิธี และดำเนินการวิเคราะห์ เพื่อผลิตเป็นรายงานข่าวกรองเสนอต่อผู้บังคับบัญชาหรือ

ผู้ใช้ข่าว อย่างไรก็ตาม หากพิจารณาเปรียบเทียบระหว่าง OSINT กับ All-Sources Intelligence ที่ยังใช้ปฏิบัติกันอย่างแพร่หลายในปัจจุบัน โดยเทียบเคียงตั้งแต่ขั้นตอนของการกำหนดความต้องการข่าวสาร การรวบรวม การดำเนินกรรมวิธีไปจนถึงการวิเคราะห์ จะเห็นจุดเด่นของ OSINT และความแตกต่างกับ All-Sources Intelligence หลายประการ

การเปลี่ยนจากวิธีหนึ่งไปเป็นอีกวิธีหนึ่ง (หรือเส้นขอบที่เบลอระหว่างวิธี) สามารถเข้าใจได้ง่ายกว่าในการนำเสนอตามภาพที่ ๘ (Hribar, ๒๐๑๔) เมื่อวงกลมที่ใหญ่ที่สุดและสีเทาอ่อนแสดงถึง OSINT คิดเป็นร้อยละ ๘๐ - ๙๐ ของข้อมูลที่เก็บรวบรวมทั้งหมด ส่วนวงกลมขนาดเล็กอื่น ๆ แสดงถึงวิธีการรวบรวมข่าวกรองอื่น ๆ ส่วนสีเทาเข้มของวงกลมขนาดเล็กแสดงถึงโซนสีเทาของ OSINT ซึ่งเป็นส่วนผสมของวิธีการรวบรวมที่ไม่สามารถจัดประเภทเป็น OSINT หรือวิธีการรวบรวมอื่น ๆ อย่างไรก็ตาม พื้นที่สีเทาก็จะสามารถขยายและครอบคลุมพื้นที่ส่วนใหญ่ได้

แผนภาพที่ ๒ – ๘ พื้นที่สีเทาของ OSINT – การเปลี่ยนวิธีการรวบรวมข้อมูลแบบถูกกฎหมาย เป็นกึ่งกฎหมาย หรือผิดกฎหมาย



ที่มา: Hribar, 2014.

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยข่าวกรองแบบเปิดของต่างประเทศ

๑. ประเทศสหรัฐอเมริกา

สำหรับรูปแบบการดำเนินงานของหน่วยข่าวกรองจากแหล่งเปิดในประเทศต่าง ๆ นั้น กล่าวได้ว่า OSINT สหรัฐอเมริกามีความเป็นรูปธรรมมากที่สุดในฐานะเป็นต้นแบบของงาน OSINT ทั่วโลก (Good Practice) แม้กระทั่งหน่วยข่าวกรองของอังกฤษ ฝรั่งเศส ออสเตรเลีย จีน ญี่ปุ่น และสิงคโปร์ ก็ใช้เป็นต้นแบบ โดยสหรัฐฯ มีหน่วยงานที่สำคัญดังนี้

๑.๑ สำนักข่าวกรองกลางสหรัฐ (Central Intelligence Agency: CIA) มีหน้าที่รับผิดชอบงานด้านการสืบราชการลับ และต่อต้านการสืบราชการลับจากนอกสหรัฐอเมริกา มีหน่วยงานด้าน OSINT ในสังกัดที่มีความสำคัญ ประกอบด้วย

๑.๑.๑ Foreign Broadcast Information Service (FBIS)

๑.๑.๒ National Collection Division (NCD) มีหน่วยงานในสังกัดกองทัพภายใต้โครงการ External Research and Analysis และมี Community Open Source Program Office (COSPO) เป็นหน่วยประสานงานในประชาคมข่าวกรองสหรัฐฯ

โดยสหรัฐฯ มีโครงสร้างการจัดตั้งหน่วยงานด้านการข่าวกรองแบบเปิดตามต้นแบบของประเทศสหรัฐอเมริกา (The US Model) ของ Best RA, Cumming A (2007) มีรายละเอียดดังนี้

๑. ผู้ช่วยรองผู้อำนวยการ, ข่าวกรองแห่งชาติ ว่าด้วยการข่าวกรองแบบเปิด (Assistant Deputy Director of National Intelligence for Open Source) มีอำนาจหน้าที่ดังนี้

๑.๑ กำหนดกลยุทธ์ นโยบาย และแนวทางปฏิบัติ ด้านการข่าวกรองแบบเปิด

๑.๒ ตรวจสอบการพัฒนาสถาปัตยกรรม “a single open source”

๑.๓ ให้คำแนะนำแก่หน่วยงานและแผนกต่าง ๆ ทั้งภายในและภายนอก ข่าวกรองแห่งชาติ เกี่ยวกับการได้มาซึ่ง OSINT

๒. คณะกรรมการว่าด้วยการข่าวกรองแบบเปิดแห่งชาติ (National Open Source Committee)

๒.๑ ให้คำแนะนำแก่องค์กรโอเพ่นซอร์สระดับชาติ

๒.๒ คณะกรรมการ ประกอบด้วย ผู้บริหารระดับสูงจากศูนย์โอเพ่นซอร์ส, สำนักงานปลัดกระทรวงกลาโหม, กระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐ, สำนักข่าวกรองกลาง (CIA), สำนักงานความมั่นคงแห่งชาติ (NSA), สำนักงานภูมิสารสนเทศแห่งชาติ, สำนักงานวิจัย กระทรวงการต่างประเทศ, สำนักข่าวกรองกลาโหม และสำนักงานสืบสวนกลางแห่งสหรัฐอเมริกา

๓) ศูนย์โอเพ่นซอร์ส (Open Source Center)

๓.๑ ก่อตั้งเมื่อปี พ.ศ. 2548 โดยผู้อำนวยการหน่วยข่าวกรองแห่งชาติ โดยมีหน่วยงาน CIA เป็นตัวแทนในการบริหาร

๓.๒ พนักงานประจำ ประมาณ ๑๐๐ อัตรา

๓.๓ ยกระดับการใช้ประโยชน์จากเนื้อหาโอเพ่นซอร์สของชุมชนข่าวกรอง เพื่อช่วยในการพัฒนาศูนย์โอเพ่นซอร์สขนาดเล็กภายในหน่วยงานที่เกี่ยวข้อง

๓.๔ การซื้อกิจการ การจัดซื้อจัดจ้าง การวิเคราะห์ การเผยแพร่ และการแบ่งปันข้อมูลโอเพ่นซอร์ส ผลิตภัณฑ์ และบริการภาครัฐ

๓.๕ จัดทำรายงาน การแปล และผลิตภัณฑ์การวิเคราะห์พร้อมให้บริการทางออนไลน์ผ่านเว็บไซต์ที่ปลอดภัยสำหรับเจ้าหน้าที่ของรัฐ (www.opensource.gov)

๒. ประเทศอังกฤษ

กลไกข่าวกรองของสหราชอาณาจักร มีหน่วยงานด้านความมั่นคงและต่อต้านข่าวกรองภายในของสหราชอาณาจักร ประกอบด้วย

๒.๑ เอ็มไอ ๕ หรือ ข่าวกรองทหาร แผนก ๕ (Military Intelligence, Section 5) มีคณะกรรมการข่าวกรองร่วม (Joint Intelligence Committee: JIC) และหน่วยงานนี้อยู่ในบังคับของพระราชบัญญัติหน่วยความมั่นคง ๑๙๘๙ (Security Service Act 1989) หน่วยงานนี้ได้รับมอบหมายให้พิทักษ์รักษาระบอบประชาธิปไตยแบบมีรัฐสภาและผลประโยชน์ทางเศรษฐกิจของประเทศอังกฤษ รวมถึงต่อต้านการก่อการร้ายและต่อต้านจารกรรมภายในสหราชอาณาจักร

๒.๒ หน่วยข่าวกรองลับ (Secret Intelligence Service: SIS)

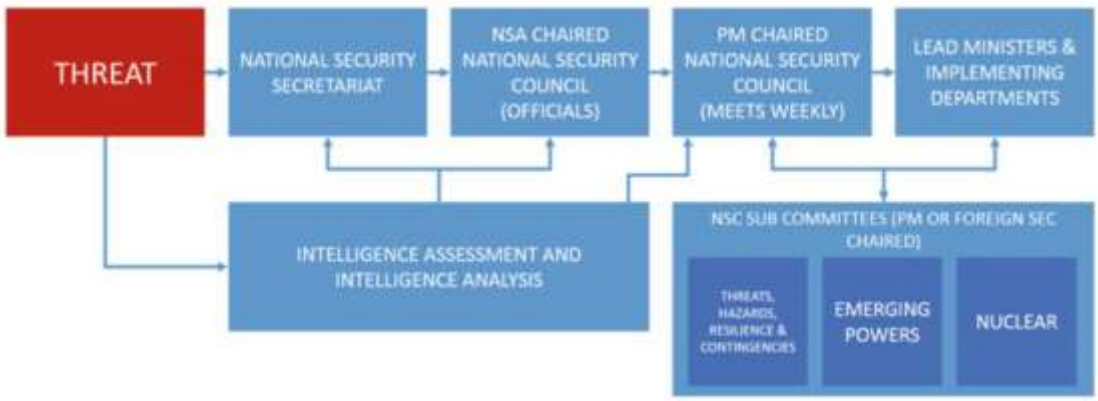
๒.๓ กองบัญชาการสื่อสารของรัฐบาล (Government Communications Headquarters: GCHQ)

๒.๔ สำนักข่าวกรองกลาโหม (Defence Intelligence: DI)

๒.๕ คณะกรรมการข่าวกรองร่วม (Joint Intelligence Committee: JIC)

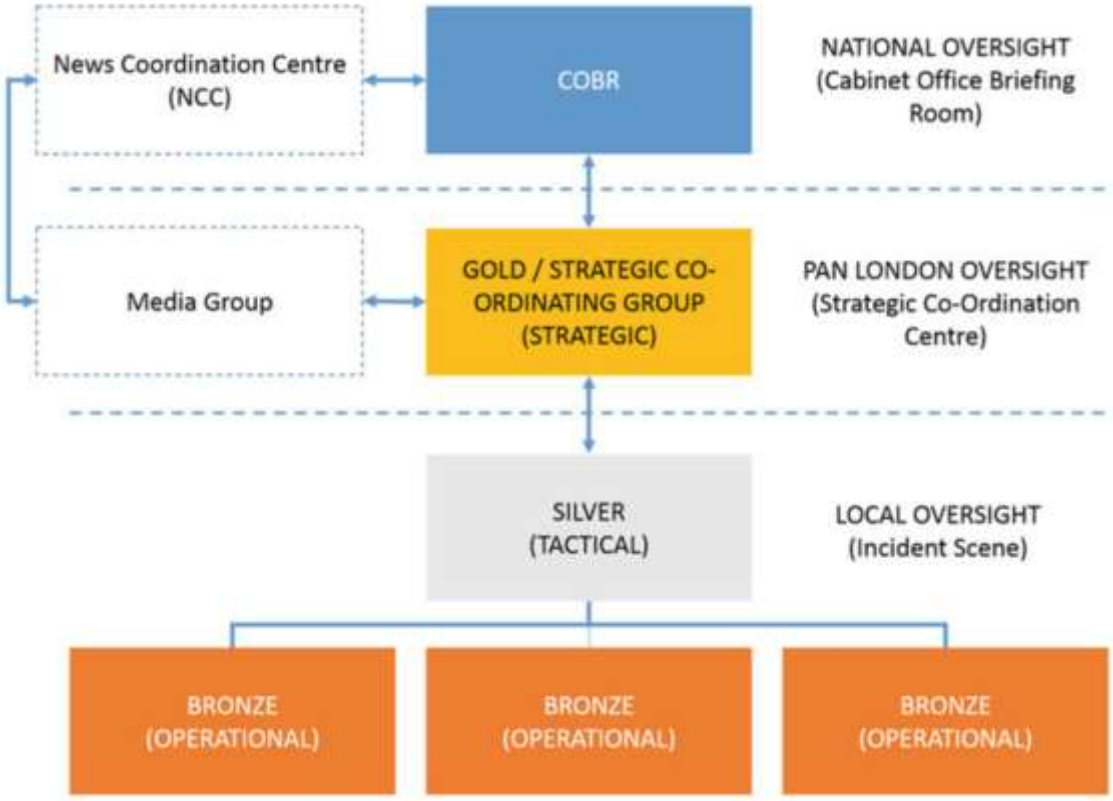
จากแผนภาพที่ ๒ – ๙ ในระดับสูงสุด สภาความมั่นคงแห่งชาติของสหราชอาณาจักร (National Security Council: NSC) และโครงสร้างสนับสนุนช่วยให้ทิศทางเชิงกลยุทธ์มีความชัดเจนมากขึ้น พิจารณารวมความเสี่ยงและภัยคุกคามด้านความมั่นคงของชาติทั้งหมด และประสานการตัดสินใจ รวมถึงการตอบสนองต่อภัยคุกคามที่กำลังเผชิญ ข้อมูลนี้นำมาจาก National Intelligence Machinery รัฐบาลสหราชอาณาจักร ให้ภาพรวมที่มีประโยชน์ว่าหน่วยสืบราชการลับทั้งหมด ไม่ว่าจะเป็น OSINT หรืออื่น ๆ จำเป็นต้องได้รับการพิจารณาในภาพรวม

แผนภาพที่ ๒ – ๙ โครงสร้างสภาความมั่นคงแห่งชาติของสหราชอาณาจักร



ที่มา: รัฐบาลในสมเด็จฯ (HM Government)

แผนภาพที่ ๒ – ๑๐ การกำกับดูแลด้านการปฏิบัติการและยุทธวิธี



ที่มา: รัฐบาลในสมเด็จฯ (HM Government)

จากแผนภาพที่ ๒ – ๑๐ อธิบายถึงการกำกับดูแลด้านการปฏิบัติการและยุทธวิธี พบว่าความสามารถในการรวบรวมข้อมูล การรวมข้อมูลจากแหล่งต่าง ๆ เพื่อประมวลผลและวิเคราะห์ข้อมูล และใช้งานเพื่อสร้างรูปภาพข้อมูลที่เป็นที่รู้จักทั่วไป ซึ่งสามารถแจ้งการตัดสินใจสั่งการของผู้บัญชาการระดับ Gold, Silver และ Bronze นั้น ในเชิงปฏิบัติแล้วยังขาดความพร้อมด้านข้อมูล เนื่องจากการเติบโตของแหล่งที่มา (Source) และความต้องการของ OSINT สามารถทำให้สิ่งต่าง ๆ เพิ่มขึ้นได้ การสร้างการรับรู้สถานการณ์ในระดับที่จำเป็นในหลายเหตุการณ์ที่เผชิญในศตวรรษที่ ๒๑ และเปิดใช้งานวิธีการสำหรับการตัดสินใจที่มีข้อมูลดีขึ้น ซึ่งจะต้องส่งผลในทุกระดับของสายการบังคับบัญชา และการตัดสินใจ

๓. ประเทศรัสเซีย

๓.๑ จัดตั้งหน่วยงาน National Center for Automated Date Exchange with Foreign Computer Networks and Data Banks (NCADE) โดยมีเครือข่ายเชื่อมโยงกับฐานข้อมูลของสหรัฐฯ แคนาดา เยอรมนี อังกฤษ และฝรั่งเศส

๓.๒ หน่วยข่าวกรองต่างประเทศของรัสเซีย (Foreign Intelligence Service of the Russian Federation - SVR) ได้พัฒนาแพลตฟอร์มดิจิทัลสำหรับชาวรัสเซียที่อาศัยอยู่ในต่างประเทศแจ้งข้อมูลภัยคุกคามที่กระทบต่อความมั่นคงแห่งชาติอย่างปลอดภัยและนิรนามผ่านเครือข่ายอินเทอร์เน็ตใต้ดิน (TOR Network) คล้ายกับโครงการ SecureDrop ซึ่งเป็นซอฟต์แวร์แบบ

Open Source ที่สนับสนุนให้องค์กรสื่อสารมวลชนหรือองค์กรพัฒนาเอกชน (NGO) สามารถรับข้อมูลข่าวสารจากบุคคลนิรนามได้อย่างปลอดภัย อย่างไรก็ตาม หน่วยข่าวกรองต่างประเทศของรัสเซีย มิได้เปิดเผยแพลตฟอร์มดังกล่าวอย่างเป็นทางการ แต่เพิ่มลิงค์ในเว็บไซต์ของหน่วยข่าวกรองต่างประเทศ เมื่อ ๓๐ ธ.ค. ๒๕๖๓ (therecord.media, ๒๕๖๔)

แนวคิดและทฤษฎีในการพัฒนาระบบข่าวกรองแบบเปิด

การพัฒนาระบบข่าวกรองแบบเปิด (OSINT) หมายถึง การพัฒนาระบบที่จัดการรวบรวมข้อมูลจากแหล่งข่าวต่าง ๆ โดยตรวจสอบภัยคุกคามทุกรูปแบบทั้งภัยคุกคามทางไซเบอร์ (Cyber Threat) และภัยคุกคามรูปแบบใหม่ (Non-Traditional Threat) แบบ Outside-In คือ การมุ่งเน้นไปที่การตรวจสอบจากแหล่งข้อมูลภายนอก ได้แก่ อินเทอร์เน็ต เครือข่ายสังคมออนไลน์ Surface web, Deep web, หรือ Dark web เพื่อค้นหาข้อมูลที่เกี่ยวข้องกับองค์กร เพื่อเพิ่มประสิทธิภาพของข่าวกรองในการรับรู้ถึงภัยคุกคาม (Threats) วิเคราะห์ข้อมูลภัยคุกคามในเชิงลึก (Insights) และลดความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามที่มีเป้าหมายโจมที่ภาพลักษณ์ สื่อ ข้อมูลผู้ใช้บริการและภายในองค์กร

นอกจากนี้ ระบบ OSINT มีความสำคัญในการวิเคราะห์และประมวลผล เพื่อให้เข้าถึงบริบท เช่น แรงจูงใจ เป้าหมาย และพฤติกรรมการโจมตีของผู้ไม่ประสงค์ดี พร้อมแนบข้อมูลจำเพาะเกี่ยวกับกลุ่มผู้ไม่ประสงค์ดี วัตถุประสงค์เบื้องหลัง Tactics, Techniques, Procedures (TTPs) ที่กลุ่มผู้ไม่ประสงค์ดีใช้มาให้ด้วย รวมถึงวิเคราะห์การโจมตีสมัยใหม่มีความซับซ้อน เช่น การใช้วิศวกรรมสังคม (Social Engineering) ส่งผลกระทบต่อทรัพย์สินขององค์กรที่อาจจะเป็นเป้าหมายของผู้ไม่ประสงค์ดี เช่น ข้อมูลองค์กร, ข้อมูลบุคลากร, source code, ชื่อโดเมน เป็นต้น ซึ่งถูกปล่อยอยู่บน Dark web เพื่อให้องค์กรสามารถเตรียมวิธีรับมือได้อย่างมีประสิทธิภาพ

แนวคิดการแบ่งประเภทระบบข่าวกรองแบบเปิด

ระบบข่าวกรองแบบเปิด แบ่งออกเป็นทั้งหมด ๔ ประเภทใหญ่ ประกอบด้วย Strategic, Tactical, Technical และ Operational โดยแต่ละประเภทมีจุดประสงค์ และระดับความเหมาะสมในการนำไปใช้งานแตกต่างกัน ดังนี้

๑. ประเภทกลยุทธ์ (Strategic) มีการวิเคราะห์ในระดับสูงให้ภาพรวม (high-level analysis) แสดงแนวโน้มและทิศทางภาพกว้างตามช่วงเวลา มุ่งเน้นไปที่ผู้รับสารที่ไม่จำเป็นต้องมีความรู้ความเข้าใจทางด้านเทคนิค เช่น สมาชิกของคณะกรรมการบริหาร ผู้บริหาร เป็นต้น ซึ่ง OSINT ประเภทนี้จะครอบคลุมถึงรายการของภัยคุกคาม (Threats) และอภิปรายถึงผลกระทบที่อาจเกิดขึ้นในกรณีที่มีการโจมตีทางไซเบอร์สำเร็จ ตัวอย่างผลผลิตจาก OSINT ประเภทนี้ ได้แก่ Whitepaper รายงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เผยแพร่โดยบริษัทผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ รายงานสรุปผลทางสถิติเรื่องการรั่วไหลของข้อมูล (Data Breach) และการโจมตีทางไซเบอร์ประเภทอื่น ๆ เป็นต้น

๒. ประเภทยุทธวิธี (Tactical) เหมาะสมกับการนำไปใช้งานโดยทีมรักษาความปลอดภัยขององค์กร เนื่องจากเป็น OSINT ที่รวบรวมข้อมูลเรื่องผู้โจมตี แนวโน้มของการโจมตีทางไซเบอร์

แรงจูงใจในการโจมตี เทคนิคและกลยุทธ์ในการโจมตี และวิธีการในการโจมตี เช่น Phishing, DDoS, Rootkit เป็นต้น ที่พยายามจะแฝงตัวเข้าในในระบบสารสนเทศขององค์กร ตัวอย่างผลผลิตจาก OSINT ประเภทนี้ ได้แก่ หมายเลข IP Address ที่มีพฤติกรรมต้องสงสัย และรายชื่อ Domain Name ที่ใช้ในการละเมิดความปลอดภัยของข้อมูลครั้งก่อนและข้อมูล Log ของระบบ

๓. ประเภทเทคนิค (Technical) จะเจาะจงไปที่การค้นหาหลักฐานจากการโจมตีทางไซเบอร์ เพื่อนำมาใช้ในการทำความเข้าใจการโจมตีครั้งอื่น ๆ ที่มีรูปแบบคล้ายคลึงกัน ยกตัวอย่าง เช่น รายงานทางเทคนิคที่รวบรวมข้อมูลและทำการวิเคราะห์ Indicator of Compromise (IOCs)* โดยรายงานทางเทคนิคด้านภัยคุกคามมากมีอายุการใช้งานที่ไม่ยาวนานเนื่องจากข้อมูลในลักษณะนี้มักเป็นข้อมูลที่ใช้ได้เพียงชั่วคราว ยกตัวอย่าง IOC ที่ควรมีการเฝ้าระวัง เช่น การเปลี่ยนแปลง Registry หรือ System File ที่น่าสงสัย การเปลี่ยนแปลงของขนาดของ HTML Response ที่ผิดปกติไปจากเดิม หรือมีปริมาณคำขอในการเรียกดูไฟล์เดิมซ้ำ ๆ มากผิดปกติ เป็นต้น

๔. ประเภทปฏิบัติการ (Operational) เป็นการรวบรวมข้อมูลที่เกี่ยวข้องว่า การโจมตีที่อาจเป็นไปได้นั้นจะเกิดขึ้นได้อย่างไรบ้าง ภายในข่าวกรองมีข้อมูลในเรื่องของจังหวะในการโจมตี เป้าหมาย แรงจูงใจ และเทคนิคที่ถูกใช้ในการโจมตี ซึ่งการรวบรวมข้อมูลประเภทนี้ ทำได้ยาก เนื่องจากเกี่ยวโยงกับการดักฟังบทสนทนาออนไลน์ของอาชญากรไซเบอร์ ทั้งบนโลกอินเทอร์เน็ตทั่วไปและใน Darknet เช่น เว็บบอร์ดใน Dark Web เป็นต้น ผ่านการแฮกเข้าไปในช่องทางการสื่อสารของเหล่าบรรดาอาชญากร การเก็บรวบรวมข้อมูลประเภทนี้ เป็นเรื่องท้าทายเนื่องจาก

๑. อาชญากรทางไซเบอร์มักจะสื่อสารกันผ่านช่องทางเข้ารหัสและการแฮกเข้าไปในช่องทางดังกล่าวไม่ใช่สิ่งที่ทำได้โดยง่าย

๒. ข้อมูลปริมาณมากที่ได้จากช่องทางออนไลน์ ทำให้การรวบรวมและวิเคราะห์ข้อมูลเป็นเรื่องที่ยากจนเกินไป เช่น การเฝ้าติดตามการสนทนาบน forum หรือห้องแชทบน Darknet ไม่ใช่เรื่องง่ายและยังใช้เวลานาน เนื่องจากต้องผ่านการวิเคราะห์เพื่อให้นำมาใช้งานได้

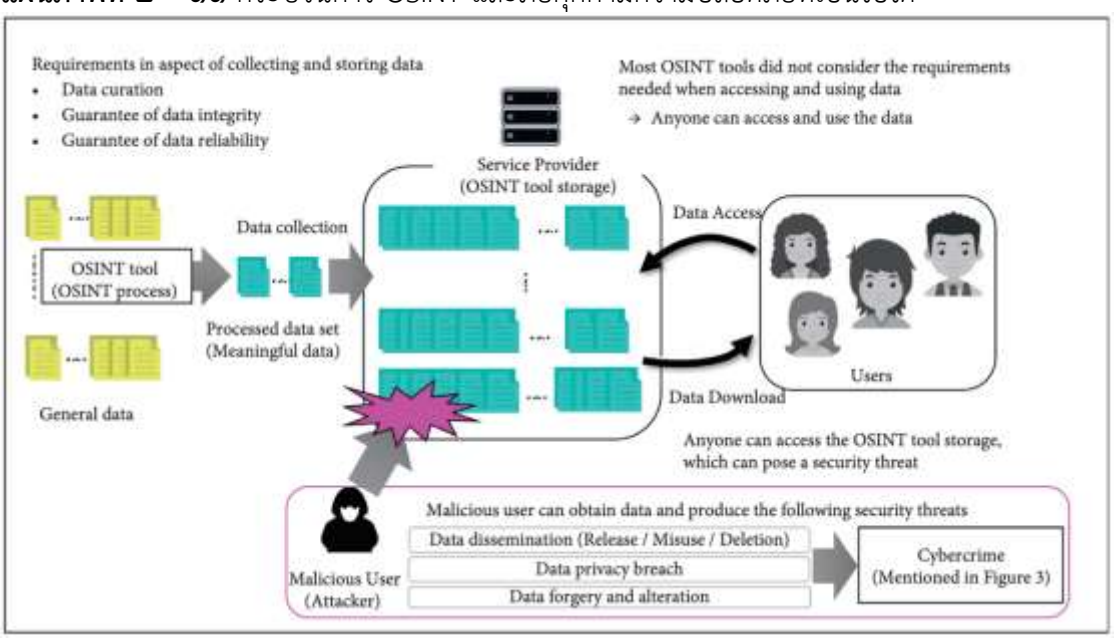
๓. กลุ่มองค์กรอาชญากรรมทางไซเบอร์ใช้วิธีการที่ซับซ้อนในการปกปิดช่องทางการสื่อสาร เช่น การใช้เทคนิคการเข้ารหัสข้อความภายในรูปภาพ (Steganography) และการใช้ภาษาที่คลุมเครือ เพื่อหลบซ่อนจุดประสงค์ที่แท้จริงของการสนทนา เป็นต้น

