รายงานการศึกษาส่วนบุคคล

(Individual Study)

เรื่อง การพัฒนาศักยภาพบุคลากรของสำนักข่าวกรองแห่งชาติเพื่อป้องกันภัยคุกคามทางไซเบอร์

จัดทำโดย นายวัธนชัย ทองประเสริฐ

รหัส 92003

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 92

วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.

ประจำปี 2563

รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง การพัฒนาศักยภาพบุคลากรของสำนักข่าวกรองแห่งชาติ
เพื่อป้องกันภัยคุกคามทางไซเบอร์

จัดทำโดย นายวัธนชัย ทองประเสริฐ
รหัส 92003

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 92
วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.
ประจำปี 2563
รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา

สำนักงาน ก.พ.

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรมของสำนักงาน ก.พ.

อ.ระรินทิพย์ ศิโรรัตน์
อาจารย์ที่ปรึกษา

ดร.วิฑูรย์ สิมะโชคดี
อาจารย์ที่ปรึกษา

บทสรุปผู้บริหาร

ปัจจุบันความก้าวหน้าของเทคโนโลยีสื่อสารและเครือข่ายอินเตอร์เน็ต นอกจากก่อให้เกิดข้อมูลข่าวสารที่มีความหลากหลาย ปริมาณมาก คลุมเครือ และเปลี่ยนแปลงอย่างรวดเร็ว ยังเปลี่ยนกระบวนทัศน์ (Paradigm) ในกระบวนการทำงานด้านความมั่นคงอีกด้วย หน่วยงานความมั่นคงจึงเข้ามามีบทบาทสำคัญในการต่อต้านภัยคุกคามทางไซเบอร์ทั้งในเชิงรุกและเชิงรับ ซึ่งถือว่าเป็นภัยคุกคามใหม่ที่มีความซับซ้อนต่อการดำเนินการ หน่วยงานภาครัฐจึงจำเป็นต้องมีการปรับตัวหรือปฏิรูปองค์กรในด้านความสามารถของบุคลากรให้มีความเชี่ยวชาญและมีองค์ความรู้ที่หลากหลายและเฉพาะด้านมากยิ่งขึ้น

ถึงแม้ว่าสำนักข่าวกรองแห่งชาติมีการผลิตข่าวกรองเพิ่มขึ้นจากแหล่งข่าวเปิด (Open Source Intelligence) และการข่าวกรองทางไซเบอร์ (Cyber Intelligence) ที่ก้าวขึ้นมามีบทบาทสำคัญที่ทำให้กระบวนการรวบรวมและวิเคราะห์ข้อมูล การสืบสวน และการปฏิบัติการข่าวสาร มีความรวดเร็วและสมบูรณ์มากขึ้น แต่วิธีการรวบรวมข่าวสาร โดยการจัดหาและการพัฒนาเครื่องมือทางเทคนิคเข้ามาใช้งานมีความจำเป็นต้องเท่าทันเทคโนโลยีที่ก้าวหน้าอย่างต่อเนื่อง อาทิ การนำเทคโนโลยีปัญญาประดิษฐ์เข้ามาสนับสนุนภารกิจการข่าวกรอง และการต่อต้านข่าวกรอง เพื่อเป็นการพัฒนากระบวนการทำงานข่าวกรองให้มีขีดความสามารถเชิงรุก ตอบสนองความต้องการของผู้ใช้ข่าวได้อย่างมีประสิทธิภาพ รวมถึงการประเมินภัยคุกคามที่อาจส่งผลกระทบต่อความมั่นคงของชาติและความสงบเรียบร้อยของประเทศ ตลอดจนทำให้ สำนักข่าวกรองแห่งชาติ เป็นศูนย์กลางองค์กรของรัฐที่ทำหน้าที่บูรณาการงานข่าวกรอง ประสานกิจการข่าวกรอง การต่อต้านข่าวกรอง ทั้งในและนอกประเทศได้อย่างมีประสิทธิภาพ นำไปสู่การพัฒนาและส่งเสริมมาตรฐานการรักษาความปลอดภัยของหน่วยงานภาครัฐฝ่ายพลเรือน และปฏิบัติตามภารกิจที่สามารถป้องกัน และแก้ไขสถานการณ์ในกรณีที่มีเหตุฉุกเฉินรุนแรงได้ ตามวิสัยทัศน์ของสำนักข่าวกรองแห่งชาติ คือ “เป็นหน่วยข่าวกรองที่ทันสมัยเพื่อความมั่นคงของชาติและประชาชน”

การกำหนดแนวทางในการพัฒนาบุคลากรด้านไซเบอร์ จำเป็นต้องสอดรับกับสภาพปัญหา ความท้าทาย และความจำเป็นต่าง ๆ ในการพัฒนาศักยภาพบุคลากรเพื่อนำไปสู่การป้องกันภัยคุกคามทางไซเบอร์ ซึ่งความท้าทายที่เห็นได้ชัดในปัจจุบัน คือ การพัฒนาบุคลากรด้านไซเบอร์ที่ทำงานด้านไซเบอร์อย่างแท้จริง ตามความหมายของงานข่าวกรองในปัจจุบัน ที่มีจำนวนบุคลากรด้านไซเบอร์น้อยมากเมื่อเทียบกับจำนวนกำลังพลส่วนใหญ่ในหน่วยงาน อีกทั้งยังมีข้อจำกัดด้านประสบการณ์ ความเชี่ยวชาญในการสืบสวน การวิเคราะห์ข้อมูล ในขณะที่บุคลากรเดิมจะมีข้อได้เปรียบด้านประสบการณ์ และมีความสามารถในการวิเคราะห์แจ้งเตือนภัยคุกคาม แต่ยังจำเป็นต้องพัฒนาศักยภาพของตนเอง เพื่อให้เท่าทันการเปลี่ยนแปลงของเทคโนโลยีและเครื่องมือดิจิทัลต่างๆ เพื่อนำไปสู่การประเมินภัยคุกคามเชิงลึกทางการข่าว จึงเป็นเหตุผลหลักที่ทำให้เกิดความไม่พร้อมของ

หน่วยงานต่อการรับมือกับภารกิจด้านการป้องกันภัยคุกคามทางไซเบอร์ ด้วยเหตุนี้การกำหนดองค์ความรู้ ความสามารถ ทักษะ และสมรรถนะมาตรฐานของบุคลากรทางด้านไซเบอร์จึงเป็นส่วนสำคัญในลำดับแรก หากต้องการสร้างหน่วยงานให้บรรลุเป้าประสงค์ ทั้งนี้สิ่งสำคัญที่สุด ได้แก่ การเตรียมบุคลากรให้มีความพร้อมทั้งในด้านความรู้ความสามารถ ทักษะการใช้งานอุปกรณ์และระบบเครือข่าย รวมไปถึงเครื่องมือทางเทคนิคที่มีอยู่ในปัจจุบัน

อย่างไรก็ดี บุคลากรทั้งหมดยังคงอยู่บนหลักนิยมของการปฏิบัติงานด้านการข่าวขององค์กร ซึ่งมุ่งส่งเสริมให้เจ้าหน้าที่ต้องเป็นผู้ที่มีความยืดหยุ่นสูง สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ มีความรู้ที่หลากหลาย เพื่อตอบสนองต่อภารกิจ การปฏิบัติงานตามสถานการณ์เฉพาะกิจหรือสถานการณ์ฉุกเฉินได้ตลอดเวลา และตอบสนองต่อความต้องการของผู้ใช้ข่าว รวมถึงต้องเผชิญกับความคาดหวังจากสาธารณะมากขึ้น ทั้งทางด้านประสิทธิภาพ ความเร็ว ความถูกต้อง และการวิเคราะห์ข้อมูลเชิงลึก ซึ่งจำเป็นที่จะต้องมีเจ้าหน้าที่ที่มีศักยภาพทั้งด้านทางการข่าวและทางเทคนิคในการประเมินสภาพแวดล้อมทางยุทธศาสตร์บนพื้นฐานของข้อเท็จจริง เพื่อแจ้งเตือนล่วงหน้าต่อผู้กำหนดนโยบายทั้งในระดับองค์กรและรัฐบาล ให้สามารถกำหนดแนวทางปฏิบัติหรือนโยบายเพื่อรักษาผลประโยชน์แห่งชาติและความมั่นคง ตามที่นายกรัฐมนตรีได้มีข้อสั่งการ เมื่อตุลาคม 2560 ให้ปฏิรูประบบงานข่าวกรอง เพื่อให้เกิดความเชื่อมั่นว่าหน่วยงานด้านการข่าวสามารถดูแลและรักษาความสงบเรียบร้อยของประเทศไว้ได้

กิตติกรรมประกาศ

การจัดทำรายงานการศึกษาส่วนบุคคล (Individual Study) เรื่อง การพัฒนาศักยภาพบุคลากรของสำนักข่าวกรองแห่งชาติเพื่อป้องกันภัยคุกคามทางไซเบอร์ สำเร็จได้ด้วยความกรุณาอย่างยิ่งจาก อ.ระรินทิพย์ ศิโรรัตน์ และ ดร.วิฑูรย์ สิมะโชคดี อาจารย์ที่ปรึกษา ผู้ซึ่งให้ความรู้ คำแนะนำ คำปรึกษา และตรวจแก้ไขข้อบกพร่องต่าง ๆ จนรายงานการศึกษาส่วนบุคคลในครั้งนี้สำเร็จสมบูรณ์ ผู้เขียนขอขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ผู้เขียนขอขอบพระคุณผู้บังคับบัญชาระดับสูงของสำนักข่าวกรองแห่งชาติ ที่ได้คัดเลือกและอนุมัติให้เข้ารับการศึกษาในหลักสูตรนี้ ซึ่งเป็นประโยชน์ต่อการทำงานในตำแหน่งนักบริหารระดับสูง ทั้งในเชิงการบริหาร กระบวนการทางความคิด และความรอบรู้ในวิชาการสาขาต่าง ๆ เป็นอย่างยิ่ง ที่สำคัญไม่น้อยไปกว่าความรู้ด้านวิชาการ ได้แก่ การสร้างเครือข่ายภาครัฐเพิ่มเติม และการแลกเปลี่ยนเรียนรู้ประสบการณ์การทำงานกับเพื่อนนักศึกษาที่มาจากหลายภาคส่วน

ท้ายที่สุดนี้ ขอขอบพระคุณคณะผู้บริหารสำนักข่าวกรองแห่งชาติด้านข่าวกรองทางเทคนิคและเครือข่าย ที่ได้เสนอแนะแนวทางการจัดทำรายงานในครั้งนี้ เพื่อใช้เป็นแนวทางในการพัฒนาศักยภาพบุคลากรในองค์กรด้านการป้องกันภัยคุกคามทางไซเบอร์ ตามภารกิจของสำนักข่าวกรองแห่งชาติ หากมีสิ่งขาดตกบกพร่องหรือผิดพลาดประการใด ผู้เขียนขออภัยเป็นอย่างสูงในข้อบกพร่องและความผิดพลาดนั้น และผู้เขียนหวังว่ารายงานการศึกษาส่วนบุคคลนี้ จักมีประโยชน์ในการพัฒนาองค์กรให้มีประสิทธิภาพและทันต่อเทคโนโลยีในปัจจุบัน ตลอดจนมีประโยชน์ต่อผู้ที่สนใจจะศึกษารายละเอียดเป็นลำดับต่อไป

นายวัธนชัย ทองประเสริฐ

18 กันยายน 2563

สารบัญ

สารบัญตาราง

สารบัญภาพ

1. วิสัยทัศน์ของตำแหน่งเป้าหมาย

(ข้อมูลส่วนบุคคลไม่เผยแพร่)

2. ข้อเสนอโครงการพัฒนางาน

2.1 การกำหนดประเด็นการศึกษา

2.1.1 ปัญหาและความท้าทายของการพัฒนาศักยภาพบุคลากรเพื่อป้องกันภัยคุกคามทางไซเบอร์

การเปลี่ยนแปลงเทคโนโลยีหรือโลกไซเบอร์ได้นำองค์กรไปสู่วิถีการทำงานแบบใหม่ในการเข้าถึงข้อมูลและการปฏิสัมพันธ์ใหม่ๆ ของแต่ละองค์กรในสภาพแวดล้อมของโลกไซเบอร์ แต่เนื่องด้วยหน่วยงานข่าวกรองส่วนใหญ่ยังคงมีกระบวนทัศน์การปฏิบัติงานอยู่ในหลักนิยมวงรอบข่าวกรองที่ได้มีการวางรากฐานมาตั้งแต่ยุคสมัยสงครามโลกครั้งที่สอง ส่งผลให้การปรับตัวของหน่วยข่าวกรองในโลกไซเบอร์ยุคใหม่จำเป็นต้องเปลี่ยนแปลงอย่างเป็นระบบ รวมถึงการปรับกรอบแนวคิด อย่างไรก็ดีการปฏิรูปกระบวนงานของหน่วยข่าวกรองที่ผ่านมายังดำเนินไปอย่างล่าช้า เนื่องด้วยการปฏิบัติงานในรูปแบบเดิมยังคงมีประสิทธิภาพทั้งในระดับยุทธศาสตร์และกลยุทธ์ แม้จะเป็นประสิทธิภาพที่ต้องแบกรับความยากมากขึ้นและใช้ต้นทุนในงานที่สูงขึ้น

