แนวทางการพัฒนาบุคลากรทางด้านไซเบอร์ของศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

เอกสารวิจัยส่วนบุคคล

โดย

นาวาเอกหญิง ศิริเนตร รักษ์วงศ์
ผู้ช่วยผู้อำนวยการกองรักษาความปลอดภัย ศูนย์ไซเบอร์ทหาร
สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

วิทยาลัยการทัพบก
กันยายน 2561

เอกสารวิจัยเรื่อง แนวทางการพัฒนาบุคลากรทางด้านไซเบอร์ของศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

โดย นาวาเอกหญิง ศิริเนตร รักษ์วงศ์

อาจารย์ที่ปรึกษา พันเอก มหศักดิ์ เทพหัสดิน ณ อยุธยา

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2561 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ

พลตรี **ผู้บัญชาการวิทยาลัยการทัพบก**
(ธีระพงษ์ เย็นอุทก)

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก **ประธานกรรมการ**
(มหศักดิ์ เทพหัสดิน ณ อยุธยา)

พลตรี **ผู้ทรงคุณวุฒิที่ปรึกษา**
(ชาติชาย ชัยเกษม)

พันเอกหญิง **กรรมการ**
(ศศพินธุ์ วัชรธรรม)

พันเอกหญิง **กรรมการ**
(ลักษม์บูล บุญคง)

พันเอกหญิง **กรรมการ**
(นวลสมร จรวงษ์)

บทคัดย่อ

ผู้วิจัย นาวาเอกหญิง ศิริเนตร รักษ์วงศ์

เรื่อง แนวทางการพัฒนาบุคลากรทางด้านไซเบอร์ของศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

วันที่ กันยายน 2561 **จำนวนคำ :** 6,474 **จำนวนหน้า :** 29

คำสำคัญ การพัฒนาบุคลากรไซเบอร์

ชั้นความลับ ไม่มีชั้นความลับ

จากการที่หลายประเทศได้ประกาศให้มิติไซเบอร์ เป็นมิติการรบที่ห้าในการทำสงคราม ถ้าหากกองทัพฝ่ายใดฝ่ายหนึ่งของประเทศคู่สงครามไม่สามารถครองมิติไซเบอร์ได้แล้วจะส่งผลกระทบกับการทำการรบในมิติอื่นๆ ตามไปด้วย ปัจจุบันกองบัญชาการกองทัพไทยได้มีการจัดตั้งศูนย์ไซเบอร์ทหาร โดยมีภารกิจปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพไทย

ความท้าทายขององค์กรที่จะพัฒนาบุคลากรให้สอดคล้องกับการเปลี่ยนแปลงอย่างรวดเร็วของไซเบอร์สเปซนั้นยังเป็นประเด็นที่จะต้องให้ความสำคัญอย่างเร่งด่วน บทบาทของบุคลากร แนวทางความก้าวหน้าในวิชาชีพ การระบุความเชี่ยวชาญในแต่ละตำแหน่งที่ความชัดเจน จะสามารถให้การสนับสนุนการปฏิบัติการทางทหารให้มีความเข้มแข็งขึ้นในทุกมิติของการทำสงครามในอนาคต

การพัฒนาบุคลากรไม่ว่าจะเป็นในด้านการจัดการระบบสารสนเทศ (Managing Information Systems) การจ้างบุคลากรที่มีความชำนาญด้านความมั่นคงปลอดภัยไซเบอร์ การวางนโยบายขององค์กร (Establishing Corporate Policy) และการสร้างวัฒนธรรมองค์กร (Building Corporate Culture) ซึ่งการดำเนินการดังกล่าวจะทำให้องค์กรสามารถที่จะทำความเข้าใจพื้นที่ปฏิบัติการของฝ่ายเราและภัยคุกคามในรูปแบบต่างๆ (Identify) ป้องกัน (Protect) ตรวจจับ (Detect) เฝ้าระวัง (Respond) และทำให้ระบบกลับมาใช้งานได้ตามปกติ (Recover) ตาม NIST Cyber Security Framework จากการถูกโจมตีทางไซเบอร์ (Cyber Attacks) ได้อย่างมีประสิทธิภาพ

ABSTRACT

AUTHOR: Capt.Sirinate Rugvong RTN.

TITLE: Cyber Human Resources Development for Cyber Military Center of Royal Thai Armed Forces Headquarters

DATE: September 2018 **WORD COUNT:** 6,474 **PAGES:** 29

KEY TERMS: Cyber Human Resources Development

CLASSIFICATION: Unclassified

Because many countries have declared the cyber as the fifth battle dimension in the war. If any army cannot dominate the cyberspace, then it will affect the battle in other dimensions as well. Currently, the Royal Thai Armed Forces have established a military cyber center. Whose mission is cyber security operation of the Royal Thai Armed Forces Headquarters.

The challenge for organizations to adapt to the rapid change of cyberspace is a matter of urgency. The role of personnel career advancement and Identifying the expertise in each position clearly will help support military operations to be strengthened in all dimensions of future warfare

Human Resource Development, in the field of Information Systems Management (Managing Information Systems), employing skilled cyber security personnel (Cybersecurity Talent), Establishing Corporate Policy, and Building Corporate Culture will help organization have better understanding about our operations. The organization will be able to identify threats, protect, detect, and recover the NIST Cyber Security Framework from Cyber Attacks.

กิตติกรรมประกาศ

การวิจัยเรื่องแนวทางการพัฒนาบุคลากรทางด้านไซเบอร์ของศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย (ศซบ.ทหาร สน.ผบ.ทสส. บก.ทท.) ในฉบับนี้ เป็นการศึกษาแนวทางการพัฒนาบุคลากรทางด้านไซเบอร์ เพื่อตอบสนองต่อยุทธศาสตร์ทหารด้านสงครามไซเบอร์ของกองทัพไทย มาตรการในการดำเนินการและขีดความสามารถที่ต้องการตามประเด็นยุทธศาสตร์ :การป้องกันเชิงรุก สำหรับการปฏิบัติการในมิติไซเบอร์กองทัพไทย เพื่อสร้างผู้ปฏิบัติงานในมิติไซเบอร์กองทัพไทย ให้มีความรู้และทักษะที่เพียงพอต่อการปฏิบัติการในมิติไซเบอร์กองทัพ เอกสารวิจัยครั้งนี้สามารถสำเร็จลุล่วงเป็นอย่างดีได้จากความช่วยเหลือของ พันเอก มหศักดิ์ เทพหัสดิน ณ อยุธยา รองผู้บัญชาการวิทยาลัยการทัพบก (ฝ่ายวิชาการ) ผู้ซึ่งเป็นอาจารย์ที่ปรึกษาของผู้วิจัย กรุณาให้คำแนะนำปรึกษา และข้อคิดเห็นต่างๆ ที่เป็นประโยชน์ต่อการทำวิจัยทุกขั้นตอน และขอขอบพระคุณ พลตรี ชาติชาย ชัยเกษม ผู้อำนวยการศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย ที่ได้กรุณาสละเวลาให้ข้อมูลความรู้ และคำแนะนำที่เป็นประโยชน์อย่างยิ่งในการศึกษาครั้งนี้ รวมทั้งกรุณาพิจารณาและตรวจสอบเอกสารวิจัยให้ถูกต้องสมบูรณ์ยิ่งขึ้น

แนวทางการพัฒนาบุคลากรทางด้านไซเบอร์ของศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

จากการที่หลายประเทศได้ประกาศให้มิติไซเบอร์ (Cyberspace) เป็นมิติการรบที่ห้าในการทำสงคราม ที่จากเดิมมิติหลักในการทำสงครามจะมีเพียงสี่มิติ คือ มิติทางบก มิติทางน้ำ มิติทางอากาศ และมิติทางอวกาศ ทั้งนี้ ประเด็นสำคัญอยู่ที่ว่าการทำสงครามในอนาคตนั้น ถ้าหากกองทัพฝ่ายใดฝ่ายหนึ่งของประเทศคู่สงครามไม่สามารถครองมิติไซเบอร์ได้แล้วจะส่งผลกระทบกับการทำการรบในมิติอื่นๆ ตามไปด้วย หรืออาจทำให้ตกเป็นฝ่ายเสียเปรียบไปโดยปริยาย[1] การปฏิบัติการเพื่อให้ได้เปรียบในมิติไซเบอร์จำเป็นต้องมีการสร้างผู้ปฏิบัติงาน ให้มีความรู้และทักษะที่เพียงพอต่อการปฏิบัติการในมิติไซเบอร์

ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย (ศซบ.ทหาร สน.ผบ.ทสส. บก.ทท.) มีความท้าทายขององค์กรที่จะพัฒนาบุคลากรเพื่อแก้ปัญหาการขาดแคลนบุคลากรที่มีความรู้เชี่ยวชาญทางด้านไซเบอร์ โดยการพัฒนาความรู้และทักษะให้สอดคล้องกับการเปลี่ยนแปลงอย่างรวดเร็วของไซเบอร์สเปซ เป็นประเด็นที่จะต้องให้ความสำคัญอย่างเร่งด่วน รวมทั้งการจัดองค์กรด้านไซเบอร์ การกำหนดแนวทางการรับราชการ การกำหนดขอบเขตแนวทางการปฏิบัติ ความเชี่ยวชาญในแต่ละตำแหน่งที่ชัดเจน มีมาตรการจูงใจ การตอบแทนที่เหมาะสม การได้รับเงินเพิ่มพิเศษ การได้รับประดับเครื่องหมายแสดงความสามารถ ให้กับผู้เชี่ยวชาญด้านไซเบอร์ จะสามารถให้การสนับสนุนการปฏิบัติการทางทหารให้มีความเข้มแข็งขึ้นในทุกมิติของการทำสงครามในอนาคต ผลลัพธ์จากการวิจัยเรื่อง แนวทางการพัฒนาบุคลากรทางด้านไซเบอร์ของศูนย์ไซเบอร์ทหาร ฯ ในฉบับนี้ ได้แนวทางการพัฒนาบุคลากร การเพิ่มพูนความรู้และทักษะทางด้านไซเบอร์ ของแผนกรักษาความปลอดภัย กองรักษาความปลอดภัย ซึ่งเป็นหัวใจสำคัญของการปฏิบัติงานด้านไซเบอร์ คือ