งานวิจัยที่เกี่ยวข้อง

Yong-Woon Hwang (๒๐๒๒) ได้ศึกษาในหัวข้อ “Current Status and Security Trend of OSINT” จากผลการศึกษา พบว่า ข้อดีของการใช้ข้อมูลที่รวบรวมโดย OSINT คือ สามารถจัดการกับภัยคุกคามความปลอดภัยที่เกิดขึ้นในโลกไซเบอร์ได้ อย่างไรก็ตาม หากผู้ใช้งานใช้ข้อมูลที่รวบรวมโดย OSINT เพื่อวัตถุประสงค์ที่เป็นอันตราย ข้อมูลเกี่ยวกับเป้าหมายของการโจมตีอาจถูกรวบรวมได้ ซึ่งอาจนำไปสู่อาชญากรรมทางไซเบอร์ต่าง ๆ เช่น การแฮ็ก มัลแวร์ และการโจมตีแบบปฏิเสธการให้บริการ (DDoS) ดังนั้น จากมุมมองของความปลอดภัยทางไซเบอร์แล้ว สิ่งสำคัญคือการใช้ข้อมูลที่รวบรวมโดย OSINT ในเชิงบวกในลักษณะที่เป็นบวก หากถูกใช้ประโยชน์ในทางลบ สิ่งสำคัญคือต้องเตรียมมาตรการรับมือที่สามารถลดความเสียหายที่เกิดจากอาชญากรรมทางไซเบอร์ ในงานวิจัยฉบับนี้ ได้อธิบายสถานะปัจจุบันและแนวโน้มความปลอดภัยของ OSINT โดยเฉพาะอย่าง

ยิ่งการนำเสนอภัยคุกคามด้านความปลอดภัยและอาชญากรรมทางไซเบอร์ที่อาจเกิดขึ้นหากข้อมูลที่รวบรวมโดย OSINT ถูกโจมตีโดยผู้ใช้ที่ประสงค์ร้าย นอกจากนี้ เพื่อแก้ปัญหาดังกล่าวจึงได้เสนอข้อกำหนดด้านความปลอดภัยที่สามารถใช้กับสภาพแวดล้อม OSINT กล่าวคือ ข้อกำหนดด้านความปลอดภัยที่เสนอนั้นจำเป็นสำหรับการรวบรวมและจัดเก็บข้อมูลอย่างปลอดภัยในสภาพแวดล้อม OSINT และสำหรับการเข้าถึงและใช้ข้อมูลที่เก็บรวบรวมโดย OSINT อย่างปลอดภัย โดยมีเป้าหมายคือการลดความเสียหายเมื่ออาชญากรรมทางไซเบอร์เกิดขึ้นในสภาพแวดล้อมของ OSINT ซึ่งได้เสนอกรอบแนวความคิดไว้ดังนี้

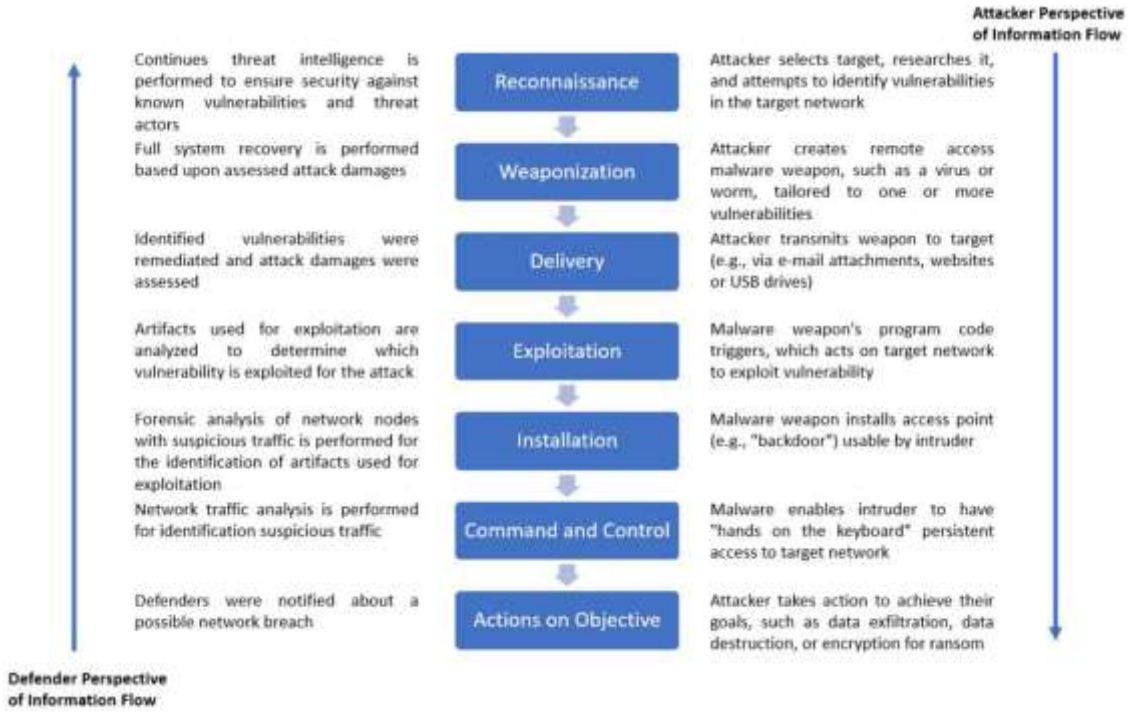
แผนภาพที่ ๒ – ๑๑ กระบวนการ OSINT และภัยคุกคามความปลอดภัยที่เป็นไปได้



ที่มา: Yong-Woon Hwang, ๒๐๒๒.

Muhammad Mudassar Yamin (๒๐๒๒) ได้ศึกษาในหัวข้อ “Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security” จากผลการศึกษา พบว่า OSINT ใช้สำหรับรวบรวมข้อมูลโดยใช้แหล่งข้อมูลสาธารณะต่าง ๆ ด้วยความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีสารสนเทศ และการใช้โซเชียลมีเดียปริมาณมหาศาลในชีวิตประจำวัน ทำให้มีแหล่งข้อมูลสาธารณะมากขึ้นกว่าเดิม ดังนั้น ส่งผลให้การเข้าถึงข้อมูลสาธารณะจากแหล่งต่าง ๆ สามารถนำไปใช้เพื่อวัตถุประสงค์ที่ผิดกฎหมายได้ การดึงข้อมูล OSINT ถือเป็นงานใหญ่ เครื่องมือ และเทคนิคหลายอย่างได้รับการพัฒนาสำหรับภารกิจนี้ ซึ่งสามารถใช้ระบุบุคคล เครื่องบิน เรือ ดาวเทียม และอื่น ๆ งานวิจัยฉบับนี้ ได้ระบุเครื่องมือที่ใช้ในการดึงข้อมูล OSINT และประสิทธิภาพที่เกี่ยวข้องกันในกรณีทดสอบที่แตกต่างกัน โดยได้จับคู่เครื่องมือที่ระบุกับ Cyber Kill Chain และใช้ในสถานการณ์ความปลอดภัยทางไซเบอร์ที่สมจริงเพื่อตรวจสอบความพร้อมในการรวบรวม OSINT ซึ่งได้เสนอกรอบแนวความคิดไว้ดังนี้

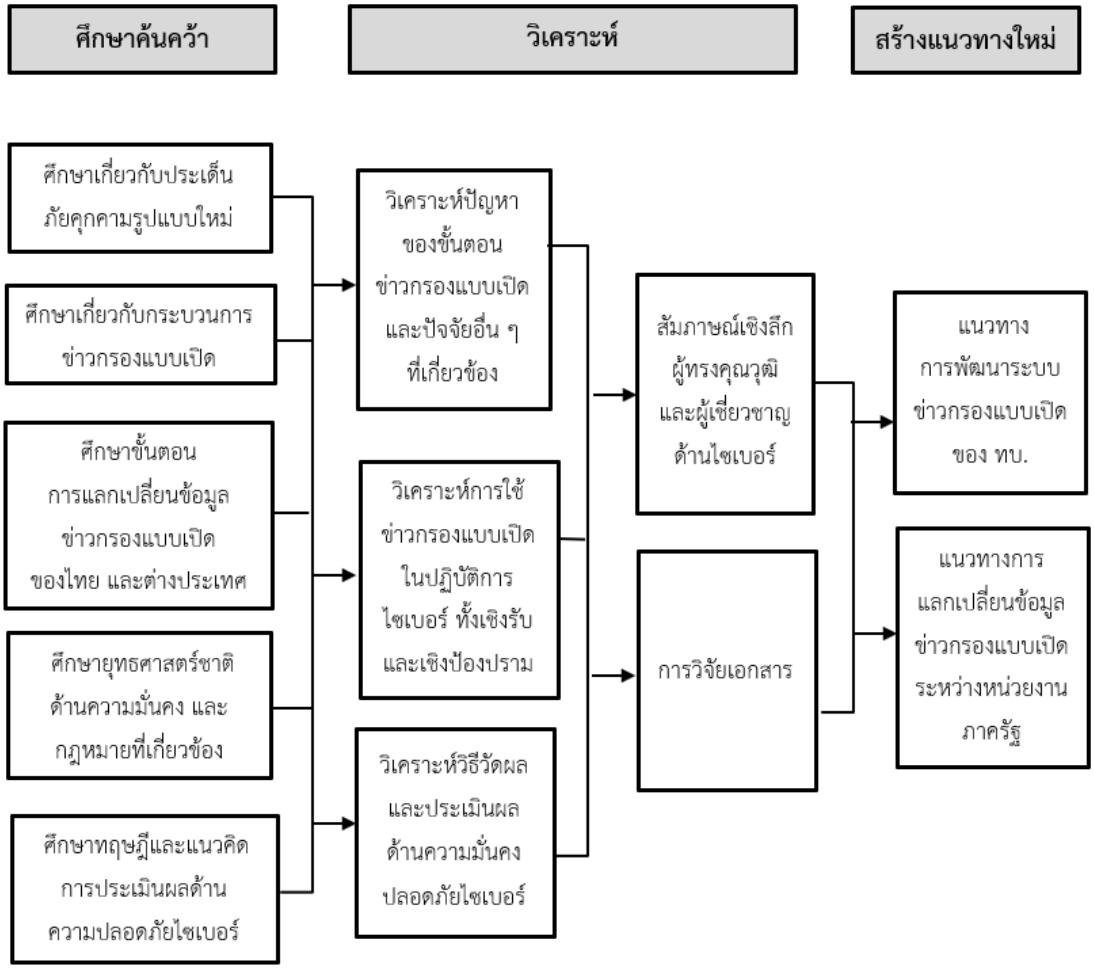
แผนภาพที่ ๒ – ๑๒ สถานการณ์โจมตีและป้องกันทั่วไปโดยใช้ Cyber Kill Chain



ที่มา: Muhammad Mudassar Yamin, ๒๐๒๒.

วัชรภูมิ์ ไวว่อง (๒๕๖๐) ได้ศึกษาเกี่ยวกับการสืบค้นและวิเคราะห์ข้อมูลข่าวกรองแบบเปิดผ่านอินเตอร์เน็ต จากผลการศึกษา พบว่า ข้อมูลที่ได้เป็นการนำข้อมูลข่าวกรองเปิดในโลกออนไลน์นำไปสู่การประมวลผลและวิเคราะห์ข้อมูลเชิงลึก แบบหาเครือข่ายความเชื่อมโยง ของข้อมูลดิบที่มีอยู่ และนำไปสู่การสอบสวนเพื่อขยายผล หาเครือข่ายของผู้ต้องสงสัย หรือบุคคลเป้าหมาย เพื่อทำการคาดการเหตุการณ์ หรือความรุนแรงต่าง ๆ ที่จะเกิดขึ้นในอนาคตได้ และพัฒนาไปสู่การสร้างเป็นระบบสืบค้นข้อมูลที่มีประสิทธิภาพยิ่งขึ้นในอนาคต

กรอบแนวคิดของการวิจัย



สรุป

จากการการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง ในการศึกษานี้ พบว่า การพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก (ทบ.) นั้น ควรพิจารณาถึงกระบวนการผลิตข่าวกรองจากแหล่งเปิด (OSINT) และวิธีการคัดเลือกเครื่องมือ (Tools) ให้เหมาะสม โดยจำเป็นต้องเริ่มต้นจากการประเมินสภาพแวดล้อมทางไซเบอร์ทั้งภายในและภายนอก ทบ.

นอกจากนี้ จากการศึกษาแนวคิดในการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยข่าวกรองแบบเปิดและแนวปฏิบัติที่ดี (Good practice) ของต่างประเทศ พบว่า ประเด็นที่ควรพิจารณา มีดังต่อไปนี้

๑. กำหนดแนวทางปฏิบัติและข้อตกลงที่ชัดเจน (Guidelines and Agreement) โดยการกำหนดวัตถุประสงค์ของการแลกเปลี่ยนข้อมูล ขอบเขตของข้อมูลที่ใช้ร่วมกัน การจัดการข้อมูลและโปรโตคอลการป้องกันข้อมูล และข้อพิจารณาทางกฎหมาย หรือจริยธรรมที่ต้องปฏิบัติตาม

๒. ตรวจสอบและประเมินแหล่งที่มา (Verify and Evaluate) ก่อนที่จะแลกเปลี่ยนข้อมูล OSINT จะต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของแหล่งที่มาเป็นสิ่งสำคัญ เพื่อให้แน่ใจว่าข้อมูลที่แบ่งปันนั้นถูกต้องและเชื่อถือได้

๓. ปกป้องความเป็นส่วนตัวและความอ่อนไหว (Privacy and Sensitivity) สิ่งสำคัญในการ Sharing คือ ต้องจัดการและแบ่งปันข้อมูลด้วยความละเอียดอ่อน โดยเฉพาะเมื่อเป็นเรื่องของข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน ปฏิบัติตามกฎหมายคุ้มครองข้อมูล และระเบียบความเป็นส่วนตัว และตรวจสอบให้แน่ใจว่ามีการใช้เทคนิคการลบข้อมูลระบุตัวตนและการแก้ไขที่เหมาะสมเมื่อแบ่งปันข้อมูลเพื่อปกป้องความเป็นส่วนตัวของแต่ละบุคคล

๔. ตรวจสอบความปลอดภัยของข้อมูล (Information Security) เป็นสิ่งสำคัญในระบบ OSINT Sharing ควรใช้มาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อปกป้องข้อมูลจากการเข้าถึง การละเมิด หรือการรั่วไหลโดยไม่ได้รับอนุญาต รวมถึงช่องทางการสื่อสารที่ปลอดภัย เทคนิคการเข้ารหัส และการควบคุมการเข้าถึงเพื่อปกป้องความสมบูรณ์และความลับของข้อมูลที่แลกเปลี่ยนกันทั้งภายในและภายนอกองค์กร

๕. เคารพกฎหมายและจริยธรรม (Legal and Ethical) สิ่งสำคัญคือต้องปฏิบัติตามขอบเขตทางกฎหมายและจริยธรรม เคารพสิทธิ์ในทรัพย์สินทางปัญญา ลิขสิทธิ์ และข้อตกลงการอนุญาต หลีกเลี่ยงการมีส่วนร่วมในกิจกรรมที่อาจละเมิดสิทธิส่วนบุคคล มีส่วนร่วมในการปฏิบัติที่ผิดกฎหมาย หรือฝ่าฝืนข้อบังคับหรือกฎหมายใดๆ

บทที่ ๓
การพิจารณาแนวคิดที่มีความสอดคล้องกับการพัฒนาระบบข่าวกรองแบบเปิด

แนวคิดของผู้ทรงคุณวุฒิ

ในการศึกษาวิจัยครั้งนี้ ได้สัมภาษณ์ผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และนักวิชาการ จำนวน ๖ ท่าน ประกอบด้วย ๑. พลอากาศตรี จเด็ด คูหะก้องกิจ ๒. พลตรี สังคม ทำจะดี ๓. พันเอก สัจจา รักติประกร ๔. พันเอก ยุทธศิลป์ ผาสุกมูล ๕. พันเอก ยุทธกร สุภาสูรย์ และ ๖. ดร.ปริญญา หอมอเนก โดยผู้ทรงคุณวุฒิได้ให้ข้อเสนอแนะ โดยมีรายละเอียดดังต่อไปนี้

๑. พลอากาศตรี จเด็ด คูหะก้องกิจ ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ข่าวกรองแบบเปิดมีความสำคัญต่องานของ สกมช. เนื่องจากว่าสำนักงานอยู่ในช่วงเริ่มต้นของการจัดตั้ง ดังนั้น จึงมีงบประมาณค่อนข้างจำกัดมาก การนำเอาข่าวกรองแบบเปิดมาใช้จึงช่วยให้สำนักงานสามารถดำเนินงานในด้านการเฝ้าระวัง ภัยคุกคามทางไซเบอร์ จากแหล่งข่าวเปิด และ แจ้งเตือนไปยังหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ได้อย่างมีประสิทธิภาพและเพียงพอภารกิจที่ได้รับ

ปัจจุบัน พบว่า ข่าวกรองแบบเปิด มีความสามารถที่หลากหลายมาก ข่าวกรองแบบเปิดบางประเภทก็สามารถใช้งานได้อย่างเพียงพอกับภารกิจของหน่วยงาน ยกตัวอย่างเช่น การค้นหาเว็บไซต์หน่วยงานของรัฐที่โดนแทรกเว็บพนัน โดยใช้ Google จากนั้นจึงแจ้งไปยังหน่วยงานของรัฐดังกล่าว เพื่อให้ทราบและดำเนินการแก้ไข ซึ่งถือว่าเป็นการสนับสนุนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้โดยตรง ทั้งนี้ ยังมีเครื่องมือด้านข่าวกรองแบบเปิดอีกเป็นจำนวนมากที่ถูกนำมาใช้สนับสนุนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งโดยข้อเท็จจริงแล้ว สกมช. ก็มีการนำเอาเครื่องมือดังกล่าว มาใช้งาน ค่อนข้างมากและได้ผล ในระดับที่น่าพึงพอใจ

อาจกล่าวได้ว่า สกมช. มีการนำหลักการวงรอบข่าวกรองมาใช้ในหน่วยงาน เพื่อสนับสนุนงานตามภารกิจด้านการเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์ ต่อหน่วยงานของรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล รวมถึงหน่วยงานของเอกชน เช่นเดียวกัน อย่างไรก็ตาม ย่อมมีปัญหาอุปสรรคในการดำเนินการ เช่น การผลิตข่าวกรองทางไซเบอร์ได้ในรูปแบบเดียว แล้วกระจายไปยังหน่วยงานประเภทต่าง ๆ ที่แตกต่างกัน เนื่องจากข้อจำกัดของสำนักงานทำให้ไม่สามารถจัดทำข่าวกรองทางไซเบอร์ ให้มีลักษณะเฉพาะเจาะจงตามประเภทของผู้ใช้งานที่แตกต่างกันได้ เป็นต้น

สกมช. จัดตั้งขึ้นมาโดยมีภารกิจ ในด้านการแลกเปลี่ยน ข้อมูลข่าวกรองทางไซเบอร์กับหน่วยงานทั้งภายในและต่างประเทศ ยกตัวอย่างเช่น CERT ของประเทศต่าง ๆ หรือ Sector CERT

หรือหน่วยงานด้านข่าวกรองของประเทศต่าง ๆ ทั้งนี้ หลายหน่วยงานมีการนำข่าวกรองแบบเปิดมาใช้ร่วมกับข่าวกรองแบบอื่น ๆ ซึ่งขึ้นอยู่กับบริบทของแต่ละหน่วยงานที่แตกต่างกันไป

ระบบข่าวกรองแบบเปิดในปัจจุบันมีการพัฒนาก้าวหน้าไปมาก จนอาจกล่าวได้ว่ามีความสามารถสูง และเพียงพอต่อการใช้งานในองค์กรทั่วไป ทั้งนี้ การจะพัฒนาให้หน่วยงานสามารถใช้ประโยชน์จากระบบข่าวกรองแบบเปิดได้นั้น หน่วยงานควรพิจารณากำหนดความต้องการข่าวสารด้านไซเบอร์ จากนั้นจะเป็นการกำหนดแผนการใช้ทรัพยากร อาทิ ด้านบุคลากร ด้านกระบวนการ และด้านเทคโนโลยี ซึ่งทั้งหมดดังที่กล่าวมาข้างต้น ควรมีการขออนุมัติถึงผู้บริหารระดับสูง หากได้รับการสนับสนุนอย่างเหมาะสม ก็จะเกิดการพัฒนาระบบข่าวกรองแบบเปิดขึ้นได้ ทั้งนี้ มีจุดที่สำคัญอีกประการหนึ่งที่ควรพิจารณาเพิ่มเติมด้วย คือ เรื่องการประเมินตามความเป็นจริง ซึ่งยังถือว่าเป็นจุดอ่อนที่สำคัญในหลายหน่วยงานในประเทศไทย ทั้งนี้ หากได้มีการประเมินถึงศักยภาพหรือระดับการพัฒนาในด้านต่าง ๆ แล้ว เราจึงจะสามารถระบุได้ว่าในปัจจุบันเรามีระบบข่าวกรองแบบเปิดอยู่ในระดับขั้นใดหรือเพียงพอต่อการทำงานเพื่อให้บรรลุตามภารกิจหรือตามแผนที่ได้รับมอบหรือไม่

๒. พลตรี สังคม ทำจะดี เลขานุการ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (สลก.กอ.รมน.)