งานข่าวกรองยุคโบราณเกี่ยวข้องอยู่ในบริบทด้านการทหาร โดยแม่ทัพหรือผู้นำทางทหารจะเป็นผู้บริหารจัดการงานข่าวกรองโดยตรงและอำนวยการบนพื้นฐานของความสัมพันธ์ความไว้วางใจระหว่างแม่ทัพกับสายลับ พัฒนาการของกระบวนงานข่าวกรองได้มีการปฏิรูปครั้งใหญ่ในอดีตจากการเปลี่ยนแปลงในยุคอุตสาหกรรม ซึ่งมีการผลิตนวัตกรรมและสิ่งประดิษฐ์ต่าง ๆ ที่สำคัญ อาทิ โทรเลข และเครื่องส่งรับวิทยุ และได้เพิ่มบทบาทของงานข่าวกรองจากการใช้สายลับไปสู่การพัฒนาขีดความความสามารถในการรวบรวมและถอดรหัส หรือสัญญาณวิทยุ เช่น การถอดแปลเครื่องเข้ารหัส Enigma ซึ่งเป็นโครงการข่าวกรองหลักในช่วงสงครามโลกครั้งที่สอง อีกทั้งทำให้มีการจัดตั้งองค์กรข่าวกรองแยกออกไป มากกว่าการเป็นองค์ประกอบในกองทัพ เพราะบทบาทของงานข่าวกรองคืออาวุธในการต่อสู้ชิงไหวชิงพริบและการต่อรองทางการเมืองของผู้นำประเทศ ซึ่งงานขององค์กรข่าวกรองจึงครอบคลุมทั้งการกำหนดความต้องการของข่าวสาร การรวบรวม ดำเนินกรรมวิธีและวิเคราะห์ข้อมูล จัดระเบียบ ตีความ และรายงานต่อให้ผู้มีอำนาจตัดสินใจเชิงนโยบาย องค์กรข่าวกรองมีหน้าที่ให้ข้อมูลสนับสนุนการตัดสินใจในระดับยุทธศาสตร์ โดยมีหลักนิยมในการทำงาน ซึ่งเรียกว่า “วงรอบข่าวกรอง” เป็นแบบแผนปฏิบัติและกำหนดระเบียบความสัมพันธ์ภายใน ระหว่างองค์กรและรัฐบาล

ภาพที่ 3 วงรอบข่าวกรอง intelligence-cycle

ที่มา : Bruenisholz, Elva. (2016). The Intelligent Use of Forensic Data: An Introduction to the Principles . (หน้า 24)

วงรอบข่าวกรอง คือ ระบบงานข่าวกรองที่มีการกำหนดรูปแบบการปฏิสัมพันธ์ระหว่างหน่วยย่อยภายใน โดยเฉพาะอย่างยิ่งความสัมพันธ์ระหว่างหน่วยรวบรวมข่าวสารกับหน่วยวิเคราะห์วิจัย โดยหน่วยรวบรวมข่าวสารจะมีการรวบรวมข้อมูลในชื่อเรียกเป็นสาขางานต่าง ๆ ได้แก่ ข่าวกรองทางสัญญาณ (SIGINT), ข่าวกรองจากแหล่งข่าวเปิด (OSINT), ข่าวกรองทางการภาพ (VISINT) และข่าวกรองจากแหล่งข่าวบุคคล (HUMINT) โดยภายในวงรอบข่าวกรองยังกำหนดวิธีการสื่อสารระหว่างหน่วยภายในขององค์กรข่าวกรอง เช่นเดียวกับการรายงานต่อรัฐบาล ซึ่งคือผู้สั่งการและกำหนดความต้องการข่าวสารข่าวกรอง (โดยปกติจะกำหนดเป็นหัวข้อข่าวสารในระดับยุทธศาสตร์และการประมาณการข่าวกรอง) ส่งกลับมายังหน่วยงานข่าวกรอง เพื่อให้หน่วยงานข่าวกรองนำไปวางแผนและดำเนินกระบวนงาน ทั้งนี้ขอบเขตของการดำเนินการด้านข่าวกรองจึงเป็นกิจกรรมที่แสวงหาข้อมูลข่าวสารสำคัญเพื่อการแจ้งเตือนเกี่ยวกับภัยคุกคามต่อผลประโยชน์และความมั่นคงของชาติตนเองเท่านั้น

ลักษณะสำคัญของกระบวนงานข่าวกรอง มีผลต่อการจัดโครงสร้างหน่วยงานที่มีการแบ่งแยกเด็ดขาดชัดเจน (Compartmentation) ระหว่างหน่วยรวบรวม (Collectors) กับหน่วยวิเคราะห์วิจัย (Analyst/Researchers) อย่างไรก็ตามในระยะกว่าสิบปีที่ผ่านมา การเปลี่ยนแปลงสภาพแวดล้อมภายนอกโดยเฉพาะการเข้าสู่โลกไซเบอร์ ส่งผลให้การทำงานของหน่วยงานข่าวกรอง

หลายกรณีไม่สอดคล้องกับลำดับขั้นตอนของวงรอบข่าวกรอง และท้าทายให้ปรับปรุงพัฒนา รวมไปถึงการปฏิรูปงานข่าวกรอง ไปสู่หน่วยข่าวกรองดิจิตัล ซึ่งจำเป็นต้องกระทำอย่างเป็นระบบ เนื่องจากในยุคที่ภาวะข้อมูลข่าวสาร Big Data ที่มีอยู่อย่างท่วมท้น ทำให้โครงสร้างและการทำงานของหน่วยงานข่าวกรองมีความไม่สอดคล้องกับความท้าทายดังกล่าว ทั้งนี้ข้อเสนอในการปฏิรูปกระบวนงานข่าวกรอง เช่น การยกระดับงานข่าวกรองจากแหล่งข่าวเปิด (OSINT) ตลอดจนการจัดตั้งศูนย์ข่าวกรองทำหน้าที่สังเคราะห์ข้อมูลข่าวสารจากทุกแหล่งข้อมูล (all sources intelligence) ด้วยเช่นกัน

ด้วยเหตุนี้ นักการข่าวกรองในอนาคตจะต้องปฏิรูปตนเองให้เป็นนักการข่าวแบบผสม (Hybrid) ที่ต้องพัฒนาทักษะและศักยภาพเพิ่มขึ้น เพราะโลกไซเบอร์ส่งผลต่อคุณสมบัติของนักการข่าวกรองจากเดิมที่อาจจะเชี่ยวชาญเพียงด้านใดด้านหนึ่ง ไปเป็นผู้ที่มีความรู้ความเชี่ยวชาญในหลากหลายสาขามากขึ้น ทั้งความรู้เท่าทันเทคโนโลยีและดิจิทัล ความรู้ด้านภาษา ความสามารถในการจัดการฐานข้อมูล ความเข้าใจเกี่ยวกับระบบเครือข่าย ข้อมูลสถิติ และอื่น ๆ เพิ่มเติมจากความรู้ความเชี่ยวชาญเฉพาะในวิชาชีพข่าวกรอง และถือเป็นความท้าทายต่อการปฏิรูปองค์กร เพื่อให้สามารถรองรับต่อความทันสมัยของเทคโนโลยี ที่หน่วยงานของรัฐต้องนำมาปรับใช้ให้เหมาะสมกับภารกิจของแต่ละองค์กรได้อย่างมีประสิทธิภาพ เพื่อรับมือต่อภัยคุกคามในรูปแบบใหม

2.1.2 ความจำเป็นในการดำเนินการพัฒนาศักยภาพบุคลากรเพื่อป้องกันภัยคุกคามทางไซเบอร์

2.1.2.1 การมีขีดความสามารถรับมือต่อภัยคุกคามทางไซเบอร์ในปัจจุบัน ด้วยเหตุที่การติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตกลายเป็นส่วนหนึ่งในชีวิตประจำวัน และการดำเนินกิจกรรมในทุกภาคส่วนทั้งเศรษฐกิจ สังคม และความมั่นคง รวมทั้งกิจกรรมไม่พึงประสงค์ต่างๆ ที่เป็นภยันตรายก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของระบบคอมพิวเตอร์ อาทิ การโจมตีทางไซเบอร์ การใช้สื่อสังคมออนไลน์ชี้นำครอบงำทางความคิด หรือการจารกรรมข้อมูลต่างๆ โลกไซเบอร์หรืออินเทอร์เน็ตได้สร้างแหล่งข้อมูลมหาศาลที่เรียกกันว่า Big Data และส่งผลกลายเป็นพัฒนาการของงานสาขาด้านการข่าวกรองคือ การข่าวกรองจากแหล่งข่าวเปิด (Open Source Intelligence) และการข่าวกรองทางไซเบอร์ (Cyber Intelligence) ที่ได้ก้าวขึ้นมามีความสำคัญอย่างมากทั้งการวิเคราะห์ข้อมูล การสืบสวน และการปฏิบัติการข่าวสาร รวมไปถึงการจัดการข้อมูล Big Data ตัวอย่างการทำงานของนักวิทยาศาสตร์ทางด้านข้อมูล (Data Scientist) ที่ต้องมีการประมวลวิเคราะห์ข้อมูลและนำไปใช้ตามวัตถุประสงค์ของผู้ว่าจ้าง เช่น บริษัท PALANTIR ซึ่งเป็นบริษัทให้บริการด้านข้อมูล โดยลูกค้าที่สำคัญ ได้แก่ สำนักงานข่าวกรองกลางสหรัฐฯ (CIA) สำนักงาน

ความมั่นคงแห่งชาติสหรัฐฯ (NSA) สำนักงานสอบสวนกลางสหรัฐฯ (FBI) และกองทัพสหรัฐฯ ผลงานสำคัญของบริษัท PALANTIR คือการวิเคราะห์ข้อมูลและสามารถตรวจพบเบาะแสสำคัญ กรณีพิสูจน์ทราบแหล่งที่อยู่ของนายอุซามะฮ์ บิน ลาดิน หัวหน้ากลุ่มอัลกออิดะฮ์ เป็นต้น ดังนั้นเจ้าหน้าที่ข่าวกรองทางเทคนิคและไซเบอร์ก็เช่นเดียวกับนักวิทยาศาสตร์ทางด้านข้อมูล (Data Scientist) ที่จำเป็นต้องพัฒนาขีดความสามารถและทักษะความเชี่ยวชาญ ให้สามารถประมวลและวิเคราะห์ข้อมูลจากโลกไซเบอร์ เพื่อแจ้งเตือนภัยคุกคามต่อความมั่นคงของชาติได้อย่างรวดเร็วทันการณ์และแม่นยำ

2.1.2.2 ศักยภาพในการตอบสนองความต้องการและความคาดหวังของผู้ใช้ข่าว ในเรื่องประสิทธิภาพด้านความเร็ว ความถูกต้อง แม่นยำและข่าวเชิงลึก เจ้าหน้าที่ผู้รับผิดชอบจำเป็นต้องมีศักยภาพทั้งด้านทางการข่าวและทางด้านเทคนิค โดยหลักการแล้วงานข่าวกรองจะเป็นการประเมินสภาพแวดล้อมทางยุทธศาสตร์ เป็นการมองไปในอนาคตบนพื้นฐานของข้อเท็จจริง การประมาณการว่าจะต้องทำได้อย่างถูกต้อง แม่นยำ หรือใกล้เคียงความจริงมากที่สุด เพื่อแจ้งเตือนล่วงหน้าต่อผู้กำหนดนโยบายทั้งในระดับองค์กรและรัฐบาล ให้สามารถกำหนดแนวทางปฏิบัติหรือนโยบายเพื่อรักษาผลประโยชน์แห่งชาติและความมั่นคง ซึ่งนายกรัฐมนตรีได้มีข้อสั่งการ เมื่อตุลาคม 2560 สั่งการให้ปฏิรูประบบงานข่าวกรอง ให้สังคมในส่วนรวมเกิดความเชื่อมั่นว่าหน่วยงานด้านการข่าวสามารถดูแลรักษาความสงบเรียบร้อยของประเทศไว้ได้

2.1.2.3 การปรับกระบวนการทำงานและการปฏิบัติตามกฎหมายที่เกี่ยวข้องเพื่อเพิ่มขีดความสามารถในการทำงานข่าวกรอง ปัจจุบันมีกฎหมายที่เอื้ออำนวยต่อการพัฒนาขีดความสามารถของระบบงานข่าวกรอง ได้แก่ พระราชบัญญัติข่าวกรองแห่งชาติ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 เป็นกฎหมายที่เสริมสร้างภาวะแวดล้อมให้เอื้อต่อการปฏิบัติการข่าวกรองของชาติ และให้อำนาจแก่องค์กรข่าวกรองดำเนินการใดๆ เพื่อให้ได้มาซึ่งข้อมูลอันเกี่ยวกับการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร และการรักษาความปลอดภัยฝ่ายพลเรือน รวมทั้งอาจใช้เครื่องมืออิเล็กทรอนิกส์ หรือเทคโนโลยีอื่นใด เพื่อดำเนินการดังกล่าว ส่วนพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น มุ่งกำหนดมาตรการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายใน ซึ่งถือเป็นภารกิจหนึ่งที่องค์กรข่าวกรองต้องเตรียมการรองรับ เฉพาะอย่างยิ่งการนำเทคโนโลยีดิจิทัลมาปรับใช้กับการทำงานข่าวกรอง รวมถึงการที่องค์กรข่าวกรองต้องปฏิบัติตามกฎหมายในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เนื่องจากเป็นหนึ่งในหน่วยงานด้านความมั่นคงที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical

Information Infrastructure) ที่ต้องมีมาตรการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างเคร่งครัด

