# รายงานการศึกษาส่วนบุคคล
# (Individual Study)

# เรื่อง การบูรณาการเครือข่ายประชาคมข่าวกรองทางไซเบอร์


## จัดทำโดย นายรัชภูมิ เวียงสิมา
## รหัส 9805



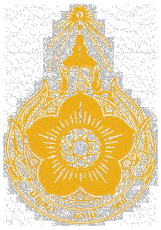
รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 98
วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.
ประจำปี 2566

# รายงานการศึกษาส่วนบุคคล
# (Individual Study)

**เรื่อง การบูรณาการเครือข่ายประชาคมข่าวกรองทางไซเบอร์**

**จัดทำโดย นายรัชภูมิ เวียงสิมา**
**รหัส 9805**

**หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 98**
**วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.**
**ประจำปี 2566**
**รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา**



**สำนักงาน ก.พ.**

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรม หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม ของสำนักงาน ก.พ.

ลงชื่อ.....

(นายวีระชัย นาควิบูลย์วงศ์)

อาจารย์ที่ปรึกษา

ลงชื่อ.....

(นางสาวบรรจงจิตต์ อังศุสิงห์)

อาจารย์ที่ปรึกษา

ลงชื่อ.....

(นายอารักษ์ พรหมณี)

อาจารย์ที่ปรึกษา

# บทสรุปสำหรับผู้บริหาร

ภัยคุกคามรูปแบบใหม่ ที่ไม่ใช่มิติการสู้รบหรือรุกรานด้วยกำลังทางการทหารเช่นเดิม แต่เป็นภัยคุกคามในยุคความก้าวหน้าทางเทคโนโลยี ที่มีลักษณะสำคัญ คือ “เป็นภัยที่มีความคลุมเครือ เชื่อมโยงหลายประเด็นหลายมิติ ไม่จำกัดพื้นที่ และสร้างความเสียหายรุนแรงเป็นวงกว้าง” ในการศึกษาครั้งนี้จะกล่าวถึงประเด็นภัยคุกคามทางไซเบอร์ ซึ่งหน่วยงานด้านการข่าวและความมั่นคง ต่างเร่งกำหนดยุทธศาสตร์และปรับกระบวนการทำงาน ให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ดังกล่าวให้ได้อย่างมีประสิทธิภาพ โดยผลการศึกษาพบว่า แนวทางสำคัญประการหนึ่งที่จะช่วยการทำงานของหน่วยงานด้านการข่าว คือ การจัดตั้งการบูรณาการเครือข่ายประชาคมข่าวกรองทางไซเบอร์ ซึ่งเป็นการดำเนินการเพื่อพัฒนาระบบงานข่าวกรองแบบบูรณาการ ของหน่วยงานด้านการข่าวและประชาคมข่าวกรอง ให้ทำงานได้อย่างมีประสิทธิภาพเพิ่มขึ้น สามารถบริหารจัดการและพัฒนาสร้างกลไกให้เกิดการบูรณาการงานข่าวกรองทางไซเบอร์ ได้เท่าทันต่อการรับมือกับความท้าทายภายใต้สภาวะแวดล้อมความมั่นคงในบริบทใหม่ โดยเฉพาะต่อปัญหาภัยคุกคามทางไซเบอร์ การบูรณาการเครือข่ายประชาคมข่าวกรองทางไซเบอร์ ยังเป็นการดำเนินงานตามภารกิจข่าวกรองที่สอดรับและระบุอยู่ในยุทธศาสตร์ชาติ(พ.ศ. 2561 - 2580) ด้านความมั่นคง แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. 2566 - 2580) ประเด็นด้านความมั่นคง แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ. 2566 - 2570) และนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ(พ.ศ.2566 - 2570) เพื่อให้ประเทศมีความมั่นคง ประชาชนมีความสุข

อย่างไรก็ตาม การขับเคลื่อนการบูรณาการในภารกิจป้องกันภัยคุกคามทางไซเบอร์ ของหน่วยงานความมั่นคงที่ผ่านมา ได้พบปัญหาและอุปสรรคที่ทำให้การทำงานไม่มีประสิทธิภาพ สรุปได้คือ 1) องค์กรต่าง ๆ ขาดความเชื่อมั่นในการแบ่งปันข้อมูลระหว่างกัน 2) หน่วยงานในเครือข่ายมีวัฒนธรรมการทำงานและกฎระเบียบที่แตกต่างกัน 3) ข้อจำกัดด้านทรัพยากรของแต่ละหน่วยงาน 4) การขาดมาตรฐานกลางรวมทั้งช่องทางในการแบ่งปันข้อมูล และ 5) การกำหนดตัวชี้วัดเพื่อสะท้อนให้เห็นผลสัมฤทธิ์ของการแบ่งปันข้อมูลระหว่างองค์กร ไม่สามารถดำเนินการให้เป็นไปตามวัตถุประสงค์ได้

จากสภาพปัญหาดังกล่าว ผู้ศึกษาจึงเสนอแนวทางการขับเคลื่อนเพื่อแก้ไขหรือพัฒนา ประกอบด้วย 1) จัดตั้งหน่วยงานเป็นเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ ตามแผน 5 ปี 2) กำหนดช่องทางการสื่อสาร หรือพัฒนาเชื่อมโยงแพลตฟอร์มแลกเปลี่ยนข้อมูลข่าวกรองทางไซเบอร์ และ 3) การพัฒนากลยุทธ์การสร้างสัมพันธ์ระหว่างหน่วยงานที่บูรณาการทั้งระดับนโนบาย และระดับปฏิบัติ ซึ่งหากดำเนินการสำเร็จจะช่วยยกระดับศักยภาพในภารกิจการป้องกันภัยคุกคามทางไซเบอร์ ให้มีประสิทธิภาพสูงขึ้น สามารถสร้างกลไกการบูรณาการอย่างเป็นระบบ สามารถนำข้อมูลข่าวสารและข่าวกรองที่สำคัญไปใช้สืบสวนขยายผล ระงับยับยั้งหรือลดระดับความเสียหายที่อาจเกิดขึ้น รวมทั้งการประเมินสถานการณ์ได้ถูกต้อง แม่นยำ และทันเวลา เพื่อปกป้องผลประโยชน์ความมั่นคงของชาติ และประชาชน อย่างมีประสิทธิภาพต่อไป

# กิตติกรรมประกาศ

การจัดทำรายงานการศึกษาส่วนบุคคล เรื่อง “การบูรณาการเครือข่ายประชาคมข่าวกรองทางไซเบอร์" เป็นส่วนหนึ่งของการฝึกอบรมหลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม (นบส.1) รุ่นที่ 98 สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ. ประจำปี 2566 ได้สำเร็จลุล่วงเรียบร้อยไปได้ด้วยดี โดยได้รับความร่วมมือและสนับสนุนข้อมูลอันเป็นประโยชน์ จากบุคคลและหน่วยงานที่เกี่ยวข้องอย่างดียิ่ง

ขอขอบพระคุณ นายธนากร บัวรัษฎ์ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ที่กรุณามอบโอกาสให้ผู้ศึกษาได้เข้าร่วมการอบรมในครั้งนี้ ถือได้ว่าเป็นประสบการณ์สำคัญของผู้ที่จะก้าวไปสู่นักบริหารที่ควรเข้ารับการศึกษาและเสริมสร้างความรู้เป็นอย่างยิ่ง

ขอขอบพระคุณ ท่านอาจารย์วีระชัย นาควิบูลย์วงศ์ อาจารย์ที่ปรึกษากลุ่มที่ 5 / อดีตเลขาธิการ ส.ป.ก. ที่เต็มเปี่ยมด้วยความเมตตาในการดูแลชี้แนะแนวทางสำคัญต่างๆ อย่างใกล้ชิด ตลอดกระบวนการจัดทำรายงานตั้งแต่ต้นจนกระทั่งแล้วเสร็จ ท่านอาจารย์บรรจงจิตต์ อังศุสิงห์ และท่านอาจารย์อารักษ์ พรหมณี ที่กรุณาให้คำแนะนำข้อคิดเห็นที่สำคัญเพิ่มเติม ในการรายงานความก้าวหน้า ซึ่งช่วยให้รายงานการศึกษาส่วนบุคคลนี้สมบูรณ์ยิ่งขึ้น และขอขอบพระคุณนายอริยะ สกุลแก้ว ผู้อำนวยการวิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ. ตลอดจนทีมงานทุกท่านที่กรุณาอำนวยความสะดวก และให้คำแนะนำอย่างดียิ่งตลอดหลักสูตร รวมทั้งผู้เข้าร่วมอบรมหลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม (นบส.1) รุ่นที่ 98 ทุกท่าน ที่ได้ร่วมแลกเปลี่ยนเรียนรู้ ช่วยเหลือแนะนำ และร่วมการทำกิจกรรมต่างๆ ทำให้การฝึกอบรมครั้งนี้ มีความสมบูรณ์แบบทั้งเนื้อหา คุณภาพการเป็นผู้นำ และการมีเครือข่ายในกลุ่มผู้บริหารจากหน่วยงานต่างๆ อันจะเป็นประโยชน์ต่อการปฏิบัติราชการให้แก่ประเทศชาติและประชาชนต่อไป

นายรัชภูมิ เวียงสิมา
15 สิงหาคม 2566

# สารบัญ


บทสรุปสำหรับผู้บริหาร ง
กิตติกรรมประกาศ จ
สารบัญ ฉ
สารบัญตาราง ช
สารบัญภาพ ซ
1. วิสัยทัศน์ของตำแหน่งเป้าหมาย 1
    1.1 การวิเคราะห์บริบทและทิศทางเชิงยุทธศาสตร์ของส่วนราชการ 1
    1.2 ตำแหน่งรองอธิบดีที่เป็นเป้าหมาย 7
    1.3 กำหนดวิสัยทัศน์ของตำแหน่งเป้าหมาย 10
2. ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ 11
    2.1 การกำหนดประเด็นการศึกษา 11
    2.2 การกำหนดข้อเสนอเชิงนโยบาย 17
    2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ 28
3. แผนพัฒนาตนเอง 30
    3.1 การวิเคราะห์ตนเอง 30
    3.2 การวางแผนพัฒนาตนเอง 30
    3.3 ผลการพัฒนาตนเอง 31
บรรณานุกรม 44
ประวัติผู้เขียนรายงานการศึกษาส่วนบุคคล 46

# สารบัญตาราง

ตารางที่ 2.1 บทบาทหน้าที่ของหน่วยงานประชาคมที่มีบทบาทนำในด้านข่าวกรองทางไซเบอร์ 22
ตารางที่ 2.2 สรุปตัวอย่างภารกิจของศูนย์ประสานข่าวกรองทางไซเบอร์ในต่างประเทศ 24
ตารางที่ 2.3 แผนขับเคลื่อนการบูรณาการเครือข่ายด้านข่าวกรองทางไซเบอร์ ระยะ 5 ปี ของ สขช. 26
ตารางที่ 2.4 เปรียบเทียบการดำเนินการก่อนและหลังการจัดตั้ง (AS – IS / TO -BE) 27
ตาราง IDP 1 การวิเคราะห์ตนเอง 32
ตาราง IDP 2 ความรู้ ทักษะ ความสามารถ และคุณลักษณะที่ต้องการพัฒนา 35
ตาราง IDP 3 แผนพัฒนารายบุคคล : ระยะเวลา 2 ปี 37
ตาราง IDP 4 แผนพัฒนารายบุคคล : ระยะเวลา 2 เดือน (ระหว่างการฝึกอบรม นบส.1) 40
ตาราง IDP 5 ผลการพัฒนาตนเองระยะ 2 เดือน (ระหว่างการฝึกอบรม นบส. 1) 42

# สารบัญภาพ

ภาพที่ 1.1 ความเชื่อมโยงของแผน 3 ระดับ ตามยุทธศาสตร์ชาติ 20 ปี 7
ภาพที่ 1.2 โครงสร้างการบริหาร สำนักข่าวกรองแห่งชาติ 7
ภาพที่ 2.1 แบบจำลองวงรอบข่าวกรอง 19
ภาพที่ 2.2 NIST Cyber Security Framework 20

## 1. วิสัยทัศน์ของตำแหน่งเป้าหมาย

**(ข้อมูลส่วนบุคคลไม่เผยแพร่)**

## 2. ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ

### 2.1 การกำหนดประเด็นการศึกษา

#### 2.1.1 ปัญหาและความท้าทายที่เลือกศึกษา

##### 2.1.1.1 บริบทสถานการณ์ความมั่นคงที่เปลี่ยนแปลงไปในปัจจุบัน

ในยุคก่อนที่โครงข่ายอินเทอร์เน็ต World Wide Web (www.) จะแพร่หลายไปทั่วโลก เมื่อปี พ.ศ.2536 สถานการณ์ภัยคุกคามความมั่นคงแบบเดิม ถูกตีกรอบอยู่ที่ภัยคุกคามทางทหาร (military threat) ที่มักเกิดขึ้นในรูปแบบของสงครามระหว่างรัฐ นำกำลังเข้าสู้รบเพื่อผลประโยชน์ต่าง ๆ อาทิ อำนาจ ดินแดน และทรัพยากร ส่วนใหญ่ยังเป็นพื้นที่จำกัดและสามารถบริหารจัดการได้ ภายใต้ขอบเขตอำนาจรัฐของประเทศใดประเทศหนึ่ง แต่หลังจากห้วงเวลาดังกล่าวเป็นต้นมา การติดต่อสื่อสารทางอินเทอร์เน็ตที่เชื่อมโยงถึงกันทั่วโลก ได้ทำให้ภัยคุกคามความมั่นคงรูปแบบใหม่ขยายขอบเขตกว้างขึ้น โดยมีลักษณะข้ามพรมแดน แพร่กระจายอย่างรวดเร็ว เชื่อมโยงกันหลายมิติหลายประเด็น จนส่งผลให้สังคมในทุกภาคส่วนทั้งภาครัฐ เอกชน ประชาสังคม และประชาชนทั่วไป มีโอกาสตกเป็นเป้าหมายของการปฏิบัติการทางไซเบอร์ เพื่อถูกแสวงประโยชน์ในทางมิชอบ ที่สำคัญ คือ การลักลอบเข้าถึงข้อมูลสารสนเทศ การบ่อนทำลายผลประโยชน์ของบุคคลหรือองค์กรด้วยเครื่องมือทางเทคนิค ที่มีพัฒนาการซับซ้อนมากขึ้นอย่างต่อเนื่อง อาทิ โปรแกรมประสงค์ร้าย หรือมัลแวร์ (Malware) ซึ่งออกแบบมาสำหรับดักรับการสื่อสารของเป้าหมาย ขโมยข้อมูล หรือสร้างความเสียหายประการอื่น

