แนวทางการพัฒนากำลังพลด้านไซเบอร์
เพื่อพร้อมรับภัยคุกคามระดับชาติ

โดย

พลตรี ปรัชญา เฉลิมวัฒน์
ผู้ชำนาญการ
สำนักงานปลัดกระทรวงกลาโหม

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60
ประจำปีการศึกษา พุทธศักราช 2560 - 2561

บทคัดย่อ

เรื่อง **แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ**

ลักษณะวิชา **วิทยาศาสตร์และเทคโนโลยี**

ผู้วิจัย **พลตรี ปรัชญา เฉลิมวัฒน์ หลักสูตร วปอ. รุ่นที่ 60**

"มิติไซเบอร์" หรือ "ไซเบอร์สเปซ" (Cyber Space) กลายเป็นศัพท์ใหม่ที่ได้รับการยอมรับในสังคมโลกอย่างรวดเร็วและเป็นสิ่งที่ยากที่จะหลีกเลี่ยงการเกี่ยวข้องด้วย ข้อมูลจำนวนมหาศาลเดินทางไปในมิติไซเบอร์ผ่านการเชื่อมต่ออินเทอร์เน็ตเพื่อตอบสนองความต้องการในเรื่องความสะดวกสบาย รวดเร็ว การแลกเปลี่ยนข้อมูลข่าวสาร การลดความซับซ้อนของการทำงาน รวมถึงการใช้บริการข้อมูลต่าง ๆ อย่างไรก็ตาม ภัยคุกคามที่ทุกชาติให้ความสำคัญในยุคปัจจุบันคือปัญหาความไม่ปลอดภัยในการใช้งานในระบบอินเทอร์เน็ตเนื่องจากมิจฉาชีพต่างก็ปรับตัวให้เข้ากับสภาพแวดล้อมที่เปลี่ยนไป นอกจากนั้นชาติที่เป็นมหาอำนาจต่างก็ยอมรับในเรื่องการยกระดับของภัยคุกคามขึ้นเป็นระดับ "สงครามไซเบอร์" ทั้งในระดับยุทธศาสตร์และระดับปฏิบัติการ ความพยายามเสริมสร้างกำลังพลด้านไซเบอร์เพื่อเตรียมรับมือกับภัยคุกคามด้านไซเบอร์ทั้งในระดับกองทัพและระดับความมั่นคงของประเทศทำให้ต้องเผชิญกับปัญหาการขาดแคลนกำลังพลด้านไซเบอร์อย่างหลีกเลี่ยงไม่ได้ เนื่องจากผู้ที่จะสามารถปฏิบัติการไซเบอร์ได้อย่างจริงจังนั้นต้องมีพื้นฐานเชิงสหวิทยาการของคอมพิวเตอร์และระบบเครือข่าย ซึ่งสิ่งต่าง ๆ เหล่านี้มีความลึกซึ้งมากกว่าการสร้างกำลังพลด้านเทคโนโลยีสารสนเทศซึ่งมีความขาดแคลนเป็นทุนเดิมอยู่แล้ว งานวิจัยนี้นำเสนอแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ในระดับชาติ โดยคำนึงถึงการบูรณาการแนวความคิดจากประเด็นปัญหาในด้านต่าง ทั้งปัจจัยด้านเวลาการพัฒนาและด้านการเสริมสร้างกำลังพลไซเบอร์ในรูปแบบกองกำลังผสมพลเรือน ตำรวจ ทหาร และการพิจารณาใช้ข้อกฎหมายที่เกี่ยวข้องกับการเตรียมกำลังพลสำรองในระดับชาติ

ผลการวิจัยพบว่าแนวทางในการพัฒนากำลังพลด้านไซเบอร์ที่ได้นำเสนอในเอกสารวิจัยนี้จะเป็นประโยชน์ต่อการกำหนดกรอบเวลา การวางแผน การดำเนินการเสริมสร้างความแข็งแกร่งของบุคลากรด้านไซเบอร์ให้กับประเทศชาติ ซึ่งหากนำไปใช้ปฏิบัติได้อย่างจริงจังจะทำให้สามารถลดปัญหาการขาดแคลนกำลังพลไซเบอร์ และทำให้เกิดความ "ยั่งยืน" ในการเสริมสร้างกำลังพลไซเบอร์ในระยะยาวได้เป็นอย่างดี นอกจากนั้นกำลังพลสำรองไซเบอร์ยังเป็นส่วนสำคัญในการพัฒนาอุตสาหกรรมซอฟท์แวร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศในอนาคต

ABSTRACT

Title A Guideline for Cybersecurity Task Force Development for Readiness to Handle National-level Cyber Threats

Field Science and Technology

Name Major General Prachya Chalermwat **Course** NDC **Class** 60

The word “Cyber Space” has been well accepted and used in general in our living days. Tremendous of data are transferred rapidly in cyber space via internet across the globe to share data, exchange information, reduce complexity of work, and access to various data services. It is very obvious that cyber threats has been raised to to be one of national-level threats. This includes cyber crimes, cyber attacks, cyber espionage as well as cyber intelligence. Cyber war is another important aspect to be aware of. Many nations have developed cyber task forces in their own ways despite the difficulty in cybersecurity development. This is due to issues in subject complexity like multi-skill level in networking, operating system, programming, not to mention lengthy time of practice. This research propose guideline for cybersecurity task forces development for readiness to handle national-level cyber threats by exploring and reviewing existing national cybersecurity strategies, interviewing in-dept experts and specialist, collecting data from online questionares. The proposed guideline and conceptual model will help develop learning cycle for sustainable national cybersecurity task force.

คำนำ

การใช้เทคโนโลยีแต่เพียงอย่างเดียวไม่สามารถแก้ไขปัญหาการเตรียมการรับภัยคุกคามด้านไซเบอร์ แต่ต้องการบุคลากรที่มีคุณภาพสูง สามารถปฏิบัติงานในไซเบอร์สเปซได้อย่างมีประสิทธิภาพ และมีความประสานสอดคล้องกับการรักษาความมั่นคงของชาติในภาพรวม ทั้งนี้ในระดับชาติได้มีการกำหนดชัดเจนว่าปัญหาจำนวนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์นั้นมีไม่เพียงพอ ในแผนปฏิบัติการเพื่อรองรับยุทธศาสตร์เพื่อความมั่นคง 2560-2564 บุคลากรด้านไซเบอร์เป็นกลุ่มบุคคลที่มีความสำคัญมากต่อการดำรงสภาพของระบบเทคโนโลยีสารสนเทศ โดยเฉพาะภาครัฐยังประสบปัญหาการขาดแคลนบุคลากรอีกเป็นจำนวนมาก ซึ่งอาจเกิดจากปัญหาด้านแรงจูงใจในค่าตอบแทนหรือขาดแคลนเจ้าหน้าที่ที่เข้าใจปัญหาการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง และเกิดจากความยากของเนื้อหาและความสลับซับซ้อนของปัญหาที่ทำให้เป็นอุปสรรคต่อบุคคลทั่วไปที่มีความรู้พื้นฐานเพียงแค่ทำงานในระบบสารสนเทศให้เข้าใจและสามารถปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ ในการพัฒนาบุคลากรโดยการสร้างแรงจูงใจจากค่าตอบแทนพิเศษที่จะได้รับเพิ่มจากการมีประกาศนียบัตร ใบรับรองต่าง ๆ ในแต่ละบุคคลจึงถือเป็นเรื่องสำคัญในแผนการปฏิบัติระดับชาติ ซึ่งจะต้องมีการดำเนินการอย่างเร่งด่วน โดยเริ่มจากการกำหนดหลักสูตรในสถานศึกษา และสถานฝึกอบรมตามมาตรฐานสากล เพื่อรองรับการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นตามความก้าวหน้าของเทคโนโลยีและการขยายตัวของการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย

พลตรี

(ปรัชญา เฉลิมวัฒน์)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 60
ผู้วิจัย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

"มิติไซเบอร์" หรือ "ไซเบอร์สเปซ" (Cyber Space) กลายเป็นศัพท์ใหม่ที่ได้รับการยอมรับในสังคมโลกอย่างรวดเร็วและเป็นสิ่งที่ยากที่จะหลีกเลี่ยงการเกี่ยวข้องด้วย ไซเบอร์สเปซมีอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานหลักและ มีคอมพิวเตอร์รวมถึงอุปกรณ์ทุกอย่างเชื่อมต่อเข้ากับระบบเครือข่ายอินเทอร์เน็ตและระบบเครือข่ายย่อยขององค์กร โดยรวมถึงเครือข่ายย่อยส่วนบุคคลและ IoT(Internet of Things) ข้อมูลจำนวนมหาศาลเดินทางไปในมิติไซเบอร์เพื่อตอบสนองความต้องการในเรื่องความสะดวกสบาย รวดเร็ว การแลกเปลี่ยนข้อมูลข่าวสาร การลดความซับซ้อนของการทำงาน รวมถึงการใช้บริการข้อมูลต่าง ๆ อย่างไรก็ตาม ภัยคุกคามที่ทุกชาติให้ความสำคัญในยุคปัจจุบันคือ ปัญหาความไม่ปลอดภัยในการใช้งานในระบบอินเทอร์เน็ตเนื่องจากมิจฉาชีพต่างก็ปรับตัวให้เข้ากับสภาพแวดล้อมที่เปลี่ยนไปในมิติไซเบอร์ นอกจากนั้นในระดับชาติที่เป็นมหาอำนาจต่างก็ยอมรับในเรื่องการยกระดับของภัยคุกคามขึ้นเป็นระดับ "สงครามไซเบอร์" ทั้งในระดับยุทธศาสตร์และระดับปฏิบัติการ ซึ่งบ่อยครั้งเมื่อเกิดความขัดแย้งและการเจรจาทางการทูตไม่สำเร็จสงครามไซเบอร์จะถูกใช้เป็นอำนาจกำลังรบเพื่อแสวงหาข้อยุติในทางอ้อม ความพยายามเสริมสร้างกำลังพลด้านไซเบอร์เพื่อเตรียมรับมือกับภัยคุกคามด้านไซเบอร์ทั้งในระดับกองทัพและระดับความมั่นคงของประเทศก่อให้เกิดปัญหาการขาดแคลนกำลังพลด้านไซเบอร์อย่างหลีกเลี่ยงไม่ได้ เนื่องจากผู้ที่จะสามารถปฏิบัติการไซเบอร์ได้อย่างจริงจังนั้นต้องมีพื้นฐานทั้งด้านคอมพิวเตอร์ ระบบเครือข่าย กลไกการทำงานของระบบอินเทอร์เน็ต ความชำนาญเฉพาะด้านเช่น การเขียนโปรแกรมในภาษาต่าง ๆ การวิเคราะห์โปรแกรม ความรู้เรื่องฮาร์ดแวร์และสถาปัตยกรรมคอมพิวเตอร์ ฐานข้อมูล ความมีไหวพริบ การเข้า/ถอดรหัส และการวิเคราะห์ภัยคุกคามได้เป็นอย่างดี ซึ่งสิ่งต่าง ๆ เหล่านี้มีความลึกซึ้งมากกว่าการสร้างกำลังพลด้านไอทีซึ่งมีความขาดแคลนเป็นทุนเดิมอยู่แล้ว

ปัจจุบันการใช้งานอินเทอร์เน็ตมีความจำเป็นและกลายเป็นส่วนหนึ่งของชีวิตประจำวันในการดำเนินกิจกรรมต่าง ๆ ทั้งในด้านการใช้งานส่วนตัวตลอดจนการใช้ในระดับชาติเช่น ด้านเศรษฐกิจและสังคม ความมั่นคงและการป้องกันประเทศ การสื่อสารโทรคมนาคมและการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานสำคัญ ด้วยเหตุนี้ประชาชนเกือบทั้งทั้งประเทศในแทบจะทุกประเทศในโลกมีส่วนหนึ่งของเวลาในชีวิตเข้าไปเกี่ยวข้องกับไซเบอร์เสปซอย่างหลีกเลี่ยงไม่ได้ จากรายงานของ ITU (International Telecommunication Union) ในปี 2560 พบว่า 51% ของประชากรทั่วโลกหรือประมาณ 3.2 พันล้านคนสามารถเข้าถึงอินเทอร์เน็ตได้ สำหรับในประเทศไทยสถิติข้อมูลในปี พ.ศ.2561 นั้นพบว่ามีผู้ใช้อินเทอร์เน็ตสูงถึงประมาณ 57 ล้านคนซึ่งคิดเป็นถึง 83% ของประชากรทั้งประเทศ จากการใช้อินเทอร์เน็ตที่เพิ่มมากขึ้นประกอบกับการที่รัฐบาลไทยมีนโยบายการพัฒนาบรอดแบรนด์อินเทอร์เน็ตให้ครอบคลุมทั้งประเทศ และการแข่งขันในตลาดโทรคมนาคมจึงทำให้ประขากรไทยสามารถเข้าถึงระบบอินเทอร์เน็ตได้ง่ายและสะดวกรวดเร็ว เกิดความสะดวกสบาย

ในการใช้ชีวิตประจำวันมากขึ้น อย่างไรก็ตามปริมาณที่เพิ่มขึ้นของผู้ใช้งานและขนาดของเครือข่ายที่ขยายมากขึ้นเรื่อย ๆ ก็สามารถทำให้เกิดความเสี่ยงต่อการนำไปใช้งานในทางที่ผิดหรือตกเป็นเหยื่อของกลุ่มมิจฉาชีพ หรืออาชญากรรมข้ามชาติในรูปแบบต่าง ๆ ซึ่งส่งผลให้มีแนวโน้มที่จะเกิดภัยคุกคามต่อชีวิตและทรัพย์สินมากขึ้นตามลำดับอย่างหลีกเลี่ยงไม่ได้ นอกจากนั้นภัยที่จะเกิดต่อระบบควบคุมดูแลการใช้งานอินเทอร์เน็ตและเครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสาธารณูปโภคจะสามารถส่งผลกระทบต่อความมั่นคงของประเทศในภาพรวมได้เป็นอย่างมาก การใช้งานในทางที่ผิดมีผลต่อการดำรงชีวิตของประชาชนและการดำเนินธุรกิจทั้งในยามปกติและยามฉุกเฉิน รวมถึงสามารถส่งผลกระทบต่อเสถียรภาพทางสังคม วัฒนธรรมและขนบธรรมเนียมประเพณีอันดีงาน การใช้สื่อออนไลน์เป็นเครื่องมือในการเผยแพร่แนวความคิดหัวรุนแรงหรือชักชวนให้คนทั่วไปมาเข้าร่วมเป็นสมาชิกของกลุ่มเพื่อก่อเหตุการณ์ทางการเมืองอันอาจนำไปสู่ความไม่สงบเรียบร้อยของชาติ สถิติของการใช้ไซเบอร์สเปซในทางที่มิชอบมีปริมาณเพิ่มขึ้นอย่างต่อเนื่อง และทวีความรุนแรง สามารถกระจายความเสียหายในการถูกโจมตีได้อย่างรวดเร็ว

ปฏิบัติการทางทหารหรือการเมืองมักใช้เทคโนโลยีด้านการข่าวที่อาศัยไซเบอร์เสปซเป็นสื่อกลางในการค้นหารวบรวม ดักฟัง ขโมยข้อมูลของฝ่ายตรงข้าม เพื่อช่วงชิงความได้เปรียบในเรื่องข้อมูลข่าวสารประกอบการตัดสินใจของผู้นำระดับสูง การใช้ความก้าวหน้าทางเทคโนโลยีด้านไซเบอร์ล้วนเป็นเครื่องมือที่สำคัญสนับสนุนการทำสงครามในรูปแบบเดิม ๆ หรือแม้แต่ใช้ความได้เปรียบทางพลังอำนาจทางไซเบอร์มาเป็นเครื่องมือในประกอบการเจรจาทางการทูตเพื่อลดความขัดแย้งในเรื่องผลประโยชน์ของชาติ ดังนั้นการรักษาความมั่นคงปลอดภัยไซเบอร์จึงเป็นประเด็นที่ทุกประเทศกล่าวถึงในยุทธศาสตร์หรือนโยบายระดับชาติ ประกอบกับการผลักดันให้เกิดภาวะเศรษฐกิจดิจิตัลเพื่อเพิ่มอัตราเร่งในการพัฒนาเศรษฐกิจในภาพรวมของประเทศซึ่งนับเป็นสิ่งสำคัญยิ่งในการขับเคลื่อนประเทศทั้งทางด้านเศรษฐกิจ การเมือง สังคมและการป้องกันประเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์จะต้องมีการดูแลรักษาให้ระบบเครือข่ายเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงใช้งานได้อย่างต่อเนื่อง มีขีดความสามารถในการป้องกันและแก้ไขปัญหาหากถูกโจมตีระบบและมีแผนการฟื้นตัวให้สามารถกลับมาใช้งานได้ตามปกติอย่างรวดเร็ว

ประเทศที่พัฒนาแล้วมักมีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาใช้ในการบริหารจัดการองค์กรอย่างเต็มรูปแบบ ตลอดจนการใช้ระบบควบคุมในทางอุตสาหกรรมขนาดใหญ่ (Industrial Control Systems) และในการบริหารจัดการโครงสร้างพื้นฐานทางสาธารณูปโภคที่สำคัญ และมักถูกโจมตีจากฝ่ายตรงข้ามอย่างต่อเนื่อง ตัวอย่างของการโจมตีที่มีผลกระทบต่อความมั่นคงของประเทศได้แก่ การโจมตีโรงไฟฟ้านิวเคลียร์ของประเทศอิหร่านในปี พ.ศ.2553 ซึ่งถูกโจมตีด้วยมัลแวร์ Stuxnet ส่งผลให้เครื่อง Centrifuges ถูกทำลายไปมากกว่า 1,000 เครื่อง และมัลแวร์ก็ได้แพร่กระจายไปยังคอมพิวเตอร์ต่าง ๆ กว่า 200,000 เครื่อง ในปี พ.ศ. 2555 ปฏิบัติการ “Operation Ababil” ของกลุ่ม Qassam Cyber Fighter โจมตีสถาบันการเงินสำคัญของสหรัฐอเมริกา เช่น NYSE (New York Stock Exchange), J.P. Morgan Chase, Bank of America และสถาบันการเงินอีกหลายแห่งด้วย DDoS (Distributed Denial of Services) ส่งผลให้การบริการทางอินเทอร์เน็ตต้องหยุดชะงัก การโจมตีที่ส่งผลกระทบต่อผู้ใช้งานอินเทอร์เน็ตทั่วโลกได้แก่การปล่อยมัลแวร์ Mirai ของแฮ็กเกอร์ โดยใช้ช่องโหว่ในอุปกรณ์ IoT (Internet of Things) โจมตีชื่อ

โดเมนทำให้ไม่สามารถเข้าถึงเว็บไซต์จำนวนมากทั่วโลก ในปี พ.ศ. 2560 WannaCry มัลแวร์ที่ส่งผลกระทบต่อความมั่นคงในระดับประเทศ เข้าโจมตีหน่วยงานสาธารณสุขของอังกฤษ ผู้ป่วยเกือบ 7,000 รายไม่สามารถเข้ารับบริการได้และ WannaCry ได้แพร่กระจายไปยังคอมพิวเตอร์ต่าง ๆ ทั่วโลกมากกว่า 150 ประเทศ การรั่วไหลของข้อมูลโดยแฮ็กเกอร์ก็สามารถส่งผลกระทบต่อเสถียรภาพของรัฐบาลได้เช่นกัน ยกตัวอย่างเช่นกรณี การรั่วไหลของข้อมูลส่วนบุคคลถึง 53 ล้านรายการของบริษัท Uber ในปี พ.ศ.2560 และกรณี Data Breaches ของผู้ใช้บริการ Florida Medicaid ของประเทศสหรัฐอเมริกามีข้อมูลส่วนบุคคลรั่วไหลไปกว่า 30,000 รายการในปี พ.ศ.2561 และบริษัท Equifax ทำข้อมูลส่วนบุคคลของผู้บริโภครั่วไหลไปกว่า 145 ล้านรายการ

นอกจากการโจมตีที่กล่าวข้างต้นแล้วยังมีการโจมตีหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) เกิดขึ้นทั่วโลก โดยในประเทศไทยการโจมตีที่สำคัญที่ผ่านได้แก่ การที่ผู้ให้บริการชื่อโดเมนไทย .th ถูกเจาะระบบและแก้ไขข้อมูลที่อยู่เว็บไซต์ขององค์กรใหญ่หลายแห่งใน พ.ศ.2555 และในปี พ.ศ. 2556 มีการโจมตี DDoS ต่อตลาดหลักทรัพย์โดยกลุ่ม Anonymous กับเว็บไซต์ของตลาดหลักทรัพย์ในไทยพร้อมกับ ตลาดหลักทรัพย์ในอเมริกา และเอเชีย ทำให้เกิดผลกระทบต่อการให้บริการหลายชั่วโมง ในปี พ.ศ. 2558 ธนาคารพาณิชย์ 5 แห่งได้รับอีเมลข่มขู่ เรียกเงินเป็นสกุล Bitcoins เพื่อแลกกับการไม่ถูกโจมตีด้วย DDoS จากกลุ่ม Amrmada Collective ซึ่งเป็นจุดเริ่มต้นของการจัดให้มีการหารือระหว่าง CEO ของธนาคารเพื่อรับมือกับการโจมตีครั้งนั้น ในปี พ.ศ.2559 เว็บไซต์ของหน่วยงานภาครัฐถูกโจมตีด้วย DDoS จากกลุ่มพลเมืองต่อต้าน Single Gateway ซึ่งทำการรณรงค์ให้สมาชิกช่วยกันโจมตีเว็บไซต์ของรัฐบาล นอกจากนั้นยังตรวจพบการเจาะระบบเข้ามายังฐานข้อมูลเพื่อโจรกรรมข้อมูลมาเผยแพร่ รวมถึงการใช้ปฏิบัติการข่าวสารในการลดความน่าเชื่อถือของรัฐบาล ในปีเดียวกัน ATM จำนวน 21 แห่งของธนาคารออมสินถูกโจมตีด้วยมัลแวร์และลอบขโมยเงินจำนวน 12 ล้านบาทเป็นมีความคล้ายคลึงกับมัลแวร์ที่ใช้โจมตีตู้ ATM ในประเทศไต้หวัน และในปี 2561 ได้มีการโจรกรรมข้อมูลลูกค้าสินเชื่อที่อยู่อาศัยของธนาคารกรุงไทย และลูกค้าบริการหนังสือค้ำประกันของธนาคารกสิกรไทย ถึงแม้จะไม่สามารถตีมูลค่าความเสียหายได้ชัดเจนแต่ก็ได้ลดความน่าเชื่อถือของธนาคารกสิกรไทยลงไปเป็นอย่างมาก ซึ่งจะเห็นได้ว่าหน่วยงานที่อยู่ในกลุ่มโครงสร้างพื้นฐานสำคัญของประเทศนั้นมีความเสี่ยงเมื่อนำระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายอินเทอร์เน็ตเข้ามาใช้ในการให้บริการและการบริหารจัดการ

การพัฒนาศักยภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องใช้บุคลากรที่มีความรู้ความสามารถที่มีมาตรฐานเทียบเท่าประเทศที่เจริญแล้ว ในระดับสากลปัญหาการขาดแคลนบุคลากรด้านไซเบอร์ยังคงเป็นปัญหากับทุกประเทศ สำหรับประเทศไทยนั้นผู้วิจัยเห็นว่าปัญหาการพัฒนากำลังพลด้านไซเบอร์ประกอบด้วยปัญหาย่อยและปัจจัยต่าง ๆ พอสรุปได้ดังนี้

1. การขาดแคลนกำลังพลด้านไซเบอร์ที่ต้องมีทั้งประสบการณ์และความทุ่มเท
2. ความยากของเนื้อหาในการพัฒนา อบรม ฝึกซ้อม
3. ระยะเวลาที่ต้องใช้ในการพัฒนาบุคลากรไซเบอร์
4. ผู้บริหารไม่ให้ความสนใจอย่างจริงจัง เช่น แต่งตั้งผู้ที่ไม่มีประสบการณ์ด้านไซเบอร์มาบริหารหน่วยงานไซเบอร์ บรรจุบุคคลที่ไม่มีความสามารถด้านไซเบอร์เข้ามาในตำแหน่ง

5. ผู้บริหารหลงประเด็นมุ่งเน้นการสร้างภาพ โครงสร้าง การจัดหาอุปกรณ์ ปรับปรุงสถานที่ทำงาน โดยไม่ได้คำนึงถึงงานที่หน่วยไซเบอร์ต้องปฏิบัติ และแผนพัฒนากำลังพลด้านไซเบอร์

6. ปัญหาสมองไหลหรือการให้ค่าตอบแทนไม่คุ้มกับค่าขีดความสามารถ

งานวิจัยนี้นำเสนอแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ในระดับชาติ โดยคำนึงถึงการบูรณาการแนวความคิดจากประเด็นปัญหาในด้านต่าง ทั้งปัจจัยด้านเวลาการพัฒนาและด้านการเสริมสร้างกำลังพลไซเบอร์ในรูปแบบกองกำลังผสมพลเรือน ตำรวจ ทหาร และการพิจารณาใช้ข้อกฎหมายที่เกี่ยวข้องกับการเตรียมกำลังพลสำรองในระดับชาติ

ผลการวิจัยคาดว่าแนวทางในการพัฒนากำลังพลด้านไซเบอร์ที่ได้นำเสนอในเอกสารวิจัยนี้จะเป็นประโยชน์ต่อการกำหนดกรอบเวลา การวางแผน การดำเนินการเสริมสร้างความแข็งแกร่งด้านไซเบอร์ให้กับประเทศชาติ โดยการใช้ข้อมูลการวิจัยและข้อพิจารณาจากการสำรวจข้อมูลพื้นฐาน การวิเคราะห์ และการสัมภาษณ์เชิงลึกต่อผู้เชี่ยวชาญและผู้บริหารระดับสูงที่เกี่ยวข้องกับกิจการความมั่นคงปลอดภัยไซเบอร์ ซึ่งหากนำไปใช้ปฏิบัติได้อย่างจริงจังจะทำให้สามารถลดปัญหาความขาดแคลนกำลังพลไซเบอร์ และทำให้เกิดความ “ยั่งยืน” ในการเสริมสร้างกำลังพลไซเบอร์ในระยะยาวได้เป็นอย่างดี นอกจากนั้นกำลังพลสำรองไซเบอร์ยังเป็นส่วนสำคัญในการพัฒนาอุตสาหกรรมซอฟท์แวร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศในอนาคต

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาวิเคราะห์สถานการณ์และการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามไซ-เบอร์ในระดับชาติ

2. เพื่อเสนอแนวทางการพัฒนากำลังพลไซเบอร์ที่เหมาะสมและมีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี

ขอบเขตของการวิจัย

การวิจัยเรื่อง “แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติ”ประกอบด้วยขอบเขตของการศึกษา ดังนี้

1. ขอบเขตด้านเนื้อหา

1.1 ศึกษาเนื้อหาเกี่ยวกับ แนวคิด ทฤษฎีที่เกี่ยวข้องกับการพัฒนากำลังพลด้านไซเบอร์ ในมุมมองที่สอดคล้องกับยุทธศาสตร์ชาติ

1.2 ศึกษาแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติที่เคยมีการเผยแพร่ไว้แล้ว เพื่อหาข้อเด่นข้อด้อย แล้วนำมาเป็นข้อมูลการวิเคราะห์และการพิจารณาเพื่อกำหนดแนวทางการพัฒนากำลังพลไซเบอร์ใหม่ที่มีความเหมาะสมกับประเทศไทยในศตวรรษที่ 21

1.3 ศึกษาข้อมูลยุทธศาสตร์ไซเบอร์ระดับชาติของประเทศไทย และต่างประเทศ รวมทั้งตัวอย่างที่รัฐบาลไทยเคยได้ยึดถือเป็นแนวทางในการจัดทำยุทธศาสตร์ไซเบอร์ชาติ เพื่อหา

ข้อเด่น ข้อด้อย และเพื่อนำมาเป็นแนวทางในการกำหนดแนวทางการพัฒนาบุคลากรไซเบอร์ขึ้นใหม่

1.4 ศึกษาและจัดทำแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติที่เหมาะสมและสอดคล้องกับยุทธศาสตร์ไซเบอร์ระดับชาติขึ้นใหม่เพื่อให้สามารถนำมาใช้กับการพัฒนากำลังพลไซเบอร์ในระดับชาติของรัฐบาลไทยและเพื่อนำไปใช้เป็นแนวทางในการวางแผน ดำเนินงาน การพิจารณปัจจัยด้านงบประมาณ สำหรับประเทศไทยต่อไป

1.5 เป็นการศึกษาเฉพาะแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติเป็นหลัก