1.1 การฝึกอบรมเพื่อให้บุคลากรสามารถปฏิบัติงานได้ตามภารกิจ

1.2 สมรรถนะที่จำเป็นสำหรับบุคลากรที่ปฏิบัติงาน

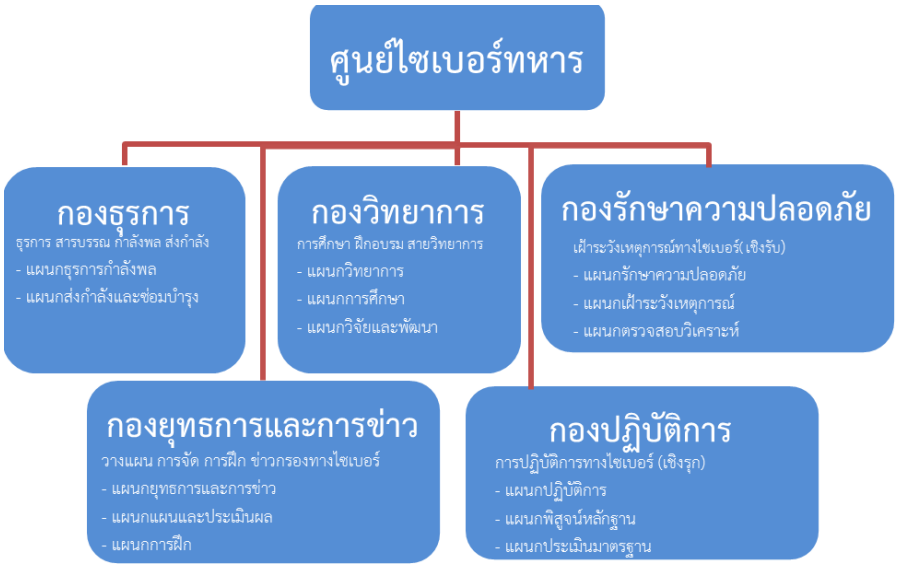
รูปที่ 1 แผนผังแสดงองค์ประกอบหลักของยุทธศาสตร์ทหารด้านสงครามไซเบอร์ กองทัพไทย พ.ศ. 2558 [1]

เพื่อตอบสนองต่อยุทธศาสตร์ทหารด้านสงครามไซเบอร์ของกองทัพไทย พ.ศ.2558 องค์ประกอบหลักของยุทธศาสตร์ทหารด้านสงครามไซเบอร์ มีดังนี้ [2]

1. มาตรการในการดำเนินการและขีดความสามารถที่ต้องการตามประเด็นยุทธศาสตร์ : การป้องกันเชิงรุกสำหรับการปฏิบัติการในมิติไซเบอร์กองทัพไทย เพื่อสร้างผู้ปฏิบัติงานในมิติไซเบอร์กองทัพไทย ให้มีความรู้และทักษะที่เพียงพอต่อการปฏิบัติการในมิติไซเบอร์กองทัพไทย โดยการพัฒนาระบบฝึกศึกษาสำหรับผู้ปฏิบัติงานในมิติไซเบอร์กองทัพไทย ได้แก่ การจัดตั้งสายวิทยาการด้านไซเบอร์ การจัดตั้งโรงเรียนสายวิทยาการด้านไซเบอร์ (RTArF CyberWarfare School) การสร้างความร่วมมือด้านการฝึกศึกษาร่วมกันทั้งภายในและภายนอกกองทัพไทย และการพัฒนาระบบฝึกจำลองยุทธร่วมทางไซเบอร์ (RTArF Cyber Range)
2. มาตรการในการดำเนินการและขีดความสามารถที่ต้องการสำหรับการปฏิบัติการในมิติไซเบอร์กองทัพไทย ตามประเด็นยุทธศาสตร์ : การผนึกกำลังป้องกันประเทศสำหรับการปฏิบัติการในมิติไซเบอร์กองทัพไทย กำหนดบทบาท หน้าที่ ความรับผิดชอบระหว่างหน่วยงานด้านไซเบอร์กองทัพไทย พัฒนาระบบการรับรองความสามารถทางไซเบอร์กองทัพไทย (RTArF Cyber Certification) เพื่อให้สามารถจำแนกระดับความชำนาญ

ของผู้ปฏิบัติงานในมิติไซเบอร์กองทัพไทย สร้างมาตรฐานของผู้ปฏิบัติงานฯ ให้อยู่ในระดับสากล และเพิ่มความน่าเชื่อถือในการปฏิบัติงานร่วมกับหน่วยงานด้านไซเบอร์นอกกระทรวงกลาโหม

ทั้งนี้เพื่อให้องค์กรสามารถที่จะทำความเข้าใจพื้นที่ปฏิบัติการของฝ่ายเราและภัยคุกคามในรูปแบบต่างๆ (Identify), ป้องกัน (Protect), ตรวจจับ (Detect), เฝ้าระวัง (Respond) และทำให้ระบบกลับมาใช้งานได้ตามปกติ (Recover) โดยในการวิจัยนี้อ้างอิงตามมาตรฐาน NIST Cyber Security Framework ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐฯ (National Institute of Standards and Technology – NIST) [3]



ศูนย์ไซเบอร์ทหารฯ มีหน้าที่เสนอความเห็น นโยบาย วางแผน อำนวยการ ประสานงาน บูรณาการปฏิบัติการ และกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ ดำเนินการจัดการฝึกศึกษา บูรณาการด้านการข่าวกรองทางไซเบอร์ และเป็นสายวิทยาการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพไทย รวมทั้งปฏิบัติงานอื่นที่ได้รับมอบหมาย มีผู้อำนวยการศูนย์ไซเบอร์ทหารเป็นผู้บังคับบัญชารับผิดชอบ มีการแบ่งส่วนราชการออกเป็น 5 กองคือ [4]

1. กองธุรการ มีหน้าที่ดำเนินการเกี่ยวกับการธุรการ การสารบรรณ การกำลังพล การบริการ การส่งกำลัง การซ่อมบำรุง และการรักษาความปลอดภัย
2. กองยุทธการและการข่าว มีหน้าที่พิจารณาเสนอความเห็น นโยบาย วางแผน อำนวยการ ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับการปฏิบัติการยุทธ์ร่วมทางไซเบอร์ การวางแผนทางทหาร การจัดกำลัง การใช้กำลังทางไซเบอร์ การประเมิน

ความพร้อมรบ การป้องกันทางไซเบอร์ การฝึกทางไซเบอร์ และการปฏิบัติการด้านข่าวกรองทางไซเบอร์

3. กองวิทยาการ มีหน้าที่วางแผน อำนวยการ ประสานงาน กำกับดูแล และดำเนินการวิเคราะห์ วิจัยพัฒนา จัดทำหลักนิยม และเผยแพร่ เกี่ยวกับการปฏิบัติการทางไซเบอร์ ความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการดำเนินการเกี่ยวกับการกำหนดคุณลักษณะเฉพาะของสิ่งอุปกรณ์ทางด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้เหมาะสมกับการปฏิบัติงานของกองบัญชาการกองทัพไทยเป็นส่วนรวม ตลอดจนทำหน้าที่วางแผน จัดทำ พัฒนาและบริหารหลักสูตร ดำเนินการให้การศึกษาฝึกอบรม จัดตำราสื่อการเรียนการสอนของวิทยาการทางด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่กำลังพลภายในกองบัญชาการกองทัพไทย และส่วนราชการที่เกี่ยวข้อง
4. กองปฏิบัติการ มีหน้าที่พิจารณาเสนอความเห็น วิเคราะห์ วางแผน ประสานงานและปฏิบัติการร่วมทางไซเบอร์ ในระดับกองบัญชาการกองทัพไทย และกองทัพไทย
5. กองรักษาความปลอดภัย มีหน้าที่ดำเนินการตรวจสอบ วิเคราะห์ ป้องกัน กู้คืน และประเมินการดำเนินงานด้านการรักษาความปลอดภัยทางไซเบอร์ จัดทำแนวทางหลักการ ระเบียบ มาตรฐานและแผนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพไทย รวมทั้งพิจารณาเสนอแนะ การดำเนินการต่อภัยคุกคาม ที่มีผลกระทบต่อระบบสารสนเทศของกองบัญชาการกองทัพไทย

สถานภาพด้านกำลังพล

- ปริมาณ: ยังไม่พอเพียง (อัตราเต็ม 151 อัตราบรรจุจริง 104 คิดเป็นร้อยละ 68.87)
- คุณภาพ: อยู่ระหว่างพัฒนาทักษะ

แนวทางการพัฒนาบุคลากรทางด้านไซเบอร์

จากประเด็นยุทธศาสตร์ เพื่อสร้างผู้ปฏิบัติงานในมิติไซเบอร์กองทัพไทย ให้มีความรู้และทักษะที่เพียงพอต่อการปฏิบัติการในมิติไซเบอร์กองทัพไทย โดยการพัฒนาระบบฝึกศึกษาสำหรับผู้ปฏิบัติงานในมิติไซเบอร์กองทัพไทย และ กำหนดบทบาท หน้าที่ ความรับผิดชอบระหว่างหน่วยงานด้านไซเบอร์กองทัพไทย พัฒนาระบบการรับรองความสามารถทางไซเบอร์กองทัพไทย (RTArF Cyber Certification) เพื่อให้สามารถจำแนกระดับความชำนาญของผู้ปฏิบัติงานในมิติไซเบอร์กองทัพไทย สร้างมาตรฐานของผู้ปฏิบัติงานให้อยู่ในระดับสากล

และเพิ่มความน่าเชื่อถือในการปฏิบัติงานร่วมกับหน่วยงานด้านไซเบอร์นอกกระทรวงกลาโหม โดยการปฏิบัติการในมิติไซเบอร์ ของศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย แบ่งเป็น 6 ส่วน ดังนี้