จากรายงานเชิงสถิติประเทศที่ก่อเหตุโจมตีทางไซเบอร์ต่อประเทศต่าง ๆ ของโลกในห้วง พ.ศ. 2565 ข้อมูลโดยบริษัทโทรคมนาคมแห่งชาติ พบว่า **กลุ่มประเทศต้นทางที่มีพฤติกรรมเจาะช่องโหว่ของระบบโดยโจมตีไปยังประเทศอื่น ๆ รวมทั้งไทย จำนวน 5 ประเทศ ได้แก่ 1) สหรัฐฯ ร้อยละ 30 2) จีน ร้อยละ 15 3) ไทย เนเธอร์แลนด์ และรัสเซีย ประเทศละร้อยละ 5 ของการโจมตีที่เกิดขึ้นทั้งหมด** ทั้งนี้ยังไม่อาจยืนยันได้ว่าประเทศดังกล่าวเป็นผู้ก่อเหตุโจมตีด้วยตนเอง หรือถูกลักลอบแสวงประโยชน์ระบบโครงสร้างพื้นฐานทางเครือข่ายเพื่อใช้เป็นเครื่องมือก่อเหตุโจมตีไปยังประเทศอื่น ๆ ดังจะเห็นได้ว่าบริบทที่เปลี่ยนแปลงไปนี้ **ส่งผลให้มาตรการรับมือภัยคุกคามในรูปแบบเดิม ไม่สามารถแก้ไขปัญหาได้อย่างมีประสิทธิภาพ เพราะภัยคุกคามรูปแบบใหม่ ในการนี้จะกล่าวเฉพาะภัยคุกคามทางไซเบอร์** มีความเชื่อมโยงกับประเด็นปัญหาอื่นๆ หลายมิติและมีผู้ที่ได้รับผลกระทบจำนวนมาก อีกทั้งมีพลวัตอยู่ตลอดเวลา ข้อมูลที่เกี่ยวข้องกับเหตุการณ์ภัยคุกคามทางไซเบอร์มีปริมาณมหาศาล จนเป็นไปได้ยากที่หน่วยงานใดหน่วยงานหนึ่งจะสามารถดำเนินการเพื่อให้ได้มาซึ่งข้อมูลจำนวนมากดังกล่าว รวมถึงการบริหารจัดการหรือใช้ประโยชน์ข้อมูล ในการป้องกันและแก้ไขปัญหาภัยคุกคามรูปแบบใหม่ได้อย่างครอบคลุมในทุกมิติของความมั่นคง

##### 2.1.1.2 ความท้าทายในภารกิจด้านความมั่นคงปัจจุบัน

ภัยคุกคามรูปแบบใหม่ Non-Traditional Threats ยังไม่มีคำนิยามที่ชัดเจน แต่อาจสรุปในภาพรวมได้ คือ ภัยคุกคามที่มีผลกระทบต่อความมั่นคงหรือความปลอดภัย ความสงบสุข และการพัฒนาของสังคมและมนุษย์ชาติ หรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงเกือบทุกมิติที่เกิดขึ้นหลังยุคสงครามเย็น เป็นภัยคุกคามด้านต่าง ๆ ที่ซับซ้อนหลากหลายมิติทั้งจากภายนอกและภายในประเทศ สืบเนื่องมาจากสภาพการเปลี่ยนแปลงของสังคม สภาพแวดล้อม กระแสโลกาภิวัตน์ และนวัตกรรมต่าง ๆ **ประเด็นความท้าทายของภัยคุกคามรูปแบบใหม่มีลักษณะ “ไม่ชัดเจน คลุมเครือ เชื่อมโยงหลายมิติ ไม่จำกัดพื้นที่ และสร้าง**

**ความเสียหายเป็นวงกว้าง"** โดยเฉพาะอย่างยิ่งความยากในการระบุและเจาะจงว่า สิ่งที่เผชิญอยู่นั้นมีรายละเอียดอย่างไร เช่น เป็นภัยคุกคามรูปแบบใด ใครเป็นตัวแสดง และมีเหตุผลอะไร

ยกตัวอย่างเช่น **การโจมตีทางไซเบอร์ต่อโรงพยาบาลแห่งหนึ่งในไทย** การโจมตีดังกล่าวอาจเป็นการโจมตีโดยตัวแสดงที่เป็นรัฐ หรือไม่ใช่รัฐก็ได้ อาจมาจากภายในประเทศหรือนอกประเทศ อาจมีสาเหตุจากปัญหาทางการเมือง หรืออาจเกิดขึ้นเพียงเพื่อต้องการผลประโยชน์ทางเศรษฐกิจหรือธุรกิจบางประการ อาจเป็นการก่อการร้าย หรืออาจเป็นส่วนหนึ่งของปฏิบัติการทางทหารจากประเทศอื่น หรืออาจเป็นเพียงการก่อกวนเพื่อผลประโยชน์บางอย่างเป็นต้น **ประเด็นสำคัญ คือการโจมตีทางไซเบอร์ที่เกิดขึ้นในโรงพยาบาลซึ่งเป็นสถานที่ที่ไม่ใช่พื้นที่การสู้รบ** แสดงให้เห็นว่าภัยคุกคามรูปแบบใหม่สามารถเกิดขึ้นในพื้นที่ที่หลากหลายมากขึ้น นอกจากความท้าทายในประเด็นภัยคุกคามแล้ว **ยังมีความท้าท้ายของหน่วยความมั่นคง** สรุปดังนี้

1) ประเด็นการเพิ่มประสิทธิภาพของผลผลิตรายงานข่าวกรอง ต้องมีคุณภาพสูงขึ้น สามารถนำไปใช้ประโยชน์แก้ไขปัญหาได้ทันกับสถานการณ์

2) การเพิ่มประสิทธิภาพของการปฏิบัติการ วิธีการ เทคโนโลยี และกระบวนการทำงานของหน่วยข่าวหน่วยความมั่นคง เพื่อป้องกันภัยคุกคามทางไซเบอร์ ได้ทันสถานการณ์และเวลา

3) การเพิ่มประสิทธิภาพของ จนท. และบุคลากร ให้มีทักษะ ความรู้ความเข้าใจ หรือมีศักยภาพทางไซเบอร์ เทคโนโลยี การวิเคราะห์ ให้ทันสมัยเพียงพอที่จะรับมือกับภัยคุกคามทางไซเบอร์

**2.1.1.3 การปรับตัวของหน่วยงานด้านความมั่นคงเพื่อรับมือกับภัยคุกคามรูปแบบใหม่**

การเปลี่ยนแปลงที่รวดเร็วทั้งด้านสภาพแวดล้อมต่าง ๆ และเทคโนโลยี ซึ่งเปลี่ยนผ่านจากยุคข้อมูลข่าวสารตั้งแต่ปี พ.ศ.2516 เข้าสู่ยุคดิจิทัลเมื่อปี พ.ศ.2551 ประกอบกับทุกประเทศเผชิญกับสภาวะ BANI world กล่าวคือ ตกอยู่ในสภาพแวดล้อมใหม่ที่มีความเปราะบาง (Brittle) มีความกังวล (Anxious) คาดเดาได้ยาก (Nonlinear) และคลุมเครือ (Incomprehensible) ซึ่งเป็นสภาพบังคับให้ทั้งภาครัฐและเอกชน ต้องปรับตัวโดยนำเทคโนโลยีที่ทันสมัย มายกระดับประสิทธิภาพกระบวนการทำงานขององค์กร

ขณะที่หน่วยความมั่นคง จำเป็นต้องปรับเปลี่ยนวิธีการทำงานเช่นเดียวกับองค์กรในภาคส่วนอื่น เพื่อให้สามารถรับมือกับภัยคุกคามในปัจจุบัน ซึ่งมีการปฏิบัติการทางไซเบอร์ที่มีเทคนิคชั้นสูง กล่าวคือใช้วิธีเจาะระบบคอมพิวเตอร์ เพื่อละเมิดมาตรการรักษาความปลอดภัยของบุคคล เอกสาร และสถานที่ เพราะปัจจุบันการรักษาความปลอดภัยล้วนแต่ใช้ระบบคอมพิวเตอร์และอินเทอร์เน็ต เข้ามามีส่วนในการบริหารจัดการทั้งสิ้น รัฐบาลหลายประเทศจึงเร่งพัฒนานโยบายและกฎหมายใหม่ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ และปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบสาธารณูปโภค อันเป็นปัจจัยสำคัญอย่างยิ่งต่อการรักษาความสงบเรียบร้อยและความเชื่อมั่นต่อเศรษฐกิจ สังคม และการเมืองของประเทศ ดังเช่น ที่ไทยได้ผลักดันกฎหมายใหม่หลายฉบับ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มุ่งเน้นการรักษาความปลอดภัยไซเบอร์ระดับประเทศในภาพรวม ซึ่งกำหนดให้มีกลไกการทำงาน คือ คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เป็นระดับนโยบายมี นรม. เป็นประธาน **คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) เป็นระดับการกำกับดูแลการดำเนินงานตามนโยบาย มี รมว.กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธาน ซึ่งผู้อำนวยการสำนักข่าวกรองแห่งชาติเป็นกรรมการโดยตำแหน่ง** และสำนักงาน

คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐมีคณะกรรมการบริหารสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กบส.) ดูแลการบริหาร สนง.

ส่วน **สำนักข่าวกรองแห่งชาติ** ได้ปฏิบัติภารกิจเกี่ยวกับภัยคุกคามทางไซเบอร์ **ตามอำนาจหน้าที่ใน พ.ร.บ.ข่าวกรองแห่งชาติ พ.ศ.2562** เช่น มาตรา 5 บัญญัติให้ สขช. ปฏิบัติงานเกี่ยวกับกิจการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร และการรักษาความปลอดภัยฝ่ายพลเรือน รวมทั้ง ติดตามสถานการณ์ภายในประเทศและต่างประเทศ ที่มีผลกระทบต่อความมั่นคงของชาติ รายงานต่อนายกรัฐมนตรีและสภาความมั่นคงแห่งชาติ นอกเหนือจากการปฏิบัติตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และนโยบายและแผนระดับชาติว่าด้วยความมั่นคง ประเด็นที่ 15

**2.1.2 สภาพปัญหาที่ผ่านมา แนวโน้มในอนาคต และผลกระทบ**

**2.1.2.1 สถานการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติ ภัยคุกคามทางไซเบอร์ คือ การกระทำใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ที่มุ่งหมายสร้างความเสียหายต่อระบบคอมพิวเตอร์ หรือข้อมูล คอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง** ซึ่งหลายกรณีอาจจัดว่าเข้าข่ายของการทำสงครามอสมมาตร (Asymmetric warfare) หากฝ่ายปฏิปักษ์สามารถใช้ปฏิบัติการทางไซเบอร์ โจมตีโครงสร้างพื้นฐานของคู่ขัดแย้งได้โดยไม่ต้องมีการเผชิญหน้าทางทหารแบบดั้งเดิม เนื่องจากปฏิบัติการทางไซเบอร์เป็นวิธีที่มีประสิทธิภาพสูง ในการเข้าถึงข้อมูลสำคัญของเป้าหมาย และยังสามารถสร้างความเสียหายได้เป็นวงกว้างในเวลารวดเร็ว ผ่านการเชื่อมต่ออินเทอร์เน็ตที่ไม่มีข้อจำกัดด้านพรมแดนทางกายภาพ **จากรายงานสถิติรูปแบบการโจมตีทางไซเบอร์ในห้วง 2565 ข้อมูลโดยบริษัทโทรคมนาคมแห่งชาติ พบรูปแบบการก่อเหตุโจมตีสูงสุด 4 ลำดับ** ดังนี้ 1) การโจมตีโดยการฝังโค้ดประสงค์ราย (Malicious Code) ร้อยละ 54 2) การโจมตีเพื่อขัดขวางการให้บริการ (Availability) ร้อยละ 18 3) การโจมตีโดยการรวบรวมจุดอ่อนของระบบ (Information Gathering) ร้อยละ 16 และ 4) การโจมตีโดยการลอบบุกรุกระบบ (Intrusion) ร้อยละ 12