2. ขอบเขตด้านประชากรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

ผู้วิจัยจะดำเนินการสัมภาษณ์เชิงลึกต่อกลุ่มผู้เชี่ยวชาญที่มีความเชี่ยวชาญทั้งทางวิชาการ ด้านการบริหาร และผู้ที่มีประสบการณ์ในการจัดทำยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหมและระดับชาติ โดยมีผู้เชี่ยวชาญ (KIs) ที่จะสัมภาษณ์เชิงลึก ที่ประกอบด้วยผู้เชี่ยวชาญ 6 คน และผู้เชี่ยวชาญด้านยุทธศาสตร์ชาติจำนวน 7 คน ทั้งนี้จำนวนผู้เชี่ยวชาญด้านวิชาการและด้านยุทธศาสตร์อาจมีการเปลี่ยนแปลงตามความเหมาะสมด้วยข้อจำกัดของเวลาและตารางการปฏิบัติของแต่ละท่าน

3. ขอบเขตด้านเวลา

ผู้วิจัยจะดำเนินการรวบรวมข้อมูลทั้งข้อมูลปฐมภูมิและข้อมูลทุติยภูมิในห้วงเวลาตั้งแต่เดือนตุลาคม 2560 – เมษายน 2561

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงผสมผสาน โดยทำการวิจัยเชิงปริมาณ (Qualitative Research) ซึ่งทำการวิจัยเนื้อหาความรู้ในเชิงประจักษ์ โดยใช้แบบสอบถาม ซึ่งปฏิบัติงานด้านไซเบอร์ของสำนักปลัดกระทรวงกลาโหม และได้วิเคราะห์ข้อมูลวิจัยในเชิงคุณภาพ โดยศึกษาจากเอกสาร ทั้งปฐมภูมิและทุติยภูมิ จากหลายแห่งความรู้ และได้ทำการสัมภาษณ์เชิงลึก ทั้งในผู้บริหารระดับสูงในกระทรวงกลาโหม ในสำนักงานปลัดกระทรวงกลาโหม อีกทั้งได้จัด Focus Groubs ในลักษณะสนทนา ถกแถลงปัญหาเชิงวิเคราะห์แบบกลุ่มของผู้ที่ปฏิบัติงานเกี่ยวข้องกับไซเบอร์โดยตรง

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบผลการวิเคราะห์การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ ซึ่งจะนำไปสู่การจัดทำแผนการพัฒนาบุคลากรด้านไซเบอร์ในภาพรวมของประเทศ

2. ทำให้ทราบถึงแนวทางพัฒนาศักยภาพบุคลากรด้านไซเบอร์ของประเทศว่าอยู่ในระดับใดและเป็นแนวทางว่าควรจะพัฒนาให้เทียบเท่าอารยประเทศเพื่อความสมดุลด้านพลังอำนาจด้านไซเบอร์หรือไม่

3. ได้แนวทางที่เหมาะสมในการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ ที่มีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี

คำจำกัดความ

อินเทอร์เน็ต (Internet)	หมายถึง	ระบบเครือข่ายคอมพิวเตอร์ที่เชื่อมโยงระหว่างประเทศต่าง ๆ ทั่วโลก โดยใช้โปรโตคอล TCP/IP เพื่อสื่อสารข้อมูลระหว่างเครื่องคอมพิวเตอร์
ระบบเครือข่าย	หมายถึง	ระบบเครือข่ายคือช่องทางการสื่อสารดิจิตอลของระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายผ่านสื่อต่าง ๆ เช่น สายไฟเบอร์อ็อปติค หรือสาย LAN เป็นต้น
ไซเบอร์สเปซ (Cyber Space)	หมายถึง	สภาพแวดล้อมในระดับประเทศที่มีการสื่อสารผ่านเครือข่ายคอมพิวเตอร์ คำว่าไซเบอร์สเปซได้รับความนิยมในปี ค.ศ. 1990 ในช่วงที่มีการขยายตัวการใช้อินเทอร์เน็ต ระบบเครือข่าย และการสื่อสารดิจิตอลจนสามารถเชื่อมต่อเครือข่ายสื่อสารข้อมูลได้ทั่วโลก
IoT (Internet of Things)	หมายถึง	ไอโอที หรือ อินเทอร์เน็ตออฟธิง คือคำกล่าวโดยรวมถึงอุปกรณ์ทุกอย่างที่เชื่อมต่อเข้ากับระบบอินเทอร์เน็ตและสามารถสื่อสารข้อมูลผ่านระบบเครือข่ายได้หลายรูปแบบ
ภัยคุกคามไซเบอร์	หมายถึง	รูปแบบของภัยคุกคามที่มากับระบบอินเทอร์เน็ตและคอมพิวเตอร์ที่เชื่อมต่อ โดยมีเป้าหมายในหลาย ๆ ระดับ ตั้งแต่ระดับผู้ใช้งานอินเทอร์เน็ตทั่วไป องค์กร หรือระดับประเทศ
สงครามไซเบอร์	หมายถึง	เป็นมิติที่ 5 ของรูปแบบการใช้กำลังในการรบหลักอันได้แก่ สงครามทางบก ทางน้ำ ทางอากาศ และในห้วงอวกาศ เป็นปฏิบัติการเพื่อสนับสนุนการทำการรบในมิติอื่น ๆ
หลักนิยมไซเบอร์	หมายถึง	แนวทางปฏิบัติที่ได้รับการพัฒนาจากประสบการณ์การใช้กำลังไซเบอร์เข้าปฏิบัติการร่วมการรบในรูปแบบอื่น ๆ
ยุทธศาสตร์ไซเบอร์	หมายถึง	การกำหนดแนวทางการบริหารจัดการไซเบอร์ในระดับยุทธศาสตร์ ในกรอบเวลาที่ยาวนานกว่าแผนทั่วไป
ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)	หมายถึง	ความพยายามทั้งหมดที่ได้ลงทุนทรัพยากรทั้งด้านบุคลากร เทคโนโลยีและกระบวนการ เพื่อบริหารจัดการความเสี่ยงภัยไซเบอร์ ทั้งนี้เพื่อให้ระบบคอมพิวเตอร์ เครือข่ายมีความมั่นคงปลอดภัยจากภัยคุกคามไซเบอร์ และสามารถให้บริการได้อย่างต่อเนื่อง

หลักนิยมทางทหาร (Military doctrine)	หมายถึง	การจัดการกำลังทหารในการมีส่วนร่วมในการทัพ ปฏิบัติการทางทหาร ยุทธการและยุทธนาการต่าง ๆ โดยจะต้องมีส่วนเกี่ยวข้องกับทฤษฎี ประวัติศาสตร์ การทดลองและการปฏิบัติ และมีความคิดริเริ่มและสร้างสรรค์อีกด้วย หลักนิยมทางทหารเป็นแนวทางสำหรับการดำเนินการ โดยเป็นการวางโครงร่างให้กับกำลังทหารทั้งหมด ซึ่งเป็นประโยชน์ในการจัดมาตรฐานของปฏิบัติการ สร้างรูปแบบทั่วไปในการบรรลุเป้าหมายทางการทหาร เพื่อให้เกิดความง่ายและความคล่องแคล่ว และยังเป็นการวางพื้นฐานของการกำหนดรูปแบบการดำเนินการของปฏิบัติการทางทหารสำหรับนักวางแผนทางการทหาร
ยุทธศาสตร์ (Strategy)	หมายถึง	วิธีการที่จะนำเครื่องมือ (Means) มาใช้เพื่อให้บรรลุจุดมุ่งหมาย (Purpose) หรือ วัตถุประสงค์ (Objective) ที่กำหนดไว้ โดยต้องเชื่อมความสัมพันธ์ให้สมดุล ระหว่างจุดหมาย (Ends) หนทางปฏิบัติ (Ways) และ เครื่องมือ (Means) ด้วยการวางกลอุบาย (Trick) โดยพิจารณาร่วมกันในเรื่องของความเหมาะสม (Suitability) การยอมรับได้ (Acceptability) และความเป็นไปได้ (Feasibility) โดยผ่านการประเมินความเสี่ยงอยู่ตลอดเวลาที่ดำเนินการ
ยุทธศาสตร์ชาติ (National Strategy)	หมายถึง	1. ศิลปะและศาสตร์ในการพัฒนาและการใช้กำลังอำนาจทางการเมืองเศรษฐกิจ และทางสังคมจิตวิทยาร่วมกับกำลังอำนาจทางทหารทั้งในยามสงบและในยามสงคราม เพื่อดำรงไว้ซึ่งวัตถุประสงค์ของชาติตัวแบบการจัดทำยุทธศาสตร์ 2. กรอบแนวทางในการจัดทำยุทธศาสตร์และยุทธศาสตร์ชาติซึ่งได้รับการพัฒนาให้สอดคล้องกับยุคสมัยมาตลอดช่วงระยะเวลาที่ผ่านมา เช่น ตัวแบบในการจัดทำยุทธศาสตร์ความมั่นคงแห่งชาติของสหรัฐอเมริกาเป็นต้น ในที่นี้จะให้หมายถึงตัวแบบที่กำหนดขึ้นเพื่อให้ประกอบด้วยหลักวิชาการว่าด้วยยุทธศาสตร์ทางด้านความมั่นคง และยุทธศาสตร์ชาติโดยมีความมุ่งหมายเพื่อกำหนดขึ้นให้เป็นกรอบแนวทางในการจัดทำยุทธศาสตร์ด้านความมั่นคงแห่งชาติและยุทธศาสตร์ชาติของประเทศไทยในศตวรรษที่ 21 เป็นสำคัญ

ผลประโยชน์แห่งชาติ (National Interest)	หมายถึง	แนวความคิดที่ได้ไตร่ตรองอย่างรอบคอบที่สุดแล้วจากบรรดาองค์ประกอบต่าง ๆ ซึ่งประมวลขึ้นเป็นความต้องการที่สำคัญที่สุดที่ชาติจะขาดเสียมิได้ทั้งนี้รวมถึงการคุ้มครองตนเองความเป็นเอกราชบูรณภาพแห่งชาติความมั่นคงทางทหารเสถียรภาพทางเศรษฐกิจกับบรรดาความมั่งคั่งทั้งหลายที่จะพึงมี
ความมุ่งประสงค์แห่งชาติ (National Purpose)	หมายถึง	การแสดงออกมาของค่านิยม (Values) ที่ค่อนข้างจะทนทานถาวร หรือไม่ค่อยจะเปลี่ยนแปลงง่ายๆ ซึ่งชาตินั้นมีอยู่ดั้งเดิม หรือตั้งแต่เริ่มแรกโดยกำหนดขึ้นตามค่านิยมทางวัฒนธรรม และจริยธรรมของชาตินั้น
นโยบายแห่งชาติ (National Policy)	หมายถึง	นโยบายแห่งชาติ (National Policy)" ในทางทหารไว้ 2 แนวทางคือ 1. "นโยบายแห่งชาติ หมายถึงแนวทางอย่างกว้าง ๆ ที่กำหนดโดยรัฐบาลในระดับชาติเพื่อที่จะส่งเสริมให้บรรลุต่อวัตถุประสงค์แห่งชาติ" (U.S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington D.C.: U.S. Department of Defense, 12 April 2001, 366.) 2. "นโยบายแห่งชาติหมายถึง แผนงานซึ่งสามารถจัดทำรายละเอียดเพื่อนำไปสู่การปฏิบัติในอันที่จะสามารถบรรลุต่อความมุ่งประสงค์แห่งชาติและส่งเสริมให้บรรลุต่อการรักษาผลประโยชน์แห่งชาติ" (วิทยาลัยการทัพบกสหรัฐอเมริกา)
วัตถุประสงค์แห่งชาติ (National Objective)	หมายถึง	บรรดาจุดมุ่งหมาย จุดมุ่งประสงค์ หรือความมุ่งประสงค์สำคัญของชาติ ซึ่งชาติมุ่งที่จะบรรลุถึง ด้วยการใช้นโยบายและความพยายาม รวมทั้งทรัพยากรของชาติทั้งปวง
พลังอำนาจแห่งชาติ (National Power)		หมายถึง เครื่องมือ (Means) ทั้งหมดของชาติ ที่ถูกนำไปใช้อย่างสมดุล สำหรับหนทางปฏิบัติ (Ways) ที่จะทำให้บรรลุในการเพิ่มพูนและรักษาผลประโยชน์แห่งชาติ (Ends)
สงครามไซเบอร์ (Cyber Warfare)	หมายถึง	การใช้คอมพิวเตอร์ อินเทอร์เน็ต และอุปกรณ์ที่เชื่อมต่อในการการทำสงคราม เช่น การโจมตีเว็บไซต์ โฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลทั้งด้านธุรกิจและการเมือง การเจาะข้อมูล รวมถึง การยุดยั้งหรือรบกวนการทำงานของระบบคอมพิวเตอร์ที่ใช้ร่วมในการสงคราม เช่น ระบบเรดาร์ ระบบควบคุมการบิน ระบบควบคุมการยิง เป็นต้น

โครงสร้างพื้นฐานสำคัญของชาติ (National Critical Infrastructure)	หมายถึง	หน่วยงานที่มีความสำคัญและจำเป็นต่อโครงสร้างพื้นฐานของประเทศ โดยมีภารกิจเกี่ยวกับเศรษฐกิจ ความมั่นคง ชีวิต และทรัพย์สิน หากเกิดความเสียหายต่อหน่วยงานเหล่านี้ อาจก่อให้เกิดความเสียหายและกระทบกับความมั่นคงของประเทศ ทั้งนี้หน่วยงานดังกล่าวสามารถแบ่งออกได้เป็นหลายกลุ่ม เช่น 1. กลุ่มไฟฟ้าและพลังงาน 2. กลุ่มการเงินการธนาคารและการประกันภัย 3. กลุ่มสื่อสารโทรคมนาคมและขนส่ง 4. กลุ่มความสงบสุขของสังคม
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure)	หมายถึง	คอมพิวเตอร์หรือ ระบบคอมพิวเตอร์ ระบบเครือข่าย ซึ่งหน่วยงานของรัฐหรือภาคเอกชนใช้ในกิจการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
Red Team	หมายถึง	หน่วยข้าศึกสมมุติ ซึ่งในทางการทหารจะทำการจัดกลุ่มคนที่มีทักษะสูง หรือ Red Team และให้ทำตัวเป็นเหมือนข้าศึกที่จะบุกเข้ามาในแนวป้องกัน โดยทั่วไปแล้ว Red Team จะใช้ประสบการณ์และความสามารถส่วนตัวในการหาแนวทางที่เป็นไปได้ในการที่จะโจมตีและบุกทะลวงแนวป้องกันอย่างมีประสิทธิภาพ โดยกระบวนการนี้ก็จะคล้าย ๆ การซ้อมรบซึ่งถูกนำมาใช้ในฝึกซ้อมการป้องกันระบบสารสนเทศได้เช่นกัน
มัลแวร์ (Malware)	หมายถึง	โปรแกรมประสงค์ร้ายต่าง ๆ ทำงานในลักษณะการโจมตีระบบ การทำให้ระบบเสียหาย รวมถึงการจารกรรมข้อมูล ย่อมาจากคำว่า Malicious Software แบ่งออกได้เป็นหลายประเภทเช่น ไวรัส (virus) หนอน (worm) ม้าโทรจัน (Trojan Horse) โปรแกรมดักจับข้อมูล (Spyware) โปรแกรมดักข้อมูลคีย์บอร์ด (Key Logger) ตลอดจนการฝังโปรแกรมประสงค์ร้าย (Maliciuos Mobile Code) ไว้ในระบบคอมพิวเตอร์ ส่วนมากโจมตีผ่านช่องโหว่ของโปรแกรม หรือระบบปฏิบัติการ
Data Breach	หมายถึง	การรั่วไหลของข้อมูล ซึ่งอาจเกิดจากความบกพร่องของระบบ หรือจากการกระทำของผู้ประสงค์ร้ายที่ทำการเจาะระบบ หลอกลวงเพื่อเอาข้อมูล เป็นต้น

Internet of Things (IoT)	หมายถึง	เครือข่ายของอุปกรณ์ทางกายภาพ รถยนต์ อุปกรณ์เครื่องใช้ในบ้าน เช่น ทีวี ตู้เย็น แอร์ เครื่องซักผ้า และสิ่งของต่าง ๆ ที่มีระบบปฏิบัติการฝังตัว (embedded system) ที่มีระบบอิเล็กทรอนิกส์ ซอฟท์แวร์ เซนเซอร์ แอ็คทูเอเตอร์ ซึ่งมีการเชื่อมต่อกันเพื่อแลกเปลี่ยนข้อมูลที่เป็นประโยชน์ต่อผู้ใช้งาน

บทที่ 2
แนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้อง

การพัฒนากำลังพลด้านไซเบอร์ต้องอาศัยบุคลากรที่มีพื้นฐานด้านคอมพิวเตอร์และเครือข่าย มีไหวพริบที่ดี รวมถึงมีขีดความสามารถในการเข้าใจการเขียนโปรแกรมในรูปแบบต่าง ๆ เพื่อให้สามารถพลิกแพลงการปฏิบัติให้เข้ากันสถานการณ์ที่เปลี่ยนไปอยู่ตลอดเวลาได้และรับมือกับผู้ที่มีขีดความสามารถในแบบเดียวกัน ดังนั้นจึงทำให้มีความยากลำบากในการค้นหาผู้ที่มีความสามารถครบถ้วนดังกล่าว ส่งผลให้เกิดปัญหาความขาดแคลนบุคลากรด้านไซเบอร์กับทุกภาคส่วนและยังคงเป็นปัญหาสำคัญในระดับประเทศ ในบทนี้จะกล่าวถึงแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องกับการพัฒนาบุคลากรด้านไซเบอร์เพื่อให้ทราบว่าปัญหานี้เป็นปัญหาที่ทุกคนมีความตระหนักและมีความพยายามในการแก้ไข หรือเตรียมการเพื่อให้มีการพัฒนากำลังพลด้านไซเบอร์ อีกทั้งยังใช้เป็นพื้นฐานแนวคิดในการพัฒนาบุคลากรด้านไซเบอร์ให้มีความยั่งยืนต่อไป

เอกสารร่างยุทธศาสตร์ชาติระยะ 20 ปี ฉบับ 24 สิงหาคม 2560 ในยุทธศาสตร์ที่ 1 คือ ยุทธศาสตร์ด้านความมั่นคงได้กล่าวถึงปัญหาความมั่นคงทางไซเบอร์ว่าเป็นหนึ่งในปัญหาความมั่นคงระดับโลก อีกทั้งยังกล่าวว่าภัยคุกคามด้านไซเบอร์เป็นหนึ่งในปัญหาสำคัญที่สามารถส่งผลกระทบต่อความมั่นคงของชาติในระดับที่รุนแรงได้ และในหัวข้อ 1.2 “การพัฒนาศักยภาพในการป้องกันประเทศ พร้อมรับมือกับภัยคุกคามทั้งทางทหารและภัยคุกคามอื่น ๆ” และในหัวข้อ 1.3.4 “ให้มีการเสริมสร้างความมั่นคงและปกป้องโครงสร้างพื้นฐาน/สาธารณูปโภคที่บริหารจัดการด้วยไซเบอร์ให้ปลอดภัยจากการโจมตี รวมถึงส่งเสริมวัฒนธรรม สร้างความตระหนักรู้ในการใช้ไซเบอร์ในทางที่เหมาะสม ตลอดจนพัฒนาขีดความสามารถขององค์กร/บุคลากรรับผิดชอบด้านไซเบอร์ให้มีความเชี่ยวชาญอย่างต่อเนื่อง เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ทั้งยามปกติ ยามเกิดเหตุ การฟื้นตัว/ฟื้นฟูหลังเกิดเหตุ และการเยียวยาแก้ไขผลกระทบ” ซึ่งจะเห็นได้ว่าองค์กรที่เกี่ยวข้องจะต้องจัดให้มีการพัฒนาบุคลากรด้านไซเบอร์เพื่อรับผิดชอบงานด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับยุทธศาสตร์ของชาติ

ปฏิบัติการทางไซเบอร์ในระดับใหญ่มักถูกใช้เมื่อเกิดความขัดแย้งระหว่างประเทศ โดยในขั้นต้นรัฐจะใช้การเจรจาทางการทูตเพื่อลดความขัดแย้งในขั้นต้นและหากการเจรจาไม่สำเร็จมักจะมีปฏิบัติการไซเบอร์สอดแทรกด้วยเสมอเพื่อแสดงให้เห็นถึงท่าทีของแต่ละฝ่าย และเป็นการย้ำเตือนให้เห็นถึงศักยภาพด้านไซเบอร์หากมีความจำเป็นต้องตัดสินใจเข้าปฏิบัติการต่อฝ่ายตรงข้าม ในอดีตนั้นสงครามไซเบอร์ถูกนำมาใช้อย่างชัดเจนครั้งแรกในสงครามอ่าวเปอร์เซียที่สหรัฐโจมตีอิรัก (Cyber War, ริชาร์ด เอ คลาร์ก, พฤษภาคม 2010) ปฏิบัติการไซเบอร์ถูกนำมาใช้เพื่อเตรียมสภาวะที่เหมาะสมให้กับปฏิบัติการทางทหารที่จะดำเนินการตามต่อมา เช่น การเข้าทำลายระบบเรดาร์ การรบกวนระบบเครือข่ายข้อมูลของฝ่ายตรงข้าม ปฏิบัติการไซเบอร์นั้นต้องใช้บุคลากรที่มีศักยภาพสูงในการเข้าปฏิบัติการ

การเคลื่อนไหวในการพัฒนาบุคลกรด้านไซเบอร์ในระดับโลกที่เห็นได้ชัดคือในปี ค.ศ. 2009 ประธานาธิบดี บารัค โอบามา ประกาศว่าระบบพื้นฐานดิจิตอลของสหรัฐอเมริกา "เป็นสินทรัพย์ยุทธศาสตร์ของชาติ" และจากนโยบายดังกล่าวในเดือนพฤษภาคม 2010 เพนตากอน ได้จัดตั้งกองบัญชาการไซเบอร์ หรือ Cyber Command โดยมี นายพล คีท บี. อเล็กซานเดอร์ ผู้บริหารของสภาความมั่งคงแห่งชาติสหรัฐอเมริกา เป็นผู้รับผิดชอบ ทั้งนี้เพื่อป้องกันเครือข่ายทหารอเมริกันและปฏิบัติการโจมตีต่อประเทศคู่ขัดแย้ง ตัวอย่างปฏิบัติการไซเบอร์ในระดับที่มีความรุนแรงได้แก่

1. ประเทศเอสโตเนียถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะรัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่างๆ จนข้อมูลเสียหายพังยับเยิน ในวันที่ 17 เดือนพฤษภาคม ปี ค.ศ. 2007

2. ตึกเพนตากอน กระทรวงกลาโหม สหรัฐอเมริกา และที่ทำการรัฐบาลของฝรั่งเศส เยอรมนี และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหายอย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา ในเดือนกันยายน ปี ค.ศ. 2007

3. เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศคีร์กีซ (Kyrgyz) ถูกโจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโตเนีย วันที่ 14 ธันวาคม ปี ค.ศ.2007

การโจมตีทางไซเบอร์เกิดขึ้นอยู่ตลอดเวลาและมีความต่อเนื่องโดยปฏิบัติการบางอย่างจะไม่เน้นการทำให้ผู้ที่ถูกโจมตีเสียหาย แต่จะเป็นการแอบขโมยข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับเพื่อนำมาใช้ประโยชน์ในอนาคตต่อไป

ภัยคุกคามด้านไซเบอร์

ภัยคุกคามด้านไซเบอร์ส่งผลกระทบต่อเป้าหมายที่ถูกโจมตีได้ทั้งทางตรงและทางอ้อมด้วยวิธีการต่าง ๆ ที่ได้รับการพัฒนารูปแบบการโจมตีอย่างไม่มีที่สิ้นสุด ระดับของการโจมตีทางไซเบอร์ได้ทวีความรุนแรงจนสามารถกล่าวได้ว่า เป็นระดับสงครามไซเบอร์ระหว่างประเทศอย่างชัดเจน ถึงแม้ว่าการระบุฝ่ายหรือระบุตัวตนของการโจมตีจะสามารถทำได้ยากหรือบางครั้งแทบจะเป็นไปไม่ได้ การวิเคราะห์โดยหน่วยงานข่าวกรองและข้อมูลประกอบในมิติอื่น ๆ สามารถบ่งชี้ได้ว่าเป็นความตั้งใจโจมตีของประเทศใด ทั้งนี้ประเทศต่าง ๆ ในโลกต่างตระหนักดีถึงภัยคุยคามด้านไซเบอร์ซึ่งสามารถส่งผลกระทบอย่างรุนแรงต่อการจราจรของระบบเครือข่ายหลัก, ระบบธุรกรรมการเงิน, ระบบสาธารณูปโภค, ระบบพลังงาน, และหน่วยงานความมั่นคง ซึ่งล้วนเป็นโครงสร้างพื้นฐานสำคัญยิ่งยวดของชาติ หลาย ๆ ชาติได้มีการจัดทำยุทธศาสตร์ชาติ, ยุทธศาสตร์ความมั่นคง, ยุทธศาสตร์ไซเบอร์, แผนงานความมั่นคงต่าง ๆ ตลอดจนปรับปรุงกฎหมายต่าง ๆ ที่เกี่ยวข้องกับการรับมือภัยคุกคามด้านไซเบอร์ นอกจากนี้การจัดตั้งหน่วยงานที่เป็นเอกเทศเพื่อดูแลด้านความมั่นคงปลอดภัยไซเบอร์ล้วนเป็นสิ่งที่อยู่ในลำดับความเร่งด่วนต้นๆ ของการเตรียมการรับมือกับภัยคุกคามด้านนี้ เอกสารฉบับนี้ต้องการให้ผู้อ่านได้ตระหนักถึงการเตรียมการรับมือของประเทศต่าง ๆ เท่าที่จะสามารถหาได้จากเอกสารอ้างอิงที่เปิดเผย ทั้งในมุมมองของหน่วยงานความมั่นคง ทางทหาร และหน่วยงานเอกชนที่เกี่ยวข้องกับการรับมือภัยคุกคามนี้ เพื่อใช้เป็นแนวทางในการเร่งรัดการเตรียมการรับมือในมิติต่าง ๆ ที่เกี่ยวข้อง ซึ่งพอสรุปได้ดังนี้

ในห้วงต้นปี พ.ค.2543 เป็นต้นมาประเทศต่าง ๆ เริ่มมีการเตรียมการทั้งทางด้าน การจัดตั้งหน่วยงาน ด้านนโยบายและยุทธศาสตร์ และการจัดทำร่างกฎหมายไซเบอร์ โดยส่วนใหญ่ในปี พ.ศ.2553 จะเริ่มเปิดเผยการเตรียมการของตนในรูปของ White Paper, ยุทธศาสตร์ชาติ, ยุทธศาสตร์ความมั่นคง, และยุทธศาสตร์ไซเบอร์ ประเทศที่เป็นผู้นำในการเตรียมการที่เห็นเด่นชัด คือสหรัฐอเมริกา ที่มีหน่วยงานสำคัญที่เกี่ยวข้องคือ Cyber Command, NSA, DHS, FBI, CIA ล้วนแต่มีปฏิบัติการด้านไซเบอร์ทั้งเชิงรุกและเชิงรับ ประเทศที่เป็นตัวละครหลักในระดับสงครามไซเบอร์นอกจากสหรัฐฯ แล้วได้แก่ จีน, รัสเซีย, เกาหลีเหนือ โดยมีแนวโน้มว่าสหรัฐฯ กับจีนเป็นคู่ขัดแย้งหลักในสงครามไซเบอร์ และประเทศไทยมักถูกใช้เป็นฐานที่ตั้งในปฏิบัติการโจมตีอยู่อย่างต่อเนื่อง

ปฏิบัติการสงครามไซเบอร์ถูกนำมาใช้อย่างจริงจังในสงครามอิรัก โดยสหรัฐอเมริกาได้นำรูปแบบของการสนับสนุนการรบหลักด้วยปฏิบัติไซเบอร์ที่เดิมเรียกว่า “ปฏิบัติการข้อมูลข่าวสาร” หรือ Information Operations ซึ่งมีทั้งการป้องกันและปฏิบัติการเชิงรุก ซึ่งมุ่งเป้าหมายสู่ระบบข้อมูลหรือ Information Systems ทั้งของฝ่ายทหารและพลเรือน ยุทธศาสตร์ แผน หรือนโยบายในระดับชาติ เช่น แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12, ยุทธศาสตร์ชาติ 20 ปี, แนวคิด Thailand 4.0 ล้วนแต่นำพาระบบปฏิบัติการของประเทศเข้าสู่โลกแห่งไซเบอร์โดยมุ่งหวังที่จะมีความได้เปรียบเชิงความหลากหลายของข้อมูล ความสะดวกและรวดเร็ว ความถูกต้องของข้อมูล และขีดความสามารถในการตรวจสอบจากภาครัฐและเอกชน เป็นต้น บทความนี้นำเสนอให้เห็นถึงมุมมองของการเตรียมการของนานาชาติในการรับมือภัยคุกคามด้านไซเบอร์ ตั้งแต่ระดับยุทธศาสตร์ นโยบายความมั่นคงแห่งชาติ หรือหลักนิยมความมั่นคงไซเบอร์ ซึ่งล้วนแต่พูดถึงภัยคุกคามด้านไซเบอร์มานับเป็นทศวรรษ ผ่านไป