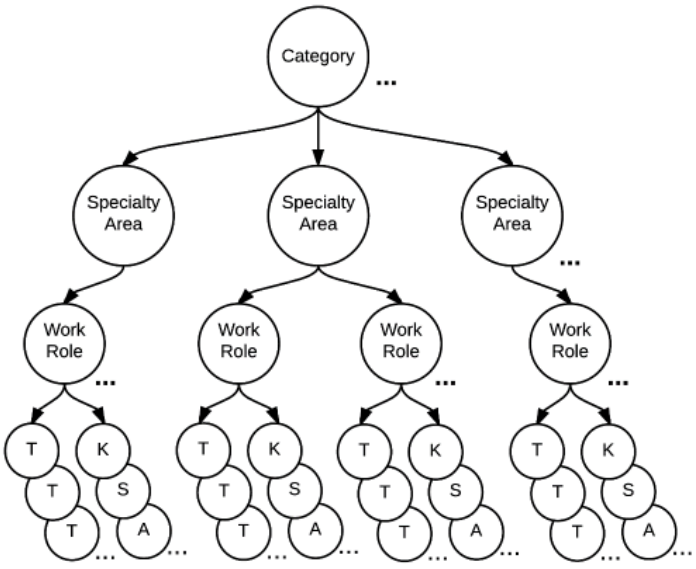
1. ส่วนบังคับบัญชา
2. ส่วนเฝ้าระวัง (ซึ่งถือเป็นหัวใจสำคัญของการปฏิบัติการด้านการรักษาความปลอดภัยทางไซเบอร์ (Cyber Security))
3. ส่วนรับมือเหตุการณ์ทางไซเบอร์
4. ส่วนพิสูจน์หลักฐานทางดิจิทัล
5. ส่วนงานข่าวกรองทางไซเบอร์
6. ส่วนประเมินตนเอง

ในงานวิจัยฉบับนี้มีการระบุงาน (Tasks), ความรู้ (Knowledge), ทักษะ (Skills), ความสามารถ (Abilities) เพื่อรองรับการปฏิบัติการในมิติไซเบอร์ของศูนย์ไซเบอร์ทหารฯ ดังนี้

งาน (Tasks)	1. การวางระบบป้องกันภัยคุกคามทางไซเบอร์ 2. เชื่อมต่อระบบป้องกันเข้ากับระบบเฝ้าระวัง 3. เฝ้าระวังภัยคุกคามทางไซเบอร์ที่มีต่อระบบเทคโนโลยีสารสนเทศของหน่วย Data collection and validation รวบรวมข้อมูลเกี่ยวกับ Alert ที่เกิดขึ้น 3.1 Alert Investigation วิเคราะห์และตรวจสอบ alert ที่เกิดขึ้นว่าเกี่ยวข้องกับเหตุการณ์ด้านความปลอดภัยหรือไม่ 3.2 Correlation หาความสัมพันธ์ของ alert นั้น ว่าเกี่ยวข้องกับภัยคุกคามหรือไม่
ความรู้ (Knowledge)	1. เข้าใจระบบเครือข่ายสารสนเทศของหน่วย 2. เข้าใจระบบการป้องกันภัยคุกคามที่มีต่อระบบเครือข่ายสารสนเทศของหน่วย 3. เข้าใจระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ (SIEM)
ทักษะ (Skills)	1. เครือข่ายสารสนเทศ (IT Network) 2. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

ความสามารถ (Abilities)	1. สามารถใช้ระบบ SIEM (Security Information and Event Management) เป็นระบบจัดเก็บและวิเคราะห์ข้อมูลแบบเรียลไทม์ เพื่อนำข้อมูลเหล่านั้นไปใช้ในการปฏิบัติการทางไซเบอร์) ได้ 2. ออกแบบระบบป้องกันภัยคุกคาม 3. วางระบบป้องกัน 4. ออกแบบระบบเฝ้าระวัง 5. วางระบบเฝ้าระวัง 6. สามารถแก้ไข Alert จากระบบ SIEM และระบบป้องกันได้

เนื่องจากงานทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีความหลากหลาย การพัฒนาหน่วยงานให้สามารถปฏิบัติภารกิจทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ ส่วนหนึ่งจะต้องสามารถระบุได้ว่าบุคลากรที่ปฏิบัติงานจะต้องมีความรู้ ความสามารถอะไรบ้าง เอกสารวิจัยฉบับนี้ใช้ขอบเขตงานของ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐฯ (National Institute of Standards and Technology – NIST) ซึ่งได้กำหนดขอบเขต การปฏิบัติงานทางด้านความมั่นคงปลอดภัยไซเบอร์ (National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework) ได้อย่างหมาะสม เป็นมาตรฐานเดียวกัน และเป็นแนวทางในการระบุว่างานแต่ละบทบาทต้องการความรู้ ความเชี่ยวชาญ อะไรบ้าง



ความสัมพันธ์ระหว่าง NICE Framework Components [5]

ตามรูป NICE Framework Component ได้จัดหมวดหมู่ภารกิจเป็น 7 ประเภทงาน (categories) ในแต่ละประเภทงาน (categories) แบ่งย่อยเป็นความเชี่ยวชาญ (specialty area) และความเชี่ยวชาญ (specialty area) มีหลายบทบาทงาน (work role) ซึ่งแต่ละบทบาทงาน (work role) จะมีการระบุงาน - T (Tasks) , ความรู้ - K (Knowledge), ทักษะ - S (Skills), ความสามารถ - A (Abilities) [6] ที่จำเป็นและเกี่ยวข้องกับภารกิจนั้น

NICE Framework Workforce Categories ได้กำหนดขอบเขตการทำงานเป็น 7 ประเภทงาน (categories) ดังนี้

1. การจัดหาอย่างปลอดภัย - Securely Provision (SP) กำหนดแนวคิด ออกแบบ สร้างระบบรักษาความปลอดภัย จัดซื้อจัดหา สร้างระบบสารสนเทศด้านความปลอดภัย รับผิดชอบการพัฒนาระบบและเครือข่าย
2. การใช้งานและบำรุงรักษา - Operate and Maintain (OM) สนับสนุนการบริหารจัดการ และ บำรุงรักษาเพื่อให้สมรรถนะและความปลอดภัยของระบบสารสนเทศมีประสิทธิภาพและประสิทธิผล
3. การดูแลและควบคุม - Oversee and Govern (OV) บริหาร กำหนดทิศทาง นโยบาย และพัฒนาองค์กรเพื่อให้งานทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีประสิทธิภาพ
4. การป้องกันระบบ - Protect and Defend (PR) ระบุ วิเคราะห์ และลดความเสี่ยงต่อระบบสารสนเทศและเครือข่าย
5. การวิเคราะห์ - Analyze ทำการตรวจสอบและประเมินผลข้อมูลทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อประโยชน์ทางการข่าว
6. การรวบรวมข้อมูลและปฏิบัติการข่าว - Collect and Operate ทำการรวบรวมข้อมูลเพื่อพัฒนาการข่าว
7. การสืบสวน - Investigate สืบสวนเหตุการณ์ หรือ อาชญากรรมทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และหลักฐานทางดิจิตัล

เพื่อให้สามารถปฏิบัติภารกิจทางมิติไซเบอร์ได้อย่างมีประสิทธิภาพ จะขอยกตัวอย่างงาน (Tasks) ในส่วนเฝ้าระวังภัยคุกคามทางไซเบอร์ ซึ่งถือเป็นหัวใจสำคัญของการปฏิบัติการด้านการรักษาความปลอดภัยทางไซเบอร์ (Cyber Security) มีดังนี้

1. การวางระบบป้องกันภัยคุกคามทางไซเบอร์
2. เชื่อมต่อระบบป้องกันเข้ากับระบบเฝ้าระวัง

3. เฝ้าระวังภัยคุกคามทางไซเบอร์ที่มีต่อระบบเทคโนโลยีสารสนเทศของหน่วย
4. Data collection and validation รวบรวมข้อมูล เกี่ยวกับ Alert ที่เกิดขึ้น
5. Alert Investigation วิเคราะห์และตรวจสอบ alert ที่เกิดขึ้น ว่าเกี่ยวข้องกับเหตุการณ์ด้านความปลอดภัยหรือไม่
6. Correlation หาความสัมพันธ์ของ alert นั้น ว่าเกี่ยวข้องกับภัยคุกคามหรือไม่

ซึ่งงาน (Tasks) ตามข้างบน เมื่อเทียบกับ NICE Framework จะอยู่ในส่วนของ

NIST SP 800-181 NICE FRAMEWORK

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Cyber Defense Analyst	PR-CDA-001	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

ประเภทของงานหลัก (Category) – Protect and Defend (PR)
ความเชี่ยวชาญ (Specialty Area) – Cyber Defense Analysis (CDA)
บทบาทงาน (Work Role) – Cyber Defense Analyst
รหัสบทบาทงาน (Work Role ID) – PR-CDA-001
รายละเอียดบทบาทงาน (Work Role Description) – Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environment for the purposes of mitigating threats.

ข้อมูลจากตารางข้างบนจะได้รายละเอียดเกี่ยวกับ งาน(Tasks), ความรู้ (Knowledge), ทักษะ (Skills), ความสามารถ (Abilities) ดังตารางต่อไปดังนี้

NIST SP 800-181 NICE FRAMEWORK

B.4 Protect and Defend (PR)

Work Role Name	**Cyber Defense Analyst**
Work Role ID	**PR-CDA-001**
Specialty Area	**Cyber Defense Analysis (CDA)**
Category	**Protect and Defend (PR)**
Work Role Description	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats.
Tasks	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Skills	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Abilities	A0010, A0015, A0066, A0123, A0128, A0159

จากตารางข้างบนจะได้รหัส งาน (Tasks), ความรู้ (Knowledge), ทักษะ (Skills), ความสามารถ (Abilities) ดังนี้

งาน (Tasks) - T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548

ความรู้ (Knowledge) - K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624

ทักษะ (Skills) - S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370

ความสามารถ (Abilities) - A0010, A0015, A0066, A0123, A0128, A0159

นำรหัสของ Tasks ที่ได้ไปเทียบกับตาราง NICE Framework ต่อไป ดังนี้

A.4 NICE Framework Tasks

Table 4 provides a listing of all the tasks that have been identified as being part of a cybersecurity work role. Each work role includes a subset of the tasks listed here. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 4 - NICE Framework Tasks

Task ID	Task Description
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.
T0006	Advocate organization's official position in legal and legislative proceedings.
T0007	Analyze and define data requirements and specifications.
T0008	Analyze and plan for anticipated changes in data capacity requirements.