2.1.2.4 นอกจากนี้ จากแบบสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทย ระดับกรม องค์การปกครองส่วนท้องถิ่นรูปแบบพิเศษ และจังหวัด ประจำปี 2563 ในข้อ P1.8.1 พบว่าหน่วยงานยังไม่มีการดำเนินการใด ๆ ที่สอดรับกับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้แก่ การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมเป้าหมาย และแนวทางตามมาตรา 42 รวมถึงการจัดการโครงสร้างพื้นฐานทางสารสนเทศของหน่วยงานเพื่อให้เป็นไปตามหลักเกณฑ์ที่กำหนด อาทิ มีการประเมินความเสี่ยงและตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (ม.54) กำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ (ม.56)

2.1.3 สภาพปัญหาที่ผ่านมาและแนวโน้มของปัญหาในอนาคต และผลกระทบที่เกิดขึ้นของการพัฒนาศักยภาพบุคลากรเพื่อป้องกันภัยคุกคามทางไซเบอร์

2.1.3.1 ความไม่ชัดเจนในการกำหนดสมรรถนะและทักษะหลักของเจ้าหน้าที่ภายในหน่วยงานในสายงานเทคนิคและเครือข่าย เนื่องด้วยเจ้าหน้าที่จำเป็นต้องสามารถสลับภารกิจในการทำงานได้ และต้องมีความยืดหยุ่นสูง จึงเป็นข้อจำกัดที่ทำให้ไม่อาจสร้างผู้เชี่ยวชาญเฉพาะด้านนั้นๆ ได้เพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่พัฒนารูปแบบและวิธีการโจมตีตลอดเวลา อย่างไรก็ดีผลลัพธ์ของงานข่าวกรองใดก็ตามจำเป็นต้องมีเจ้าหน้าที่ที่มีทักษะทางการข่าวที่ต้องอาศัยประสบการณ์ในการทำงานสูงและมีองค์ความรู้ทั้งในเชิงกว้างและเชิงลึกเกี่ยวกับสถานการณ์ความมั่นคง เช่น การเมือง การก่อการร้าย ความสัมพันธ์ระหว่างประเทศ สงคราม และ พ.ร.บ.ด้านต่างๆ รวมทั้งต้องผสมผสานความรู้ทางด้านเทคนิค ได้แก่ ทักษะการเขียนโปรแกรมคอมพิวเตอร์ ทักษะด้านเครือข่ายคอมพิวเตอร์และการสื่อสาร ทักษะการพิสูจน์หลักฐานทางดิจิทัล เป็นต้น จึงจะสามารถเผชิญหน้าต่อความเสี่ยง ทั้งการโจมตีและการจารกรรมทางไซเบอร์ นอกจากนี้เจ้าหน้าที่ต้องพัฒนาทักษะให้เข้าใจธรรมชาติและพัฒนาการของสื่อสังคมออนไลน์ที่ยังไม่มีการเปิดการเรียนการสอน ทำให้เจ้าหน้าที่ต้องเรียนรู้และสั่งสมประสบการณ์ด้วยตนเอง ทั้งนี้ สื่อประเภทเครือข่ายสังคมออนไลน์เป็นเครื่องมือสำคัญของประชาชนในการรวมตัวดำเนินกิจกรรมทางสาธารณะและการเคลื่อนไหวกิจกรรมทางการเมือง สื่อดังกล่าวมีโอกาสถูกนำมาใช้ในทางที่ผิด เพื่อโจมตี บ่อนทำลาย หรือบิดเบือนข้อเท็จจริง รวมถึงการแพร่กระจายถ้อยคำที่สร้างความเกลียดชังที่มีฐานมาจากอคติและการเลือกปฏิบัติ ซึ่งอาจ

ทำให้เกิดความเกลียดชังและสร้างปัญหาความแตกแยกภายในประเทศ รวมถึงส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศในกรณีที่มีการใช้สื่อประเภทนี้โจมตีหรือบ่อนทำลายประเทศอื่น

2.1.3.2 เจ้าหน้าที่ข่าวกรองทางเทคนิค มีความรู้และประสบการณ์ที่แตกต่างกันออกไป แม้จะได้รับการแก้ไขด้วยการบรรจุข้าราชการรุ่นใหม่ ที่มีสมรรถนะสูงขึ้นในด้านความรู้ทางดิจิทัลและไซเบอร์ ในตำแหน่ง “นักการข่าวไซเบอร์” ซึ่งมีทักษะในการประยุกต์ใช้ความรู้ทางเทคนิคเพื่อสืบค้นและวิเคราะห์ข้อมูลข่าวสารที่อยู่บนระบบเครือข่ายเข้ามาทำงานแล้ว แต่ยังมีข้อจำกัดด้านประสบการณ์ ความเชี่ยวชาญการสืบสวน การวิเคราะห์ ประมวล ประเมินภัยคุกคามเชิงลึกในทางการข่าว ขณะที่บุคลากรเดิมมีข้อได้เปรียบด้านประสบการณ์และความสามารถในการวิเคราะห์แจ้งเตือนภัยคุกคาม แต่ยังต้องพัฒนาศักยภาพด้านการรู้เท่าทันการเปลี่ยนแปลงของเทคโนโลยีและเครื่องมือดิจิทัลต่างๆ อย่างไรก็ดี บุคลากรทั้งหมดยังต้องอยู่บนหลักนิยมของการปฏิบัติงานด้านการข่าวขององค์กร ซึ่งมุ่งส่งเสริมให้เจ้าหน้าที่ต้องเป็นผู้ที่มีความยืดหยุ่นสูง สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพและมีความรู้ที่หลากหลายเพื่อตอบสนองต่อภารกิจและการปฏิบัติงานตามสถานการณ์เฉพาะกิจหรือฉุกเฉิน (task force) ซึ่งมีอยู่สม่ำเสมอในลักษณะที่ไม่ใช้งานประจำ

2.1.3.3 วัฒนธรรมขององค์กรที่มีข้อจำกัดจากวัฒนธรรมแบบราชการ (Hierarchy Culture) และการแบ่งส่วนงานที่เข้มงวด ซึ่งมักต่อต้านการเปลี่ยนแปลง โดยสมาชิกในองค์กรเห็นว่าเป็นเรื่องไม่จำเป็น มีความเสี่ยงมาก และเป็นความคิดแบบคลั่งไคล้ แม้วัฒนธรรมแบบราชการมีลักษณะเด่นที่เป็นการทำงาน ซึ่งเน้นโครงสร้างการทำงานมีระเบียบแบบแผน มีขั้นตอนและกระบวนการทำงานที่ดี มีความมั่นคง และมีผู้นำควบคุมกำกับดูแลเพื่อให้การปฏิบัติงานไปเป็นอย่างราบรื่น แต่ธรรมชาติของการปฏิบัติงานของหน่วยข่าวกรองจำเป็นต้องมีวัฒนธรรมความร่วมมือการทำงานเป็นทีม ทุกคนมีส่วนร่วมในการทำกิจกรรมต่างๆ โดยมีผู้นำเป็นที่ปรึกษารวมถึงวัฒนธรรมแบบเน้นความคิดสร้างสรรค์และมีนวัตกรรมใหม่ๆ ขณะที่ข้อจำกัดในการเผยแพร่ข่าวสารและชุดความรู้ข้อมูลภายในหน่วยงาน สำหรับองค์กรข่าวกรองจะมีค่านิยมในการทำงานบนหลักการพื้นฐานเรื่องการแบ่งส่วนงาน และการจำกัดให้ทราบเท่าที่จำเป็น ซึ่งทำให้การบูรณาการการทำงานเกิดขึ้นชั่วคราวหรือเฉพาะกิจ จึงต้องมีการปรับเปลี่ยนและพัฒนาไปสู่หลักการทำงานแบบแลกเปลี่ยนและเชื่อมโยงข้อมูลซึ่งจะเข้ามาแทนที่ หลักสูตรการข่าวที่เป็นพื้นฐานการทำงานการข่าวแบบมืออาชีพจำเป็นต้องปรับเปลี่ยนเช่นกัน ทั้งนี้โดยหลักการทำงานยังคงต้องใช้แหล่งข่าวบุคคล แต่กิจกรรมและกระบวนการบางอย่างจะให้ความสำคัญโลกเสมือนหรือโลกดิจิทัลมากขึ้น ทั้งการเฝ้าติดตามความเคลื่อนไหวของเป้าหมาย การอำนวยการแหล่งข่าวบุคคล และการรวบรวมข่าวสารทางเทคนิค ดังนั้นบุคลากรขององค์กรข่าวกรองในอนาคตสัดส่วนของกลุ่มคนที่รู้ดิจิทัล (Digital Literacy) มีแนวโน้มจะเป็นบุคลากร

กลุ่มใหญ่ของหน่วยงาน แต่ผู้ที่มีทักษะทางเทคนิคเชิงลึกยังมีสัดส่วนที่น้อยอยู่ ส่วนหนึ่งเป็นผลจากการพัฒนาทักษะด้านดิจิทัลของบุคลากรภาครัฐตามแนวทางของสำนักงานคณะกรรมการข้าราชการพลเรือน ที่มุ่งเน้นไปที่ทักษะทางเทคนิคในระดับพื้นฐานเท่านั้น

2.2 การกำหนดข้อเสนอเชิงนโยบาย

ข้อเสนอเชิงนโยบายสำหรับการพัฒนาศักยภาพบุคลากรให้มีความพร้อมสำหรับภารกิจด้านการป้องกันภัยคุกคามทางไซเบอร์นั้น จำเป็นต้องจำแนกออกเป็นกระบวนการต่างๆ ที่สำคัญ ดังนี้

1) แนวทางการบริหารจัดการบุคลากรตามหลัก PDCA
2) การวิเคราะห์และกำหนดแนวทางการพัฒนาบุคลากรด้านไซเบอร์
3) แนวทางในการแก้ไขปัญหาหรือพัฒนานโยบายที่สอดคล้องกับการวิเคราะห์
4) ปัจจัยที่อาจมีผลกระทบต่อความสำเร็จของการดำเนินการตามข้อเสนอแนวทางบริหารจัดการที่เป็นรูปธรรม

2.2.1 แนวทางการบริหารจัดการบุคลากรตามหลัก PDCA

แนวทางการบริหารจัดการบุคลากรให้มีความพร้อมสำหรับภารกิจด้านการป้องกันภัยคุกคามทางไซเบอร์นั้น จำเป็นต้องอาศัยหลักการที่เหมาะสมมาปรับใช้กับการบริหารจัดการองค์กรขนาดใหญ่ ซึ่งรายงานการศึกษาส่วนบุคคลฉบับนี้ขอหยิบยกหลักการ PDCA ซึ่งถูกคิดค้นโดย วอล์ทเตอร์ ชิวฮาร์ท (Walter Shewhart) โดยหลักการดังกล่าวมีรูปแบบเป็นวงจรหรือแนวคิดการบริหารคุณภาพในการทำงานประเภทหนึ่ง เป็นตัวย่อของศัพท์ภาษาอังกฤษที่ประกอบไปด้วย P (Plan) คือ การวางแผน D (Do) คือการลงมือปฏิบัติ C (Check) คือการตรวจสอบ และ A (Action) คือดำเนินการปรับปรุงแก้ไขส่วนที่มีปัญหา

จากการศึกษาพบว่าหลักการดังกล่าวสามารถนำมาประยุกต์ใช้เป็นแนวทางในการพัฒนาศักยภาพบุคลากรของหน่วยงานให้มีความพร้อมสำหรับภารกิจด้านการป้องกันภัยคุกคามทางไซเบอร์ เนื่องจากที่ผ่านมาหลักการดังกล่าวได้รับความนิยมถูกนำไปใช้ในการบริหารจัดการองค์กรขนาดใหญ่หลายแห่งในประเทศญี่ปุ่น เช่น บริษัท TOYOTA ที่ถือเป็นองค์กรระดับโลกที่มีการนำหลักการ PDCA นี้มาใช้ในกระบวนการผลิตรถยนต์ รวมทั้งการพัฒนาศักยภาพบุคคลในองค์กร และพัฒนาจนกลายเป็น TOYOTA WAY ในปัจจุบัน ดังนั้นจึงเป็นข้อพิสูจน์ให้เห็นว่าหลักการ PDCA สามารถนำมาใช้เพื่อปรับปรุงและพัฒนาระบบการทำงานขององค์กรให้ดีขึ้นได้แม้กระทั่งองค์กรนั้นไม่ได้เกี่ยวข้องกับการผลิตในอุตสาหกรรม รวมถึงนำไปปรับใช้เพื่อพัฒนาการทำงานในวงรอบข่าวกรองที่ประกอบด้วย การกำหนดความต้องการของข่าวสาร (Requirements) การรวบรวม (Collection) การดำเนินกรรมวิธี (Processing) และการวิเคราะห์ (Analysis) ได้ เพราะหลักการ PDCA Plan-Do-

Check-Act สามารถนำมาประยุกต์ใช้ได้กับงานทุกประเภทแม้กระทั่งการดำเนินชีวิตประจำวัน สรุปสาระสำคัญได้ ดังนี้