ดังนั้นภัยคุกคามในไซเบอร์สเปซจึงเป็นสิ่งที่เราไม่สามารถจะหลีกเลี่ยงได้ เนื่องจากระบบสื่อสารข้อมูลของทุกประเทศถูกเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตที่ประกอบไปด้วยสายไฟเบอร์ออพติคโยงใยกันไปแทบจะทั่วทุกแห่งในโลก เหล่าแฮ็กเกอร์ที่ยากจะระบุสัญชาติได้สามารถท่องไปในไซเบอร์สเปซเพื่อปฏิบัติการต่อเป้าหมายที่เขาต้องการโดยไม่ต้องเดินทางให้เสียเวลา โดยใช้เครื่องมือการโจมตีที่ไม่มีใครคาดถึง สามารถเข้าควบคุมระบบปฏิบัติการของเครื่องคอมพิวเตอร์เป้าหมายได้โดยเหยื่อไม่รู้ตัว การโจมตีทางไซเบอร์นั้นมีผลกระทบต่อความมั่นคงในระดับชาติได้ เช่น เป้าหมายที่เป็นโครงสร้างพื้นฐานสำคัญ ระบบไฟฟ้า ระบบน้ำประปา หากถูกโจมตีหรือรบกวน ย่อมสั่นคลอนเสถียรภาพของประเทศนั้น ๆ ได้ไม่ว่าจะเป็นประเทศเล็ก ๆ หรือประเทศมหาอำนาจก็ตาม ดังนั้นหลาย ๆ ประเทศที่ตื่นตัวต่อภัยคุกคามด้านไซเบอร์จึงมักกำหนดหลักนิยม หรือ ยุทธศาสตร์ไซเบอร์ขึ้นมาเพื่อใช้เป็นแนวทางในการบริหารจัดการต่อภัยคุกคามที่อาจจะเกิดขึ้นได้ทุกขณะ ในส่วนต่อไปจะกล่าวถึงการที่ประเทศต่าง ๆ ได้มีการเตรียมการจัดทำหลักนิยม ยุทธศาสตร์ หรือนโยบายที่เกี่ยวข้องกับไซเบอร์ เพื่อให้ผู้อ่านได้ทราบถึงความสำคัญของภัยคุกคามไซเบอร์ที่ทุกประเทศต่างก็ต้องตระหนัก

แนวคิดเรื่องกำลังพลสำรองด้านไซเบอร์

กระทรวงกลาโหมเป็นหน่วยงานความมั่นคงหลักของชาติ และอยู่ในกลุ่มหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศที่ต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ซึ่ง

ประกอบด้วยสำนักปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ซึ่งต่างก็ประสบปัญหาการขาดแคลนและไม่สามารถพัฒนาบุคลากรด้านไซเบอร์ให้เพียงพอกับความต้องการและเพื่อให้ทันกับการเปลี่ยนแปลงทางเทคโนโลยีและภัยคุกคามด้านไซเบอร์ได้ บทความความนี้นำเสนอแนวคิดเรื่องการบริหารจัดการกำลังพลสำรองด้านไซเบอร์ โดยอาศัยกลไกการเตรียมกำลังพลสำรองที่กระทรวงกลาโหมมีอยู่แล้ว เพื่อคัดสรรบุคลากรในระดับพลทหารที่มีพื้นฐานความรู้ด้านไซเบอร์เช่น วิทยาการคอมพิวเตอร์ วิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ มารับการฝึกทหารเบื้องต้นแบบจำกัด และให้ข้อเสนอเพื่อรับการฝึกที่เน้นหนักด้านปฏิบัติการไซเบอร์เพื่อให้สามารถปฏิบัติงานในหน่วยงานไซเบอร์ของ กห. ได้ ทั้งนี้ยังคงใช้ห้วงเวลาเดียวกับการเกณฑ์ทหารตามปกติคือในห้วงสองปี หลังจากที่ปลดประจำการแล้วกำลังพลไซเบอร์สำรองที่มีประสิทธิภาพสูงอาจได้รับการทาบทามให้บรรจุในตำแหน่งหลักในหน่วยไซเบอร์ของ กห. นอกจากนั้น กห. เองยังสามารถเรียกระดมกำลังพลไซเบอร์สำรองที่ได้ทำการฝึกฝนและได้เคยปฏิบัติงานในหน่วยไซเบอร์กลับมาเพื่อสนับสนุนยุทธศาสตร์การผนึกกำลังได้ตามวงรอบการฝึกหรือเมื่อมีความต้องการ ทั้งนี้เพื่อให้สามารถบรรลุวัตถุประสงค์ของการเตรียมกำลังพลด้านไซเบอร์ โดยอาจต้องมีปรับปรุงกฎหมายที่เกี่ยวข้องเพื่อให้รองรับการปฏิบัติของหน่วยที่รับผิดชอบ ปัญหาที่มักพบในการปฏิบัติงาน เช่น

1. ผู้ปฏิบัติงานด้านไซเบอร์ต้องใช้ทักษะที่พิเศษ และใช้ระยะเวลาในการฝึกที่นานกว่าการฝึกทหาร ฝึกบุคคลทำการรบทั่วไป อีกทั้งบุคลากรที่มีวุฒิด้านวิทยาการคอมพิวเตอร์ หรือไอที ก็ไม่ใช่ว่าจะสามารถปฏิบัติงานในปฏิบัติการไซเบอร์ได้เสมอไป

2. ความขาดแคลนบุคลากรด้านไซเบอร์นับเป็นปัญหาใหญ่ในระดับชาติ และระดับสากล

ข้อมูลเชิงข้อเท็จจริงและสมมุติฐานที่เกี่ยวข้องกับแนวคิดการนำกำลังพลสำรองด้านไซเบอร์ให้มามีผลบังคับใช้เพื่อลดปัญหาการขาดแคลนบุคลากรไซเบอร์ได้แก่

1. การยุทธได้มีการเพิ่มมิติของไซเบอร์เข้าไปในการปฏิบัตินอกเหนือจากมิติการรบทางบก ทางทะเล ทางอากาศ และอวกาศ แต่การพัฒนาบุคลากรยังไม่สามารถตอบสนองได้ทันหน่วยงานไซเบอร์ที่จัดตั้งขึ้นก็ยังไม่สามารถปฏิบัติการได้อย่างมีประสิทธิภาพเนื่องจากการไม่สามารถบรรจุบุคลากรให้ตรงกับสายงานได้อย่างจริงจัง

2. การฝึกกำลังพลสำรองไม่เคยมีส่วนใดเกี่ยวข้องกับการฝึกบุคลกรด้านไซเบอร์เนื่องจากเป็นมิติการรบที่เพิ่งเกิดขึ้นใหม่ ทั้ง ๆ ที่สามารถบริหารจัดการให้นำกำลังพลเหล่านั้นมาฝึกเพื่อปฏิบัติงานด้านไซเบอร์ในหน่วยงานไซเบอร์ได้อย่างพอเพียง

3. การฝึกผู้ที่มีพื้นฐานด้านไอที หรือวิทยาการคอมพิวเตอร์ ให้สามารถปฏิบัติงานด้านไซเบอร์สามารถทำได้ผลดีกว่าการฝึกบุคคลทั่วไปที่ไม่มีความรู้ด้านนี้มาก่อน

ข้อพิจารณา

การเกณฑ์ทหารมีการดำเนินการในทุก ๆ ปี เพื่อเสริมสร้างกำลังพลสำรอง ซึ่งมีเงื่อนไขบางอย่างเช่นการเรียน รด. เพื่อขอผ่อนผัน/ยกเว้นการเกณฑ์ทหาร ได้ซึ่งถูกระบุไว้ในในข้อกำหนดของ พรบ. ที่เกี่ยวข้อง ซึ่งในทุก ๆ การเกณฑ์ทหารจะมีบุคลากรที่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศอยู่แล้ว แรงจูงใจให้บุคลลเหล่านั้นมีความอยากที่จะสมัครเป็นทหาร (ไซเบอร์) จะสามารถ

ทำให้กองทัพสามารถสร้างเสริมกองกำลังไซเบอร์ขึ้นได้อย่างรวดเร็ว โดยอาจเสนอให้มีการผ่อนผันพิเศษสำหรับผู้ที่มีวุฒิที่เหมาะสมกับการฝึกต่อไปในด้านไซเบอร์ และให้สามารถเข้าประจำการเป็น “ทหารใหม่ไซเบอร์” ที่สามารถนำมาใช้งานตามหน่วยที่เกี่ยวข้องด้านไซเบอร์เมื่อผ่านการฝึกตามที่กลาโหมได้ออกแบบไว้

การยื่นข้อเสนอพิเศษให้บุคลากรที่มีพื้นฐานด้านคอมพิวเตอร์อยู่แล้ว เป็นการสร้างทางเลือกให้แก่ผู้ที่คิดจะหลีกเลี่ยงการเกณฑ์ทหารด้วยมีภาพลักษณ์ของการฝึกทหารใหม่ที่มีการใช้ความรุนแรง การพิจารณานำกำลังพลสำรองไซเบอร์มาใช้ปฏิบัติงานนั้นอาจต้องมีการดำเนินงานดังต่อไปนี้

1. กห. จัดตั้งคณะทำงานเพื่อหาแนวทางร่วมกันระหว่างหน่วยที่เกี่ยวข้องเพื่อให้ได้ข้อสรุปการบริหารจัดการกำลังสำรองไซเบอร์ เพื่อนำไปสู่การจัดทำแผนและการปฏิบัติได้อย่างเป็นรูปธรรม

2. กำหนดแนวทางในการจัดการกำลังพลสำรองที่ปลดประจำการ (ผ่านการเกณฑ์ทหารไปแล้ว) แต่ทำงานในสาขาที่เกี่ยวข้องอยู่แล้ว พิจารณาการเรียกเข้ามาเพื่อเป็นผู้ฝึกให้กับ “ทหารใหม่ไซเบอร์” ได้เป็นอย่างดี โดยที่เขาเหล่านั้นก็ถือได้ว่ามารับใช้ประเทศชาติในอีกทางหนึ่งในมิติของไซเบอร์

3. พิจารณาปรับปรุงกฎหมายที่เกี่ยวข้อง เช่น พรบ. กำลังสำรอง ๒๕๕๘

หลักนิยมความมั่นคงไซเบอร์

หลักนิยมในการรบมักเป็นพื้นฐานแนวคิดที่มีวิวัฒนาการจากประสบการณ์ในการรบที่ผ่านมาในทางทหาร ซึ่งแต่ละประเทศก็จะมีหลักนิยมในการรบที่แตกต่างกันไป หรือตามแนวทางที่ประเทศมหาอำนาจใช้ เช่นเดียวกันกับในมิติไซเบอร์ เมื่อมีการนำปฏิบัติการไซเบอร์เข้ามาใช้ในระดับประเทศจนถึงยกระดับเป็นสงครามไซเบอร์นั้นก็จะมีการกำหนดหลักนิยมความมั่นคงทางไซเบอร์ขึ้นมาอย่างชัดเจน ในส่วนนี้จะกล่าวถึงเอกสารและหลักฐานต่าง ๆ ที่ได้มีการรวบรวมไว้จากการเผยแพร่ในรูปสิ่งพิมพ์ และข้อมูลจากอินเทอร์เน็ตโดยจะแบ่งข้อมูลเป็นสองกลุ่ม โดยผู้เขียนได้แยกข้อมูลออกเป็นสองตาราง ตารางแรกซึ่งจะมีข้อมูลของเอกสารที่หน่วยงานความมั่นคงของประเทศนั้น ๆ ได้มีการเผยแพร่ ส่วนตารางที่สองจะเป็นข้อมูลของหน่วยงานรัฐที่เป็นภาคพลเรือนที่ได้มีการกล่าวถึงนโยบายไซเบอร์ ในภาพรวมของประเทศ

สงครามไซเบอร์

กระทรวงกลาโหมของสหรัฐฯ ได้นำระบบการสื่อสารข้อมูลในอินเทอร์เน็ตมาเป็นพื้นฐานในการสร้างเครือข่ายข้อมูลเพื่อสนับสนุนปฏิบัติการรบทั้งในภาคพื้นดิน ทางอากาศ และทางทะเล ซึ่งทำให้เกิดความคล่องตัวในปฏิบัติการทางทหารขนาดใหญ่ (campaign) และในสงครามอิรักนั้นปฏิบัติการข้อมูลข่าวสาร (Information Operations) เป็นหัวใจสำคัญของการรบในสมรภูมินั้น ซึ่งปฏิบัติการข่าวสารประกอบด้วยห้าส่วนปฏิบัติการหลัก คือ Electronic Warfare, Computer Network Operations, Psychological Operations, Operation Security, และ Military

Deception [JP 3-13] ถึงแม้ว่าระบบคอมพิวเตอร์เน็ตเวิร์กได้ถูกนำมาใช้อย่างจริงจังในสงครามขนาดใหญ่ แต่ก็ยังเป็นการยากสำหรับผู้บังคับบัญชาในการกำหนดหลักนิยมสำหรับปฏิบัติการข่าวสาร ส่งผลให้ขาดความชัดเจนในส่วนของกระบวนการตัดสินใจ ความรับผิดชอบในคำสั่งการ และการปฏิบัติของหน่วยปฏิบัติ จึงได้มีแนวคิดในการที่จะกำหนดหลักนิยมของการปฏิบัติการข่าวสารและพัฒนาไปสู่หลักนิยมการรบในมิติไซเบอร์โดยจะกล่าถึงรายละเอียดในบทต่อไป

คำว่ามิติไซเบอร์ (Cyberspace) ได้มีการกำหนดไว้ใน JP 3-12 Cyberspace Operations ในปี ค.ศ. 2011 และได้เกิดความสับสนกับ JP 3-13 Information Operations ปี ค.ศ. 2012 อย่างไรก็ตามเพื่อมิให้เกิดความสับสนและมุ่งเน้นไปที่แนวคิดของหลักนิยมของปฏิบัติการในมิติไซเบอร์ผู้เขียนจะใช้ข้อมูลที่อยู่ใน JP 3-12 เป็นหลักประกอบกับเอกสารของ Brett T. Williams [14] ที่เขียนขึ้นให้มีความง่ายในการเข้าใจ Cyberspace Operations สำหรับผู้บังคับบัญชาระดับสูงในกองบัญชาการร่วม (Joint Force Commanders) เป็นพื้นฐานของแนวคิด

วิวัฒนาการการพัฒนาหลักนิยมด้านไซเบอร์ของสหรัฐอเมริกาและประเทศอื่น ๆ

Andrew Colarik และ Lech Janczewski ได้กล่าวถึง Cyber Warfare Doctrine ในบทความการจัดตั้งหลักนิยมไซเบอร์วอร์แฟร์ของประเทศนิวซีแลนด์ และได้พยายามอธิบายว่าทำไมระบบ IT (Information Technology) และส่วนประกอบสนับสนุนอื่น ๆ จึงถือเป็นเป้าหมายทางทหาร ในยามที่เกิดความขัดแย้ง และได้นำเสนอกรอบแนวคิดของกระบวนการในการตัดสินใจเพื่อใช้เป็นพื้นฐานของหลักนิยมสงครามไซเบอร์ โดยเน้นจุดตัดสินใจของผู้นำระดับประเทศเป็นจุดเริ่มต้นของการพัฒนาหลักนิยมสงครามไซเบอร์ และความร่วมมือในการปฏิบัติงานร่วมกันระหว่างทุกภาคส่วน และควรได้รับความเห็นชอบจาก Security Council ระดับชาติ (เช่น สมช.) ก่อนที่จะนำเสนอให้ผู้นำประเทศลงนามรับรอง เพื่อที่นำออกเผยแพร่สู่สาธารณะต่อไป

David J Smith ผู้อำนวยการศูนย์ไซเบอร์ของ Potomac Institute for Policy Studies ได้กล่าวในบทความของเขาถึงปฏิบัติการไซเบอร์ของประเทศรัสเซียว่ามีระดับความสำคัญกว่าภัยคุกคามจากประเทศจีน หนึ่งในเหตุผลที่สนับสนุนเรื่องนี้คือ ปฏิบัติการไซเบอร์ของรัสเซียยากที่จะถูกค้นพบ โดยรัสเซียเป็นประเทศที่มีความชัดเจนในการสนับสนุนปฏิบัติการไซเบอร์ของกลุ่มแฮ็กเกอร์โดยองค์กรระดับรัฐบาล และได้มีการรวมหลักนิยมสงครามไซเบอร์ไว้ในปฏิบัติการทางทหาร โดยมีปฏิบัติการอย่างกว้างขวางในด้านสงครามข่าวสาร เช่น intelligence, counterintelligence, deceit, disinformation, electronic warfare เป็นต้น รัสเซียมีการกำหนดชัดเจนในการตอบโต้ด้วย information warfare เพื่อจะให้บรรลุวัตถุประสงค์ทางการเมืองโดยไม่ต้องใช้กำลังทางทหาร “war without tanks” และใน ค.ศ. 2008 การโจมตีประเทศจอร์เจียด้วย cyber attack และกำลังทางทหารเป็นครั้งแรกของการทดสอบหลักนิยมของสงครามไซเบอร์ของรัสเซีย และสหรัฐฯ เองก็ได้เรียนรู้จากสงครามนี้ถึงผลกระทบของ DDoS attack รัสเซียได้กำหนด หลักนิยมของการรักษาความมั่นคงปลอดภัยข้อมูล ซึ่งกำหนดแนวทางการแชร์ข้อมูล สิ่งที่เป็นเอกลักษณ์ของรัสเซียคือการใช้กลุ่มเยาวชนที่มีขีดความสามารถในปฏิบัติการไซเบอร์เป็นกองกำลังสำคัญ เพราะ 1. ทำให้ต้นทุนในปฏิบัติการต่ำ และ 2. การพิสูจน์หลักฐานย้อนกลับไปยากที่จะทราบว่าเป็นการสนับสนุนโดยรัฐบาลจนเกิดอุตสาหกรรม “Botnets for hire” ซึ่งสามารถเห็นอย่างชัดเจนในการโจมตีประเทศเอสโตเนีย

และยุทธศาสตร์ของรัสเซียก็มีความชัดเจนในการทำสงครามไซเบอร์ต่อประเทศสหรัฐฯ

ในทำนองเดียวกันบทความของ Keir Giles แห่ง ICT Studies ประเทศสหราชอาณาจักรก็ได้สนับสนุนแนวคิดเช่นเดียวกับที่ D J Smith กล่าวไว้ คือในปี ค.ศ. 2011 ได้มีประกาศร่าง Conventional on International Information Security และในทางทหารเป็นแนวคิดของหลักการสงครามไซเบอร์ ชื่อ “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space” ซึ่งในที่นี้คำว่า information space น่าจะหมายถึง cyberspace ที่ฝั่งประเทศตะวันตกใช้กันอย่างกว้างขวาง ซึ่งหลักการนี้ได้กล่าวเชิงสรุปว่า ปฏิบัติการในมิติไซเบอร์จะเกิดขึ้นหลังจากความล้มเหลวทางการเจรจาทางการทูตเสมอ นอกจากนั้น Joint Doctrine Note 2/13: Information Superiority ของกระทรวงกลาสหราชอาณาจักร ยังได้กล่าวถึงความเป็นผู้นำสูงสุดในเรื่องของข้อมูลข่าวสาร ซึ่งยังไม่มีการกำหนดไว้ชัดเจนถึงหลักการที่ดีที่สุดในปฏิบัติการสำหรับโดเมนของไซเบอร์ โดยเอกสารนี้มีวัตถุประสงค์เพื่อกำหนดความชัดเจนของคำว่า “Information Superiority” และให้แนวทางเพื่อที่จะทำให้บรรลุวัตถุประสงค์และสามารถนำมาใช้งานร่วมกับปฏิบัติการอื่น ๆ ทั้งนี้เพื่อให้กระบวนการตัดสินใจของผู้บังคับบัญชามีประสิทธิภาพ โดยจะพัฒนาจากหลักนิยมที่มีอยู่ในปัจจุบัน หลัก “Best Practice” เพื่อที่จะสร้างเอกสารให้ผู้บังคับบัญชาและเจ้าหน้าที่สามารถปฏิบัติงานร่วมกันได้อย่างมีประสิทธิภาพ โดยแบ่งเป็นสามส่วนหลักคือ 1. กำหนดหลักการพื้นฐานของ information superiority 2. การทำให้สามารถมีความเป็น information superiority และ 3. การ exploit สังเกตุได้ว่าสิ่งที่แตกต่างของเอกสารของสหราชอาณาจักรคือใช้คำว่า “exploit” หรือการแสวงประโยชน์ อย่างชัดเจนแสดงให้เห็นถึงความสำคัญของการปฏิบัติเชิงรุกในโดเมนไซเบอร์

ในฝั่งประเทศยุโรป ENISA ได้เผยแพร่ National Cyber Security Strategies: Practical Guide on Development and Execution เพื่อเป็นแนวทางในการพัฒนาและดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับประเทศในสมาชิกของ EU (European Union) ENISA คือ หน่วยงานที่เป็นศูนย์กลางด้าน network และ information security ของ EU ซึ่งตั้งอยู่ในประเทศกรีก ทั้งนี้เพื่อสนับสนุนกลุ่มประเทศสมาชิกในการเสริมสร้างศักยภาพด้านไซเบอร์ ด้วยการให้คำแนะนำในเรื่องนโยบาย การจัดทำยุทธศาสตร์ รวมถึงการฝึกฝนบุคลากรเพื่อให้สามารถดำเนินการที่จำเป็นสำหรับปฏิบัติการด้านไซเบอร์ได้

ในประเทศสหรัฐอเมริกาได้มีวิวัฒนาการของการพัฒนาหลักนิยมสงครามไซเบอร์มาอย่างต่อเนื่อง ในปี ค.ศ. 2001 Lt Col. Lionel D Alford Jr แห่งกองทัพอากาศของสหรัฐฯ ได้นำเสนอบทความ Cyber Warfare: A New Doctrine and Taxonomy ในเอกสารสิ่งพิมพ์ Open Forum โดยได้กล่าวถึงวิวัฒนาการของการนำซอฟท์แวร์มาเป็นเครื่องในการโจมตีเพื่อให้สามารถบรรลุวัตถุประสงค์ทางทหารได้เช่นกัน และระดับของความรุนแรงในการโจมตีได้มีการเพิ่มขึ้นอย่างต่อเนื่อง อย่างไรก็ตามในขณะนั้นหลักนิยมในด้านนี้ยังมิได้มีการพัฒนาขึ้นอย่างจริงจังถึงแม้ว่าจะมีการ JP 3-13.1 Joint Doctrine for Command Control Warfare และข้อกำหนดของกลาโหม DoD 5000.2-R ในการควบคุมกระบวนการจัดหาอาวุธยุทโธปกรณ์ ซึ่งหลักนิยมในขณะนั้นเน้นที่ระบบรักษาความปลอดภัยของ C4I ซึ่งขาดความครอบคลุมในเรื่องของสงครามไซเบอร์ในภาพรวม Alford ได้เสนอว่าระบบทางการทหารที่ควบคุมด้วยซอฟท์แวร์เป็นเป้าหมายสำคัญของการโจมตีทาง

ไซเบอร์ และระบบ C4I ยิ่งมีความวิกฤติต่อการถูกโจมตีเนื่องจากมีการเชื่อมโยงทางเครือข่ายกันอย่างกว้างขวาง และได้นำเสนอนิยามศัพท์ทางไซเบอร์เช่น Cyber warfare, Cyber infiltration, Cyber assult เป็นต้น

Michael Warner ได้นำเสนอข้อคิดเกี่ยวกับ หลักนิยมทางทหารสำหรับปฏิบัติการไซเบอร์ของสหรัฐฯ ห้วงปี ค.ศ.1992-2014 ใน The Cyber Defense Review โดยได้กล่าวถึงเอกสารของ Joint Publication ที่ใช้ในปฏิบัติการไซเบอร์ที่ผ่านมา เช่น JP 3-13.1 เปรียบเทียบการเปลี่ยนของ JP 3-12 ซึ่งจะไม่กล่าวถึงการจัด classification ของคอมพิวเตอร์เน็ตเวิร์ก โดยใช้คำศัพท์บัญญัติใหม่เพื่อให้มีความกระจ่างในความเข้าใจที่ตรงกันโดยใช้คำว่า “Cyberspace Opertaions” ซึ่งจะประกอบด้วยภารกิจหลักสามประการคือ 1. เชิงรุก (Offensive) 2. เชิงรับ (Defensive) และดำรงสภาพ (Sustaining) ระบบของ DoD โดยที่ปฏิบัติการในมิติไซเบอร์จะใช้กระบวนการตัดสินบังคับบัญชา เช่นเดียวกับปฏิบัติในโดเมนอื่น ๆ ปฏิบัติการเชิงรับอาจเป็นได้ทั้งแบบ passive และ active ที่เพิ่มขอบเขตของปฏิบัติการออกนอกพื้นที่ของ DoD network ซึ่งนำไปสู่ระดับของ “การใช้กำลัง” (use of forces) ผู้บังคับบัญชาควบคุมสั่งการปฏิบัติการในมิติไซเบอร์โดยใช้ปฏิบัติการหลักสี่ประการ 1. Cyberspace defense 2. Cyberspace attack 3. Cyberspace ISR, และ 4. Cyberspace OPE. ปฏิบัติการสองอย่างแรกคงเป็นที่คุ้นเคยกันแต่สองปฏิบัติการหลังเป็นสิ่งใหม่ที่ถูกกำหนดไว้ใน JP 3-12 โดยที่ Cyberspace ISR มาจากปฏิบัติการย่อย intelligence, surveillance, และ reconnaisance และ Cybespace OPE มาจากปฏิบัติการ operational preparation environment ปฏิบัติการ OPE ไม่เกี่ยวข้องกับ intelligence กระทำเพื่อที่จะวางแผน และเตรียมการสำหรับปฏิบัติทางทหารที่จะตามมาขั้นต่อไป โดยที่หลักนิยมสำหรับปฏิบัติการไซเบอร์จะไม่เน้นหนักที่คำศัพท์ command control warfare และ information operations อีกต่อไป อย่างไรก็ตาม Warner ได้สรุปว่าความเปลี่ยนแปลงในหลักการที่กำหนดไว้ใน JP 3-13.1 (ค.ศ.1996) และ JP 3-12 (ค.ศ.2013) ไม่ได้มีมากนัก สิ่งที่มีความแตกต่างอย่างชัดเจนคือ “หลักนิยม” ที่เน้นหนักการใช้คำแทนโดเมนที่เกิดใหม่ว่า “cyberspace” เนื่องจากเทคโนโลยีสารสนเทศได้สร้างเครื่องมือใหม่ ๆ ขึ้นมาอย่างหลากหลายและเป็นโอกาสที่ปฏิบัติการทางทหารสามารถนำไปใช้เพื่อการต่อสู้ในสงครามได้

เอกสารและหน่วยงานความมั่นคงที่เกี่ยวข้องกับความมั่นปลอดภัยไซเบอร์

ตารางต่อไปนี้รวมรวมข้อมูลเกี่ยวกับเอกสารและหน่วยงาน ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยประเภทเอกสารที่เกี่ยวข้องได้แก่ White Paper, ยุทธศาสตร์ไซเบอร์แห่งชาติ, ยุทธศาสตร์การป้องกันประเทศ, หลักนิยมทางทหาร, และนโยบายความมั่นคง ฯลฯ เพื่อความกระชับของตารางที่มีข้อมูลจำนวนมากผู้เขียนกำหนดไว้เป็นอักษรย่อในหมายเหตุ และหากมีข้อมูลจะมีรายชื่อขององค์กรที่รับผิดชอบ ตามด้วยปี ค.ศ. ที่ได้รับการเผยแพร่ นอกจากนั้น ในหมายเหตุในตารางจะมีข้อมูลแต่ละประเทศที่มีการะบุข้อมูลประเทศที่เป็นพันธมิตร หมายเหตุ: N/A = Not Available, <u>พันธมิตร</u>: N = NATO-based/alliance, US = USA alliance, K = UK, C = Commonwealth of Independent States, RU = Russia, <u>เอกสาร</u>: WP = White Paper, CS = National Cyber Strategy, DS = National Defense Strategy, MD = Military Doctrine, SP = Security Policy

ตารางที่ 2-1 เปรียบเทียบหลักนิยมทางทหาร white paper นโยบายความมั่นคงของประเทศต่าง ๆ (ต่อ)

ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี (ค.ศ.)	หมายเหตุ*, พันธมิตร
1	อัลบาเนีย	Interinstitutional Maritime Operational Center (IMOC)	2011	N/A
2	อาเจนติน่า	Jefatura VI	2008	หน่วย C4I
3	ออสเตรีย WP	Abwehramt*	2008	Military intelligence organization
4	ออสเตรเลีย CS	Cyber Security Operations Center	2009	ส่วนหนึ่งของ DoD ภายใต้ Defence Signals Directorate, มีบุคลากร 130 คน, UK
5	เบลารุส MD	Belarus Armed Forces		N/A
6	บราซิล DS	Cyber-Warfare Communication Centre, Center of Cyber Defense*	2008	*มีบุคลากร 100 คน, US
7	แคนนาดา CS	Canadian Forces NOC	2010	N/A
8	จีน WP	4th & 3rd General Staff Departments	2009	N/A
9	โคลอมเบีย CS	Colombia CERT	2009	MoD รับผิดชอบหลัก
10	เกาหลีเหนือ[1]	Specialized units in military	2011	มหาวิทยาลัยสนับสนุน offensive training, RU
11	เดนมาร์ก MD	Danish cyber network operations unit	2010	ใช้กำลังพลหลักจาก DoD หลายหน่วยงานที่เกี่ยวข้อง
12	เอสโธเนีย CS	Cyber Security Alliance*/Cyber Security Strategy Committee	2011	*ภายใต้องค์กร Defence League, N