นำรหัสของ Knowledge ที่ได้ไปเทียบกับตาราง NICE Framework ต่อไป ดังนี้

A.5 NICE Framework Knowledge Descriptions

Table 5 provides a listing of the various kinds of information applied directly to the performance of a function. Selected knowledge ID/descriptions from this list are included for every work role in the Detailed work role Listing in Appendix B. The first six are common to all the cybersecurity work roles. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 5 - NICE Framework Knowledge Descriptions

KSA ID	Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
K0005	Knowledge of cyber threats and vulnerabilities.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.
K0007	Knowledge of authentication, authorization, and access control methods.
K0008	Knowledge of applicable business processes and operations of customer organizations.
K0009	Knowledge of application vulnerabilities.
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
K0012	Knowledge of capabilities and requirements analysis.

นำรหัสของ Skill ที่ได้ไปเทียบกับตาราง NICE Framework ต่อไป ดังนี้

A.6 NICE Framework Skills Descriptions

Table 6 provides a listing of cybersecurity skills. A skill is the observable competence to perform a learned psychomotor act. Selected skills descriptions from this list are included for each work role in the Detailed work role Listing in Appendix B. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 6 - NICE Framework Skills Descriptions

Skill ID	Description
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
S0002	Skill in allocating storage capacity in the design of data management systems.
S0003	Skill of identifying, capturing, containing, and reporting malware.
S0004	Skill in analyzing network traffic capacity and performance characteristics.
S0005	Skill in applying and incorporating information technologies into proposed solutions.
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0007	Skill in applying host/network access controls (e.g., access control list).
S0008	Skill in applying organization-specific systems analysis principles and techniques.
S0009	Skill in assessing the robustness of security systems and designs.
S0010	Skill in conducting capabilities and requirements analysis.
S0011	Skill in conducting information searches.
S0012	Skill in conducting knowledge mapping (e.g., map of knowledge repositories).
S0013	Skill in conducting queries and developing algorithms to analyze data structures.
S0014	Skill in conducting software debugging.

นำรหัสของ Ability ที่ได้ไปเทียบกับตาราง NICE Framework ต่อไป ดังนี้

A.7 NICE Framework Ability Descriptions

Table 7 provides a listing of cybersecurity abilities. Ability is competence to perform an observable behavior or a behavior that results in an observable product. Selected ability descriptions from this list are included in each work role in the Detailed work role Listing in Appendix B. This listing will be updated periodically [1]. The definitive source for the most current version of this material can be found in the Reference Spreadsheet for NIST Special Publication 800-181 [4].

Table 7 - NICE Framework Ability Descriptions

Ability ID	Description
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
A0002	Ability to match the appropriate knowledge repository technology for a given application or environment.
A0003	Ability to determine the validity of technology trend data.
A0004	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.
A0005	Ability to decrypt digital data collections.
A0006	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures.
A0007	Ability to tailor code analysis for application-specific concerns.

สุดท้ายจะได้งาน (Tasks) ของผู้ปฏิบัติงานทางด้านเฝ้าระวังภัยคุกคามทางไซเบอร์ที่มีต่อระบบเทคโนโลยีสารสนเทศของหน่วย ดังนี้

งาน (Tasks) - T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548

รหัสงาน (Task ID)	รายละเอียด
T0020	พัฒนาเนื้อหาสำหรับเครื่องมือป้องกันไซเบอร์
T0023	อธิบายลักษณะและวิเคราะห์เครือข่ายเพื่อระบุกิจกรรมผิดปกติและภัยคุกคามที่อาจเกิดขึ้นกับทรัพยากรเครือข่าย
T0043	ประสานงานกับเจ้าหน้าที่ป้องกันไซเบอร์ทั่วทั้งองค์กรเพื่อตรวจสอบความถูกต้องของการแจ้งเตือนระบบเครือข่าย

รหัสงาน (Task ID)	รายละเอียด
T0088	ตรวจสอบให้แน่ใจว่าผลิตภัณฑ์ที่ใช้เทคโนโลยี cybersecurity หรือเทคโนโลยีการควบคุมการรักษาความปลอดภัยแบบอื่น ๆ ลดความเสี่ยงที่ระบุไว้ในระดับที่ยอมรับได้
T0155	เอกสารและเหตุการณ์ที่เพิ่มขึ้น (รวมถึงประวัติเหตุการณ์สถานะและผลกระทบที่อาจเกิดขึ้นสำหรับการดำเนินการต่อไป) ที่อาจส่งผลต่อสิ่งแวดล้อมอย่างต่อเนื่อง
T0164	ดำเนินการวิเคราะห์แนวโน้มไซเบอร์และรายงาน
T0166	ดำเนินการหาความสัมพันธ์เกี่ยวกับเหตุการณ์โดยใช้ข้อมูลที่รวบรวมมาจากหลายแหล่งภายในองค์กรเพื่อรับทราบสถานการณ์และกำหนดประสิทธิภาพของการโจมตีที่สังเกตได้
T0178	ดำเนินการตรวจสอบด้านความปลอดภัยและระบุช่องโหว่ด้านความปลอดภัยในสถาปัตยกรรมความปลอดภัย เพื่อเป็นคำแนะนำสำหรับการรวมไว้ในกลยุทธ์การลดความเสี่ยง
T0187	วางแผนและแนะนำปรับเปลี่ยนตามผลการฝึกหรือสภาพแวดล้อมของระบบ
T0198	จัดเตรียมรายงานสรุปประจำวันเกี่ยวกับกิจกรรมเครือข่ายและกิจกรรมที่เกี่ยวข้องกับการปฏิบัติในการป้องกันไซเบอร์
T0214	รับและวิเคราะห์การแจ้งเตือนเครือข่ายจากแหล่งต่างๆภายในองค์กรและพิจารณาสาเหตุที่เป็นไปได้ของการแจ้งเตือนดังกล่าว
T0258	ให้การตรวจสอบระบุตัวตนและแจ้งเตือนถึงการโจมตี / การบุกรุกที่เป็นไปได้กิจกรรมผิดปกติและใช้งานผิดประเภทและแยกแยะเหตุการณ์และเหตุการณ์เหล่านี้ออกจากกิจกรรมที่ไม่เป็นอันตราย
T0259	ใช้เครื่องมือป้องกันไซเบอร์เพื่อติดตามและวิเคราะห์กิจกรรมของระบบอย่างต่อเนื่องเพื่อระบุกิจกรรมที่เป็นอันตราย
T0260	วิเคราะห์กิจกรรมที่เป็นอันตรายที่ระบุเพื่อหาจุดอ่อน วิธีการนำไปใช้ประโยชน์ หาผลกระทบต่อระบบและข้อมูล

รหัสงาน (Task ID)	รายละเอียด
T0290	กำหนดกลวิธีเทคนิคและขั้นตอน (tactics, techniques, and procedures - TTPs) สำหรับชุดการบุกรุก
T0291	ตรวจสอบ topologies เครือข่ายเพื่อทำความเข้าใจเกี่ยวกับการไหลของข้อมูลผ่านเครือข่าย
T0292	แนะนำการแก้ไขช่องโหว่ของสภาพแวดล้อม
T0293	ระบุและวิเคราะห์ความผิดปกติในการเข้าชมเครือข่ายโดยใช้ metadata. ข้อมูลเมทา(อังกฤษ: metadata) หมายถึง ข้อมูลหรือสารสนเทศที่ถูกจัดทำขึ้นอย่างมีโครงสร้างเพื่อใช้ในการบรรยายทรัพยากรสารสนเทศ ในด้านลักษณะเนื้อหา และบริบทที่เกี่ยวข้องซึ่งได้แก่ลักษณะทางกายภาพและการผลิตทรัพยากรสารสนเทศ ตลอดจนความสัมพันธ์ (Relation) ระหว่างองค์ประกอบที่ใช้ในการบรรยายทรัพยากรสารสนเทศ โดยมีวัตถุประสงค์เพื่อตอบสนองการทำงาน คือ การสืบค้น และการบริหารจัดการ ซึ่งประกอบไปด้วยการกำหนดสิทธิในการใช้ การกำหนดความคุ้มครองทรัพย์สินทางปัญญา การสงวนรักษา [8]
T0294	ดำเนินการวิจัยการวิเคราะห์และหาความสัมพันธ์ในชุดข้อมูลต้นฉบับทั้งหมดที่หลากหลาย (เพื่อบ่งชี้และแจ้งเตือน)
T0295	ตรวจสอบการแจ้งเตือนของระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS) กับเครือข่ายโดยใช้เครื่องมือวิเคราะห์แพ็คเก็ต
T0296	แยกและลบมัลแวร์
T0297	ระบุแอ็พพลิเคชันและระบบปฏิบัติการของอุปกรณ์เครือข่ายบนพื้นฐานการรับส่งข้อมูลเครือข่าย
T0298	สร้างการโจมตีหรือกิจกรรมที่เป็นอันตรายขึ้นจากการรับส่งข้อมูลเครือข่าย
T0299	ระบุกิจกรรมการเชื่อมโยงเครือข่ายและระบบปฏิบัติการ (OS)
T0310	ช่วยในการสร้างลายเซ็นที่สามารถนำไปใช้กับเครื่องมือป้องกันเครือข่ายในโลกไซเบอร์เพื่อตอบสนองต่อภัยคุกคามใหม่หรือที่สังเกตได้ภายในระบบเครือข่ายหรือวงล้อม