Plan (P) เริ่มต้นที่ Plan คือขั้นตอนการวางแผนก่อนที่เริ่มปฏิบัติงานจริง มีการกำหนดลำดับความสำคัญของงาน และครอบคลุมถึงการกำหนดหัวข้อวัตถุประสงค์ที่ชัดเจนที่ต้องการลงมือปฏิบัติ ปรับปรุงเปลี่ยนแปลง หรือพัฒนาสิ่งใหม่ๆ โดยในขั้นตอนนี้เจ้าหน้าที่ทุกคนในองค์กรต้องรับทราบและเป็นที่เข้าใจตรงกัน เพราะถือว่าเป็นองค์ประกอบที่มีความสำคัญที่จะส่งผลช่วยให้การทำงานในขั้นตอนถัดไปเป็นไปด้วยความราบรื่นและถูกต้องตรงตามวัตถุประสงค์ที่ตั้งไว้ นอกจากนี้การวางแผนสามารถช่วยให้คาดการณ์สิ่งที่จะเกิดขึ้นในอนาคต และช่วยลดและป้องกันการสูญเสียทั้งด้านบุคลากร งบประมาณ และเวลาได้อีกด้วย ทั้งนี้สามารถนำมาปรับใช้ในการทำงานด้านการข่าว ได้แก่ ขั้นตอนการกำหนดความต้องการของข่าวสาร (Requirements) ที่มีเรื่องของการวางแผนการปฏิบัติเข้ามาเกี่ยวข้อง

Do (D) หลังจากที่ได้วางแผน (Plan) กำหนดวัตถุประสงค์อย่างรอบคอบแล้ว ในขั้นตอนถัดไปคือ การลงมือทำหรือการปฏิบัติตามขั้นตอนตามแผนงานที่ได้กำหนดไว้อย่างเป็นระบบและให้มีความต่อเนื่องเพื่อผลลัพธ์ที่ดีที่สุด โดยในขั้นตอนการปฏิบัตินี้ควรศึกษาถึงวิธีการที่เหมาะสมที่สุดสำหรับการทำงานนั้นๆ ด้วย เพื่อให้เกิดประสิทธิภาพสูงสุด รวมถึงในระหว่างการปฏิบัติงานควรเก็บข้อมูลที่สำคัญหรือข้อผิดพลาดต่างๆ ของการทำงานเอาไว้เพื่อประโยชน์ในการทำงานขั้นตอนต่อไปทั้ งนี้สามารถนำมาปรับใช้ในการทำงานด้านการข่าว ได้แก่ ขั้นตอนการรวบรวมข่าวสาร (Collection) ที่มีการแปลงความต้องการข่าวสารมาเป็นแผนการปฏิบัติการ

Check (C) คือขั้นตอนการตรวจสอบว่าหลังจากนำแผนที่วางไว้ไปปฏิบัติจริง (Do) แล้วสามารถบรรลุวัตถุประสงค์หรือมาตรฐานที่ได้กำหนดไว้หรือไม่ ทั้งนี้สิ่งที่ควรคำนึงถึงคือ ต้องรู้ว่าจะต้องตรวจสอบอะไรบ้างและจำนวนบ่อยครั้งแค่ไหน การตรวจสอบการทำงานควรจะมีการจดบันทึกในรูปแบบต่างๆ ไว้ เช่น ระบบบันทึกการตรวจสอบ เอกสารการตรวจสอบ เป็นต้น เพื่อให้สะดวกในการปรับปรุง และแก้ไขในการทำงานครั้งต่อไปให้ข้อมูลที่ได้จากการตรวจสอบเป็นประโยชน์ สำหรับขั้นตอนถัดไปคือการดำเนินการการปรับปรุงแก้ไข (Action) ทั้งนี้สามารถนำมาปรับใช้ในการทำงานด้านการข่าว ได้แก่ ขั้นตอนการดำเนินกรรมวิธี (Processing) ที่เป็นขั้นตอนการนำข้อมูลข่าวสารมาตรวจสอบ เพื่อประเมินความน่าเชื่อถือ และประมวลเป็นเรื่องราว เหตุการณ์

Action (A) สุดท้ายที่ Action คือ กระบวนการปรับปรุงแก้ไขส่วนที่มีปัญหา โดยขั้นตอนนี้เป็นการนำเอาผลลัพธ์ที่ได้จากขั้นตอนการตรวจสอบ (Check) มาวิเคราะห์และตรวจสอบสาเหตุความผิดพลาดที่เกิดขึ้นมาประเมินเพื่อพัฒนาแผนและหาแนวทางการแก้ไขปัญหาที่เกิด เพื่อป้องกันไม่ให้ปัญหาเดิมเกิดขึ้นอีกในระยะยาว ถึงแม้ว่าจะไม่มีข้อบกพร่องจากกระบวนการทำงานที่ผ่านมาแต่ก็ควรจะมีวิธีในการพัฒนาปรับปรุงการทำงานของตนเองอยู่เสมอ เพื่อให้การดำเนินงานครั้งต่อไปมี

ประสิทธิภาพที่ดีกว่าเดิม สามารถนำมาปรับใช้ในการทำงานด้านการข่าว ได้แก่ ขั้นตอนการวิเคราะห์ (Analysis) ที่เป็นการนำข่าวสารที่ดำเนินกรรมวิธีแล้ว มาวิเคราะห์ทำให้เกิดความถูกต้องแม่นยำ

อนึ่ง ในองค์กรหรือบริษัทญี่ปุ่นจะมีวงจรพัฒนาคุณภาพที่คล้ายคลึงกับ PDCA ที่รู้จักกันเป็นอย่างดี เช่น “Kaizen” ที่เป็นการระบุว่ามีจุดไหนหรือส่วนไหนของการดำเนินการที่ควรปรับปรุง และมีวิธีการปรับปรุงที่มีความเหมาะสมอย่างไรบ้าง ทำให้ในครั้งต่อไปสามารถทำงานได้ดีขึ้นกว่าเดิม ดังนั้นการทำงานของ PDCA โดยหลังจากเสร็จกระบวนการปรับปรุงแก้ไข (Action) แล้ว วงจรบริหารคุณภาพก็จะวนเข้าสู่กระบวนการวางแผน (Plan) เพื่อเริ่มวางแผนใหม่ครั้งใหม่สำหรับการปฏิบัติการในครั้งต่อไป ซึ่งวงจรบริหารงานคุณภาพ PDCA จะสามารถวนอย่างนี้ไปโดยไม่มีที่สิ้นสุดเพื่อเป็นการป้องกันปัญหาที่จะเกิดและเป็นการพัฒนาคุณภาพอย่างต่อเนื่อง

2.2.2 การวิเคราะห์และกำหนดแนวทางการพัฒนาบุคลากรด้านไซเบอร์

ในการวิเคราะห์และกำหนดแนวทางพัฒนาบุคลากรด้านไซเบอร์ หรือนักการข่าวไซเบอร์ภายใต้กรอบการปฏิบัติของหลักการ PDCA ทั้งขั้นตอนการวางแผน การลงมือปฏิบัติ การตรวจสอบและการปรับปรุงแก้ไขปัญหาขีดความสามารถของบุคลากรด้านไซเบอร์และกระบวนงานข่าวกรองทางดิจิทัลและไซเบอร์ในสภาวะปัจจุบัน อันเป็นการปรับปรุงจุดอ่อนและเสริมสร้างจุดแข็ง อีกทั้งเพื่อยกระดับศักยภาพด้านดิจิทัลและไซเบอร์ขององค์กรให้สอดรับกับสภาพปัญหาความท้าทาย และความจำเป็นต่าง ๆ เห็นควรวางแผนและขับเคลื่อนไปสู่การปฏิบัติที่สำคัญอย่างน้อย 4 แนวทาง ดังนี้

(1) การระบุและกำหนดความรู้ ทักษะ และสมรรถนะมาตรฐานของบุคลากรด้านไซเบอร์

กรณีข้างต้นต่อสภาพปัญหาความท้าทายทางด้านบุคลากรด้านไซเบอร์ของหน่วยงานคือบุคลากรที่ทำงานด้านไซเบอร์ที่แท้จริงตามความหมายงานข่าวกรองเชิงไซเบอร์และดิจิทัลนั้น ยังมีอยู่จำนวนน้อยถึงน้อยมากที่สำเร็จการศึกษาจากสายงานคอมพิวเตอร์โดยตรงเมื่อเปรียบเทียบกับจำนวนกำลังพลส่วนใหญ่ในหน่วยงาน ซึ่งกลายเป็นสาเหตุหลักที่ทำให้เกิดความไม่พร้อมของหน่วยงานที่จะมารองรับกับภารกิจด้านการป้องกันภัยคุกคามทางไซเบอร์ เพราะการที่จะดำเนินภารกิจด้านการป้องกันภัยคุกคามทางไซเบอร์นั้น จำเป็นต้องรวบรวมบุคลากรที่มีความรู้ความเชี่ยวชาญทางเทคนิคเฉพาะด้านมาทำงานร่วมกัน อาทิ ผู้เชี่ยวชาญด้านเครือข่าย ผู้เชี่ยวชาญด้านโปรแกรมมิ่ง และผู้เชี่ยวชาญด้านฐานข้อมูล และ Big data เป็นต้น ตัวอย่างเช่น หากต้องการสร้างเครือข่ายการติดต่อสื่อสารภายในองค์กรที่มีประสิทธิภาพและมีมาตรการรักษาความปลอดภัยที่ล้ำเลิศ หน่วยงานจำเป็นจะต้องนำผู้ที่มีความรู้ทางด้านเครือข่ายมาเป็นผู้ออกแบบมิใช่จะนำบุคลากรที่เป็นโปรแกรมเมอร์มาดำเนินการได้หรือถ้าทำได้ก็อาจได้ไม่ดีเท่าที่ควรเช่นเดียวกัน หากต้องการเขียนโปรแกรมมัลแวร์หรือสร้างไวรัสขึ้นมาเพื่อเป้าหมายด้านการสืบสวนทางการข่าว แต่กลับมอบให้ผู้เชี่ยวชาญด้านเครือข่ายเป็นผู้ดำเนินการก็มีความเสี่ยงที่จะล้มเหลว เพราะไม่ใช่ความถนัดชำนาญของผู้เชี่ยวชาญด้านเครือข่าย

ด้วยเหตุนี้การระบุและกำหนดองค์ความรู้ ทักษะ และสมรรถนะมาตรฐานของบุคลากรด้านไซเบอร์โดยครอบคลุมทั้งในแนวระนาบและแนวดิ่ง จึงเป็นความสำคัญในลำดับแรก หากต้องการที่จะสร้างหน่วยงานให้บรรลุเป้าประสงค์ที่วางไว้ เช่น หากต้องการสร้างบุคลากรให้มีขีดความสามารถ ทั้งในด้านการป้องกันป้องปราม และดำเนินการเชิงรุกต่อการดำเนินการกับภัยคุกคามด้านไซเบอร์ สิ่งสำคัญที่สุดก็คือ การเตรียมบุคลากรให้มีความพร้อม ทั้งในด้านความรู้ความสามารถ มีทักษะการใช้งานกับอุปกรณ์เครือข่ายและเครื่องมือทางเทคนิคที่มีอยู่ในปัจจุบัน

(2) การกำหนดแนวทางการพัฒนาความรู้ ทักษะ และสมรรถนะของบุคลากรด้านไซเบอร์

แม้หน่วยงานได้กำหนดความรู้ ทักษะ และสมรรถนะมาตรฐานของบุคลากรด้านไซเบอร์แล้ว ก็ยังไม่เพียงพอที่จะทำให้การปฏิบัติงานบรรลุเป้าหมายยุทธศาสตร์และสามารถตอบสนองต่อความท้าทายได้อย่างยั่งยืนในระยะยาว เพราะในระบบราชการ หน่วยงานจำเป็นจะต้องบริหารทรัพยากรบุคคลที่มีอยู่ให้เกิดศักยภาพสูงสุด จากการที่ในระบบการสรรหาบุคลากรขององค์กรที่ผ่านมาสอดคล้องตามยุคสมัย แต่ก็ยังก้าวไม่ทันความเปลี่ยนแปลงเทคโนโลยีเชิงดิจิทัล ด้วยเหตุนี้หน่วยงานจะต้องมีการปรับปรุงพัฒนาสมรรถนะ ตลอดจนทักษะความชำนาญให้เกิดขึ้นโดยสอดคล้องกับความเปลี่ยนแปลง ทั้งนี้ขั้นตอนการฝึกอบรม (Training & Retraining) และการพัฒนาบุคลากรถือว่าเป็นขั้นตอนที่สำคัญ เนื่องด้วยวัตถุประสงค์ของการฝึกอบรมและพัฒนา คือการพัฒนาศักยภาพและเสริมสร้างจุดแข็งของบุคลากรให้มีประสิทธิภาพมากยิ่งขึ้น รวมถึงการลดจุดอ่อนที่ควรปรับปรุงของแต่ละบุคคล การฝึกอบรมเป็นเครื่องมือที่จะทำให้เกิดการเรียนรู้ในระยะสั้น หากต้องการให้ผู้อบรมได้รับความรู้ทักษะและแรงจูงใจในการนำสิ่งที่เรียนรู้มาประยุกต์ใช้ต่อไปนั้น