[1] สาธารณรัฐประชาธิปไตยประชาชนเกาหลี (Democratic People's Republic of Korea)

ตารางที่ 2-1 เปรียบเทียบหลักนิยมทางทหาร white paper นโยบายความมั่นคงของประเทศต่าง ๆ (ต่อ)

ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี (ค.ศ.)	หมายเหตุ*, พันธมิตร
13	ฝรั่งเศส WP	NASIS[2]	2009	หน่วยงานภายใต้ สน.นายกรัฐมนตรี บริหารโดย รมว.กห.
14	จอร์เจีย SP	National Security Concept	2005	นำโดย MoD
15	เยอรมันนี MD	National Cyberdefence Centre*, BSI**	2011	*ภายใต้ MoI, ** หน่วยงานความมั่นคงของเยอรมัน
16	อินเดีย MD	Defence IW Agency, DIA*, National Technical Intelligence Communication Centre, Joint Cybersquad**	2009	*รับผิดชอบ offensive, **สามารถแฮ็กองค์กรรัฐได้อย่างถูกกฎหมายเพื่อตรวจสอบช่องโหว่, US
17	อิสราเอล	IDF[3] Unit 8200, Shin Bet, C4I Corps, Matzov[4], National Cybernetic Taskforce*	2009	หน่วยงานขนาด 80 คน เพื่อป้องกันระบบ, U
18	อิหร่าน	Passive Defense Organization*, Cyberwarfare Unit ใน IRGC[5]**	2010	*หน่วยงานใน กห.อิหร่าน, **มี จนท.ไซเบอร์ประมาณ 2,400 คน(ใหญ่เป็นลำดับสองของโลก)
19	อิตาลี CS	Military Electronic Warfare Unit, Telematics Section	2011	N/A
20	คาซัคสถาน	Ministry of Communication and		India

[2] National Agency for the Security of Information Systems

[3] Israel Defense Forces

[4] Centre for Encryption and Information Security

[5] Islamic Revolutionary Guard Corps

ตารางที่ 2-1 เปรียบเทียบหลักนิยมทางทหาร white paper นโยบายความมั่นคงของประเทศต่าง ๆ (ต่อ)

ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี (ค.ศ.)	หมายเหตุ*, พันธมิตร
		Information		
21	มาเลเซีย SP	Cybersecurity Malaysia	2007	เป็นส่วนหนึ่งของ Ministry of Science, Technology and Innovation
22	พม่า DS	Defense Services Computer Directorate, Army of Myanmar	1990	
23	เนเธอร์แลนด์ CS, SP	National Cyber Security Board, National Cyber Security Centre	2012	ไม่มีหน่วยเฉพาะสำหรับ cyberwarfare, Alliance: Luxembourg, Belgium
24	นอร์เวย์ CS	Ministry of Defence	2010	กห.รับผิดชอบหลัก
25	โปแลนด์ DS	Independent Information Force	TBE[6]	ภายใต้กองทัพบก, N
26	เกาหลีใต้[7] WP	Cyber War Centre/Command	2010	หน่วยงานอิสระ แต่ดูแลโดย กห.กลต. ทั้ง defensive และ offensive, กห. ร่วมกับสถาบันการศึกษาสร้าง cyberwarfare school,
27	รัสเซีย MD	FAGCI[8], FSS[9]*	2010	*เฉพาะงาน cryptography และ code-breaking

[6] กำลังจัดตั้ง

[7] The Republic of Korea

[8] Federal Agency of Government Communications and Information

[9] Federal Security Service

ตารางที่ 2-1 เปรียบเทียบหลักนิยมทางทหาร white paper นโยบายความมั่นคงของประเทศต่าง ๆ (ต่อ)

ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี (ค.ศ.)	หมายเหตุ*, พันธมิตร
28	สวิตเซอร์แลนด์ SP	Centre for Electronic Operations of AFCSO[10], Military CERT, NOC	2010	กห. รับผิดชอบหลัก
29	ตรุกี DS	Cyber Army Command, BILGEM	2010	General Staff รับผิดชอบของทั้งประเทศ
30	สหราชอาณาจักร CS	Cyber Security Operations Centre, OCSIA[11]	2009	ลงทุนด้านนี้อีก $1.6 billion
31	สหรัฐอเมริกา SS	DHS, FBI, DoD, US Cyber Command, NSA, CIA	1990	เริ่มบุกเบิกด้านนี้ตั้งแต่ 1990
32	ไทย DS	Cyber Center MoD/RTAF/Army/Navy/Air Force	2016	ยังไม่มีหน่วยระดับชาติรับผิดชอบหลัก (ยกเว้น ThaiCERT) อยู่ในระหว่างจัดทำกฎหมายไซเบอร์เพื่อจัดตั้งหน่วยงานรับผิดชอบหลัก ในส่วนของกลาโหมได้มีการจัดตั้งศูนย์ไซเบอร์ต่าง ๆ ตามหน่วยงานหลัก
33	ฟินแลนด์ SP, MD	Ministry of Transport and Communications	2006	กห จัดทำ MD เป็นส่วนหนึ่งของ SP

นโยบายและหน่วยงานภาคพลเรือนที่เกี่ยวข้องกับไซเบอร์

หมายเหตุ: N/A = Not Available/ไม่มีข้อมูล

- พันธมิตร: N = NATO-based/alliance, US = USA alliance, K = UK, C = Commonwealth of Independent States, RU = Russia

[10] Armed Forces Command Support Organization

[11] Office of Cyber Security and Information Assurance

- <u>เอกสาร</u>: WP = White Paper, CS = National Cyber Strategy, NS/DS = National Defense/Security Strategy, SP = Security Policy

ตารางที่ 2-2 นโยบายและหน่วยงานพลเรือนที่เกี่ยวข้อง (ต่อ)				
ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี	หมายเหตุ*, พันธมิตร
1	อันติกัวและบาบูดา	National CERT[12], Regional Cyber Forensics Lab	2009	N/A
2	เบลเยี่ยม	ไม่มีหน่วยรับผิดชอบหลัก, Belgium Armed Forces	2000	เนเธอร์แลนด์
3	บรูไน	CERT	2004	ภายใต้ Ministry of Communication, กห. ไม่ใช่หน่วยรับผิดชอบหลัก
4	บัลเกเรีย WP	National Cyber Authority	2010	มี กห. รับผิดชอบโดยใช้กำลังพลสำรอง และ จนท.IT, N
5	โครเอเชีย DS	Signals Unit	2005	กห.รับผิดชอบหลัก
6	คิวบา	Ministry of Informatics and Telecommunications	2011	RU
7	ไซปรัส	CyberEthics, CERT*	2004	*มีสอง CERT สำหรับรัฐบาล กับหน่วยเอกชนและการศึกษา
8	สาธารณรัฐเช็ก DS, WP	Cyber & Information Security Department*	2008	รับผิดชอบโดย MoI, กห. ออก Wp ในปี 2011
9	กาน่า	CERT (planned)	2009	Ministry of Communications
10	ฮังการี CS/DS	National Cybersecurity Center	2004	เป็นส่วนหนึ่งของ สำนักนายกฯ
11	อินโดนีเซีย	ไม่เผยแพร่เอกสารใด ยกเว้น		กห. ไม่มี Cyberwarfare

[12] Computer Emergency Response Team

ตารางที่ 2-2 นโยบายและหน่วยงานพลเรือนที่เกี่ยวข้อง (ต่อ)				
ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี	หมายเหตุ*, พันธมิตร
		แต่ในภาพรวมมีการทำกฎหมายไซเบอร์		
12	ญี่ปุ่น MD, WP	National Information Security Center*, Cyber Defence Unit in C4[13]**, Cyber Clean Center**	2005	*สนับสนุนในระดับรัฐบาล, ** หน่วยใน JSDF[14], **โดย Ministry of Internal Affairs & Communications
13	จอร์แดน	C4ISR[15]	2010	Jordanian Armed Forces
14	เคนย่า	CERT, หลักสูตร		Ministry of Information & Communication, มีการสร้างบุคลากรไซเบอร์โดย Kenya Armed Forces Technical College
15	ลัทเวีย WP	กฎหมาย IT Security, Cyber-Security REsponse Agency*		*มีผู้เชี่ยวชาญ 8 คน, Ministry of Transport รับผิดชอบการพัฒนานโยบายด้าน IT Security , NA
16	ลิทธัวเนีย CS	เป็นส่วนหนึ่งของ NATO Cooperative Cyber Defence Centre of Excellence	2011	MoD รับผิดชอบหลัก, NA
17	ลักเซมเบอร์ก CS	CERT	2003	โดย Ministry of Economy & Foreign Trade, มี MoD กับเนเธอร์แลนด์
18	มัลดีฟส์ CS	MNDF & PS[16]	2011	ได้รับการช่วยเหลือจาก

[13] Command, Control, Communications, and Computer Systems

[14] Japan Self-Defense Forces [2008]

[15] Command, Control, Communications, and Computer, Surveillance, and Reconnaissance

[16] Maldives National Defence Force and Police Service

ตารางที่ 2-2 นโยบายและหน่วยงานพลเรือนที่เกี่ยวข้อง (ต่อ)				
ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี	หมายเหตุ*, พันธมิตร
				US FBI[17]
19	มัลตา CS, DS	Malta Information Technology Agency, NISA[18], CERT	2010	ไม่มีผู้รับผิดชอบหลักในกห.
20	โมร็อคโค NS	ไม่มีข้อมูลระบุความรับผิดชอบ	2013	MoU กับประเทศมาเลเซีย
21	นิวซีแลนด์ WP	Netsafe*, ORB[19], MED[20]**, CCIP[21], NCSC[22]	2010	*เน้นสร้างความตระหนักฯ, **เป็นหน่วยงานหลักด้านไซเบอร์
22	ไนจีเรีย	National Cybersecurity Initiative, NCWG[23], Directorate for Cybersecurity*	2004	*ภายใต้ National Security Advisor
23	โอมาน	OCERT	2010	รับผิดชอบ public IT infra. ป้องกัน financial transaction
24	ปากีสถาน	National Response Centre for Cyber Crimes*	2003	*ภายใต้ Federal Investigation Agency
25	โปรตุเกต	Knowledge Society Agency	2010	กำลังพัฒนายุทธศาสตร์
26	ฟิลิปปินส์	GCERT*, National Cyber Security Office	2004	*จัดตั้งโดย task force for security of critical infrastructure

[17] Federal Bureau of Investigation

[18] National Information Security Agency

[19] Online Reporting Botton

[20] Ministry of Economic Development

[21] Centre for Critical Infrastructure Protection

[22] National Cyber Security Centre หน่วยงานในสังกัด Government Communications Security Bureau

[23] Nigerian Cybercrime Working Group

ตารางที่ 2-2 นโยบายและหน่วยงานพลเรือนที่เกี่ยวข้อง (ต่อ)				
ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี	หมายเหตุ*, พันธมิตร
27	เซอร์เบีย NS	Cyber Crime Department	2005	ออกกฎหมายเพื่อควบคุมการใช้อินเทอร์เน็ต กระบวนการยุติธรรม
28	สิงค์โปร์ CP	Singapore Infocomm Technology Security Authority	2010	*ภายใต้ Internal Security Department ใน Ministry of Home Affairs -->สามารถเรียกพลด้าน IT เพื่อบรรจุเป็น cyber defenders ได้[24]
29	สโลวาเกีย NS	สมาชิก NATO Cooperative Cyber Defence Centre of Excellence		NA
30	สโลเวเนีย NS	จะตั้ง National Cyber Coordination body		Amy เป็นผู้ตอบสนองหลัก
31	อาฟริกาใต้ CP	Cyber Inspectorate, National Cybersecurity Advisory Council	2012	GB
32	สเปน NS	CERT, National Cryptology Center*	2010	*ภายใต้ National Intelligence Centre
33	สหรัฐอาหรับ เอมิเรด	Cyber Operations Centre*, CERT**	2011	*ส่วนหนึ่งของ Command Control System ทำร่วมกับมหาวิทยาลัย Khalifa, ** โดย Telecommunications REgulatory Authority
34	เวียตนาม SP	CERT*, International Data Group	2011	*ภายใต้ General Department of Logistics and TEchnology ในกระทรวง Public Security

[24] Tyler Thia, “Singapore seeks volunteers to beef up cyber defense”, ZDNet, 28 Sep 2010

ตารางที่ 2-2 นโยบายและหน่วยงานพลเรือนที่เกี่ยวข้อง (ต่อ)				
ลำดับ	ประเทศ/เอกสาร	องค์กร	ปี	หมายเหตุ*, พันธมิตร
35	ซิมบับเว SP, CP	MICT	2010	ไม่ระบุหน่วยงานหลักที่รับผิดชอบ
36	ไทย	ThaiCERT*, กระทรวง DE[25], ETDA[26], EGA[27]		จัดตั้งปี 2000 ภายใต้ NECTEC สวทช. จากนั้นย้ายมาอยู่กับ สพธอ. (ETDA) ทั้ง ETDA และ EGA อยู่ภายใต้การกำกับดูแลของ DE

จากการสำรวจวรรณกรรมที่เกี่ยวข้องกับหลักนิยมนั้นแสดงให้เห็นว่า ประเทศต่าง ๆ ได้ให้ความสำคัญกับภัยคุกคามด้านไซเบอร์เป็นอย่างมาก อย่างไรก็ตามปัญหาการขาดแคลนบุคลากรด้านไซเบอร์ก็ยังคงเป็นปัญหาใหญ่สำหรับองค์กรทั่วไป ทั้งภาครัฐและเอกชนอย่างหลีกเลี่ยงไม่ได้ ทั้งนี้เนื่องจากการพัฒนาบุคลากรด้านไซเบอร์นั้นต้องการคนที่มีไหวพริบดี และมีขีดความสามารถหลากหลายในสาขาเช่น Computer Architecture and programming, Internetworking, Assembly programming, Social Engineering, Social Media exploitation เป็นต้น ซึ่งจะเห็นได้ว่าลำพังบุคลากรที่มีพื้นฐานความรู้ด้านคอมพิวเตอร์และเครือข่ายยังมีปัญหาการขาดแคลนบุคลากรอยู่เป็นทุนเดิมอยู่แล้ว ความยากของปัญหายิ่งเพิ่มขึ้นอีกหลายเท่าตัวในมิติของไซเบอร์เนื่องจากต้องการบุคลากรที่มีความรู้ในขั้นดีและหลากหลาย อีกทั้งยังต้องมีไหวพริบที่ดี สามารถตอบสนองต่อการคุกคามทางไซเบอร์ที่มีความเปลี่ยนแปลงอยู่ตลอดเวลา ในบทต่อไปจะกล่าวถึงปัญหาการพัฒนาบุคลากรด้านไซเบอร์ในภาพรวมของประเทศ

ปัญหาการพัฒนาบุคลากรด้านไซเบอร์

ปัญหาการสร้างบุคลากรด้านไซเบอร์ถูกระบุว่าเป็นปัญหาใหญ่สำหรับประเทศมหาอำนาจ เช่น สหรัฐอเมริกา ในเอกสาร White Paper ของ CSIS (Center for Strategic & International Studies[28] ในชื่อเรื่อง “A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters” กล่าวถึงปัญหาการขาดแคลนบุคลากรไซเบอร์ไว้ว่า “ในสหรัฐอเมริกามี

[25] Ministry of Digital Economy and Society, กระทรวงดิจิตัลเพื่อเศรษฐกิจและสังคม

[26] Electronic Transactions Development Agency, สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

[27] Electronic Government Agency, สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

[28] https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf

ผู้เชี่ยวชาญด้านไซเบอร์ที่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพในไซเบอร์สเปซ จำนวนประมาณ 1,000 คน แต่ความต้องการบุคลากรที่แท้จริงนั้นมีถึง 10,000 ถึง 30,000 คน”[29] นอกจากปัญหาในมุมมองของจำนวนที่ขาดแคลนแล้ว ปัญหาเรื่องคุณภาพก็เป็นอีกประเด็นปัญหาสำคัญของการพัฒนาบุคลากรด้านไซเบอร์

ปัญหาการขาดแคลนบุคลากรที่ยากต่อการพัฒนาได้แก่ การพัฒนาบุคลากรในระดับ Red Team ซึ่งจะทำหน้าที่ในการโจมตีเครือข่ายที่ถูกกำหนดให้เป็นเป้าหมาย ในขณะที่ Blue Team จะทำหน้าที่ตรวจสอบความปลอดภัยของระบบในไซเบอร์สเปซ และทำหน้าที่เหมือนกับการตั้งรับในการรบในสงครามปกติ นอกจากนั้นเอกสารของ CSIS ยังกล่าวถึง Cybersecurity Workforce ซึ่งมิใช่เป็นแต่เพียงกำลังพลของทหาร แต่ยังรวมถึงผู้เชี่ยวชาญที่ทำงานอยู่ภายใต้สัญญาการทำงานระหว่างรัฐกับภาคเอกชน โดยเฉพาะอย่างยิ่งบุคลากรด้านไซเบอร์ที่ทำงานกับโครงสร้างพื้นฐานสำคัญยิ่งยวด เช่น ระบบไฟฟ้า ระบบโรงงานที่มีการควบคุมด้วยระบบคอมพิวเตอร์ เป็นต้น แนวทางที่นำเสนอโดย CSIS สรุปได้ดังนี้

1. ให้การสนับสนุน และให้งบประมาณในการพัฒนาบุคลากรด้านไซเบอร์ในระดับโรงเรียน

2. สนับสนุนการพัฒนาและการยอมรับประกาศนียบัตรวิชาชีพด้านไซเบอร์ที่มีความยากในการสอบผ่าน และเฝ้าตรวจการทำงานขององค์ประกอบต่าง ๆ ที่เกี่ยวข้อง

3. บูรณาการกระบวนการจ้างงาน, การจัดหา, และการฝึกอบบรมบุคลากรเพื่อยกระดับขีดความสามารถของผู้ที่ต้องทำงานในการออกแบบ สร้าง ทำงาน และป้องกันระบบของหน่วยงานภาครัฐ

4. สร้างแนวทางการทำงานในวิชาชีพไซเบอร์ (Career Path) ให้เป็นเช่นเดียวกับแนวทางสำหรับวิศวกร หรือแพทย์ ที่ต้องใช้บคุลากรที่มีขีดความสามารถสูงกว่าบุคคลทั่วไป

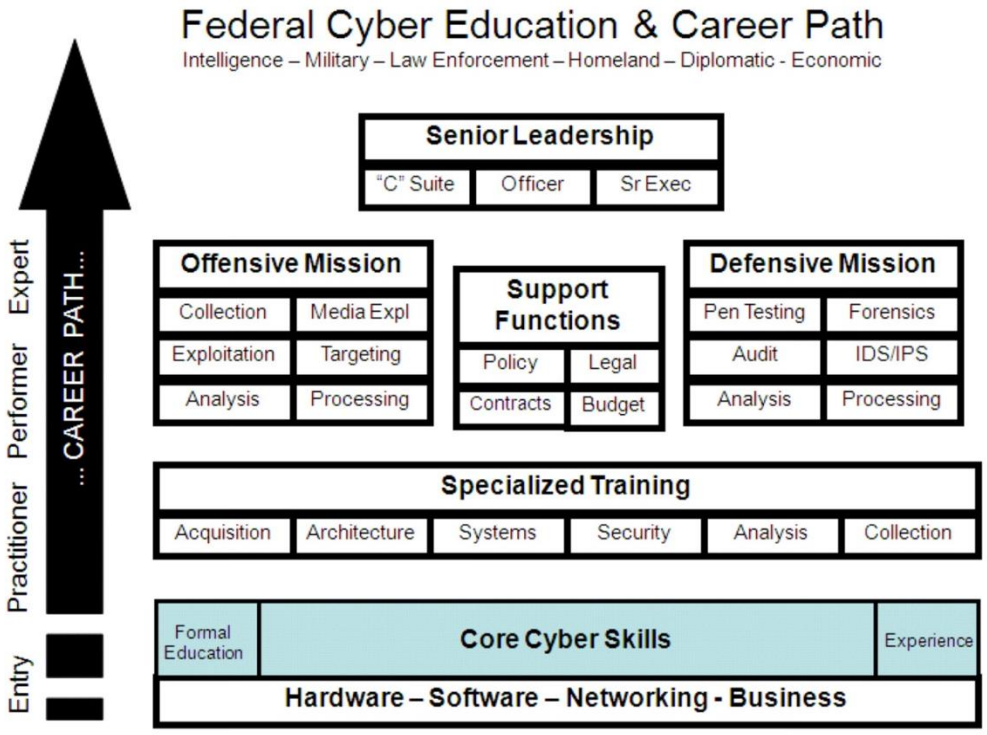
นอกจากนั้น CSIS ยังนำเสนอแนวทางการพัฒนาบุคลากรด้านไซเบอร์โดยให้วิสัยทัศน์สำหรับการศึกษาสำหรับการประกอบวิชาชีพด้านไซเบอร์ตั้งแต่ระดับเริ่มต้นไปจนถึงระดับผู้บริหาร (รูปที่ 1) โดยจะเริ่มต้นที่ระดับ Entry, Practitioner, Performer, และ Expert โดยระดับ Entry จะมีการศึกษาขั้นพื้นฐานที่เรียกว่า Core Cyber Skills เช่น Hardware, Software, Networking, และ Business ในระดับ Practitioner จะเป็นการฝึกอมรมในเรื่องเฉพาะทางที่เกี่ยวข้องกับ Acquisition, Architecture, Systems, Security, Analysis, และ Collection ในระดับ Performer และ Expert จะแบ่งออกเป็นตามหน้าที่การทำงานคือ Offensive Mission, Support Functions, และ Defensive Mission ซึ่ง Offensive Mission จะศึกษาในหัวข้อ Collection, Media Exploitation, Exploitation, Targeting, Analysis, และ Processing ในส่วนของ Support Functions จะศึกษาในเรื่อง Policy, Legal, Contracts, และ Budget และในส่วนของ Defensive Mission จะศึกษาในหัวข้อ Penetration Testing, Forensics, Audit, IDS/IPS, Analysis, และ Processing โดยที่แนวทางการประกอบวิชาชีพจะมีการเลื่อนลำดับขั้นขึ้นไปจนถึงระดับ Senior Leadership ซึ่งประกอบ

---

[29] Jim Gosler, Sandia Fellow, NSA Visiting Scientist, and the founding Director of the CIA’s Clandestine Information Technology Office

ไปด้วย “C” Suite, Officer, และ Senior Executive

แผนภาพที่ 2-1 การศึกษาด้านไซเบอร์และแนวทางประกอบวิชาชีพไซเบอร์



ที่มา: CSIS (Center for Strategic & International Studies

Morgan Zantua, Marc Dupuis, และ Barbara Endicott-Popovsky ได้นำเสนอบทความเรื่อง “Re-engineering the Cybersecurity Human Capital Crisis”, ตุลาคม 2559 ในเอกสารวิจัยจาก Research Gate (www.researchgate.net) พบว่าความต้องการบุคลากรด้านไซเบอร์ ในระดับโลกนั้นมีมากกว่าขีดความสามารถในการผลิตถึงจำนวนสองล้านคนในปี ค.ศ.2017 และได้นำเสนอ Cybersecurity Rapid Education Apprenticeship Training to Employment System (CREATES) เพื่อที่จะพยายามแก้ไขปัญหาการขาดแคลนบุคลากรด้านไซเบอร์ Morgan และพวกได้ทำการวิจัยข้อมูล ณ CIAC (Center for Information Assurance Cybersecurity) ที่มหาวิทยาลัยวอชิงตัน ร่วมกับมหาวิทยาลัยฮาวาย เพื่อพัฒนาหลักสูตร Information Assurance (IA) ตั้งแต่ปี ค.ศ. 2007 เขาได้ผลิตบุคลากรด้านไซเบอร์โดยเฉพาะเรื่อง IA ได้ดังนี้

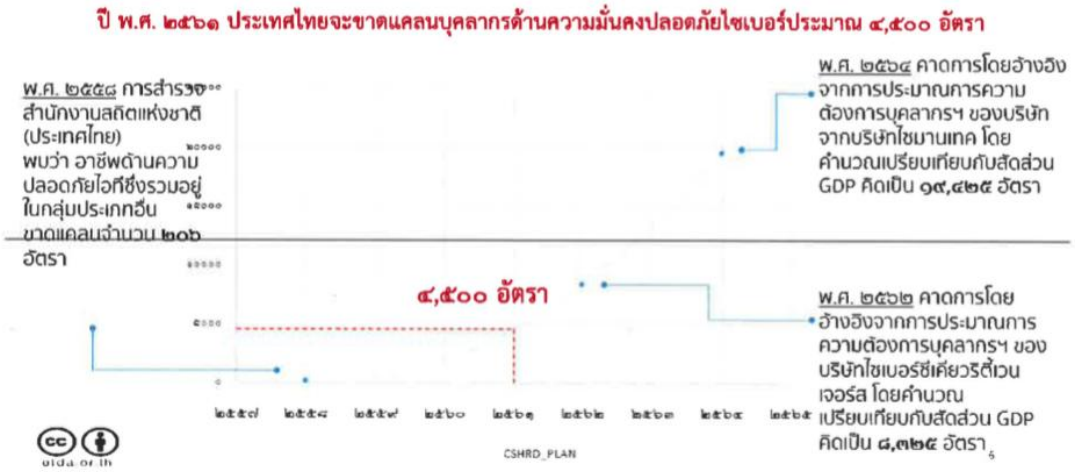
1. ผู้ที่ผ่านการสอบประกาศนียบัตร IA จำนวน 107 คน
2. ปริญญาโทสาขา Information Management เอก IA จำนวน 40 คน
3. ปริญญาโทสาขา Library and Information Science เอก IA จำนวน 4 คน
4. ปริญญาโทสาขา Strategic Planning in Critical Infrastructure จำนวน 76 คน
5. ปริญญาโทสาขา Cybersecurity and Leadership จำนวน 26 คน

6. ปริญญาเอกในทุกสาขาที่มีวิชาเอก IA จำนวน 8 คน

ผู้เขียนได้ได้กล่าวถึงแนวทางการแก้ปัญหานี้ด้วยโมเดล CREATES ซึ่งได้ชี้ให้เห็นว่า กองทัพมีกำลังพลที่เป็นผู้เกษียณอายุราชการ นอกประจำการ ทหารกองหนุน กองเกิน ที่รับการศึกษาที่มีพื้นฐานที่พร้อมต่อการนำมาต่อยอดและมีการฝึกใช้งานและมีประสบการณ์มาเป็นอย่างดี มีความเป็นไปได้สูงที่จะนำมาเข้าหลักสูตรการอบรมให้สามารถทำงานปฏิบัติการด้านไซเบอร์ได้เป็นอย่างดี โมเดลที่นำเสนอนี้นอกจากจะสามารถร่นระยะเวลาในการพัฒนาบุคลากรด้านไซเบอร์ให้มีความกระชับมากขึ้นแล้ว ในเชิงปริมาณยังสามารถทำให้ผลิตบุคลากรด้านไซเบอร์ให้สามารถปฏิบัติงานด้าน IA ได้อย่างมีประสิทธิและมีความเพียงพอในอนาคต หลักสูตร CREATS ที่ผู้เขียนได้นำเสนอเป็นการสร้างสายการผลิตบุคลากรในระดับประกาศนียบัตร หลักสูตรสองปี หลักสูตรปริญญาตรี ปริญญาโท และปริญญาเอก โดยมุ่งเน้นกำลังพลที่จะถ่ายโอนมาจากกระทรวงกลาโหม โดยผู้ที่ผ่านหลักสูตรในโมเดลที่นำเสนอจะสามารถปฏิบัติงานด้านไซเบอร์ได้ทั้งในภาครัฐและเอกชน ทั้งนี้บริษัทเอกชนขนาดใหญ่เช่น Amazon, Microsoft และ Google ต่างให้ค่าตอบแทนสำหรับบุคลากรด้านไซเบอร์ที่มีศักยภาพสูงทั้งในสหรัฐอเมริกาและจากทุกประเทศทั่วโลก ในอีกมุมมองหนึ่งโครงการนี้ยังช่วยส่งเสริมมูลค่าของการประกอบวิชาชีพด้านไซเบอร์ให้มีค่าตอบแทนที่เหมาะสม