รหัสงาน (Task ID)	รายละเอียด
T0332	แจ้งให้ทราบถึงผู้ที่ได้รับมอบหมาย ผู้ตอบสนองต่อเหตุการณ์ไซเบอร์และทีมงานฝ่ายบริการด้านความปลอดภัยไซเบอร์ ของเหตุการณ์ไซเบอร์ที่สงสัยและกล่าวถึงประวัติเหตุการณ์สถานะและผลกระทบที่อาจเกิดขึ้นสำหรับการดำเนินการต่อไปตามแผนการตอบสนองต่อเหตุการณ์ในโลกไซเบอร์ขององค์กร
T0469	วิเคราะห์และรายงานแนวโน้มความมั่นคงขององค์กร
T0470	วิเคราะห์และรายงานแนวโน้มแนวโน้มความปลอดภัยของระบบ
T0503	ตรวจสอบแหล่งข้อมูลภายนอก (เช่นเว็บไซต์ผู้ให้บริการการป้องกันไซเบอร์, ทีมกู้ภัยฉุกเฉินของคอมพิวเตอร์, โฟกัสด้านความปลอดภัย) เพื่อป้องกันภัยคุกคามไซเบอร์และพิจารณาว่าปัญหาด้านความปลอดภัยใดที่อาจส่งผลกระทบต่อองค์กร
T0504	ประเมินและตรวจสอบความปลอดภัยเกี่ยวกับการปฏิบัติตามระบบและการทดสอบ
T0526	ให้คำแนะนำด้านความปลอดภัยไซเบอร์บนพื้นฐานตามภัยคุกคามและช่องโหว่ที่สำคัญ
T0545	ทำงานร่วมกับผู้มีส่วนได้ส่วนเสียในการแก้ไขปัญหาความปลอดภัยของคอมพิวเตอร์และการปฏิบัติตามข้อกำหนด
T0548	ให้คำแนะนำและข้อมูลสำหรับการกู้คืนภัยพิบัติ การจัดเตรียมและความต่อเนื่องของแผนการดำเนินงาน

ความรู้ (Knowledge) - K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261,

K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624

รหัสความรู้ (KSA ID)	รายละเอียด
K0001	ความรู้เกี่ยวกับแนวคิดและโปรโตคอลเครือข่ายคอมพิวเตอร์และวิธีการรักษาความปลอดภัยเครือข่าย
K0002	ความรู้เกี่ยวกับกระบวนการบริหารความเสี่ยง (เช่นวิธีประเมินและบรรเทาความเสี่ยง)
K0003	ความรู้เกี่ยวกับกฎหมายข้อบังคับนโยบายและจริยธรรมที่เกี่ยวข้องกับความปลอดภัยในโลกไซเบอร์และความเป็นส่วนตัว
K0004	ความรู้เกี่ยวกับการรักษาความปลอดภัยไซเบอร์และความเป็นส่วนตัว
K0005	ความรู้เกี่ยวกับภัยคุกคามและช่องโหว่
K0006	ความรู้เกี่ยวกับผลกระทบการดำเนินงานเฉพาะของ lapses cybersecurity
K0007	ความรู้เกี่ยวกับการรับรอง, การอนุมัติ และวิธีการควบคุมการเข้าถึง
K0013	ความรู้เกี่ยวกับเครื่องมือการป้องกันไซเบอร์, การประเมินความเสี่ยงและความสามารถ
K0015	ความรู้เกี่ยวกับคอมพิวเตอร์อัลกอริทึม
K0018	ความรู้เกี่ยวกับอัลกอริทึมการเข้ารหัส
K0019	ความรู้เกี่ยวกับวิทยาการเข้ารหัสและแนวคิดการจัดการคีย์รหัสลับ
K0024	ความรู้เกี่ยวกับระบบฐานข้อมูล
K0033	ความรู้เกี่ยวกับกลไกการควบคุมการเข้าถึงโฮสต์ / เครือข่าย (เช่นรายการควบคุมการเข้าถึงรายการความสามารถ)
K0040	ความรู้เกี่ยวกับแหล่งเผยแพร่ข้อมูลที่มีช่องโหว่ (เช่นการแจ้งเตือนคำแนะนำ errata และประกาศ)
K0042	ความรู้เกี่ยวกับการตอบสนองต่อเหตุการณ์และวิธีการจัดการ

รหัสความรู้ (KSA ID)	รายละเอียด
K0044	ความรู้เกี่ยวกับการรักษาความปลอดภัยไซเบอร์,หลักการความเป็นส่วนตัวและความต้องการขององค์กร (เกี่ยวกับการรักษาความลับ,ความสมบูรณ์,ความพร้อมใช้งาน, การรับรองความถูกต้อง,การปฏิเสธ)
K0046	ความรู้เกี่ยวกับวิธีการตรวจจับการบุกรุกและเทคนิคในการตรวจจับการบุกรุกของโฮสต์และเครือข่าย
K0049	ความรู้เกี่ยวกับหลักการและวิธีการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (เช่นไฟร์วอลล์,การเข้ารหัส)
K0056	ความรู้เกี่ยวกับการเข้าถึงเครือข่าย,ข้อมูลประจำตัวและการจัดการการเข้าถึง (เช่นโครงสร้างพื้นฐานของคีย์สาธารณะ Oauth OpenID SAML และ SPML)
K0059	ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศใหม่และที่เกิดขึ้นใหม่ (IT) และเทคโนโลยี cybersecurity
K0060	ความรู้เกี่ยวกับระบบปฏิบัติการ
K0061	ความรู้เกี่ยวกับการไหลของข้อมูลบนเครือข่าย (เช่น Transmission Control Protocol [TCP] และ Internet Protocol [IP], Open System Interconnection Model [OSI], ไลบรารีโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศรุ่นปัจจุบัน [ITIL])
K0065	ความรู้เกี่ยวกับการควบคุมการเข้าถึงการปรับตัวตามนโยบายและความเสี่ยง
K0070	ความรู้เกี่ยวกับระบบและภัยคุกคามความปลอดภัยโปรแกรมประยุกต์และจุดอ่อน (เช่นรหัสโทรศัพท์มือถือการเขียนสคริปต์ข้ามไซต์,ภาษาเชิงกระบวนการ Structured Query Language [PL / SQL] and injectionsการแข่งขันช่องแอบแฝง,การโจมตีแบบมุ่งเน้นผลตอบแทน , โค้ดที่เป็นอันตราย
K0074	ความรู้เกี่ยวกับแนวคิดหลักในการจัดการความปลอดภัย (เช่นการจัดการเผยแพร่การจัดการ Patch)

รหัสความรู้ (KSA ID)	รายละเอียด
K0075	ความรู้เกี่ยวกับเครื่องมือออกแบบระบบรักษาความปลอดภัยวิธีการและเทคนิค
K0093	ความรู้เกี่ยวกับเครื่องมือออกแบบระบบรักษาความปลอดภัยวิธีการและเทคนิค
K0098	ความรู้เกี่ยวกับโครงสร้างการรายงานและกระบวนการภายในองค์กรของตนเอง
K0104	ความรู้เกี่ยวกับการรักษาความปลอดภัยเครือข่ายส่วนตัวเสมือน (VPN)
K0106	ความรู้เกี่ยวกับสิ่งที่ก่อให้เกิดการโจมตีเครือข่ายและความสัมพันธ์ของการโจมตีระบบเครือข่ายกับภัยคุกคามและความเสี่ยงต่างๆ
K0107	ความรู้เกี่ยวกับการสืบสวนการรายงานข้อมูลการสืบสวนเครื่องมือและกฎหมาย / ข้อบังคับเกี่ยวกับการคุกคามข้อมูลภายใน
K0110	ความรู้เกี่ยวกับยุทธวิธีฝ่ายตรงข้ามเทคนิคและขั้นตอน
K0111	ความรู้เกี่ยวกับเครื่องมือเครือข่าย (เช่น ping, traceroute, nslookup)
K0112	ความรู้เกี่ยวกับสถาปัตยกรรมการรักษาความปลอดภัยเครือข่าย
K0113	ความรู้เกี่ยวกับการสื่อสารในระบบเครือข่ายประเภทต่างๆ (เช่น LAN, WAN, MAN, WLAN, WWAN)
K0116	ความรู้เกี่ยวกับนามสกุลไฟล์(e.g., .dll, .bat, .zip, .pcap, .gzip).
K0139	ความรู้เกี่ยวกับภาษาคอมพิวเตอร์และคอมไพเลอร์
K0142	ความรู้เกี่ยวกับกระบวนการจัดการเก็บรวบรวม,ขีดความสามารถและข้อจำกัด
K0143	ความรู้เกี่ยวกับการเก็บข้อมูลจราจร การกรองและการเลือก
K0157	ความรู้เกี่ยวกับนโยบายการรักษาความปลอดภัยไซเบอร์และนโยบายด้านความปลอดภัยข้อมูลขั้นตอนและระเบียบข้อบังคับ
K0160	ความรู้เกี่ยวกับเวกเตอร์โจมตีทั่วไปบนเลเยอร์เครือข่าย
K0161	ความรู้เกี่ยวกับการโจมตีที่แตกต่างกัน (เช่น passive, active, insider, close-in, distribution attacks)
K0162	ความรู้เกี่ยวกับผู้โจมตีในโลกไซเบอร์ (เช่นภัยคุกคามจากภายใน, องค์กรที่ไม่ได้รับการสนับสนุนจากประเทศและประเทศที่สนับสนุน)
K0167	ความรู้เกี่ยวกับการบริหาร, ระบบเครือข่ายและ operating system hardening