ทั้งนี้ อาจจัดประเภทของผู้ก่อเหตุภัยคุกคามทางไซเบอร์ที่สำคัญเป็น 3 กลุ่ม ได้แก่

**1) กลุ่มอาชญากรทางไซเบอร์ (Cybercriminal)** มีมูลเหตุจูงใจหลัก คือ ผลประโยชน์ทางการเงิน อีกทั้งมีการก่อเหตุในลักษณะข้ามชาติ ผ่านการให้บริการโจมตีทางไซเบอร์ในเชิงพาณิชย์ (Crime-as-a-Service - CaaS) ทำให้อาชญากรที่ไม่มีทักษะด้านคอมพิวเตอร์ สามารถเข้าถึงเครื่องมือสำเร็จรูปที่มีประสิทธิภาพสูง เช่น มัลแวร์ขโมยข้อมูล (Trojan) และมัลแวร์เรียกค่าไถ่ (Ransomware) เพื่อขโมยข้อมูลแล้วนำไปรีดไถทรัพย์จากบุคคล หรือองค์กรที่มีแนวโน้มจะสร้างผลตอบแทนได้มาก เช่น สถาบันการเงิน องค์กรธุรกิจ บริการที่สำคัญของภาครัฐ รวมถึงประชาชนทั่วไปที่ตกเป็นเหยื่อของการหลอกลวงทางออนไลน์ จึงเป็นภัยคุกคามที่ได้รับความสนใจจากสังคม แต่ยากต่อการติดตามดำเนินคดีเนื่องจากมีอุปสรรคในทางปฏิบัติค่อนข้างมาก เพราะจำเป็นต้องได้รับความร่วมมือจากหน่วยงานบังคับใช้กฎหมายระหว่างประเทศ อาทิ การปราบปรามกลุ่มแฮ็กเกอร์รับจ้าง กลุ่มนายหน้าซื้อขายข้อมูลคอมพิวเตอร์ แก๊งคอลเซ็นเตอร์ เว็บไซต์พนัน เว็บไซต์หลอกลวงลงทุน และเว็บไซต์ค้าสิ่งของผิดกฎหมาย เป็นต้น

**2) กลุ่มนักเคลื่อนไหวทางไซเบอร์ (Hacktivist)** มีมูลเหตุจูงใจหลัก คือ การขับเคลื่อนประเด็นทางสังคมหรือการเมือง โดยใช้วิธีโจมตีทางไซเบอร์หรือการปฏิบัติการข่าวสารทางออนไลน์ ส่วนใหญ่มีเป้าหมายเป็นหน่วยงานภาครัฐและองค์กรอื่น ๆ ที่มีความใกล้ชิดกับรัฐบาล เช่น การโจมตีเพื่อเปลี่ยนแปลงหน้าเว็บไซต์ (Web defacement) การเจาะระบบฐานข้อมูลขององค์กรหรือเจ้าหน้าที่รัฐ แล้วนำไปเผยแพร่

และการโจมตีเพื่อขัดขวางการให้บริการ (Distributed Denial of Service - DDoS) เพื่อทำให้เว็บไซต์ขององค์กรไม่สามารถเข้าใช้งานได้ ซึ่งมุ่งผลทำลายภาพลักษณ์ของรัฐบาลหรือกลุ่มผลประโยชน์ ที่เป็นฝ่ายตรงข้าม ดังนั้น การก่อเหตุของกลุ่ม Hacktivist จึงมีแนวโน้มสอดรับกับระดับความรุนแรงของสถานการณ์ทางการเมืองหรือสังคมในแต่ละช่วงเวลา

**3) กลุ่มแฮ็กเกอร์ที่ได้รับการสนับสนุนจากรัฐ (State-Sponsored Hacker)** เป็นกลุ่มที่มีศักยภาพทางเทคนิคสูงและเน้นการแฝงตัวในระบบ หรือ Advanced Persistent Threat (APT) มีมูลเหตุจูงใจหลัก คือ การจารกรรมข้อมูลความลับทางราชการ หรือทรัพย์สินทางปัญญาที่เกี่ยวข้องกับผลประโยชน์ของชาติ รวมถึงการปฏิบัติการข่าวสาร และการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญ เพื่อบ่อนทำลายผลประโยชน์ของฝ่ายตรงข้าม โดยไทยมีแนวโน้มตกเป็นเป้าหมายของกลุ่ม APT เพิ่มขึ้นอย่างต่อเนื่อง เพราะตั้งอยู่ในพื้นที่แข่งขันอิทธิพลระหว่างกลุ่มประเทศมหาอำนาจทั้งในและนอกภูมิภาค

**2.1.2.2 ภัยคุกคามจากการปฏิบัติการข่าวกรองทางการสื่อสารของประเทศต่าง ๆ**

การแย่งชิงอิทธิพลทางภูมิรัฐศาสตร์ และการแข่งขันทางเทคโนโลยีระหว่างชาติมหาอำนาจเพื่อกำหนดทิศทางของระเบียบโลกใหม่ เป็นมูลเหตุที่ทำให้รัฐบาลต่าง ๆ เร่งยกระดับศักยภาพการปฏิบัติการข่าวกรองและการต่อต้านข่าวกรอง (หมายถึง การกระทำใด ๆ เพื่อให้ทราบถึงความมุ่งหมาย กำลังความสามารถ ความเคลื่อนไหว และวิถีของบุคคลหรือองค์กรทั้งภายในประเทศและต่างประเทศ ที่อาจมีพฤติการณ์เป็นภัยคุกคามต่อความมั่นคง ผลประโยชน์ของชาติ รวมถึงการดำเนินการต่อต้านบุคคลหรือองค์กรใดที่มุ่งหมายจะได้ไปซึ่งความลับของชาติ หรือก่อเหตุจารกรรม บ่อนทำลาย ก่อวินาศกรรม การก่อการร้าย หรือการอื่นใดอันเป็นภัยคุกคามต่อชาติ) ในระยะที่ผ่านมา **ฝ่ายความมั่นคงของประเทศต่าง ๆ จึงเล็งเห็นความสำคัญของการพัฒนาขีดความสามารถด้าน “การข่าวกรองทางการสื่อสาร” โดยประยุกต์ใช้เทคโนโลยีสารสนเทศที่ก้าวหน้า เช่น ฐานข้อมูลขนาดใหญ่ (Big Data) ระบบเรียนรู้อัตโนมัติ (Machine Learning) และปัญญาประดิษฐ์ (Artificial Intelligence) ไปพัฒนาระบบงานข่าวกรองให้มีประสิทธิภาพสูงขึ้น และสร้างความได้เปรียบเหนือกว่าประเทศคู่แข่งขันอื่น ๆ ผ่านการปฏิบัติการทางไซเบอร์ในลักษณะเชิงรุก เพื่อให้ได้มาซึ่งข้อมูลข่าวกรองของเป้าหมาย**

แนวโน้มดังกล่าวสะท้อนได้จาก พฤติกรรมของกลุ่มแฮ็กเกอร์ที่ได้รับการสนับสนุนจากรัฐซึ่งอยู่เบื้องหลังการจารกรรมข้อมูลความลับทางราชการ และทรัพย์สินทางปัญญาที่สำคัญต่อผลประโยชน์ของชาติ รวมทั้งโจมตีทางไซเบอร์ต่อระบบสาธารณูปโภคและโครงสร้างพื้นฐานสารสนเทศของฝ่ายปฏิปักษ์ ดังนั้นจึงตรวจพบความเคลื่อนไหวลักษณะดังกล่าวมาก ในประเทศที่เป็นคู่ขัดแย้งหรือตกอยู่ในพื้นที่แย่งชิงอิทธิพลระหว่างมหาอำนาจ เช่น รัสเซีย ยูเครน จีน ไต้หวัน คาบสมุทรเกาหลี ภูมิภาคตะวันออกกลาง และเอเชียแปซิฟิก รวมถึงเขตแดนของสหรัฐฯ และพันธมิตร

**2.1.2.3 แนวโน้มในอนาคต** สถานการณ์และภัยคุกคามด้านความมั่นคงทั้งในระดับโลก ภูมิภาค และประเทศไทยเปลี่ยนแปลงไปอย่างรวดเร็ว มีความสลับซับซ้อน รุนแรงมากขึ้นและมีความเชื่อมโยงระหว่างกันในทุกมิติ การคาดการณ์สถานการณ์จึงกระทำได้ยากมากขึ้น **โดยแนวโน้มสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น พร้อมกับความก้าวหน้าทางเทคโนโลยีและผู้ใช้อินเทอร์เน็ตทั้งในไทยและทั่วโลกที่มีจำนวนมหาศาล จะเป็นปัจจัยสำคัญที่ทำให้เทคโนโลยีไซเบอร์ กลายเป็นภัยคุกคามในวงกว้างทวีความรุนแรงซับซ้อนมากขึ้น และมีแนวโน้มขยายตัวตามการใช้เทคโนโลยีสมัยใหม่** จากสถานการณ์ดังกล่าว หน่วยงานด้านการข่าวและประชาคมข่าวกรองต้องมีความพร้อมกับสถานการณ์ภัยคุกคามทุกมิติ ทุกรูปแบบ

สามารถบริหารจัดการให้เกิดการบูรณาการงานข่าวกรอง ได้เท่าทันต่อการรับมือกับความท้าทายภายใต้สภาวะแวดล้อมความมั่นคง ในบริบทใหม่ที่ขยายตัวอย่างรวดเร็ว

**2.1.2.4 ผลกระทบจากภัยคุกคามทางไซเบอร์ต่อผลประโยชน์แห่งชาติของไทย**

**1) ผลกระทบด้านความมั่นคง-การทหาร** มาจากปฏิบัติการจารกรรมทางไซเบอร์ของกลุ่มแฮ็กเกอร์ที่ได้รับการสนับสนุนจากรัฐ ที่ส่วนใหญ่มุ่งเป้าต่อหน่วยงานระดับนโยบายด้านการต่างประเทศ กลาโหม ฝ่ายบริหารและนิติบัญญัติ การปกครองส่วนภูมิภาค รวมถึงผู้ให้บริการโทรคมนาคมแก่หน่วยงานดังกล่าว และสถาบันอุดมศึกษา โดยมีรูปแบบการโจมตีที่พบบ่อยครั้ง เช่น การเจาะระบบอีเมลของเจ้าหน้าที่ การปลอมแปลงหน้าเว็บไซต์สำหรับเข้าใช้งานเครือข่ายภายในองค์กร และการส่งอีเมลหลอกลวงแบบเฉพาะเจาะจงเป้าหมาย เพื่อแพร่กระจายมัลแวร์ขโมยข้อมูล อาทิ ShadowPad และ PlugX ซึ่งปรากฏข่าวสารว่ามีความเชื่อมโยงกับปฏิบัติการทางไซเบอร์ของจีนในหลายพื้นที่ทั่วโลก โดยถูกดัดแปลงคุณสมบัติให้แตกต่างไปจากเดิมอย่างต่อเนื่องเพื่อหลบเลี่ยงการตรวจสอบ นอกจากนี้ ยังปรากฏข่าวสารกลุ่มอาชญากรทางไซเบอร์เจาะระบบหน่วยงานภาครัฐในไทย เพื่อขโมยข้อมูลไปขายให้กลุ่มแฮ็กเกอร์ที่มีความเชื่อมโยงกับรัฐบาลต่างชาติ รวมถึงพบสิ่งบ่งชี้การโจมตีทางไซเบอร์ (Indicator of Compromise - IOCs) ที่มีความเชื่อมโยงกับปฏิบัติการทางไซเบอร์ของประเทศอื่น ๆ เช่น เวียดนาม เกาหลีเหนือ รัสเซีย และอิหร่าน เป็นต้น

**2) ผลกระทบด้านเศรษฐกิจ-สังคม** มาจากกลุ่มอาชญากรทางไซเบอร์ ส่วนใหญ่ใช้วิธีโจมตีทางไซเบอร์ด้วย Ransomware ต่อองค์กรขนาดใหญ่ทั้งในภาครัฐและเอกชน โดยเปิดเผยการก่อเหตุต่อสาธารณะเพื่อสร้างแรงกดดันให้องค์กรที่ตกเป็นเหยื่อ ยอมจ่ายเงินแลกกับการไม่เปิดเผยข้อมูลของผู้ใช้บริการองค์กร หรือทรัพย์สินทางปัญญาที่สำคัญต่อความอยู่รอดของธุรกิจ ตัวอย่างเหตุการณ์ที่สร้างความเสียหายอย่างร้ายแรง เช่น **1) การโจมตีสถานพยาบาล** โดยเข้ารหัสข้อมูลประวัติการรักษาของผู้ป่วย ข้อมูลส่วนบุคคลของเจ้าหน้าที่ และระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาล จนไม่สามารถให้บริการได้ **2) การโจมตีผู้ให้บริการแพลตฟอร์มซื้อขายสินค้าออนไลน์** ผู้ให้บริการโทรคมนาคม และผู้ให้บริการระบบสาธารณูปโภค โดยขโมยข้อมูลส่วนบุคคลของผู้ใช้บริการ รวมถึงข้อมูลธุรกรรมทางการเงินไปประมูลขายต่อให้กลุ่มแฮ็กเกอร์ในเว็บไซต์ใต้ดิน (Dark web) ที่สามารถเข้าถึงได้จากทั่วโลก ซึ่งมีแนวโน้มจะถูกนำไปแสวงประโยชน์ต่อเหยื่ออย่างเฉพาะเจาะจงต่อไป และ **3) ขบวนการหลอกลวงทางออนไลน์** โดยมีการแพร่มัลแวร์ขโมยเงินผ่านแอปพลิเคชันและเว็บไซต์ที่ปลอมแปลงขึ้น ซึ่งมีประชาชนตกเป็นเหยื่อจำนวนมากและยากต่อการสืบสวนติดตามและบังคับใช้กฎหมายดำเนินคดี เพราะผู้ก่อเหตุมีฐานปฏิบัติการอยู่ในต่างประเทศ