บทความ “ปัญหาการขาดแคลนมืออาชีพด้านความปลอดภัยไซเบอร์” (ไม่ปรากฏนามผู้เขียน, CIO World & Business, 6 กันยายน 2559) กล่าวถึงปัญหาความขาดแคลนบุคลากรด้านไซเบอร์ไว้ว่า การลงทุนด้านความปลอดภัยของระบบเทคโนโลยีสารเทศนั้น 1 ใน 3 ของงบลงทุนด้านนี้ต้องจ่ายให้กับการพัฒนาศักยภาพของผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ ซึ่งหน่วยงานใหญ่ ๆ ที่มีความต้องการผู้เชี่ยวชาญด้านไซเบอร์ เช่น แคสเปอร์สกี้ นั้นความท้าทายมิได้จำกัดแต่เพียงความรู้ความสามารถเชิงเทคนิคเท่านั้น “ความจำเป็นสำหรับผู้จัดการด้านระบบความปลอดภัยนั้นต้องอาศัยคุณสมบัติที่สูงกว่า เพราะนอกจากความรู้ทางด้านเทคนิคแล้ว หน้าที่ความรับผิดชอบของผู้จัดการยังต้องสื่อสารกับระดับบริหารและดูแลแผนกลยุทธ์โดยรวมอีกด้วย” ภาพที่ 2 แสดงให้เห็นถึงความต้องการเพิ่มจำนวนผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ในกลุ่มอุตสาหกรรมต่าง ๆ เช่น ที่พักอาศัย, กระทรวงกลาโหม, อี-คอมเมิร์ซ, การพยาบาล/ท่องเที่ยว,บริการทางการเงิน, และ ไอที/เทเลคอม ซึ่งในบทความดังกล่าวได้แสดงให้เห็นว่า ในฐานะของบริษัทขนาดใหญ่ที่ทำอุตสาหกรรมด้านความปลอดภัยไซเบอร์ มีความจำเป็นอย่างยิ่งที่จะต้องพัฒนาบุคลากรในระดับผู้เชี่ยวชาญขึ้นอีกเป็นจำนวนมากเพื่อเพิ่มความมั่นใจให้กับการบริการของเขา และได้พัฒนาหลักสูตร “IT Security Fundamentals” เพื่อสร้างบุคลากรด้านไอทีที่มีความเป็นมืออาชีพมากขึ้น

แผนภาพที่ 2-2 ประมาณการความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างปี พ.ศ. 2558-2564



ในเอกสารข่าวประชาสัมพันธ์ของการประชุมเป็นบทความออนไลน์เรื่อง “ประชุมโต๊ะกลม ACIOA ย้ำการขาดแคลนคนสาย Cybersecurity เป็นความเสี่ยงระดับประเทศ” เมื่อ 8 เมษายน 2560 การจัดประชุมโต๊ะกลม ACIOA (ASEAN CIO Association) เรื่อง “Shortage of Qualify Thai Cyber Security for the Next 5-10 years” ซึ่งจัดขึ้นเพื่อการพบปะหารือร่วมกันระหว่างผู้ทรงคุณวุฒิจากมหาวิทยาลัยต่าง ๆ ของประเทศไทยที่เปิดหลักสูตร ICT Security องค์กรด้านการพัฒนาการศึกษา Cybersecurity ผู้บริหารด้านสารสนเทศ ผู้แทนจากกลุ่มวิสาหกิจหน่วยงานความมั่นคง กลุ่มธุรกิจทางการเงินการธนาคาร กลุ่มอุตสาหกรรม แพทย์ และกลุ่มอื่น ๆ ที่เกี่ยวข้องโดยตรงให้ทราบถึงทิศทางและเทคโนโลยีด้านความปลอดภัยไซเบอร์ที่กำลังเปลี่ยนแปลงภายใต้โมเดล Thailand 4.0 เพื่อสร้างบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ให้สามารถรองรับทิศทางเทคโนโลยีที่เปลี่ยนแปลงไป และทำให้ตัวชี้วัดด้าน Cybersecurity ที่มีผลต่อการจัดอันดับ e-Government ของประเทศไทยในระดับนานาชาติให้ดีขึ้น โดยสรุป การขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เป็นความเสี่ยงระดับประเทศ ซึ่งทั้งภาครัฐ ภาคเอกชน และภาคการป้องกันประเทศ หน่วยงานหลายภาคส่วนควรร่วมกันผลักดันเป็นวาระแห่งชาติ ในบริบทของ National Cybersecurity ทั้งในเชิงรุกและเชิงรับ เพื่อสนับสนุนการวางแผนระดับประเทศระยะกลาง ระยะยาว ในการสร้างผู้เชี่ยวชาญด้านไซเบอร์ซึ่งรวมถึงการสร้างความเข้าใจ ความตระหนักด้านความมั่นคงปลอดภัยภาคสาธารณะ ทั้งด้านการวิจัย และด้านหลักสูตรการเรียนการสอน

หนึ่งในอุปสรรคสำคัญของวงการการรักษาความมั่นคงปลอดภัยไซเบอร์คือความไม่เพียงพอของผู้เชี่ยวชาญการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อปริมาณความต้องการของตลาดแรงงาน (“ความต้องการบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้นอย่ามหาศาล แต่การพัฒนาคนยังทำได้ไม่ทัน”, ข่าวสั้น, Cybrary, Security Week, 24 มกราคม 2560) บริษัท Cybersecurity Ventures ได้ทำการสำรวจและประเมินว่าในปี พ.ศ.2563 มูลค่าการจ้างงาน

บุคลากรด้านไซเบอร์ในตลาดแรงงานทั่วโลกจะเพิ่มสูงถึง 1.7 พันล้านเหรียญสหรัฐ สาเหตุมาจากการที่หน่วยงานต่าง ๆ เริ่มตระหนักถึงความเสียหายจากการโจมตีทางไซเบอร์และจำเป็นต้องมีบุคลากรที่เชี่ยวชาญมาช่วยในการป้องกัน โดยในช่วงปี พ.ศ.2557-2559 มูลค่าเฉลี่ยความเสียหายต่อการถูกโจมตีแต่ละครั้งสูงถึง 7 ล้านเหรียญสหรัฐ และข้อมูลจากเว็บไซต์ Indeed.com สำหรับประกาศหางานพบว่าประเทศที่มีความต้องการบุคลากรด้านนี้มากที่สุดคือ ประเทศอิสราเอล รองลงมาคือประเทศไอร์แลนด์ สหราชอาณาจักร และสหรัฐอเมริกา และประเทศในแถบเอเชียแปซิฟิก เช่น ญี่ปุ่น มาเลเซีย และสิงค์โปร์ ได้เริ่มตระหนักถึงความสำคัญของปัญหาการขาดแคลนบุคลากรดานไซเบอร์ และได้มีโครงการสนับสนุนการพัฒนาบุคลากรด้วยมาตรการต่าง ๆ ทั้งการพยายามเพิ่มหลักสูตรการศึกษา และการพัฒนาทักษะบุคลากรให้มีความเชี่ยวชาญมากขึ้น สำหรับประเทศไทย ปัจจุบันได้มีหลายหน่วยงานพยายามผลักดันการพัฒนาบุคลากรในด้านนี้ เช่น ได้เริ่มมีการเปิดสอนวิชาด้านความมั่นคงปลอดภัยไซเบอร์ในมหาวิทยาลัยในระดับปริญญาตรี อีกทั้งมีการเปิดให้บุคคลทั่วไปเข้ารับการอบรมและสอบใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์โดยไม่เสียค่าใช้จ่าย เช่น โครงการ iSEC (https://isec.tisa.or.th) เป็นต้น

แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ (น.อ.ประยูร ธรรมาธิวัฒน์, 2558, 63-70) กำหนดแนวทางการพัฒนาขีดความสามารถของบุคลากรภายใต้ปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ให้มีการเตรียมความพร้อมต่อปฏิบัติการสงครามไซเบอร์อย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกทางไซเบอร์เพื่อเสริมสร้างทักษะในการปฏิบัติงานเพื่อให้มีความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ มีความยั่งยืนและสามารถพึ่งพาตนเองได้ โดยได้ให้ขอเสนอแนะพอสรุปได้คือ ด้านกำลังพล ด้านการบริหารจัดการ ด้านเทคโนโลยี และด้านงบประมาณ โดยในส่วนของกำลังพลจัดให้มีการฝึกอบรมด้านไซเบอร์ให้มีความรู้ในระดับสากล มีการฝึกปฏิบัติจริงด้านสงครามไซเบอร์และปลูกฝังให้มีภาวะผู้นำในทุกระดับ จัดให้มีการฝึกร่วมระหว่างหน่วยงานทั้งภายในและภายนอกกองทัพอากาศ การสร้างความตระหนัก การพิจารณาเพิ่มค่าตอบแทนพิเศษให้กับผู้ที่ปฏิบัติงานด้านสงครามไซเบอร์ กำหนดเส้นทางการเจริญเติบโตที่ชัดเจน มีหลักสูตรการเรียนการสอนในสายวิทยาการ การเพิ่มพูนความรู้ให้กับหน่วยที่เกี่ยวข้องอย่างต่อเนื่อง กำหนดคุณสมบัติการรับสมัครกำลังพลใหม่ กำหนดแนวทางการคัดเลือกบุคลากรที่มีความรู้ความสามารถด้านไซเบอร์เพื่อสร้างนักรบไซเบอร์ของกองทัพอากาศ โดยในส่วนของการบริหารจัดการมีประเด็นพอสรุปได้คือ การปรับปรุงหลักนิยมของกองทัพอากาศ กำหนดให้มีหลักการและแนวทางการปฏิบัติด้านสงครามไซเบอร์ ปรับปรุงแผนยุทธศาสตร์ของกองทัพอากาศให้มีเป้าหมายหลักและเป้าหมายรองที่ชัดเจน จัดทำแผนแม่บทด้านสงครามไซเบอร์ ปรับปรุงโครงสร้างหน่วย ทั้งฝ่ายอำนวยการและหน่วยปฏิบัติให้มีหน่วยงานรองรับ มีการปรับปรุงข้อมูลต่าง ๆ อยู่อย่างสม่ำเสมอ มีมาตรการเตรียมความพร้อมเพื่อรับมือการโจมตีทางไซเบอร์ แสงหาความร่วมมือกับชาติอื่น ๆ ในภูมิภาคอาเซียนและในระดับโลก นำกระบวนการบริหารงานให้มีคุณภาพของ Deming Circle มาใช้ประกอบการบริหารจัดการ นำกระบวนการบริหารความเสี่ยงมาใช้ในการบริหารจัดการเพื่อให้ได้ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด การปกป้องความลับ การคงสภาพ และความพร้อมใช้งานเพื่อให้สามารถทำงานและบริการได้ตามปกติ กำหนดให้หน่วยจัดทำแผนบริหารความเสี่ยง นำระบบสมรรถนะมาใช้ในการพัฒนาองค์กร ใช้กระบวนการจัดการความรู้ การถ่ายโอนความรู้อย่างมี

ระบบ กำหนดหลักเกณฑ์และแนวทางในการวัดขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ จัดให้มีระบบจำลองยุทธด้านไซเบอร์ จัดให้ผู้บริหารระดับสูงของหน่วยทุกระดับมีความรู้ความเข้าใจปฏิบัติการสงครามไซเบอร์ เพื่อให้มีการสนับสนุนในทุกมิติอย่างจริงจัง ในด้านเทคโนโลยี ผู้เขียนเสนอแนะให้จัดหาเครื่องมือที่ทันสมัยให้กับหน่วยอย่างพอเพียง นำหลักการที่เป็นมาตรฐานสากลมาช่วยเป็นมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ จัดให้มีระบบแจ้งเตือนภัยไปยังหน่วยและผู้ที่เกี่ยวข้องเมื่อถูกโจมตี พิจารณาจัดหาอาวุธไซเบอร์ที่ทันสมัยและปรับปรุงอาวุธให้ทันสมัยก้าวทันเทคโนโลยีที่เปลี่ยนไปอยู่เสมอ ในด้านงบประมาณ ให้ความสำคัญกับภารกิจด้านสงครามไซเบอร์ ด้วยการสนับสนุนงบประมาณให้พอเพียง สำหรับการใช้โปรแกรมที่ถูกกฎหมายแทนการใช้ซอฟท์แวร์เถื่อน นอกจากนั้นยังเสนอแนะให้พัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ให้เพียงพอต่อความต้องการของกองทัพอากาศ และกำหนดตำแหน่งและมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ มีการวิจัยเชิงนวัตกรรมด้านเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การตระหนักรู้ของกำลังพลถึงภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์และสงครามไซเบอร์ และมีการประเมินความเสี่ยงของหน่วยว่าอยู่ในระดับที่มีความเสี่ยงต่อการโจมตีอย่างไรเพื่อให้สามารถปรับตัวให้มีความพร้อมในการรับมือกับการโจมตีทางไซเบอร์

ยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ

เพื่อให้เกิดความเข้าใจในพัฒนาการของการรับมือภัยคุกคามด้านไซเบอร์ผู้วิจัยได้ทำการสำรวจยุทธศาสตร์ไซเบอร์ของแต่ละชาติ ซึ่งมักมีการกำหนดแนวนโยบายในการพัฒนาบุคลกรด้านไซเบอร์ประกอบด้วยและเปรียบเทียบเนื้อหาของแนวนโยบายที่กำหนดไว้ในยุทธศาสตร์ไซเบอร์ว่าแต่ละประเทศมีการเตรียมการรับมือกับภัยคุกคามด้านไซเบอร์ไปในลักษณะใด ตารางที่ 2 แสดงผลการเปรียบเทียบยุทธศาสตร์ไซเบอร์ของประเทศต่าง ๆ จำนวน 22 ประเทศ โดยแบ่งปัจจัยพิจารณาเป็นการเน้นการป้องกัน CI และ CII รวมถึงระบบ IT ของรัฐบาล ความปลอดภัยออนไลน์ การพัฒนาศักยภาพ และเรื่องอื่น ๆ ที่แต่ละประเทศกำหนดไม่เหมือนกัน รวมถึงหน่วยงานที่ทำหน้าที่เป็นหน่วยงานไซเบอร์ระดับชาติ

ตารางที่ 2-3 เปรียบเทียบยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ (ต่อ)				
ประเทศ (SO)/ค.ศ.	*CI, CII, Gov.System*	*ความปลอดภัยออนไลน์*	*พัฒนาศักยภาพ*	*อื่น ๆ/National Cyber Unit*
แคนาดา (3)/2018	ปกป้อง Critical Systems, ให้รัฐเป็นผู้นำด้านไซเบอร์	ปกป้องภัยจากอาชญากรรมไซเบอร์	สนับสนุนงานวิจัยขั้นก้าวหน้า, นวัตกรรมดิจิตอล, สร้าง cyber skills	ความร่วมมือกับมิตรประเทศ
เยอรมัน (11)/2011	ปกป้อง CII, ระบบ IT	ควบคุมอาชญากรรมไซเบอร์, ใช้ระบบ IT ที่เชื่อถือได้ (Trust)	เพิ่มมาตรการการรักษาความปลอดภัยไซเบอร์ในสาธารณะ, พัฒนาบุคลากรไซเบอร์	ตั้งหน่วย Cyber Response Centre, ตั้งคณะกรรมการไซเบอร์ชาติ, ประสานงานกับนานาชาติ, สนับสนุนเครื่องมือในการรักษาความปลอดภัยไซเบอร์
ฝรั่งเศส (5)/2015	ปกป้อง CI, ระบบ IT ของรัฐ	ความเชื่อถือได้, ข้อมูลส่วนบุคคล	พัฒนาบุคลากร, สนับสนุนเทคโนโลยีธุรกิจดิจิตัล	สร้างความตระหนัก, เสริมสร้างเสถียรภาพไซเบอร์ของชาติ และร่วมมือกับนานาชาติ ช่วยเหลือประเทศอื่นๆ
อิตาลี (6)/2013	ปกป้อง CI, เป้าหมายทางยุทธศาสตร์ไซเบอร์	ปกป้องทรัพย์สินทางปัญญา, นวัตกรรม ของทั้งภาครัฐ/เอกชน, เฝ้าระวังอาชญากรรมไซเบอร์	เพิ่มศักยภาพในการป้องกัน	สร้างความตระหนักในภัยไซเบอร์, สร้างความร่วมมือกับมิตรประเทศ
โครเอเชีย (8)/2015	-	เพิ่มความปลอดภัย/เชื่อถือได้ในการใช้ไซเบอร์เสปซ	พัฒนาระบบการศึกษาด้านไซเบอร์, เพิ่มความเชื่อมั่นในระบบ e-services	พัฒนากรอบแนวคิดกฎหมายไซเบอร์, ยกระดับการสร้างความตระหนัก, สนับสนุนการวิจัย/พัฒนาด้านไซเบอร์, พัฒนา/เสริมสร้างระบบ information sharing
เบลเยี่ยม (4)(*มีแต่	-	เพิ่มความเชื่อมั่นในการใช้	พัฒนาศักยภาพเพื่อสนับสนุน	สนับสนุนงานด้านไซเบอร์แก่องค์กรอื่น ๆ ของรัฐ,

ตารางที่ 2-3 เปรียบเทียบยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ (ต่อ)				
ประเทศ (SO)/ค.ศ.	*CI, CII, Gov.System*	*ความปลอดภัยออนไลน์*	*พัฒนาศักยภาพ*	*อื่น ๆ/National Cyber Unit*
ยุทธศาสตร์ไซเบอร์ กห.)/2014		ระบบ	ปฏิบัติการทางทหาร	ประสานความร่วมมือกับมิตรประเทศ
ลัทเวีย (5)/2014	ปกป้อง CI, IT ของรัฐ	การสร้างความตระหนัก	พัฒนาบุคลากรไซเบอร์	การจัดการวิกฤต, ความร่วมมือกับมิตรประเทศ
เนเธอแลนด์ (5)/2013	ปกป้อง CI, IT ของรัฐและอื่น ๆ ที่สำคัญ, Resilience	จัดการกับอาชญากรรมไซเบอร์, ปกป้องข้อมูลส่วนบุคคล	ลงทุนในการพัฒนา ICT ที่ปลอดภัย, มีบุคลากรที่เพียงพอ	แสวงหาความร่วมมือกับมิตรประเทศในดิจิตัลโดเมน, ลงทุนในนวัตกรรมไซเบอร์
นอรเวย์ (7)/2012	ทุกองค์กร(รัฐ/เอกชน) ต้องมี ISMS*, ปกป้อง CI	รักษาความปลอดภัยของ online service ของ public administration, ใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ/ปลอดภัย, เฝ้าระวังการโจมตีของอาชญากรไซเบอร์	ระบบ ICT Infrastructure ต้องมีความเชื่อถือได้, ปลอดภัย และมีการเฝ้าระวังอย่างเข้มงวด, มีขีดความสามารถในการเฝ้าระวังการโจมตีระบบ ICT	สร้างความตระหนัก, ยกระดับขีดความสามารถของบุคลากร, มีงานวิจัย/นวัตกรรมไซเบอร์ที่มีคุณภาพสูง
โปแลนด์ (7)/2013	เพิ่มระดับการป้องกัน ICT Infrastructure, ป้องกัน/ต่อสู้กับภัยคุกคามไซเบอร์	สร้างความตระหนัก	ประเมินขีดความสามารถของการรักษาความปลอดภัยไซเบอร์, สร้างและจัดทำระบบบริหารจัดการรวมศูนย์	ลดระดับผลกระทบต่อการโจมตี ICT, กำหนดแนวทางให้กับภาคเอกชน, สร้างระบบบริหารจัดการความร่วมมือระหว่างองค์กร
โปรตุเกส (6)/2013	ให้ความสำคัญ CI โดยให้ CNCS* รับผิดชอบ, ป้องกันไซเบอร์สเปซ, รับประกันและ	ทบทวนกฎหมาย, เพิ่มขีดความสามารถของตำรวจปราบปราอาชญากรรมไซเบอร์,	บูรณาการปฏิบัติระหว่างยุทธศาสตร์ทหารกับ CNCS, กำหนด process	CNCS, พูดถึงการปฏิบัติทางทหารในไซเบอร์สเปซ, การแชร์ข้อมูล, จัดตั้ง CSIRT, หน่วยงานบริหารจัดการวิกฤตไซเบอร์, การวิจัยและพัฒนาด้านไซ

ตารางที่ 2-3 เปรียบเทียบยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ (ต่อ)				
ประเทศ (SO)/ค.ศ.	*CI, CII, Gov.System*	*ความปลอดภัยออนไลน์*	*พัฒนาศักยภาพ*	*อื่น ๆ/National Cyber Unit*
	ป้องกัน CII ด้วยระบบ SPIIN*	สร้างความตระหนัก, เน้นการป้องกัน		เบอร์, แสวงหาความร่วมมือ
สหรัฐ (3)/2003	ป้องกันการโจมตี CI, ระบบ ICT ของรัฐ	การสร้างความตระหนัก	ลดช่องโหว่ในการโจมตี, ระบบการตอบสนองต่อการโจมตี, การพัฒนาบุคลากร	ลดเวลาในการฟื้นฟู ลดความเสียหายจากการโจมตี, โปรแกรมลดช่องโหว่, ความร่วมมือในระดับนานาชาติ
ตุรกี (5)/2016	ปกป้อง CI, กำหนด CI, ให้ผ่านมาตรการที่กำหนด, มีบอร์ดกำกับดูแล CI	การสร้างความตระหนัก, privacy, confidentiality	ยกระดับการป้องกันด้านไซเบอร์, การพัฒนาบุคลากรไซเบอร์	บูรณาการ Cybersecurity เข้ากับ National Security, Risk Management, ออกกฎหมายเพื่อให้สอดคล้องกับหลักสากล, และมาตรฐาน
สหราชอาณาจักร (3)/2016	Active Defense, ปกป้อง CI, ระบบของรัฐ	ทำให้อินเทอร์เน็ตปลอดภัย, ลดอาชญากรรมไซเบอร์, ป้องกัน terrorism	ทำความเข้าใจ threats, **ตอบโต้การโจมตี, Sovereign (offensive, cryptography), CS skills, การแสกนไซเบอร์สเปซ	(Defend/Deter/Develop), บริหารจัดการ incidents, ยกระดับวิทยาการไซเบอร์และเทคโนโลยี, ความร่วมมือระหว่างประเทศ, จัดตั้ง NCSC (National Cyber Security Centre
รัสเซีย (3)/2016 (ปรับปรุงจาก 2000)	ลดผลกระทบทางลบจากการใช้ระบบ IT, CII (ไม่พูดถึง CI เลย)	เพิ่มประมาณการใช้/ระดับความปลอดภัยให้กับระบบ IT	ยกระดับ IT security	กล่าวแยก action plans ด้าน Economy, ยุทธศาสตร์, การศึกษา
ออสเตรเลีย (5)/2016	ระบบป้องกันที่แข็งแกร่งและฟื้นตัวได้รวดเร็ว, ป้องกัน CI	ส่งเสริมการใช้งานอย่างปลอดภัย/ฟรี/เสรีในไซเบอร์สเปซ, สร้างความตระหนัก	นวัตกรรมไซเบอร์ผ่านภาคธุรกิจ, ความเป็นประเทศที่ใช้ไซเบอร์อย่างชาญฉลาด	ความร่วมมือระดับชาติ (รัฐบาล/เอกชน/การศึกษาวิจัย) ทำ Cyber Initiatives
จีน (9)/2016	ป้องกันอธิปไตยไซเบอร์อย่างเฉียบขาด, ความมั่นของของ	ยกระดับความเข้มแข็งของวัฒนธรรมออนไลน์, จัดการ	ใช้นวัตกรรมขับเคลื่อนการพัฒนาเทคโนโลยีด้าน CS, ยกระดับ	ส่งเสริมงานวิจัยด้านไซเบอร์, talent projects, เสริมสร้างการให้ความร่วมมือกับมิตรประเทศ

ตารางที่ 2-3 เปรียบเทียบยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ (ต่อ)				
ประเทศ (SO)/ค.ศ.	*CI, CII, Gov.System*	*ความปลอดภัยออนไลน์*	*พัฒนาศักยภาพ*	*อื่น ๆ/National Cyber Unit*
	รัฐ, CII, ทำระบบ network - องรัฐบาลให้สมบูรณ์ด้วยการบังคับใช้กฎหมาย	กับการก่อการร้ายและอาชญากรรมไซเบอร์	ความสามารถในการป้องกันไซเบอร์สเปซ, สร้าง protection forces	
อิสราเอล ()/ 2011[30],2016[31]	ยุทธศาสตร์ Defense & Deterrence, Attack*, ปกป้อง essential services, ระบบของรัฐ	ป้องกันอาชญากรรมไซเบอร์	ยกระดับความสามารถในการป้องกัน และการวิจัยพัฒนา, ปฏิบัติการเชิงรุก, การพัฒนาบุคลากร	ตั้งหน่วยงาน National Cyber Bureau ขึ้นกับสำนักนายกฯ รับผิดชอบงานด้านไซเบอร์, National Cyber Defense Authority
มาเลเซีย ()/2006[32]	ปกป้อง CNII และ CI	Culture of Security, สร้างความตระหนัก	พัฒนาโปรแกรม/framework สนับสนุนนโยบาย, สนับสนุนการวิจัยด้านไซเบอร์	ประเมินความเสี่ยงของ CNII, ความร่วมมือกับมิตรประเทศ, นโยบายการเข้ารหัส
สิงค์โปร์ (4)/2016	Resilience of CII (protection program), Recovery plan	สร้างความปลอดภัยให้ไซเบอร์สเปซ, National Cybercrime Action Plan	พัฒนา Cybersecurity Ecosystem, สนับสนุนงานวิจัย, startup	NCIRT (National Cyber Incident Response Team), NCSC (National Cyber Security Centre), NCA (National Cyber Agency), ความร่วมมือกับมิตรประเทศ
ญี่ปุ่น (4)/2015	มาตรการป้องกัน CI, สร้างความปลอดภัยให้ระบบ IoT, การบริหารองค์กร, สภาวะ	สร้างสังคมไซเบอร์ให้ประชาชนมีความปลอดภัย, เพิ่มมาตรการป้องกัน,	สร้างความก้าวหน้าให้กับงานวิจัย/พัฒนา, สร้างกำลังพลด้านไซเบอร์ให้เพียงพอและมี	สร้างสันติภาพและเสถียรภาพของประชาคมนานาชาติ และความมั่นคงของชาติ, ความร่วมมือกับมิตรประเทศ

[30] "Advancing National Cyberspace Capabilities, Resolution No.3611 of the Governmnet August 7, 2011
[31] Guidelines for National Cyber Strategy, INSS (Institute for National Security Studies, 2016
[32] MALAYSIA'S NATIONAL CYBER SECURITY POLICY 2006

ตารางที่ 2-3 เปรียบเทียบยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ (ต่อ)				
ประเทศ (SO)/ค.ศ.	*CI, CII, Gov.System*	*ความปลอดภัยออนไลน์*	*พัฒนาศักยภาพ*	*อื่น ๆ/National Cyber Unit*
	แวดล้อมของภาคธุรกิจ	ปรับปรุง Scio-Economic Vitality	ประสิทธิภาพและการพัฒนาที่ยั่งยืน	
ไทย (8)/2017[33]	ปกป้อง CII, ผลประโยชน์/ความมั่นคงของชาติ, ความร่วมมือภายในประเทศ	ความเชื่อมั่น/ไว้วางใจในกิจกรรมไซเบอร์, สร้างความตระหนัก, วัฒนธรรมการใช้ไซเบอร์สเปซที่เหมาะสม, ป้องกัน/ปราบปรามอาชญากรรมไซเบอร์	พัฒนาศักยภาพด้านการรับมือภัยคุกคามไซเบอร์, เสริมสร้างเศรษฐกิจดิจิตอล	ส่งเสริมบทบาทที่สร้างสรรค์ในความร่วมมือด้านไซเบอร์ในระดับภูมิภาคและนานาชาติ

(หมายเหตุ ** SO = Strategic Objectives, ISMS = Information Security Management System, CNCS=National Centre for Cybersecurity, SPIIN=National Information Infrastructure Protection System, CS=Cybersecurity, CNII=Critical National Information Infrastructure)

ที่มา: https://ccdcoe.org/cyber-security-strategy-documents.html

[33] ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ๒๕๖๐-๒๕๖๔

นอกจากข้อมูลที่สำคัญในตารางที่ 3 ในภาพรวม EU ได้เผยแพร่เอกสาร Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) เพื่อให้เป็นแนวทางในการจัดทำ Cybersecurity Strategy ของประเทศสมาชิก และในส่วนของสหราชอาณาจักรที่มียุทธศาสตร์ไซเบอร์ฉบับปรับปรุงจากปี 2011 มีประเด็นที่สำคัญและทำให้ผู้รับนโยบายสามารถเข้าใจได้ง่ายโดยแบ่งออกเป็น 3 ส่วนคือ

1. Defend – ปกป้องเครือข่าย ข้อมูล และระบบ รวมถึงแผน Resilience และ รัฐ/เอกชน, ประชาชนรู้จักการป้องกันตนเองจากภัยคุกคามไซเบอร์

2. Deter – มีความแข็งแกร่งในการตกเป็นเป้าหมายการโจมตี ทำการตรวจสอบ เข้าใจ สืบสวน และหยุดการกระทำ และการลงโทษผู้กระทำผิด และจะทำการเชิงรุกเมื่อจำเป็น