รหัสความรู้ (KSA ID)	รายละเอียด
K0168	ความรู้เกี่ยวกับกฎหมายรัฐบัญญัติ (หลักเกณฑ์ของสาขาบริหารและ / หรือแนวทางและขั้นตอนทางกฎหมายด้านการบริหาร / ทางอาญา)
K0177	ความรู้เกี่ยวกับขั้นตอนการโจมตีแบบไซเบอร์ (เช่นการลาดตระเวน, การสแกน,การเข้าถึงสิทธิ์, การเพิ่มสิทธิ, การรักษาสิทธิ์, การเข้าถึง, การแสวงหาประโยชน์เครือข่าย,การติดตาม)
K0179	ความรู้เกี่ยวกับแนวคิดสถาปัตยกรรมความปลอดภัยของเครือข่ายรวมถึงโทโพโลยีโปรโตคอลส่วนประกอบและหลักการ (เช่นการประยุกต์ใช้การป้องกันในเชิงลึก)
K0180	ความรู้เกี่ยวกับหลักการบริหารระบบเครือข่ายโมเดลวิธีการ (เช่นการตรวจสอบประสิทธิภาพของระบบแบบ end-to-end) และเครื่องมือ.
K0190	ความรู้เกี่ยวกับเทคนิคการเข้ารหัส
K0191	ผลกระทบจากการติดตั้งลายเซ็นสำหรับไวรัสมัลแวร์และการโจมตี
K0192	ความรู้เกี่ยวกับพอร์ตและบริการของ Windows / Unix
K0203	ความรู้เกี่ยวกับรูปแบบความปลอดภัย (เช่นรุ่น Bell-LaPadula, แบบจำลองความสมบูรณ์ของ Biba, แบบจำลองความสมบูรณ์แบบ Clark-Wilson)
K0221	ความรู้เกี่ยวกับรูปแบบ OSI และโปรโตคอลเครือข่ายพื้นฐาน (เช่น TCP/ IP)
K0222	ความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้องหน่วยงานด้านกฎหมาย, ข้อจำกัดและข้อบังคับเกี่ยวกับการป้องกันไซเบอร์
K0260	ความรู้เกี่ยวกับข้อมูลที่สามารถระบุตัวตนได้ (Personally Identifiable Information - PII) มาตรฐานความปลอดภัยข้อมูล
K0261	ความรู้เกี่ยวกับมาตรฐานความปลอดภัยข้อมูลของอุตสาหกรรมบัตรชำระเงิน (Payment Card Industry - PCI)
K0262	ความรู้เกี่ยวกับมาตรฐานความปลอดภัยข้อมูลส่วนบุคคล (Personal Health Information - PHI)
K0290	ความรู้เกี่ยวกับระบบการทดสอบความปลอดภัยและวิธีการประเมินผล

รหัสความรู้ (KSA ID)	รายละเอียด
K0297	ความรู้เกี่ยวกับการออกแบบมาตรการตอบโต้เพื่อระบุความเสี่ยงด้านความปลอดภัย
K0300	ความรู้เกี่ยวกับการสร้างแผนที่เครือข่ายและการสร้างเครือข่าย topologies
K0301	ความรู้เกี่ยวกับการวิเคราะห์ระดับแพ็กเก็ต (packet – level) โดยใช้เครื่องมือที่เหมาะสม (เช่น Wireshark, tcpdump)
K0303	ความรู้เกี่ยวกับการใช้เครื่องมือ sub – netting
K0318	ความรู้เกี่ยวกับคำสั่งของระบบปฏิบัติการ
K0322	ความรู้เกี่ยวกับระบบฝังตัว (embedded system)
K0324	ความรู้เกี่ยวกับเครื่องมือและแอพพลิเคชันของระบบป้องกันการบุกรุก (Intrusion Detection System – IDS) / Intrusion Prevention System (IPS)
K0332	ความรู้เกี่ยวกับโปรโตคอลเครือข่ายเช่น TCP / IP การกำหนดค่าโฮสต์แบบไดนามิกระบบชื่อโดเมน (DNS) และบริการไดเรกทอรี
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.
K0342	ความรู้เกี่ยวกับหลักการและเครื่องมือในการทดสอบการเจาะ
K0624	ความรู้เกี่ยวกับความเสี่ยงด้านความปลอดภัยของแอปพลิเคชัน (เช่น โครงการความปลอดภัยด้านเว็บของ Open Web Application 10 อันดับแรก)

ทักษะ (Skills) - S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370

รหัสทักษะ (Skill ID)	รายละเอียด
S0020	ทักษะในการพัฒนาและปรับใช้ลายเซ็น
S0025	ทักษะในการตรวจจับการบุกรุกโดยใช้โฮสต์และเครือข่ายโดยใช้เทคโนโลยีการตรวจจับการบุกรุก (เช่น Snort)

รหัสทักษะ (Skill ID)	รายละเอียด
S0027	ทักษะในการกำหนดว่าระบบรักษาความปลอดภัยจะทำงานอย่างไร (รวมทั้งความยืดหยุ่นและความสามารถในการพึ่งพาได้) และการเปลี่ยนแปลงสภาพการปฏิบัติงานหรือสภาพแวดล้อมจะส่งผลต่อผลลัพธ์เหล่านี้อย่างไร
S0036	ทักษะในการประเมินความเพียงพอของการออกแบบระบบรักษาความปลอดภัย
S0054	ทักษะในการใช้วิธีจัดการกับเหตุการณ์
S0057	ทักษะในการใช้โปรโตคอลวิเคราะห์
S0063	ทักษธในการเก็บรวบรวมข้อมูลจากแหล่งข้อมูลการป้องกันไซเบอร์ที่หลากหลาย
S0078	ทักษะในการจำแนกประเภทของช่องโหว่และการโจมตีที่เกี่ยวข้อง
S0096	ทักษะในการอ่านและการตีความลายเซ็น (เช่น snort)
S0147	ทักษะในการประเมินการควบคุมความปลอดภัยตามหลักการและหลักความปลอดภัยในโลกไซเบอร์ (เช่น CIS CSC, NIST SP 800-53, กรอบความปลอดภัยของอินเทอร์เน็ตเป็นต้น
S0156	ทักษะในการทำการวิเคราะห์ระดับแพ็กเก็ต
S0167	มีทักษะในการรับรู้ถึงช่องโหว่ในระบบรักษาความปลอดภัย (เช่นการสแกนช่องโหว่และการปฏิบัติตามข้อกำหนด
S0169	ทักษะในการวิเคราะห์แนวโน้ม
S0367	ทักษะในการประยุกต์ใช้หลักการความปลอดภัยในโลกไซเบอร์และข้อมูลส่วนบุคคลตามความต้องการขององค์กร (เกี่ยวกับการรักษาความลับความสมบูรณ์ความพร้อมใช้งานการตรวจสอบสิทธิ์การไม่ปฏิเสธ)
S0370	ทักษะในการใช้การป้องกันไซเบอร์โครงสร้างและกระบวนการรายงานของผู้ให้บริการภายในองค์กรของตนเอง

ความสามารถ (Abilities) - A0010, A0015, A0066, A0123, A0128, A0159

รหัสความสามารถ (Ability ID)	รายละเอียด
A0010	ความสามารถในการวิเคราะห์มัลแวร์
A0015	ความสามารถในการวิเคราะห์ช่องโหว่และรู้จักช่องโหว่ในระบบรักษาความปลอดภัย
A0066	ความสามารถในการรวบรวมข้อมูลทั้งหมดที่ใช้ในการวิเคราะห์และ / หรือวางแผนผลิตภัณฑ์ได้อย่างถูกต้องและครบถ้วน
A0123	ความสามารถในการรักษาความปลอดภัยในโลกไซเบอร์และหลักความเป็นส่วนตัวตามความต้องการขององค์กร (เกี่ยวข้องกับความลับข้อมูล,ความสมบูรณ์การใช้งาน,การรับรองความถูกต้อง,การไม่ปฏิเสธ)
A0128	ความสามารถในการใช้เทคนิคในการตรวจจับการบุกรุกของโฮสต์และเครือข่ายโดยใช้เทคโนโลยีการตรวจจับการบุกรุก
A0159	ความสามารถในการตีความข้อมูลที่เก็บรวบรวมโดยเครื่องมือเครือข่าย (เช่น Nslookup, Ping และ Traceroute)

แนวทางการนำไปใช้ในการพัฒนาบุคลากร

จากข้อมูลรายละเอียดของ Tasks KSAs ใน NICE Framework อธิบายถึงงานด้านความปลอดภัยไซเบอร์ได้ทั้งหมด โดยระบุความรู้ ทักษะ ความสามารถ ที่เกี่ยวข้อง สามารถนำไปเป็นแนวทางในการพัฒนาบุคลากร การวางแผน การฝึกอบรม การศึกษา และการฝึกปฏิบัติการจำลอง เป็นแนวทางวางแผนการสรรหาบุคลากรของศูนย์ไซเบอร์ทหารฯ ทั้งนี้เพื่อให้สามารถปฏิบัติภารกิจของหน่วยได้บรรลุเป้าหมายอย่างมีประสิทธิภาพและประสิทธิผลตรงตามยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ.2558

เพื่อจะให้ได้หลักสูตรการฝึกอบรมและการฝึกปฏิบัติการจำลอง จะมีการทำตารางตรวจสอบ (Checklist) เจ้าหน้าที่ไซเบอร์แต่ละบุคคลตามตำแหน่งงาน แต่ละภารกิจจะมีความแตกต่างกันระหว่างงาน (Tasks), ความรู้ (Knowledge), ทักษะ (Skills) และความสามารถ (Abilities) หลังจากนั้นจะสรุปวิเคราะห์ข้อมูลเพื่อจัดการฝึกอบรมตามความสำคัญเร่งด่วน เพื่อให้ได้บุคลากรที่สามารถปฏิบัติงานไซเบอร์ได้บรรลุภารกิจ ดังตัวอย่างนี้

ตารางตรวจสอบความสามารถในการทำงาน (Checklist Tasks)

ชื่อ _____ ตำแหน่ง _____ แผนก _____ กอง _____		
รหัสงาน (Task ID)	รายละเอียด	Pass (/)
T0020	พัฒนาเนื้อหาสำหรับเครื่องมือป้องกันไซเบอร์	
T0023	อธิบายลักษณะและวิเคราะห์เครือข่ายเพื่อระบุกิจกรรมผิดปกติและภัยคุกคามที่อาจเกิดขึ้นกับทรัพยากรเครือข่าย	
T0043	ประสานงานกับเจ้าหน้าที่ป้องกันไซเบอร์ทั่วทั้งองค์กรเพื่อตรวจสอบความถูกต้องของการแจ้งเตือนระบบเครือข่าย	
. . .	. . .	
T0548	ให้คำแนะนำและข้อมูลสำหรับการกู้คืนภัยพิบัติการจัดเตรียมและความต่อเนื่องของแผนการดำเนินงาน	

ตารางตรวจสอบความรู้ที่มี (Checklist Knowledge)

ชื่อ _____ ตำแหน่ง _____ แผนก _____ กอง _____		
รหัสความรู้ (KSA ID)	รายละเอียด	Pass (/)
K0001	ความรู้เกี่ยวกับแนวคิดและโปรโตคอลเครือข่ายคอมพิวเตอร์และวิธีการรักษาความปลอดภัยเครือข่าย	
K0002	ความรู้เกี่ยวกับกระบวนการบริหารความเสี่ยง (เช่นวิธีประเมินและบรรเทาความเสี่ยง)	

ตารางตรวจสอบความรู้ที่มี (Checklist Knowledge) (ต่อ)

รหัสความรู้ (KSA ID)	รายละเอียด	Pass (/)
K0003	ความรู้เกี่ยวกับกฎหมายข้อบังคับนโยบายและจริยธรรมที่เกี่ยวข้องกับความปลอดภัยในโลกไซเบอร์และความเป็นส่วนตัว	
.	.	