**3) ผลกระทบด้านสังคม-จิตวิทยา** มาจากการโจมตีทางไซเบอร์ของกลุ่ม Hacktivist ส่วนใหญ่เป็นการทำ Web defacement ต่อเว็บไซต์ของหน่วยงานราชการหรือบุคคลสำคัญ รวมถึงการขโมยข้อมูลของกลุ่มเป้าหมายดังกล่าวไปเผยแพร่ต่อสาธารณะ เพื่อให้เกิดความเสื่อมเสียต่อภาพลักษณ์ความน่าเชื่อถือ ซึ่งมักเกิดขึ้นในห้วงที่มีสถานการณ์ความขัดแย้งในประเทศ นอกจากนี้ ยังมีภัยคุกคามจากการปฏิบัติการข่าวสารที่ได้รับสนับสนุนจากรัฐบาลต่างชาติ ซึ่งมุ่งเน้นเผยแพร่ข้อมูลที่บ่อนทำลายความเชื่อมั่นของประชาชนต่อกลุ่มการเมือง/กลุ่มผลประโยชน์ที่เป็นฝ่ายตรงข้ามกับตน ขณะที่สนับสนุนการขยายผลเนื้อหาข่าวสารที่เป็นคุณต่อกลุ่มที่เป็นฝ่ายเดียวกับตน โดยการปฏิบัติการจะมีทิศทางสอดคล้องกับบริบทความขัดแย้งด้านนโยบายต่างประเทศของกลุ่มมหาอำนาจ ที่เข้ามาแผ่ขยายอิทธิพลใน ASEAN เช่น ประเด็นสถานการณ์สู้รบบริเวณชายแดนเมียนมา ข้อพิพาทการใช้ประโยชน์พื้นที่ลุ่มแม่น้ำโขง เหตุการณ์ความไม่สงบในพื้นที่สามจังหวัดชายแดนภาคใต้ โครงการก่อสร้างโครงสร้างพื้นฐานที่ได้รับงบประมาณสนับสนุนจากต่างชาติ และการ

ผลักดันข้อตกลงด้านเขตเศรษฐกิจหรือกฎหมายระหว่างประเทศ ซึ่งหากไม่มีมาตรการรับมือที่เหมาะสมก็มีโอกาสบานปลายกลายเป็นผลกระทบด้านความมั่นคง-การทหาร และด้านเศรษฐกิจ-สังคม ต่อไปได้

**2.1.3 ความจำเป็นในการดำเนินการ**

**2.1.3.1 ความจำเป็นในการจัดตั้งเครือข่ายบูรณาการข่าวกรองทางไซเบอร์**

ผู้ก่อเหตุโจมตีทางไซเบอร์มีการพัฒนาเทคนิควิธีการโจมตี ที่มีความซับซ้อนและยากต่อการตรวจสอบยิ่งขึ้น ทำให้หน่วยงานใดหน่วยงานหนึ่งไม่สามารถใช้ทรัพยากรที่มีอยู่จำกัด ไปดำเนินการโดยลำพังเพื่อติดตามเฝ้าระวัง หรือยุติพฤติการณ์ของกลุ่มผู้ก่อเหตุได้อย่างมีประสิทธิภาพ หน่วยงานด้านความมั่นคงทั่วโลก จึงเล็งเห็นความสำคัญของการสร้างเครือข่ายความร่วมมือ เพื่อแบ่งปันทรัพยากรและร่วมกันปฏิบัติภารกิจ เฉพาะอย่างยิ่งในด้านการแลกเปลี่ยนองค์ความรู้ทางเทคนิค และการแจ้งเตือนข่าวกรองภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานในเครือข่ายสามารถนำไปใช้ป้องกันและแก้ไขปัญหาได้ทันสมัย ทันต่อสถานการณ์ รวมทั้งใช้เป็นข้อมูลในการติดตามตรวจสอบความเคลื่อนไหวของกลุ่มแฮ็กเกอร์ต่างๆ ต่อไป

นอกจากนี้ การจัดตั้งเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ของหน่วยประชาคมยังเป็นไปเพื่อให้สอดรับกับรูปแบบและนโยบายของ คณะทำงานแบบบูรณาการในระดับนานาชาติ ซึ่งเป็นตัวกลางประสานงานและแลกเปลี่ยนข้อมูลข่าวกรองทางไซเบอร์กับประชาคมโลก ยกตัวอย่าง**คณะทำงานบูรณาการด้านความมั่นคงปลอดภัยไซเบอร์ในสหสภาพยุโรป** ดำเนินการโดย ENISA (European Union Agency for Cybersecurity) **มีวัตถุประสงค์ในการขยายขอบเขตความร่วมมือและความช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของสมาชิกสหภาพยุโรป** ซึ่งการจัดตั้งคณะทำงานดังกล่าวช่วยส่งเสริมให้ประเทศสมาชิกมีความเป็นเอกภาพ มีศูนย์กลางแลกเปลี่ยนข้อมูลข่าวกรองทางไซเบอร์ที่ชัดเจน อีกทั้งยังช่วยส่งเสริมให้เกิดการพัฒนาองค์ความรู้ และเทคโนโลยีใหม่ ๆ ในการคาดการณ์สถานการณ์ทางไซเบอร์ล่วงหน้า เพื่อรับมือกับการโจมตีที่อาจจะเกิดขึ้นในอนาคตได้อย่างแม่นยำ

**2.1.3.2 ความจำเป็นในการพัฒนาบุคลากร**

ความจำเป็นในการสร้างบุคลากร ให้มีทักษะความเชี่ยวชาญเฉพาะด้านไซเบอร์เป็นสิ่งที่สำคัญเป็นอย่างยิ่ง เนื่องจากกลุ่มแฮ็กเกอร์มีพัฒนาการในการค้นหาวิธีการ ที่จะโจมตีทางไซเบอร์หรือเจาะระบบอย่างต่อเนื่อง หากบุคลากรด้านไซเบอร์ขององค์กรขาดความรู้ที่เท่าทันต่อสถานการณ์ดังกล่าว ถือเป็นจุดอ่อนสำคัญที่สุดในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ องค์กรจึงต้องกำหนดแผนการสร้างพัฒนาบุคลากรด้านไซเบอร์อย่างต่อเนื่อง รวมทั้งสร้างเวทีแลกเปลี่ยนเรียนรู้ระหว่างหน่วยงาน เพื่อยกระดับศักยภาพของบุคลากร ให้มีขีดความสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

**2.1.3.3 ความจำเป็นในการพัฒนาเทคโนโลยี**

การนำเทคโนโลยีที่ทันสมัยมาใช้ สามารถช่วยเพิ่มประสิทธิภาพการทำงานขององค์กร และกระตุ้นให้บุคลากรตื่นตัวที่จะพัฒนาทักษะองค์ความรู้ด้านเทคโนโลยี อีกทั้งยังเป็นการลดช่องโหว่หรือจุดอ่อนจากภัยคุกคามทางไซเบอร์ที่เกิดจากเทคโนโลยีที่ไม่ทันสมัย เนื่องจากมัลแวร์ในปัจจุบันได้ถูกพัฒนาหรือมีศักยภาพสูงจนเทคโนโลยีเดิมหรือรุ่นเก่าไม่สามารถป้องกันได้ ฉะนั้นการพัฒนานวัตกรรมและเทคโนโลยีให้ทันสมัยอยู่เสมอ จึงสามารถป้องกันและลดความเสี่ยงจากการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ

กล่าวโดยสรุปคือ จากปัญหาความซับซ้อนของภัยคุกคามทางไซเบอร์ ซึ่งเกิดขึ้นอย่างต่อเนื่องทุกประเทศทั่วโลก และมีความทับซ้อนกันในหลายมิติด้านความมั่นคงของชาติ **จึงเป็นไปได้ยากที่หน่วยงานใดหน่วยงานหนึ่งจะรับมือกับปัญหาที่เกิดขึ้นโดยลำพัง จึงจำเป็นต้องมีการจัดตั้งคณะทำงาน**

**บูรณาการเพื่อประสานความร่วมมือกับทั้งหน่วยงานภายในและต่างประเทศ** ควบคู่ไปกับการเร่งพัฒนาบุคลากรให้พร้อมรับมือกับภัยคุกคามรูปแบบใหม่ ให้เท่าทันการเปลี่ยนแปลงที่เกิดขึ้น ประกอบกับการเร่งพัฒนาเทคโนโลยีในการทำงาน ให้สอดคล้องกับสถานการณ์ความเปลี่ยนแปลงทางเทคโนโลยีของโลก และสามารถคาดการณ์ทิศทางและแนวโน้มการโจมตี ที่อาจจะเกิดขึ้นในอนาคตได้อย่างแม่นยำ

## 2.2 การกำหนดข้อเสนอเชิงนโยบาย

### 2.2.1 หลักการและแนวคิดที่ใช้เป็นแนวทางในการจัดทำข้อเสนอ

#### 2.2.1.1 แนวคิดการบริหารราชการแบบบูรณาการ

พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546 ระบุความหมายของการบริหารราชการแบบบูรณาการว่า เป็นการร่วมมือกันในระหว่างส่วนราชการที่เกี่ยวข้อง เพื่อให้มีการปฏิบัติงานร่วมกัน หรือมีแผนการดำเนินงานที่สอดคล้องไปในทิศทางเดียวกัน ซึ่งจะทำให้ภารกิจที่สำคัญของรัฐในแต่ละด้าน เกิดผลสำเร็จเป็นประโยชน์แก่ประชาชนส่วนรวมและมีความประหยัด โดยใช้ทรัพยากรร่วมกันให้เกิดประโยชน์สูงสุด รวมทั้งสามารถลดขั้นตอนการปฏิบัติราชการให้เกิดความรวดเร็วและมีประสิทธิภาพจากการร่วมมือปฏิบัติงานของทุกฝ่ายที่เกี่ยวข้อง ทั้งนี้ พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546 ได้กำหนดแนวทางในมาตรา 10 ไว้ว่า ในกรณีที่ภารกิจใดมีความเกี่ยวข้องกับหลายส่วนราชการ หรือเป็นภารกิจที่ใกล้เคียงหรือต่อเนื่องกัน ให้ส่วนราชการที่เกี่ยวข้องนั้นกำหนดแนวทางการปฏิบัติราชการ เพื่อให้เกิดการบริหารราชการแบบบูรณาการร่วมกัน โดยมุ่งให้เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ ซึ่งมีองค์ประกอบที่ต้องพิจารณาอย่างน้อย 5 ประการ ดังนี้

**1) โครงสร้างส่วนราชการ** ต้องมีวิธีการที่จะทำให้แต่ละหน่วยงานสามารถทำงานต่อเนื่องกันเป็นแบบยุทธศาสตร์ให้ได้ ความเข้าใจของผู้ปฏิบัติเป็นสิ่งสำคัญซึ่งต้องเข้าใจว่าการทำงานตามโครงสร้างกับการทำงานตามยุทธศาสตร์นั้นไม่ใช่การเลือกทำ แต่เป็นความต่อเนื่องที่ต้องพยายามเชื่อมกันและสอดคล้องกับการปรับโครงสร้างองค์กร

**2) ระบบการทำงาน** การบริหารงานของระบบราชการ โดยเฉพาะการทำงานแบบบูรณาการจำเป็นต้องบริหารให้เกิดสมดุลระหว่างการทำงานเชิงยุทธศาสตร์ (agenda) กับการทำงานตามภารกิจ (functional) หมายความว่า การบริหารระบบราชการในอนาคต ต้องทำควบคู่กันไปทั้งการทำงานแบบบูรณาการตามยุทธศาสตร์และตามภารกิจของสายงานปกติ ต้องมีการกำหนดหน่วยงานกลางในการ บูรณาการเพื่อประสานการทำงานของหน่วยงานต่าง ๆ เข้าด้วยกัน

**3) การจัดสรรงบประมาณ** ต้องปรับเปลี่ยนวิธีการจัดสรรงบประมาณให้สามารถแก้ไขปัญหาต่าง ๆ ได้ครอบคลุม บริหารงบประมาณให้เกิดเอกภาพ ยืดหยุ่น คล่องตัว มีประสิทธิภาพ และสอดคล้องกับการบริหารงานเชิงยุทธศาสตร์

**4) การปรับเปลี่ยนวัฒนธรรมการทำงาน** สิ่งสำคัญจะต้องทำให้คนเห็นความสำคัญของการปรับเปลี่ยนวัฒนธรรมการทำงาน ให้มุ่งเน้นไปที่ความสำเร็จของงานเป็นหลัก สร้างผลงานที่อยู่บนพื้นฐานทางวัฒนธรรม เป้าหมายหลักของการทำงานคือเน้นประชาชนเป็นศูนย์กลาง สร้างวัฒนธรรมการทำงานแบบไร้พรมแดน ลดขอบเขตบทบาทของหน่วยงานลง ใช้ทรัพยากรและปัญญาร่วมกัน ช่วยเหลือกันเพื่อให้งานสำเร็จโดยไม่ถือว่าไม่ใช่งานของตน เพื่อให้การทำงานรวดเร็ว ง่ายดาย และมีประสิทธิภาพ