ทั้งนี้ ด้วยความจำเป็นในการดำเนินภารกิจหน้าที่อันหลากหลาย ประกอบกับจำนวนบุคลากรที่มีข้อจำกัด สิ่งเหล่านี้จึงจำเป็นที่จะต้องสร้างบุคลากรให้รองรับแล้วนำบุคลากรเหล่านี้มาทำงานร่วมกันและทำให้เกิดประสิทธิภาพมากที่สุด ผู้บังคับบัญชาจะมีส่วนสำคัญในการขับเคลื่อนการพัฒนา (Development) โดยเฉพาะการหาวิธีการที่จะพัฒนาเพื่อฝึกฝนและปรับเปลี่ยนพฤติกรรมของบุคลากร ให้มีนิสัยและพฤติกรรมที่แสดงออกเป็นนิสัยถาวรที่เกิดขึ้นอยู่เสมอ ขณะเดียวกันการพัฒนาก็เป็นเครื่องมือที่จะช่วยทำให้บุคลากรเกิดการเรียนรู้อย่างต่อเนื่องในระยะยาวและเป็นกระบวนการเสริมสร้างบุคลากรแต่ละคนให้มีความพร้อมและความเชี่ยวชาญในหลายด้าน เป็นกระบวนการสร้างบุคลากรหนึ่งคนให้มีความเชี่ยวชาญมากกว่าหนึ่งด้านขึ้นไปเพื่อทดแทนจำนวนบุคลากรที่มีอยู่อย่างจำกัด สามารถทำงานแบบผสม (Hybrid) ซึ่งเริ่มจากการประเมินระดับพื้นฐานความรู้ความสามารถของบุคลากรด้านไซเบอร์แต่ละคนที่มีความแตกต่างกันและค้นหาความสนใจ เพื่อที่จะนำไปสู่การออกแบบหลักสูตรการอบรมต่างๆ ให้เหมาะสมในแต่ละบุคคล

การสร้างบุคลากรให้มีความรู้ความเชี่ยวชาญในแต่ละด้านนั้น จำเป็นต้องริเริ่มจากการปูพื้นฐานในระดับพื้นฐานต่อยอดไปจนถึงระดับบริหาร (admin) และพัฒนาถึงเป้าหมายสูงสุด

ในการเป็นผู้เชี่ยวชาญเฉพาะด้าน (expert) โดยจำเป็นต้องจัดส่งบุคลากรเข้ารับการอบรมตามลำดับขั้น มีการกำหนดแผนเสริมสร้างบุคลากรที่เชี่ยวชาญในด้านต่างๆ ให้มีจำนวนสมดุลกัน ทั้งการพัฒนาโปรแกรมเมอร์ การพัฒนาบุคลากรด้านงานเครือข่าย และการพัฒนาบุคลากรด้านฐานข้อมูล ต้องสร้างทั้ง 3 ส่วนให้มีจำนวนสอดคล้องกัน โดยไม่สามารถที่จะเร่งพัฒนาความเชี่ยวชาญด้านใดด้านหนึ่งเป็นการเฉพาะก่อน เพราะความเชี่ยวชาญในแต่ละด้านนั้นจำเป็นต่อการที่จะนำไปใช้ประโยชน์พร้อมกันแบบบูรณาการอย่างไม่สามารถแยกจากกันได้

(3) การพัฒนากระบวนการทำงานโดยการสรรหาพัฒนาเครื่องมือปฏิบัติงานเชิงดิจิทัลมาประยุกต์ใช้ในภารกิจข่าวกรองและต่อต้านข่าวกรองทั้งระบบ

การพัฒนาเครื่องมือปฏิบัติงานเชิงดิจิทัลมีผลต่อการปรับปรุงกระบวนงานข่าวกรองอย่างมากตั้งแต่การรวบรวม การคัดเลือก สืบสวน ตรวจสอบ และวิเคราะห์/สังเคราะห์ เนื่องด้วยโลกไซเบอร์ทำให้เกิดกิจกรรมและข้อมูลออนไลน์มหาศาล ด้วยความก้าวหน้าของเทคโนโลยีทำให้การดำเนินงานของเจ้าหน้าที่มีความสะดวกมากขึ้น เฉพาะอย่างยิ่งในการสืบสวน/คัดกรองข้อมูลข่าวสารที่เอื้ออำนวยประโยชน์ทางการข่าว การวิเคราะห์ Big Data ตลอดจนการวิเคราะห์ความสัมพันธ์เชื่อมโยงของข้อมูล ซึ่งช่วยยกระดับขีดความสามารถในการทำงานสืบสวนของบุคลากรด้านข่าวกรองทั้งในด้านความรวดเร็วและความแม่นยำ เช่น กรณีสถานการณ์ความไม่สงบในจังหวัดชายแดนภาคใต้ การใช้เครื่องมือที่สามารถวิเคราะห์ข้อมูลในเชิงสถิติหรือ Statistical Analytics Tool ช่วยให้บุคลากรสามารถต่อภาพความสัมพันธ์เชื่อมโยงของแต่ละเหตุการณ์ได้ชัดเจนมากขึ้น ในขณะที่ปัจจุบันเครื่องมือปฏิบัติงานเชิงดิจิทัลเหล่านี้ได้รับการพัฒนาให้สามารถใช้งานแบบเฉพาะเจาะจงมากขึ้น เช่น การเจาะเข้าถึงข้อมูลเป้าหมายที่มีความเสี่ยงอาจเป็นภัยคุกคามต่อความมั่นคงได้

(4) การเสริมสร้างสภาพแวดล้อมวัฒนธรรมองค์กรที่สนับสนุนประสิทธิภาพในการทำงาน

แม้การแบ่งส่วนงานจะมีความเด็ดขาดชัดเจน (Compartmentation) เป็นหลักนิยม (Doctrine) ของการทำงานของหน่วยข่าวกรองทั่วโลก เนื่องจากเป็นการทำงานที่ต้องรักษาความปลอดภัยในการทำงานอย่างเข้มงวด อย่างไรก็ตามการทำงานในลักษณะการแบ่งแยกเด็ดขาดทำให้การถ่ายทอดหรือไหลเวียนองค์ความรู้ ทักษะ ประสบการณ์ภายในงาน หรือการส่งมอบงาน/ส่งต่องานจำเป็นต้องใช้เวลา ไม่ได้เกิดขึ้นโดยอัตโนมัติและไม่สามารถเรียนรู้จากที่ใดได้ ขณะที่รูปแบบการทำงานยุคใหม่ที่มีเทคโนโลยีเข้ามาเกี่ยวข้องตลอดจนพัฒนาการของความเสี่ยงด้านภัยคุกคาม ทำให้หน่วยงานต้องปรับลดกำแพงกั้นระหว่างงานจากการแบ่งส่วนงานเด็ดขาด ไปสู่แนวคิดความร่วมมือในการทำงานแบบมีส่วนร่วม หรือการทำงานเป็นทีม ตลอดจนการทำงานแบบทีมข้ามสายงาน (Cross Functional Team) ที่มีการบูรณาการงานระหว่างกัน ซึ่งงานข่าวกรองไซเบอร์ได้ช่วยให้แนวทางในการปฏิบัติงานดังกล่าวมีความสะดวกง่ายขึ้นจากการบูรณาการงานที่ไร้ลักษณะทางกายภาพ (Virtual) ในหลายๆ กิจกรรม

นอกจากนี้ การแปลงองค์ความรู้แนวทางปฏิบัติงานต่างๆ ให้อยู่ในรูปแบบดิจิทัล มาเป็นบทเรียนขนาดสั้น จะช่วยให้บุคลากรได้เรียนรู้เมื่อใดก็ได้ที่สะดวกและการเรียนรู้นั้นจะบูรณาการเข้ากับงานในรูปแบบการเรียนรู้เชิงประยุกต์ต่างๆ ทั้งนี้การดำเนินการดังกล่าวไม่เพียงแต่จะกลายเป็นการเรียนรู้ด้วยตนเองเท่านั้น แต่ยังเป็นการขับเคลื่อนด้วยตนเองด้วยเช่นกันในฐานะผู้นำด้านเทคโนโลยีที่ก้าวหน้ายอมรับการเรียนรู้ด้วยแรงจูงใจในตนเองเป็นวิธีที่ดีที่สุดในการเปลี่ยนแปลงให้เกิดขึ้น จะส่งผลดีให้เกิดวัฒนธรรมการเรียนรู้ภายในองค์กรที่สามารถทำให้เกิดขึ้นได้ในทุกที่ทุกเวลาโดยต่อเนื่อง

2.2.3 แนวทางในการแก้ไขปัญหาหรือพัฒนานโยบายที่สอดคล้องกับการวิเคราะห์

ภายใต้กรอบ PDCA เมื่อได้กำหนดแผนและแนวทางปรับปรุงพัฒนาขีดความสามารถของบุคลากรด้านไซเบอร์และกระบวนงานข่าวกรองทางดิจิทัลและไซเบอร์ด้วยการกำหนดคุณสมบัติและสมรรถนะพื้นฐานของบุคลากรด้านไซเบอร์ขององค์กรแล้ว ในการกำหนดแนวทาง การพัฒนาบุคลากรด้านไซเบอร์ให้เป็นระบบและมีความต่อเนื่องเพื่อให้เกิดประสิทธิภาพสูงสุด เห็นควรพิจารณาการขับเคลื่อนให้เป็นระบบและควบคู่ไปด้วยพร้อมเพรียงกัน ซึ่งรวมถึงการตรวจสอบข้อผิดพลาดหรือความเบี่ยงเบนต่างๆ ในระหว่างเส้นทางการพัฒนาบุคลากรและกระบวนงานที่จะส่งเสริมการพัฒนาบุคลากร ดังนี้

(1) ให้มีการจัดตั้งคณะทำงานเพื่อหาแนวทางร่วมกันระหว่างส่วนงานที่เกี่ยวข้องเพื่อให้ได้ข้อสรุปการบริหารเพื่อพัฒนาบุคลากรด้านไซเบอร์ ซึ่งผู้ปฏิบัติงานต้องมีส่วนร่วมในการให้ข้อคิดเห็นและปัญหาอุปสรรคต่อแนวทางในการพัฒนาศักยภาพบุคลากรด้านไซเบอร์ เพื่อนำไปสู่การออกแบบและจัดทำแผนการปฏิบัติได้อย่างเป็นรูปธรรม โดยผู้บริหารและบุคลากรต้องเข้าใจถึงวัตถุประสงค์และยุทธศาสตร์ภายใต้กรอบการพัฒนาศักยภาพบุคลากร ทั้งนี้คณะทำงานชุดนี้คือกลไกสำคัญในการกำกับดูแลขับเคลื่อนแผนงานและประเมินความสำเร็จของการพัฒนาบุคลากรด้านไซเบอร์ในทุกระดับและทุกขั้นตอน ตามที่จะนำเสนอในลำดับถัดไป

(2) จำแนกความชำนาญและพฤติกรรม สมรรถนะมาตรฐานของแต่ละประเภทบุคลากร ตลอดจนเส้นทางการพัฒนาศักยภาพบุคลากรด้านไซเบอร์ ตามกรอบคุณลักษณะอันพึงประสงค์ของนักการข่าวกรอง สอดคล้องกับแผนพัฒนาบุคลากรตามแผนแม่บทความมั่นคงปลอดภัย (ICT Security Master Plan 2015) ในการระบุและกำหนดความรู้ความสามารถ ทักษะ และสมรรถนะของบุคลากรด้านไซเบอร์ สามารถระบุได้เพียงสังเขปในตาราง ดังนี้

ตารางที่ 1 คุณลักษณะที่พึงประสงค์ของบุคลากรด้านไซเบอร์

<table>
<tr><th></th><th colspan="4">คุณลักษณะที่พึงประสงค์ด้านความรู้ ความสามารถ ทักษะ และสมรรถนะของบุคลากรด้านไซเบอร์</th></tr>
<tr><th></th><th>กลุ่มพัฒนาเครือข่าย</th><th>กลุ่มโปรแกรมเมอร์</th><th>กลุ่มพิสูจน์หลักฐานทางไซเบอร์</th><th>กลุ่มต่อต้านข่าวกรองทางไซเบอร์</th></tr>
<tr><td>ความรู้ด้านการข่าว</td><td colspan="4">- ความรู้เกี่ยวกับการข่าวและวงรอบข่าวกรอง
- ความรู้ความเชี่ยวชาญเรื่องภัยคุกคามด้านต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงของประเทศ
- ความรู้เรื่องบริบทโลก แนวโน้มสถานการณ์โลก และความสัมพันธ์ระหว่างประเทศ
- ความรู้เกี่ยวกับแนวทาง ทิศทางหรือนโยบายของการพัฒนาประเทศ เฉพาะในประเด็นที่เกี่ยวข้องกับองค์กร เช่น ยุทธศาสตร์ชาติ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนปฏิรูปประเทศ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ เป็นต้น
- ความรู้ด้านเกี่ยวกับกฎหมาย/ระเบียบ/กฎกระทรวงต่าง ๆ ที่เกี่ยวกับการปฏิบัติราชการ</td></tr>
<tr><td>ความรู้ด้านดิจิทัลและไซเบอร์</td><td colspan="4">- ความรู้ด้านเทคโนโลยีที่เกี่ยวข้องกับงาน เช่น แนวโน้มที่จะเกิดขึ้นในยุคดิจิทัลในอนาคต ผลกระทบต่าง ๆ ของเทคโนโลยีในปัจจุบัน</td></tr>
<tr><td>ความรู้ความสามารถเฉพาะทาง</td><td>ระบบเครือข่ายคอมพิวเตอร์และระบบปฏิบัติการคอมพิวเตอร์</td><td>วิทยาศาสตร์ หรือ วิศวกรรมศาสตร์คอมพิวเตอร์</td><td>Cyber Forensic Cyber Investigation</td><td>Data Science</td></tr>
<tr><td>ทักษะหลัก (Hard Skills)</td><td colspan="4">• ระบบเครือข่ายและ Cloud
• AI / การเรียนรู้ของเครื่อง
• Internet of Things (IoTs)
•การรักษาความปลอดภัยทางไซเบอร์</td></tr>
<tr><td>ทักษะรอง (Soft Skills)</td><td colspan="4">- การสื่อสาร - การทำงานร่วมกัน
- ให้คำปรึกษา - การฝึกสอน
- การแก้ปัญหา - การริเริ่ม/นวัตกรรม</td></tr>
</table>