3. Develop - มีนวัตกรรม, พัฒนาอุตสาหกรรมไซเบอร์, งานวิจัยและพัฒนา มีบุคลากรที่เพียงพอ

โดยเป้าหมายทั้งหมดนี้จะกระทำการร่วมมือกับมิตรประเทศ ให้เกิดการพัฒนาเชิงเศรษฐกิจ และความปลอดภัยในมิติไซเบอร์โดยยึดถือผลประโยชน์ของชาติเป็นหลัก ซึ่งล้วนเป็นหัวใจสำคัญของยุทธศาสตร์ไซเบอร์ของหลาย ๆ ประเทศ

กรอบความคิดทางการวิจัย (Conceptual Model)

แนวทางการพัฒนากำลังพลด้านไซเบอร์ที่จะทำการวิจัยมีพื้นฐานแนวความคิดจากปัญหาต่าง ๆ แนวคิด ทฤษฎี และจากการทบทวนวรรณกรรมที่เกี่ยวข้องมา ดังนั้นสมมติฐานการพัฒนากำลังพลไซเบอร์จึงเกี่ยวข้องกันในหลายมิติดังต่อไปนี้

1. การพัฒนากำลังพลไซเบอร์ตามแนวทางปกติ ตามวงรอบการฝึก การอบรมในหลักสูตรต่าง ๆ

2. กำลังพลสำรองไซเบอร์สามารถพัฒนาขึ้นได้จากการเกณฑ์ทหารเพื่อคัดเลือกบุคคลที่จะสามารถทำงานในหน่วยไซเบอร์ในห้วงเวลา ๒ ปีของการเข้าประจำการ และยังเป็นโอกาสให้สามารถบรรจุบุคลากรที่มีขีดความสามารถเหมาะสมเข้าปฏิบัติงานในหน่วยไซเบอร์ได้อย่างเพียงพอ ซึ่งอาจต้องมีการแก้ไข พ.ร.บ. ที่เกี่ยวข้อง และต้องมีการอนุโลมในการฝึกทางทหารให้มีปริมาณลดน้อยลงให้เหมาะสมกับการทำงานในหน่วยไซเบอร์

3. แนวความคิดกำลังพลไซเบอร์ภายนอกหมุนเวียน เข้าประจำการเป็นห้วงเวลาที่เหมาะสมและหลังจากนั้นสามารถไปทำงานตามองค์กร บริษัท ได้ตามปกติ เช่น ในวงรอบ 1 ปีอาจทำงานที่บริษัทเอกชน เช่น Googleหรือ Microsoft เป็นเวลา 9 เดือนและอีก 3 เดือนมาปฏิบัติหน้าที่ทหารประจำการหน่วยไซเบอร์เป็นเวลา 3 เดือน ซึ่งรัฐต้องมีภาระในการบริหารจัดการเวลาให้สามารถมีความต่อเนื่อง และอาจต้องแก้ไขกฎหมายยกเว้นที่เกี่ยวข้อง

4. การสร้างกองกำลังไซเบอร์เฉพาะกิจจากบุคคลภายนอก

สรุป

สรุปแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องกับการพัฒนาบุคลากรด้านไซเบอร์ ได้ว่า การใช้เทคโนโลยีแต่เพียงอย่างเดียวไม่สามารถแก้ไขปัญหาการเตรียมการรับภัยคุกคามด้านไซเบอร์ แต่ต้องการบุคลากรที่มีคุณภาพสูง สามารถปฏิบัติงานในไซเบอร์สเปซได้อย่างมีประสิทธิภาพ และมีความประสานสอดคล้องกับการรักษาความมั่นคงของชาติในภาพรวม ทั้งนี้ในระดับชาติได้มีการกำหนดชัดเจนว่าปัญหาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ไม่เพียงพอ (แผนปฏิบัติการเพื่อรองรับยุทธศาสตร์เพื่อความมั่นคง 2560-2564 ข้อ 2.2.4) บุคลากรด้านไซเบอร์เป็นกลุ่มบุคคลที่มีความสำคัญมากต่อการดำรงสภาพของระบบเทคโนโลยีสารสนเทศ โดยเฉพาะภาครัฐยังประสบปัญหาการขาดแคลนบุคลากรอีกเป็นจำนวนมาก ซึ่งอาจเกิดจากแรงจูงใจในค่าตอบแทนหรือขาดแคลนเจ้าหน้าที่ที่เข้าใจปัญหาการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง และเกิดจากความยากของเนื้อหาและความสลับซับซ้อนของปัญหาที่ทำให้เป็นอุปสรรคต่อบุคคลทั่วไปที่มีความรู้พื้นฐานเพียงแค่ทำงานในระบบสารสนเทศให้เข้าใจและสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ ในการพัฒนาบุคลากรโดยการสร้างแรงจูงใจจากค่าตอบแทนพิเศษที่จะได้รับเพิ่มจากการมีประกาศนียบัตรใบรับรองต่าง ๆ ในแต่ละบุคคลจึงถือเป็นเรื่องสำคัญในแผนการปฏิบัติระดับชาติ ซึ่งจะต้องมีการดำเนินการอย่างเร่งด่วน โดยเริ่มจากการกำหนดหลักสูตรในสถานศึกษา และสถานฝึกอบรมตามมาตรฐานสากล เพื่อรองรับการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นตามความก้าวหน้าของเทคโนโลยีและการขยายตัวของการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยแบบผสมผสานซึ่งประกอบด้วยการวิจัยเชิงคุณภาพ และการวิจัยเชิงปริมาณ เพื่อค้นหาแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศให้มีความยั่งยืน บุคลากรด้านไซเบอร์มีประสิทธิภาพพร้อมรับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงและถูกยกระดับให้กลายเป็นพลังอำนาจแห่งชาติ ข้อมูลที่ใช้ในการวิจัยนำมาจากการศึกษาวรรณกรรมที่เกี่ยวข้อง จากการสัมภาษณ์เชิงลึก การสนทนาในกลุ่มเฉพาะ และข้อมูลจากแบบสอบถาม แต่เนื่องจากระยะเวลาที่มีจำกัด และความยากในการประสานเข้าสัมภาษณ์เชิงลึกผู้วิจัยได้อาศัยสื่อการสื่อสารทาง Social Media ในการพูดคุยและสัมภาษณ์ และผู้บริหารระดับสูงส่วนใหญ่ค่อนข้างเห็นด้วยกับแนวคิดในการพัฒนาบุคลากรที่ผู้วิจัยนำเสนอในภาพรวม โดยมีรายละเอียดการวิจัยดังต่อไปนี้

ขั้นตอนการดำเนินการวิจัย

1. ศึกษาแนวคิด ทฤษฎี ที่เกี่ยวข้องกับการพัฒนาบุคลากรด้านไซเบอร์ของชาติมหาอำนาจ
2. ศึกษารูปแบบ หลักนิยมการทำสงครามไซเบอร์ของชาติต่าง ๆ ประกอบกับแนวคิดของภัยคุกคามไซเบอร์ในวรรณกรรมที่เกี่ยวข้อง
3. สัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ทรงคุณวุฒิที่เป็นผู้บริหารระดับสูง ระดับกลาง รวมถึงผู้เชี่ยวชาญด้านไซเบอร์ เพื่อรับทราบข้อมูลโดยตรงจากผู้มีประสบการณ์ในการบริหารและปฏิบัติงานไซเบอร์โดยตรง
4. จัดการสนทนากลุ่ม (Focus Group) ระหว่างผู้บริหารและผู้เชี่ยวชาญด้านไซเบอร์
5. วิเคราะห์ผลที่ได้จากแบบสอบถามผู้ที่เกี่ยวข้องกับการปฏิบัติงานด้านสงครามไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์
6. วิเคราะห์ผลจากการสัมภาษณ์ และการสนทนากลุ่ม
7. วิเคราะห์แนวทางที่เหมาะสมสำหรับการพัฒนาบุคลากรด้านไซเบอร์ของประเทศ
8. สรุปแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศ

แหล่งข้อมูล

1. ขอบเขตพื้นที่

1.1 หน่วยขึ้นตรงสำนักงานปลัดกระทรวงกลาโหม โดยเฉพาะในส่วนของศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ศูนย์ไซเบอร์ของหน่วยต่าง ๆ เช่น ศูนย์ไซเบอร์กองทัพบก กองทัพเรือ และกองทัพอากาศ

1.2 บุคลากรที่ทำงานด้านไซเบอร์ในหน่วยงานเอกชน

2. ผู้ให้ข้อมูลสำคัญ

2.1 ผู้บังคับบัญชาระดับสูงของกระทรวงกลาโหม

2.2 ผู้บังคับบัญชาของหน่วยงานที่รับผิดชอบโดยตรงในศูนย์ไซเบอร์ของกลาโหม

2.3 ผู้เชี่ยวชาญด้านไซเบอร์ในหน่วยงานเอกชน

การเก็บรวบรวมข้อมูล

เนื่องจากงานวิจัยนี้เป็นการวิจัยแบบผสมผสาน การเก็บรวบรวมข้อมูลของงานวิจัยนี้ประกอบด้วยข้อมูลจากสามส่วนคือ

1. การสัมภาษณ์ ผู้วิจัยสัมภาษณ์ด้วยตนเอง โดยการบันทึกข้อมูลด้วยการจดบันทึกและ/หรือบันทึกด้วยเครื่องบันทึกเสียง และ/หรือภาพเคลื่อนไหว และการสนทนาผ่านสื่อสังคมออนไลน์

2. การสนทนากลุ่ม ผู้วิจัยได้จัดสนทานกลุ่มและได้บันทึกข้อมูลด้วยการจดบันทึก

3. การแจกจ่ายแบบสอบถาม (ออนไลน์) โดยแจกจ่ายไปยังผู้ปฏิบัติงานที่เกี่ยวข้องโดยตรง ดำเนินการเก็บรวบรวมข้อมูลจากแบบสอบถามด้วยตนเองและรับคืนพร้อมตรวจสอบความสมบูรณ์ของการกรอกแบบสอบถาม

เครื่องมือที่ใช้ในการวิจัย

การวิจัยนี้ใช้เครื่องมือในการวิจัยดังต่อไปนี้

1. การสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ (In-depth Interview)
2. แนวคำถามสำหรับการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ
3. การทดสอบความเที่ยงตรงของเครื่องมือที่ใช้ในการวิจัย
   3.1 ความเที่ยงตรงตามเนื้อหา (Content Validity)
   3.1 ความเชื่อมั่น (Reliability)

การวิเคราะห์ข้อมูล

ข้อมูลของการวิจัยมาจากการวิเคราะห์สามส่วนคือ การวิเคราะห์ข้อมูลเชิงปริมาณ การวิเคราะห์ข้อมูลเชิงคุณภาพ และการวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม

1. การวิเคราะห์ข้อมูลเชิงปริมาณ (Qualitative Analysis) เป็นการนำแบบสอบถามกับกลุ่มกำลังพลที่ปฏิบัติหน้าที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยใช้ระบบแบบสอบถามออนไลน์เพื่อตอบคำถามต่าง ๆ ที่ได้กำหนดขึ้นตามวัตถุประสงค์ของการวิจัย เช่น ความคิดเห็นเกี่ยวกับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ความคิดเห็นเกี่ยวกับปัจจัยที่มีผลกระทบต่อการปฏิบัติงานและการพัฒนากำลังพลด้านไซเบอร์ ข้อเสนอแนะในการปรับปรุงกระบวนการพัฒนาบุคลากรไซเบอร์ จากนั้นใช้กระบวนการทางสถิติทั่วไปเพื่อวิเคราะห์ผลจากแบบสอบถาม

2. การวิเคราะห์ข้อมูลเชิงคุณภาพ (Qualitative Analysis) ประกอบด้วย 4 ขั้นตอนหลักคือ การตรวจสอบข้อมูล การทำดัชนีข้อมูล การทำข้อสรุปชั่วคราวและการกำจัดข้อมูล และ การสร้างบทสรุปและพิสูจน์บทสรุป ซึ่งจะทำตามลำดับเมื่อได้รวบรวมข้อมูลที่จะนำมาวิเคราะห์จะใช้แนวคิดทฤษฎีในสองวิธีการคือ การวิเคราะห์ข้อมูลโดยการตีความสร้างข้อสรุปแบบอุปนัย (ได้จากการสังเกตและการสัมภาษณ์จากสิ่งที่เป็นรูปธรรม) และ การวิเคราะห์ข้อมูลจากเนื้อหาจากเอกสารโดยต้องคำนึงถึงบริบท หรือสภาพแวดล้อมของข้อมูลเอกสารที่นำมาวิเคราะห์ประกอบและเปรียบเทียบการเปลี่ยนแปลงที่เกิดขึ้น

3. การวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม จะใช้การสรุปประเด็นสำคัญจากผู้ให้ข้อมูลที่มีประสบการณ์ในการปกครองหรือการทำงานในหน่วยที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และนำข้อมูลการสนทนากลุ่มมาเปรียบเทียบเพื่อหาข้อสรุปเพื่อพัฒนาแนวทางการพัฒนาบุคลากรไซเบอร์ต่อไป

บทที่ 4
ผลการวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อค้นหาแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศให้มีความยั่งยืน เพื่อให้บุคลากรด้านไซเบอร์มีประสิทธิภาพพร้อมรับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงและถูกยกระดับให้กลายเป็นพลังอำนาจแห่งชาติที่สำคัญอีกด้านหนึ่ง

การวิเคราะห์ข้อมูล

ข้อมูลที่นำมาวิเคราะห์มาจากสามส่วนดังที่กล่าวไปในบทที่ผ่านมา คือ ข้อมูลจากแบบสอบถามออนไลน์ ข้อมูลจากเอกสาร ระเบียบ คำสั่ง หลักนิยม วรรณกรรม และงานวิจัยที่เกี่ยวข้อง และข้อมูลจากการสัมภาษณ์ จากนั้นจึงนำข้อมูลมาวิเคราะห์เนื้อหา โดยมุ่งเน้นข้อมูลตัวแปรอิสระในการวิจัย โดยมีผลการวิเคราะห์ข้อมูลตามลำดับดังนี้

1. วิเคราะห์จากแบบสอบถาม

1.1 ข้อมูลของผู้ตอบแบบสอบถาม

ตารางที่ 4-1 ข้อมูลบุคคลของผู้ที่ให้ข้อมูลในแบบสอบถาม

ข้อมูลบุคคล	รายละเอียด	จำนวน	หมายเหตุ
เพศ	ชาย	152	
	หญิง	18	
อายุ	25-34	80	
	35-44	44	
	45 ปีขึ้นไป	46	
วุฒิการศึกษา	ต่ำกว่าปริญญาตรี	18	
	ปริญญาตรี	112	
	ปริญญาโท	37	
	ปริญญาเอก	3	
ระดับชั้นยศ	ไม่มีชั้นยศ (พลเรือน)	16	
	ร.ต.-ร.อ.	73	
	พ.ต.-พ.อ.	77	
	ชั้นยศนายพล	4	
ประสบการณ์ทำงาน	5 ปี ลงมา	88	
	6-10 ปี	37	
	11-15 ปี	25	
	16-20 ปี	14	
	21 ปีขึ้นไป	6	

ข้อมูลบุคคลที่ได้จากการตอบแบบสอบถามส่วนใหญ่เป็นผู้ชายมากกว่าผู้หญิง และมีอายุส่วนใหญ่อยู่ในวัย 25-34 ปีเป็นหลัก แต่ที่น่าสังเกตอีกประการหากรวมบุคลากรที่มีอายุตั้งแต่ 35 ปีขึ้นไปจะมีจำนวนรวมกันมากว่าผู้มีอายุน้อยกลุ่มแรกซึ่งถือได้ว่าอยู่ในห้วงวัยทำงาน และส่วนใหญ่มีวุฒิการศึกษาในระดับปริญญาตรีซึ่งถือว่าเป็นเรื่องปกติของสัดส่วนทั่วไปในสังคม ในเรื่องของสัดส่วนของยศของผู้ให้ข้อมูลถือว่าไม่มีนัยสำคัญมากนักแต่ก็แสดงให้เห็นว่ามีการกระจายตัวในปริมาณเท่า ๆ กันระหว่างกลุ่มที่มีชั้นยศ ร.ต.-ร.อ. กับอีกกลุ่มที่มีชั้นยศ พ.ต.ขึ้นไป และผู้ให้ข้อมูลส่วนใหญ่มีอายุงานต่ำกว่า 5 ปีในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ มีส่วนน้อยที่ประสบการณ์สูงระดับ 21 ปีขึ้นไปซึ่งคาดว่าเป็นระดับผู้บริหาร และรองลงมาเป็นผู้ที่มีประสบการณ์การทำงานในห้วง 16-20 ปี จำนวน 14 คน

1.2 พื้นฐานความรู้การปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในส่วนนี้ใช้ค่าข้อมูลเชิงสถิติ เพื่อแบ่งช่วงของความเห็นออกเป็น 5 ระดับคือ มากที่สุด = 4.21-5.00, มาก = 3.41-4.20, ปานกลาง = 2.61-3.40, น้อย = 1.81-2.60, และ น้อยมาก = 1.00-1.80 โดยสรุปผลลัพธ์ของการแปลข้อมูลทั้งหมดตามตารางที่ 4-2

ตารางที่ 4-2 พื้นฐานความรู้การปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

รายละเอียด	แปลความ
1. พื้นฐานความรู้เกี่ยวกับปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
1.1 เข้าใจความหมายของการรักษาความมั่นคงปลอดภัยไซเบอร์	ปานกลาง
1.2 ทราบถึงผลกระทบของภัยคุกคามไซเบอร์	มาก
1.3 มีความรู้เกี่ยวกับการป้องกันภัยไซเบอร์เช่น ไวรัส หนอน มัลแวร์ ฯลฯ	ปานกลาง
1.4 เข้าใจความหมายของสงครามไซเบอร์	ปานกลาง
1.5 เข้าใจขอบเขตความรู้พื้นฐานในการเข้าปฏิบัติงานด้านไซเบอร์	น้อย
1.6 ผู้ร่วมงานมีประสิทธิภาพและสามารถปฏิบัติงานไซเบอร์ได้ในลักษณะทีม	น้อย
1.7 มีความมั่นใจและมีขีดความสามารถใช้อุปกรณ์ที่เกี่ยวข้องกับการทำงาน	น้อย
1.8 มีแหล่งความรู้ ที่ปรึกษา สำหรับสนับสนุนการแก้ไขปัญหาเพียงพอ	น้อย
2. ทักษะการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
2.1 มีความสามารถในการบริหารงานและแก้ไขปัญหาระบบเครือข่าย	ปานกลาง
2.2 มีขีดความสามารถในการปฏิบัติงานในลักษณะ blue team (ทีมป้องกัน)	ปานกลาง
2.3 มีขีดความสามารถปฏิบัติหน้าที่เป็น red team (ทีมโจมตี) ได้	น้อยมาก
2.4 มีความสามารถในการใช้มัลแวร์เป็นเครื่องมือสำหรับปฏิบัติการไซเบอร์	น้อยมาก
2.5 ผ่านการอบรมหลักสูตรด้านไซเบอร์ขั้นกลาง ขั้นสูง	น้อยมาก
2.6 มีประกาศนียบัตรวิชาชีพระดับสากล เช่น CISSP, CISA, CEH	น้อยมาก
3. ขีดความสามารถในการพัฒนาบุคลากร/การเป็นผู้ฝึกสอน/อื่นๆ	
3.1 ผ่านการอบรมผู้ฝึกสอน หรือสามารถเป็นผู้พัฒนาบุคลากรไซเบอร์ได้	น้อยมาก

รายละเอียด	แปลความ
3.2 ผ่านการดูงาน/ร่วมงานประชุมสัมนาด้านไซเบอร์ในระดับสากล เช่น BlackHat, DEFCON	น้อยมาก
3.3 เคยเป็นผู้บรรยายให้กับบุคลากรด้านไซเบอร์ในการประชุมสัมมนา	น้อยมาก
3.4 หน่วยงานของรัฐที่รับผิดชอบหลักด้านไซเบอร์สนับสนุนการพัฒนาบุคลากรระดับผู้ฝึกสอน	น้อยมาก
3.5 รัฐ/เอกชนมีอุปกรณ์/เครื่องช่วยฝึก/ผู้ฝึกสอนที่เหมาะสม และมีการสนับสนุนจากองค์กรภาครัฐ/เอกชน	น้อยมาก
3.6 มีความพึงพอใจต่อการปฏิบัติงานใน “หน้าที่” การรักษาความมั่นคงปลอดภัยไซเบอร์	มาก
3.7 มีความเชื่อมั่นในขีดความสามารถขององค์กร/หน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	น้อย
3.8 ได้รับโอกาสในการพัฒนาศักยภาพตามหน้าที่การปฏิบัติงานการรักษาความมั่นคงปลอดภัยไซเบอร์จากหน่วยงาน/องค์กรที่เหมาะสม	น้อย

ผลการวิเคราะห์ข้อมูลในหัวข้อพื้นฐานความรู้เกี่ยวกับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์พบว่า ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ส่วนใหญ่ทราบถึงผลกระทบของภัยคุกคามด้านไซเบอร์ และมีความเข้าใจเกี่ยวกับความหมายของสงครามไซเบอร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ และการระวังป้องกันภัยคุกคามทั่วไปเช่น หนอน ไวรัส มัลแวร์ ในระดับปานกลาง แต่มีส่วนน้อยที่เข้าใจขอบเขตความรู้พื้นฐานในการเข้าปฏิบัติงานไซเบอร์ มีความมั่นใจและมีขีดความสามารถในการใช้อุปกรณ์ที่เกี่ยวข้องกับการทำงาน และการมีแหล่งความรู้ ที่ปรึกษา ที่สามารถสนับสนุนการแก้ไขปัญหาได้เพียงพอ

ในส่วนของหัวข้อทักษะการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น ผู้ปฏิบัติงานมีความสามารถในการบริหารงานและแก้ไขปัญหาระบบเครือข่าย และการมีขีดความสามารถในการปฏิบัติงานเป็น blue team อยู่ในระดับปานกลางแต่มีขีดความสามารถในการปฏิบัติหน้าทีเป็น red team และการใช้มัลแวร์เป็นเครื่องมือสำหรับปฏิบัติการไซเบอร์อยู่ในระดับค่อนข้างต่ำ และมีส่วนน้อยที่ผ่านการอบรมหลักสูตรด้านไซเบอร์ขั้นกลางและขั้นสูง มีส่วนน้อยมากที่มีประกาศนียบัตรวิชาชีพระดับสากล

ในส่วนของหัวข้อขีดความสามารถในการพัฒนาบุคลากรหรือการเป็นผู้ฝึกสอน มีส่วนน้อยมาที่ผ่านการอบรมระดับผู้ฝึกสอนหรือสามารถเป็นผู้พัฒนาบุคลากรไซเบอร์ได้ อีกทั้งมีส่วนน้อยมากที่เคยผ่านการดูงานหรือร่วมงานประชุมสัมมนาด้านไซเบอร์ในระดับสากล หรือเคยเป็นผู้บรรยายให้กับบุคลากรด้านไซเบอร์ในการประชุมสัมนา นอกจากนี้ยังขาดการสนับสนุนจากหน่วยงานของรัฐที่รับผิดชอบหลักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แต่ผู้ปฏิบัติงานส่วนใหญ่มีความพึงพอใจต่อการปฏิบัติหน้าที่ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งถือว่าเป็นภาระหน้าที่ที่ได้รับการยอมรับจากบุคคลอื่น ๆ ในหน่วยงานเดียวกัน ผู้ปฏิบัติงานไม่มีความเชื่อมั่นในขีดความสามารถขององค์กรที่ทำหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และไม่ค่อยได้รับโอกาสในการ

พัฒนาศักยภาพตามหน้าที่การปฏิบัติงานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

2. วิเคราะห์จากวรรณกรรมและงานวิจัยที่เกี่ยวข้อง

ยุทธศาสตร์ชาติด้านความมั่นคงมีเป้าหมายการพัฒนาที่สำคัญ คือ ประเทศชาติมั่งคง ประชาชนมีความสุข เน้นการบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคง ปลอดภัย เอกราชอธิปไตย และมีความสงบเรียบร้อยในทุกระดับ ตั้งแต่ระดับชาติ สังคม ชุมชน โดยมุ่งเน้นการพัฒนาคน เครื่องมือ เทคโนโลยี และระบบฐานข้อมูลขนาดใหญ่ให้มีความพร้อมสามารถรับมือภัยคุกคามและภัยพิบัติได้ทุกรูปแบบ และทุกระดับความรุนแรง โดยมีนโยบายและแผนอื่น ๆ ที่เกี่ยวข้องและส่งเสริมต่อยุทธศาสตร์ชาติด้านความมั่นคงคือ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ.2560-2564) โดยในยุทธศาสตร์ที่ 5 การเสริมความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่นคงและยั่งยืน โดยมีเป้าหมายคือ ประเทศไทยมีความพร้อมต่อการรับมือภัยคุกคาม ทั้งทางทหารและภัยคุกคามอื่น ๆ ซึ่งหมายรวมถึงภัยคุกคามด้านไซเบอร์ด้วย และในยุทธศาสตร์ที่ 7 การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์ โดยมีแนวทางการพัฒนาคือให้ปรับปรุงโครงสร้างพื้นฐานโทรคมนาคมของประเทศให้ทั่วถึงและมีประสิทธิภาพ ส่งเสริมการใช้เทคโนโลยีดิจิตัลในการสร้างมูลค่าเพิ่มทางธุรกิจ การส่งเสริมนวัตกรรมการวิจัยและการพัฒนาอุตสาหกรรมดิจิตัลและเทคโนโลยีอวกาศของไทย พัฒนาความรู้และทักษะของประชาชน และโดยเฉพาะให้มีการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งจะเห็นได้ว่าการพัฒนาบุคลากรด้านไซเบอร์ได้รับความสำคัญในระดับที่กำหนดไว้ในยุทธศาสตร์ระดับชาติ นอกจากนั้นในยุทธศาสตร์ที่ 5 ของแผนพัฒนาดิจิตัลเพื่อเศรษฐกิจและสังคม กล่าวถึงการพัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิตัล ซึ่งเป็นการพัฒนาบุคลากรผู้ทำงานให้มีความสามารถในการสร้างสรรค์ รู้จักใช้เทคโนโลยีดิจิตัลอย่างชาญฉลาด โดยเฉพาะการพัฒนาทักษะด้านเทคโนโลยีดิจิตัลในบุคลากรภาครัฐ ภาคเอกชน ให้มีความรู้ความสามารถ ความเชี่ยวชาญในระดับมาตรฐานสากล จะเห็นได้ว่าการพัฒนาบุคลากรนั้นได้ถูกบรรจุอยู่ในแผนระดับชาติเพราะเป็นพื้นฐานสำคัญในการพัฒนาประเทศและการรับมือกับภัยคุกคามในรูปแบบต่าง ๆ

2.1 ในเรื่องที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2560-2564) ได้ระบุให้ภัยคุกคามไซเบอร์เป็นหนึ่งในภัยคุกคามความมั่นคง และในประเด็นที่ 3.7.15 เรื่องการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์มีการกำหนดเป้าหมายทางยุทธศาสตร์ให้ ประเทศไทยมีความมั่นคงปลอดภัยและมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ และมีกลยุทธ์พอสรุปได้คือ 1) พัฒนาขีดความสามารถทั้งองค์กรภาครัฐ ฝ่ายทหาร ตำรวจ พลเรือนและภาคส่วนต่าง ๆ 2) พัฒนากรอบความร่วมมือระหว่างประเทศ 3) พัฒนาทรัพยากรมนุษย์ องความรู้ และการสร้างความตระหนัก 4) ปกป้อง ป้องกันภัยคุกคามทางไซเบอร์ บูรณาการการจัดการความมั่นคงไซเบอร์ระหว่างหน่วยงานภาครัฐและเสริมสร้างเครือข่ายในทุกภาคส่วน 5) พัฒนาการบังคับใช้กฎหมาย ระเบียบ รวมถึงเทคโนโลยีที่เกี่ยวข้อง 6) ส่งเสริมการพัฒนาขีดความสามารถขององค์กร ให้บุคลากรที่เกี่ยวข้องมีความรู้ความชำนาญในระดับสากล

2.2 ในแผนเตรียมความพร้อมแห่งชาติ (พ.ศ.2560-2564) ด้านวิกฤตการณ์ด้านความมั่นคงได้มีการกล่าวว่า ประเทศไทยกำลังเผชิญกับภัยคุกคามรูปแบบใหม่ที่นำไปสู่วิกฤตการณ์

ด้านความมั่นคงในหลายเรื่องเช่น การก่อวินาศกรรม การก่อการร้าย การค้ามนุษย์ ปัญหาแรงงานต่างด้าว การค้ายาเสพติด การฟอกเงิน โรคอุบัติใหม่ ความเห็นต่างทางการเมือง และที่สำคัญคือ “การโจมตีทางไซเบอร์” ทั้งนี้เนื่องจากประเทศไทยโดยสภาพภูมิศาสตร์ที่ได้เปรียบจึงกลายเป็นศูนย์กลางการคมนาคมของภูมิภาคตะวันออกเฉียงใต้ ทั้งทางบก ทางเรือ และทางอากาศ ดังนั้นจึงมีทั้งข้อดีและมีความเสี่ยงต่อการเป็นประเทศทางผ่าน การเป็นแหล่งซ่องสุม แหล่งพักพิงของอาชญากรข้ามชาติ หรือแม้แต่ใช้เป็นฐานบัญชาการของอาชญากรเพื่อกระทำผิดในประเทศอื่น ๆ โดยเฉพาะอย่างยิ่งการโจมตีทางไซเบอร์ต่อประเทศอื่น ๆ