**5) กลยุทธ์ในการสื่อสาร (Communication) การประสานงาน (Coordination) และ การปฏิบัติการร่วมกัน (Cooperation)** โดยเฉพาะการขอรับการสนับสนุนภารกิจที่ซับซ้อน มีเกี่ยวข้องกับขั้นตอนกระบวนการต่าง ๆ มาก จำเป็นต้องมีการวางแผนกลยุทธ์ที่ดี เพื่อให้เกิดผลผลิตที่ได้จากการแบ่งปันทรัพยากรการทำงานร่วมกัน

**2.2.1.2 การข่าวกรองทางไซเบอร์ และวงรอบข่าวกรอง**

พื้นที่ไซเบอร์ (Cyberspace) เป็น 1 ใน 5 มิติสงคราม สำหรับการปฏิบัติการด้านความมั่นคง นอกเหนือจากพื้นที่ทางบก อากาศ ทะเล และอวกาศ โดยพื้นที่ไซเบอร์ทำให้เกิดการเชื่อมโยงกันระหว่างมิติทั้ง 5 ดังกล่าว จึงส่งผลให้การนิยามคำว่า “ไซเบอร์” ให้ชัดเจนนั้นทำได้ยาก โดยยังคงมีการเปลี่ยนแปลงความหมายตลอดระยะเวลา 10 ปีที่ผ่านมา และมีการขยายขอบเขตคำจำกัดความอย่างต่อเนื่อง อย่างไรก็ตาม Carnegie Mellon Software Engineering Institute ให้คำนิยามของ “การข่าวกรองทางไซเบอร์ (Cyber Intelligence)” ว่าเป็นวิธีการที่ทำให้ได้มาซึ่งข้อมูล เพื่อนำมาใช้ในการวิเคราะห์ สืบสวน ติดตาม และคาดการณ์ความสามารถทางไซเบอร์ และการปฏิบัติการที่จะสามารถนำไปใช้เพื่อตัดสินใจสำหรับการวางแผนปฏิบัติการได้ดียิ่งขึ้น

อย่างไรก็ดี ข่าวกรองทางไซเบอร์มีขั้นตอนกระบวนการ ให้ได้มาซึ่งรายงานข่าวกรองตามทฤษฎีวงรอบข่าวกรอง (Intelligence Cycle) ประกอบด้วย 6 ขั้นตอน ดังนี้

**ขั้นที่ 1 การกำหนดทิศทางของประเด็นข่าวกรอง (Direction)** ระบุหน่วยงานผู้ใช้ข่าว และ ระบุขอบเขตของข่าวสารที่จะนำเสนอให้สอดคล้องกับความต้องการของผู้ใช้ข่าว

**ขั้นที่ 2 การรวบรวมข่าวสาร (Collection)** ระบุแหล่งข้อมูลหรือวิธีการให้ได้มาซึ่งข่าวสารที่ผู้ใช้ข่าวต้องการทราบ

**ขั้นที่ 3 การจัดการข้อมูล (Processing)** จัดระเบียบข้อมูลให้อยู่ในสภาพพร้อมใช้งาน เช่น เรียบเรียงข้อมูลตามลำดับเวลา/ลำดับความสำคัญ และปรับรูปแบบข้อมูลให้เป็นแบบแผนเดียวกัน

**ขั้นที่ 4 การวิเคราะห์ข้อมูล (Analysis)** ระบุเหตุและผลของสถานการณ์ให้เห็นความเชื่อมโยงของประเด็นต่าง ๆ โดยหากมีช่องโหว่ที่ทำให้ไม่สามารถแสดงความสัมพันธ์ของเหตุผลได้ ให้ระบุข้อมูลที่ขาดหายไปแล้วย้อนกลับไปดำเนินการในขั้นที่ 2

**ขั้นที่ 5 การนำเสนอรายงานข่าวกรอง (Dissemination)** จัดทำรายงานโดยเรียบเรียงผลการวิเคราะห์ให้อยู่ในรูปแบบที่เข้าใจง่าย และสะดวกต่อการนำไปใช้ประโยชน์ รวมทั้งกำหนดช่องทางแจกจ่ายรายงานไปยังผู้ใช้ข่าวให้มีความสะดวกรวดเร็วและปลอดภัย

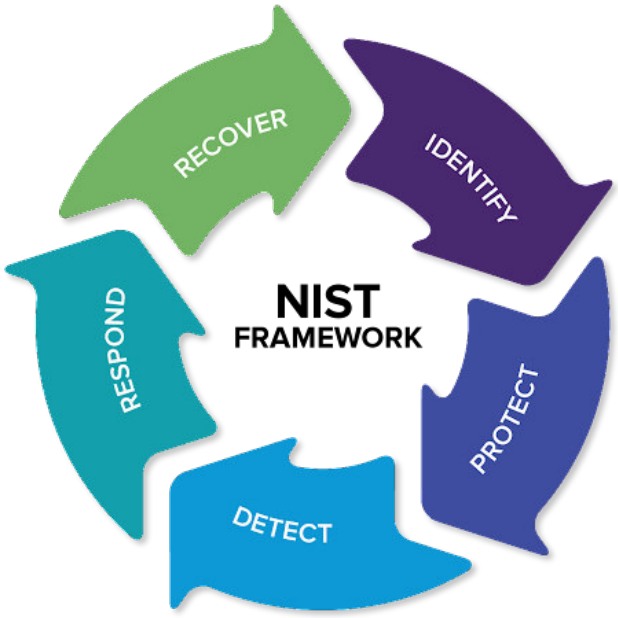
**ขั้นที่ 6 การวิเคราะห์กระแสตอบรับ (Feedback)** กำหนดช่องทางรับฟังความคิดเห็นของผู้ใช้ข่าว เพื่อนำไปปรับปรุงการจัดทำรายงานครั้งต่อไป


**ภาพที่ 2.1** แบบจำลองวงรอบข่าวกรอง
ของ Office of the Director of National Intelligence (2011) อ้างถึงใน Böhm, I. & Lolagar, S. (2021)

**2.2.1.3 การแบ่งปันข้อมูลเพื่อสนับสนุนการปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกรอบแนวคิด NIST Cyber Security Framework**

การปกป้องหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในภาคส่วนต่าง ๆ ให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ จำเป็นต้องอาศัยความร่วมมือด้านข่าวกรองทั้งระดับประเทศและระหว่างประเทศ เพื่อสนับสนุนการปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกรอบแนวคิดของ National Institute of Standards and Technology (NIST) สหรัฐฯ ซึ่งมีหลักปฏิบัติ 5 ขั้นตอน ได้แก่

ขั้นที่ 1 การระบุความเสี่ยงจากภัยคุกคาม (Identify)
ขั้นที่ 2 การปกป้องระบบจากภัยคุกคาม (Protect)
ขั้นที่ 3 การตรวจจับภัยคุกคาม (Detect)
ขั้นที่ 4 การตอบสนองเหตุการณ์ภัยคุกคาม (Respond)
ขั้นที่ 5 การฟื้นฟูความเสียหายจากภัยคุกคาม (Recover)




**ภาพที่ 2.2** NIST Cyber Security Framework อ้างถึงใน Armis (2023)

**2.2.2 ข้อมูลที่เกี่ยวข้องเพื่อประกอบการจัดทำข้อเสนอ**

**2.2.2.1 บทบาทหน้าที่ของหน่วยงานที่มีภารกิจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ได้กำหนด**หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)** ไว้เป็น 8 กลุ่ม ได้แก่ 1) ด้านความมั่นคง 2) ด้านบริการภาครัฐที่สำคัญ 3) ด้านการเงินการธนาคาร 4) ด้านเทคโนโลยีสารสนเทศและคมนาคม 5) ด้านการขนส่งและโลจิสติกส์ 6) ด้านพลังงานและสาธารณูปโภค 7) ด้านสาธารณสุข และ 8) อื่นๆ รวมทั้งให้จัดตั้ง **หน่วยงานทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Sectorial CERT) และหน่วยงานควบคุมหรือกำกับดูแล (Regulator) สำหรับ CII ในแต่ละกลุ่ม**

สำหรับสำนักข่าวกรองแห่งชาติ ถูกจัดเป็นหน่วยงาน CII และเป็น Sectorial CERT กลุ่มด้านความมั่นคงของรัฐในภารกิจอื่น รวมทั้งอยู่ระหว่างขั้นตอนการรับมอบหน้าที่เป็นหน่วยกำกับดูแล Regulator สำหรับกลุ่มงานด้านความมั่นคงในภารกิจอื่น ซึ่งที่ผ่านมาสำนักข่าวกรองแห่งชาตินอกจากจะปฏิบัติภารกิจด้านไซเบอร์ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 แล้วยังปฏิบัติหน้าที่ตาม พ.ร.บ.ข่าวกรองแห่งชาติ พ.ศ.2562 และนโยบายและแผนระดับชาติว่าด้วยความมั่นคง ประเด็นที่ 15

**2.2.2.2 หน่วยงานที่มีบทบาทนำในภารกิจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เฉพาะที่สำคัญ มีดังนี้**

**1) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** เป็นหน่วยงานที่มีภารกิจผสมผสานในเชิงนโยบายและเป็นหน่วยระดับปฏิบัติ ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 โดยมีบทบาทนำในการกำหนดนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงมีหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thai CERT) เพื่อรับแจ้งเหตุภัยคุกคามทางไซเบอร์ในทุกภาคส่วนที่เกี่ยวข้องกับความมั่นคงของรัฐ

**2) ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) และศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)** เป็นกลุ่มความร่วมมือของสถาบันการเงิน และผู้ให้บริการโทรคมนาคม ซึ่งเป็นประชาคมที่มีศักยภาพสูงทั้งด้านการผลิตรายงานข่าวสารภัยคุกคามทางไซเบอร์ และการเผชิญเหตุการโจมตีทางไซเบอร์ เนื่องจากมีความพร้อมด้านงบประมาณ เทคโนโลยี และโครงสร้างการบริหารจัดการองค์กรที่มีความยืดหยุ่นกว่าหน่วยราชการ ทำให้สามารถแบ่งปันข้อมูลข่าวสาร ที่มีคุณภาพแก่หน่วยงานทั้งในและนอกประชาคมได้อย่างต่อเนื่อง อีกทั้งได้รับความเชื่อถือจากกลุ่มเครือข่ายทั้งภาครัฐและเอกชน

**3) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)** มีบทบาทนำด้านการบังคับใช้กฎหมาย โดยมุ่งเน้นภารกิจรักษาความมั่นคงปลอดภัยไซเบอร์ที่เชื่อมโยงกับการก่ออาชญากรรมทางเทคโนโลยีเป็นหลัก ดังนั้น จึงมีความเชี่ยวชาญเฉพาะทางในด้านข่าวกรองเพื่อการสืบสวนติดตามพฤติการณ์ของกลุ่มอาชญากรทางไซเบอร์ทั้งในและต่างประเทศ

**4) ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย และ กองข่าวกรองเทคนิคและเทคโนโลยีข่าวกรอง สำนักข่าวกรอง กรมข่าวทหาร** เป็นหน่วยงานที่มุ่งเน้นภารกิจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เชื่อมโยงกับมิติความมั่นคงด้านการทหาร และการรักษาความสงบเรียบร้อยในประเทศเป็นหลัก จึงมีความเชี่ยวชาญเฉพาะทางในด้านข่าวกรองและการต่อต้านข่าวกรอง ต่อเป้าหมายกลุ่มแฮ็กเกอร์ที่ได้รับการสนับสนุนจากรัฐ รวมถึงกลุ่มนักเคลื่อนไหวทางไซเบอร์ (Hacktivist) ที่ใช้การโจมตีทางไซเบอร์เป็นเครื่องมือขับเคลื่อนประเด็นผลประโยชน์ทางการเมืองหรือสังคม โดยเป็นหน่วยงานที่มีความพร้อมด้านทรัพยากรมากกว่าหน่วยประชาคมอื่น ๆ ในกลุ่มภาครัฐ

**5) สำนักข่าวกรองแห่งชาติ** เป็นหน่วยข่าวพลเรือนที่มีภารกิจครอบคลุมการปฏิบัติการข่าวกรองและการต่อต้านข่าวกรอง ในทุกมิติที่เกี่ยวข้องกับความมั่นคงของชาติ โดยบริบทของสภาพแวดล้อมด้านความมั่นคงระดับโลกที่เปลี่ยนแปลงไปอย่างรวดเร็ว ส่งผลให้ขอบเขตของภารกิจในปัจจุบันขยายวงกว้างเกินกว่าทรัพยากรที่มีอยู่เดิม ทั้งด้านบุคลากร งบประมาณ และเทคโนโลยี จึงเป็นปัจจัยให้ต้องปรับเปลี่ยนกระบวนการทำงาน โดยมุ่งเน้นการบูรณาการเพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิภาพยิ่งขึ้น และนำเทคโนโลยีที่ทันสมัยมาประยุกต์ใช้ เพื่อยกระดับคุณภาพการผลิตรายงานข่าวกรอง ให้สามารถแจ้งเตือนหน่วยประชาคมในทุกภาคส่วนได้อย่างเท่าทันต่อสถานการณ์