ในเชิงป้องกัน OSINT สามารถมีบทบาทสำคัญในการสนับสนุนความพยายามด้านความปลอดภัยทางไซเบอร์ขององค์กรและแผนกต่าง ๆ ด้วยการรวบรวมข้อมูลจากแหล่งข้อมูลที่เปิดเผยต่อสาธารณะ เช่น โซเชียลมีเดีย ฟอรัมออนไลน์ และเพจข่าว OSINT สามารถแจ้งเตือนล่วงหน้าเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้น ช่องโหว่ และการโจมตี ข้อมูลนี้สามารถนำไปใช้ในการพัฒนามาตรการเชิงรุกเพื่อลดความเสี่ยงและเสริมสร้างการป้องกัน ส่วนในเชิงรุกยังสามารถใช้ OSINT เป็นเครื่องมือในการป้องปราม เพื่อกีดกันผู้ที่อาจเป็นศัตรูจากการมีส่วนร่วมในกิจกรรมที่เป็นอันตราย โดยการแสดงความรู้ต่อสาธารณะเกี่ยวกับความสามารถ ความตั้งใจ และความเปราะบางของฝ่ายตรงข้าม OSINT สามารถยับยั้งพวกเขาจากการพยายามเปิดการโจมตีหรือกิจกรรมที่เป็นอันตรายในรูปแบบอื่น ๆ

อย่างไรก็ตาม สิ่งสำคัญคือต้องทราบว่าการใช้ OSINT เพื่อจุดประสงค์ที่ไม่เหมาะสมจะต้องกระทำภายในขอบเขตทางกฎหมายและจริยธรรม การใช้ OSINT เพื่อรวบรวมข้อมูลเพื่อจุดประสงค์ที่ไม่เหมาะสม เช่น การโจมตีทางไซเบอร์ เป็นสิ่งที่ผิดกฎหมายและผิดจรรยาบรรณ เป็นสิ่งสำคัญสำหรับองค์กรและแผนกต่าง ๆ เพื่อให้แน่ใจว่าการใช้ OSINT นั้นสอดคล้องกับพันธกิจและค่านิยมของพวกเขา และพวกเขาปฏิบัติตามหลักเกณฑ์ทางกฎหมายและจริยธรรมเมื่อใช้ OSINT ทั้งในบริบทเชิงรับและเชิงรุก โดย OSINT สามารถช่วยงานด้านความปลอดภัยทางไซเบอร์ได้หลายวิธี ได้แก่

๑. Threat Intelligence สามารถใช้เพื่อรวบรวมข้อมูลเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้นกับความปลอดภัยทางไซเบอร์ขององค์กร ข้อมูลนี้สามารถช่วยในการระบุเวกเตอร์การโจมตีที่อาจเกิดขึ้น ตลอดจนเครื่องมือ เทคนิค และขั้นตอน (TTP) ที่ใช้โดยผู้คุกคาม สิ่งนี้สามารถช่วยในการพัฒนากลยุทธ์การป้องกันที่มีประสิทธิภาพเพื่อป้องกันหรือบรรเทาการโจมตีทางไซเบอร์

๒. การประเมินช่องโหว่ (Vulnerability Assessment) สามารถใช้ OSINT เพื่อระบุช่องโหว่ที่อาจเกิดขึ้นในโครงสร้างพื้นฐานด้านไอทีและแอปพลิเคชันขององค์กร ซึ่งอาจรวมถึง

ข้อมูลเกี่ยวกับซอฟต์แวร์ที่ไม่ได้แพตช์ ระบบที่กำหนดค่าผิดพลาด หรือจุดอ่อนอื่นๆ ที่ผู้โจมตีอาจนำไปใช้ประโยชน์ได้ ด้วยการใช้ OSINT เพื่อระบุช่องโหว่เหล่านี้ องค์กรสามารถดำเนินการเพื่อแพตช์หรือบรรเทาก่อนที่จะถูกโจมตี

๓. การรับรู้ทางวิศวกรรมสังคม (Social Engineering Awareness) สามารถใช้เพื่อสร้างความตระหนักรู้เกี่ยวกับการโจมตีทางวิศวกรรมสังคม เช่น ฟิชชิง โดยระบุตัวอย่างการโจมตีเหล่านี้ในธรรมชาติ จากการศึกษาการโจมตีเหล่านี้ องค์กรสามารถเข้าใจกลยุทธ์ที่ผู้โจมตีใช้ได้ดีขึ้น และพัฒนาโปรแกรมการฝึกอบรมและการรับรู้ที่มีประสิทธิภาพมากขึ้นสำหรับกำลังพลของหน่วย

๔. การจัดการภาพลักษณ์ขององค์กร (Reputation Management) สามารถใช้ OSINT เพื่อตรวจสอบชื่อเสียงออนไลน์หรือภาพลักษณ์ขององค์กร รวมถึงการกล่าวถึงบนโซเชียลมีเดียและแพลตฟอร์มออนไลน์อื่นๆ สิ่งนี้สามารถช่วยองค์กรในการระบุภัยคุกคามที่อาจเกิดขึ้นกับแบรนด์หรือชื่อเสียงของตน และดำเนินการเพื่อลดผลกระทบด้านลบ

๕. การตามล่าภัยคุกคามทางไซเบอร์ (Cyber Threat Hunting) สามารถใช้ OSINT เพื่อค้นหาภัยคุกคามที่อาจเกิดขึ้นกับความปลอดภัยทางไซเบอร์ขององค์กรในเชิงรุก ด้วยการใช้ OSINT เพื่อระบุกิจกรรมที่ผิดปกติหรือตัวบ่งชี้การประนีประนอมอื่น ๆ องค์กรสามารถดำเนินการเพื่อตรวจสอบภัยคุกคามที่อาจเกิดขึ้นก่อนที่จะบานปลายไปสู่การโจมตีเต็มรูปแบบ

โดยรวมแล้ว OSINT สามารถเป็นเครื่องมือที่มีค่าสำหรับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ในการรวบรวมข้อมูลเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้น ช่องโหว่ และการโจมตี ด้วยการใช้ข้อมูลนี้ในการพัฒนากลยุทธ์การป้องกันเชิงรุก องค์กรสามารถปกป้องทรัพย์สินที่สำคัญของตนจากภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้น

วงรอบข่าวกรอง (Intelligence Cycle) ในส่วนของหน่วยงานของผมไม่ได้ปฏิบัติอย่างชัดเจน เพราะเป็นฝ่ายเลขาฯ ของหน่วยงาน จากประสบการณ์ที่เคยทำงานในส่วน ขว.ทบ. ขอสรุป “วงรอบข่าวกรอง” ประกอบด้วยขั้นตอนต่อไปนี้

๑. การวางแผนและกำหนดทิศทาง ขั้นตอนนี้เกี่ยวข้องกับการระบุความต้องการข่าวกรองขององค์กรและการกำหนดทรัพยากรและวิธีการที่จะใช้ในการรวบรวมข้อมูล

๒. การรวบรวม ขั้นตอนนี้เกี่ยวข้องกับการรวบรวมข้อมูลจากแหล่งต่างๆ เช่น ข้อมูลข่าวกรองแบบโอเพ่นซอร์ส (OSINT) ข่าวกรองมนุษย์ (HUMINT) และข่าวกรองสัญญาณ (SIGINT)

๓. การประมวลผล ขั้นตอนนี้เกี่ยวข้องกับการวิเคราะห์และตีความข้อมูลที่รวบรวมไว้ และเปลี่ยนเป็นรูปแบบที่ผู้มีอำนาจตัดสินใจสามารถนำไปใช้ได้

๔. การวิเคราะห์และการผลิต ขั้นตอนนี้เกี่ยวข้องกับการนำข้อมูลที่ได้รับการประมวลผลไปใช้ในการผลิตผลิตภัณฑ์ข่าวกรอง เช่น รายงานหรือการบรรยายสรุป ที่สามารถใช้เพื่อแจ้งการตัดสินใจ

๕. การเผยแพร่ ขั้นตอนนี้เกี่ยวข้องกับการแบ่งปันผลิตภัณฑ์ข่าวกรองกับผู้มีอำนาจตัดสินใจซึ่งจำเป็นต้องรู้ข้อมูลเพื่อทำการตัดสินใจ

ในแง่ของภารกิจการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อาจมีหลายจุดในวงรอบข่าวกรองที่อาจเกิดปัญหาหรืออุปสรรคขึ้นได้ ตัวอย่างเช่น

ขั้นตอนที่ ๑ การวางแผนและกำหนดทิศทาง หากองค์กรไม่มีความเข้าใจที่ชัดเจนเกี่ยวกับข้อกำหนดด้านความปลอดภัยทางไซเบอร์ หรือหากไม่จัดสรรทรัพยากรที่เพียงพอสำหรับการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ก็อาจไม่สามารถระบุและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ

ขั้นตอนที่ ๒ การรวบรวม หากองค์กรไม่สามารถเข้าถึงแหล่งข้อมูลที่ถูกต้อง หรือหากขาดความเชี่ยวชาญด้านเทคนิคในการรวบรวมและวิเคราะห์ข้อมูลอย่างมีประสิทธิภาพ องค์กรอาจพลาดภัยคุกคามที่สำคัญหรือไม่สามารถระบุช่องโหว่ได้

ขั้นตอนที่ ๓ การประมวลผล หากองค์กรไม่สามารถประมวลผลข้อมูลที่รวบรวมในเวลาที่เหมาะสมและมีประสิทธิภาพ องค์กรอาจไม่สามารถผลิตผลิตภัณฑ์ข่าวกรองที่ดำเนินการได้ทันเวลาเพื่อป้องกันหรือบรรเทาการโจมตีทางไซเบอร์

ขั้นตอนที่ ๔ การวิเคราะห์และการผลิต: หากองค์กรขาดความเชี่ยวชาญในการวิเคราะห์ข้อมูลที่รวบรวมและเปลี่ยนเป็นผลิตผลข่าวกรองที่นำไปปฏิบัติได้ องค์กรอาจไม่สามารถแจ้งข้อมูลการตัดสินใจได้อย่างมีประสิทธิภาพ

ขั้นตอนที่ ๕ การเผยแพร่: หากองค์กรไม่มีกลไกที่มีประสิทธิภาพในการเผยแพร่ผลิตภัณฑ์ข่าวกรองไปยังผู้มีอำนาจตัดสินใจในเวลาที่เหมาะสมและทันท่วงที ก็อาจไม่สามารถป้องกันหรือบรรเทาการโจมตีทางไซเบอร์ได้

การพัฒนาแนวทางข่าวกรองแบบเปิดที่มีประสิทธิภาพจำเป็นต้องมีกลยุทธ์ที่ครอบคลุมซึ่งรวมเอาบุคลากร กระบวนการ และเทคโนโลยีเข้าไว้ด้วยกัน คำแนะนำบางประการสำหรับการพัฒนาแนวทางการพัฒนาข่าวกรองแบบเปิดสำหรับหน่วยงานความมั่นคงมีดังนี้

๑. บุคลากร: หน่วยงานควรจ้างและฝึกอบรมบุคลากรที่มีความเชี่ยวชาญในการวิเคราะห์ OSINT และมีประสบการณ์ด้านความปลอดภัยทางไซเบอร์ บุคลากรควรมีความรู้ในด้านต่าง ๆ เช่น ข่าวกรองภัยคุกคาม การวิเคราะห์เครือข่าย และการทำเหมืองข้อมูล ควรมีการฝึกอบรมและพัฒนาวิชาชีพเป็นประจำ เพื่อให้แน่ใจว่าบุคลากรจะทันกับเทคนิคและเทคโนโลยีใหม่ๆ

๒. กระบวนการ: หน่วยงานควรกำหนดกระบวนการและขั้นตอนที่ชัดเจนสำหรับการรวบรวม วิเคราะห์ และเผยแพร่ข้อมูล OSINT กระบวนการควรได้รับการจัดทำเป็นเอกสารอย่างดีและควรมีแนวทางสำหรับการเก็บรวบรวม การวิเคราะห์ และการแบ่งปันข้อมูล หน่วยงานควรพัฒนาโปรโตคอลสำหรับจัดการข้อมูลที่ละเอียดอ่อนและรับประกันความปลอดภัยของข้อมูล

๓. เทคโนโลยี: หน่วยงานควรใช้เทคโนโลยีที่ทันสมัยเพื่อสนับสนุนการรวบรวม วิเคราะห์ และแบ่งปันข้อมูล OSINT ซึ่งอาจรวมถึงการใช้เครื่องมือวิเคราะห์ขั้นสูงเพื่อประมวลผลข้อมูลปริมาณมาก การใช้การเรียนรู้ของเครื่องและอัลกอริทึม AI เพื่อทำให้ส่วนต่างๆ ของกระบวนการวิเคราะห์เป็นแบบอัตโนมัติ และใช้ประโยชน์จากรูปแบบเทคโนโลยีบนคลาวด์เพื่อเปิดใช้งานการแบ่งปันข้อมูลอย่างปลอดภัยระหว่างหน่วยงานต่างๆ

๔. การทำงานร่วมกัน: หน่วยงานควรทำงานเพื่อสร้างความร่วมมือและความร่วมมือกับหน่วยงานอื่น ๆ ทั้งในและต่างประเทศ สิ่งนี้จะช่วยขยายการเข้าถึงข้อมูล OSINT ของหน่วยงานและปรับปรุงความสามารถในการแบ่งปันข้อมูลกับหน่วยงานอื่น ๆ

๕. การปรับปรุงอย่างต่อเนื่อง: หน่วยงานควรประเมินกระบวนการและเทคโนโลยีของ OSINT เป็นประจำเพื่อระบุจุดที่ต้องปรับปรุง ซึ่งสามารถทำได้ผ่านการตรวจสอบตามปกติ รับฟังความคิดเห็นของผู้ใช้งาน และการเปรียบเทียบแนวทางปฏิบัติที่ดีที่สุดในเชิงภาคการปฏิบัติงาน

โดยสรุป การพัฒนาแนวทางการพัฒนาข่าวกรองแบบเปิดที่มีประสิทธิผลจำเป็นต้องมุ่งเน้นไปที่บุคลากร กระบวนการ เทคโนโลยี การทำงานร่วมกัน และการปรับปรุงอย่างต่อเนื่อง เมื่อปฏิบัติตามคำแนะนำเหล่านี้ หน่วยงานด้านความปลอดภัยสามารถพัฒนาความสามารถ OSINT ที่มีประสิทธิภาพซึ่งสามารถรองรับภารกิจด้านความปลอดภัยทางไซเบอร์ได้

๓. พันเอก สัจจา รักติประกร กรมข่าวทหารบก

ข่าวกรองแบบเปิดเป็นส่วนสำคัญในการป้องกันประเทศหรือภารกิจของกองทัพ โดยเฉพาะภัยคุกคามรูปแบบใหม่ที่มีความหลากหลายมากขึ้น เครื่องมือและแนวทางการปฏิบัติในการรวบรวมข่าวกรองแบบเดิมไม่สามารถรับมือได้ครอบคลุมทั้งหมด แต่ข้อมูลข่าวสารจากแหล่งข่าวเปิดซึ่งมีเป็นจำนวนมากและหลากหลาย สามารถเป็นแหล่งที่ใช้แสวงประโยชน์รับมือกับเป้าหมายใหม่ๆ เช่น กลุ่มก่อการร้าย และอาชญากรรมข้ามชาติได้ อย่างไรก็ตาม ข้อมูลข่าวสารเหล่านั้น ต้องผ่านการกลั่นกรองความน่าเชื่อถือ การดำเนินกรรมวิธี เพื่อให้สามารถนำไปใช้ประโยชน์ได้ ซึ่งเป็นหน้าที่ของเจ้าหน้าที่วิเคราะห์ที่ต้องจัดการกับข้อมูลจากแหล่งข่าวเปิด นอกเหนือจากเดิมที่ประมวล ดำเนินกรรมวิธีเฉพาะจากแหล่งปิดเท่านั้น นอกจากนี้ ข่าวกรองแบบเปิด ยังเป็นประโยชน์อย่างยิ่งในการวิเคราะห์ข่าวกรองทั้งระดับยุทธศาสตร์ ยุทธการ ยุทธวิธี และระดับเทคนิค

ข่าวกรองแบบเปิด เป็นแหล่งข้อมูลข่าวสารจากแหล่งเปิดทุกแหล่ง รวมถึงความรู้และข้อมูลที่ได้จากผู้เชี่ยวชาญและนักวิชาการ โดยเฉพาะที่มีบทบาทเกี่ยวข้องกับงานด้านความมั่นคง โดยอาศัยความก้าวหน้าของเทคโนโลยีสารสนเทศในการสืบค้นและจัดหาข้อมูล ทั้งนี้ ผลผลิตของงานข่าวกรองแบบเปิด จะช่วยให้เจ้าหน้าที่และหน่วยงานความมั่นคงสามารถนำมาใช้ในการประมาณการณ์สถานการณ์ต่างๆ ในลักษณะของการแจ้งเตือนภัยคุกคาม หรือความเคลื่อนไหวของกำลังความสามารถของฝ่ายตรงข้ามที่อาจจะเป็นรัฐหรือไม่ใช่รัฐที่อาจจะเป็นภัยคุกคามต่อความมั่นคงของประเทศ

สำหรับขั้นตอนวงรอบข่าวกรองที่เป็นอุปสรรคต่อภารกิจของ ขว.ทบ. คือ ขั้นตอนการรวบรวม (collection) ซึ่งขั้นตอนดังกล่าวเป็นองค์ประกอบสำคัญของการผลิตข่าวกรอง ที่อาศัยข่าวสารจากแหล่งเปิดประมาณร้อยละ ๘๕–๙๐ ของข่าวสารทั้งหมด เพื่อจัดทำรายงานข่าวกรอง โดยอุปสรรคที่ส่งผลกระทบต่อภารกิจของหน่วย คือ ปริมาณข้อมูลที่มีจำนวนมากในข่าวกรองแบบเปิด ทำให้ต้องใช้เวลาในการคัดเลือกข้อมูลที่มีความน่าเชื่อถือมาใช้ประโยชน์ รวมถึงต้องหลีกเลี่ยงความเสี่ยงจากการลวงของฝ่ายตรงข้าม

ข้อเสนอแนะในการพัฒนาแนวทางการพัฒนาระบบข่าวกรองแบบเปิดของหน่วยงานด้านความมั่นคง รายละเอียดดังนี้

๑. การพัฒนาบุคลากร: การเพิ่มศักยภาพของบุคลากรเป็นส่วนสำคัญที่สุดในการใช้ประโยชน์จาก OSINT ด้วยการพัฒนาความรู้ความชำนาญด้านการรวบรวมข้อมูลข่าวสารและการวิเคราะห์ รวมถึงการพัฒนาความชำนาญด้านภาษาต่างประเทศ (โดยเน้นภาษาประเทศเพื่อนบ้าน)

จะช่วยให้งานข่าวกรองจากแหล่งข่าวเปิดสามารถตอบสนองความต้องการของงานด้านการข่าวได้อย่างรวดเร็วและเชื่อถือได้ ซึ่งในเบื้องต้นอาจจะเป็นการเรียนรู้จากบุคคล/หน่วยงานอื่น ทั้งจากภายในประเทศและจากประเทศพันธมิตร รวมถึงการเรียนรู้จากการปฏิบัติ ซึ่งจะนำไปสู่การเรียนรู้ด้วยตนเองด้วยการพัฒนาหลักสูตรเฉพาะ เพื่อให้เหมาะสมกับความต้องการที่แท้จริง

๒. การแลกเปลี่ยนข้อมูลข่าวสารและข่าวกรอง: ข่าวกรองยุคใหม่จะต้องมีการกระจาย/แลกเปลี่ยนระหว่างทหารกับพลเรือน และระหว่างประชาคมข่าวกรองให้มากขึ้น สำหรับข่าวกรองยุทธศาสตร์ ต้องให้ความสำคัญกับการแลกเปลี่ยนข่าวกรองกับประเทศเพื่อนบ้าน และประเทศพันธมิตรสำคัญ

๓. การรวบรวมข้อมูล: จะต้องตระหนักถึงสภาวะแวดล้อมของข้อมูลข่าวสารในยุคปัจจุบัน ที่มีลักษณะเป็นพลวัตร และซับซ้อน ดังนั้น จะต้องมีการคัดเลือกข้อมูลจากแหล่งข่าวเปิดที่มีความเชื่อถือได้มาเข้าสู่กระบวนการข่าวกรอง

๔. การปรับเปลี่ยนทัศนคติต่อแหล่งข่าวเปิด: ว่าเป็นเครื่องมือที่มีคุณค่าและมีศักยภาพในระบบงานข่าวกรอง สามารถนำมาเติมเต็มงานข่าวกรองที่มีชั้นความลับ

๕. การกำหนดชั้นความลับ: ไม่ควรกำหนดสูงเกินความจำเป็น เพื่อให้หน่วย/บุคคลที่ต้องการข้อมูลนั้นๆ สามารถเข้าถึงและนำไปใช้ประโยชน์ได้

๖. โอกาสในการเข้าถึงข้อมูล: สิ่งสำคัญในการปรับปรุงการดำเนินงานข่าวกรองจากแหล่งข่าวเปิด จะต้องตระหนักว่า หน่วยข่าวกรองทุกหน่วยของทุกประเทศต่างมีโอกาสในการเข้าถึงข้อมูลข่าวสารจากแหล่งข่าวเปิดเท่าเทียมกัน ดังนั้น ทุกประเทศ/ทุกองค์กร จึงมีโอกาสในการพัฒนาศักยภาพด้านข่าวกรองจากแหล่งข่าวเปิด ได้เท่าเทียมกัน

๔. พันเอก ยุทธศิลป์ ผาสุขมูล รองผู้อำนวยการศูนย์ไซเบอร์ทหาร

ข่าวกรองแบบเปิด (Open-source intelligence หรือ OSINT) มีบทบาทสำคัญ กล่าวคือ

๑. สามารถนำมาสรุปเป็นสถานการณ์ปัจจุบันตามห้วงระยะเวลา และเป็นข้อมูลขั้นต้นในการพิจารณาแนวโน้มของภัยคุกคามทางไซเบอร์ในด้านต่างๆ ได้

๒. เป็นการประหยัดงบประมาณ เพราะไม่ต้องมีค่าใช้จ่าย สามารถนำมาใช้ประโยชน์ในเนื้อหาที่เกี่ยวข้องได้โดยตรง

ข่าวกรองแบบเปิด (Open-source intelligence หรือ OSINT) มีส่วนสนับสนุนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กล่าวคือ

๑. การสนับสนุนการรับมือเหตุการณ์ทางไซเบอร์ และการพิสูจน์มีส่วนสนับสนุนในเรื่องต่าง ๆ โดยเฉพาะตาม NIST Cyber Security Framework ซึ่งองค์กรเป็นแนวทางในการปฏิบัติงาน ตั้งแต่เรื่องการระบุตัวตนและสินทรัพย์ การป้องกัน การตรวจจับ การตอบสนอง การฟื้นฟูระบบ ในแต่ละเรื่องสามารถหาข้อมูลจากแหล่งข่าวกรองแบบเปิดเพื่อมาสนับสนุนในการปฏิบัติงานในแต่ละขั้นตอนได้

๒. มีส่วนในการเป็นมูลฐาน/นำมาเป็นสถิติ ในการกำหนดภัยคุกคามทางไซเบอร์ทั้งในปัจจุบันและอนาคต เพื่อนำไปเป็นตัวกำหนดในการพัฒนาบุคลากรตลอดจนจัดหาเครื่องมือในการดำเนินงานด้านไซเบอร์

ในส่วนของวงรอบข่าวกรอง มี ๔ ขั้นตอน คือ การวางแผน รวบรวม ดำเนินกรรมวิธีการใช้กระจายข่าวกรอง สำหรับการปฏิบัติของหน่วย ซึ่งในแต่ละขั้นต้องใช้เจ้าหน้าที่เฉพาะมาดำเนินการ ในการปฏิบัติงานจริงหน่วยมีเจ้าหน้าที่ไม่เพียงพอที่จะแยกทำทุกขั้นตอน จึงทำวงรอบข่าวกรองทั้ง ๔ วงรอบด้วยกำลังพลที่จำกัด ขั้นตอนที่เป็นปัญหาอุปสรรค คือ ขั้นตอนการวางแผน ที่จะต้องนำไปสู่ผลผลิตที่สามารถใช้ได้จริง และขั้นตอนการดำเนินกรรมวิธี ซึ่งจะต้องใช้กำลังพลที่มีความรู้ความสามารถในการคิด วิเคราะห์ ตลอดจนอาจจะต้องมีความรู้ด้านเทคนิคประกอบด้วย

ข้อเสนอแนะในการพัฒนาแนวทางการพัฒนาระบบข่าวกรองแบบเปิด ของหน่วยงานด้านความมั่นคง กล่าวคือ

๑. ด้านบุคลากร ต้องมีอัตรากำลังพลตามวงรอบข่าวกรองเพื่อดำเนินการให้ได้ข่าวกรองแบบเปิดที่ทันสมัยและใช้ประโยชน์ได้ นอกจากนั้น จะต้องมีการพัฒนากำลังพลดังกล่าว เช่น การอบรมให้ความรู้ การเข้าเรียนหลักสูตรต่างๆที่เกี่ยวข้อง เป็นต้น

๒. ด้านกระบวนการ มีการดำเนินการที่เป็นขั้นตอน/ถูกต้อง เป็นไปตามมาตราฐาน

๓. ด้านเทคโนโลยี มีเครื่องมือในการรวบรวมข่าวเปิด หรือสามารถรวบรวม วิเคราะห์จาก Social Media หรือ จาก Internet ได้อย่างรวดเร็ว

๕. พันเอก ยุทธกร สุภาสูรย์ รองผู้บัญชาการ โรงเรียนรักษาความปลอดภัย ศูนย์รักษาความปลอดภัย (รร.รปภ.ศรภ.)