2.3 เจตนารมณ์ของแผนแม่บทความมั่นคงปลอดภัยไซเบอร์ จัดให้มีการพัฒนากลไกการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์เพื่อแก้ปัญหาแบบองค์รวม ทั้งการรับมือกับเหตุการณ์ทั่วไป อาชญากรรมไซเบอร์ และการรับมือภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อเศรษฐกิจและสังคมทั้งในระยะสั้นและระยะยาว โดยกำหนดองค์กรรับผิดชอบระดับชาติดำเนินการขับเคลื่อนแผนอย่างเป็นรูปธรรม

2.4 ในส่วนของแผนปฏิบัติการมีวัตถุประสงค์ต่าง ๆ พอสรุปได้ดังนี้ 1) สร้างความมั่นคงปลอดภัยทางไซเบอร์ทั้งในระดับบุคคล หน่วยงานภาคธุรกิจและภาครัฐ ระดับประเทศและระหว่างประเทศ ให้มีรูปแบบการรับมือภัยคุกคามไซเบอร์ตามมาตรฐานสากล 2) สร้างมาตรการรับมือกับภัยไซเบอร์ ตามมาตรฐานสากลเพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญให้มีความมั่นคงปลอดภัยจากการคุกคามทางไซเบอร์ 3) กำหนดองค์กรในการบริหารจัดการ พัฒนาและสร้างศักยภาพด้านไซเบอร์ในทุกมิติ รวมถึงเสริมสร้างความเข้มแข็งด้านไซเบอร์ ด้วยการสร้างความร่วมมือทั้งในระดับประเทศและต่างประเทศ 4) พัฒนาและปรับปรุงแก้ไขกฎหมายไซเบอร์ให้ทันต่อสถานการณ์โลก ตลอดจนบริหารจัดการการบังคับใช้กฎหมายไซเบอร์

2.5 ในส่วนของวรรณกรรมเอกสารที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้เขียนได้ทบทวนวรรณกรรมยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ และนำมาสรุปไว้ในตารางเดียวกันเพื่อให้ผู้อ่านได้เห็นถึงความแตกต่างในเนื้อหาสาระที่แต่ละประเทศมุ่งเน้น เช่น การพัฒนาศักยภาพของบุคลากรด้านไซเบอร์มักเป็นหนึ่งในเสาหลักของการกำหนดยุทธศาสตร์ไซเบอร์ในระดับชาติ นอกจากนั้นการแสวงหาความร่วมมือระหว่างประเทศมักถูกกำหนดไว้เป็นกลไกสำคัญในผนึกกำลังทางด้านไซเบอร์รวมถึงการลดความขัดแย้งระหว่างประเทศ โดยมีรายละเอียดในตารางที่ 2

2.6 แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ (น.อ.ประยูร ธรรมาธิวัฒน์, 2558, 63-70) กำหนดแนวทางการพัฒนาขีดความสามารถของบุคลากรภายใต้ปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ให้มีการเตรียมความพร้อมต่อปฏิบัติการสงครามไซเบอร์อย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกทางไซเบอร์เพื่อเสริมสร้างทักษะในการปฏิบัติงาน เพื่อให้มีความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ มีความยั่งยืนและสามารถพึ่งพาตนเองได้

3. วิเคราะห์จากการสัมภาษณ์เชิงลึก

จากการวิเคราะห์ข้อมูลการสัมภาษณ์สามารถสรุปผลได้ดังนี้

3.1 ความเห็นเกี่ยวกับหน่วยงานที่มีความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ว่า เห็นควรจัดตั้งหน่วยงานระดับชาติที่รับผิดชอบการประสานงาน นโยบาย

เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีกฎหมายรองรับและเป็นหน่วยงานระดับชาติที่สามารถประสานการปฏิบัติระหว่างหน่วยงานไซเบอร์ของทุกภาคส่วนทั้งภาคความมั่นคง ราชการและเอกชน และบางท่านให้ความเห็นว่าควรมีบทบาทหลักในการพัฒนาบุคลากรด้านไซเบอร์ในระดับต่าง ๆ บุคลากรในองค์กรที่รับผิดชอบหลักด้านความมั่นคงปลอดภัยไซเบอร์ควรมีขีดความสามารถในด้านปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ และมีขีดความสามารถในการปฏิบัติการข่าวกรองไซเบอร์

3.2 ความเห็นเกี่ยวกับปัญหาการขาดแคลนบุคลากรด้านไซเบอร์ ผู้ให้สัมภาษณ์ส่วนใหญ่ยตระหนักว่ามีปัญหาการขาดแคลนบุคลากรที่จะมาทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ถึงแม้ว่าหลายหน่วยงานจะมีการจัดตั้งหน่วยปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น ศูนย์ไซเบอร์ต่าง ๆ แล้วก็ตาม ตำแหน่งต่าง ๆ ที่ได้กำหนดไว้ให้ปฏิบัติหน้าที่ตามที่ได้ออกแบบไว้มักไม่สามารถบรรจุบุคลากรที่เหมาะสมกับตำแหน่งต่าง ๆ เหล่านั้นได้อย่างจริงจัง การเปิดอัตรากำลังและรับสมัครงานในตำแหน่งที่ต้องใช้ความสามารถพิเศษในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้นไม่สามารถใช้ได้อย่างจริงจัง ทั้งนี้เนื่องจาก บุคลากรในหน่วยที่รับสมัครเองก็ไม่มีขีดความสามารถในการคัดเลือก ออกข้อสอบ สัมภาษณ์ให้เนื้อหาที่ควรจะเป็นประโยชน์ต่อการเข้ามาปฏิบัติหน้าที่ในตำแหน่งนั้น ๆ นอกจานั้นผู้ที่มาสมัครสอบเองส่วนใหญ่มีเพียงความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศและไม่ค่อยมีประสบการณ์ในการทำงานโดยตรงกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ยังไม่รวมปัญหาเรื่องการบรรจุบุคลากรที่มีความไม่เหมาะสมเข้าในตำแหน่งที่ต้องการ นอกจากปัญหาการขาดแคลนบุคลากรในระดับปฏิบัติงานแล้ว ในส่วนของการบริหารงานมักจะไม่ได้พิจารณาการเข้ารับตำแหน่งจากความรู้ ความสามารถ หรือคุณวุฒิที่เหมาะสม ส่วนใหญ่มักยึดติดกับการพิจารณาการเข้าสู่ตำแหน่งผู้บริหารด้วยอาวุโส ใครทำงานมานานกว่ากัน หรือเป็นพรรคพวกของใครเป็นประเด็นหลัก

3.3 ผู้ให้สัมภาษณ์ส่วนใหญ่ให้ความเห็นว่าปัญหาเรื่องค่าตอบแทนที่ไม่เหมาะสมส่งผลกระทบต่อการจัดโครงสร้างของหน่วยงานไซเบอร์โดยตรง ปัญหานี้มักไม่สามารถบรรจุกำลังพลเข้าตามอัตราตามที่คิดไว้หรือได้บุคลากรที่ไม่สามารถทำงานได้ตามที่คาดหวัง ความขาดแคลนบุคลากรด้านไซเบอร์ทำให้อัตราการจ้างงานในตำแหน่งที่ต้องใช้ขีดความสามารถเฉพาะทางด้านไซเบอร์นั้นมีอัตราการจ้างงานที่สูง องค์กรต่างแย่งชิงบุคลากรด้านไซเบอร์ด้วยค่าตอบแทนที่สูงกว่าการจ้างงานปกติของคนที่ทำงานด้านไอที ถึงแม้ว่าหน่วยราชการบางหน่วยกำลังปรับปรุงระเบียบเพื่อเพิ่มค่าตอบแทนให้มีลักษณะคล้ายนักบิน ผู้ปฏิบัติงานเสี่ยงภัยจากการกู้ระเบิด ค่าปีกโดดร่ม แต่จำนวนที่เพิ่มเมื่อเทียบกับการไปทำงานในบริษัทเอกชนหรือบริษัทข้ามชาตินั้นไม่สามารถจะหยุดหรือต้านการไหลของบุคลากรไซเบอร์ไปยังภาคเอกชน เพราะภาคเอกชนเองก็ประสบปัญหาการขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เช่นกัน

4. วิเคราะห์ผลการสนทนากลุ่ม

สรุปผลการวิเคราะห์การสนทนากลุ่มผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หัวข้อย่อย ๆ ต่าง ๆ ได้ดังนี้

4.1 ในด้านความสามารถในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อสนทนาในกลุ่มผู้เชี่ยวชาญส่วนใหญ่ยอมรับว่าผู้ร่วมงานที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ยังมีขีดความสามารถอยู่ในระดับที่ต้องพัฒนาเมื่อเทียบกับผู้ที่ปฏิบัติงานด้านนี้

ในประเทศมหาอำนาจ มีส่วนน้อยเท่านั้นที่มีขีดความสามารถในระดับที่สามารถแข่งขันกับต่างประเทศในสนามประลองความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดโดยประเทศที่เป็นผู้นำด้านนี้ จากการสนทนาผู้เชี่ยวชาญระดับสูงส่วนใหญ่เข้าใจปัญหาการพัฒนาบุคลากรด้านนี้ดีว่าต้องใช้ทั้งเวลาและทรัพยากร รวมถึงต้องมีขีดความสามารถเฉพาะตัวเป็นทุนเดิมอยู่จึงจะสามารถยกระดับขีดความสามารถในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในระดับที่พึงพอใจได้ ผู้เชี่ยวชาญส่วนใหญ่เข้าใจว่าผู้ปฏิบัติงานอย่างน้อยควรมีความรู้พื้นฐานด้านการโปรแกรมภาษาคอมพิวเตอร์ ระบบเครือข่ายและโปรโตคอลของระบบอินเทอร์เน็ต

4.2 ในด้านกระบวนการพัฒนาผู้ฝึกสอนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น การสนทนาในกลุ่มผู้เชี่ยวชาญส่วนใหญ่ยังคงเห็นว่ายังมีปัญหาความขาดแคลนผู้ฝึกสอนเป็นอย่างมาก ถ้าเป็นการฝึกสอนในระดับ advanced มักจะต้องพึ่งพาผู้เชี่ยวชาญการรักษาความมั่นคงปลอดภัยไซเบอร์จากต่างประเทศ ปัญหาข้างเคียงที่เกี่ยวข้องกับการฝึกสอนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์คือเรื่องหลักสูตรที่จะนำมาใช้ หน่วยงานไซเบอร์เองยังคงไม่มีทิศทางที่แน่นอนว่าจะให้บุคลากรที่จะปฏิบัติหน้าที่ไปศึกษาวิชาอะไร ซึ่งแม้แต่ในประเทศที่เจริญแล้วยังคงมีปัญหาในการฝึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสมจริงเหมือนกับการฝึกในทางทหาร ซึ่งการฝึกในปัจจุบันมักสมมุติเหตุการณ์การโจมตีด้านไซเบอร์ที่ไม่อาจบอกได้ว่าสมมุติฐานนั้นเชื่อถือได้แค่ไหนเนื่องจากมีความไม่แน่นอนของเหตุการณ์ที่จะเกิดขึ้นจากการโจมตีทางไซเบอร์

4.3 ในด้านทรัพยากรสนับสนุนการพัฒนาบุคลากรผู้สนทนาส่วนใหญ่ให้ความเห็นพ้องกันว่านอกจากปัญหาการขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แล้ว ในส่วนของการสนับสนุนทรัพยากรเพื่อใช้ในการพัฒนาบุคลากรด้านนี้ยังคงเป็นประเด็นปัญหาใหญ่ที่ไม่ค่อยได้รับการสนับสนุนอย่างเพียงพอ ทำให้แผนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ได้ ความขาดแคลนทรัพยากรในด้านงบประมาณเป็นปัญหาหลักขององค์กรที่เป็นหน่วยงานภาครัฐซึ่งมีงบประมาณค่อนข้างจำกัดอยู่แล้ว การส่งบุคลากรเข้าศึกษาอบรมตามหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มักต้องใช้งบประมาณที่ค่อนข้างสูง จากข้อจำกัดของงบประมาณยิ่งส่งผลทำให้จำนวนบุคลากรที่จะส่งไปพัฒนาหรืออบรมหลักสูตรต่าง ๆ มีจำนวนที่ค่อนข้างจำกัด ซึ่งส่งผลต่อระยะเวลาในการพัฒนาบุคลกรในภาพรวมขององค์กร

สรุปผลการวิจัย

การวิจัยในหัวข้อการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นี้เป็นการวิจัยแบบผสมผสานเพื่อค้นหาแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศให้มีความยั่งยืนและมีความเชื่อมั่นในการนำไปปฏิบัติได้จริง บุคลากรด้านไซเบอร์มีประสิทธิภาพพร้อมรับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงและถูกยกระดับให้กลายเป็นพลังอำนาจแห่งชาติที่สามารถทำให้เกิดผลกระทบอย่างรุนแรงต่อความมั่นคงของชาติได้

ผลการสำรวจความคิดเห็นจากกลุ่มประชากรผู้ที่ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารระดับสูง และการสัมภาษณ์ผู้ทรงคุณวุฒิ ได้ข้อสรุปว่า

ส่วนใหญ่มีความคิดเห็นสอดคล้องกับปัญหาที่ผู้วิจัยได้ยกประเด็นขึ้นมา โดยมีบางส่วนเป็นกลาง และไม่มีผู้ที่ความคิดเห็นคัดค้าน ทั้งในเรื่องของประเด็นการขาดแคลนกำลังพลด้านไซเบอร์ที่ต้องมีทั้งประสบการณ์และความทุ่มเท ความยาก/สลับซับซ้อน/ปริมาณของเนื้อหาในการพัฒนา อบรม ฝึกซ้อม ระยะเวลาที่ต้องใช้ในการพัฒนาบุคลากรไซเบอร์ ผู้บริหารไม่ให้ความสนใจอย่างจริงจัง เช่น บรรจุบุคคลที่ไม่มีความสามารถด้านไซเบอร์เข้ามาในตำแหน่ง ผู้บริหารหลงประเด็นไม่ได้คำนึงถึงเนื้องานที่หน่วยไซเบอร์ต้องปฏิบัติ และแผนพัฒนากำลังพลด้านไซเบอร์ และปัญหาสมองไหลหรือการให้ค่าตอบแทนไม่คุ้มกับค่าขีดความสามารถ

ผลการวิจัยนี้นอกจากได้ศึกษาวิเคราะห์แนวทางในการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามไซเบอร์ในระดับชาติ โดยค้นคว้าการพัฒนาหลักนิยม/ยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ (ตามรายละเอียดในเอกสารวิจัยในการทบทวนวรรณกรรมที่เกี่ยวข้อง) ยังสามารถสรุปแนวทางในการกำหนดแผนการพัฒนาบุคลากรด้านไซเบอร์ ของประเทศ โดยแนวทางดังกล่าวนี้มีความสอดคล้องกับยุทธศาสตร์ชาติในภาพรวม ยุทธศาสตร์ไซเบอร์ของชาติ และมีการรองรับจากแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องอย่างเด่นชัด อีกทั้งยังมีข้อมูลสนับสนุนจากผลการสัมภาษณ์เชิงลึก และการสอบถามบุคลากรที่เกี่ยวข้องกับงานพัฒนาบุคลกรด้านไซเบอร์ในระดับประเทศ

แนวทางการพัฒนาบุคลากรไซเบอร์

จากการศึกษาข้อมูลในการทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง ผสมผสานกับผลการสำรวจความคิดเห็นที่ได้นำมาศึกษาเปรียบเทียบกับข้อมูลการทบทวนวรรณกรรมที่เกี่ยวข้อง ผู้วิจัยเสนอแนวทางการพัฒนาบุคลากรไซเบอร์ตามโมเดลที่แสดงในรูปที่ 3 แนวทางการพัฒนาบุคลากรไซเบอร์ประกอบด้วยโครงสร้างของกำลังพลไซเบอร์ที่นำเสนอเป็นโมเดลของแนวความคิดที่จะสามารถนำมาประยุกต์ใช้ได้กับการบริหารจัดการกำลังพลไซเบอร์ของประเทศไทย โดยกำลังพลไซเบอร์โดยประกอบด้วยบุคลากรไซเบอร์จาก

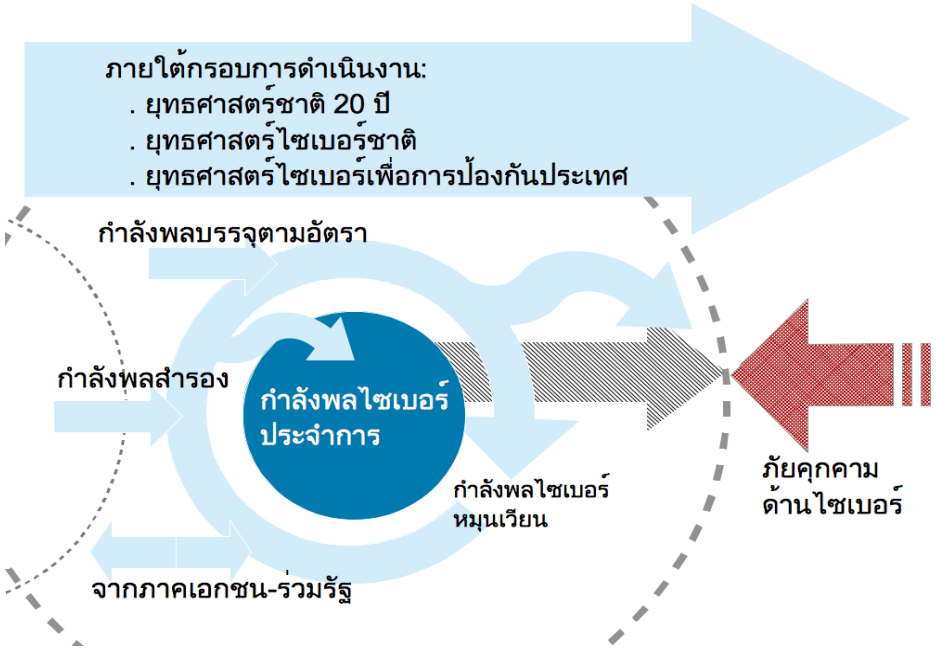
1. กำลังพลหลักประจำการ
2. กำลังพลสำรอง และ
3. กำลังพลไซเบอร์จากภาคเอกชนร่วมกับรัฐ หรืออาสาสมัคร

โดยที่กำลังพลไซเบอร์ประจำการคือบุคลากรที่อยู่ในอัตราการจัดของหน่วยนั้นอยู่แล้ว กำลังพลสำรอง ได้แก่บุคลากรที่มิใช่กำลังหลัก เช่น พลทหาร ทหารกองหนุน เป็นต้น ทั้งนี้กำลังพลจากภาครัฐ บริษัท ต้องสามารถทำงานในหน่วยงานภาครัฐรวมถึงได้สิทธิประโยชน์ตามสัดส่วนของเวลาทำงาน เช่น ทำงานที่บริษัทไมโครซอฟท์ 9 เดือน และเข้าทำงานเต็มเวลา ณ ศูนย์ไซเบอร์เป็นเวลา 9 เดือน เป็นต้น

แผนภาพที่ 4-1 แสดงกรอบความคิดทางการวิจัย ที่ประกอบด้วยโครงสร้างของกำลังพลไซเบอร์ที่นำเสนอเป็นโมเดลของแนวความคิดที่น่าจะสามารถนำมาประยุกต์ใช้ได้กับการบริหารจัดการกำลังพลไซเบอร์ของประเทศไทย ซึ่งประกอบด้วยบุคลากรไซเบอร์จาก กำลังพลหลักประจำการ กำลังพลสำรอง และจากภาคเอกชนร่วมกับรัฐ โดยที่กำลังพลไซเบอร์ประจำการคือบุคลากรที่อยู่ในอัตราการจัดของหน่วยนั้นอยู่แล้ว กำลังพลสำรอง ได้แก่บุคลากรที่มิใช่กำลังหลัก เช่น

พลทหาร ทหารกองหนุน เป็นต้น

แผนภาพที่ 4-1 กรอบความคิดทางการวิจัยที่มีกำลังพลไซเบอร์ประจำการเป็นองค์ประกอบหลักและมีการสนับสนุนกำลังพลจากส่วนต่าง ๆ อย่างต่อเนื่อง



บทที่ 5
สรุป และข้อเสนอแนะ

การวิจัยในหัวข้อการพัฒนาบุคลากรด้านไซเบอร์นี้เป็นการวิจัยแบบผสมผสาน (Mixed Method Procedure) ประกอบด้วยการวิจัยเชิงคุณภาพ และการวิจัยเชิงปริมาณ (Qualitative and Quantitative Research) เพื่อค้นหาแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศให้มีความยั่งยืน บุคลากรด้านไซเบอร์มีประสิทธิภาพพร้อมรับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงและถูกยกระดับให้กลายเป็นพลังอำนาจแห่งชาติ ในบทนี้จะกล่าวถึงข้อสรุปของงานวิจัย การอภิปรายผลการวิจัย และข้อเสนอแนะ

สรุป

ผลการวิจัยนี้ได้ศึกษาวิเคราะห์แนวทางในการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามไซเบอร์ในระดับชาติ ซึ่งได้ข้อสรุปเป็นแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศที่ต้องมีการบูรณาการ ทรัพยากรบุคคลจากทุกภาคส่วน มีการวางแผนเพื่อให้สามารถบรรลุวัตถุประสงค์ของการพัฒนาบุคลากรด้านนี้ ผลการวิจัยทำให้ทราบว่าทุกประเทศต่างตื่นตัวและมีการเตรียมความพร้อมเพื่อรับมือกับภัยคุกคามด้านไซเบอร์ มีการกำหนดยุทธศาสตร์ไซเบอร์ขึ้นมาเป็นส่วนประกอบของยุทธศาสตร์ความมั่นคงของชาติ มีการกำหนดหลักนิยมของการปฏิบัติการไซเบอร์ซึ่งผู้วิจัยได้รวบรวมและนำมาเรียบเรียงเพื่อทำการเปรียบเทียบสาระสำคัญของยุทธศาสตร์และหลักนิยม มีการจัดตั้งหน่วยงานที่รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับนโยบายและในระดับปฏิบัติการ โดยมีรายละเอียดการอภิปรายผลและข้อเสนอแนะในหัวข้อต่อไปนี้

ผลการวิจัยนี้นอกจากได้ศึกษาวิเคราะห์แนวทางในการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามไซเบอร์ในระดับชาติแล้ว ยังสามารถสรุปแนวทางในการกำหนดแผนการพัฒนาบุคลากรด้านไซเบอร์ของประเทศ โดยแนวทางดังกล่าวนี้มีความสอดคล้องกับยุทธศาสตร์ชาติในภาพรวม และมีการรองรับจากแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องอย่างเด่นชัด อีกทั้งยังมีข้อมูลสนับสนุนจากผลการสัมภาษณ์เชิงลึก และการสอบถามบุคลากรที่เกี่ยวข้องกับงานพัฒนาบุคลากรด้านไซเบอร์ในระดับประเทศ ผลการวิจัยชี้ให้เห็นอย่างมีนัยสำคัญว่าการขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้นเป็นปัญหาเร่งด่วนที่ต้องมีการแก้ไขทั้งระดับแผนและระดับปฏิบัติการ เนื่องจากบุคลากรส่วนน้อยที่มีขีดความสามารถในระดับผู้ฝึกสอนและไม่มีแผนแม่บทระดับชาติที่จะฝึกสอนผู้ฝึกสอน (train the trainers) ส่งผลให้ระยะเวลาในการพัฒนาบุคลากรด้านนี้ต้องใช้เวลานานกว่าการที่มีจำนวนผู้ฝึกสอนเป็นจำนวนมาก การแก้ไขปัญหาการขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้นต้องมีการวางแผนระยะยาว กำหนดเป้าหมายการเรียนรู้ที่สามารถปรับให้เข้ากับสภาพของภัยคุกคามที่เปลี่ยนไป และสนับสนุนทรัพยากรต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาบุคลากรให้มีศักยภาพเป็นที่ยอมรับได้ในระดับสากล

ข้อเสนอแนะ

ถึงแม้งานวิจัยนี้จะได้ศึกษารวบรวมข้อมูลที่สำคัญและเกี่ยวข้องกับประเด็นของปัญหาในหลากหลายมิติและได้นำเสนอข้อสรุปแนวทางการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แล้วก็ตาม ยังมีประเด็นปัญหาบางส่วนที่ไม่ได้ถูกครอบคลุมในการศึกษาวิจัยครั้งนี้ ผู้วิจัยมีข้อเสนอแนะของการวิจัยจำแนกตามประเภทได้แก่ ข้อเสนอแนะเชิงการบริหารบุคลากร ข้อเสนอแนะเชิงนโยบายและแผน ข้อเสนอแนะเชิงกฎ ระเบียบ กฎหมายที่เกี่ยวข้อง

1. ข้อเสนอแนะเชิงการบริหารบุคลากร

1.1 มีการจัดตั้งคณะทำงานเพื่อหาแนวทางร่วมกันระหว่างหน่วยที่เกี่ยวข้องเพื่อให้ได้ข้อสรุปการบริหารจัดการกำลังพลสำรองไซเบอร์ เพื่อนำไปสู่การจัดทำแผนและการปฏิบัติได้อย่างเป็นรูปธรรม

1.2 มีการยื่นข้อเสนอพิเศษให้บุคลากรที่มีพื้นฐานด้านคอมพิวเตอร์อยู่แล้ว เป็นการสร้างทางเลือกให้แก่ผู้ที่คิดจะหลีกเลี่ยงการเกณฑ์ทหารด้วยมีภาพลักษณ์ของการฝึกทหารใหม่ที่มีการใช้ความรุนแรง แต่สามารถเข้ารับการเกณฑ์ทหารด้วยการฝึกแบบพิเศษเพื่อให้สามารถเข้าทำการในลักษณะปฏิบัติการไซเบอร์ได้ทั้งในหน่วยทหารและองค์กรที่มีความต้องการบุคลากรด้านไซเบอร์

2. ข้อเสนอแนะเชิงนโยบายและแผน

2.1 กำหนดแนวทางในการจัดการกำลังพลสำรองที่ปลดประจำการ (ผ่านการเกณฑ์ทหารไปแล้ว) แต่ทำงานในสาขาที่เกี่ยวข้องอยู่แล้ว พิจารณาการเรียกเข้ามาเพื่อเป็นผู้ฝึกให้กับ “ทหารใหม่ไซเบอร์” ได้เป็นอย่างดี โดยที่เขาเหล่านั้นก็ถือได้ว่ามารับใช้ประเทศชาติในอีกทางหนึ่งในมิติของไซเบอร์

2.2 กำหนดนโยบายกำลังพลสำรองไซเบอร์ เพื่อนำทหารกองหนุน/กองเกินที่มีประสบการณ์ด้านไซเบอร์มาประกอบกำลังในสถานการณ์ฉุกเฉิน และการทำให้บุคลกรไซเบอร์สามารถทำงานได้ทั้งภาครัฐและเอกชน อาศัยหลักการ “แบ่งเวลา” ตามความเหมาะสมหรือความต้องการของบุคคลนั้น ๆ

3. ข้อเสนอแนะเชิงกฎ ระเบียบ กฎหมายที่เกี่ยวข้อง

3.1 พิจารณาปรับปรุงกฎหมายที่เกี่ยวข้อง เช่น พรบ. กำลังสำรอง ๒๕๕๘

3.2 เร่งรัด พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ที่จะนำไปสู่การจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) และจัดตั้งสำนักงาน กปช. เพื่อเป็นองค์กรรับผิดชอบงานไซเบอร์ในระดับชาติ ทั้งนี้ กปช. ควรเป็นอิสระจากกระทรวงทบวงกรม และขึ้นตรงต่อสำนักนายกรัฐมนตรี ต้องไม่อยู่ในความดูแลของกระทรวงใดกระทรวงหนึ่ง เพื่อให้เกิดเอกภาพในการบังคับบัญชา การควบคุม และการสั่งการทั้งในยามปกติและยามฉุกเฉิน

3.3 พิจารณาปรับปรุงข้อกฎหมายที่เกี่ยวข้องกับการประกาศสถานการณ์ฉุกเฉินสำหรับการบริหารจัดการภัยคุกคามไซเบอร์ที่มีความวิกฤตและกระทบต่อความมั่นคงของชาติ เช่น การให้มีอำนาจเรียกพล/รวมพลไซเบอร์/ใช้ทรัพยากรไซเบอร์จากหน่วยงานเอกชน/หน่วยงานภายนอก

บรรณานุกรม

ภาษาไทย

หนังสือ

กรองแก้ว ฉายสภาวธรรม. สาระน่ารู้กับไซเบอร์สเปซ, กรุงเทพฯ : ต้นธรรม, 2537.