**ตารางที่ 2.1** บทบาทหน้าที่ของหน่วยงานประชาคมที่มีบทบาทนำในด้านข่าวกรองภัยคุกคามทางไซเบอร์

| หน่วยงาน | ขอบเขตภารกิจโดยสังเขป |
|---|---|
| สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) / ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thai CERT) | กำหนดนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ |
| ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) สำหรับหน่วยงาน CII ในภาคส่วนต่าง ๆ อาทิ ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) และ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) | เป็นศูนย์กลางในการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ ในกลุ่มสมาชิกที่เป็นหน่วยงาน CII ภาคการเงินการธนาคาร และภาคโทรคมนาคม เพื่อสร้างความตระหนักรู้ รวมทั้งประสานงานและรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่อสมาชิก รวมถึงองค์กรอื่น ๆ ที่เกี่ยวข้อง |
| กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท) และ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) | สืบสวนสอบสวนและปราบปรามอาชญากรรมทางเทคโนโลยีที่มีความซับซ้อน ด้วยความเชี่ยวชาญตามหน้าที่อำนาจและกฎหมายที่กำหนดโทษสำหรับอาชญากรรมทางเทคโนโลยี อาทิ ประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นอันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง |
| ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย และ กองข่าวกรองเทคนิคและเทคโนโลยีข่าวกรอง สำนักข่าวกรอง กรมข่าวทหาร | บูรณาการการพัฒนาขีดความสามารถด้านไซเบอร์ของกองทัพไทย ทั้งด้านกำลังพล ยุทโธปกรณ์ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งบูรณาการการปฏิบัติการทางไซเบอร์เข้ากับการปฏิบัติการทางทหารในมิติอื่น ๆ ในลักษณะการปฏิบัติการร่วมได้อย่างมีประสิทธิภาพ |
| สำนักข่าวกรองแห่งชาติ (สขช.) | ปฏิบัติการข่าวกรองและต่อต้านข่าวกรอง ทั้งในและต่างประเทศ รวมถึงปฏิบัติการข่าวกรองและต่อต้านข่าวกรองทางการสื่อสาร (SIGINT) |

**2.2.2.3 แบบอย่างของการจัดตั้งศูนย์ประสานข่าวกรองทางไซเบอร์ในต่างประเทศ**

การบูรณาการความร่วมมือด้านข่าวกรองทางไซเบอร์เป็นสิ่งจำเป็น และหลายประเทศให้ความสำคัญ เพราะเป็นแนวทางที่จะทำให้เกิดความร่วมมือระหว่างองค์กรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่มีความเชี่ยวชาญเฉพาะด้านแตกต่างกันไปตามภารกิจขององค์กร ซึ่งหากบูรณาการได้สำเร็จจะทำให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิภาพ และเป็นปัจจัยบวกต่อการพัฒนาศักยภาพเครือข่ายหน่วยงานภาครัฐได้อย่างเป็นองค์รวม ตามแนวคิด collaborative government โดยมีตัวอย่างของการบูรณาการภารกิจศูนย์ประสานข่าวกรองทางไซเบอร์ของต่างประเทศ ที่ไทยสามารถนำมาใช้เป็นแบบอย่างในการดำเนินงานจัดตั้งหน่วยงานบูรณาการ ได้ดังนี้

**1) Cyber Threat Intelligence Integration Center (CTIIC) ของสหรัฐฯ** รัฐบาลสหรัฐฯ จัดตั้งศูนย์บูรณาการข่าวกรองภัยคุกคามทางไซเบอร์ เพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์สำหรับผู้กำหนดนโยบายของสหรัฐฯ รวมถึงภัยคุกคามทางไซเบอร์จากต่างประเทศและภัยคุกคามต่อผลประโยชน์ของสหรัฐฯ เพื่อให้มีการประเมินข่าวกรองภัยคุกคามทางไซเบอร์ที่ประสานงานกัน และแบ่งปันข้อมูลอย่างทันท่วงที เมื่อเผชิญกับเหตุการณ์และการละเมิดความปลอดภัยทางไซเบอร์ โดย CTIIC ทำงานร่วมกับหน่วยงานต่าง ๆ ในสหรัฐฯ เพื่อสร้างขีดความสามารถแบบบูรณาการ ในการปกป้องประเทศจากภัยคุกคามทางไซเบอร์ ซึ่ง CTIIC จะดำเนินการค้นคว้า วิเคราะห์ วิจัย รวมข้อมูลข่าวกรองทางไซเบอร์ และสนับสนุนข้อมูลเพื่อบรรเทาภัยคุกคาม ประสานงาน บูรณาการ รวมถึงสร้างความร่วมมือเชิงนวัตกรรมและความสามารถ และแบ่งปันข้อมูลที่เกี่ยวข้องกับการสอบสวนภัยคุกคามทางไซเบอร์ภายในสหรัฐอเมริกา และกองบัญชาการไซเบอร์ของสหรัฐฯ ในการปกป้องประเทศจากการโจมตีทางไซเบอร์ครั้งสำคัญ

**2) Cyber and Critical Technology Intelligence Centre (CCTIC) ของออสเตรเลีย** ศูนย์ข่าวกรองไซเบอร์และเทคโนโลยีที่สำคัญของประเทศออสเตรเลีย ทำงานร่วมกับพันธมิตรขับเคลื่อนนวัตกรรมและนำเสนอข้อมูลเชิงลึก ที่เกี่ยวกับโลกไซเบอร์และเทคโนโลยีสำคัญ เพื่อสนับสนุนการตัดสินใจที่ซับซ้อนของทางรัฐบาล ลักษณะสำคัญของงานคือการใช้ความเชี่ยวชาญด้านไซเบอร์และเทคโนโลยีเพื่อประเมินข่าวกรองจากแหล่งข้อมูลที่มีทั้งหมด ศูนย์ตั้งเป้าหมายที่จะเป็นกระบอกเสียงประชาสัมพันธ์และได้รับความไว้วางใจในประเด็นทางไซเบอร์และเทคโนโลยี ปัจจุบันดำเนินการลงทุนในนวัตกรรมและการวิจัยเพื่อพัฒนาข้อมูลเชิงลึกด้านข่าวกรองทางไซเบอร์ และให้ข้อมูลการประเมินแก่ผู้มีอำนาจตัดสินใจระดับสูงของประเทศ ศูนย์ยังมีเป้าหมายเพื่อส่งเสริมความร่วมมือกับพันธมิตร ด้านการวิจัยและพัฒนาร่วมกับหน่วยงานที่ไม่ใช่ภาครัฐ ช่วยจัดหาทุน กำหนดรูปแบบและปรับใช้วิทยาศาสตร์การวิจัยและเทคโนโลยีขั้นสูง เพื่อสร้างความยืดหยุ่นของประเทศต่อภัยคุกคามที่กำลังพัฒนาไปข้างหน้าอย่างต่อเนื่อง

**3) Cybersecurity Collaboration Center in Pangyo ของเกาหลีใต้** สำนักข่าวกรองสาธารณรัฐเกาหลีใต้ (NIS) เปิดศูนย์ความร่วมมือด้านความปลอดภัยทางไซเบอร์ ออกแบบมาเพื่อกำหนดระบบการตอบสนองต่อวิกฤติทางไซเบอร์อย่างเป็นระบบ และครอบคลุมกฎหมายที่เกี่ยวข้อง ส่งเสริมการแบ่งปันข้อมูลระหว่างภาคเอกชนและภาครัฐเกี่ยวกับ ความปลอดภัยทางไซเบอร์และการทำงานร่วมกันเพื่อตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับชาติ ศูนย์แห่งนี้จะรวบรวมผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ทั้งจากภาครัฐและเอกชนมาไว้ในที่เดียว โดยมีเป้าหมายร่วมกันในการตอบสนองต่อภัยคุกคามทางไซเบอร์ ภายในศูนย์จะมีสิ่งอำนวยความสะดวกต่าง ๆ เช่น ห้องวิเคราะห์ ห้องแบ่งปันเทคโนโลยี และพื้นที่ฝึกอบรมด้านการศึกษา ศูนย์ดังกล่าวจะมีบทบาทช่วยผู้เชี่ยวชาญที่เข้ามาทำงานร่วมกัน ยิ่งไปกว่านั้น

สำนักข่าวกรองเกาหลีใต้ วางแผนที่จะพัฒนาระบบการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ระดับชาติ และเพิ่มกลุ่มผู้เข้าร่วมเป็นสองเท่าในอนาคต

**ตารางที่ 2.2** สรุปตัวอย่างภารกิจของศูนย์ประสานข่าวกรองทางไซเบอร์ในต่างประเทศ

| หน่วยงาน | จุดเด่น |
|---|---|
| Cyber Threat Intelligence Integration Center (CTIIC) ของสหรัฐฯ | แบ่งปันข้อมูลที่เกี่ยวข้องกับการสอบสวนภัยคุกคามทางไซเบอร์ภายในสหรัฐอเมริกา และกองบัญชาการไซเบอร์ของสหรัฐฯ ในการปกป้องประเทศจากการโจมตีทางไซเบอร์ครั้งสำคัญ |
| Cyber and Critical Technology Intelligence Centre (CCTIC) ของออสเตรเลีย | มีการใช้ความเชี่ยวชาญด้านไซเบอร์และเทคโนโลยีเพื่อประเมินข่าวกรองจากแหล่งข้อมูลที่มีทั้งหมด โดยปัจจุบันดำเนินการลงทุนในนวัตกรรมและการวิจัยเพื่อพัฒนาข้อมูลเชิงลึกด้านข่าวกรองทางไซเบอร์ |
| Cybersecurity Collaboration Center in Pangyo ของเกาหลีใต้ | รวบรวมผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ทั้งจากภาครัฐและเอกชนมาไว้ในที่เดียว โดยมีเป้าหมายร่วมกันในการตอบสนองต่อภัยคุกคามทางไซเบอร์ ภายในศูนย์จะมีสิ่งอำนวยความสะดวก เช่น ห้องวิเคราะห์ ห้องแบ่งปันเทคโนโลยี และพื้นที่ฝึกอบรมด้านการศึกษา |

**2.2.3 แนวทางในการแก้ไขปัญหาหรือพัฒนานโยบายที่สอดคล้องกับการวิเคราะห์**

จากการวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ข้างต้น ที่ประกอบด้วยปัญหาความท้าทาย สภาพปัญหา ผลกระทบที่เกิดขึ้น รวมทั้งหลักการแนวคิดในการกำหนดข้อเสนอเชิงนโยบายเกี่ยวกับการบูรณาการเครือข่ายประชาคมข่าวกรองทางไซเบอร์ ผู้ศึกษามีข้อเสนอแนวทางในการแก้ไข ดังนี้

**2.2.3.1 จัดตั้งเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ระหว่างหน่วยงาน**

มาตรา 5 ของ พ.ร.บ.ข่าวกรองแห่งชาติ พ.ศ.2562 กำหนดหน้าที่และอำนาจให้ สขช. เป็นศูนย์กลางประสานการข่าวกรอง การต่อต้านข่าวกรอง และการรักษาความปลอดภัยฝ่ายพลเรือนกับหน่วยข่าวกรองอื่นภายในประเทศ และเป็นหน่วยข่าวกรองหลักในการประสานกิจการการข่าวกรอง การต่อต้านข่าวกรองกับหน่วยข่าวกรองต่างประเทศ ในเรื่องที่เกี่ยวกับความมั่นคงแห่งชาติ นอกจากนี้ ในมาตรา 12 และ 13 กำหนดให้ สขช. จัดตั้งศูนย์ประสานข่าวกรองแห่งชาติ (ศป.ข.) ปฏิบัติภารกิจข้างต้น รวมถึงให้ความรู้และประสานความร่วมมือด้านการข่าวกับภาครัฐ ภาคเอกชน และประชาชน จึงกำหนดเป้าหมายสร้างเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ ในระยะ 5 ปี ดังนี้

**ระยะปีที่ 1** จัดตั้งหน่วยงานบูรณาการข่าวกรองไซเบอร์ไม่น้อยกว่า 2 หน่วยงาน ได้แก่ สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) และกระทรวงการต่างประเทศ (กต.) เนื่องจากเป็นองค์กรหลักในระดับนโยบายความมั่นคงของประเทศ อีกทั้งยังเป็นองค์กรที่ตกเป็นเป้าหมายของการโจมตีทางไซเบอร์อย่างต่อเนื่อง นอกจากนั้นยังมีการประสานงานกับ สขช. อย่างต่อเนื่อง

**ระยะปีที่ 2** จัดตั้งหน่วยงานบูรณาการไปยังภาครัฐและเอกชนอื่น ที่อยู่นอกกลุ่มหน่วยงาน CII ด้านความมั่นคง จำนวนไม่น้อยกว่า 2 หน่วยงาน ได้แก่ ธนาคารแห่งประเทศไทย และ บมจ.โทรคมนาคมแห่งชาติ เนื่องจากเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศระดับประเทศ หากถูกโจมตีทางไซเบอร์จะก่อให้เกิดความเสียหายด้านเศรษฐกิจอย่างสูง

**ระยะปีที่ 3** บูรณาการไปยังหน่วยงานความมั่นคงในต่างประเทศ โดยกำหนดไว้ 2 แห่ง คือ นอกภูมิภาค ASEAN ได้แก่ สหรัฐฯ และสหราชอาณาจักร ส่วนในภูมิภาค ASEAN กำหนดไว้อย่างน้อย 2 ประเทศ ซึ่งทั้งหมดเป็นหน่วยข่าวกรองมิตรประเทศที่มีการประสานงานกับ สขช. มาอย่างต่อเนื่อง