ในขั้นตอนการตรวจสอบ (Check) ขีดความสามารถเชิงดิจิทัลของบุคลากร ในปัจจุบันมีรูปแบบการวัดผลหรือมาตรฐานความรู้ความสามารถของบุคลากรด้านไซเบอร์ที่เป็นที่นิยม คือ การกำหนดตัวชี้วัดจากใบประกาศนียบัตร หรือ IT Certificate ซึ่งเป็นประกาศนียบัตรในผลิตภัณฑ์หรือการบริการต่างๆไม่ว่าจะเป็นซอฟต์แวร์ (Software) หรือฮาร์ดแวร์ (Hardware) ว่าบุคคลนั้นมีความรู้ความชำนาญในเรื่องของผลิตภัณฑ์หรือบริการนั้นๆสามารถที่จะทำงานที่เกี่ยวข้องกับผลิตภัณฑ์นั้นได้อย่างมีประสิทธิภาพ IT Certificate ที่เป็นที่นิยม เช่น ไมโครซอฟท์ ซันไมโครซิสเต็ม ซิสโก้ซิสเต็ม ออราเคิล และโนเวล ซึ่งประกาศนียบัตรของแต่ละผลิตภัณฑ์ก็มีรายละเอียดที่แตกต่างกันไป อย่างไรก็ตาม สำหรับประเทศไทยการยกระดับมาตรฐานบุคลากรด้าน IT ก็มีการกำหนดไว้ในแผนแม่บทความมั่นคงปลอดภัย (ICT Security Master Plan 2015) ซึ่งพิจารณาแล้วเห็นว่าบุคลากรด้านไซเบอร์ของหน่วยงานจำเป็นต้องเข้ารับการอบรมและผ่านเกณฑ์ความรู้ความสามารถทางด้านเทคโนโลยีสารสนเทศด้าน Core Competency และ ICT Security ตามเกณฑ์ของ ICT Security Master Plan 2015 ถึงระดับ 3 เป็นอย่างน้อย ดังนี้

ระดับ 5 : End User/ผู้ใช้งานทั่วไป

ระดับ 4 : บุคลากรปฏิบัติการด้านสารสนเทศ ระดับ PC และระบบงาน

ระดับ 3 : บุคลากรระบบเครือข่าย บริหารระบบ

ระดับ 2 : ผู้บริหารระดับกลาง ผู้บริหารด้านสารสนเทศ ระดับกระบวนงานและกรรมวิธี

ระดับ 1 : ผู้บริหารระดับสูง ผู้บริหารระดับนโยบาย และวิสัยทัศน์

ตารางที่ 2 แสดงการจำแนกความชำนาญและพฤติกรรม สมรรถนะของแต่ละประเภทบุคลากร

ประเภทบุคลากร	**ความชำนาญ**	**พฤติกรรมสมรรถนะ**
ระดับ 5 ระดับ 4	มีความรู้ด้านความมั่นคงปลอดภัยด้านสารสนเทศในระดับปฏิบัติการ รวมทั้งมีวินัยในการใช้ ICT ตามภารกิจ และมีความซื่อสัตย์ในการค้นหา จัดเก็บ และรักษาข้อมูล	1.1 สามารถใช้เทคโนโลยีสารสนเทศได้อย่างถูกต้องตามหลักความมั่นคงปลอดภัย 1.2 สามารถค้นหาจัดเก็บและรักษาข้อมูลโดยใช้ระบบเทคโนโลยี 1.3 ใช้สารสนเทศตามหลักความมั่นคงปลอดภัย
ระดับ 4 ระดับ 3	สามารถเสนอแนะและมีความชำนาญในการจัดเก็บและวิเคราะห์ข้อมูลความมั่นคง	2.1 สามารถกำหนดรูปแบบการจัดเก็บข้อมูลในองค์กรตามความรับผิดชอบของตนเองในองค์กรได้อย่างถูกต้องสมบูรณ์ตามหลักความมั่นคงปลอดภัย

ประเภทบุคลากร	ความชำนาญ	พฤติกรรมสมรรถนะ
	ปลอดภัย เข้าใจและสามารถใช้อุปกรณ์ความมั่นคงปลอดภัยในระดับเครือข่ายและคอมพิวเตอร์ได้	2.2 สามารถใช้โปรแกรมและอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องจำเป็นในการปฏิบัติงานในขั้นชำนาญการได้เป็นอย่างดี 2.3 บำรุงรักษาอุปกรณ์ขั้นพื้นฐานได้อย่างถูกวิธีและสามารถใช้ได้อย่างต่อเนื่อง
ระดับ 3 ระดับ 2	สามารถวิเคราะห์ประมวลผลแปรข้อมูลสารสนเทศให้เกิดเป็นองค์ความรู้และสามารถถ่ายทอดสื่อสารรวมทั้งแก้ไข ปัญหาเบื้องต้นด้านความมั่นคงปลอดภัยให้กับผู้ปฏิบัติการได้	3.1 กำกับดูแลการปฏิบัติงานให้บรรลุตามเป้าประสงค์ที่กำหนดและสอดส่องการโจมตีจากภายในและภายนอก 3.2 ระบุแนวทางใหม่ๆ ในการบริหาร จัดการระบบงานภายในความต้องการด้านความมั่นคงปลอดภัยได้ 3.3 สามารถนำข้อมูลด้านความมั่นคงปลอดภัยระหว่างหน่วยงานมาบูรณาการกัน เพื่อใช้ประโยชน์ร่วมกันได้ 3.4 สามารถวิเคราะห์และประเมินผล การถูกโจมตีหรือการเกิดปัญหาด้านความมั่นคงปลอดภัย 3.5 สามารถวิเคราะห์และดำเนินการแก้ไขปัญหาที่เกิดจากความมั่นคงปลอดภัยตามมาตรฐานการบริหารจัดการความปลอดภัย
ระดับ 2	สามารถให้ข้อเสนอแนะแก่ผู้ที่เกี่ยวข้องเพื่อการตัดสินใจแก้ไขปัญหาด้านความมั่นคงปลอดภัยที่มีความซับซ้อนและสามารถพัฒนาบุคลากรให้สามารถใช้เทคโนโลยีสารสนเทศ ได้อย่างปลอดภัย	4.1 สามารถวิเคราะห์ระบบและให้ข้อเสนอแนะแก่ผู้เกี่ยวข้องตามความต้องการเมื่อเกิดปัญหาความปลอดภัยในด้านเทคโนโลยีสารสนเทศ 4.2 กำกับดูแลแนวทางปฏิบัติงานโดยใช้เทคโนโลยีสารสนเทศแก่เจ้าหน้าที่ระดับปฏิบัติการได้อย่างชัดเจน 4.3 สามารถสร้างระบบข้อมูลสารสนเทศที่มั่นคงปลอดภัยที่ต้องการใช้งานได้

ประเภทบุคลากร	ความชำนาญ	พฤติกรรมสมรรถนะ
		4.4 สามารถเชื่อมโยงเครือข่ายข้อมูลสารสนเทศระหว่างหน่วยงานได้ทุกระดับ ตั้งแต่หน่วยงานจนถึงระดับประเทศอย่างมั่นคงปลอดภัย
ระดับ 1	กำหนดนโยบายสั่งการและผลักดันการใช้ระบบสารสนเทศตามหลักความมั่นคงปลอดภัยให้สอดคล้องกับภารกิจขององค์กรตลอดจนบรรลุผลสำเร็จเชื่อมโยงเครือข่ายในเชิงบูรณาการทั้งในระดับประเทศและสากล	5.1 มีความเป็นผู้นำในการกำหนดนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและผลักดันให้เกิดการนำไปใช้ได้จริง จนเกิดเป็นผลสัมฤทธิ์ตามวิสัยทัศน์ของหน่วยงาน 5.2 สามารถระบุความเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศจากสถานการณ์ภายนอกได้อย่างแม่นยำ 5.3 เข้าใจในเรื่องการบริหารความเสี่ยงความต่อเนื่องธุรกิจ การจัดการกับภัยฉุกเฉิน และมาตรฐานสากลด้านบริหารความมั่นคงปลอดภัย

(3) จัดตั้งคณะทำงานเพื่อขับเคลื่อนการแปลงองค์ความรู้พื้นฐานและความรู้ที่สำคัญในงานข่าวกรองให้อยู่ในระบบดิจิทัล รวมทั้งพัฒนาเครื่องมือรวบรวมคัดกรอง Big Data ที่สนับสนุนภารกิจงานข่าวกรอง

(4) วางระบบงาน Virtual working Team เพื่อส่งเสริมปัจจัยบวกให้แก่สภาพแวดล้อมในการทำงานและวัฒนธรรมความร่วมมือในการทำงานแบบ Virtual ให้สอดคล้องกับการปฏิบัติงานยุคดิจิทัล โดยเฉพาะการเพิ่มศักยภาพในการปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยไม่มีข้อจำกัดเรื่องเวลาและสถานที่ มีการทำงานแบบยืดหยุ่น รวมทั้งใช้แพลตฟอร์มเทคโนโลยีเข้ามาเป็นเครื่องมือสนับสนุนการทำงานได้

(5) จำลองทีมปฏิบัติการไซเบอร์เฉพาะกิจในหลายระดับในการป้องกันภัยคุกคามทางไซเบอร์ เพื่อเป็นการซักซ้อมและเพิ่มประสบการณ์การทำงานให้แก่บุคลากรที่เอื้อให้เกิดการผสมผสานระหว่างบุคลากรรุ่นอาวุโสและรุ่นใหม่ ที่มีความแตกต่างกันทั้งกรอบแนวคิด (mindset) ทักษะเชิงอนาล็อกและดิจิทัล การแลกเปลี่ยนมุมมองความคิด และการถ่ายทอดความชำนาญส่งมอบต่อกันและกัน

(6) จัดโครงการแข่งขันทักษะความสามารถด้านการสืบสวนทางไซเบอร์และการต่อต้านข่าวกรองทางไซเบอร์ ในลักษณะเดียวกับการแข่งขันแฮกเกอร์ เพื่อกระตุ้นให้เกิดการริเริ่ม

สร้างสรรค์และพัฒนานวัตกรรมการทำงานรูปแบบใหม่ให้ทันท่วงที สามารถรับมือกับภัยคุกคามทางระบบไซเบอร์ได้

ทั้งนี้ เพื่อให้สอดรับกับข้อมูลที่เกี่ยวข้อง จึงได้จัดทำแนวทางในการขับเคลื่อนเพื่อให้เกิดการพัฒนาทักษะของบุคลากรด้านไซเบอร์ตามมาตรฐานสากล ภายใต้กรอบการพัฒนาคนและงานตามหลัก PDCA ดังนี้

แผนงานที่ 1 การพัฒนาความรู้ด้านการข่าว

- การจัดทำองค์ความรู้เกี่ยวกับการข่าวกรองและวงรอบข่าวกรอง ภัยคุกคามด้านต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงของประเทศ แนวโน้มสถานการณ์โลก และความสัมพันธ์ระหว่างประเทศ แนวทางและทิศทางหรือนโยบายของการพัฒนาประเทศ เฉพาะในประเด็นที่เกี่ยวข้องกับองค์กร ข้อกฎหมายที่เกี่ยวข้อง ได้แก่ พ.ร.บ.ข่าวกรองแห่งชาติ พ.ศ.2562 พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 และการระมัดระวังเกี่ยวกับข้อกฎหมายด้านสิทธิมนุษยชน
- การจัดทำแผนการฝึกด้านการข่าวในการบังคับใช้กฎหมาย ตามอำนาจและหน้าที่ตามกฎหมาย และการปฏิบัติหน้าที่ตามหลักสิทธิมนุษยชน
- การจัดฝึกอบรมโดยการถ่ายทอดความรู้ภายในหน่วยงาน และการแลกเปลี่ยนประสบการณ์กับหน่วยงานพันธมิตร และหน่วยข่าวกรองมิตรประเทศ
- การจำลองเหตุการณ์จริง โดยใช้สถานที่จำลองเสมือนกำลังเกิดเหตุการณ์จริง
- การสอบวัดความรู้ และทบทวนการฝึก
- ประเมินผลการปฏิบัติ

แผนงานที่ 2 การพัฒนาความรู้ด้านดิจิทัลและไซเบอร์ การพัฒนาทักษะ และเสริมองค์ความรู้ด้านเทคโนโลยีที่เกี่ยวข้องกับงาน เช่น แนวโน้มที่จะเกิดขึ้นในยุคดิจิทัลในอนาคต ผลกระทบต่าง ๆ ของเทคโนโลยีในปัจจุบัน

- การจัดทำแผนการดำเนินงาน เช่น การเชิญวิทยากรภายนอกมาให้ความรู้
- การจัดประชุมแลกเปลี่ยนแนวคิดองค์ความรู้ และวิเคราะห์แนวโน้มด้านไซเบอร์ในอนาคต
- การร่วมพัฒนา แลกเปลี่ยนองค์ความรู้ และจัดทำแผนงานโครงการกับหน่วยงานที่เกี่ยวข้อง เช่น การจัดทำโครงการพัฒนาเครื่องมือสำหรับงานสืบสวน ร่วมกับคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)

แผนงานที่ 3 การพัฒนาความรู้ความสามารถเฉพาะทางด้านไซเบอร์ 4 แขนง ประกอบด้วย 1) ระบบเครือข่ายและระบบปฏิบัติการ 2) วิศวกรรมซอฟต์แวร์ 3) การพิสูจน์หลักฐานและการสืบสวนทางไซเบอร์ 4) วิทยาศาสตร์ข้อมูล การวิเคราะห์ข้อมูล และการแสดงข้อมูล