“ปัญหาการขาดแคลนมืออาชีพด้านความปลอดภัยไซเบอร์” CIO World & Business, 6 กันยายน 2559.

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

จินดา สระสมบูรณ์, นาวาอากาศหญิง. “ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย” เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2557.

ประยูร ธรรมาธิวัฒน์, นาวาอากาศเอก. “แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2557.

รัฐพล ภักดีภูมิ. “การรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันและการพัฒนามาตรการการรักษาความปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2558.

วิโรจน์ ธันวรักษ์กิจพล, พลเรือตรี. “แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2556.

สุชาติ ผ่องพุฒิ, พลตรี. “แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2556.

สุทธิศักดิ์ สลักคำ, พลตรี. “ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2557.

อรัญ นำผล, พลเรือตรี. “การวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2556.

เอกสารไม่ตีพิมพ์

ป้องกันราชอาณาจักร, วิทยาลัย. “การขับเคลื่อนประเทศไทย”. (ร่าง) ยุทธศาสตร์ชาติระยะ 20 ปี (พ.ศ.2560 - 2579), 2560.

ปรัชญา เฉลิมวัฒน์, พันเอก, หลักนิยมการรบในมิติไซเบอร์, RTAF Air Warfare Journal, ฉบับที่ 64, ปีที่ 17, เม.ย.-มิ.ย. 2560.

สภากลาโหม. “ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศของกระทรวงกลาโหม พ.ศ. 2559”, 2559.

สำนักนายกรัฐมนตรีสิงคโปร์. “ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์”, 2529.
คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, สำนักงาน. “คู่มือ Cyber Security สำหรับประชาชน”, 2557.

ภาษาอังกฤษ

Books

Brett T Williams. “The Joint Force Commander’s Guide to Cyberspace Operations”, Rowman & Littlefield, 2017.

JFC Fuller. Meoirs of an Unconventional Soldier. I. Nicholson and Watson; 1st Edition edition, 1936.

James A Lewis, Katrina Timlin. Cybersecurity & Cyberwarfare : Preliminary Assessment of National Doctrine and Organization, Center for Strategic and International Studies, United Nations Institute for Disarmament Research (UNIDIR), 2012.

Keir Giles. “Russia's Public Stance on Cyberspace Issues”. NATO CCD COE Publications, 2012.

Karen Evans and Franklin Reeder. A Human Capital Crisis in Cybersecurity : Technical Proficiency Matters. CSIS (Center for Strategic & International Studies, November 15, 2010.

Michael E Ruiz and Richard Redmond, DOD. Cyber Command & Control : A Military Doctrinal Perspective on Collaborative Situation Awareness for Decision Making. Virginia Commonwealth University, USA, 2012.

Michael A. Vane. Cyberspace Operations Concept Capability Plan. TRADOC Pamphet 525-7-8, The United States Army, Feb. 22, 2010.

Richard A. Clarke. Cyber War. An Imprint of Harper Collins Publishers, 2012.

Non-Published Document

“Cyberspace Operations”. Joint Publication 3-12 (R), 2011.

Information Operations, Joint Publication 3-13, Nov. 27, 2012.

J.A. Lewis, K. Timlin. “Cybersecurity and Cyberwarfare 2011 : Preliminary Assessment of National Doctrine and Organization”, Center for Strategic and International Studies, UNIDIR, 2011.

J Reid, and LR Tyler. “Cyber Doctrine : Towards a coherent evolutionary framework for learning resilience”. Institute for Security & Resilience, University College London.

David J Smith. “Russia Cyber Operations”. July 2012.

Vivian Balakrishnan. Singapore’s Cybersecurity Strategy. 2012.

“National Cyber Security Strategies”. Practical Guide on Development and Execution, ENISA, December 2012.

Journals

A M Colarik and L Janczewski. “Establishing Cyber Warfare Doctrine”. Journal of Strategic Security, Vol Warfare : A New Doctrine and Taxonomy”. US Air Force, April 2001.

D K Mulligan and F B Schneider. “Doctrine for Cybersecurity”. Journals The MIT Press. May 15, 2011.

Homeland Security. “Cyber Resilience Review (CRR)”. Method Description and Solf-Assessment User Guide, February 2016.

Ministry of Defence, UK. “Joint Doctrine Note 2/13 : Information Superiority”, Development, Concepts and Doctrine Centre, , August 2013.

Electronic Data Base

Notes on Military Doctrine for Cyberspace Operations in the United States, Michael Warner, 1992-2014, Aug 27, 2015, (Online) Available : [http://www.cyberdefensereview.org/2015/08/27/notes-on-military-doctrine-for-cyberspace/

“Re-Engineering the Cybersecurity Human Capital Crisis”, Morgan Zautua, Marc Dupuis, Barara Endicott-Popovsky, Research Gate, (Online) Available : http://www.researchgate,net/publication/305778185_Reengineering_the_Cybersecurity_Human_Capital_Crisis, ตุลาคม 2559.

ประวัติย่อผู้วิจัย

ชื่อ	พลตรี ปรัชญา เฉลิมวัฒน์
วัน เดือน ปีเกิด	17 ตุลาคม 2504
การศึกษา	โรงเรียนเตรียมทหาร รุ่นที่ 21
	โรงเรียนนายร้อยพระจุลจอมเกล้า รุ่นที่ 32
	โรงเรียนเสนาธิการทหารบก หลักสูตรหลักประจำ ชุดที่ 80
	The George Washington University (Master of Science)
	George Mason University (Doctor of Philosophy)
ประวัติการทำงาน	นายทหารซ่อมบำรุงสายสื่อสาร ส.พัน.9
	อาจารย์ส่วนการศึกษา โรงเรียนนายร้อยพระจุลจอมเกล้า
	ผู้อำนวยการกองพิธีการ สำนักวิเทศน์สัมพันธ์ สำนักนโยบายและแผนกลาโหม
	รองผู้อำนวยการศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม
	กรรมการ การไฟฟ้าส่วนภูมิภาค
	กรรมการ การไฟฟ้านครหลวง
ตำแหน่งปัจจุบัน	ผู้ชำนาญการ สำนักงานปลัดกระทรวงกลาโหม

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์เทคโนโลยี

เรื่อง แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติ

ผู้วิจัย พล.ต.ปรัชญา เฉลิมวัฒน์ หลักสูตร วปอ. รุ่นที่ 60

ตำแหน่ง ผู้ชำนาญการสำนักงานปลัดกระทรวงกลาโหม

ความเป็นมาและความสำคัญของปัญหา

"มิติไซเบอร์" หรือ "ไซเบอร์สเปซ" (Cyber Space) กลายเป็นศัพท์ใหม่ที่ได้รับการยอมรับในสังคมโลกอย่างรวดเร็วและเป็นสิ่งที่ยากที่จะหลีกเลี่ยงการเกี่ยวข้องด้วย ไซเบอร์สเปซมีอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานหลักและ มีคอมพิวเตอร์รวมถึงอุปกรณ์ทุกอย่างเชื่อมต่อเข้ากับระบบเครือข่ายอินเทอร์เน็ตและระบบเครือข่ายย่อยขององค์กร โดยรวมถึงเครือข่ายย่อยส่วนบุคคลและ IoT ข้อมูลจำนวนมหาศาลเดินทางไปในมิติไซเบอร์เพื่อตอบสนองความต้องการในเรื่องความสะดวกสบาย รวดเร็ว การแลกเปลี่ยนข้อมูลข่าวสาร การลดความซับซ้อนของการทำงาน รวมถึงการใช้บริการข้อมูลต่าง ๆ อย่างไรก็ตาม ภัยคุกคามที่ทุกชาติให้ความสำคัญในยุคปัจจุบันคือ ปัญหาความไม่ปลอดภัยในการใช้งานในระบบอินเทอร์เน็ตเนื่องจากมิจฉาชีพต่างก็ปรับตัวให้เข้ากับสภาพแวดล้อมที่เปลี่ยนไปในมิติไซเบอร์ นอกจากนั้นชาติที่เป็นมหาอำนาจต่างก็ยอมรับในเรื่องการยกระดับของภัยคุกคามขึ้นเป็นระดับ "สงครามไซเบอร์" ทั้งในระดับยุทธศาสตร์และระดับปฏิบัติการ ซึ่งบ่อยครั้งเมื่อเกิดความขัดแย้งและการเจรจาทางการทูตไม่สำเร็จสงครามไซเบอร์มักถูกใช้เป็นพลังอำนาจเพื่อแสวงหาข้อยุติในทางอ้อม ความพยายามเสริมสร้างกำลังพลด้านไซเบอร์เพื่อเตรียมรับมือกับภัยคุกคามด้านไซเบอร์ทั้งในระดับกองทัพและระดับความมั่นคงของประเทศต้องเผชิญกับปัญหาการขาดแคลนกำลังพลด้านไซเบอร์อย่างหลีกเลี่ยงไม่ได้ เนื่องจากผู้ที่จะสามารถปฏิบัติการไซเบอร์ได้อย่างจริงจังนั้นต้องมีพื้นฐานทั้งด้านคอมพิวเตอร์ ระบบเครือข่าย กลไกการทำงานของระบบอินเทอร์เน็ต ความชำนาญเฉพาะด้านเช่นการเขียนโปรแกรมในภาษาต่าง ๆ ความรู้เรื่องฮาร์ดแวร์และสถาปัตยกรรมคอมพิวเตอร์ ฐานข้อมูล ความมีไหวพริบ การเข้า/ถอดรหัส และการวิเคราะห์ภัยคุกคามได้เป็นอย่างดี ซึ่งสิ่งต่าง ๆ เหล่านี้มีความลึกซึ้งมากกว่าการสร้างกำลังพลด้านเทคโนโลยีสารสนเทศซึ่งมีความขาดแคลนเป็นทุนเดิมอยู่แล้ว

ในระดับสากลปัญหาการขาดแคลนบุคลากรด้านไซเบอร์ยังคงเป็นปัญหากับทุกประเทศ

สำหรับประเทศไทยนั้นผู้วิจัยเห็นว่าปัญหาการพัฒนากำลังพลด้านไซเบอร์ประกอบด้วยปัญหาย่อยและปัจจัยต่าง ๆ พอสรุปได้ดังนี้

1. การขาดแคลนกำลังพลด้านไซเบอร์ที่ต้องมีทั้งประสบการณ์และความทุ่มเท

2. ความยาก/สลับซับซ้อน/ปริมาณของเนื้อหาในการพัฒนา อบรม ฝึกซ้อม

3. ระยะเวลาที่ต้องใช้ในการพัฒนาบุคลากรไซเบอร์

4. ผู้บริหารไม่ให้ความสนใจอย่างจริงจัง เช่น แต่งตั้งผู้ที่ไม่มีประสบการณ์ด้านไซเบอร์มาบริหารหน่วยงานไซเบอร์ บรรจุบุคคลที่ไม่มีความสามารถด้านไซเบอร์เข้ามาในตำแหน่ง

5. ผู้บริหารหลงประเด็นมุ่งเน้นการสร้างภาพ โครงสร้าง การจัดหาอุปกรณ์ ปรับปรุงสถานที่ทำงาน โดยไม่ได้คำนึงถึงงานที่หน่วยไซเบอร์ต้องปฏิบัติ และแผนพัฒนากำลังพลด้านไซเบอร์

6. ปัญหาสมองไหลหรือการให้ค่าตอบแทนไม่คุ้มกับค่าขีดความสามารถ

งานวิจัยนี้นำเสนอแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ในระดับชาติ โดยคำนึงถึงการบูรณาการแนวความคิดจากประเด็นปัญหาในด้านต่าง ทั้งปัจจัยด้านเวลาการพัฒนาและด้านการเสริมสร้างกำลังพลไซเบอร์ในรูปแบบกองกำลังผสมพลเรือน ตำรวจ ทหาร และการพิจารณาใช้ข้อกฎหมายที่เกี่ยวข้องกับการเตรียมกำลังพลสำรองในระดับชาติ

ผลการวิจัยคาดว่าแนวทางในการพัฒนากำลังพลด้านไซเบอร์ที่ได้นำเสนอในเอกสารวิจัยนี้จะเป็นประโยชน์ต่อการกำหนดกรอบเวลา การวางแผน การดำเนินการเสริมสร้างความแข็งแกร่งด้านไซเบอร์ให้กับประเทศชาติ โดยการใช้ข้อมูลการวิจัยและข้อพิจารณาจากการสำรวจข้อมูลพื้นฐาน การวิเคราะห์ และการสัมภาษณ์เชิงลึกต่อผู้เชี่ยวชาญและผู้บริหารระดับสูงที่เกี่ยวข้องกับกิจการความมั่นคงปลอดภัยไซเบอร์ ซึ่งหากนำไปใช้ปฏิบัติได้อย่างจริงจังจะทำให้สามารถลดปัญหาความขาดแคลนกำลังพลไซเบอร์ และทำให้เกิดความ “ยั่งยืน” ในการเสริมสร้างกำลังพลไซเบอร์ในระยะยาวได้เป็นอย่างดี นอกจากนั้นกำลังพลสำรองไซเบอร์ยังเป็นส่วนสำคัญในการพัฒนาอุตสาหกรรมซอฟท์แวร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศในอนาคต

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาวิเคราะห์แนวทางในการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามไซเบอร์ในระดับชาติ

2. เพื่อเสนอแนวทางการพัฒนากำลังพลไซเบอร์ที่เหมาะสมและมีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี

ขอบเขตของการวิจัย

การวิจัยเรื่อง “แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติ”ประกอบด้วยขอบเขตของการศึกษา ดังนี้

1. ขอบเขตด้านเนื้อหา

1.1 ศึกษาเนื้อหาเกี่ยวกับ แนวคิด ทฤษฎีที่เกี่ยวข้องกับการพัฒนากำลังพลด้านไซเบอร์ ในมุมมองที่สอดคล้องกับยุทธศาสตร์ชาติ

1.2 ศึกษาแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติที่เคยมีการเผยแพร่ไว้แล้ว เพื่อหาข้อเด่นข้อด้อย แล้วนำมาเป็นข้อมูลการวิเคราะห์และการพิจารณาเพื่อกำหนดแนวทางการพัฒนากำลังพลไซเบอร์ใหม่ที่มีความเหมาะสมกับประเทศไทยในศตวรรษที่ 21

1.3 ศึกษาข้อมูลยุทธศาสตร์ไซเบอร์ระดับชาติของประเทศไทย และต่างประเทศ รวมทั้งตัวอย่างที่รัฐบาลไทยเคยได้ยึดถือเป็นแนวทางในการจัดทำยุทธศาสตร์ไซเบอร์ชาติ เพื่อหาข้อเด่น ข้อด้อย และเพื่อนำมาเป็นแนวทางในการกำหนดแนวทางการพัฒนาบุคลากรไซเบอร์ขึ้นใหม่

1.4 ศึกษาและจัดทำแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติที่เหมาะสมและสอดคล้องกับยุทธศาสตร์ไซเบอร์ระดับชาติขึ้นใหม่เพื่อให้สามารถนำมาใช้กับการพัฒนากำลังพลไซเบอร์ในระดับชาติของรัฐบาลไทยและเพื่อนำไปใช้เป็นแนวทางในการวางแผน ดำเนินงาน การพิจารณปัจจัยด้านงบประมาณ สำหรับประเทศไทยต่อไป

1.5 เป็นการศึกษาเฉพาะแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ระดับชาติเป็นหลัก

2. ขอบเขตด้านประชากรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

ผู้วิจัยจะดำเนินการสัมภาษณ์เชิงลึกต่อกลุ่มผู้เชี่ยวชาญที่มีความเชี่ยวชาญทั้งทางวิชาการ ด้านการบริหาร และผู้ที่มีประสบการณ์ในการจัดทำยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหมและระดับชาติ โดยมีผู้เชี่ยวชาญ (KIs) ที่จะสัมภาษณ์เชิงลึก ที่ประกอบด้วยผู้เชี่ยวชาญ 6 คน และผู้เชี่ยวชาญด้านยุทธศาสตร์ชาติจำนวน 7 คน ทั้งนี้จำนวนผู้เชี่ยวชาญด้านวิชาการและด้านยุทธศาสตร์อาจมีการเปลี่ยนแปลงตามความเหมาะสมด้วยข้อจำกัดของเวลาและตารางการปฏิบัติของแต่ละท่าน

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยแบบผสมผสาน (Mixed Method Procedure) ประกอบด้วยการวิจัยเชิงคุณภาพ และการวิจัยเชิงปริมาณ (Qualitative and Quantitative Research) เพื่อค้นหาแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศให้มีความยั่งยืน บุคลากรด้านไซเบอร์มีประสิทธิภาพพร้อมรับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงและถูกยกระดับให้กลายเป็นพลังอำนาจ แห่งชาติ

ขั้นตอนการดำเนินการวิจัย

1. ศึกษาแนวคิด ทฤษฎี ที่เกี่ยวข้องกับการพัฒนาบุคลากรด้านไซเบอร์ของชาติมหาอำนาจ

2. ศึกษารูปแบบ หลักนิยมการทำสงครามไซเบอร์ของชาติต่าง ๆ ประกอบกับแนวคิดของภัยคุกคามไซเบอร์ในวรรณกรรมที่เกี่ยวข้อง

3. สัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ทรงคุณวุฒิที่เป็นผู้บริหารระดับสูง ระดับกลาง รวมถึงผู้เชี่ยวชาญด้านไซเบอร์ เพื่อรับทราบข้อมูลโดยตรงจากผู้มีประสบการณ์ในการบริหารและปฏิบัติงานไซเบอร์โดยตรง

4. จัดการสนทนาไลน์กลุ่ม (Focus Group) ระหว่างผู้บริหารและผู้เชี่ยวชาญด้านไซเบอร์

5. วิเคราะห์ผลที่ได้จากแบบสอบถามผู้ที่เกี่ยวข้องกับการปฏิบัติงานด้านสงครามไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์

6. วิเคราะห์ผลจากการสัมภาษณ์ และการสนทนากลุ่ม

7. วิเคราะห์แนวทางที่เหมาะสมสำหรับการพัฒนาบุคลากรด้านไซเบอร์ของประเทศ

8. สรุปแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศ

ผลการวิจัย

การวิจัยในหัวข้อการพัฒนาบุคลากรด้านไซเบอร์นี้เป็นการวิจัยแบบผสมผสาน (Mixed Method Procedure) ประกอบด้วยการวิจัยเชิงคุณภาพ และการวิจัยเชิงปริมาณ (Qualitative and Quantitative Research) เพื่อค้นหาแนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศให้มีความยั่งยืน บุคลากรด้านไซเบอร์มีประสิทธิภาพพร้อมรับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงและถูกยกระดับให้กลายเป็นพลังอำนาจแห่งชาติ

ผลการสำรวจความคิดเห็นจากกลุ่มประชากรผู้ที่ปฏิบัติงานในหน่วยงานไซเบอร์ ผู้บริหารระดับสูง และการสัมภาษณ์ผู้ทรงคุณวุฒิ ได้ข้อสรุปว่า ส่วนใหญ่มีความคิดเห็นสอดคล้องกับ

ปัญหาที่ผู้วิจัยได้ยกประเด็นขึ้นมา โดยมีบางส่วนเป็นกลาง และไม่มีผู้ที่ความคิดเห็นคัดค้าน ทั้งในเรื่องของประเด็นการขาดแคลนกำลังพลด้านไซเบอร์ที่ต้องมีทั้งประสบการณ์และความทุ่มเท, ความยาก/สลับซับซ้อน/ปริมาณของเนื้อหาในการพัฒนา อบรม ฝึกซ้อม, ระยะเวลาที่ต้องใช้ในการพัฒนาบุคลากรไซเบอร์, ผู้บริหารไม่ให้ความสนใจอย่างจริงจัง เช่น บรรจุบุคคลที่ไม่มีความสามารถด้านไซเบอร์เข้ามาในตำแหน่ง, ผู้บริหารหลงประเด็นไม่ได้คำนึงถึงเนื้องานที่หน่วยไซเบอร์ต้องปฏิบัติ และแผนพัฒนากำลังพลด้านไซเบอร์, และปัญหาสมองไหลหรือการให้ค่าตอบแทนไม่คุ้มกับค่าขีดความสามารถ

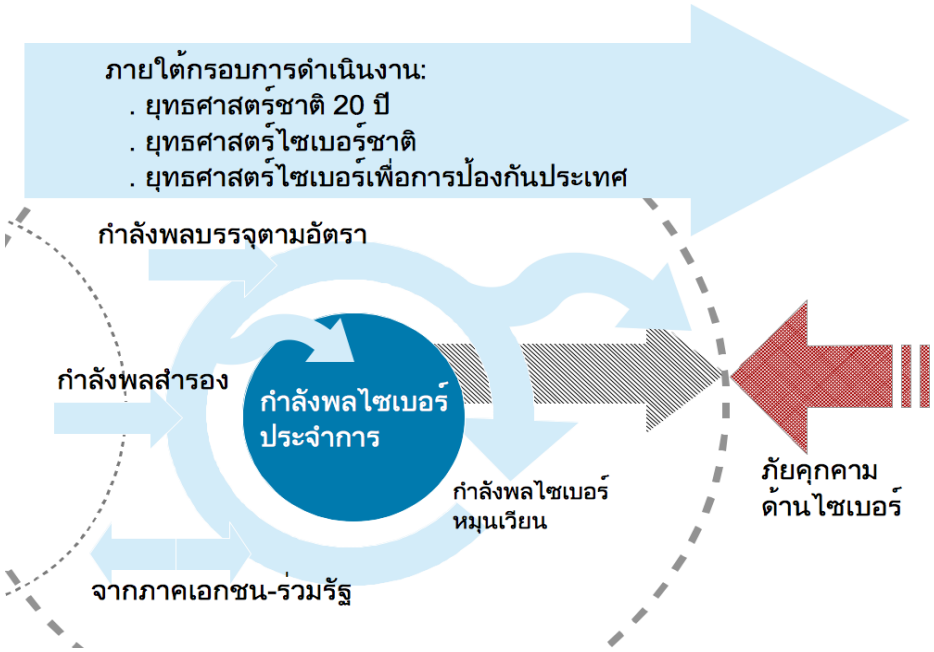
ผลการวิจัยนี้นอกจากได้ศึกษาวิเคราะห์แนวทางในการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามไซเบอร์ในระดับชาติ โดยค้นคว้าการพัฒนาหลักนิยม/ยุทธศาสตร์ไซเบอร์ของชาติต่าง ๆ (ตามรายละเอียดในเอกสารวิจัยในการทบทวนวรรณกรรมที่เกี่ยวข้อง) ยังสามารถสรุปแนวทางในการกำหนดแผนการพัฒนาบุคลากรด้านไซเบอร์ ของประเทศ โดยแนวทางดังกล่าวนี้มีความสอดคล้องกับยุทธศาสตร์ชาติในภาพรวม ยุทธศาสตร์ไซเบอร์ของชาติ และมีการรองรับจากแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องอย่างเด่นชัด อีกทั้งยังมีข้อมูลสนับสนุนจากผลการสัมภาษณ์เชิงลึก และการสอบถามบุคลากรที่เกี่ยวข้องกับงานพัฒนาบุคลกรด้านไซเบอร์ในระดับประเทศ

แนวทางการพัฒนาบุคลากรไซเบอร์

จากผลการสำรวจความคิดเห็นผสมผสานกับข้อมูลการทบทวนวรรณกรรมที่เกี่ยวข้อง ผู้วิจัยสามารถสรุปแนวทางการพัฒนาบุคลากรไซเบอร์ตามโมเดลที่แสดงในรูป แนวทางการพัฒนาบุคลากรไซเบอร์ประกอบด้วยโครงสร้างของกำลังพลไซเบอร์ที่นำเสนอเป็นโมเดลของแนวความคิดที่จะสามารถนำมาประยุกต์ใช้ได้กับการบริหารจัดการกำลังพลไซเบอร์ของประเทศไทย โดยกำลังพลไซเบอร์โดยประกอบด้วยบุคลากรไซเบอร์จาก

1. กำลังพลหลักประจำการ
2. กำลังพลสำรอง และ
3. กำลังพลไซเบอร์จากภาคเอกชนร่วมกับรัฐ หรืออาสาสมัคร

โดยที่กำลังพลไซเบอร์ประจำการคือบุคลากรที่อยู่ในอัตราการจัดของหน่วยนั้นอยู่แล้ว กำลังพลสำรอง ได้แก่บุคลากรที่มิใช่กำลังหลัก เช่น พลทหาร ทหารกองหนุน เป็นต้น ทั้งนี้กำลังพลจากภาครัฐ บริษัท ต้องสามารถทำงานในหน่วยงานภาครัฐรวมถึงได้สิทธิประโยชน์ตามสัดส่วนของเวลาทำงาน เช่น ทำงานที่บริษัทไมโครซอฟท์ 9 เดือน และเข้าทำงานเต็มเวลา ณ ศูนย์ไซเบอร์เป็นเวลา 9 เดือน เป็นต้น



แนวทางการพัฒนาบุคลากรไซเบอร์ที่มีกำลังพลไซเบอร์ประจำการเป็นองค์ประกอบหลักและมีการสนับสนุนกำลังพลจากส่วนต่าง ๆ อย่างต่อเนื่อง มีปัจจัยในความสำเร็จดังนี้

ข้อเสนอแนะ

โดยสรุปข้อเสนอแนะของการวิจัยจำแนกตามประเภทได้แก่ ข้อเสนอแนะเชิงการบริหารบุคลากร ข้อเสนอแนะเชิงนโยบายและแผน ข้อเสนอแนะเชิงกฎ ระเบียบ กฎหมายที่เกี่ยวข้อง

1. ข้อเสนอแนะเชิงการบริหารบุคลากร

1.1 มีการจัดตั้งคณะทำงานเพื่อหาแนวทางร่วมกันระหว่างหน่วยที่เกี่ยวข้องเพื่อให้ได้ข้อสรุปการบริหารจัดการกำลังพลสำรองไซเบอร์ เพื่อนำไปสู่การจัดทำแผนและการปฏิบัติได้อย่างเป็นรูปธรรม

1.2 มีการยื่นข้อเสนอพิเศษให้บุคลากรที่มีพื้นฐานด้านคอมพิวเตอร์อยู่แล้ว เป็นการสร้างทางเลือกให้แก่ผู้ที่คิดจะหลีกเลี่ยงการเกณฑ์ทหารด้วยมีภาพลักษณ์ของการฝึกทหารใหม่ที่มีการใช้ความรุนแรง แต่สามารถเข้ารับการเกณฑ์ทหารด้วยการฝึกแบบพิเศษเพื่อให้สามารถเข้าทำการในลักษณะปฏิบัติการไซเบอร์ได้ทั้งในหน่วยทหารและองค์กรที่มีความต้องการบุคลากรด้านไซเบอร์

2. ข้อเสนอแนะเชิงนโยบายและแผน

2.1 กำหนดแนวทางในการจัดการกำลังพลสำรองที่ปลดประจำการ (ผ่านการเกณฑ์ทหารไปแล้ว) แต่ทำงานในสาขาที่เกี่ยวข้องอยู่แล้ว พิจารณาการเรียกเข้ามาเพื่อเป็นผู้ฝึกให้กับ

“ทหารใหม่ไซเบอร์” ได้เป็นอย่างดี โดยที่เขาเหล่านั้นก็ถือได้ว่ามารับใช้ประเทศชาติในอีกทางหนึ่งในมิติของไซเบอร์

2.2 กำหนดนโยบายกำลังพลสำรองไซเบอร์ เพื่อนำทหารกองหนุน/กองเกินที่มีประสบการณ์ด้านไซเบอร์มาประกอบกำลังในสถานการณ์ฉุกเฉิน และการทำให้บุคลกรไซเบอร์สามารถทำงานได้ทั้งภาครัฐและเอกชน อาศัยหลักการ “แบ่งเวลา” ตามความเหมาะสมหรือความต้องการของบุคคลนั้น ๆ

3. ข้อเสนอแนะเชิงกฎ ระเบียบ กฎหมายที่เกี่ยวข้อง

3.1 พิจารณาปรับปรุงกฎหมายที่เกี่ยวข้อง เช่น พรบ. กำลังสำรอง ๒๕๕๘

3.2 เร่งรัด พ.ร.บ. ไซเบอร์ที่จะทำให้มีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) และจัดตั้งสำนักงาน กปช. เพื่อเป็นองค์รับผิดชอบงานไซเบอร์ในระดับชาติ ทั้งนี้ กปช. ควรขึ้นตรงต่อสำนักนายกรัฐมนตรี และต้องไม่อยู่ในความดูแลของกระทรวงใดกระทรวงหนึ่ง เพื่อให้เกิดความมีเอกภาพในการบังคับบัญชาและการสั่งการ

3.3 พิจารณาปรับปรุงข้อกฎหมายที่เกี่ยวข้องกับการประกาศสถานการณ์ฉุกเฉิน ** สำหรับการบริหารจัดการภัยคุกคามไซเบอร์ที่มีความวิกฤตและกระทบต่อความมั่นคงของชาติ เช่น การให้มีอำนาจเรียกพล/รวมพลไซเบอร์/ใช้ทรัพยากรไซเบอร์จากหน่วยงานเอกชน/หน่วยงานภายนอก