**ระยะปีที่ 4 – 5** จัดตั้งหน่วยงานบูรณาการกับหน่วยงานภายในประเทศเพิ่มขึ้นอย่างน้อย 1 หน่วยงาน

**2.2.3.2 กำหนดช่องทางการสื่อสาร หรือพัฒนาเชื่อมโยงแพลตฟอร์มแลกเปลี่ยนข้อมูลข่าวกรองทางไซเบอร์**

การโจมตีทางไซเบอร์เกิดขึ้นอยู่อย่างต่อเนื่องโดยไม่จำกัดห้วงเวลา เพราะผู้โจมตีจะปรับเปลี่ยนกลยุทธ์ เทคนิค และกรรมวิธี (Tactics, Technique and Procedures – TTPS) เรื่อยไปจนกว่าจะบรรลุผลสำเร็จ ดังนั้น จึงควรกำหนดช่องทางการสื่อสาร หรือการพัฒนาระบบการแจ้งเตือนข่าวกรองทางไซเบอร์ให้หน่วยงานที่บูรณาการกัน ผ่านช่องทางการสื่อสารที่เหมาะสม ปลอดภัยและสะดวก เพื่อให้กระบวนการแจ้งเตือนเป็นไปอย่างรวดเร็ว และหน่วยงานในเครือข่ายสามารถนำข้อมูลไปพิจารณาใช้ประโยชน์โดยไม่มีข้อจำกัดด้านเวลา ตัวอย่างเช่น การพัฒนาแพลตฟอร์มแลกเปลี่ยนข้อมูลมัลแวร์ หรือ Malware Information Sharing Platform (MISP) ซึ่งเป็นระบบที่อำนวยความสะดวกให้ศูนย์ CSOC ของแต่ละหน่วยงานสามารถบันทึกข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ที่ตรวจพบ และใช้เป็นฐานข้อมูลกลางในการแลกเปลี่ยนกับหน่วยงานทั้งในและต่างประเทศ ได้อย่างสะดวกรวดเร็ว ทั้งข้อมูลเชิงเทคนิค (low level) และรายงานเชิงวิเคราะห์ (high level) ซึ่งจะขับเคลื่อนการพัฒนาระบบ MISP เพื่อเชื่อมโยงกับแพลตฟอร์มของหน่วยงานที่บูรณาการตามข้อ 2.2.3.1 หรืออาจจะเป็นช่องทางสื่อสารหรือแพลตฟอร์มอื่น ๆ ก็ได้

**2.2.3.3 พัฒนากลยุทธ์การสร้างสัมพันธ์ระหว่างหน่วยงานที่บูรณาการทั้งระดับ นโนบาย และระดับปฏิบัติ**

เพื่อให้การดำเนินการด้านการบูรณาการข่าวกรองทางไซเบอร์ เป็นไปอย่างมีประสิทธิภาพ การพัฒนากลยุทธ์เพื่อสร้างความสัมพันธ์ที่ใกล้ชิดแน่นแฟ้นของหน่วยสมาชิกทั้งในระดับนโยบาย และระดับผู้ปฏิบัติ ต้องมีอย่างต่อเนื่อง โดยอาจพิจารณาดำเนินการผ่านกลไกดังต่อไปนี้

**1) การจัดประชุมตามสถานการณ์พิเศษ** กรณีเกิดเหตุการณ์โจมตีต่อระบบโครงสร้างพื้นฐานที่สำคัญของหน่วยงานสมาชิกในประชาคม หรือเหตุโจมตีที่สำคัญ ๆ ให้หน่วยงานสมาชิกขอเปิดการประชุมเฉพาะกรณีได้ และออกรายงานการรับมือกับเหตุโจมตีในนามคณะทำงานบูรณาการด้านไซเบอร์

**2) การจัดประชุมสถานการณ์ตามปกติ (เป็นไตรมาส)** เพื่อสรุปสถานการณ์ทางไซเบอร์ ทบทวนแผนงาน ผลการดำเนินงานของการบูรณาการประชาคมข่าวกรองทางไซเบอร์ โดยให้หน่วยงานในประชาคมร่วมนำเสนอข้อมูลรายงานการวิเคราะห์ ผลผลิตที่ได้จากการบูรณาการ องค์ความรู้ และเครื่องมือใหม่ ๆ

**3) จัดกิจกรรม Roadshow และกิจกรรมสัมพันธ์** ทั้งในระดับนโยบาย และเจ้าหน้าที่ผู้ปฏิบัติ เช่น เยี่ยมชมศูนย์ CSOC ของแต่ละหน่วยประชาคม โดยเริ่มต้นจากหน่วยงานภาครัฐในประเทศก่อนขยายไปสู่ภาคเอกชน หน่วยงานในระดับ ASEAN และหน่วยงานนอก ASEAN ตามลำดับ

**4) จัดงานเสวนาแลกเปลี่ยนองค์ความรู้ และสถานการณ์ข่าวสารเทคโนโลยีที่น่าสนใจ** เพื่อให้บุคลากรหน่วยงานในประชาคม ได้ใช้โอกาสแสดงความรู้ความสามารถหรือแลกเปลี่ยนเรียนรู้ระหว่างกัน รวมทั้งเป็นการสร้างสภาพแวดล้อมที่ดีให้ จนท. มีความภูมิใจในการปฏิบัติงานตามภารกิจทางไซเบอร์

**ตารางที่ 2.3** แผนขับเคลื่อนการบูรณาการเครือข่ายด้านข่าวกรองทางไซเบอร์ระยะ 5 ปี ของ สขช.

| แผนงาน/กิจกรรม | ปีที่ 1 | ปีที่ 2 | ปีที่ 3 | ปีที่ 4 -5 |
|---|---|---|---|---|
| **1. จัดตั้งหน่วยงานบูรณาการข่าวกรองทางไซเบอร์** | | | | |
| 1.1 จัดตั้งเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ กับหน่วยงานภายในประเทศ ไม่น้อยกว่า 2 แห่ง | ✓ | | | |
| 1.2 จัดตั้งเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ กับหน่วยงาน CII นอกกลุ่มความมั่นคง ไม่น้อยกว่า 2 แห่ง | | ✓ | | |
| 1.3 จัดตั้งเครือข่ายแลกเปลี่ยนข่าวกรองทางไซเบอร์กับหน่วยข่าวมิตรประเทศใน ASEAN 2 แห่ง และนอก ASEAN 2 แห่ง คือ สหรัฐฯ และสหราชอาณาจักร | | ✓ | ✓ | |
| 1.4 จัดตั้งเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ กับหน่วยงานภาครัฐหรือเอกชนอื่น เพิ่มขึ้นอย่างน้อย 1 แห่ง | | | | ✓ |
| **2. กำหนดช่องทางสื่อสารหรือเชื่อมโยงแพลตฟอร์มแลกเปลี่ยนข้อมูลข่าวกรองทางไซเบอร์** | | | | |
| 2.1 เชื่อมโยงแพลตฟอร์มกับหน่วยงาน 2 แห่ง (สมช. และ กต.) | ✓ | | | |
| 2.2 เชื่อมโยงแพลตฟอร์มกับหน่วยงาน CII นอกกลุ่มความมั่นคง อย่างน้อย 2 แห่ง (ธปท. และ บมจ. โทรคมนาคมแห่งชาติ) | | ✓ | | |
| 2.3 กำหนดระบบแลกเปลี่ยนข่าวสารกับหน่วยข่าวมิตรประเทศ จำนวน 4 แห่ง | | | ✓ | ✓ |
| **3. พัฒนากลยุทธ์การสร้างสัมพันธ์ระหว่างหน่วยงานที่บูรณาการทั้งระดับ นโนบาย และระดับปฏิบัติ** | | | | |
| 3.1 จัดประชุมตามสถานการณ์พิเศษ | ✓ | ✓ | ✓ | ✓ |
| 3.2 การจัดประชุมสถานการณ์ตามปกติรายไตรมาส | ✓ | ✓ | ✓ | ✓ |
| 3.3 จัดกิจกรรม Roadshow และกิจกรรมสัมพันธ์ | ✓ | ✓ | ✓ | ✓ |
| 3.4 จัดงานเสวนาแลกเปลี่ยนองค์ความรู้ และสถานการณ์ข่าวสารเทคโนโลยีที่น่าสนใจ | ✓ | ✓ | ✓ | ✓ |

ทั้งนี้ ภายหลังการดำเนินการตามแนวทางการพัฒนาดังกล่าวข้างต้น จะช่วยยกระดับศักยภาพในภารกิจการป้องกันภัยคุกคามทางไซเบอร์ให้มีประสิทธิภาพสูงขึ้น สามารถนำข้อมูลข่าวสาร และข่าวกรองที่สำคัญไปใช้สืบสวนขยายผล ระงับยับยั้ง ลดระดับความเสียหาย ที่อาจเกิดขึ้นกับหน่วยงานเครือข่ายบูรณาการ รวมทั้งผลประโยชน์ความมั่นคงของชาติ และประชาชน โดยผู้ศึกษาขอนำเสนอสรุปผลการเปรียบเทียบการดำเนินการก่อนและหลัง การสร้างเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ (AS – IS / TO - BE) ดังนี้

**ตารางที่ 2.4** เปรียบเทียบการดำเนินการก่อนและหลังการจัดตั้ง (AS – IS / TO -BE)

| AS – IS | แนวทางการพัฒนา | TO –BE |
|---|---|---|
| สขช. ดำเนินการรวบรวมข้อมูลข่าวสารและปฏิบัติการทางไซเบอร์เฉพาะหน่วยตนเอง | จัดตั้งหน่วยงานเป็นเครือข่ายบูรณาการข่าวกรองทางไซเบอร์ตามแผน 5 ปี | มีหน่วยงานที่เกี่ยวข้องอื่นทั้งในและต่างประเทศ แลกเปลี่ยนข้อมูลและร่วมปฏิบัติการต่อต้านภัยคุกคามทางไซเบอร์ |
| ปัจจุบันยังไม่มีช่องทางหรือแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวสารสำคัญทางไซเบอร์ เพื่อการใช้ประโยชน์ข้อมูลในกระบวนการข่าวกรองทางไซเบอร์ | กำหนดช่องทางสื่อสารหรือพัฒนา/กำหนดแพลตฟอร์มเชื่อมโยงแลกเปลี่ยนข้อมูลข่าวกรองทาง ไซเบอร์ | หน่วยงานที่บูรณาการมีช่องทางสื่อสารเฉพาะสำหรับแลกเปลี่ยนแจ้งเตือน หรือการนำข้อมูลไปใช้ประโยชน์ในการต่อต้านและป้องกันภัยคุกคามทางไซเบอร์ |
| ความไว้วางใจและความร่วมมือในการแลกเปลี่ยนข้อมูลข่าวกรองทางไซเบอร์ อยู่ในระดับเบื้องต้น ไม่มีความสัมพันธ์เชิงลึก | พัฒนากลยุทธ์การสร้างสัมพันธ์ระหว่างหน่วยงานที่บูรณาการทั้งระดับ นโนบาย และระดับปฏิบัติ | หน่วยงานและบุคลากรของเครือข่ายบูรณาการมีความร่วมมือด้านข่าวสาร ด้านการปฏิบัติการ ด้านเทคโนโลยี และการพัฒนาบุคลากรทางไซเบอร์ |

**2.2.4 ปัจจัยที่อาจมีผลกระทบต่อความสำเร็จของการพัฒนาและแนวทางบริหารจัดการ**

ปัจจัยสำคัญที่อาจมีผลกระทบต่อความความสำเร็จ ในการบูรณาการเครือข่ายข่าวกรองทางไซเบอร์ มีดังนี้

**2.2.4.1 ปัญหาด้านงบประมาณ**

ในการบริหารโครงการที่มีแผนงานเกี่ยวข้องกับการบูรณาการ หรือการประสานงานร่วมกับหลายหน่วยงาน ต้องใช้งบประมาณสูง เนื่องจากมีความจำเป็นในการจัดกิจกรรม การประชุม และการพัฒนาสัมพันธ์ทั้งในระดับองค์กรและระดับบุคคล หากมีการเปลี่ยนแปลงในระดับนโยบายด้านการเงินอาจส่งผลกระทบให้ไม่สามารถคงสถานะความเป็นคณะทำงานได้ เพราะได้รับจัดสรรงบประมาณไม่เพียงพอ

**แนวทางบริหารจัดการ: ใช้กลไกของ ศป.ข. ช่วยบริหารจัดการในระยะแรกของการจัดตั้งคณะบูรณาการ** โดย สขช. จะต้องแสดงให้หน่วยประชาคมมองเห็นโอกาส และประโยชน์จากช่องทางของคณะบูรณาการ เพื่อดึงดูดให้หน่วยงานในประชาคมต้องการเข้าร่วม และคงสถานะในการเป็นคณะบูรณาการ เกิดการปฏิบัติการร่วม เพื่อสร้างผลผลิตด้านการข่าวกรองทางไซเบอร์ แจกจ่ายให้กับหน่วยงานในประชาคมข่าวกรอง เมื่อผลผลิตที่ได้จากคณะบูรณาการแสดงผลลัพธ์เชิงประจักษ์ จะทำให้เหตุผลความจำเป็นในการขอสนับสนุนงบประมาณมีความเหมาะสมต่อไป รวมทั้งเร่งผลักดันให้มีการเสนอแผนงานโครงการบูรณาการของหน่วยงานประจำปี

**2.2.4.2 ปัญหาความร่วมมือในการเชื่อมโยงระบบสารสนเทศระหว่างหน่วยงาน**

หลายครั้งเมื่อมีการพัฒนาระบบสารสนเทศ เพื่อการแบ่งปันข้อมูลระหว่างหน่วยงาน กลับไม่มีการผลักดันในระดับนโยบายเพื่อนำไปสู่การขับเคลื่อนในระดับปฏิบัติ ส่งผลให้ระบบถูกทิ้งร้าง