ข้อดีที่สำคัญของข่าวกรองแบบเปิด (Open-source intelligence หรือ OSINT) คือ สามารถรวบรวมข่าวสารง่ายและปริมาณมาก จากการรวบรวมข้อมูลข่าวสารจากแหล่งข้อมูลเปิดจากอินเตอร์เน็ต สื่อสังคมออนไลน์ และมีเดียต่างๆ ในการรวบรวมข้อมูลเป้าหมาย หรือ ภารกิจของหน่วยที่ได้รับมอบหมาย ยิ่งถ้าหากองค์กรใดสามารถประเมินค่า (คัดแยกความเกี่ยวข้อง ความน่าเชื่อถือ ความถูกต้องจริง/เท็จ) และตีความ (วิเคราะห์ สนธิ อนุมาน) ออกมาเป็นข่าวกรองได้ดีกว่าและเร็วกว่า จะทำให้องค์กรนั้นได้เปรียบจากงานข่าวกรอง

โดยในเชิงรับสามารถตรวจสอบข้อมูลที่เผยแผ่สาธารณะ ในข้อมูลที่ต้องการเปิดเผยและข้อมูลชั้นความลับไม่ต้องการให้เปิดเผย เพื่อให้ทราบขีดความสามารถ แนวทางการปฏิบัติ พฤติกรรมของฝ่ายตรงข้าม เพื่อป้องกันหรือลดความร้ายแรงจากการบ่อนทำลาย การจารกรรมและการก่อวินาศกรรม กับบุคคล เอกสาร สถานที่ ขององค์นั้น ๆ สำหรับเชิงรุกจะเป็นเครื่องมือช่วยหาจารชน องค์กร หรือ แนวทางการปฏิบัติที่จะกระทำกับองค์กรของเรา เพื่อหาความเชื่อมโยงของเป้าหมายและเครือข่ายเบื้องต้น นำไปสู่การขยายผลกำหนดแนวทางทำลายหรือลดทอนขีดความสามารถของฝ่ายตรงข้ามได้อย่างรวดเร็ว

อย่างไรก็ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่ให้ความหมาย “การรักษาความมั่นคงปลอดภัยไซเบอร์” คือ “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ การทหาร และความสงบเรียบร้อยภายในประเทศ โดยสามารถสนับสนุนความมั่งคงทางทหาร ในการตรวจสอบข้อมูลข่าวสารและเอกสารลับ ของหน่วยงาน

ที่ถูกเผยแพร่ จากอินเตอร์เน็ตและ สื่อสังคมออนไลน์ เพื่อค้นหาที่มาของข้อมูลและผู้เผยแพร่ เพื่อนำไปสู่มาตรการในการป้องกันข้อมูลที่รั่วไหลต่อไป

ปัจจุบันหน่วยงานยังการปฏิบัติสอดคล้องกับวงรอบข่าวกรอง (Intelligence Cycle) ซึ่งการปฏิบัติงานในทุกขั้นตอนไม่เป็นอุปสรรคต่อภารกิจไซเบอร์ แต่ต้องมีการพัฒนา ส่งเสริม ปรับรูปแบบการปฏิบัติงานทั้งในด้านบุคลากร กระบวนการ และเทคโนโลยี เพื่อสร้างความพร้อมสำหรับรองรับการรวบรวมข่าวกรองแบบเปิด (OSINT) ที่จะมีการเปลี่ยนแปลงด้วยอัตราเร่งที่รวดเร็วมาก

ปัจจุบันหลายหน่วยงานมีการแลกเปลี่ยนข้อมูลข่าวกรองแบบเปิดแล้ว ทั้งการจำกัดเฉพาะเจ้าหน้าที่ เช่น ข้อมูลทะเบียนราษฎร์ของ มท. ข้อมูลทะเบียนยานพาหนะของกรมขนส่งทางบก เป็นต้น หรือข้อมูลบางประเภทที่เปิดโอกาสให้บุคคลทั่วไปสามารถร้องขอเพื่อเข้าถึงได้ นอกจากนี้มีการแลกเปลี่ยนข้อมูลกันในระดับเจ้าหน้าที่เพื่อร่วมมือบูรณาการกันปฏิบัติ ซึ่งหากในอนาคตหากสามารถเปิดให้มีกระบวนการแลกเปลี่ยนข้อมูลฯ อย่างเต็มที่ จะเปิดโอกาสให้การปฏิบัติงานมีประสิทธิภาพเพิ่มมากขึ้น

ข้อเสนอแนะในการพัฒนาแนวทางการพัฒนาระบบข่าวกรองแบบเปิด ของหน่วยงานด้านความมั่นคง กล่าวคือ

๑. ด้านบุคลากร ควรส่งเสริมบุคลากร ด้านความรู้ในการใช้งาน ระบบข่าวกรองแบบเปิด ในด้านอินเตอร์เน็ต และสื่อสังคมออนไลน์ จากเครื่องมือที่สามารถใช้งานได้แบบไม่เสียค่าใช้จ่ายที่หลากหลาย พร้อมระบุข้อความค้นหาเป้าหมาย หรือ ประเภทข้อมูลเป้าหมายที่เกี่ยวข้องเพื่อเพิ่มประสิทธิภาพ และปริมาณข้อมูลจากผลลัพธ์เพิ่มขึ้น

๒. ด้านกระบวนการ ควรออกแบบระบบการปฏิบัติงาน สร้างองค์ความรู้และการยอมรับในการปรับเปลี่ยนรูปแบบ รวมทั้งจัดบุคลากรหรือหน่วยงานมารับผิดชอบเพื่อรองรับงานที่เกิดขึ้นใหม่อย่างชัดเจน

๓. ด้านเทคโนโลยี ควรจัดหาเครื่องมือในการสืบค้นข้อมูลข่าวกรองแบบเปิดสำเร็จรูป เช่น Orbit หรือ cobweb เป็นต้น ที่สามารถสืบค้นข้อมูลได้รวดเร็วและแยกประเภทของข้อมูลที่สืบค้นเรียบร้อยแล้วพร้อมแสดงผลเป็น Link chart ความเชื่อมโยงของเครือข่ายเป้าหมายหรือบุคคล สืบค้น พร้อมจัดทำรายงานอัตโนมัติ ลดเวลาในการทำงานของเจ้าหน้าที่วิเคราะห์ หรือขยายผลการสืบค้นในเครือข่ายที่สนใจเพิ่มเติม

๖. ดร.ปริญญา หอมอเนก กรรมการผู้ทรงคุณวุฒิด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ข่าวกรองแบบเปิด Open-source intelligence หรือ OSINT มีบทบาทสำคัญกับทั้งปฏิบัติการด้านไซเบอร์ทั้งเชิงรุก (Offensive) และเชิงรับ (Defensive) ในมุมมองความมั่นคงที่เกี่ยวข้องกับภารกิจด้านการทหาร โดย OSINT สามารถแบ่งได้เป็น ๔ ส่วน กล่าวคือ

ส่วนที่ ๑ ไซเบอร์เชิงรุก (Offensive) หรือ “Red Team” เป็นปฏิบัติการเชิงรุกที่เน้น “การรวบรวมข้อมูลก่อนกระบวนการโจมตี” โดยทำการโจมตีไปยังระบบเครือข่ายเป้าหมายเสมือนว่าเป็นผู้โจมตีจริง ๆ เพื่อให้เป้าหมายต่าง ๆ หยุดทำงาน หรือเกิดช่องโหว่ให้สามารถเข้าไปหาผลประโยชน์ต่างๆ จากช่องทางเหล่านั้นได้

ส่วนที่ ๒ ไซเบอร์เชิงรับ (Defensive) หรือ “Blue Team” เป็นปฏิบัติการเชิงรับที่เน้น “การเรียนรู้ด้านการป้องกัน การตรวจสอบ และรับมือ” จากการโจมตีของฝั่ง Red Team เพื่อให้ระบบเครือข่าย หรืออุปกรณ์ที่สำคัญต่าง ๆ ปลอดภัยจากการโจมตี และสามารถทำงานได้อย่างปกติ เพราะฝั่ง Red Team ก็จะเสมือนเป็นคนคอยสอดส่องช่องโหว่ (Vulnerability) ที่อาจหลุดรอดออกไป

ส่วนที่ ๓ การประเมินและตรวจสอบดิจิทัล (Audit) ประกอบด้วย Intelligence Gathering, Threat Intelligence และ Cyber Security Operation Center (CSOC) ทำหน้าที่ในการตรวจสอบภัยคุกคามทางไซเบอร์ที่ได้จากระบบ (CTI)

ส่วนที่ ๔ การตรวจพิสูจน์หลักฐานดิจิทัล (Forensics) ประกอบด้วย การตอบสนองเหตุการณ์ (Incident Response: IR) ข้อมูลจาก OSINT สามารถใช้ในการวิเคราะห์และตรวจสอบเพื่อตระหนักถึงความรุนแรงของเหตุการณ์และพบแนวโน้มการโจมตีหรือข้อมูลที่เป็นปัจจัยสำคัญ

ในส่วนของวงรอบข่าวกรอง มี ๔ ขั้นตอน คือ การวางแผน รวบรวม ดำเนินกรรมวิธีและการใช้กระจายข่าวกรอง โดยส่วนที่สำคัญ คือ กระบวนการรวบรวมข้อมูลผ่านเครื่องมือ Offensive OSINT ซึ่งในปัจจุบันมีหน่วยงานด้านความมั่นคงของประเทศไทยมีการเลือกใช้เครื่องมือ OSINT ที่มีความหลากหลาย ในส่วนของกระบวนการแลกเปลี่ยนข้อมูล OSINT ระหว่างหน่วยงานในประเทศไทย เพื่อใช้งานประโยชน์ข้อมูลร่วมกัน พบว่า ยังไม่มีปรากฏให้เห็นอย่างชัดเจน

ข้อเสนอแนะในการพัฒนาแนวทางการพัฒนาระบบข่าวกรองแบบเปิด (OSINT) ของหน่วยงานด้านความมั่นคง กล่าวคือ

๑. ด้านบุคลากร ควรส่งเสริมให้กำลังพลศึกษา ติดตามเทคโนโลยีที่เกี่ยวข้องและเครื่องมือที่ใช้ และแนวโน้มทางด้านไซเบอร์ เช่น เทคนิคในการสืบค้นข้อมูลจากแหล่งข้อมูลเปิด การเผยแพร่ข้อมูลอย่างมีจริยธรรม เป็นต้น

๒. ด้านกระบวนการ ควรพิจารณาทางเลือกในการพัฒนาระบบฯ ให้เหมาะสมกับบริบทของศูนย์ไซเบอร์ ทบ. โดยควรยึดหลักวัตถุประสงค์ วิสัยทัศน์ พันธกิจ ของ ทบ. เป็นสำคัญ กล่าวคือ

๒.๑ ประยุกต์ใช้ Open source (Pure OSINT)

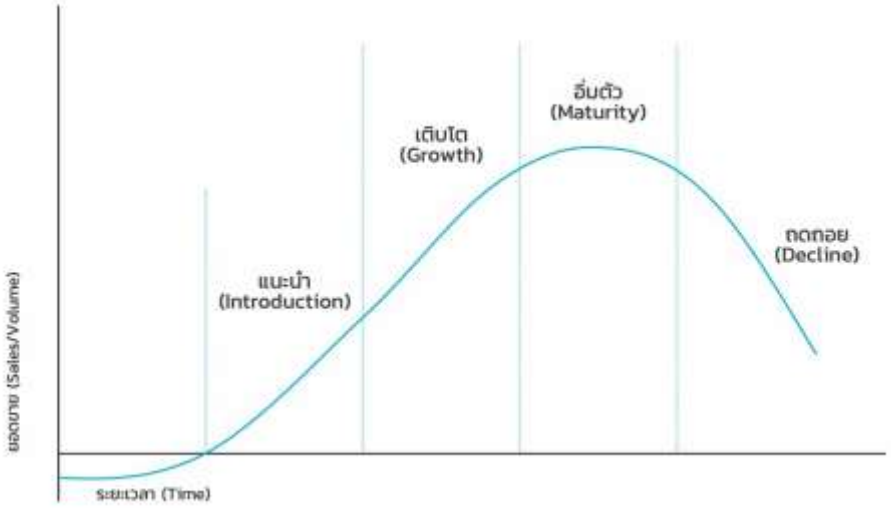
๒.๒ ประยุกต์ใช้ Open source ร่วมกับซื้อโปรแกรมแบบเสียค่าบริการประเภท Enterprise/ Premium ซึ่งจำเป็นต้องใช้งบประมาณ

๒.๓ พัฒนาเอง (In-House Development) ไม่แนะนำให้พัฒนาระบบขึ้นใช้งานเอง เนื่องจากบุคลากรที่มีความเชี่ยวชาญของ ทบ. มีการเลื่อนตำแหน่งเป็นประจำ อาจส่งให้ไม่สามารถพัฒนาระบบได้อย่างต่อเนื่อง

๒.๔ ซอฟต์แวร์เชิงพาณิชย์ (Commercial Software)

๓. ด้านเทคโนโลยี ควรมุ่งเน้นการนำเทคโนโลยีมาใช้ในกองทัพ โดยพัฒนาระบบฯ หรือเลือกใช้เครื่องมือที่เหมาะสมเพื่อให้เกิดความยั่งยืน (sustainability) อย่างไรก็ตาม การพัฒนาเฟรมเวิร์ค (Framework) จำเป็นต้องพิจารณาถึงวงจรชีวิตผลิตภัณฑ์ หรือ Product Life Cycle ซึ่งประกอบด้วย ๔ ช่วง คือ ช่วงแนะนำ (Introduction) ช่วงเติบโต (Growth) ช่วงเติบโตเต็มที่หรือจุดสูงสุด (Maturity) และช่วงถดถอย (Decline)

แผนภาพที่ ๓ - ๑ วงจรชีวิตผลิตภัณฑ์ (Product Life Cycle)



ที่มา : ออนไลน์, 2563.

แนวคิดการพัฒนาระบบข่าวกรองแบบเปิด

แนวคิดการพัฒนาระบบข่าวกรองแบบเปิด (Open Source Intelligence: OSINT) มุ่งเน้นการเก็บรวบรวมข้อมูลและข่าวสารจากแหล่งที่มาเปิดเผยต่าง ๆ เพื่อใช้สนับสนุนการวิเคราะห์และตัดสินใจของกองทัพบกหรือหน่วยงานด้านความมั่นคง แนวคิดนี้สนับสนุนการเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ทางกายภาพ และความมั่นคงขององค์กรในด้านต่างๆ ในการศึกษาวิจัยครั้งนี้ ได้เสนอมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ (Standard) พร้อมแนวคิดการพัฒนาระบบฯ ที่เกี่ยวข้อง รายละเอียดดังนี้

People / Process / Technology Framework

การพัฒนาองค์กรมีความจำเป็นจะต้องคำนึงการพัฒนาในทุก ๆ ด้าน เพื่อให้องค์กรสามารถขับเคลื่อนไปข้างหน้าได้อย่างต่อเนื่อง โดยในบทความนี้จะกล่าวถึงพื้นฐานการพัฒนาใน ๓ ด้าน ประกอบด้วย People (บุคคล), Process (กระบวนการ), และ Technology (เทคโนโลยี) ซึ่งมีความสำคัญในการสร้างและดำเนินการบริการอย่างมีประสิทธิภาพ โดยมีความสัมพันธ์กันดังนี้

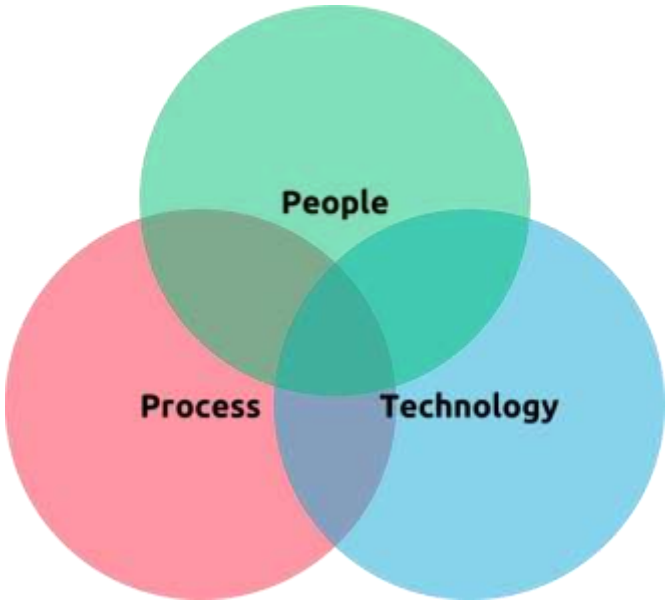
๑. People (บุคคล) บุคลากรที่เกี่ยวข้องในการให้บริการเทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญใน ITSM คอยดำเนินการและสนับสนุนกระบวนการต่างๆ เช่น บุคลากรด้านสนับสนุนผู้ใช้ ผู้จัดการความขัดแย้ง (Conflict Manager) และผู้จัดการการเปลี่ยนแปลง (Change Manager) ซึ่งความสามารถของบุคคลในการทำงานร่วมกันและมีความรู้เกี่ยวกับการดำเนินการบริการเป็นสิ่งสำคัญในการให้บริการที่มีประสิทธิภาพและประสบความสำเร็จ

๒. Process (กระบวนการ) กระบวนการเป็นการกำหนดและดำเนินการตามขั้นตอนที่ถูกกำหนดใน ITIL เพื่อให้บริการเทคโนโลยีสารสนเทศมีคุณภาพและประสิทธิภาพสูง ตัวอย่างของ

กระบวนการที่สำคัญ ได้แก่ การบริหารจัดการเหตุการณ์ (Incident Management) การจัดการการเปลี่ยนแปลง (Change Management) และการบริหารจัดการความรู้ (Knowledge Management) นอกจากนี้ องค์กรยังสามารถนำกระบวนการที่เป็นมาตรฐานหรือกรอบการทำงานเข้ามาใช้เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรได้ เช่น มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS หรือ ISO/IEC ๒๗๐๐๑:๒๐๑๓) หรือ NIST Cybersecurity Framework เป็นต้น

๓. Technology (เทคโนโลยี) เทคโนโลยีเป็นเครื่องมือสำคัญในการให้บริการเทคโนโลยีสารสนเทศ การเลือกและการใช้เทคโนโลยีที่เหมาะสมเป็นสิ่งสำคัญ ตัวอย่างเช่น การใช้เครื่องมือและซอฟต์แวร์ในการจัดการบริการ เครื่องมือการตรวจสอบและจัดการเหตุการณ์ ระบบการจัดการฐานข้อมูล เป็นต้น การเลือกใช้เทคโนโลยีที่เหมาะสมและมีประสิทธิภาพสูงสามารถช่วยให้การให้บริการเป็นไปได้อย่างมีประสิทธิภาพและคุณภาพสูง

แผนภาพที่ ๓ - ๒ แนวคิด People / Process / Technology



ที่มา : People-process-technology model

NIST Cybersecurity Framework

NIST Cybersecurity Framework เป็นแนวทางในการจัดการความมั่นคงปลอดภัยของระบบสารสนเทศและเทคโนโลยีที่พัฒนาโดย National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา โดยแนวคิดนี้นำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุดของการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ รวมถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ในขณะที่ธุรกิจยังคงดำเนินต่อไปได้อย่างเนื่อง ซึ่งประเทศไทยได้นำ NIST มาเป็นต้นแบบส่วนหนึ่งในการจัดทำ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งกรอบมาตรฐานนี้มีองค์ประกอบหลักสามารถอธิบายได้ดังนี้

๑. Framework Core เป็นส่วนที่สำคัญที่สุดของ NIST Cybersecurity Framework ประกอบด้วยแบบแผน ๕ ฟังก์ชั่นหลัก ได้แก่ Identify (การระบุและสรุประเบียบว่าด้วย), Protect (การป้องกัน), Detect (การตรวจจับ), Respond (การตอบสนอง), และ Recover (การกู้คืน) โดยแต่ละองค์ประกอบจะเป็นเป้าหมายของกิจกรรมที่สามารถเข้าถึงได้จากทุกมุมมองในการจัดการความมั่นคงปลอดภัย

แผนภาพที่ ๓ - ๓ ฟังก์ชั่นหลัก ของ NIST Framework

ที่มา : National Institute of Standards and Technology. (2018).

๒. Framework Implementation Tiers เป็นระดับที่ช่วยให้องค์กรสามารถประเมินความเสี่ยงในด้านความมั่นคงปลอดภัยและการจัดการความเสี่ยง โดยแบ่งเป็น ๔ ระดับ ได้แก่ Partial (บางส่วน), Risk Informed (ความรู้สึกเห็นความเสี่ยง), Repeatable (เป็นประจำ), และ Adaptive (ปรับเปลี่ยนได้)

๓. Framework Profile เป็นข้อกำหนดเพิ่มเติมที่ช่วยให้องค์กรสามารถกำหนดเป้าหมายความมั่นคงปลอดภัยและวิธีการที่เหมาะสมสำหรับองค์กรตนเอง โดยพิจารณาตามความต้องการธุรกิจ ข้อกำหนดทางกฎหมาย และแนวทางปฏิบัติที่เกี่ยวข้อง

๔. Framework Implementation Guidance เป็นคำแนะนำที่ช่วยให้องค์กรสามารถนำเอา NIST Cybersecurity Framework ไปใช้งานได้อย่างมีประสิทธิภาพ ซึ่งประกอบไปด้วยเทคนิค ขั้นตอน และแนวทางที่เกี่ยวข้องในการจัดการความมั่นคงปลอดภัย

กล่าวโดยสรุปได้ว่า NIST Cybersecurity Framework ช่วยให้องค์กรสามารถพัฒนาและดำเนินการในด้านความมั่นคงปลอดภัยของระบบสารสนเทศและเทคโนโลยีอย่างมีระบบ ซึ่งช่วยให้องค์กรมีการจัดการความเสี่ยงและความมั่นคงปลอดภัยที่มีประสิทธิภาพและเหมาะสมกับความต้องการขององค์กรและสภาพแวดล้อมที่เปลี่ยนไปอย่างรวดเร็วในโลกดิจิทัลปัจจุบัน

Global Digital Compact (GDC)

เป็นกรอบแนวทางในการนำเทคโนโลยีดิจิทัลมาใช้เพื่อการพัฒนาอย่างยั่งยืนของมวลมนุษยชาติ ซึ่งช่วยสนับสนุนเป้าหมายของ SDGs (Sustainable Development Goals) โดย GDC ประกอบด้วย ๘ เรื่อง เนื่องจากทุกฝ่ายเล็งเห็นว่าเทคโนโลยีดิจิทัลเป็นเครื่องมือสำคัญในการดำเนิน

ธุรกิจ และมีส่วนสำคัญอย่างยิ่งต่อการปรับปรุงคุณภาพชีวิตของมนุษย์ในศตวรรษนี้ โดยกรอบ ๘ เรื่องของ GDC มีรายละเอียดดังนี้

๑. Digital Inclusion and Connectivity การสร้างสังคมดิจิทัลอย่างยั่งยืนไม่ได้หมายความถึงเพียงแค่การใช้เทคโนโลยีและการเชื่อมต่อระหว่างกันเท่านั้น แต่ยังรวมถึงการใช้อย่างมีความเท่าเทียมกัน มีความทั่วถึงครอบคลุมทุกพื้นที่ เกิดความคุ้มค่า นำมาประยุกต์ใช้ให้เกิดประโยชน์ โดยควรต้องจัดการกับช่องว่างทางดิจิทัลทั้งเรื่องทักษะ ภาษา และเนื้อหา

๒. Internet Governance ความจำเป็นต่อการกำกับดูแลอินเทอร์เน็ต เพราะปัจจุบันอินเทอร์เน็ตมีการใช้งานร่วมกันหลายภาคส่วน ทั้งฝ่ายรัฐบาล เอกชน และประชาสังคม จึงควรจะต้องมีแนวทางในการบริหารจัดการให้ทุกฝ่ายใช้อินเทอร์เน็ตร่วมกันด้วยความสันติสุข และจำเป็นต้องมีธรรมาภิบาล หรือหลักการบริหารจัดการที่ดี มีกระบวนการในการกำหนดหลักการใช้งานอินเทอร์เน็ต มีกฎเกณฑ์ กฎระเบียบ และข้อตกลงร่วมกัน เพื่อให้การใช้งานอินเทอร์เน็ตเกิดความราบรื่น

๓. Data Protection สังคมดิจิทัลเติบโตอย่างรวดเร็ว เกิดข้อมูลและมีการนำข้อมูลไปใช้ประโยชน์กันอย่างมาก ซึ่งในบางกรณีมีการละเมิดข้อมูลส่วนบุคคล ดังนั้นจึงต้องสร้างความตระหนักรู้ถึงการปกป้องข้อมูลส่วนตัวและความเป็นส่วนตัว โดยข้อมูลส่วนบุคคลที่อยู่ในองค์กรหรือหน่วยงานควรจะต้องมีกระบวนการในการเก็บ ใช้ และเปิดเผยข้อมูล รวมถึงการประมวลผลให้ถูกต้องตามกฎหมาย โดยองค์กรจะต้องปฏิบัติตามกฎหมาย GDPR และสำหรับองค์กรในประเทศไทยต้องปฏิบัติตามกฎหมาย PDPA (ซึ่ง DP ที่อยู่ในกฎหมายทั้งสองฉบับนั้นย่อมาจาก Data Protection)

๔. Human Rights Online มนุษย์ทุกคนที่ใช้ชีวิตในโลกออนไลน์ ควรได้สิทธิ์พื้นฐานเดียวกันกับการใช้ชีวิตแบบออฟไลน์ นั่นหมายความว่าสิทธิมนุษยชนบนออนไลน์ควรต้องมีความเชื่อมโยงและพึ่งพาซึ่งกันและกันกับโลกออฟไลน์ โดยสิทธิมนุษยชนบนโลกออนไลน์นั้นควรจะต้องครอบคลุมถึงการถูกปั่นความคิดใน social media การหลอกลวงในรูปแบบของ Information Disorder ด้วย ประกอบด้วย (๑) Misinformation หรือข้อมูลที่ผิด (๒) Disinformation หรือข้อมูลที่ถูกบิดเบือน และ (๓) Mal-information หรือข้อมูลที่แฝงเจตนาร้าย

๕. Digital Trust and Security เรื่องความไว้วางใจและความมั่นคงปลอดภัยทางดิจิทัลในที่ประชุมล่าสุดกล่าวถึง Cybersecurity โดยปัจจุบันความไว้วางใจและความปลอดภัยทางดิจิทัลมีความจำเป็นต่อการดำเนินธุรกิจและใช้ชีวิตประจำวัน ซึ่งการรักษาความไว้วางใจในโลกดิจิทัลเป็นงานที่ซับซ้อน เนื่องจากมีการใช้ Cyber Space มากขึ้นเรื่อย ๆ รวมทั้ง การรักษาความมั่นคงปลอดภัยทางดิจิทัลที่มีประสิทธิภาพก็เป็นเรื่องที่สำคัญมากที่ต้องให้ความสำคัญยิ่งยวดเช่นกัน ดังนั้น การใช้ชีวิตของมนุษย์ทุกคนจึงควรให้ความสำคัญกับข้อมูลความเป็นส่วนตัว การเข้ารหัสเพื่อความปลอดภัย ความปลอดภัยของเครือข่าย และความสามารถในการจัดการกับความเสี่ยงจากอาชญากรรมคอมพิวเตอร์ได้อย่างรู้เท่าทันและทันท่วงที

๖. AI and other Emerging Technologies ด้วยศักยภาพที่ชาญฉลาดของ AI ทำให้ปัจจุบันมีการใช้ AI กันอย่างแพร่หลาย ที่พบเห็นกันอย่างมากมายคือการใช้ AI อย่างไร้คุณธรรม เช่น ใช้ AI ในการสร้าง Clip Deep Fake ตัดต่อใบหน้าผู้นำระดับโลกแล้วให้พูดเรื่องไม่จริง สร้างความเสียหายและสับสนต่อสังคมโลก นอกจากนี้ยังมีการนำเทคโนโลยีอุบัติใหม่ไปประยุกต์ใช้ในเชิงลบด้วย ไม่ว่าจะเป็นเทคโนโลยี Blockchain, Quantum Computing, AR/VR ซึ่งการใช้เทคโนโลยีอย่าง

ไร้คุณธรรมจำเป็นจะต้องมีการจัดการประเด็นเหล่านี้อย่างจริงจังและรัดกุม รวมถึงการใช้ Generative AI อย่างเช่น ChatGPT อย่างมีคุณธรรมและอยู่ในสภาวะที่กฎหมายสามารถควบคุมการใช้งาน Generative AI ได้