- การพัฒนาทักษะ โดยการจัดฝึกอบรมในลักษณะการถ่ายทอดให้ความรู้ภายในหน่วยงาน
- การจัดฝึกอบรมจากหน่วยงานภายนอกและการแลกเปลี่ยนเรียนรู้ระหว่างหน่วยงานภายนอก
- การแลกเปลี่ยนเรียนรู้ ศึกษาดูงานกับหน่วยข่าวมิตรประเทศ เพื่อแลกเปลี่ยนประสบการณ์และวิธีการในการรับมือ และแก้ไขปัญหา
- การถ่ายทอด และเก็บรักษาองค์ความรู้ที่ได้ในระหว่างการฝึกอบรม รวมถึงการแลกเปลี่ยนเรียนรู้

แผนการปฏิบัติ

ตารางที่ 3 แผนงานที่ 1 การพัฒนาความรู้ด้านการข่าว แผนงานที่ 2 การพัฒนาความรู้ด้านดิจิทัลและไซเบอร์ และแผนงานที่ 3 การพัฒนาความรู้ความสามารถเฉพาะทางด้านไซเบอร์ 4 แขนง

ลำดับ	แผน/กิจกรรม	เดือนที่											
		1	2	3	4	5	6	7	8	9	10	11	12
แผนงานที่ 1 การพัฒนาความรู้ด้านการข่าว													
1.	จัดตั้งคณะทำงานเพื่อออกแบบหลักสูตรสำหรับการฝึก	↔											
2.	ประชุมร่วมกันเพื่อวางแนวทางในการสอน		↔										
3.	จัดทำแผน ตารางสอน กำหนดขอบเขตเนื้อหา และผู้รับผิดชอบ		↔	↔									
4.	ดำเนินการฝึกอบรม				↔	↔	↔						
5.	ทดสอบวัดความรู้							↔					
6.	ติดตามประเมินผล								↔	↔			

ลำดับ	แผน/กิจกรรม	เดือนที่											
		1	2	3	4	5	6	7	8	9	10	11	12
7.	ทบทวนการฝึกหลังกลับไปปฏิบัติงานจริง											↔	
แผนงานที่ 2 การพัฒนาความรู้ด้านดิจิทัลและไซเบอร์													
1.	จัดตั้งคณะทำงาน	↔											
2	ประชุมเพื่อกำหนดแนวทางในการพัฒนาทักษะ และองค์ความรู้ประจำปี	←	→	→					←	→	→		
3.	จัดตั้งคณะทำงานที่รับผิดชอบโครงการร่วมกับหน่วยนอก	↔											
4.	จัดทำแผนการอบรม/บรรยาย/การเชิญวิทยากร		←	→	→								
5.	ดำเนินการตามแผนงานที่กำหนด		←	→	→	→	→	→	→	→	→	→	→
6.	ติดตามและประเมินผล						↔						↔
แผนงานที่ 3 การพัฒนาความรู้ความสามารถเฉพาะทางด้านไซเบอร์ 4 แขนง													
1.	จัดทำแผน/โครงการในการดำเนินงาน	↔											
2.	จัดทำแผนพัฒนาทักษะเจ้าหน้าที่ในหน่วยงาน		↔										
3.	จัดทำแผนฝึกอบรมเพื่อพัฒนาทักษะและแลกเปลี่ยนเรียนรู้ระหว่างหน่วยงาน		↔										
4.	จัดทำแผนสำหรับการแลกเปลี่ยนประสบการณ์			↔									

ลำดับ	แผน/กิจกรรม	เดือนที่											
		1	2	3	4	5	6	7	8	9	10	11	12
	และศึกษาดูงานกับหน่วยข่าวมิตรประเทศ												
5.	ดำเนินการตามแผนงาน	←	—	—	—	—	—	—	—	—	—	—	→
6.	จัดทำเอกสารองค์ความรู้หลังการฝึกอบรม และแลกเปลี่ยนเรียนรู้	←	—	—	—	—	—	—	—	—	—	—	→
7.	บรรยายเพื่อถ่ายทอดองค์ความรู้แก่เจ้าหน้าที่ในแขนงอื่น ๆ	←	—	—	—	—	—	—	—	—	—	—	→
8.	ติดตามและประเมินผลการเข้ารับการฝึกอบรม และการแลกเปลี่ยนเรียนรู้						↔						↔

2.2.4 ปัจจัยที่อาจมีผลกระทบต่อความสำเร็จของการดำเนินการตามข้อเสนอ แนวทางบริหารจัดการที่เป็นรูปธรรม

โดยปกติการดำเนินการใด ๆ ก็ตาม มักพบว่ามีปัจจัยเสี่ยงใน 4 ด้าน ได้แก่ 1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) 2) ความเสี่ยงด้านการเงิน (Financial Risk) 3) ความเสี่ยงด้านการปฏิบัติการ (Operation Risk) และ 4) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) สำหรับการดำเนินระบบงานข่าวกรอง เฉพาะอย่างยิ่งการมุ่งการพัฒนาบุคลากรเพื่อยกระดับศักยภาพของบุคลากรด้านไซเบอร์ไปสู่ความสำเร็จตามวัตถุประสงค์ได้นั้น มีความเป็นไปได้ที่จะเผชิญกับปัจจัยเสี่ยงในการนำข้อเสนอและแผนงานต่างๆ ข้างต้นไปสู่การปฏิบัติ พบว่า ปัจจัยเสี่ยงที่มีความเป็นไปได้หรืออาจได้รับผลกระทบมากที่สุด คือ ความเสี่ยงด้านการปฏิบัติการ (Operation Risk) ซึ่งสามารถแจกแจงวิเคราะห์ได้ตามตารางต่อไปนี้

ตารางที่ 4 แสดงปัจจัยความเสี่ยงด้านการปฏิบัติการ (Operation Risk) ซึ่งอาจมีผลต่อความสำเร็จและแนวทางการบริหารจัดการ

ลำดับที่	ปัจจัยที่อาจมีผลต่อความสำเร็จ	แนวทางการบริหารจัดการ
1	ประเด็นการพัฒนาทักษะทางไซเบอร์ให้ตรงตามความต้องการของผู้ใช้งานอย่างแท้จริง	- ผู้เข้ารับการพัฒนาศักยภาพต้องเรียนรู้แนวทางจัดการความเสี่ยงในการพัฒนาระบบที่ใช้งาน คือ การกำหนดให้ผู้พัฒนาซอฟต์แวร์ระบบติดตั้งซอฟต์แวร์ที่ต้องครอบคลุมเรื่องการรักษาความปลอดภัย เป็นเทคโนโลยีที่เข้ากันได้กับระบบที่มีอยู่และรองรับเทคโนโลยีดิจิทัลในอนาคต โดยให้บุคลากรผู้ใช้งานสามารถทดสอบการทำงานและความเสี่ยงเป็นระยะ -การสืบสวนทางสื่อสังคมออนไลน์มีความเสี่ยงในการลงทุนด้านเครื่องมือทางเทคนิคที่จะเกิดขึ้น การวางแผนพัฒนาทักษะและเทคโนโลยีในระยะยาวจะช่วยให้สามารถลดค่าใช้จ่ายที่จะเกิดขึ้นในอนาคตได้ แต่ต้องใช้ระยะเวลาในการพัฒนา แนวทางจัดการปัญหาในระยะสั้นหรือในระหว่างที่พัฒนาบุคลากรอาจจัดหาผู้เชี่ยวชาญมาเป็นที่ปรึกษาและทำงานร่วมกัน
2	ประเด็นการเตรียมทีมบุคลากรที่มีความรอบรู้ในการบริหารจัดการระบบและเครื่องมือพิเศษ	- คัดเลือกบุคลากรที่มีศักยภาพและบุคลากรรุ่นใหม่ที่มีความรู้ด้านเทคโนโลยีสารสนเทศ หรือวิทยาการคอมพิวเตอร์ ให้เข้ามาปฏิบัติหน้าที่โดยให้เรียนรู้จากการปฏิบัติงานจริง และอบรมจากผู้พัฒนาระบบหรือเครื่องมือพิเศษโดยตรง - ขอความร่วมมือจากหน่วยข่าวต่างประเทศที่เป็นพันธมิตรในการอบรมให้ความรู้ในเรื่องระบบและเครื่องมือพิเศษ ในลักษณะการฝึกปฏิบัติงานไปพร้อมกับการทำงานจริง (On Job Training : OJT) เพื่อเรียนรู้และพัฒนาทักษะการทำงาน ยกระดับแนวทางการศึกษาหาเทคนิค และระบบเทคโนโลยี

ลำดับที่	ปัจจัยที่อาจมีผลต่อความสำเร็จ	แนวทางการบริหารจัดการ
		ต่างๆที่สามารถรับมือต่อภัยคุกคาม และสนับสนุนการปฏิบัติการสืบสวนบนไซเบอร์
3.	ประเด็นเรื่องเครื่องมือพิเศษและการปรับเปลี่ยนเทคโนโลยีที่รวดเร็วในการเอื้ออำนวยต่อประสิทธิภาพการปฏิบัติงานของบุคลากร	- เครื่องมือเทคโนโลยีแต่ละชนิดมีราคาสูง และเปลี่ยนแปลงอย่างรวดเร็ว ประกอบกับการจัดซื้อจัดหาต้องปฏิบัติตามกฎระเบียบทางราชการที่ยุ่งยาก สลับซับซ้อน มีความเสี่ยง ในช่วงหลังการจัดหางบประมาณไม่ได้เป็นอุปสรรคมากเท่ากับการปฏิบัติตามกฎระเบียบที่ยุ่งยาก จึงเห็นสมควรปรับปรุงกฎระเบียบการจัดซื้อใหม่ ให้สะดวกต่อการปฏิบัติ หรือปรับเปลี่ยนเป็นการเช่าซื้อ ซึ่งจะสามารถรับมือกับการเปลี่ยนแปลงเทคโนโลยีที่รวดเร็วได้ - การจัดหาเครื่องมือพิเศษ ควรวางแผนงบประมาณว่าควรจะมีเครื่องมืออะไรบ้าง ทั้งในเชิงรุกและเชิงรับ เพื่อตอบสนองต่อบทบาทของหน่วยงานในด้านการสืบสวนทางสื่อออนไลน์ในอนาคต
4	ประเด็นการปฏิบัติในการพิสูจน์ทราบหาตัวตนผู้กระทำความผิดบนสื่อสังคมออนไลน์ เพื่อป้องกันภัยคุกคามทางไซเบอร์	- ควรมีการจัดสร้างระบบการตรวจสอบข้อมูลจราจรบนอินเทอร์เน็ตที่ถูกต้องตามกฎหมาย หรือ Lawful Interception ซึ่งหมายถึงการจัดตั้งองค์กรกลางระดับชาติที่ชอบด้วยกฎหมาย มีหน้าที่ออกกฎระเบียบและวางโครงสร้างระบบอินเทอร์เน็ตของประเทศ ให้ง่ายต่อการตรวจสอบและเก็บรวบรวมข้อมูลทางเทคนิค สะดวกและรวดเร็วต่อการสืบสวนพิสูจน์ทราบผู้กระทำผิดต่างๆ ทั้งอาชญากรทางคอมพิวเตอร์ หรือผู้ก่อการร้ายที่ใช้อินเทอร์เน็ต เป็นเครื่องมือในการเผยแพร่แนวความคิดรุนแรง เป็นต้น

ลำดับที่	ปัจจัยที่อาจมีผลต่อความสำเร็จ	แนวทางการบริหารจัดการ
5	ประเด็นความร่วมมือกับหน่วยงานภาคเอกชนและบริษัทต่างชาติ กรณีการขอความร่วมมือในการตรวจสอบข้อมูล	-หน่วยงานความมั่นคงควรหาช่องทางในการขอความร่วมมือกับบริษัทต่างชาติที่ให้บริการสื่อสังคมออนไลน์ เพื่อออกมาตรการป้องกันมิให้ผู้ประสงค์ร้ายต่อความมั่นคงของชาติ หรือเป็นภัยคุกคามทางไซเบอร์เข้ามาใช้ประโยชน์ รวมทั้งสร้างความร่วมมือและความไว้วางใจในการตรวจสอบและสืบสวนข้อมูลบนเครือข่ายในประเด็นที่เกี่ยวข้องกับความมั่นคงของชาติให้มีประสิทธิภาพ รวมถึงเร่งแก้ไขปัญหาความไม่รัดกุมในการรับจดทะเบียน การใช้บริการเครือข่ายอินเทอร์เน็ตและโทรศัพท์เคลื่อนที่โดยเร็ว

2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ

ภาวะผู้นำหมายถึง กระบวนการหรือวิธีการที่ทำให้เกิดปฏิสัมพันธ์ระหว่างบุคคล หรือกลุ่มบุคคล ก่อให้เกิดการกระทำ หรือกิจกรรมเพื่อให้สามารถปฏิบัติภารกิจที่ได้รับมอบหมาย โดยใช้อำนาจ อิทธิพล แรงจูงใจ และการตัดสินใจอย่างมีศิลปะ รวมถึงการมีส่วนร่วมในการเปลี่ยนแปลงและสร้างทัศนคติ ความเชื่อมั่น เพื่อนำไปสู่การดำเนินการใดๆให้ประสบผลสำเร็จ ทั้งนี้ในการศึกษาเกี่ยวกับภาวะผู้นำและการขับเคลื่อนของนักทฤษฎีหรือนักคิดที่มีชื่อเสียงเป็นที่ยอมรับ เพื่อเป็นทางเลือกในการนำมาปรับใช้กับองค์กรให้เหมาะสมนั้น เห็นว่าทฤษฎีภาวะผู้นำตามหลักแนวคิดของ Bernad M. Bass (1999) มีความเหมาะสมอย่างยิ่งที่ผู้บริหารในองค์กรข่าวกรองควรจะนำมาประยุกต์ใช้ เพื่อให้เกิดการขับเคลื่อนต่อการดำเนินงานและการพัฒนาศักยภาพบุคลากรให้สอดคล้องตามวัตถุประสงค์ของหน่วยงาน ภายใต้ยุทธศาสตร์ไทยแลนด์ 4.0 โดยผู้บริหารจำเป็นต้องมีภาวะผู้นำดังนี้