เนื่องจากไม่มีหน่วยงานใดนำข้อมูลสำคัญบันทึกลงในระบบ เมื่อมีข้อมูลไม่เพียงพอหรือข้อมูลไม่มีคุณภาพจะส่งผลให้ไม่มีผู้เข้าใช้งานระบบ รวมทั้งระบบไม่สามารถแสดงผลลัพธ์ได้ตรงตามวัตถุประสงค์ ส่งผลต่อการขับเคลื่อนคณะทำงานเป็นไปอย่างยากลำบาก เนื่องจากหน่วยงานต่าง ๆ ไม่ยอมเปิดเผยข้อมูลที่มีคุณภาพต่อการนำไปวางแผนและใช้ประโยชน์ ต่อมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน

**แนวทางบริหารจัดการ: ผลักดันให้หน่วยงานประชาคมใช้งานระบบ MISP** หรือแพลตฟอร์มอื่น ๆ ที่กำหนดร่วมกัน โดยอาจจัดทำในลักษณะตัวชี้วัดผลการดำเนินงาน จัดทำรายงานเชิงสถิติว่าหน่วยงานใดเข้าบันทึกข้อมูล และสามารถใช้ประโยชน์จากระบบได้มากน้อยตามลำดับ นอกจากนี้ ยังมีความจำเป็นต้องผลักดันให้กรอบการทำงานเชิงบูรณาการด้านข่าวกรองทางไซเบอร์ ถูกบรรจุเข้าไปอยู่ในแผนงานโครงการของหน่วยงาน รวมทั้งการสร้างคุณภาพของรายงานข่าวกรอง และข้อมูลที่นำไปแชร์ เพื่อให้หน่วยงานเห็นความสำคัญและประโยชน์ที่จะได้รับ จากการประสานความร่วมมือและบูรณาการข่าวกรองทางไซเบอร์

**2.2.4.3 ปัญหาความไว้วางใจ**

เป็นปัญหาหลักที่สำคัญ สำหรับการบรูณาการด้านข่าวกรองทางไซเบอร์ระหว่างประชาคม เนื่องจากปัญหาภัยคุกคามทางไซเบอร์เป็นปัญหาที่กระทบต่อระบบสารสนเทศในองค์กร และมักเกี่ยวข้องกับข้อมูลอ่อนไหว ซึ่งกระทบต่อชื่อเสียงและความน่าเชื่อถือของหน่วยงานที่ตกเป็นเป้าโจมตี และอาจส่งผลให้หน่วยงานถูกฟ้องร้องและดำเนินคดี หากมีข้อมูลของหน่วยงานรั่วไหลสู่สาธารณะ หลายหน่วยงานจึงเลือกที่จะปิดบังปัญหา และนำเสนอเฉพาะส่วนที่เป็นประโยชน์ต่อหน่วยงานเท่านั้น

**แนวทางบริหารจัดการ: จัดทำข้อกำหนดมาตรฐานในการเก็บรักษาหรือเปิดเผยข้อมูลระหว่างสมาชิกคณะทำงาน** โดยให้เป็นข้อตกลงที่ยอมรับร่วมกันทุกฝ่าย เพื่อสร้างความมั่นใจว่าข้อมูลอ่อนไหวที่ส่งผลกระทบต่อหน่วยงาน จะไม่รั่วไหลหรือถูกนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาต นำไปสู่ความไว้ใจระหว่างหน่วยงานให้กล้าที่จะเปิดเผยข้อมูลของตนเองมากขึ้น

**2.2.4.4 ปัจจัยแห่งความสำเร็จ (Key Success Factors)** ปัจจัยแห่งความสำเร็จในการดำเนินการตามข้อเสนอ ได้แก่ จนท.ระดับนโยบายและระดับปฏิบัติ ต้องมีวิสัยทัศน์/ทัศนคติที่เห็นถึงความจำเป็นความสำคัญในภารกิจด้านไซเบอร์ การได้รับความร่วมมือจากหน่วยงานต่าง ๆ ที่เกี่ยวข้องในการบูรณาการและการได้รับการสนับสนุนในการแลกเปลี่ยนข้อมูลข่าวสาร และข่าวกรองที่มีความสำคัญมีคุณภาพ

## 2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ

การบูรณาการกับหน่วยงานต่าง ๆ มีความจำเป็นต้องใช้ความเป็นผู้นำที่มีสมรรถนะด้านการบูรณาการ การรับฟังความคิดเห็น โดยเฉพาะอย่างยิ่งการปรับตัวได้ดีในสภาพแวดล้อมที่มีการเปลี่ยนแปลง มีความท้าทายซับซ้อนของงานที่เกิดขึ้นตลอดเวลา รวมถึงสามารถแก้ไขปัญหาเฉพาะหน้าได้ดี ดังนั้นผู้นำการขับเคลื่อนข้อเสนอ จึงจะต้องมีคุณลักษณะและทักษะที่จำเป็น ดังนี้

### 2.3.1 ทักษะทางเทคนิค

ใช้เมื่อรู้อย่างแน่ชัดว่าปัญหานั้นคือสิ่งใด ต้องมีทางออกชัดเจน ทั้งนี้ ทักษะทางเทคนิค คือสิ่งที่มาพร้อมกับการเข้ารับการศึกษา การเข้ารับการฝึกอบรมเฉพาะทางในด้านต่าง ๆ

### 2.3.2 ทักษะในการปรับตัว

ใช้เมื่อไม่รู้แน่ชัดว่าปัญหานั้นคือสิ่งใด ไม่มีคำตอบสำหรับการแก้ไขปัญหาอย่างแน่นอน จะต้องมีการนำเอาองค์ความรู้มาประยุกต์ใช้เพื่อช่วยในการแก้ไขปัญหา โดยมากปัญหามักเกิดขึ้นโดยไม่คาดคิด จึงทำ

ให้ไม่สามารถเตรียมหนทางแก้ไขปัญหาได้ทัน สิ่งจำเป็นสำหรับทักษะการปรับตัวคือ ความสามารถในการสื่อสารในรูปแบบต่าง ๆ ให้เหมาะสมกับคู่สนทนา

**2.3.3 ทักษะการรับรู้ภายใน (inner work)**

เป็นทักษะการตระหนักรู้ในตนเอง นักวิจัยด้านความฉลาดทางอารมณ์ค้นพบว่า ทักษะดังกล่าวเป็นสิ่งบ่งชี้ประสิทธิภาพของการเป็นผู้นำที่ดี เนื่องจากผู้นำที่มีความฉลาดทางอารมณ์สูง จะสามารถนำพาให้เกิดผลผลิตและผลกำไรได้ในระดับสูง การรับรู้ภายในทำให้ผู้นำสามารถอ่านสถานการณ์ภายนอกได้อย่างถูกต้อง ในการจัดตั้งคณะทำงานการบูรณาการเครือข่ายประชาคมข่าวกรองทางไซเบอร์ จะต้องทำงานร่วมกับหลายภาคส่วน ซึ่งมีองค์ประกอบและวัฒนธรรมองค์กรที่แตกต่างกันอย่างสิ้นเชิง อีกทั้งงานด้านความมั่นคงปลอดภัยไซเบอร์เป็นงานที่มีความเครียดและความกดดันในระดับสูง เนื่องจากต้องแบกรับความคาดหวังขององค์กร และมักเป็นงานที่หลายคนมองข้ามและไม่ให้ความสำคัญ ดังนั้น ผู้นำในการบริหารจัดการคณะทำงานดังกล่าวจะต้องเป็นผู้ที่มีความฉลาดทางอารมณ์ สามารถอ่านสถานการณ์ได้อย่างถูกต้อง จัดการความขัดแย้งโดยไม่สร้างความแคลงใจ หรือผลกระทบให้กับฝ่ายหนึ่งฝ่ายใด รวมทั้งสามารถสร้างแรงจูงใจผลักดันให้บุคลากรเกิดความรู้สึกอยากมีส่วนร่วมในกิจกรรมของหน่วยงานอย่างเต็มใจ

**2.3.4 ทักษะการรับรู้ภายนอก (outer work)**

เป็นทักษะในการแสดงวิสัยทัศน์ พันธกิจ ค่านิยม และวัตถุประสงค์ของหน่วยงาน ว่ามีการวางแผนในการพัฒนาอย่างไร โดยวัดจากระดับความสำเร็จของงาน ทั้งในด้านประสิทธิภาพ การรับผิดชอบ การวัดผลได้ การมองเห็นได้ เป็นจุดเด่นของการรับรู้ภายนอก ซึ่งเป็นสิ่งสะท้อนถึงความสามารถในการบริหารจัดการภายในองค์กร

## 3. แผนพัฒนาตนเอง

**(ข้อมูลส่วนบุคคลไม่เผยแพร่)**

## บรรณานุกรม


*แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ.2561-2580).* (2566) : สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. สืบค้นจาก https://www.nesdc.go.th/ewt_news.php?nid=13651 เมื่อ 5 ก.ค.2566

Armis Security Ltd. (2023). *Better Cybersecurity with Alignment to the NIST Framework*. สืบค้นจาก https://www.armis.com/solutions/nist/ เมื่อ 31 ก.ค. 2566

Bonfanti , M. E. Cyber, Intelligence, and Security. In *Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice* (1st ed., Vol. 2). Tel Aviv, Israel , 2018 , pp. 105-118.

Böhm, Isabelle & Lolagar, Samuel. (2021). Open source intelligence: Introduction, legal, and ethical considerations. *International Cybersecurity Law Review.* 2. 10.1365/s43439-021-00042-7.

Cyber and Critical Technology Intelligence Centre. *Cyber and Critical Technology Intelligence Centre | Office of National Intelligence.* สืบค้นจาก https://www.oni.gov.au/national-intelligence-community/cctic เมื่อ 2 ก.ค. 2566

D. Fernández Vázquez, O. Pastor Acosta, C. Spirito, S. Brown and E. Reid, "Conceptual framework for cyber defense information sharing within trust relationships," *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia, 2012, pp. 1-17.

ENISA (2020). *ENISA unveils its New Strategy towards a Trusted and Cyber Secure Europe*. สืบค้นจาก https://www.enisa.europa.eu/news/enisa-news/enisa-unveils-its-new-strategy-on-cybersecurity-for-a-trusted-and-cyber-secure-europe เมื่อ 7 ส.ค.66

Fromiti. (2023). *Organized crime / cybercrime module 13 key issues: Criminal groups engaging in cyber organized crime.* สืบค้นจาก https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html เมื่อ 1 ก.ค. 2566

Hilbert, M. (2020). Digital technology and social change: the digital transformation of society from a historical perspective. *Dialogues in Clinical Neuroscience*, Jun 22(2), 189-194. doi: 10.31887/DCNS.2020.22.2/mhilbert. PMID: 32699519; PMCID: PMC7366943.

NT cyfence (2020). สรุปสถิติภัคุกคาม ปี 2565 จากศูนย์ CSOC ของ NT cyfense. สืบค้นจาก https://www.cyfence.com/article/2022-threat-statistics-summary-from-csoc-by-nt-cyfence/ เมื่อ 7 ส.ค.66

Thought Bridge. (2023). *Integrated Model of Leadership©: KI Thoughtbridge Adaptive Development.* สืบค้นจาก https://www.kithoughtbridge.com/about-us/integrated-model-of-leadership เมื่อ 1 ก.ค.2566

The National Counterintelligence and Security Center. (2023). *How We Work*. สืบค้นจาก https://www.dni.gov/index.php/ncsc-how-we-work/241-about/organization/cyber-threat-intelligence-integration-center เมื่อ 2 ก.ค. 2566

**ประวัติผู้เขียนเอกสารรายงานการศึกษาส่วนบุคคล**

**นายรัชภูมิ เวียงสิมา**

**ประวัติการศึกษา**

ปริญญาตรี อักษรศาสตร์บัณฑิต สาขาภาษาไทย มหาวิทยาลัยศิลปากร พ.ศ.2530

**ประสบการณ์การรับราชการ**

- ปี 2531 จนถึง 2558 ปฏิบัติหน้าที่ประจำ สำนักปฏิบัติการข่าวกรองและต่อต้านข่าวกรองในภาคตะวันออกเฉียงเหนือ
- ปี 2548 ปฏิบัติหน้าที่ เจ้าหน้าที่ซักถาม/หัวหน้าชุดซักถามประจำ ศูนย์วิวัฒน์สันติ จ.ปัตตานี กองอำนวยการรักษาความมั่นคงภายในภาค 4 (กอ.รมน.ภาค 4)
- ปี 2549 จนถึง 2558 ปฏิบัติหน้าที่ ประจำ ศูนย์ประสานข่าวกรองแห่งชาติ ภาค 3 (ศป.ข.ภาค 3)
- ปี 2558 จนถึง 2561 ปฏิบัติหน้าที่อัครราชทูตที่ปรึกษา ประจำสถานเอกอัครราชทูต ณ กรุงมะนิลา
- ปี 2563 นักการข่าวเชี่ยวชาญ ปฏิบัติหน้าที่ประจำสำนักปฏิบัติการข่าวกรองและต่อต้านข่าวกรองใน 5 จังหวัดชายแดนภาคใต้
- ปี 2564 จนถึงปัจจุบัน ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

**ตำแหน่งหน้าที่ปัจจุบันและสถานที่ทำงาน**

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักข่าวกรองแห่งชาติ