๗. Global Digital Commons การให้ความสำคัญกับระบบเปิด เพื่อให้เกิดการแบ่งปันอย่างอิสระ เช่น ส่งเสริมมาตรฐานแบบเปิด ซอฟต์แวร์โอเพ่นซอร์ส ข้อมูลเปิด แบบจำลอง AI แบบเปิด รวมไปถึงเนื้อหาแบบเปิด เพื่อให้เกิดประโยชน์ของการเปลี่ยนแปลงทางดิจิทัล แหล่งข้อมูลเหล่านี้เรียกว่า Digital Commons มีการเรียกร้องให้รัฐบาล เอกชน องค์กรระหว่างประเทศ และภาคประชาสังคมทำงานเพื่อสร้างรูปแบบความร่วมมือใหม่ๆ แต่ทั้งนี้จะต้องอยู่ในกรอบแนวทางและกฎเกณฑ์สากล

๘. Accelerating Progress Towards the SDGs กระบวนการเร่งรัดต่อการขับเคลื่อนกรอบแนวทางในการนำเทคโนโลยีดิจิทัลมาใช้เพื่อการพัฒนาอย่างยั่งยืน เพื่อสนับสนุนเป้าหมาย SDGs ทั้ง ๑๗ ประการ โดยการใช้ประโยชน์จากเทคโนโลยีดิจิทัลเพื่อการพัฒนาที่ทั่วถึง เสมอภาค และยั่งยืนเป็นงานที่ต้องใช้ความร่วมมือระหว่างประเทศ รวมทั้งทุกฝ่ายควรต้องให้ความสำคัญเรื่องความมั่นคงปลอดภัย การมีความเป็นส่วนตัว ไม่ละเมิดสิทธิมนุษยชน ต้องคำนึงถึงส่วนรวมและประชาสังคมเป็นเป้าหมายสำคัญ

กรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cyber security capacity maturity model: CMM)

CMM เป็นแบบจำลองการประเมินศักยภาพและขีดความสามารถในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศทั่วโลก มีวัตถุประสงค์เพื่อใช้ประเมินศักยภาพและขีดความสามารถการบริหารจัดการระดับประเทศ พัฒนาโดย The Global Cyber Security Capacity Centre แห่ง University of Oxford มีเป้าหมายช่วยเพิ่มขีดความสามารถการบริหารจัดการภัยไซเบอร์ของประเทศให้เป็นระบบ มีประสิทธิผล เป็นที่ยอมรับในระดับสากล ซึ่ง The Global Cyber Security Capacity Centre ได้นำ CMM มาใช้ประเมินความสามารถด้านการบริหารจัดการภัยไซเบอร์มาแล้วกว่า ๑๐๐ ประเทศทั่วโลก การพัฒนา “กรอบแนวคิดในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ” ได้แนวคิดมาจากเอกสาร CMM โดยนำมาปรับแต่งเพิ่มเติมให้เหมาะกับสถานการณ์ปัจจุบันและสภาวะแวดล้อมของประเทศไทย โดยแบ่งมิติการพัฒนายุทธศาสตร์ดังกล่าวออกเป็น ๕ มิติ ดังนี้

มิติที่ ๑ Cybersecurity Policy and Strategy เป็นมิติที่เกี่ยวข้องกับการประเมินขีดความสามารถในการพัฒนานโยบายและกลยุทธ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของประเทศ ซึ่งแบ่งออกเป็น ๖ ปัจจัย ดังต่อไปนี้

๑. National Cybersecurity Strategy เกี่ยวข้องกับขีดความสามารถในการพัฒนากลยุทธ์ความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ องค์กรที่เกี่ยวข้องและเนื้อหาของกลยุทธ์ดังกล่าว

๒. Incident Response เกี่ยวข้องกับขีดความสามารถในการระบุและกระบวนการในการตอบสนองต่อภัยคุกคามด้านไซเบอร์ระดับประเทศ

๓. Critical Infrastructure (CI) Protection เกี่ยวข้องกับขีดความสามารถในการระบุโครงสร้างพื้นฐานที่สำคัญยิ่งยวดของประเทศ และการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ

๔. Crisis Management เกี่ยวข้องกับขีดความสามารถในการวางแผนบริหารจัดการกับวิกฤตการณ์ฉุกเฉิน การฝึกฝนเตรียมรับวิกฤตการณ์ฉุกเฉิน และการสร้างสถานการณ์จำลองให้พนักงานในองค์กรเตรียมพร้อมรับมือกับวิกฤตการณ์ทางไซเบอร์ต่าง ๆ

๕. Cyber Defense Consideration เกี่ยวข้องกับขีดความสามารถในการออกแบบระบบป้องกันภัยไซเบอร์ระดับประเทศและการนำกลยุทธ์การป้องกันทางไซเบอร์ของภาครัฐไปปฏิบัติจริง

๖. Communications Redundancy เกี่ยวข้องกับขีดความสามารถในการวางแผนให้ระบบสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องเมื่อเกิดภัยคุกคามทางไซเบอร์ยังสามารถติดต่อกันได้ มีการระบุหน้าที่ของบุคลากรที่เกี่ยวข้องอย่างชัดเจน รวมไปถึงการมีแผนสำรองเมื่อระบบการสื่อสารล้มเหลว เช่น ระบบโทรศัพท์เคลื่อนที่ เป็นต้น

มิติที่ ๒ Cyber Culture and Society เป็นมิติที่เกี่ยวข้องกับการประเมินมุมมองและทัศนคติของประชาชนในประเทศในเรื่องความเชื่อมั่นด้านความมั่นคงปลอดภัยด้านไซเบอร์ในการใช้

บริการอินเทอร์เน็ต หรือ Online Service ต่าง ๆ รวมทั้งความเข้าใจของประชาชนในเรื่องความเสี่ยงในการใช้อินเทอร์เน็ต ซึ่งแบ่งออกเป็น ๕ ปัจจัยย่อย ดังต่อไปนี้

๑. Cybersecurity Mind-set เกี่ยวข้องกับการประเมินระดับการให้ความสำคัญต่อเรื่องความมั่นคงปลอดภัยไซเบอร์ ทัศนคติต่อความมั่นคงปลอดภัยด้านไซเบอร์ และการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ ภาคเอกชน รวมทั้งผู้ใช้บริการ Online Service ต่าง ๆ

๒. Trust and Confidence on the Internet เกี่ยวข้องกับการประเมินความเชื่อมั่นด้านความปลอดภัยไซเบอร์ของผู้ใช้บริการ Online Service, E-Government และ E-Commerce

๓. User Understanding of Personal Information Protection Online เกี่ยวข้องกับการประเมินผู้ใช้บริการอินเทอร์เน็ตของภาครัฐและภาคเอกชนในเรื่องความตระหนักและความเข้าใจถึงภัยไซเบอร์ที่มากับ Online Service, E-Government และ E-Commerce

๔. Reporting Mechanisms เกี่ยวข้องกับการสำรวจช่องทางการส่งรายงานที่เกี่ยวข้องกับอาชญากรรมไซเบอร์อย่างเป็นระบบ

๕. Media and social media เกี่ยวข้องกับการสำรวจการให้ความรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในการใช้งาน social media

มิติที่ ๓ Cybersecurity Education, Training and Skills เป็นมิติที่เกี่ยวข้องกับการประเมินการบริหารจัดการเรื่องการเพิ่มความตระหนักให้ประชาชนรู้ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์ของทั้งภาครัฐและภาคเอกชน นอกจากนี้ยังประเมินการอบรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ ภาคเอกชนและประชาชนทั่วไป ซึ่งแบ่งออกเป็น 3 ปัจจัย ดังต่อไปนี้

๑. Awareness Raising เกี่ยวข้องกับความหลากหลายและรูปแบบของโครงการในการเพิ่มความตระหนักรู้ถึงความเสี่ยงและภัยคุกคามไซเบอร์.

๒. Framework for Education เกี่ยวข้องกับระบบการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ คุณภาพของผู้สอนในประเทศ และยังมีการตรวจสอบความสนใจด้านความมั่นคงปลอดภัยไซเบอร์ในภาครัฐและภาคเอกชน

๓. Framework for Professional Training เกี่ยวข้องกับระบบการอบรมด้านความมั่นคงปลอดภัยไซเบอร์ และยังมีการตรวจสอบแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร

มิติที่ ๔ Legal and Regulatory Frameworks เป็นมิติที่เกี่ยวข้องกับการประเมินขีดความสามารถของรัฐบาลในการร่างกฎหมายและออกกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งแบ่งออกเป็น ๓ ปัจจัย ดังต่อไปนี้

๑. Legal Frameworks เกี่ยวข้องกับขอบเขตของกฎหมายและการบังคับใช้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๒. Criminal Justice System เกี่ยวข้องกับความสามารถในการบังคับใช้กฎหมายเพื่อการสืบสวนสอบสวนอาชญากรรมไซเบอร์ รวมทั้งความสามารถของศาลในการตัดสินคดีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์

๓. Formal and Informal Cooperation Frameworks to Combat Cybercrime เกี่ยวข้องกับความร่วมมือขององค์กรทั้งภายในประเทศและต่างประเทศในการจัดการกับอาชญากรรมไซเบอร์

มิติที่ ๕ Standards, Organizations and Technologies เป็นมิติที่เกี่ยวข้องกับการประเมินประสิทธิผลในการใช้เทคโนโลยีความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยไซเบอร์ในระดับบุคคล ระดับองค์กร และ โครงสร้างพื้นฐานของประเทศ นอกจากนี้ยังมีการตรวจสอบมาตรฐานการควบคุม และการพัฒนาเทคโนโลยีเพื่อลดความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งแบ่งออกเป็น ๗ ปัจจัย คือ

๑. Adherence to Standards เกี่ยวข้องกับการประเมินขีดความสามารถของรัฐบาลในการร่างมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศและการนำมาตรฐานความมั่นคงปลอดภัยไซเบอร์มาปฏิบัติจริงในประเทศ

๒. Internet Infrastructure Resilience เกี่ยวข้องกับการประเมินความเชื่อมั่นของประชาชนในเรื่องการให้บริการอินเทอร์เน็ตและโครงสร้างพื้นฐานสำคัญของประเทศ

๓. Software Quality เกี่ยวข้องกับการตรวจสอบคุณภาพการใช้งานของโปรแกรมและความต้องการคุณสมบัติต่าง ๆ ในโปรแกรมด้านความมั่นคงปลอดภัยไซเบอร์จากภาครัฐและภาคเอกชน

๔. Technical Security Controls เกี่ยวข้องกับการควบคุมความมั่นคงปลอดภัยไซเบอร์ในทางเทคนิคของบุคคลทั่วไป ภาครัฐและภาคเอกชน

๕. Cryptographic Controls เกี่ยวข้องกับการควบคุมการเข้ารหัสของทุกภาคส่วนในอุตสาหกรรมและบุคคลทั่วไป เพื่อป้องกันไม่ให้ข้อมูลสำคัญถูกเผยแพร่โดยไม่ได้รับอนุญาต

๖. Cybersecurity Marketplace เกี่ยวข้องกับการส่งเสริมตลาดให้มีการแข่งขันในการพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ และธุรกิจประกันที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๗. Responsible Disclosure เกี่ยวข้องกับหน่วยงานที่มีหน้าที่ในการเก็บข้อมูลและเผยแพร่ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีความเกี่ยวข้องกับทุกภาคส่วนในอุตสาหกรรม

สรุป

จากผลการพิจารณาแนวคิดที่มีความสอดคล้องกับการพัฒนาระบบข่าวกรองแบบเปิดในการศึกษาครั้งนี้ ผู้วิจัยได้เก็บข้อมูลสำคัญผ่านกระบวนการสัมภาษณ์เชิงลึก (In-depth interview) จากผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญด้านไซเบอร์ และนักวิชาการ รวมถึงได้ดำเนินการศึกษาและวิจัยเอกสารต่าง ๆ (Documentation Research) เช่น มาตรฐานสากล กรอบการพัฒนาซอฟต์แวร์ เป็นต้น

เพื่อนำมาประยุกต์ใช้ในการจัดทำแนวทางพัฒนาระบบข่าวกรองแบบเปิดฯ ของ ทบ. โดยจะเปรียบเทียบหาความสัมพันธ์ระหว่าง OSINT กับ NIST Framework และวิเคราะห์ข้อดีข้อเสียในการออกแบบทางเลือกในการพัฒนาระบบข่าวกรองแบบเปิดฯ ซึ่งจะกล่าวต่อไปในบทที่ ๔

นอกจากนี้ การวิจัยครั้งนี้ ใช้กรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity capacity maturity model: CMM) ของ GCSCC แห่ง University of Oxford ซึ่งแบ่งมิติของการประเมินขีดความสามารถออกเป็น ๕ มิติ เป็นเครื่องมือในการประเมินขีดความสามารถของ ทบ. ในการรับมือกับภัยคุกคามทางไซเบอร์ เพื่อวิเคราะห์แนวโน้มความพร้อมศักยภาพด้านไซเบอร์ในอนาคต

บทที่ ๔
วิเคราะห์สถานภาพในการพัฒนาระบบข่าวกรองแบบเปิด ของกองทัพบก

การศึกษาวิจัย เรื่อง “แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก” ผู้วิจัยได้ทำการค้นคว้าข้อมูล ๑. เพื่อศึกษาและวิเคราะห์กระบวนการข่าวกรองแบบเปิด (Open-Source Intelligence: OSINT) ในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อนำไปสู่การปฏิบัติจริงทั้งในการแก้ปัญหาทางไซเบอร์ในระยะสั้น และระยะยาว ๒. เพื่อจัดทำข้อเสนอแนะแนวทางการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก ว่าด้วยการข่าวกรองแบบเปิด ซึ่งผู้วิจัยจะทำการศึกษาค้นคว้าข้อมูลต่าง ๆ โดยใช้วิธีการวิจัย ๒ วิธี คือ ๑. การวิจัยเอกสาร (Documentary research) และ ๒. การวิจัยเชิงคุณภาพ (Qualitative research) สามารถวิเคราะห์สถานภาพในการพัฒนาระบบข่าวกรองแบบเปิด ของกองทัพบก ได้ดังนี้

การวิเคราะห์สถานภาพ

๑. วิเคราะห์กระบวนการข่าวกรองแบบเปิด

แม้ว่าในปัจจุบันยังไม่มีกรอบการพัฒนาระบบข่าวกรองแบบเปิด หรือ “OSINT development framework” เฉพาะที่รองรับงานทุกด้าน รวมถึงงานในมิติการปฏิบัติการไซเบอร์ ซึ่งมีความสำคัญอย่างมาก เนื่องจากการรวบรวมและการวิเคราะห์ข้อมูลที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์สามารถตรวจจับและตอบสนองต่อภัยคุกคาม ความเสี่ยงทางไซเบอร์ การระบาดของมัลแวร์ ความร้ายแรงทางไซเบอร์ และอื่น ๆ ได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม ด้วยความก้าวหน้ายุคดิจิทัลทำให้มีเครื่องมือ (Tool) เทคโนโลยี (Technology) และกระบวนการ (Process) ที่เป็นที่นิยมใช้กันในชุมชน (Community) ให้เลือกเป็นจำนวนมาก เพื่อนำมาปรับใช้กับองค์กร

จากผลการศึกษา พบว่า กระบวนการข่าวกรองแบบเปิด (OSINT Process) เป็นส่วนหนึ่งของวงรอบข่าวกรอง (Intelligence Cycle) และมีขั้นตอนที่คล้ายกัน ซึ่งอาจประสบปัญหา/อุปสรรคขึ้นได้ ตัวอย่างดังตารางที่ ๔ – ๑

ตารางที่ ๔ – ๑ ปัญหา/อุปสรรคของวงรอบข่าวกรอง (Intelligence Cycle) แบบดั้งเดิม

ขั้นตอน	ปัญหา/อุปสรรค
ขั้นตอนที่ ๑ การวางแผนและกำหนดทิศทาง	• หากไม่จัดสรรทรัพยากรที่เพียงพอสำหรับการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับ

ขั้นตอน	ปัญหา/อุปสรรค
	ความปลอดภัยทางไซเบอร์ ก็อาจไม่สามารถระบุและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ
ขั้นตอนที่ ๒ การรวบรวม	• ไม่สามารถเข้าถึงแหล่งข้อมูลที่ถูกต้อง • ขาดความเชี่ยวชาญด้านเทคนิคในการรวบรวมและวิเคราะห์ข้อมูลอย่างมีประสิทธิภาพ • มีความเป็นไปได้ที่ข้อมูลที่รวบรวมอาจมีความไม่เชื่อถือได้ จึงต้องมีการตรวจสอบและยืนยันข้อมูลที่ถูกต้องเพื่อให้ได้ข้อมูลที่มีคุณภาพและน่าเชื่อถือ • การเก็บข้อมูลอาจเผชิญกับปัญหาที่เกี่ยวข้องกับความเป็นส่วนตัว และกฎหมายด้านความมั่นคง
ขั้นตอนที่ ๓ การประมวลผล	• ไม่สามารถผลิตผลิตภัณฑ์ข่าวกรองที่ดำเนินการได้ทันเวลา • การใช้เทคนิคและเครื่องมือในการเก็บข้อมูลและวิเคราะห์อาจเผชิญกับข้อจำกัดทางเทคนิค เช่น การสะดวกและความสามารถในการรวบรวมข้อมูลจากแหล่งที่ไม่เปิดเผย การประมวลผลข้อมูลที่มีปริมาณมาก เป็นต้น
ขั้นตอนที่ ๔ การวิเคราะห์และการผลิต	• เจ้าหน้าที่ขาดความเชี่ยวชาญในการวิเคราะห์ข้อมูลที่รวบรวมและเปลี่ยนเป็นผลิตผลข่าวกรองที่นำไปปฏิบัติได้ • บางครั้งการเก็บข้อมูลอาจเผชิญกับข้อมูลที่สะเพร่าหรือข้อมูลที่ไม่ครบถ้วน ทำให้การวิเคราะห์และการตัดสินใจอาจเป็นไปได้ลำบากและไม่แม่นยำพอ

ตารางที่ ๔ – ๑ ปัญหา/อุปสรรคของวงรอบข่าวกรอง (Intelligence Cycle) แบบดั้งเดิม (ต่อ)

ขั้นตอน	ปัญหา/อุปสรรค
	เวลาและทรัพยากรที่จำกัด เนื่องจากการวิเคราะห์ข้อมูลอาจเสียเวลาและทรัพยากรมาก เนื่องจากต้องทำการวิเคราะห์ข้อมูลขนาดใหญ่หรือการวิเคราะห์เชิงลึก

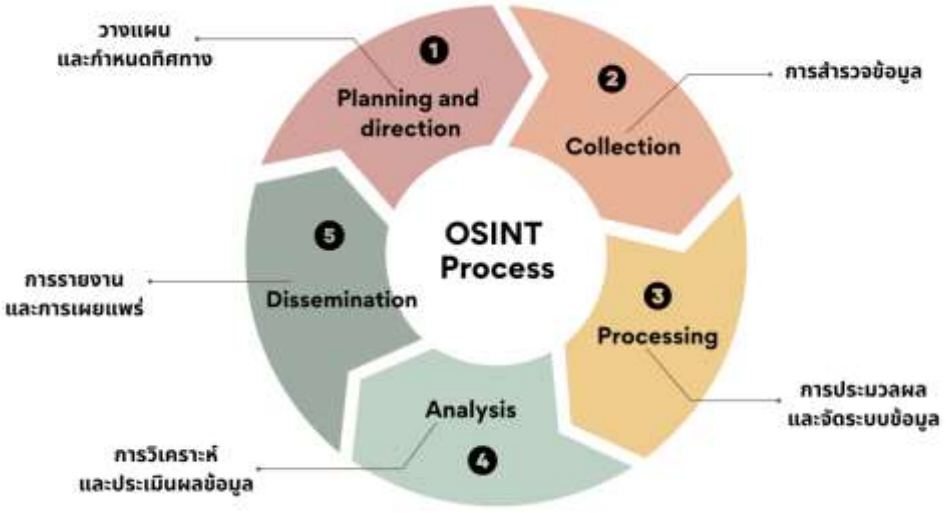
ขั้นตอนที่ ๕ การเผยแพร่	ไม่มีกลไกที่มีประสิทธิภาพในการเผยแพร่ผลิตภัณฑ์ข่าวกรองไปยังผู้มีอำนาจตัดสินใจในเวลาที่เหมาะสมและทันท่วงที

ที่มา : จากผลการศึกษา บทที่ ๒ การทบทวนวรรณกรรม และบทที่ ๓ การพิจารณาแนวคิดที่มีความสอดคล้องกับการพัฒนาระบบข่าวกรองแบบเปิด

ดังนั้น การจัดการปัญหาและอุปสรรคเหล่านี้ในวงรอบข่าวกรองจำเป็นต้องมีการวางแผนอย่างรอบคอบและพิจารณาด้านทั้งเทคนิค ความมั่นคง และความเป็นไปได้ เพื่อให้การเก็บข้อมูล OSINT และวิเคราะห์ข้อมูลเป็นไปอย่างมีประสิทธิภาพและเป็นระบบ ทั้งนี้ การสร้างความร่วมมือระหว่างผู้เชี่ยวชาญด้านข่าวกรองและผู้ใช้ข้อมูลจึงเป็นสิ่งสำคัญในการแก้ไขปัญหาและอุปสรรคที่เกิดขึ้นในกระบวนการวงรอบข่าวกรอง

ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยจึงขอเสนอองค์ประกอบหลักในการพิจารณา เพื่อพัฒนากระบวนการข่าวกรองแบบเปิด (OSINT Process) ของกองทัพบก รายละเอียดดังแผนภาพที่ ๔ - ๑

แผนภาพที่ ๔ - ๑ กระบวนการข่าวกรองแบบเปิด (OSINT Process) ของกองทัพบก



ขั้นตอนที่ ๑ OSINT Planning and direction (วางแผนและกำหนดทิศทาง) - ระบุวัตถุประสงค์ของการสำรวจ OSINT และความต้องการข้อมูล วางแผนกระบวนการสำรวจ และวิเคราะห์ที่เหมาะสมกับวัตถุประสงค์ที่กำหนด ประกอบด้วยขั้นตอนย่อยซึ่งสามารถอธิบายได้ดังนี้

๑. กำหนดวัตถุประสงค์ (Objective Setting) กำหนดวัตถุประสงค์เพื่อให้ข้อมูลข่าวกรองเปิดช่วยในการตรวจสอบและประเมินความเสี่ยงทางไซเบอร์ ตรวจสอบความผิดปกติในระบบเครือข่าย หรือตรวจสอบการเข้าถึงที่ไม่ได้รับอนุญาตในระบบ เป็นต้น

๒.วางแผนการรวบรวมข้อมูล (Data Gathering Planning) โดยใช้เทคนิคและเครื่องมือที่เหมาะสม เช่น การสำรวจและตรวจสอบช่องโหว่ในระบบเครือข่าย การตรวจสอบฐานข้อมูลเปิดที่มีข้อมูลที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ เป็นต้น

๓. การนำทางและความเสี่ยง (Navigation and Risk Management) กำหนดแผนที่การนำทางในกระบวนการรวบรวมข้อมูล ซึ่งรวมถึงการกำหนดวิธีการนำทางในการค้นหาแหล่งข้อมูล และการระบุความเสี่ยงที่อาจเกิดขึ้นในการเข้าถึงแหล่งข้อมูล

ขั้นตอนที่ ๒ OSINT Collection (การสำรวจข้อมูล) - สำรวจและเก็บรวบรวมข้อมูลจากแหล่งข้อมูลที่เปิดเผย เช่น เว็บไซต์ โซเชียลมีเดีย บันทึกข้อมูลสาธารณะ ใช้เครื่องมือและเทคนิคต่าง ๆ เพื่อเก็บรวบรวมข้อมูลอย่างมีประสิทธิภาพ ประกอบด้วยขั้นตอนย่อยซึ่งสามารถอธิบายได้ดังนี้

๑. การกำหนดแหล่งข้อมูล จะต้องกำหนดแหล่งข้อมูลที่เหมาะสมและเกี่ยวข้องกับวัตถุประสงค์ เช่น เว็บไซต์สาธารณะ เว็บบอร์ด สื่อสังคมออนไลน์ บทความวิชาการ เป็นต้น

๒. การเปรียบเทียบแหล่งข้อมูล ควรเปรียบเทียบแหล่งข้อมูลต่าง ๆ เพื่อตัดสินใจเลือกใช้แหล่งข้อมูลที่เป็นไปตามความเหมาะสมและมีคุณภาพสูงที่สุด

๓. การจัดเก็บข้อมูล ควรจัดเก็บข้อมูลที่ได้จากแหล่งข้อมูล ซึ่งอาจเป็นการดาวน์โหลดไฟล์ บันทึกข้อมูลลงในฐานข้อมูล หรือใช้เครื่องมือสำเร็จรูปที่ช่วยในการจัดเก็บข้อมูลอย่างสะดวกและมีระบบ

ขั้นตอนที่ ๓ OSINT Processing (การประมวลผลและจัดระบบข้อมูล) - ประมวลผลข้อมูลที่สำรวจเพื่อตัดสินใจเกี่ยวกับความสำคัญและความเหมาะสม จัดระบบข้อมูลให้เป็นรูปแบบที่ใช้งานได้ในการวิเคราะห์ต่อไป ประกอบด้วยขั้นตอนย่อยซึ่งสามารถอธิบายได้ดังนี้

๑. การนำเข้าข้อมูลจะมีการนำเข้าข้อมูล OSINT ที่เก็บรวบรวมมาจากแหล่งต่าง ๆ เข้าสู่ระบบที่ใช้ในการวิเคราะห์ ระบบอาจเป็นฐานข้อมูล หรือเครื่องมือวิเคราะห์ที่ใช้ในการประมวลผลข้อมูล OSINT

๒. การเชื่อมต่อข้อมูล เช่น การเชื่อมต่อข้อมูลจากแหล่งต่าง ๆ เพื่อรวมข้อมูลที่เกี่ยวข้องหรือการเชื่อมต่อระบบที่ใช้ในการประมวลผล

๓. การคัดกรองและปรับข้อมูล โดยข้อมูลที่นำเข้าอาจมีความหลากหลายและมีรูปแบบที่แตกต่างกัน ในขั้นตอนนี้จะมีการคัดกรองและปรับข้อมูลเพื่อให้เป็นไปตามความต้องการและรูปแบบที่เหมาะสมสำหรับการวิเคราะห์ อาจมีการตัดส่วนที่ไม่เกี่ยวข้องกับวัตถุประสงค์การวิเคราะห์ออก

ขั้นตอนที่ ๔ OSINT Analysis (การวิเคราะห์และประเมินผลข้อมูล) - กระบวนการคัดกรองและวิเคราะห์ข้อมูลที่รวบรวมเพื่อเลือกและจัดระเบียบข้อมูลที่สำคัญและมีความสำคัญสูง เพื่อให้เกิดความเข้าใจในการรับมือกับความเสี่ยงทางไซเบอร์ วิเคราะห์แนวโน้มและรูปแบบโจมตีทางไซเบอร์ เพื่อให้สามารถพยากรณ์และตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพ ประกอบด้วยขั้นตอนย่อยซึ่งสามารถอธิบายได้ดังนี้

๑. การวิเคราะห์ข้อมูล จะมีการวิเคราะห์และตีความข้อมูล OSINT เพื่อทำความเข้าใจเกี่ยวกับข้อมูล การวิเคราะห์ข้อมูลอาจใช้เครื่องมือวิเคราะห์ข้อมูล และเทคนิคทางสถิติเพื่อช่วยในการสร้างความเข้าใจและการสรุปผลข้อมูล

๒. การสร้างแบบจำลองและรูปแบบ อาจใช้การสร้างแบบจำลองหรือรูปแบบทางคณิตศาสตร์ที่เหมาะสม เช่น การใช้เทคนิคการเรียนรู้เชิงลึก (Deep Learning) หรือ

การประมวลผลภาษาธรรมชาติ (Natural Language Processing) เพื่อสกัดข้อมูลสำคัญและสร้างรูปแบบในการวิเคราะห์ เป็นต้น

๓. การวิเคราะห์แนวโน้มและทิศทาง เป็นสิ่งสำคัญเพื่อตรวจสอบการเปลี่ยนแปลงและพยากรณ์สถานการณ์ที่อาจเกิดขึ้นในอนาคต โดยอาจใช้เครื่องมือเชิงสถิติ หรือเทคนิคการเรียนรู้เชิงลึก เพื่อตรวจสอบแนวโน้มและพยากรณ์สถานการณ์ต่าง ๆ

ขั้นตอนที่ ๕ OSINT Dissemination (การเผยแพร่) - รวบรวมข้อมูลที่วิเคราะห์แล้วให้เป็นรายงานที่เข้าใจง่ายและเป็นประโยชน์ นำเสนอข้อมูลแก่ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ประกอบด้วยขั้นตอนย่อยซึ่งสามารถอธิบายได้ดังนี้

๑. ตรวจสอบความเหมาะสม โดยตรวจสอบและประเมินความเหมาะสมของข้อมูล OSINT เพื่อให้แน่ใจว่าข้อมูลที่จะถูกแจกจ่ายเป็นข้อมูลที่เหมาะสม และมีประโยชน์ต่อการดำเนินงานปฏิบัติการ และการตัดสินใจในระดับทางกลยุทธ์

๒. การสร้างรายงานและสารสนเทศ ต้องเป็นไปในรูปแบบที่กระชับและมีประสิทธิภาพ จึงควรสร้างรายงานและสารสนเทศที่สื่อถึงข้อมูล OSINT อย่างชัดเจนและเข้าใจได้ง่าย รวมถึง การกำหนดรูปแบบของข้อมูล เช่น สรุปผล หรือแผนภาพที่ช่วยในการสื่อสารข้อมูลได้ชัดเจน เป็นต้น

๓. การเผยแพร่ข้อมูล ข้อมูล OSINT โดยใช้ช่องทางที่เหมาะสม เช่น เว็บไซต์ หรือพอร์ทัล (Portal) ที่ใช้ร่วมกัน แชทหรือสื่อสังคมออนไลน์ หรืออีเมล เพื่อให้ผู้ที่มีส่วนเกี่ยวข้องสามารถเข้าถึงข้อมูลได้

๔. การจัดการความปลอดภัย โดยการใช้ระบบรักษาความปลอดภัยที่เหมาะสมในการส่งข้อมูล รวมถึงการรักษาความลับและความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่เหมาะสมหรือไม่ได้รับอนุญาต

๕. การระบุและติดตามผู้รับข้อมูล ควรระบุผู้รับข้อมูลที่มีความเกี่ยวข้องและสามารถนำข้อมูลไปใช้ประโยชน์ได้ รวมถึง การติดตามว่าข้อมูลที่แจกจ่ายมีผลกระทบหรือมีการใช้งานอย่างไรในการปฏิบัติการไซเบอร์

๒. วิเคราะห์การใช้ OSINT ในปฏิบัติการไซเบอร์

๒.๑ การวิเคราะห์การใช้ OSINT ในปฏิบัติการไซเบอร์เชิงรับ (Passive OSINT)

“Passive OSINT” เป็นกระบวนการใช้ข้อมูลที่เปิดเผยต่อสาธารณะ เพื่อรวบรวมข้อมูลและวิเคราะห์สถานการณ์ด้านความมั่นคงปลอดภัยของระบบไซเบอร์ โดยไม่ต้องเข้าถึงระบบหรือแหล่งข้อมูลที่เป็นเจ้าของอยู่ สามารถสรุปสาระสำคัญได้ดังนี้

๒.๑.๑ การค้นคว้าภัยคุกคามไซเบอร์ (Cyber Threat Intelligence) สามารถใช้ OSINT เพื่อรวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ขององค์กร ข้อมูลนี้สามารถช่วยในการระบุเวกเตอร์การโจมตีที่อาจเกิดขึ้น ตลอดจนเครื่องมือ เทคนิค และขั้นตอน (TTP) ที่ใช้โดยผู้คุกคาม สิ่งนี้สามารถช่วยในการพัฒนากลยุทธ์การป้องกันที่มีประสิทธิภาพเพื่อป้องกันหรือบรรเทาการโจมตีทางไซเบอร์

๒.๑.๒ การประเมินช่องโหว่ (Vulnerability Assessment) สามารถใช้ OSINT เพื่อระบุช่องโหว่ที่อาจเกิดขึ้นในโครงสร้างพื้นฐานด้านไอทีและแอปพลิเคชันขององค์กร ซึ่งอาจรวมถึง

ตรวจสอบเวอร์ชั่นปัจจุบันของซอฟต์แวร์และระบบปฏิบัติการที่เป็นที่ใช้กันอยู่ เพื่อตระหนักถึงช่องโหว่ที่รู้จักและความเสี่ยงที่อาจเกิดขึ้น ระบบที่กำหนดค่าผิดพลาด หรือจุดอ่อนอื่น ๆ ที่ผู้โจมตีอาจนำไปใช้ประโยชน์ได้ ด้วยการใช้ OSINT เพื่อระบุช่องโหว่เหล่านี้ องค์กรสามารถดำเนินการเพื่อแพตช์หรือบรรเทาก่อนที่จะถูกโจมตี

๒.๑.๓ การตรวจสอบหลักฐานดิจิทัล (Digital Forensics) สามารถใช้ OSINT ตรวจสอบหลักฐานดิจิทัลที่เผยแพร่ต่อสาธารณะ เช่น ภาพหน้าจอ, โพสต์สื่อสังคมออนไลน์ เพื่อระบุความเสี่ยงหรือการกระทำที่เกี่ยวข้องกับระบบไซเบอร์

๒.๑.๔ การรับรู้ทางวิศวกรรมสังคม (Social Engineering Awareness) สามารถใช้ OSINT เพื่อสร้างความตระหนักรู้เกี่ยวกับการโจมตีทางวิศวกรรมสังคม เช่น Phishing โดยระบุตัวอย่างการโจมตีเหล่านี้ จากการศึกษาการโจมตีเหล่านี้ องค์กรสามารถเข้าใจกลยุทธ์ที่ผู้โจมตีใช้ได้ดีขึ้น และพัฒนาโปรแกรมการฝึกอบรมและการรับรู้ที่มีประสิทธิภาพมากขึ้นสำหรับกำลังพลของหน่วย

๒.๑.๕ การจัดการภาพลักษณ์ขององค์กร (Reputation Management) สามารถใช้ OSINT เพื่อตรวจสอบชื่อเสียงออนไลน์หรือภาพลักษณ์ขององค์กร รวมถึงการกล่าวถึงบนโซเชียลมีเดียและแพลตฟอร์มออนไลน์อื่น ๆ สิ่งนี้สามารถช่วยองค์กรในการระบุภัยคุกคามที่อาจเกิดขึ้นกับชื่อเสียงขององค์กร และดำเนินการเพื่อลดผลกระทบด้านลบ

การใช้งาน Passive OSINT ช่วยให้ผู้ใช้สามารถรับรู้เกี่ยวกับความเสี่ยงและช่องโหว่ที่อาจเกิดขึ้นในระบบไซเบอร์ และสามารถพัฒนามาตรการความมั่นคงปลอดภัยที่เหมาะสมต่อไปได้ อย่างไรก็ตาม ต้องตระหนักอยู่เสมอว่า การใช้งาน OSINT ต้องปฏิบัติตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องในเขตอำนาจทางกฎหมายที่มีผลบังคับใช้

๒.๒ การวิเคราะห์การใช้ OSINT ในปฏิบัติการไซเบอร์เชิงรุก (Active OSINT)

“Active OSINT” เป็นกระบวนการที่ใช้ข้อมูลที่เปิดเผยต่อสาธารณะเพื่อเข้าถึงและทดสอบระบบหรือแหล่งข้อมูลที่เป็นเจ้าของอยู่ โดยวัตถุประสงค์ของ Active OSINT อาจเป็นการระบุช่องโหว่หรือความอ่อนแอในระบบ หรือเข้าถึงข้อมูลที่ต้องการจากแหล่งที่มีความปกคลุมหรือถูกควบคุม สามารถสรุปสาระสำคัญได้ดังนี้

๒.๒.๑ การตามล่าภัยคุกคามทางไซเบอร์ (Cyber Threat Hunting) สามารถใช้ OSINT เพื่อค้นหาภัยคุกคามที่อาจเกิดขึ้นกับความปลอดภัยทางไซเบอร์ขององค์กรในเชิงรุก ด้วยการใช้ OSINT เพื่อระบุกิจกรรมที่ผิดปกติหรือตัวบ่งชี้การประนีประนอมอื่น ๆ องค์กรสามารถดำเนินการ เพื่อตรวจสอบภัยคุกคามที่อาจเกิดขึ้นก่อนที่จะบานปลายไปสู่การโจมตีเต็มรูปแบบ

๒.๒.๒ การสำรวจข้อมูล (Reconnaissance) ใช้ข้อมูลที่เปิดเผยต่อสาธารณะเพื่อระบุข้อมูลเชิงบุคคลหรือรายละเอียดเกี่ยวกับเป้าหมาย เช่น ชื่อ, ที่อยู่, หมายเลขโทรศัพท์ เพื่อใช้ในกระบวนการโจมตีต่อไป

๒.๒.๓ การแบ่งกลุ่มและการตรวจสอบข้อมูล (Enumeration) ใช้ข้อมูลที่เปิดเผยต่อสาธารณะเพื่อระบุและตรวจสอบข้อมูลเกี่ยวกับระบบหรือเป้าหมาย เช่น รายชื่อผู้ใช้งาน, รายชื่อเซิร์ฟเวอร์ เพื่อใช้ในการวางแผนการโจมตี

๒.๒.๔ การติดตามร่องรอยและการค้นหาข้อมูล (Digital footprints) ใช้ข้อมูลที่เปิดเผยต่อสาธารณะเพื่อติดตามและค้นหาข้อมูลเพิ่มเติมเกี่ยวกับเป้าหมาย เช่น การค้นหาที่อยู่ IP, การตรวจสอบโฮสต์ที่ใช้งาน, การตรวจสอบโดเมนเนม เพื่อใช้ในการวางแผนการโจมตี

การใช้งาน Active OSINT ช่วยให้ผู้ใช้สามารถเข้าถึงข้อมูลที่ไม่เปิดเผยและทดสอบความมั่นคงปลอดภัยของระบบได้อย่างระมัดระวัง โดยสามารถระบุช่องโหว่และปรับปรุงระบบให้มีความปลอดภัยมากยิ่งขึ้นได้ อย่างไรก็ตาม ต้องตระหนักอยู่เสมอว่า การใช้งาน OSINT ต้องปฏิบัติตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องในเขตอำนาจทางกฎหมายที่มีผลบังคับใช้

ตารางที่ ๔ – ๒ การประยุกต์ใช้ OSINT ในปฏิบัติการไซเบอร์

ปฏิบัติการไซเบอร์	การประยุกต์ใช้ OSINT
ปฏิบัติการไซเบอร์เชิงรุก (Offensive)	• การตามล่าภัยคุกคามทางไซเบอร์ (Cyber Threat Hunting) • การสำรวจข้อมูล (Reconnaissance) • การแบ่งกลุ่มและการตรวจสอบข้อมูล (Enumeration)
ปฏิบัติการไซเบอร์เชิงรับ (Defensive)	• การประเมินช่องโหว่ (Vulnerability Assessment) • การรับรู้ทางวิศวกรรมสังคม (Social Engineering Awareness) • การจัดการภาพลักษณ์ขององค์กร (Reputation Management)
การประเมินและตรวจสอบดิจิทัล (Audit)	• การค้นคว้าภัยคุกคามไซเบอร์ (Cyber Threat Intelligence)
การตรวจพิสูจน์หลักฐานดิจิทัล (Forensics)	• การตรวจสอบหลักฐานดิจิทัล (Digital Forensics) • การติดตามร่องรอยและการค้นหาข้อมูล (Digital footprints)

ที่มา : จากผลการศึกษา บทที่ ๓ การพิจารณาแนวคิดที่มีความสอดคล้องกับการพัฒนาระบบข่าวกรองแบบเปิด

การประเมินขีดความสามารถด้านไซเบอร์ (Cybersecurity Capacity)

ผู้วิจัยได้ทำการศึกษาแนวคิดในการประเมินความพร้อมด้านไซเบอร์ ของประเทศไทย โดยใช้กรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cyber security capacity maturity model: CMM) แห่ง University of Oxford มาประยุกต์ใช้ให้เหมาะสมกับสถานการณ์ปัจจุบันและสภาวะแวดล้อมของประเทศไทย ตามบริบทของภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่งคง ซึ่งแบ่งออกเป็น ๕ มิติ สามารถประเมินผลได้ดังนี้

มิติที่ ๑ Cybersecurity Policy and Strategy หรือ การประเมินขีดความสามารถในการพัฒนานโยบายและกลยุทธ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของประเทศ จากการศึกษา พบว่า ประเทศไทย มีการประกาศโครงสร้างหน่วยงานป้องกันภัยคุกคามทางไซเบอร์ระดับชาติ ภายใต้ พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ มีการกำหนดคณะกรรมการ และอำนาจหน้าที่รับผิดชอบอย่างชัดเจน และมีการประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง ทั้งภาครัฐและเอกชน (บางส่วน)

มิติที่ ๒ Cyber Culture and Society หรือ การประเมินมุมมองและทัศนคติของประชาชนในเรื่องความเชื่อมั่นด้านความมั่นคงปลอดภัยด้านไซเบอร์ จากการศึกษา พบว่า คนไทยมีการรับรู้ถึงความเสี่ยงทางไซเบอร์ที่เพิ่มขึ้น เช่น การโจมตีไซเบอร์ การฉ้อโกงออนไลน์ การละเมิดความเป็นส่วนตัวออนไลน์ และการแพร่ระบาดของไวรัสและมัลแวร์ อีกทั้ง การใช้สื่อสังคมออนไลน์ในการแสดงความคิดเห็น การร่วมกิจกรรมกับกลุ่มหรือองค์กรที่มีความเชื่อเห็นเดียวกัน เป็นส่วนหนึ่งของการเสริมสร้างความเชื่อมั่นและการต่อต้านต่อเหตุการณ์หรือประเด็นที่เกี่ยวข้องกับสังคมหรือการเมืองในประเทศไทย

มิติที่ ๓ Cybersecurity Education, Training and Skills หรือ การประเมินการบริหารจัดการเรื่องการเพิ่มความตระหนักให้ประชาชนรู้ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์ของทั้งภาครัฐและภาคเอกชน จากการศึกษา พบว่า ประเทศไทยมีการพัฒนาหลักสูตรการศึกษาที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านไซเบอร์ในระดับทั้งสูงและต่ำ เช่น หลักสูตรปริญญาตรีและปริญญาโทในสาขาวิทยาการคอมพิวเตอร์ วิทยาการข้อมูล เป็นต้น ทั้งนี้ เพื่อสร้างการเรียนรู้และทักษะที่จำเป็นสำหรับความเข้าใจและการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านไซเบอร์

มิติที่ ๔ Legal and Regulatory Frameworks หรือ การประเมินขีดความสามารถของรัฐบาลในการร่างกฎหมายและออกกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ จากการศึกษา พบว่า ประเทศไทยมีการบังคับใช้กฎหมายด้านไซเบอร์ ได้แก่ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และ พ.ร.บ. คุ้มครองส่วนบุคคลฯ

มิติที่ ๕ Standards, Organizations and Technologies หรือ การประเมินประสิทธิผลในการใช้เทคโนโลยีความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยไซเบอร์ในระดับบุคคล ระดับองค์กร และโครงสร้างพื้นฐานของประเทศ จากการศึกษา พบว่า ประเทศไทยมีการใช้และรับรู้มาตรฐานด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับด้านไซเบอร์ เช่น ISO/IEC 27001 (Information Security Management System), NIST Cybersecurity Framework, และมาตรฐานการรักษา

ความลับของข้อมูลทางการแพทย์ (HIPAA) ที่เกี่ยวข้องกับสายงานทางการแพทย์ นอกจากนี้ ประเทศไทยมีหลายองค์กรที่มีบทบาทและความรับผิดชอบในด้านความมั่นคงปลอดภัยด้านไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เป็นต้น

ดังนั้น เมื่อพิจารณาด้านความสามารถด้านไซเบอร์ (Cybersecurity Capacity) ของประเทศไทยในการพัฒนาระบบข่าวกรองแบบเปิด (OSINT development framework) สามารถกล่าวได้ว่า ประเทศไทยมีความสามารถในการเข้าถึงและรวบรวมข้อมูลสาธารณะที่มีอยู่ในเครือข่ายอินเทอร์เน็ต โดยใช้เทคโนโลยีและเครื่องมือที่เหมาะสม เช่น เครื่องมือการสืบค้น โครงสร้างข้อมูล และข้อมูลสาธารณะที่เปิดเผย เป็นต้น ภายใต้กฎหมายด้านไซเบอร์ที่มีการบังคับใช้ ได้แก่ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และ พ.ร.บ. คุ้มครองส่วนบุคคลฯ รวมถึงกฎระเบียบอื่น ๆ ที่เกี่ยวข้อง

ความสัมพันธ์ระหว่าง OSINT กับ NIST Cybersecurity Framework

NIST Cyber Security Framework (CSF) ประกอบด้วยมาตรฐาน แนวปฏิบัติ และแนวปฏิบัติที่ดีที่สุด (Best Practice) ในการจัดการความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ โดยไม่คำนึงถึงประเภทขององค์กรหรือพันธกิจ กิจกรรม มาตรการตอบโต้ ความรับผิดชอบ และวัตถุประสงค์ที่เกี่ยวข้องกับการสร้างความเชื่อมั่นในการรักษาความปลอดภัย โดยสามารถสรุปและอภิปรายได้ด้วย NIST CSF

ถึงแม้ว่า OSINT (Open Source Intelligence) และ NIST Cybersecurity Framework จะเป็นสองแนวคิดที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านไซเบอร์ แต่ก็มีความสำคัญและบทบาทที่แตกต่างกัน ดังนั้น จำเป็นต้องตระหนักอยู่เสมอว่า การประยุกต์ใช้กับ OSINT ในมิติความปลอดภัยทางไซเบอร์ ต้องได้รับการปรับแต่งตามความต้องการ (Requirement) และระดับความเสี่ยงเฉพาะขององค์กร

ตารางที่ ๔ – ๓ Applying NIST Cybersecurity Framework to OSINT

องค์ประกอบหลัก	การประยุกต์ใช้
Identify (การระบุ)	• ระบุและทำความเข้าใจเป้าหมายการรักษาความปลอดภัยทางไซเบอร์ขององค์กร รวมถึงการปกป้องทรัพย์สินที่สำคัญ ข้อกำหนดการปฏิบัติตามข้อกำหนด และวัตถุประสงค์ในการบริหารความเสี่ยง • ใช้ OSINT เพื่อรวบรวมข้อมูลเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้น ช่องโหว่ และความเสี่ยงเฉพาะสำหรับภูมิทัศน์ความปลอดภัยทางไซเบอร์ขององค์กร • ประเมินความสามารถของ OSINT ในปัจจุบันขององค์กร และระบุช่องว่างหรือพื้นที่สำหรับการปรับปรุงในการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์
Protect (การป้องกัน)	• พัฒนาและใช้มาตรการเพื่อปกป้องทรัพย์สินที่สำคัญ และข้อมูลที่ละเอียดอ่อนตามข้อมูลเชิงลึกที่ได้รับจาก OSINT • ใช้ประโยชน์จาก OSINT เพื่อระบุแนวทางปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยทางไซเบอร์ มาตรฐานสากล และภัยคุกคามที่เกิดขึ้นใหม่ ที่สามารถแนะนำการดำเนินการตามมาตรการป้องกัน • ใช้การควบคุมความปลอดภัย เช่น การควบคุมการเข้าถึง การแบ่งส่วนเครือข่าย การเข้ารหัส และกลไกการพิสูจน์ตัวตน โดยยึดตามการค้นพบของ OSINT
Detect (การตรวจจับ)	• ใช้เครื่องมือและเทคนิค OSINT เพื่อตรวจสอบและตรวจจับเหตุการณ์ความปลอดภัยทางไซเบอร์ การโจมตี หรือช่องโหว่ที่อาจเกิดขึ้น • สร้างระบบเพื่อรวบรวมและวิเคราะห์ข้อมูล OSINT สำหรับ indicators of compromise (IOCs) ข่าวกรองภัยคุกคาม และกิจกรรมที่ผิดปกติ • รับข่าวสารเกี่ยวกับเวกเตอร์การโจมตีใหม่ ๆ แคมเปญมัลแวร์ ช่องโหว่ กลวิธี และเทคนิคของผู้คุกคามที่เกิดขึ้นใหม่ผ่านแหล่งที่มาของ OSINT

ตารางที่ ๔ – ๓ Applying NIST Cybersecurity Framework to OSINT (ต่อ)

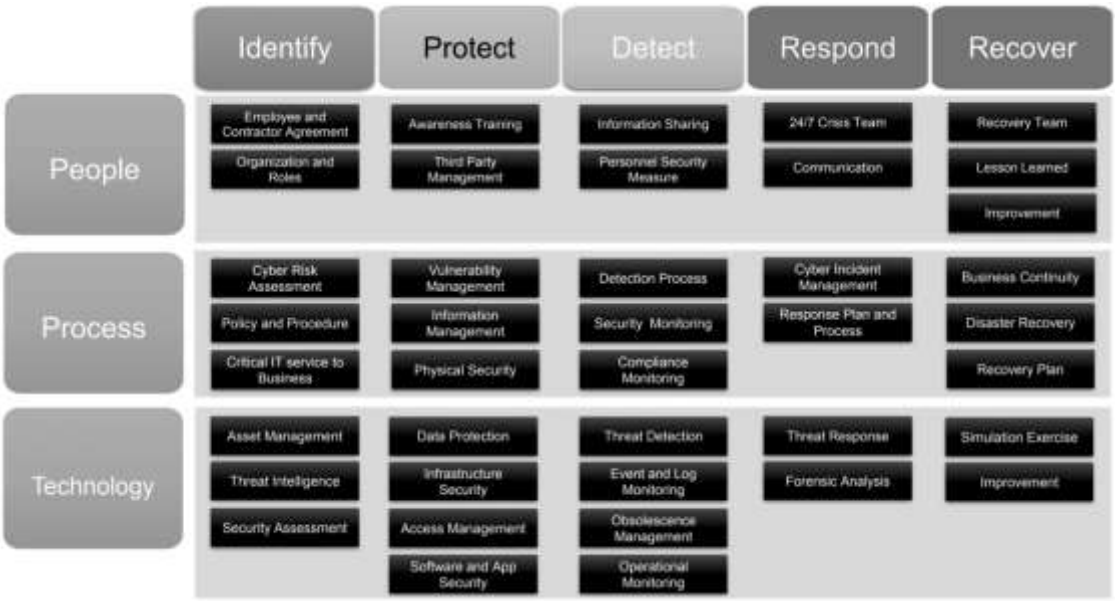
องค์ประกอบหลัก	การประยุกต์ใช้
Respond (การตอบสนอง)	• พัฒนาแผนการตอบสนองต่อเหตุการณ์ที่รวมการใช้ OSINT ในระหว่างเหตุการณ์ความปลอดภัยทางไซเบอร์

	• ใช้ประโยชน์จาก OSINT เพื่อรวบรวมข้อมูลตามเวลาจริงเกี่ยวกับเหตุการณ์ รวมถึงตัวแสดงภัยคุกคาม ลักษณะเฉพาะของมัลแวร์ โครงสร้างพื้นฐานคำสั่งและการควบคุม และรายละเอียดอื่น ๆ ที่เกี่ยวข้อง • รวมข่าวกรองที่ได้รับจาก OSINT เข้ากับกระบวนการตอบสนองเหตุการณ์เพื่อเป็นแนวทางในการตัดสินใจ การกักกัน และความพยายามในการกำจัด
Recover (การกู้คืน)	• ใช้ OSINT เพื่อประเมินผลกระทบของเหตุการณ์ด้านความปลอดภัยในโลกไซเบอร์และช่วยเหลือในกระบวนการกู้คืน • ใช้ประโยชน์จาก OSINT เพื่อระบุและแก้ไขช่องโหว่หรือจุดอ่อนที่ถูกโจมตีในระหว่างเหตุการณ์ • รวมการค้นพบ OSINT เข้ากับแผนการกู้คืนเพื่อเพิ่มความยืดหยุ่นในอนาคต อัปเดตการควบคุมความปลอดภัย และป้องกันเหตุการณ์ที่คล้ายคลึงกัน

ที่มา : ผลการวิเคราะห์ความสัมพันธ์ระหว่าง OSINT กับ NIST Std. ที่ทางผู้วิจัยเสนอ

ผู้วิจัยได้ดำเนินการประยุกต์ใช้กรอบการคืนสภาพได้ด้านไซเบอร์ (Cyber Resilience) สำหรับปฏิบัติการไซเบอร์ OSINT ซึ่งได้อ้างอิงตามแนวคิด NIST Cybersecurity Framework โดยแยกหัวข้อเป็นการระบุ (Identify), การตรวจจับ (Detect), การป้องกัน (Protect), การตอบสนอง (Respond) และการคืนสภาพ (Recover) แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับปฏิบัติการไซเบอร์ OSINT โดยใช้วิธีการ Mapping กับเสาหลักของความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ๑. บุคลากร (People) ๒. กระบวนการ (Process) และ ๓. เทคโนโลยี (Technology) ดังแผนภาพที่ ๔ - ๒

แผนภาพที่ ๔ - ๒ กรอบการคืนสภาพได้ด้านไซเบอร์ (Cyber Resilience) ในปฏิบัติการไซเบอร์ OSINT



ที่มา : ACIS - How to Implement the NIST Framework, 2023.

จากแผนภาพที่ ๔ - ๒ อธิบายได้ว่า

๑. การระบุความเสี่ยง (Identification) เป็นสิ่งที่ควรทำเป็นอันดับแรก เนื่องจากเป็นการทำความเข้าใจในการบริหารจัดการภายในองค์กร ตั้งแต่เรื่องบุคลากร ขีดความสามารถข้อมูล และระบบภายในต่าง ๆ ตลอดจนทรัพย์สินทั้งหมดขององค์กร เพื่อนำมาประเมินความเสี่ยง และวางแผนจัดการภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อองค์กรได้อย่างเหมาะสม

๒. การป้องกัน (Protect) เป็นส่วนที่มีความสำคัญมากที่สุด จากทั้ง ๕ หลักการ การป้องกันจะเริ่มตั้งแต่การวางกลไกและขั้นตอนเพื่อรักษาความปลอดภัย กระบวนการจัดการข้อมูล การควบคุมการเข้าถึง และใช้งานระบบ นอกจากนี้ ยังรวมถึงการฝึกอบรมและสร้างความตระหนักให้บุคลากรถึงเรื่องความสำคัญของความปลอดภัยไซเบอร์อีกด้วย

๓. การตรวจจับ (Detect) จุดสำคัญของส่วนนี้ คือ การเฝ้าระวังและติดตามเหตุการณ์หรือกิจกรรมน่าสงสัยที่อาจเป็นภัยคุกคามทางไซเบอร์ซึ่งกระทบต่อองค์กร รวมถึงการตรวจสอบหาช่องโหว่ของระบบ เพื่อที่จะได้พัฒนาระบบให้มีความต้านทานต่อภัยคุกคามทางไซเบอร์ได้มากยิ่งขึ้น

๔. การตอบสนอง (Respond) หลังจากตรวจพบความผิดปกติที่ส่งผลต่อความปลอดภัยเทคโนโลยีสารสนเทศแล้ว ทางองค์กรจำเป็นต้องมีการตอบสนองต่อเหตุการณ์ดังกล่าวอย่างเหมาะสม โดยการวางแนวทางปฏิบัติให้ชัดเจน มีการวิเคราะห์หาสาเหตุและสื่อสารกันระหว่างองค์กรในกรณีที่อาจต้องขอความช่วยเหลือจากหน่วยงานภายนอก เพื่อหาแนวทางการป้องกันและลดโอกาสเกิดปัญหาซ้ำได้ในอนาคต

๕. การกู้คืนระบบ (Recovery) เมื่อถูกโจมตีทางไซเบอร์ ทางองค์กรจำเป็นต้องทำให้ระบบกลับมาใช้งานได้เป็นปกติอย่างรวดเร็วที่สุด เพื่อให้ธุรกิจดำเนินต่อไปได้อย่างต่อเนื่อง และ

ลดความสูญเสียทั้งด้านการเงิน และด้านชื่อเสียงขององค์กร ดังนั้น จึงต้องมีการวางแผนการกู้คืนอย่างมีระบบ และมีการติดต่อสื่อสารที่ดีทั้งภายในและภายนอกองค์กร

การออกแบบแนวทางในการพัฒนาระบบข่าวกรองแบบเปิด

ในการศึกษาวิจัยครั้งนี้ ได้ออกแบบการพัฒนาระบบข่าวกรองแบบเปิด ของกองทัพบก ไว้ ๔ แนวทาง โดยมีรายละเอียดดังต่อไปนี้

แนวทางที่ ๑ ประยุกต์ใช้ Open source (Pure OSINT)

แนวทางที่ ๒ ประยุกต์ใช้ Open source ร่วมกับซื้อโปรแกรมแบบเสียค่าบริการประเภท Enterprise/ Premium

แนวทางที่ ๓ ประยุกต์ใช้ Open source (Pure OSINT) ร่วมกับการพัฒนาระบบฯ ขึ้นใช้เอง (In-House Development)

แนวทางที่ ๔ จัดหาซอฟต์แวร์เชิงพาณิชย์ (Commercial Software)

ตารางที่ ๔ – ๔ เปรียบเทียบข้อดีและข้อเสียของแต่ละแนวทางการพัฒนาฯ

แนวทาง	ข้อดี	ข้อเสีย
แนวทางที่ ๑ ประยุกต์ใช้ Open source (Pure OSINT)	• ไม่ต้องเสียค่าลิขสิทธิ์ • สามารถนำไปใช้ แก้ไข ดัดแปลง พัฒนา และจำหน่ายแจกจ่ายได้โดยเสรี • นิยมมาตรฐานเปิด (Open standard) • มีชุมชนให้ความช่วยเหลือมาก	• อาจถูกโจมตีจากรูรั่ว/ช่องโหว่ของซอฟต์แวร์ที่ผู้ออกแบบจงใจทิ้งไว้ (Backdoor) • ง่ายต่อการติดไวรัส/มัลแวร์ (Virus/Malware)
แนวทางที่ ๒ ประยุกต์ใช้ Open source ร่วมกับซื้อโปรแกรมแบบเสียค่าบริการประเภท Enterprise/ Premium	• ประหยัดงบประมาณในการลงทุนทางเทคโนโลยีได้บางส่วน • สามารถเลือกฟังก์ชันการทำงานได้หลากหลายตามประเภทที่เสียค่าบริการ	• ซอฟต์แวร์ลิขสิทธิ์มักจะมีข้อจำกัดในการปรับแต่ง • มีข้อกำหนดและเงื่อนไขในการใช้งานที่จำกัดทำให้ไม่สามารถแชร์หรือกระจายซอฟต์แวร์ได้อย่างอิสระ

ตารางที่ ๔ – ๔ เปรียบเทียบข้อดีและข้อเสียของแต่ละแนวทางการพัฒนาฯ (ต่อ)

แนวทาง	ข้อดี	ข้อเสีย
แนวทางที่ ๓ ประยุกต์ใช้ Open source (Pure OSINT) ร่วมกับพัฒนาเอง (In-House Development)	• เพิ่มเงื่อนไขและความต้องการต่าง ๆ ได้ไม่จำกัด • มีความยืดหยุ่นในการทำงานได้ดีกว่า หากเกิดการเปลี่ยนแปลงในการใช้งาน	• ใช้ระยะเวลาในการออกแบบและพัฒนานานเพื่อที่จะให้ได้คุณสมบัติตรงตามที่ต้องการ

	• ประหยัดค่าใช้จ่ายในการพัฒนาและบำรุงรักษาระบบ	• ทีมงานพัฒนาฯ อาจถูกกดดันอย่างมาก เพราะถูกคาดหวังว่าต้องได้คุณสมบัติตามความต้องการ • ไม่เหมาะกับหน่วยงานที่มีการโยกย้ายตำแหน่งบ่อยๆ
แนวทางที่ ๔ ซอฟต์แวร์เชิงพาณิชย์ (Commercial Software)	• โปรแกรมที่ได้มีคุณภาพดีกว่าเนื่องจากผู้ใช้จำนวนมากได้ทดสอบและแจ้งแก้ไขปัญหาของการใช้งานกับผู้ผลิตโปรแกรมมาเป็นอย่างดี • ความเสี่ยงในการใช้งานต่ำและผู้ใช้สามารถศึกษาคุณสมบัติของโปรแกรมได้โดยตรงจากคู่มือ	• ราคาสูง • ไม่มีความยืดหยุ่นและอาจไม่เหมาะสมกับงานที่จำเป็นต้องปรับเปลี่ยนหรือแก้ไขระบบอยู่บ่อย ๆ

ที่มา : จากผลการศึกษา บทที่ ๓ การพิจารณาแนวคิดที่มีความสอดคล้องกับการพัฒนาระบบข่าวกรองแบบเปิด

สรุป

ปัจจุบันยังไม่มีกรอบการพัฒนาระบบข่าวกรองแบบเปิด (OSINT development framework) เฉพาะที่รองรับงานทุกด้าน รวมถึงงานในมิติการปฏิบัติการไซเบอร์ ดังนั้น การพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก จึงจำเป็นต้องออกแบบและดำเนินการให้สอดคล้องตามพันธกิจ (Mission) ของกองทัพเป็นสำคัญ (Military OSINT) ทั้งในปฏิบัติการไซเบอร์เชิงรับและเชิงรุก เพื่อ ๑) ระบุจุดอ่อนที่เกี่ยวข้องกับบุคคล เทคโนโลยี และระบบ ๒) กำหนดขอบเขตของการปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์การป้องกันในทุกๆ ช่วงของการโจมตี ๓) สร้างประสบการณ์ขององค์กรเกี่ยวกับวิธีการตรวจจับและควบคุมการโจมตี และ ๔) พัฒนากิจกรรมเกี่ยวกับการตอบสนองและการแก้ไขการโจมตีเพื่อกลับสู่สภาวะการทำงานปกติ ซึ่งผู้วิจัยจึงได้เสนอแนะแนวทางในการพัฒนาระบบข่าวกรองแบบเปิดไว้ ๔ แนวทาง และได้นำกรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ หรือ NIST Cyber Security Framework มาประยุกต์ใช้กับกองทัพบก เพื่อช่วยให้องค์กรสามารถวางแผน ป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

ในการวิจัยครั้งนี้ เป็นการทำศึกษาวิจัย เรื่อง “แนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก” โดยผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยไว้ ๒ ข้อ คือ

วัตถุประสงค์การวิจัยข้อที่ ๑ เพื่อศึกษาและวิเคราะห์กระบวนการข่าวกรองแบบเปิด (Open-Source Intelligence: OSINT) ในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อนำไปสู่การปฏิบัติจริงทั้งในการแก้ปัญหาทางไซเบอร์ในระยะสั้น และระยะยาว

วัตถุประสงค์การวิจัยข้อที่ ๒ เพื่อจัดทำข้อเสนอแนะแนวทางการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก ว่าด้วยการข่าวกรองแบบเปิด

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ ๑ สรุปได้ดังนี้

จากผลการศึกษา นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยข่าวกรองแบบเปิด ของต่างประเทศ พบว่า

๑. ประเทศสหรัฐอเมริกา มีความเป็นรูปธรรมมากที่สุด ในฐานะเป็นต้นแบบของงาน OSINT ของทั่วโลก (Good Practice) แม้กระทั่งหน่วยข่าวกรองของอังกฤษ ฝรั่งเศส ออสเตรเลีย จีน ญี่ปุ่น และสิงคโปร์ ก็ใช้เป็นต้นแบบ โดยสหรัฐฯ มีหน่วยงานที่สำคัญ ได้แก่ สำนักข่าวกรองกลางสหรัฐ (CIA) โดยสหรัฐฯ มีโครงสร้างการจัดตั้งหน่วยงานด้านการข่าวกรองแบบเปิด ประกอบด้วย Assistant Deputy Director of National Intelligence for Open Source, National Open Source Committee และ Open Source Center

๒. ประเทศอังกฤษ มีกลไกข่าวกรองของสหราชอาณาจักร มีหน่วยงานด้านความมั่นคงและต่อต้านข่าวกรองภายในของสหราชอาณาจักร ประกอบด้วย เอ็มไอ ๕, หน่วยข่าวกรองลับ (Secret Intelligence Service: SIS), กองบัญชาการสื่อสารของรัฐบาล, สำนักข่าวกรองกลาโหม และคณะกรรมการข่าวกรองร่วม

๓. ประเทศรัสเซีย จัดตั้งหน่วยงาน National Center for Automated Date Exchange with Foreign Computer Networks and Data Banks (NCADE) โดยมีเครือข่ายเชื่อมโยงกับฐานข้อมูล ของสหรัฐฯ แคนาดา เยอรมนี อังกฤษ และฝรั่งเศส นอกจากนี้ หน่วยข่าวกรองต่างประเทศของรัสเซีย (Foreign Intelligence Service of the Russian Federation - SVR) ได้พัฒนาแพลตฟอร์มดิจิทัลสำหรับชาวรัสเซียที่อาศัยอยู่ในต่างประเทศแจ้งข้อมูลภัยคุกคามที่กระทบต่อความมั่นคงแห่งชาติอย่างปลอดภัยและนิรนามผ่านเครือข่ายอินเทอร์เน็ตใต้ดิน (TOR Network)

คล้ายกับโครงการ SecureDrop ซึ่งเป็นซอฟต์แวร์แบบ Open Source ที่สนับสนุนให้ NGO สามารถรับข้อมูลข่าวสารจากบุคคลนิรนามได้อย่างปลอดภัย

กรณีของประเทศไทย พบว่า ตามยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑-๒๕๘๐) และยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ยังไม่มีการกล่าวถึงกรอบการพัฒนาระบบการข่าวกรองแบบเปิด (OSINT development framework) รวมถึงการศึกษา วิจัย และพัฒนาด้านของการผลิตข่าวกรองจากแหล่งเปิด (OSINT) ซึ่งถือได้ว่ามีน้อยมาก เมื่อเปรียบเทียบกับองค์การข่าวกรองชั้นนำของโลก ซึ่งสาเหตุสำคัญเป็นผลเนื่องจากข้อจำกัดด้านความรู้ เพราะความรู้ด้านข่าวกรองมักจำกัดอยู่เฉพาะในหน่วยงานด้านการข่าวกรองของรัฐ ขณะที่สถาบันการศึกษาของประเทศไทยยังขาดองค์ความรู้ (Knowledge) และบุคลากร (People) ด้านนี้อย่างมากเช่นกัน

อย่างไรก็ตาม จากผลการวิเคราะห์กระบวนการข่าวกรองแบบเปิด พบว่า กระบวนการข่าวกรองแบบเปิด (OSINT Process) เป็นส่วนหนึ่งของวงรอบข่าวกรอง (Intelligence Cycle) และมีขั้นตอนที่คล้ายกัน ซึ่งอาจประสบปัญหา/อุปสรรคขึ้นได้ รายละเอียดดังนี้

ขั้นตอนที่ ๑ การวางแผนและกำหนดทิศทาง - ขาดบุคลากรที่มีความรู้และทักษะในการจัดสรรทรัพยากร สำหรับการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ อาจส่งผลให้ไม่สามารถระบุและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ

ขั้นตอนที่ ๒ การรวบรวม - ขาดความเชี่ยวชาญด้านเทคนิคในการรวบรวมและวิเคราะห์ข้อมูลอย่างมีประสิทธิภาพ ข้อมูลที่รวบรวมมีความไม่น่าเชื่อถือ จำเป็นต้องมีการตรวจสอบและยืนยันข้อมูล (Data Verification) เพื่อให้ได้ข้อมูลที่มีคุณภาพ (Data Quality) และน่าเชื่อถือ

ขั้นตอนที่ ๓ การประมวลผล - เทคนิคและเครื่องมือในการเก็บข้อมูลและวิเคราะห์อาจเผชิญกับข้อจำกัดทางเทคนิค เช่น ความสะดวกและความสามารถในการรวบรวมข้อมูลจากแหล่งที่ไม่เปิดเผย การประมวลผลข้อมูลที่มีปริมาณมาก เป็นต้น

ขั้นตอนที่ ๔ การวิเคราะห์และการผลิต - บุคลากรขาดความเชี่ยวชาญในการวิเคราะห์ข้อมูลที่รวบรวมและเปลี่ยนเป็นผลิตผลข่าวกรองที่นำไปปฏิบัติได้

ขั้นตอนที่ ๕ การเผยแพร่ - ไม่มีกลไกที่มีประสิทธิภาพในการเผยแพร่ผลิตภัณฑ์ข่าวกรองไปยังผู้มีอำนาจตัดสินใจในเวลาที่เหมาะสมและทันท่วงที

ดังนั้น การกำหนดแนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก จึงจำเป็นต้องออกแบบและดำเนินการให้สอดคล้องตามพันธกิจ (Mission) ของกองทัพเป็นสำคัญ (Military OSINT) ทั้งในปฏิบัติการไซเบอร์เชิงรับและเชิงรุก

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ ๒ สรุปได้ดังนี้

จากผลการศึกษา พบว่า ในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพบก ว่าด้วยการข่าวกรองแบบเปิด จำเป็นต้องพิจารณาตามแนวคิด ๓ เสาหลักของความมั่นคงปลอดภัยไซเบอร์เป็นสำคัญ และแนวคิดจากของผู้ทรงคุณวุฒิ ดังนั้น หากวิเคราะห์ปัญหาและอุปสรรคในการพัฒนาระบบ OSINT ของประเทศไทย สามารถแบ่งออกเป็น ๓ ประเด็นปัญหาใหญ่ ประกอบด้วย

๑. ด้านบุคลากร (People) - ขาดบุคลากรที่มีความเชี่ยวชาญในการวิเคราะห์ OSINT และมีประสบการณ์ด้านความปลอดภัยทางไซเบอร์ ซึ่งบุคลากรควรมีความรู้ในด้านต่าง ๆ เช่น ข่าวกรองภัยคุกคาม การวิเคราะห์เครือข่าย และการทำเหมืองข้อมูล อีกทั้ง ควรมีการฝึกอบรมและพัฒนาวิชาชีพเป็นประจำ

๒. ด้านกระบวนการ (Process) - ปัจจุบันประเทศไทย มีหน่วยงาน สำนักพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. จัดทำระบบศูนย์แลกเปลี่ยนข้อมูลกลาง (Government Data Exchange: GDX) ขึ้น เน้นการแลกเปลี่ยนข้อมูลให้บริการประชาชนเป็นหลัก แต่ยังขาดกระบวนการแลกเปลี่ยนข้อมูลภัยคุกคาม (Threats) รวมถึงภัยคุกคามทางไซเบอร์ (Cyber Threats) ระหว่างหน่วยงานรัฐกับรัฐ หรือในบริบทของหน่วยงานด้านความมั่นคง

๓. ด้านเทคโนโลยี (Technology) - เครื่องมือสำหรับการรวบรวมข้อมูล OSINT ในปัจจุบันมีให้สำหรับผู้ใช้ส่วนตัว ไม่ใช่โดเมนเฉพาะของรัฐบาลและหน่วยงานบังคับใช้กฎหมาย ดังนั้น ผู้วิจัยจึงได้ศึกษาและสรุปตัวอย่างเครื่องมือ OSINT ที่เป็นที่นิยมในปัจจุบันไว้แล้วตามบทที่ ๒ การทบทวนวรรณกรรม และงานวิจัยที่เกี่ยวข้อง

ข้อเสนอแนะ

การวิจัยครั้งนี้ ได้เสนอแนวทางการพัฒนาระบบข่าวกรองแบบเปิด เพื่อสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกองทัพบก รายละเอียดดังนี้

๑. ข้อเสนอแนะเชิงนโยบาย

การปรับปรุงกระบวนการและรูปแบบของนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยข่าวกรองแบบเปิด ควรนำกรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ หรือ National cyber security capacity maturity model:

CMM แห่ง University of Oxford มาประยุกต์ใช้ประเมินขีดความสามารถด้านไซเบอร์ในภาพรวมของประเทศไทย ตามบริบทของภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่งคง ซึ่งแบ่งออกเป็น ๕ มิติ โดยมีรายละเอียดดังนี้

ตารางที่ ๕ – ๑ การประเมินขีดความสามารถด้านไซเบอร์ (capacity maturity model: CMM)

ขีดความสามารถ	ผลการประเมิน
มิติที่ ๑ Cybersecurity Policy and Strategy	• มีการประกาศโครงสร้างหน่วยงานป้องกันภัยคุกคามทางไซเบอร์ระดับชาติ ภายใต้ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ • มีการกำหนดคณะกรรมการ และอำนาจหน้าที่รับผิดชอบอย่างชัดเจน • มีการประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน (บางส่วน)
มิติที่ ๒ Cyber Culture and Society	• คนไทยมีการรับรู้ถึงความเสี่ยงทางไซเบอร์ที่เพิ่มขึ้น เช่น การโจมตีไซเบอร์ การฉ้อโกงออนไลน์ การละเมิดความเป็นส่วนตัวออนไลน์ และการแพร่ระบาดของไวรัสและมัลแวร์ อีกทั้ง การใช้สื่อสังคมออนไลน์ในการแสดงความคิดเห็น การร่วมกิจกรรมกับกลุ่มหรือองค์กรที่มีความเชื่อเห็นเดียวกัน เป็นส่วนหนึ่งของการเสริมสร้างความเชื่อมั่นและการต่อต้านต่อเหตุการณ์หรือประเด็นที่เกี่ยวข้องกับสังคมหรือการเมืองในประเทศไทย

ตารางที่ ๕ – ๑ การประเมินขีดความสามารถด้านไซเบอร์ (capacity maturity model: CMM) (ต่อ)

ขีดความสามารถ	ผลการประเมิน
มิติที่ ๓ Cybersecurity Education, Training and Skills	• ประเทศไทยมีการพัฒนาหลักสูตรการศึกษาที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านไซเบอร์ในระดับทั้งสูงและต่ำ เช่น หลักสูตรปริญญาตรีและปริญญาโทในสาขาวิทยาการคอมพิวเตอร์ วิทยาการข้อมูล เป็นต้น ทั้งนี้ เพื่อสร้างการเรียนรู้และทักษะที่จำเป็นสำหรับความเข้าใจและการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านไซเบอร์
มิติที่ ๔ Legal and Regulatory Frameworks	• ประเทศไทยมีการบังคับใช้กฎหมายด้านไซเบอร์ ได้แก่ พ.ร.บ. คอมพิวเตอร์ฯ พ.ร.บ. การรักษาความ

	มั่นคงปลอดภัยไซเบอร์ฯ และ พ.ร.บ. คุ้มครองส่วนบุคคลฯ
มิติที่ ๕ Standards, Organizations and Technologies	• ประเทศไทยมีการใช้และรับรู้มาตรฐานด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับด้านไซเบอร์ เช่น ISO/IEC 27001 (Information Security Management System), NIST Cybersecurity Framework, และมาตรฐานการรักษาความลับของข้อมูลทางการแพทย์ (HIPAA) ที่เกี่ยวข้องกับสายงานทางการแพทย์ • ประเทศไทยมีหลายองค์กรที่มีบทบาทและความรับผิดชอบในด้านความมั่นคงปลอดภัยด้านไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เป็นต้น

ดังนั้น ตามบริบทของการพัฒนาขีดความสามารถด้านไซเบอร์ เพื่อพัฒนาระบบข่าวกรองแบบเปิด ถึงแม้ว่าจะไม่มี OSINT Capacity Maturity Model ที่เป็นมาตรฐานสากล แต่ในการวิจัยครั้งนี้ ผู้วิจัยได้จัดทำเกณฑ์การประเมินขีดความสามารถด้านไซเบอร์ สำหรับ OSINT แบ่งได้ ๕ ระดับ ดังแผนภาพที่ ๕ – ๑

แผนภาพที่ ๕ – ๑ เกณฑ์การประเมินขีดความสามารถด้านไซเบอร์

สำหรับโมเดลดังกล่าวเรียกว่า โมเดลความพร้อมของขีดความสามารถด้าน OSINT ทั้ง ๕ ระดับ ใช้วัดระดับวุฒิภาวะของหน่วนงาน สรุปอธิบายได้ดังนี้

๑. ขั้นเริ่มต้น (Initial)

๑.๑ มีการดำเนินการจำกัด หรือไม่มีการรับรู้ของ OSINT

๑.๒ ดำเนินการแบบเฉพาะกิจ ไม่มีการวางแผนการดำเนินการ และ OSINT ที่ไม่สอดคล้องกับการปฏิบัติ

๑.๓ ไม่ทุ่มเททรัพยากร หรือเครื่องมือสำหรับ OSINT

๑.๔ การบูรณาการเพียงเล็กน้อยหรือไม่มีเลยของ OSINT เข้าไปกระบวนการการตัดสินใจ

๒. ขั้นพื้นฐาน (Basic)

๒.๑ การรับรู้และการใช้ OSINT ที่จำกัด

๒.๒ มีการปฏิบัติ OSINT แบบเฉพาะกิจบางอย่าง

๒.๓ มีการใช้เครื่องมือและทรัพยากร OSINT พื้นฐาน

๒.๔ OSINT ถูกรวมเข้ากับกระบวนการตัดสินใจเป็นครั้งคราว

๓. ขั้นพัฒนา (Developing)

๓.๑ เพิ่มการรับรู้และการรับรู้ถึงคุณค่าของ OSINT

๓.๒ แนวทางปฏิบัติและกระบวนการ OSINT ที่เป็นทางการมากขึ้น

๓.๓ ทรัพยากรเฉพาะสำหรับ OSINT

๓.๔ มีการใช้เครื่องมือและเทคโนโลยี OSINT อย่างแข็งขัน

๓.๕ OSINT ถูกรวมเข้าไว้ในพื้นที่เฉพาะของกระบวนการตัดสินใจ

๔. ขั้นสูง (Advanced)

๔.๑ กลยุทธ์และแนวทางปฏิบัติของ OSINT ที่ครอบคลุม

๔.๒ สร้างกระบวนการและผังการปฏิบัติงาน (work flow) สำหรับการรวบรวม วิเคราะห์ และเผยแพร่ OSINT

๔.๓ ทีม OSINT เฉพาะทางหรือบทบาทภายในองค์กร

๔.๔ เครื่องมือ เทคโนโลยี และแพลตฟอร์ม OSINT ขั้นสูง

๔.๕ OSINT ถูกรวมเข้ากับกระบวนการตัดสินใจในหลายด้าน

๕. ขั้นสมบูรณ์ (Mature)

๕.๑ OSINT ผสานเข้ากับวัฒนธรรม กระบวนการ และผังการปฏิบัติงาน (work flow) ขององค์กรอย่างสมบูรณ์

๕.๒ กลยุทธ์ OSINT ที่แข็งแกร่งและการกำกับดูแลในสถานที่ที่ดำเนินการ

๕.๓ การปรับปรุงอย่างต่อเนื่องและนวัตกรรมในแนวปฏิบัติของ OSINT

๕.๔ เครื่องมือ OSINT ขั้นสูง เทคโนโลยี และแพลตฟอร์มที่ใช้งาน

๕.๕ OSINT ขับเคลื่อนกระบวนการตัดสินใจทั่วทั้งองค์กร

ดังนั้น ข้อเสนอแนะเชิงนโยบาย เมื่อเปรียบเทียบกับโมเดลดังกล่าว อธิบายได้ดังนี้

๑.๑ แผนการพัฒนาขีดความสามารถด้านไซเบอร์ สำหรับ OSINT ระยะสั้น

หมายถึง แผนการพัฒนา ปีที่ ๑-๒ โดยเกณฑ์การประเมินขีดความสามารถด้านไซเบอร์ ควรอยู่ที่ระดับที่ ๑ เริ่มต้น (Initial) หรือ ระดับที่ ๒ พื้นฐาน (Basic) ซึ่งมีความหมายโดยภาพรวมว่า องค์กรเริ่มมีการตระหนักรู้ถึงการใช้งาน OSINT เริ่มมีการประยุกต์ใช้ OSINT ในการปฏิบัติงานของบางหน่วยงานขององค์กร มีเครื่องมือพื้นฐาน และมีการนำ OSINT ไปบูรณาการในกระบวนการตัดสินใจขององค์กร

๑.๒ แผนการพัฒนาขีดความสามารถด้านไซเบอร์ สำหรับ OSINT ระยะยาว

หมายถึง แผนการพัฒนา ปีที่ ๓-๕ โดยเกณฑ์การประเมินขีดความสามารถด้านไซเบอร์ ควรอยู่ที่ระดับที่ ๓ กำลังพัฒนา (Developing) หรือระดับที่ ๔ ขั้นสูง (Advance) หรือระดับที่ ๕ สมบูรณ์ (Mature) ขึ้นอยู่กับความพร้อมของแต่ละองค์กร ซึ่งมีความหมายโดยภาพรวมว่า มีการเพิ่มขึ้นของการตระหนักรู้และเห็นคุณค่าของ OSINT อย่างต่อเนื่อง มีการประกาศใช้กระบวนการข่าวกรองแบบเปิด (OSINT Process) ทั้ง ๕ ขั้นตอน อย่างชัดเจน มีการกำหนดโครงสร้างทีมงานปฏิบัติการ (Specialist Team) หน้าที่และความรับผิดชอบ (Role and responsibility) อย่างชัดเจน รวมถึงการประยุกต์ใช้เครื่องมือขั้นสูง เทคโนโลยี หรือแพลตฟอร์มเฉพาะด้าน และมีการนำ OSINT ไปบูรณาการในกระบวนการตัดสินใจในหลายหน่วย หรือทั่วทั้งองค์กร

๒. ข้อเสนอแนะเชิงปฏิบัติ

๒.๑ การออกแบบแนวทางในการพัฒนาระบบข่าวกรองแบบเปิด

ในการศึกษาวิจัยครั้งนี้ ได้ออกแบบการพัฒนาระบบข่าวกรองแบบเปิด ของกองทัพบก ไว้ ๔ แนวทาง ซึ่งประเด็นความท้าทายในการเลือกแนวทางของ ทบ. เพื่อนำไปประยุกต์ใช้จริงนั้น จำเป็นต้องมีการวิเคราะห์สภาพแวดล้อมขององค์กรร่วมด้วย กล่าวคือ

แนวทางที่ ๑ ประยุกต์ใช้ Open source (Pure OSINT) - สำหรับการใช้เครื่องมือ โดยวิธีนี้มีจุดอ่อนโดยอาจถูกโจมตีจากรูรั่ว/ช่องโหว่ของซอฟต์แวร์ที่ผู้ออกแบบจงใจทิ้งไว้ (Backdoor) จึงง่ายต่อการติดไวรัส/มัลแวร์ (Virus/Malware)

แนวทางที่ ๒ ประยุกต์ใช้ Open source ร่วมกับซื้อโปรแกรมแบบเสียค่าบริการประเภท Enterprise/ Premium - สำหรับการใช้เครื่องมือ โดยวิธีนี้สามารถเลือกฟังก์ชันการทำงานได้หลากหลายตามประเภทที่เสียค่าบริการ (Enterprise/ Premium)

แนวทางที่ ๓ ประยุกต์ใช้ Open source (Pure OSINT) ร่วมกับการพัฒนาระบบฯ ขึ้นใช้เอง (In-House Development) - สำหรับการใช้เครื่องมือ โดยวิธีนี้ใช้ระยะเวลาในการออกแบบและพัฒนานาน เพื่อที่จะให้ได้คุณสมบัติตรงตามที่ต้องการ และทีมงานพัฒนาฯ อาจถูกกดดันอย่างมาก เนื่องจากถูกคาดหวังว่าต้องได้คุณสมบัติตามความต้องการ จึงไม่เหมาะกับหน่วยงานที่มีการโยกย้ายตำแหน่งบ่อยๆ

แนวทางที่ ๔ จัดหาซอฟต์แวร์เชิงพาณิชย์ (Commercial Software) - สำหรับการใช้เครื่องมือ โดยวิธีนี้องค์กรจะได้โปรแกรมที่มีคุณภาพ เนื่องจากผู้ใช้จำนวนมากได้ทดสอบและแจ้งแก้ไขปัญหาของการใช้งานกับผู้ผลิตโปรแกรมมาเป็นอย่างดี แต่ต้องแลกกับงบประมาณค่อนข้าง

สูง อีกทั้ง ไม่มีความยืดหยุ่นและอาจไม่เหมาะสมกับงานที่จำเป็นต้องปรับเปลี่ยนหรือแก้ไขระบบอยู่บ่อย ๆ

ดังนั้น การออกแบบแนวทางในการพัฒนาระบบข่าวกรองแบบเปิด เป็นกระบวนการที่ต้องคำนึงถึงหลายปัจจัย กล่าวคือ ต้องออกแบบและดำเนินการให้สอดคล้องตามพันธกิจ (Mission) ของกองทัพเป็นสำคัญ ทั้งในปฏิบัติการไซเบอร์เชิงรับและเชิงรุก และดำเนินการภายใต้กรอบแนวคิด NIST Cybersecurity Framework โดยแยกหัวข้อเป็นการระบุ (Identify) การตรวจจับ (Detect) การป้องกัน (Protect) การตอบสนอง (Respond) และการคืนสภาพ (Recover)

๒.๒ การรักษาความปลอดภัยในการปฏิบัติการ (Operational Security)

การรักษาความปลอดภัยในการปฏิบัติการ (OPSEC) ถูกกล่าวไว้อย่างกว้างขวางในการปฏิบัติการทางทหารหลากหลายรูปแบบ เช่น การสงครามด้านบัญชาการและควบคุม (Command and Control Warfare: C2W) การปฏิบัติการข่าวสาร (Information Operations: IO) และได้รับผลกระทบต่อมาตรการรักษาความปลอดภัยอื่น ๆ ได้แก่ มาตรการรักษาความปลอดภัยด้านการติดต่อสื่อสาร (Communication Security: COMSEC) มาตรการต่อต้านข่าวกรอง (Counter-Intelligence) มาตรการรักษาความปลอดภัยข้อมูลข่าวสาร (Information Security: INFOSEC) การรักษาความปลอดภัยสัญญาณ (Signal Security: SIGSEC), การรักษาความปลอดภัยการรับ-ส่งสัญญาณ (Transmission Security: TRANSEC)

ตาม Joint Publication ๓-๑๓.๓, Operations Security ๒๐๐๖ กำหนดให้ OPSEC เป็นกระบวนการในการระบุข้อมูลข่าวสารวิกฤติใดที่ฝ่ายเราสามารถล่วงรู้มาจากฝ่ายข้าศึกหรือฝ่ายตรงข้าม แล้วนำมาตีความให้เกิดประโยชน์ต่อฝ่ายเรา ตลอดจนนำไปสู่การเลือกใช้มาตรการที่เหมาะสมในการปฏิบัติจนสามารถกำจัด หรือลดทอนขีดความสามารถของข้าศึกในการค้นหาข้อมูลข่าวสารวิกฤตของฝ่ายเรา โดยความสัมพันธ์ระหว่าง OPSEC และ OSINT สามารถอธิบายได้ว่า OSINT เป็นภาพสะท้อนของการรักษาความปลอดภัยในการปฏิบัติงาน (OPSEC) ในหลาย ๆ ด้าน เช่น การเตรียมข้อมูลในสภาวะแวดล้อมการปฏิบัติการ (JIPOE) เป็นวิธีการที่เป็นประโยชน์สำหรับผู้วางแผนรักษาความปลอดภัยในการปฏิบัติการ ผู้เชี่ยวชาญฝ่ายการข่าวดำเนินการวิเคราะห์ภารกิจของการปฏิบัติการฝ่ายเรา ซึ่งจะให้มุมมองที่ดีในพื้นที่แนวโน้มที่ฝ่ายข้าศึกสามารถเก็บรวบรวมข้อมูลและระบุส่วนประกอบข้อมูลที่สำคัญของฝ่ายเรา (EEFI) ทำให้มั่นใจว่าผู้วางแผนการรักษาความปลอดภัยในการปฏิบัติการสามารถกำหนดข้อมูลวิกฤตที่ไม่มีชั้นความลับและเกี่ยวข้องกับการรักษาความปลอดภัยในการปฏิบัติการเข้าไว้ในบัญชีข้อมูลวิกฤตได้ทั้งหมด

๒.๓ การตระหนักถึงความเป็นส่วนตัวและจริยธรรมไซเบอร์ (Awareness of Privacy and Ethical)

ปัจจุบันภาครัฐให้ความสำคัญกับความเสี่ยงทางด้านความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นอุปสรรคที่เกิดจากการโจมตีทางไซเบอร์จากภายนอก หรือการรั่วไหลของข้อมูลส่วนบุคคลและข้อมูลภายในหน่วยงานรัฐ ความเสี่ยงดังกล่าวสามารถส่งผลกระทบต่อการดำเนินงานและความปลอดภัยทางข้อมูลส่วนบุคคลของผู้ที่มีส่วนเกี่ยวข้องทั้งภายใน และภายนอกหน่วยงาน

ดังนั้น ในการพัฒนาระบบข่าวกรองแบบเปิด จำเป็นต้องมีกระบวนการการกำกับดูแลที่เข้มงวด และปฏิบัติตามแนวนโยบายและกฎหมายที่เกี่ยวข้อง รวมถึงการสร้างความตระหนักรู้และเตรียมความพร้อมด้านความปลอดภัยไซเบอร์ให้กำลังพล ทบ. อย่างต่อเนื่อง โดยการจัดการอบรมเกี่ยวกับความเสี่ยงจากการโจมตีทางไซเบอร์ การรั่วไหลของข้อมูลสารสนเทศ และความรู้ด้าน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล สรุปได้ว่า การปฏิบัติตามจริยธรรมไซเบอร์ (Cyber Ethics) เป็นเรื่องสำคัญในการใช้และดำเนินการกับข้อมูล OSINT เพื่อให้มีการใช้ข้อมูลอย่างเหมาะสมและถูกต้อง ควรมีการกำหนดแนวทางที่ชัดเจนต่อไป

๓. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

งานด้านความมั่นคงและการป้องกันประเทศ เป็นงานสำคัญที่ต้องใช้ข้อมูลข่าวกรองและข้อมูลเชิงลึก มาใช้ในการวางแผน วิเคราะห์ และตัดสินใจ ดังนั้น การประยุกต์ใช้ OSINT กับมิติด้านการทหารในการทำวิจัยครั้งต่อไป มีข้อเสนอแนะดังนี้

๓.๑ การประยุกต์ใช้ OSINT เพื่อวิเคราะห์ขีดความสามารถของฝ่ายตรงข้าม OSINT ช่วยในการเก็บข้อมูลและวิเคราะห์เกี่ยวกับศักยภาพและกลยุทธ์ของฝ่ายตรงข้าม เช่น ประเภทของอาวุธยุทโธปกรณ์ จำนวนกำลังพล และยุทธศาสตร์การรบ รวมถึง การติดตามกิจกรรมของกลุ่มก่อการร้ายหรือทหารประจำชาติอื่น ๆ ที่อาจมีผลกระทบต่อกองทัพ

๓.๒ การประยุกต์ใช้ OSINT เพื่อติดตามข่าวสารของกองทัพ OSINT ช่วยให้กองทัพเข้าใจสภาพความเสี่ยงและสถานการณ์ในปัจจุบัน ด้วยการติดตามข้อมูลที่มาจากแหล่งข่าวสารต่าง ๆ เช่น เว็บไซต์ทางการของกองทัพ เว็บไซต์ข่าว เว็บไซต์โซเชียลมีเดีย เว็บไซต์ข่าวกรอง เป็นต้น

๓.๓ การประยุกต์ใช้ OSINT เพื่อวิเคราะห์ศักยภาพเชิงภูมิศาสตร์ OSINT เป็นเครื่องมือที่มีประสิทธิภาพในการวิเคราะห์ข้อมูลเชิงภูมิศาสตร์ เช่น การวิเคราะห์ทางภูมิศาสตร์ เพื่อเข้าใจเกี่ยวกับทัศนคติทางสังคมและทางทัศนคติของประชากรในพื้นที่ที่เกี่ยวข้อง ข้อมูล OSINT ช่วยในการวางแผนกลยุทธ์ในการเผชิญหน้ากับปัญหาภูมิศาสตร์และสภาพแวดล้อม

๓.๔ การประยุกต์ใช้ OSINT เพื่อวิเคราะห์เศรษฐกิจ OSINT ช่วยในการเก็บข้อมูลและวิเคราะห์ทางเศรษฐกิจที่สำคัญต่อกองทัพ เช่น ข้อมูลทางการเงิน อุตสาหกรรม การค้า เป็นต้น ช่วยในการวางแผนกลยุทธ์ทางกองทัพที่เกี่ยวข้องกับทัศนคติเศรษฐกิจและการใช้ทรัพยากรของประเทศ และต่างประเทศ

๓.๕ การประยุกต์ใช้ OSINT เพื่อแบ่งปันข้อมูลและสร้างความร่วมมือ OSINT เป็นเครื่องมือที่ช่วยในการแบ่งปันข้อมูลและความร่วมมือกับหน่วยงานทางกองทัพ และพันธมิตรในระดับชาติ และระหว่างประเทศ การแบ่งปันข้อมูลเชิงกลยุทธ์ช่วยเสริมสร้างความเข้มแข็งในการป้องกันและต่อสู้กับภัยคุกคามทางด้านกองทัพ

บรรณานุกรม

ภาษาไทย

กองบัญชาการทหารสูงสุด. “หลักนิยมการปฏิบัติการร่วมกองทัพไทย พ.ศ. ๒๕๕๐ ด้านข่าวกรองร่วม”. กรุงเทพฯ : กองบัญชาการทหารสูงสุด, ๒๕๕๐.

เจตน์พงศ์ โชคสวัสดิ์วรกุล. “วงรอบข่าวกรอง : ๔ หรือ ๕ ขั้นตอนดี”. หน้า ๓๒-๓๔, ๒๕๕๓.

เจษฎา มีบุญลือ. “เอกสารทางวิชาการ เรื่อง ความมั่นคงแห่งชาติ : การสร้างชาติไทยให้ยั่งยืน”. กรุงเทพฯ : ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. หน้า ๑-๕๔, ๒๕๕๓.

ฉัตรพงศ์ ฉัตราคม. “การผลิตข่าวกรองจากแหล่งข่าวเปิด”. จุลสารความมั่นคงศึกษา. พิมพ์ครั้งที่ ๑. กรุงเทพฯ: บริษัท สแควร์ ปริ๊นซ์ ๙๓ จำกัด, ๒๕๕๓.

ปัณฑ์ชนิต สมุทรสาคร. “บทบาทงานข่าวกรองกับการแก้ไขปัญหายาเสพติด”. National Defence Studies Institute Journal, ๑๐(๒), หน้า ๒๖-๔๐, ๒๕๖๒.

“พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. ๒๕๖๒”, ราชกิจจานุเบกษา. เล่ม ๑๓๖ ตอนที่ ๕๐, ๑๖ เมษายน ๒๕๖๒.

“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒”, ราชกิจจานุเบกษา. เล่ม ๑๓๖ ตอนที่ ๖๙, ๒๗ พฤษภาคม ๒๕๖๒.

วัชรภูมิ์ ไวว่อง. “การศึกษาการสืบค้นและวิเคราะห์ข้อมูลข่าวกรองแบบเปิดผ่านอินเตอร์เน็ต”. วิศวสารลาดกระบัง, ปีที่ ๓๔, ฉบับที่ ๔, ๒๕๖๐.

ภาษาต่างประเทศ

Best, Richard A., and Alfred Cumming. “Open Source Intelligence (OSINT): Foreign Affairs, Defense, and Trade Division.” 2007.

Evangelista, J.R.G., et al. “Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence”, Journal of Applied Security Research, vol. 16, no. 3, 2020, pp. 345-369.

Glassman, M., & Kang, M. J. “Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)”, Computers in Human Behavior, vol. 28, no. 2, 2012, pp. 673-682.

“Google Web Server”. (Online). Available: https://www.yeahhub.com/shodan-search-examples, 2023.

Hribar, G., Podbregar, I., & Ivanuša, T. “OSINT: A 'Grey Zone'?”, International Journal of Intelligence and CounterIntelligence, vol. 27, no. 3, 2014, pp. 529-549.

Hwang, Yong-Woon, et al. “Current Status and Security Trend of OSINT”, Wireless Communications and Mobile Computing, vol. 2022, 2022, pp. 1-14.

“Network Footprint”. (Online). Available: https://www.maltego.com, 2023.

“OSINT Framework”. (Online). Available: https://osintframework.com, 2023.

“OSINT Landscape”. (Online). Available: https://blog.sociallinks.io/osint-landscape, 2023.

Revell, Q., Smith, T., & Stacey, R. “Tools for OSINT-Based Investigations”, Advanced Sciences and Technologies for Security Applications, 2016, pp. 153-165.

U. S. Joint U.S. Joint Force Command, “Joint Intelligence: Joint Publication 2-0”, CreateSpace Independent Publishing Platform, 2014.

Yamin, Muhammad M., et al. “Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security”, Mathematics, vol. 10, 2022, p. 2054.

ภาคผนวก

ผนวก ก
ประเด็นคำถามสัมภาษณ์ผู้ทรงคุณวุฒิ

๑. ท่านคิดว่า ข่าวกรองแบบเปิด (Open-source intelligence หรือ OSINT) มีบทบาทสำคัญอย่างไรต่อองค์กรหรือหน่วยงานของท่าน ทั้งในด้านเชิงรับและเชิงรุก

๒. ท่านคิดว่า ข่าวกรองแบบเปิด (Open-source intelligence หรือ OSINT) มีส่วนสนับสนุนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างไรบ้าง

๓. ปัจจุบันวงรอบข่าวกรอง (Intelligence Cycle) ในหน่วยงานของท่านมีการปฏิบัติหรือไม่ หากมีการดำเนินการอยากทราบว่าขั้นตอนใดของวงรอบดังกล่าว เป็นปัญหา/อุปสรรค ต่อภารกิจด้านไซเบอร์ หรือภารกิจในหน่วยของท่านที่รับผิดชอบ และในมุมมองของท่านมีความคิดเห็นอย่างไร

๔. ปัจจุบันท่านทราบหรือไม่ว่า มีหน่วยงานใดบ้างที่มีกระบวนการแลกเปลี่ยนข้อมูลข่าวกรองแบบเปิด (OSINT) ระหว่างหน่วยงาน เพื่อใช้ประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์

๕. ข้อเสนอแนะในการพัฒนาแนวทางการพัฒนาระบบข่าวกรองแบบเปิด ของหน่วยงานด้านความมั่นคง (อาทิ ด้านบุคคลากร ด้านกระบวนการ และด้านเทคโนโลยี) ตามที่ท่านเข้าใจ

คำจำกัดความ

ข่าวกรองแบบเปิด กล่าวคือ เป็นส่วนหนึ่งในวิธีการสืบสวน สอบสวน ด้วยการรวบรวมและวิเคราะห์ข้อมูลที่รวบรวมจากแหล่งสาธารณะ หรือแหล่งเปิดบนอินเตอร์เน็ต และโซเชียลมีเดีย ส่วนใหญ่ให้บริการฟรีและมีประสิทธิภาพมาก ดังนั้น OSINT จึงถูกนำมาใช้ในขั้นตอนการสำรวจ เพื่อวางแผนการโจมตีทางไซเบอร์ เช่น การโจมตีแบบฟิชชิง (Phishing) วิศวกรรมสังคม (Social Engineering) เป็นต้น

ประวัติย่อผู้วิจัย

ชื่อ	พลตรี นิพัฒน์ เล็กฉลาด
วัน เดือน ปีเกิด	๑๔ พฤษภาคม พ.ศ. ๒๕๑๐
การศึกษา	ทางทหารหลักสูตร: - หลักสูตรหลักประจำ รร.สธ.ทบ. ชุดที่ ๗๘ (พ.ศ. ๒๕๔๓) - โรงเรียนนายร้อยพระจุลจอมเกล้า รุ่นที่ ๓๗ (พ.ศ.๒๕๓๓) - โรงเรียนเตรียมทหาร รุ่นที่ ๒๖ (พ.ศ.๒๕๒๘) ทางพลเรือนคุณวุฒิ: - ปริญญาโท วิทยาศาสตรมหาบัณฑิต สาขา วิทยาการคอมพิวเตอร์ (จุฬาลงกรณ์มหาวิทยาลัย พ.ศ. ๒๕๔๑) - ปริญญาตรี วิทยาศาสตรบัณฑิต สาขา วิศวกรรมไฟฟ้า (โรงเรียนนายร้อยพระจุลจอมเกล้า พ.ศ. ๒๕๓๓, รุ่นที่ ๓๗)
ประวัติการทำงานโดยย่อ	ในประเทศ - ประจำแผนก แผนกงบประมาณ กปช.สส. (พ.ศ.๒๕๔๓) - หน.แผนกซ่อมเครื่องอิเล็กทรอนิกส์ กซสอ.สส. (พ.ศ. ๒๕๔๖) - หน.ผสสท.กสสท.ศทท. (พ.ศ. ๒๕๔๙) - หน.ผวอ.กพร.ศทท. (พ.ศ. ๒๕๕๕) - ผอ.กอง กรช.ศชบ.ทบ. (พ.ศ. ๒๕๕๙) - รอง ผอ.ศชบ.ทบ. (พ.ศ. ๒๕๖๒) ราชการสนามต่างประเทศ - กกล.๙๗๒ ไทย/ติมอร์ตะวันออกผลัดที่ ๔ (ตั้งแต่ ๔ ก.ค. ๒๕๔๔ - ๓๑ ม.ค. ๒๕๔๕)
ตำแหน่งปัจจุบัน	ผู้อำนวยศูนย์ไซเบอร์กองทัพบก (พ.ศ. ๒๕๖๔)