. .	. .	
K0624	ความรู้เกี่ยวกับความเสี่ยงด้านความปลอดภัยของแอปพลิเคชัน (เช่น โครงการความปลอดภัยด้านเว็บของ Open Web Application 10 อันดับแรก)	

ตารางตรวจสอบทักษะจากการฝึกฝน (Checklist Skills)

ชื่อ _____ ตำแหน่ง _____ แผนก _____ กอง _____		
รหัสทักษะ (Skill ID)	รายละเอียด	Pass (/)
S0020	ทักษะในการพัฒนาและปรับใช้ลายเซ็น	
S0025	ทักษะในการตรวจจับการบุกรุกโดยใช้โฮสต์และเครือข่ายโดยใช้เทคโนโลยีการตรวจจับการบุกรุก (เช่น Snort)	
S0027	ทักษะในการกำหนดระบบรักษาความปลอดภัยจะทำงานอย่างไร และการเปลี่ยนแปลงสภาพการปฏิบัติงานหรือสภาพแวดล้อมจะส่งผลต่อผลลัพธ์เหล่านี้อย่างไร	
. . .	. . .	
S0370	ทักษะในการป้องกันไซเบอร์โครงสร้างและกระบวนการรายงาน	

ตารางสอบถามความสามารถในการทำงาน (Checklist Abilities)

ชื่อ _____ ตำแหน่ง _____ แผนก _____ กอง _____		
รหัสความสามารถ (Ability ID)	รายละเอียด	Pass (/)
A0010	ความสามารถในการวิเคราะห์มัลแวร์	
A0015	ความสามารถในการวิเคราะห์ช่องโหว่และรู้จักช่องโหว่ในระบบรักษาความปลอดภัย	

A0066	ความสามารถในการรวบรวมข้อมูลทั้งหมดที่ใช้ในการวิเคราะห์และ / หรือวางแผนผลิตภัณฑ์ได้อย่างถูกต้องและครบถ้วน	
. . .	. . .	
A0159	ความสามารถในการตีความข้อมูลที่เก็บรวบรวมโดยเครื่องมือเครือข่าย (เช่น Nslookup, Ping และ Traceroute)	

ขั้นตอนต่อไปสรุปข้อมูล Knowledge , Skills, Abilities แต่ละแผนก

สรุปการตรวจสอบความรู้ที่มีของแผนก (Checklist Knowledge)

แผนก _____ กอง _____		
รหัสความรู้ (KSA ID)	รายละเอียด	จำนวน
K0001	ความรู้เกี่ยวกับแนวคิดและโปรโตคอลเครือข่ายคอมพิวเตอร์และวิธีการรักษาความปลอดภัยเครือข่าย	
K0002	ความรู้เกี่ยวกับกระบวนการบริหารความเสี่ยง (เช่นวิธีประเมินและบรรเทาความเสี่ยง)	

สรุปการตรวจสอบความรู้ที่มีของแผนก (Checklist Knowledge) (ต่อ)

รหัสความรู้ (KSA ID)	รายละเอียด	จำนวน
K0003	ความรู้เกี่ยวกับกฎหมายข้อบังคับนโยบายและจริยธรรมที่เกี่ยวข้องกับความปลอดภัยในโลกไซเบอร์และความเป็นส่วนตัว	
. . .	. . .	
K0624	ความรู้เกี่ยวกับความเสี่ยงด้านความปลอดภัยของแอปพลิเคชัน (เช่นโครงการความปลอดภัยด้านเว็บของ Open Web Application 10 อันดับแรก)	

สรุปการตรวจสอบทักษะที่มีของแผนก (Checklist Skills)

แผนก _____ กอง _____		
รหัสทักษะ (Skill ID)	รายละเอียด	จำนวน
S0020	ทักษะในการพัฒนาและปรับใช้ลายเซ็น	
S0025	ทักษะในการตรวจจับการบุกรุกโดยใช้โฮสต์และเครือข่ายโดยใช้เทคโนโลยีการตรวจจับการบุกรุก (เช่น Snort)	
S0027	ทักษะในการกำหนดว่าระบบรักษาความปลอดภัยจะทำงานอย่างไร (รวมทั้งความยืดหยุ่นและความสามารถในการพึ่งพาได้) และการเปลี่ยนแปลงสภาพการปฏิบัติงานหรือสภาพแวดล้อมจะส่งผลต่อผลลัพธ์เหล่านี้อย่างไร	
. . .	. . .	
S0370	ทักษะในการใช้การป้องกันไซเบอร์โครงสร้างและกระบวนการรายงานของผู้ให้บริการภายในองค์กรของตนเอง	

สรุปการตรวจสอบความสามารถที่มีของแผนก (Checklist Abilities)

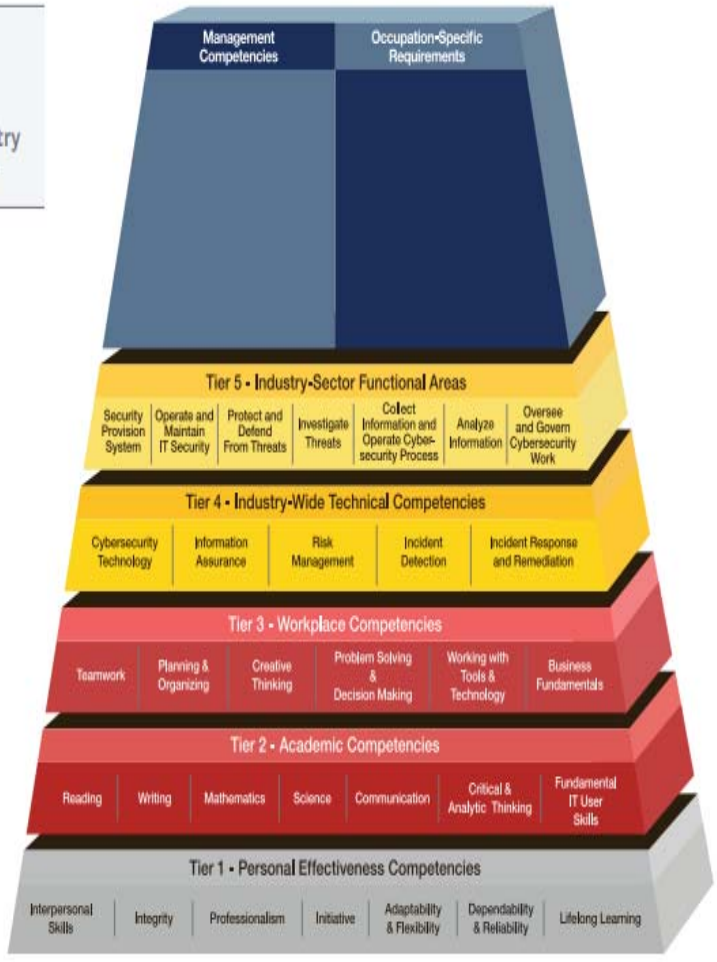
แผนก _____ กอง _____		
รหัสความสามารถ (Ability ID)	รายละเอียด	จำนวน
A0010	ความสามารถในการวิเคราะห์มัลแวร์	
A0015	ความสามารถในการวิเคราะห์ช่องโหว่และรู้จักช่องโหว่ในระบบรักษาความปลอดภัย	
A0066	ความสามารถในการรวบรวมข้อมูลทั้งหมดที่ใช้ในการวิเคราะห์และ / หรือวางแผนผลิตภัณฑ์ได้อย่างถูกต้องและครบถ้วน	
. . .	. . .	
A0159	ความสามารถในการวิเคราะห์มัลแวร์	

ต่อไปวิเคราะห์ความรู้ (Knowledge) , ทักษะ (Skills) และ ความสามารถ (Abilities) ที่ยังขาดแคลนและมีความจำเป็นเร่งด่วน เพื่อมาจัดลำดับความสำคัญและจัดการฝึกอบรมต่อไป

ข้อกำหนดสมรรถนะทั่วไปสำหรับงานความปลอดภัยไซเบอร์

นอกจากความสามารถทางไซเบอร์ตามแบบของ NICE Framework แล้วเพื่อให้การปฏิบัติงานทางไซเบอร์มีสมรรถนะที่สูงขึ้นได้มีการเพิ่มความสามารถด้านอื่นเข้าเป็นโมเดลสมรรถนะด้านความปลอดภัยไซเบอร์ U.S. Department of Labor (DOL) ได้ขยายตัวแบบ NICE Framework โดยรวมถึงความสามารถที่จำเป็น "เพื่อความปลอดภัยในการโต้ตอบกับไซเบอร์สเปซ " รูปแบบความสามารถจะเป็นแบบแบ่งชั้นแบบพีระมิดแสดงสมรรถนะตามระดับผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ต่างๆ จากระดับเริ่มต้นไปจนถึงผู้จัดการหรือหัวหน้าอาวุโส (ตามรูป) [7]

Figure 4.
U.S. Department of Labor's Cybersecurity Industry Competency Model.



Source: CareerOneStop.