(1) มีอิทธิพลอย่างมีอุดมการณ์ หมายถึง การปฏิบัติตนให้เป็นแบบอย่างที่ดี ทำให้ผู้ปฏิบัติงานเกิดความภาคภูมิใจเมื่อร่วมงานกัน สามารถถ่ายทอดวิสัยทัศน์ไปยังผู้ตาม มีภาวะการควบคุมอารมณ์ในสถานการณ์วิกฤต มีความน่าเชื่อถือ ไว้วางใจ มีศีลธรรมและจริยธรรม ประพฤติตนให้เกิดประโยชน์แก่ส่วนรวม และแน่วแน่ในอุดมการณ์ มุ่งเน้นผลประโยชน์ของชาติและประชาชนเป็นหลัก โดยไม่ใช้ความรู้ที่ได้จากการปฏิบัติงานไปในเรื่องส่วนตัว

(2) สร้างแรงบันดาลใจ จูงใจให้ผู้ตามเกิดแรงบันดาลใจ กระตือรือร้น ท้าทายต่องานที่รับผิดชอบ สร้างเจตคติแง่บวก โดยผู้บริหารจะต้องแสดงออกถึงการอุทิศตัว โน้มน้าวให้ผู้ปฏิบัติงานเกิดความรู้สึกร่วมต่อเป้าหมาย และวิสัยทัศน์ของหน่วยงาน คือ “เป็นหน่วยข่าวกรองที่ทันสมัย เพื่อความมั่นคงของชาติและประชาชน” เป็นสำคัญ ต้องแสดงให้เห็นถึงความตั้งใจแน่วแน่ว่าจะสามารถบรรลุเป้าหมายได้ ช่วยให้ผู้ปฏิบัติงานมองข้ามผลประโยชน์ตน มุ่งสร้างแรงบันดาลใจและกระตุ้นให้เกิดภูมิปัญญา เพื่อให้ผู้ปฏิบัติงานสามารถผ่านพ้นอุปสรรค กระตุ้นให้เกิดความรู้สึกภาคภูมิใจในการปฏิบัติงานในฐานะหน่วยข่าวกรองพลเรือน มุ่งไปสู่วิสัยทัศน์แห่งการพัฒนาไปสู่ความเป็นเลิศและผู้นำเทคโนโลยีข่าวกรอง

(3) กระตุ้นเชาว์ปัญญา ผู้บริหารต้องสามารถกระตุ้นให้ผู้ปฏิบัติงานเกิดการสร้างสรรค์สิ่งใหม่ ๆ แสวงหาแนวทางใหม่ ๆ มาแก้ปัญหาในหน่วยงาน ต้องสร้างความเชื่อมั่นว่าปัญหาทุกอย่างมีวิธีการแก้ไข กระตุ้นให้ผู้ปฏิบัติงานรู้สึกท้าทายหากเกิดปัญหา ต้องพิสูจน์ว่าสามารถเอาชนะอุปสรรคได้โดยมาจากความร่วมมือร่วมใจของทุกคน ส่งเสริมและสนับสนุนการเรียนรู้ทุกรูปแบบ เช่น การจัดทำโครงการที่ส่งเสริมต่อการพัฒนาตนเองทั้งในและต่างประเทศ เปิดโอกาสให้ผู้ปฏิบัติงานได้เสนอแนวคิด และเทคโนโลยีใหม่ ๆ เพื่อใช้สำหรับปฏิบัติงานด้านการข่าว โดยไม่ทำให้ผู้เสนอรู้สึกอับอาย หรือรู้สึกด้อยค่า

(4) การคำนึงถึงปัจเจกบุคคล คือ การดูแลเอาใจใส่ต่อผู้ปฏิบัติงานเป็นรายบุคคล ทำให้รู้สึกถึงคุณค่าและมีความสำคัญ ผู้บริหารต้องเป็นผู้แนะแนวทางและเป็นที่ปรึกษา เพื่อการพัฒนาผู้ปฏิบัติงาน ต้องเอาใจใส่เป็นพิเศษในความต้องการของแต่ละบุคคล เพื่อมุ่งผลสัมฤทธิ์และความก้าวหน้าของแต่ละคน เปิดโอกาสให้เรียนรู้สิ่งใหม่ ๆ เข้าใจและยอมรับความแตกต่างระหว่างบุคคล

(5) นำการปรับตัว หมายถึง ความสามารถของในการหยั่งรู้ และตอบสนองต่อสภาวะแวดล้อมที่เปลี่ยนแปลงไปตลอดเวลา ผู้บริหารต้องสำรวจสภาพแวดล้อมภายนอก พิสูจน์ทราบภัยคุกคามและโอกาส ทำความเข้าใจช่องว่างระหว่างขีดความสามารถและสิ่งท้าทาย ทดลองนำความคิดใหม่ๆมาใช้โดยเรียนรู้จากประสบการณ์เดิม หัวใจสำคัญของการปรับตัวคือ ความคล่องตัวในการประสานงาน และเปิดกว้างที่จะรับความคิดใหม่ๆภายนอกองค์กร

(6) การจัดการอย่างเป็นระบบ เนื่องจากการพัฒนาบุคลากรด้านไซเบอร์ เป็นกระบวนการที่ใช้เวลา และต้องอาศัยความร่วมมือของหลายฝ่าย ผู้บริหารจึงจำเป็นต้องมีการจัดการอย่างเป็นระบบ ซึ่งนอกจากการบริหารจัดการบุคลากรแล้ว ยังรวมถึงการวางเป้าหมายระยะสั้นและระยะยาว การจัดทำแผนเพื่อให้บรรลุเป้าหมายต่างๆ การติดตามงบประมาณ และการระดมความคิดใหม่ๆ อยู่ตลอดเวลา การจัดการปัญหาและการแก้ปัญหาความขัดแย้ง

(7) ความสามารถในการสื่อสาร โน้มน้าว และเจรจาต่อรอง เนื่องจากการดำเนินการเพื่อพัฒนาบุคลากรด้านไซเบอร์ หรือนักการข่าวไซเบอร์ ครอบคลุมถึงการกำหนดการรับสมัครบุคคลที่มีคุณสมบัติเฉพาะ ซึ่งจำเป็นต้องได้รับความเห็นชอบจากคณะกรรมการบริหารในการจัดสรรอัตราจำนวนเจ้าหน้าที่ที่สามารถบรรจุได้ ขณะที่การดำเนินการยังรวมถึงการจัดหาเครื่องมือทางเทคนิคที่มีความทันสมัย และต้องใช้งบประมาณจำนวนมาก การพัฒนาบุคลากรอย่างต่อเนื่องจำเป็นต้องได้รับความร่วมมือจากส่วนงานที่เกี่ยวข้องที่อยู่ข้ามสายงานการบังคับบัญชา รวมถึงการแสวงหาความร่วมมือจากภายนอก ซึ่งครอบคลุมไปยังหน่วยงานภาครัฐ ภาคเอกชน (ในและต่างประเทศ) และหน่วยข่าวกรองมิตรประเทศ จึงจำเป็นต้องอาศัยความสามารถในการสื่อสาร การโน้มน้าว และการเจรจาต่อรองของผู้บริหาร เพื่อให้สามารถขับเคลื่อนข้อเสนอได้อย่างมีประสิทธิภาพ

(8) การมอบหมายงานอย่างมีประสิทธิภาพ และการกระจายอำนาจ การพัฒนาบุคลากรด้านไซเบอร์ ไม่สามารถดำเนินการได้โดยส่วนงานใดส่วนงานหนึ่งเพียงลำพัง แต่เป็นการดำเนินการที่ต้องอาศัยความร่วมมือระหว่างสำนัก/กองที่เกี่ยวข้องในการร่วมมือกัน ดังนั้น การมอบหมายงานอย่างมีประสิทธิภาพ ให้กับเจ้าหน้าที่ในส่วนงานที่เกี่ยวข้อง ควบคู่กับการมอบหมายให้ตัดสินใจแทน ในขอบเขตอำนาจที่สามารถกระทำได้ จึงเป็นปัจจัยสำคัญที่จะทำให้ผู้บริหารสามารถผลักดันการดำเนินการตามข้อเสนอให้บรรลุวัตถุประสงค์ได้

คุณสมบัติความเป็นผู้นำหรือมีภาวะผู้นำตามองค์ประกอบดังกล่าวข้างต้น มีความสำคัญอย่างยิ่งที่จะส่งผลให้ผู้บริหารสามารถขับเคลื่อนและกำกับงานข่าวกรองด้านไซเบอร์และดิจิทัล ไปสู่ความสำเร็จในการพัฒนางานข่าวกรอง การพัฒนาศักยภาพบุคลากรให้สอดคล้องตามวัตถุประสงค์ของหน่วยงาน รวมถึงกระตุ้นให้มุ่งนำไปสู่การพัฒนานวัตกรรมใหม่ เพื่อการเป็นองค์กรข่าวกรองดิจิทัลที่ทันสมัยและยั่งยืน

3. แผนพัฒนาตนเอง

(ข้อมูลส่วนบุคคลไม่เผยแพร่)

บรรณานุกรม

พรชัย เจดามาน. **ภาวะผู้นำการเปลี่ยนแปลง ศตวรรษที่ 21 : ไทยแลนด์ 4.0.** สืบค้นจาก http://www.emld-rmu.com/index.php/article1/9-articles/142-21-4-0

สมศักดิ์ วานิชยาภรณ์ และ นิสรา ใจซื่อ. (2562). **การขับเคลื่อนองค์การดิจิทัลเพื่อก้าวสู่การพัฒนาประเทศไทย 4.0.** วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยมหาสารคาม. ปีที่ 38 (ฉบับที่ 3), 78-91 . สืบค้นจาก http://research.msu.ac.th/msu_journal/upload/articles/article2497_29486.pdf

สำนักข่าวกรองแห่งชาติ. (2562) **แผนยุทธศาสตร์สำนักข่าวกรองแห่งชาติ พ.ศ. 2559 - 2564.**

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2550). **แผนแม่บท ICT Security แห่งชาติ** สืบค้นจาก http://www.sea12.go.th/ict/ict_plan/ICT%20Security.pdf

สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร. (2559). **ภาครัฐไทยกับการก้าวเข้าสู่รัฐบาลดิจิทัล.** เอกสารวิชาการอิเล็กทรอนิกส์. สืบค้นจาก http://www.parliament.go.th/library

อรุณรุ่ง เอื้ออารีสุขสกุล และ ธีระวัฒน์ จันทึก. (2558) **การบริหารจัดการคนเก่งเชิงกลยุทธ์: ปัจจัยสำคัญสู่ความได้เปรียบทางการแข่งขันอย่างยั่งยืน**. Veridian E-Journal ฉบับภาษาไทย มหาวิทยาลัยศิลปากร, ปีที่ 8 (ฉบับที่ 3), 1096-1112. สืบค้นจาก https://he02.tci-thaijo.org/index.php/Veridian-E-Journal/article/view/47987

David Siman-Tov and Noam Alon. (2018). **The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs.** Journal of Cyber, Intelligence, and Security, The Institute for National Security Studies. Volume 2 (No. 1), 73-92. Retrieved from https://www.inss.org.il/wp-content/uploads/2018/05/Cyber2.1ENG_5.pdf

Gabi Siboni and Hadas Klein. (2018) **Developing Organizational Capabilities to Manage Cyber Crises.** Journal of Cyber, Intelligence, and Security, The Institute for National Security Studies. Volume 2 (No. 1), 93-104. Retrieved from https://www.inss.org.il/wp-content/uploads/2018/05/Cyber2.1ENG_5.pdf

ประวัติผู้เขียนรายงานการศึกษาส่วนบุคคล

นายวัธนชัย ทองประเสริฐ

ประวัติการศึกษา

ปริญญาตรี ศิลปศาสตรบัณฑิต (รัฐศาสตร์) มหาวิทยาลัยรามคำแหง 2529

ประสบการณ์การรับราชการ

หัวหน้าสำนักข่าวกรองแห่งชาติ จังหวัดเชียงใหม่

อัครราชทูตที่ปรึกษา สถานเอกอัครราชทูต ณ กรุงพนมเปญ

ผลงานทางวิชาการ

เอกสารวิจัยเรื่อง “การประเมินภัยคุกคามทางไซเบอร์ในระยะ 5 ปี (2561-2565)” เสนอสถาบันการข่าวกรอง สำนักข่าวกรองแห่งชาติ เพื่อประกอบการศึกษาหลักสูตรการบริหารจัดการความมั่นคงแห่งชาติ (บมช.) รุ่นที่ 11

ตำแหน่งหน้าที่ปัจจุบันและสถานที่ทำงาน

ผู้อำนวยการกอง 2 สำนักข่าวกรองแห่งชาติ

สำนักข่าวกรองแห่งชาติ เลขที่ 321 ถนนราชดำเนินนอก เขตดุสิต กรุงเทพฯ 10300