โดยรูปแบบจะประกอบด้วย 3 สมรรถนะพื้นฐาน ได้แก่
ระดับที่ 1 (Tier 1) - สมรรถนะส่วนบุคคล
ระดับที่ 2 (Tier 2) - สมรรถนะทางวิชาการ
ระดับที่ 3 (Tier 3) - สมรรถนะการทำงานที่จำเป็นสำหรับบุคคลทุกคนในการปฏิบัติงานความปลอดภัยไซเบอร์
อีก 2 สมรรถนะเฉพาะทางพื้นฐาน ได้แก่
ระดับที่ 4 – สมรรถนะระดับเทคนิคทั่วไปและ
ระดับที่ 5 – สมรรถนะที่จำเป็นสำหรับแต่ละขอบเขตงาน
และสุดท้ายสมรรถนะการบริหาร ซึ่งเป็นส่วนบนสุดของปีระมิด ได้แก่
สมรรถนะการจัดการและความต้องการเฉพาะอาชีพ
ผู้ทำวิจัยเขียนเป็นสมรรถนะ ทางด้านไซเบอร์เบื้องต้น แบ่งเป็นระดับความสามารถ ต้น กลาง สูง [8] ดังนี้

ประเภททักษะ	ระดับความสามารถ (Proficiency Level)	ต้น	กลาง	สูง
ระดับที่ 1 สมรรถนะส่วนบุคคล	ทักษะด้านมนุษยสัมพันธ์			
	ความซื่อสัตย์ คุณธรรม			
	ความสามารถในอาชีพ			
	ความคิดริเริ่ม			
	การปรับตัวและความยืดหยุ่น			
	ความเชื่อถือได้			
	ศึกษาหาความรู้ สนใจเทคโนโลยีและองค์ความรู้ใหม่ๆ ในสาขาอาชีพ			
ระดับที่ 2 สมรรถนะทางวิชาการ	การอ่าน			
	การเขียน			
	การคำนวณ			
ระดับที่ 2	ทางวิทยาศาสตร์			
	การสื่อสาร			

ประเภททักษะ	ระดับความสามารถ (Proficiency Level)	ต้น	กลาง	สูง
สมรรถนะทางวิชาการ (ต่อ)	การคิดเชิงวิพากษ์และวิเคราะห์			
	ทักษะพื้นฐานเทคโนโลยีสารสนเทศ			
ระดับ 3 สมรรถนะการทำงานที่จำเป็น	การทำงานเป็นทีม			
	การวางแผนและการจัดการ			
	ความคิดสร้างสรรค์			
	การแก้ปัญหาและการตัดสินใจ			
	การทำงานกับเครื่องมือและเทคโนโลยี			
	พื้นฐานทางธุรกิจ			
ระดับ 4 สมรรถนะระดับเทคนิคทั่วไป	เทคโนโลยีความปลอดภัยไซเบอร์			
	การประกันข้อมูล			
	การจัดการความเสี่ยง			
	การตรวจจับเหตุการณ์			
	การตอบสนองเหตุการณ์และการแก้ไขปัญหา			
ระดับ 5 สมรรถนะที่จำเป็นสำหรับ แต่ละขอบเขตงาน	ระบบรักษาความปลอดภัย			
	ดำเนินการและรักษาความปลอดภัยไอที			
	ป้องกันและกำจัดจากภัยคุกคาม			
	ตรวจสอบภัยคุกคาม			
	รวบรวมข้อมูลและดำเนินการกระบวนการความปลอดภัยไซเบอร์			
	วิเคราะห์ข้อมูล			
	ดูแลและควบคุมงานด้านความปลอดภัยไซเบอร์			
สมรรถนะการจัดการ				
ความต้องการเฉพาะอาชีพ				

การดำรงและพัฒนาศักยภาพทางมิติไซเบอร์

เพื่อให้กระบวนการผลิต รักษา และพัฒนาบุคลากรที่ปฏิบัติงานมิติไซเบอร์ของกองบัญชาการกองทัพไทยในทุกระดับมีความเหมาะสม ต่อเนื่อง เพียงพอ ทั้งเชิงคุณภาพและปริมาณ โดยมีเป้าหมาย ได้แก่ ผลักดันให้มีการจัดทำแนวทางและหลักสูตรการผลิตบุคลากรที่ปฏิบัติงานมิติไซเบอร์ในระดับโรงเรียนทหาร ให้มีความพร้อมในการปฏิบัติงานโดยทันทีเมื่อสำเร็จการศึกษา ได้รับคุณวุฒิตรงตามคุณสมบัติเฉพาะตำแหน่งที่กำหนดในอัตราของหน่วยงาน ที่เกี่ยวข้องโดยจะต้องมีความสามารถในการป้องกันและโจมตีระบบเครือข่ายคอมพิวเตอร์เป็นอย่างน้อย พัฒนาความรู้ความสามารถด้านมิติไซเบอร์ทั้งระดับผู้บริหารและผู้ปฏิบัติ รวมทั้งสร้างความตระหนักรู้ให้แก่กำลังพลทั่วไปให้ทราบถึงภัยคุกคามทางมิติไซเบอร์ เพื่อให้มีความระมัดระวังและให้การใช้งานมิติไซเบอร์ในทุกระดับมีความปลอดภัย จัดทำแนวทางและระเบียบหลักสูตร ระเบียบปฏิบัติประจำ และกำหนดให้มีการฝึก/ฝึกร่วมการป้องกันไซเบอร์ในทุกระดับ ตั้งแต่ขั้นการวางแผนถึงขั้นการปฏิบัติการเพื่อพัฒนาทักษะของผู้ปฏิบัติงานมิติไซเบอร์ และทดสอบแนวคิดทฤษฎีที่เกี่ยวข้อง จัดทำแนวทางการรับราชการที่เหมาะสม และกำหนดมาตรการรักษาและจูงใจผู้ปฏิบัติงานมิติไซเบอร์ ได้แก่ การได้รับเงินเพิ่มพิเศษ และการได้รับการประดับเครื่องหมายแสดงความสามารถ เป็นต้น [9] จัดทำแนวทางเพื่อกำหนดกระบวนการสำรวจ คัดสรร จัดทำบัญชีผู้เชี่ยวชาญ ด้านมิติไซเบอร์ของหน่วยงานราชการและเอกชน ให้มีความพร้อมสำหรับการปฏิบัติงานร่วมกับบุคลากรที่ปฏิบัติงานมิติไซเบอร์ของกระทรวงกลาโหม [10]

รายงานฉบับนี้เป็นส่วนหนึ่งในการพัฒนาบุคลากรเพื่อเป็นแนวทางในการจัดการฝึกอบรมผู้ปฏิบัติงานด้านไซเบอร์ให้สามารถปฏิบัติภารกิจได้ลุล่วง โดยในวิจัยฉบับนี้ได้ศึกษาในแผนกรักษาความปลอดภัย กองรักษาความปลอดภัย ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย เพื่อให้ความรู้ให้ผู้สนใจนำไปดำเนินการต่อในส่วนที่เหลือ หรือพัฒนางานวิจัยฉบับนี้ ด้วยการหาแนวทางในการประเมินสมรรถนะภายหลังจากการได้รับการพัฒนาขีดความสามารถในด้านการปฏิบัติการทางไซเบอร์ในหน้าที่ต่างๆกัน

เอกสารอ้างอิง

[1] ยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ. 2558

[2] เรื่องเดียวกัน.

[3] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800_181 August 2017

[4] อัตราเฉพาะกิจ ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

[5] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800_181 August 2017

[6] ดร.บรรจง หะรังษี. NICE กรอบการดำเนินงานสำหรับการพัฒนาความรู้และขีดความสามารถของบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ [อินเทอร์เน็ต]. 2561 [เข้าถึงเมื่อ 2561 พฤษภาคม 28]; [หน้า 1] เข้าถึงได้จาก http://www.tnetsecurity.com/content_audit/NICE.pdf

[7] University of Phoenix, Cybersecurity Workforce Competencies : [Internet]. 2017 [cited 2018 Feb 10]. Available from: https://iamcybersafe.org/wp_content/uploads/2017/01/University_of_Phoenix_ISC2_cybersecurity_report.pdf

[8] National Initiative for Cybersecurity Careers and Studies (NICES). Cybersecurity Workforce Development Toolkit , [Internet]. [cited 2018 Jan 6]. Available from: https://niccs-us-cert.gov/workforce-development/cybersecurity_workforce_development_toolkit

[9] แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ. 2560-2564

[10] เรื่องเดียวกัน

ประวัติย่อผู้วิจัย

ยศ ชื่อ นาวาเอกหญิง ศิริเนตร รักษ์วงศ์

วัน เดือน ปี เกิด 18 กรกฎาคม 2511

ประวัติสำเร็จการศึกษา

พ.ศ.2533	วิทยาศาสตร์บัณฑิต (สถิติ) มหาวิทยาลัยธรรมศาสตร์
พ.ศ.2538	พัฒนบริหารศาสตรบัณฑิตทางสถิติประยุกต์ (การวิจัยดำเนินงาน) สถาบันบัณฑิตพัฒนบริหารศาสตร์
พ.ศ.2549	วิทยาศาสตร์มหาบัณฑิต (วิทยาการคอมพิวเตอร์) สถาบันบัณฑิตพัฒนบริหารศาสตร์

ประวัติการทำงาน

พ.ศ.2539-2543	นายทหารวิศวกรรมระบบ กองปฏิบัติการ กรมการสนเทศทหาร กองบัญชาการทหารสูงสุด
พ.ศ.2543-2552	นายทหารบริหารฐานข้อมูล กองสารสนเทศทางทหาร กรมการสนเทศทหาร กองบัญชาการทหารสูงสุด
พ.ศ.2552-2557	หัวหน้าแผนกวิชาระบบควบคุมบังคับบัญชาและอำนวยการสื่อสารร่วมผสม กองวิชาการสื่อสารอิเล็กทรอนิกส์ ศูนย์ฝึกอบรมเทคโนโลยีสารสนเทศและการสื่อสารทหาร กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย
พ.ศ.2557-2560	ผู้ช่วยผู้อำนวยการกองวิชาเทคโนโลยีสารสนเทศ ศูนย์ฝึกอบรมเทคโนโลยีสารสนเทศและการสื่อสารทหาร กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย
พ.ศ.2560-2561	ผู้ช่วยผู้อำนวยการกองวิทยาการ ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

ตำแหน่งปัจจุบัน ผู้ช่วยผู้อำนวยการกองรักษาความปลอดภัย ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย