การพัฒนาระบบการคัดเลือกกำลังสำรองซึ่งเชี่ยวชาญด้านไซเบอร์เพื่อสนับสนุนการป้องกันภัยคุกคามด้านไซเบอร์ของกองทัพบก

ภัยคุกคามทางด้านไซเบอร์ (Cyber Threats)

ยุทธศาสตร์ชาติ ประเด็นด้านความมั่นคง หัวข้อ “การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ เพื่อยกระดับขีดความสามารถของกองทัพและหน่วยงานด้านความมั่นคงทั้งระบบของประเทศ ให้มีความพร้อมในการป้องกันและรักษาอธิปไตยของประเทศ รวมทั้งสามารถติดตาม ป้องกัน แก้ไข และรับมือกับปัญหาความมั่นคงทุกมิติทุกรูปแบบและทุกระดับแบบบูรณาการให้มีความพร้อมและเพียงพอต่อการป้องกันภัยคุกคามทุกมิติ ทุกรูปแบบ และทุกระดับความรุนแรง”[1]

ภัยคุกคามทางด้าน ไซเบอร์เป็นภัยร้ายแรงที่ส่งผลต่อวีถีชีวิตของประชาชนในประเทศ การโจมตีระบบเครือข่ายคอมพิวเตอร์ ถือเป็นภัยคุกคามที่สร้างความเสียหายแก่พลังอำนาจของชาติในทุกๆด้าน กองทัพบกในฐานะเป็นกำลังหลักด้านความมั่นคง ได้มีการบริหารจัดการเกี่ยวกับภัยคุกคามด้านไซเบอร์มาระยะเวลาหนึ่ง ผู้วิจัยได้วิเคราะห์สภาพแวดล้อมที่เกี่ยวข้องแล้วได้กำหนดวัตถุประสงค์ในการทำวิจัยดังนี้ 1. เพื่อศึกษาสภาพแวดล้อมของปัญหาด้านไซเบอร์ของกองทัพบก 2. เพื่อศึกษาสภาพแวดล้อม คุณลักษณะอันพึงประสงค์ของกำลังสำรอง ด้านเทคนิคการค้นหาข้อมูลในเครือข่าย ด้านโปรแกรมเมอร์ ด้านการรักษาความปลอดภัย ด้านการเชื่อมโยงเครือข่ายรักษาความปลอดภัย และด้านออกแบบการรักษาความปลอดภัย 3. เพื่อเสนอแนะคุณลักษณะอันพึงประสงค์ ของกำลังพลสำรองซึ่งเชี่ยวชาญงานด้านไซเบอร์ที่เหมาะสมกับการบรรจุเพื่อสนับสนุนการป้องกันภัยคุกคามด้านไซเบอร์ของกองทัพบก

สภาวะแวดล้อมของปัญหาด้านไซเบอร์ของกองทัพบก

ภัยคุกคามทางด้านไซเบอร์ในวงการทหารถือว่าเป็นภัยที่คุกคามความมั่นคงของชาติซึ่งเชื่อมโยง ไปสู่ด้านต่าง ๆ การกระทำทั้งหมดนั้นเป็นภัยที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในทางที่ผิดกฎหมายรวมทั้งการละเมิดต่อศีลธรรมและความสงบสุขของสังคม เป็นภัยร้ายแรงด้านการทหาร ซึ่งมีผลกระทบต่อระบบ การควบคุม การบังคับบัญชา การสื่อสาร สาระสนเทศ และการลาดตระเวน C^4ISR (Command Control Communications Computers Intelligence Surveillance and Reconnaissance) ภัยคุกคามทางด้านไซเบอร์มีหลายรูปแบบ ดังนี้

1. การโจมตีด้วยวิธีเจาะระบบ (Hacking) เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์ หรืออาศัยโปรแกรมแฮก หลากหลายรูปแบบ ที่สามารถดาวน์โหลดโปรแกรมแฮกมาใช้ได้ง่ายในโลกอินเทอร์เน็ต ไม่ต้องเป็นผู้เชี่ยวชาญก็สามารถเจาะระบบได้ ผู้ใช้งานอินเทอร์เน็ตจะต้องเฝ้าระวังและป้องกันตนเองให้ปลอดภัย แฮกเกอร์นั้นมีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการท้าทายโดยการเจาะระบบให้สำเร็จหรือมีจุดประสงค์เพื่อต้องการทำลายระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศ

2.การโจมตีโดยทำการฝังโปรแกรมลักลอบโจรกรรมข้อมูล คือ การใช้สปายแวร์ (Spyware) หรือประตูหลัง (Back Door) ระบบคอมพิวเตอร์มีระบบรักษาความมั่นคงแต่ยังมีรูรั่วหรือช่องโหว่ของระบบรักษาความมั่นคงที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว้โดยเป็นกลไกลับทางซอฟต์แวร์หรือฮาดแวร์ จึงทำให้ผู้ไม่ประสงค์ดี สามารถใช้ช่องโหว่นี้ผ่านระบบรักษาความมั่นคงเข้ามาในระบบและสร้างความเสียหายต่อระบบคอมพิวเตอร์ได้

3. การโจมตีด้วยโปรแกรมมัลแวร์ (Malware) หมายถึงซอฟแวร์ที่เขียนขึ้นที่มีวัตถุประสงค์ในทางร้ายหรือเป็นภัยคุกคามต่อระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ให้ไปทำความเสียหายต่อคอมพิวเตอร์ที่เจ้าของหรือผู้ใช้ไม่ได้อนุญาต โปรแกรมมัลแวร์จะส่งผลให้คอมพิวเตอร์เสียหาย คือ สูญเสียความลับทางข้อมูล สูญเสียข้อมูลและเสถียรภาพของ

ระบบปฏิบัติการของคอมพิวเตอร์ โปรแกรมมัลแวร์นั้นมีทั้งที่เป็นไวรัสคอมพิวเตอร์ และหนอนคอมพิวเตอร์

4. การโจมตีโดยใช้ไวรัสคอมพิวเตอร์ (Computer Virus) คือโปรแกรมคอมพิวเตอร์ที่บุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้คอมพิวเตอร์เครื่องนั้น ส่วนมากมีความประสงค์จะสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ โดยไวรัสจะฝังตัวอยู่ในแฟ้มข้อมูล เมื่อเปิดเครื่องคอมพิวเตอร์และมีการเปิดแฟ้มข้อมูลใช้เครื่องคอมพิวเตอร์ก็จะติดไวรัสและจะแพร่ไปยังเครื่องอื่น ๆ ด้วย

5. การโจมตีด้วยหนอนคอมพิวเตอร์ (Computer Worm) หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้ โดยมากจะคัดลอกและกระจายตัวของหนอนคอมพิวเตอร์เองในเครือข่ายและข้ามเครือข่ายได้ ทำลายข้อมูลและสร้างความเสียหายให้กับคอมพิวเตอร์

6. การโจมตีด้วยระเบิดเวลา (Logic Bomb) อีกความหมายหนึ่งคือระเบิดตรรกะ หมายถึงซอฟต์แวร์ แอพพลิเคชั่นหรือชุดคำสั่งคอมพิวเตอร์โดยผู้เขียนโปรแกรมตั้งเวลากำหนดไว้อาจจะกำหนดเป็นวันที่หรือการกดปุ่มบนแป้นพิมพ์เพื่อให้มีการปิดระบบคอมพิวเตอร์หรือปิดเครือข่ายทั้งหมด รวมทั้งการลบข้อมูลหรือซอฟต์แวร์ต่าง ๆ บนเน็ตเวิร์กทิ้งทั้งหมด

7. การโจมตีด้วยโทรจัน (Trojan) คือ โปรแกรมที่เป็นเหมือนโปรแกรมธรรมดาทั่วไป และอาจจะดูเหมือนไม่มีอันตรายอะไร แต่โปรแกรมนี้จะมีลักษณะแอบแฝงเพื่อทำอันตรายต่อระบบคอมพิวเตอร์ โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมมาให้ เมื่อผู้ใช้คอมพิวเตอร์นำโปรแกรมโทรจันไปติดตั้งในระบบเครือข่ายคอมพิวเตอร์ของตนเองแล้ว โปรแกรมนี้จะทำการขโมยข้อมูลผู้ใช้ รหัสผ่าน หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิตและข้อมูลส่วนบุคคลอื่น ๆ

8. การโจมตีโดยใช้หุ่นยนต์ (Botnet) เป็นภัยคุกคามด้านสารสนเทศที่เกิดกลับกลุ่มของเครื่องคอมพิวเตอร์ที่มีโปรแกรมไม่พึงประสงค์ติดตั้งอยู่ ซึ่งโปรแกรมไม่พึงประสงค์นั้นจะทำการรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ต โดยอาจจะเป็นคำสั่งที่ให้ทำการโจมตีระบบเครือข่ายหรือส่งสแปม และโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์นั้น

9. การโจมตีแบบ (DoS/DDos) การโจมตีสภาพพร้อมใช้งานของระบบคอมพิวเตอร์ โดยมีการโจมตีมาจากหลายที่โดยแต่ละที่จะโจมตีเป้าหมายเดียวกันภายในเวลาเดียวกัน เพื่อทำให้บริการต่างๆ ของระบบคอมพิวเตอร์ไม่สามารถให้บริการได้ตามปกติมีผลกระทบต่อการให้บริการและเกิดความล่าช้าในการตอบสนองของผู้รับบริการจนกระทั่งระบบไม่สามารถให้บริการได้ต่อไปและทำให้เกิดเว็บไซต์ล่มในที่สุด

10. การโจมตีด้วย (Ransomware) คือ มัลแวร์เรียกค่าไถ่เป็นซอฟต์แวร์ที่ได้รับการพัฒนาขึ้นเพื่อเข้ารหัสลับไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ หรือปิดกั้นไม่ให้ผู้ใช้เข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ได้โดยเรียกร้องให้เหยื่อจ่ายเงินเพื่อจะได้รับกุญแจถอดรหัสไฟล์หรือปลดล็อกการใช้งานเครื่องคอมพิวเตอร์ซึ่งปัจจุบันจะมีภัยคุกคามลักษณะนี้เพิ่มมากขึ้น [2]

กองทัพบก ได้เล็งเห็นความสำคัญในด้านการรักษาความมั่งคงปลอดภัยไซเบอร์เช่นกัน ได้ขออนุมัติหลักการจัดตั้ง ศูนย์ไซเบอร์กองทัพบก (Army Cyber Centre) ขึ้น โดยเริ่มทดลองปฏิบัติงานตั้งแต่ 1 ตุลาคม 2557 นับเป็นความท้าทายของกองทัพในการดำเนินการด้านไซเบอร์ ท่ามกลางสถานการณ์ทางการเมืองที่อ่อนไหว และภายใต้การจับตามองของนานาประเทศ โดยเฉพาะประเทศกลุ่มสมาชิกอาเซียน ดังนั้นการกำหนดกรอบความคิดในการปฏิบัติงาน (Framework) เพื่อสร้างหลักประกันความสำเร็จในการดำเนินการ จึงเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่ง ทั้งนี้เพื่อใช้เป็นแนวทางการปฏิบัติงาน (Guide Line) รวมถึงการสร้างความสำนึก ความตระหนัก และสร้างความรู้เข้าใจของกำลังพลทุกระดับชั้น กรอบแนวทางการปฏิบัติงานของศูนย์ไซเบอร์กองทัพบกยึดถือการดำเนินงานตามหลักหน้าที่พื้นฐานของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology ; NIST) ทั้ง 5 ประการ (IPDRR : Identify Protect Detect Respond Recover) ดังนี้

1. การระบุ (Identify) เป็นการศึกษาสภาพแวดล้อม ทำความเข้าใจบริบท ทรัพยากร และงานสำคัญเพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เริ่มจาก
การบริหารจัดการทรัพย์สิน (Asset Management ; AM)
การดำเนินการตรวจสอบสภาพแวดล้อม (Environmental Scanning ; ES)
การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย (Risk Assessment ; RA)
การประเมินช่องโหว่ของระบบ (Vulnerability Assessment ; VA)
การประกันความเสี่ยงด้านสารสนเทศ (Information Assurance ; IA)
การทดสอบเจาะระบบ (Penetration Testing ; Pen-Test)
และการกำหนดกลยุทธ์บริหารจัดการความเสี่ยง (Risk Management Strategy ; RMS)
เป็นต้น

2. การป้องกัน (Protect) เป็นการดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อ จำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์โดยกำหนด
มาตรการควบคุมการเข้าถึง (Access Control)
การยืนยันและรับรองตัวบุคคล (Authentic)
การสร้างความสำนึกความตระหนักและการฝึกอบรม (Awareness and Training)
และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการ และวิธีปฏิบัติ ตลอดจนเทคโนโลยีการรักษาความปลอดภัยไซเบอร์ต่างๆ เช่น
ระบบตรวจหาการบุกรุก (Intrusion Detection System ; IDS)
ระบบป้องกันการบุกรุก (Intrusion Protection System ; IPS)

3. การตรวจจับ (Detect) เป็นการตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวัง หรือตรวจติดตามอย่างต่อเนื่อง โดยการเฝ้าระวัง สืบค้น ตรวจสอบ วิเคราะห์ข้อมูลและพฤติการณ์ต่างๆ (Monitoring and Analysis) ที่ส่งผลกระทบหรือเป็นภัยต่อระบบสารสนเทศ จาก ห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operations Center ; CSOC) รวมถึงการตรวจสอบ

ระบบสารสนเทศ (IT Audit) และหลักฐานทางดิจิตอลโดยกระบวนการทางวิทยาศาสตร์ (Digital Forensics) เพื่อดำเนินการทางกฎหมายต่อไป

4. การตอบสนอง (Respond) เป็นการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง โดยจัดชุดปฏิบัติการฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Team ; CERT) เพื่อทำหน้าที่ช่วยเหลือผู้ใช้งานที่ประสบปัญหาการคุกคามด้านไซเบอร์ในเบื้องต้น, การประสานการใช้งานระบบสำรอง (Backup System) คอยประสานการปฏิบัติกับหน่วยงานที่เกี่ยวข้อง, ควบคุมจำกัดขอบเขตและลดผลกระทบที่เกิดขึ้น (Mitigation) ตลอดจนควบคุมพยานหลักฐานต่างๆ เพื่อรอการพิสูจน์ต่อไป นอกจากนี้ยังมีชุดปฏิบัติการไซเบอร์เชิงรุก (Cyber Warrior) เพื่อทำหน้าที่ปฏิบัติการภารกิจต่อเป้าหมายที่เป็นภัยคุกคามทั้งด้านไซเบอร์ และการปฏิบัติการข่าวสาร (Information Operations ; IO) บนไซเบอร์ในกรณีที่มีความจำเป็น

5. การคืนสภาพ (Recover) เป็นการดำเนินการกู้คืนสภาพระบบสารสนเทศที่ได้รับความเสียหายจากการถูกคุกคามด้านไซเบอร์ ทั้ง ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และระบบฐานข้อมูลสารสนเทศ เพื่อรองรับการดำเนินงานอย่างต่อเนื่อง รวมถึงการจัดทำแผนการกู้คืนสภาพทั้งด้านขีดความสามารถ และการบริการให้ได้ตามเวลาที่กำหนด โดยจัดชุดปฏิบัติการกู้คืนระบบ (System Recovery Team ; SRT) ดำเนินการตามขั้นตอนการกู้คืนสภาพ เพื่อให้ระบบกลับคืนสภาพสามารถใช้การได้ตามปกติ

การดำเนินงานต่างๆ ดังกล่าว นับเป็นความท้าทายด้านความรู้ ความสามารถของคนในกองทัพบก เพราะเป็นเรื่องใหม่ที่องค์กรต่างๆ ทั่วโลกต่างให้ความสำคัญ โดยเฉพาะกองทัพบก ได้มีนโยบายและดำเนินการสรรหาบุคคลที่ต้องใช้ความรู้ ความสามารถ และประสบการณ์เฉพาะด้าน ที่แตกต่างและเหนือกว่างานด้านเทคโนโลยีสารสนเทศ (Information Technology; IT) ปกติ ซึ่งจะมีการกำหนด หมายเลขความชำนาญการทางทหาร (ชกท.) ขึ้นมาเป็นพิเศษ เพื่อรองรับคุณสมบัติด้านคุณวุฒิตามสาขาวิชาชีพ และตามตำแหน่งหน้าที่การงาน รวมถึงการพิจารณากำหนดค่าตอบแทนวิชาชีพ ตามความ

เหมาะสมในสาขาต่างๆ เช่นเดียวกับ หมอ พยาบาล ที่ปฏิบัติงานในตำแหน่งโดยไม่ต้องจำกัดชั้นยศ ทั้งนี้เพื่อให้เกิดประสิทธิภาพในการปฏิบัติงาน สร้างแรงจูงใจและเสริมสร้างขวัญกำลังใจของเจ้าหน้าที่ในการทำงาน ไม่เกิดภาวะสมองไหล ปัจจัยการปฏิบัติงานด้านไซเบอร์ของกองทัพจะทำให้เกิดประสิทธิภาพ ประสิทธิผล นอกเหนือจาก องค์กร (Organization) ระบบการทำงาน (Function) บุคลากร (Human Resource) องค์ความรู้ (Knowledge) และแรงจูงใจ (Incentive) แล้ว สิ่งที่สำคัญอีกประการ คือ ข้อกฎหมาย (Law) เนื่องจากการปฏิบัติงานด้านไซเบอร์ มักจะมีความล่อแหลม และเกี่ยวพันกับข้อกฎหมาย ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งกระทรวงเทคโนโลยี สารสนเทศและการสื่อสาร เป็นผู้รักษากฎหมาย โดยเนื้อหาสาระของกฎหมายส่วนใหญ่มุ่งเน้นไปในด้านอาชญากรรมคอมพิวเตอร์ (Computer Crime) แต่การปฏิบัติงานของกองทัพจะมุ่งเน้นไปในงานไซเบอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ ดังนั้น กองทัพควรจะพิจารณาในเรื่องกฎหมายพิเศษที่เกี่ยวข้องกับความมั่นคงของชาติด้านไซเบอร์ เพื่อให้อำนาจ หน้าที่ และเป็นเกราะคุ้มกันเจ้าหน้าที่ของหน่วยงานไซเบอร์ของกองทัพที่มีการจัดตั้งหน่วยทั้งระดับกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ในการปฏิบัติงานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของชาติ (National Cyber Security) ทำนองเดียวกับ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) ก็จะมีกฎหมายความมั่นคง เช่น พรบ. การรักษาความมั่นคงภายในราชอาณาจักร ใช้เป็นเครื่องมือทางกฎหมาย เป็นต้น

กรอบการปฏิบัติงานไซเบอร์ในด้านการรักษาความมั่นคงของชาติ เบื้องต้นในระหว่างที่ยังไม่มีกฎหมายรองรับ จะเน้นไปในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร โดยจะเริ่มต้นการดำเนินการสำรวจตรวจสอบทรัพย์สินอุปกรณ์ต่างๆ ที่เกี่ยวข้องกับไซเบอร์ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบฐานข้อมูล รวมถึงระบบคอมพิวเตอร์ที่เชื่อมโยงกับอาวุธยุทโธปกรณ์ ระบบควบคุมอาวุธยิง ระบบค้นหาและติดตามเป้าหมาย ระบบลาดตระเวนและเฝ้าตรวจ ฯลฯ การดำเนินการตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์ โดยเฉพาะการโจมตี การบุกรุก และการใช้โปรแกรมไวรัส และมัลแวร์ การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย โดยเฉพาะเครือข่ายอินเตอร์เน็ตและเครือข่ายไร้สาย การประเมินช่องโหว่ของระบบสารสนเทศ ทั้งอุปกรณ์เครือข่าย

Hub Switching Ports อุปกรณ์คอมพิวเตอร์ โปรแกรมระบบงาน และระบบฐานข้อมูลต่างๆ การประกันความเสี่ยงด้านสารสนเทศ โดยเฉพาะอุปกรณ์คอมพิวเตอร์ โปรแกรมระบบงาน และระบบฐานข้อมูลต่างๆ เพื่อให้เกิดความต่อเนื่องในการใช้งาน การปฏิบัติการทดสอบเจาะระบบสารสนเทศ เป็นการฝึกปฏิบัติการ (Workshop) ภายในห้องปฏิบัติการไซเบอร์ (Cyber War Room) ที่กำลังพัฒนาปรับปรุงจากห้องฝึกอบรมคอมพิวเตอร์เดิมขึ้นมาใหม่ เพื่อรองรับการฝึก การทดสอบ และการปฏิบัติงานจริง การบริหารจัดการความเสี่ยงระบบสารสนเทศ ในกรณีที่เกิดการโจมตีไซเบอร์ เกิดความเสียหาย หรือเกิดปัญหาข้อขัดข้องต่างๆ โดยการจัดทำแผนฉุกเฉิน และการกำหนดกลยุทธ์บริหารจัดการความเสี่ยง การกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ เพื่อควบคุมสิทธิการใช้งานระบบสารสนเทศ และการเข้าถึงข้อมูลในระดับต่างๆ ของผู้ที่มีสิทธิ์ รวมถึงการป้องกันการเข้าใช้งานจากบุคคลที่ไม่มีสิทธิ์ การยืนยันรับรองตัวบุคคลด้านสารสนเทศ เพื่อยืนยันรับรองตัวตนและความถูกต้องของบุคคลที่มีสิทธิ์เข้าใช้งาน และเก็บบันทึกไว้สำหรับการตรวจสอบ การสร้างความสำนึกความตระหนักและการฝึกอบรม เป็นการดำเนินการรณรงค์ ชี้แจง ทำความเข้าใจ ปลูกฝังจิตสำนึก สร้างความตระหนัก รวมถึงการฝึกอบรมความรู้ความเข้าใจในกฎ ระเบียบ ข้อบังคับ และแนวทางการปฏิบัติต่างๆ รวมถึงการสร้างภาคีประชาคมเครือข่ายไซเบอร์กองทัพบก (Army Cyber Communities) ซึ่งได้มีการดำเนินการไปแล้วทั้ง 4 พื้นที่ กองทัพภาค การดำเนินการเฝ้าระวัง ตรวจสอบ วิเคราะห์ไซเบอร์ และข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง การเตรียมการปรับปรุงห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operations Center ; CSOC) เพื่อใช้เป็นศูนย์ปฏิบัติการฯ ในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะระบบคอมพิวเตอร์ของหน่วยต่างๆ ทั้งกองทัพบก การตรวจสอบระบบสารสนเทศ เป็นกระบวนการตรวจสอบภายในด้านสารสนเทศ เช่นเดียวกับ การตรวจสอบภายในด้านการเงินและงบประมาณ การตรวจพิสูจน์หลักฐานทางดิจิตอล เป็นกระบวนการทางกฎหมาย ซึ่งจำเป็นจะต้องใช้ความชำนาญการเป็นพิเศษ เพื่อใช้เป็นหลักฐานในการดำเนินการทางกฎหมายต่อไป การปฏิบัติการฉุกเฉินด้านไซเบอร์ ในกรณีที่มีการคุกคามด้านไซเบอร์ จะมีชุดปฏิบัติการฉุกเฉินด้านไซเบอร์ของกองทัพบก (Army CERT) เข้าไปปฏิบัติการในพื้นที่ที่เกิดเหตุ โดยชุดปฏิบัติการดังกล่าวจะประสานความร่วมมือในการปฏิบัติการกับระดับชาติ (Thai CERT) ระดับกระทรวงกลาโหม

และระดับเหล่าทัพ ในกรณีที่เกิดความเสียหายต่อระบบสารสนเทศ จะมีชุดการปฏิบัติการกู้คืนระบบ (System Recovery Team ; SRT) เข้าไปดำเนินการปฏิบัติการกู้คืนระบบเพื่อให้สามารถกับมาใช้งานได้ตามปกติ

การดำเนินการปฏิบัติการข่าวสารบนไซเบอร์ จะเป็นการใช้ประโยชน์จากไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร ในกรณีการใช้ข่าวสารและสื่อไซเบอร์เพื่อเผยแพร่โจมตีให้ร้ายสถาบันพระมหากษัตริย์และกองทัพ การโจมตีให้ร้ายหรือบิดเบือนข้อเท็จจริงที่มีผลกระทบต่อความมั่นคงของชาติ การเผยแพร่ ยั่วยุ ปลุกปั่นให้เกิดความแตกแยกเกลียดชังของคนในสังคม การเผยแพร่หรือบิดเบือนข้อเท็จจริงที่มีผลกระทบต่อการรักษาความสงบเรียบร้อย การเผยแพร่ข้อมูลข่าวสารที่มีผลกระทบต่อการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ และการเผยแพร่ข้อมูลข่าวสารที่มีผลกระทบต่อความสัมพันธ์ระหว่างประเทศโดยเฉพาะประเทศเพื่อนบ้าน เป็นต้น โดยดำเนินการเฝ้าระวัง ค้นหา ติดตาม ตรวจสอบความเคลื่อนไหวข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง ตามที่กล่าวมาแล้วเพื่อรวบรวม สังเคราะห์ วิเคราะห์ และพิสูจน์ทราบความเคลื่อนไหวข้อมูลข่าวสาร จากกลุ่มบุคคล และเครือข่ายต่างๆ ในโลกไซเบอร์ เพื่อเป็นหลักฐานในการดำเนินการทางกฎหมาย หรือกำหนดมาตรการในการปฏิบัติการข่าวสารในด้านอื่นๆ เช่น การตอบโต้ข่าวสาร การบิดเบือนข้อมูล การสร้างความสับสน การลดกระแสและลดความน่าเชื่อถือของข่าวสาร ตลอดจนการกำหนดเป็นเป้าหมายในการปฏิบัติการเชิงรุกเมื่อจำเป็นต่อไป[3]

สภาวะแวดล้อมภัยคุกคามด้านไซเบอร์ของกองทัพบกจะพบประเด็นสำคัญคือ เป็นปัญหาในวงจำกัด มีการรับรู้เพียงกำลังพลบางกลุ่มเช่น ฝ่ายกรรมวิธีข้อมูล หน่วยทหารสื่อสาร การเผยแพร่อันตรายภัยคุกคามด้านไซเบอร์ค่อนข้างมีการนำเสนอน้อย และมีการตอบรับค่อนข้างต่ำ ซึ่งรวมถึงผู้บังคับบัญชาระดับสูงหรือผู้บังคับหน่วย การโจมตีด้านไซเบอร์ จะมีวัตถุประสงค์หลักๆ ได้แก่ การทำให้เกิดความล่าช้า การรบกวน โดยการทำลายระบบ การขโมยข้อมูลเพื่อไปใช้ประโยชน์ด้านอื่น กองทัพบกมีการจัดตั้งองค์กรเพื่อรองรับภัยคุกคามด้านไซเบอร์ มีการปฏิบัติงานที่เป็นระบบ แต่ยังขาดแคลนบุคลากรในการปฏิบัติงานด้านไอที

ผู้วิจัยได้ค้นคว้าเพิ่มเติมในคุณลักษณะของบุคคลากรที่จะนำมาบรรจุในบัญชีกำลังสำรองเพื่อเรียกเข้ารับราชการในกองทัพบกเพื่อช่วยเหลืองานด้านไซเบอร์ดังนี้

1. เป็นนักวิเคราะห์ข้อมูลข่าวสารมีความรู้ทางเทคนิคเพื่อค้นหาการโจมตีบนเครือข่าย
2. เป็นนักโปรแกรมเมอร์ วิจัยพัฒนาเครื่องมือ/อุปกรณ์ (Hardware) และเขียนชุดคาสั่ง (Software) สนับสนุน การปฏิบัติด้านไซเบอร์
3. เป็นผู้ดูแลระบบการรักษาความปลอดภัย เพื่อป้องกันการโจมตีด้านไซเบอร์ มีอุดมการณ์ยึดมั่นในสถาบันหลักของชาติ
4. เป็น นักวิเคราะห์ปรับปรุงเครือข่ายความมั่นคงปลอดภัยของหน่วยต่างๆ ในกองทัพบกให้มีมาตรฐานเชื่อมโยงและสามารถทางานร่วมกันได้อย่างมีประสิทธิภาพ
5. เป็นนักออกแบบและใช้งานระบบเครือข่ายออกแบบและดูแลระบบด้านความมั่นคงปลอดภัยให้มีมาตรฐาน จึงกำหนดเป็นวัตถุประสงค์เพิ่มเติมคือ

เพื่อศึกษาสภาพแวดล้อมคุณลักษณะอันพึงประสงค์ของกำลังสำรอง ด้านเทคนิคการค้นหาข้อมูลในเครือข่าย ด้านโปรแกรมเมอร์ ด้านการรักษาความปลอดภัย ด้านการเชื่อมโยงเครือข่ายรักษาความปลอดภัย และด้านออกแบบการรักษาความปลอดภัย

ด้านเทคนิคการค้นหาข้อมูลในเครือข่าย ในโลกไซเบอร์สเปซมีข้อมูลมากมายมหาศาล การที่เราจะค้นหาข้อมูลให้พบอย่างรวดเร็วจึงต้องพึ่งพา Search Engine Site ซึ่งจะทำหน้าที่รวบรวมรายชื่อเว็บไซต์ต่างๆ เอาไว้ โดยจัดแยกเป็นหมวดหมู่ ผู้ใช้งานเพียงแต่ทราบหัวข้อที่ต้องการค้นหาแล้วป้อนคำหรือข้อความของหัวข้อนั้นๆ ลงไปในช่องที่กำหนด คลิกปุ่มค้นหา เท่านั้น รอสักครู่ข้อมูลอย่างย่อๆ และรายชื่อเว็บไซต์ที่เกี่ยวข้องจะปรากฏให้เราเข้าไปศึกษาเพิ่มเติมได้ทันที การค้นหาข้อมูลมี 2 วิธี คือ 1. การค้นหาในรูปแบบ Index Directory 2. การค้นหาในรูปแบบ Search Engine

การค้นหาในรูปแบบ Index Directory

วิธีการค้นหาข้อมูลแบบ Index ข้อมูลจะมีความเป็นระเบียบเรียบร้อยมากกว่าการค้นหาข้อมูลด้วย วิธีของ Search Engine โดยจะถูกคัดแยกข้อมูลออกมาเป็นหมวดหมู่ และจัดแบ่งแยก Site ต่างๆออก เป็นประเภท สำหรับวิธีใช้งาน สามารถที่จะ Click เลือกข้อมูลที่ต้องการจะดูได้เลยใน Web Browser จากนั้นที่หน้าจอก็จะแสดงรายละเอียดของหัวข้อปลีกย่อยลึกลงมาอีกระดับหนึ่ง ปรากฏขึ้นมาให้เราเลือก ส่วนจะแสดงออกมาให้เลือกเยอะแค่ไหนขึ้นอยู่กับขนาดของฐานข้อมูลใน Index ว่าในแต่ละประเภท จัดรวบรวมเก็บเอาไว้มากน้อยเพียงใด เมื่อเข้าไปถึงประเภทย่อยที่สนใจแล้ว ที่เว็บเพจจะแสดงรายชื่อของเอกสารที่เกี่ยวข้องกับ ประเภทของข้อมูลนั้นๆออกมา หากคิดว่าเอกสารใดสนใจหรือต้องการอยากที่จะดู สามารถ Click ลงไปยัง Link เพื่อขอเชื่อมต่อทางไซต์ก็จะนำเอาผลของข้อมูลดังกล่าวออกมาแสดงผลทันที นอกเหนือไปจากนี้ ไซต์ที่แสดงออกมานั้นทางผู้ให้บริการยังได้เรียบเรียงโดยนำเอา Site ที่มีความเกี่ยว ข้องมากที่สุดเอามาไว้ตอนบนสุดของรายชื่อที่แสดง

การค้นหาในรูปแบบ Search Engine

วิธีการอีกอย่างที่นิยมใช้การค้นหาข้อมูลคือการใช้ Search Engine ซึ่งผู้ใช้ส่วนใหญ่กว่า 70% จะใช้วิธีการค้นหาแบบนี้ หลักการทำงานของ Search Engine จะแตกต่างจากการใช้ Indexลักษณะของมันจะเป็นฐานข้อมูลขนาดใหญ่มหาศาลที่กระจัดกระจายอยู่ทั่วไปบน Internet ไม่มีการแสดงข้อมูลออกมาเป็นลำดับขั้นของความสำคัญ การใช้งานจะเหมือนการสืบค้นฐานข้อมูล อื่นๆคือพิมพ์คำสำคัญ (Keyword) ที่ต้องการค้นหาเข้าไป จากนั้น Search Engine ก็จะแสดงข้อมูลและ Site ต่างๆที่เกี่ยวข้องออกมา[4]

ด้านการค้นหาข้อมูลต่างๆ ที่ได้มาอาจจะมีทั้ง ข้อมูลเชิงลบ และเชิงบวก นักวิเคราะห์ต้องมีความสามารถ ในการเชื่อมโยงข้อมูลที่ตัวเองค้นพบในสื่อต่างๆ รายงานและเสนอรูปแบบในการดำเนินการต่อข้อมูลเชิงทั้งเชิงลบและเชิงบวก

ด้านโปรแกรมเมอร์ วิจัยพัฒนาเครื่องมือ/อุปกรณ์ (Hardware) และเขียนชุดคำสั่ง (Software) สนับสนุน การปฏิบัติด้านไซเบอร์ “มีหน้าที่หลักในการเขียนโปรแกรมคอมพิวเตอร์ เพื่อให้ได้ซอฟต์แวร์ที่มีประสิทธิภาพในการประมวลผล มี Growth Mindset ในการเรียนรู้เป็นคุณสมบัติที่สำคัญที่สุดของโปรแกรมเมอร์เก่งๆ Mindset ในการเรียนรู้เป็นเรื่องสำคัญที่สุดคำว่า Mindset คำที่ใกล้เคียงที่สุดน่าจะเป็น “ทัศนคติ” ส่วน Growth Mindset นั้น เป็นทัศนคติที่เชื่อว่าทุกอย่างเปลี่ยนแปลง และพัฒนาได้ ถ้าคนที่ไม่มี Growth Mindset ก็อาจจะคิดว่าเราไม่มีความสามารถ ในขณะคนที่มี Growth Mindset จะทบทวนดูว่าทำตรงไหนได้ไม่ดีบ้างแล้วลองพัฒนาตัวเอง โปรแกรมเมอร์เก่งๆ ทุกคนเชื่อมั่นในศักยภาพของตัวเองว่าเก่งกว่านี้ได้ และเรื่องไหนที่ไม่เก่ง ถ้าให้เวลาฝึกหรือลองเรียนรู้ ก็สามารถเก่งได้ในทางตรงกันข้าม มีคนจำนวนมากที่พูดอยู่ตลอดว่าตัวเอง ไม่มีพรสวรรค์ กรณีนี้เรียกว่า Fixed Mindset คือปักใจเชื่อว่าตนเองไม่มีความสามารถซึ่งเรียกว่า Fixed Mindset เป็นการทำลายความสามารถตัวเองทางอ้อม ไม่มีใครที่เขียนโปรแกรมได้ดีโดยเคยไม่ทำเรื่องผิดพลาดมาก่อน อุตสาหกรรมซอฟต์แวร์บ้านเราโตได้ยากการจะไปแข่งขันกับประเทศอื่นๆ คงลำบากเพราะเราขาด นักพัฒนาซอฟต์แวร์ (Software Developer) หรือโปรแกรมเมอร์ (Programmer) ซึ่งเป็นหัวใจสำคัญของการพัฒนาอุตสาหกรรมซอฟต์แวร์ ถ้าเรามีจำนวนไม่มากพอก็เหมือนขาดวัตถุดิบ โปรแกรมเมอร์หลายคนก้าวขึ้นสู่การเป็น CTO (Chief Technology Officer) อนาคตของอาชีพโปรแกรมเมอร์ไม่ใช่เป็นแค่คนเขียน Code ไปตลอดชีวิต เส้นทางของอาชีพนี้มีสิ่งใหม่ที่จะต้องเรียนรู้ตลอด เราไม่ได้พูดถึงคนที่เขียนแค่โปรแกรมง่ายๆอย่างมาทำหน้าเว็บ ใช้ Tool เขียน script ง่ายๆ หรือเขียนโปรแกรมบนมือถือแค่บางภาษา แต่อาชีพโปรแกรมเมอร์คือเส้นทางสู่ความเป็น IT Architecture และ Chief Technology Officer มีความท้าทาย และความยากของการพัฒนาซอฟต์แวร์ตามเทคโนโลยีที่เปลี่ยนไปตลอด แต่แน่นอนถ้าตัวเองเป็นแค่ coder จมปลักอยู่กับแค่การเขียนโปรแกรมภาษาใดภาษาหนึ่ง เขียนโปรแกรมซ้ำซากๆ เมื่อเทคโนโลยีเปลี่ยน เราก็อาจขาดความก้าวหน้า อาชีพโปรแกรมเมอร์ต้องเรียนรู้อยู่ตลอด พยายามทำสิ่งใหม่ๆที่คนยังไม่ทำกันหรือเป็นคนกลุ่มแรกๆ เป็นสิ่งที่ต้องการมาก[5]

จากบทความจะเห็นได้ว่า คุณลักษณะโปรแกรมเมอร์ ที่มีความสามารถจะมีแนวคิดหัวก้าวหน้า คิดเชิงบวกเป็นนักสร้างสรรค์ซึ่งจำเป็นอย่างยิ่งในการที่จะออกแบบโปรแกรมป้องกันระบบให้กับหน่วยงานราชการ แต่ทั้งนี้ก็มีข้อเท็จจริงอยู่ว่า ภัยคุกคามทางไซเบอร์ต่างๆ ไม่เคยหยุดนิ่ง มีการพัฒนาอย่างต่อเนื่อง ทั้งระบบ ซอร์ฟแวร์ หรือ ฮาร์ดแวร์ แต่ก็เกิดจากความสามารถของมนุษย์

ด้านดูแลระบบการรักษาความปลอดภัย เพื่อป้องกันการโจมตีด้านไซเบอร์ ในปี 2018 มีเรื่องราวเกิดขึ้นบนโลกไซเบอร์มากมาย เริ่มต้นจากอัตราการละเมิดข้อมูลผ่านโลกออนไลน์เพิ่มขึ้นอย่างชัดเจน รวมถึงเกิดการก่ออาชญากรรมทางไซเบอร์ไม่เว้นแต่ละสัปดาห์ ทำให้การหาวิธีการป้องกันภัยกลายเป็นปัจจัยหลักที่สำคัญสำหรับธุรกิจ และผู้บริหารองค์กร ไม่ว่าจะขนาดเล็ก หรือใหญ่ต่างต้องคำนึงถึงเรื่องความปลอดภัยเป็นอันดับแรก

ดังนั้น มาเตรียมพร้อมสำหรับปี 2019 กับ 10 เทรนด์ความปลอดภัยในโลกไซเบอร์ ที่ทุกส่วนที่เกี่ยวข้อง ควรจะต้องนำมาพิจารณา เพื่อที่จะสามารถป้องกัน และรับมือกับอาชญากรบนโลกไซเบอร์ได้อย่างมีประสิทธิภาพ

1. เทคโนโลยีบล็อกเชนจะได้รับความนิยมอย่างแพร่หลายมากขึ้นเทคโนโลยี Blockchain เป็นระบบการทำธุรกรรม ที่ไม่อิงศูนย์กลาง ทำให้ไม่สามารถ เปลี่ยนแปลง ความถูกต้องของข้อมูลได้ จะไม่มีใครมาละเมิด เปลี่ยนแปลง หรือ พยายาม หลอกลวง ผ่านระบบ block chain ได้ จึงสามารถนำมาแก้ปัญหาต่าง ๆ ด้านความปลอดภัยได้

2. แฮกเกอร์เก่งขึ้นความสามารถในการเขียนโค้ดแบบซับซ้อนเพื่อใช้โจมตีของแฮกเกอร์คือภัยอันดับแรกเมื่อมีการพูดถึงภัยคุกคามเกิดขึ้นบนโลกไซเบอร์ เนื่องจากพวกเขามีการพัฒนาความสามารถ และเรียนรู้ตามการเปลี่ยนแปลงที่เกิดขึ้นอยู่ตลอดเวลา ซึ่งนั่นแสดงให้เห็นว่าเหล่าแฮกเกอร์นั้นอาจเดินเร็วกว่าระบบรักษาความปลอดภัยอยู่ก้าวหนึ่งเสมอ

3. การป้องกันการจู่โจมบนโลกไซเบอร์จะมีความยากมากขึ้นอาชญากรรมบนโลกไซเบอร์กำลังเติบโต และมีปริมาณเพิ่มสูงขึ้นอย่างมาก ส่งผลให้การป้องกันทำได้ยากขึ้นด้วย

เช่นกัน เนื่องจากตัวแฮกเกอร์เองมีความเข้าใจในตัวระบบ และสามารถเข้าถึงระบบเพื่อเจาะข้อมูลได้ง่ายไม่แพ้กับเจ้าของระบบหรือเจ้าของธุรกิจเลยทีเดียว อีกทั้งรูปแบบของอาชญากรรมทางไซเบอร์จะมีความหลากหลายมากขึ้น ส่งผลทำให้การเตรียมการเพื่อรับมือ หรือป้องกันได้ยากขึ้นเช่นกัน

4. ธุรกิจประกันภัยความเสี่ยงบนโลกไซเบอร์จะเป็นที่ต้องการมากขึ้นในปี 2019 อุตสาหกรรมประกันภัยจะมีการพัฒนา และมีการนำเสนอผลิตภัณฑ์ด้านการประกันภัยบนโลกไซเบอร์เพิ่มมากขึ้น เพื่อตอบสนองความต้องการของกลุ่มลูกค้า โดยเฉพาะในกลุ่มธุรกิจที่เกี่ยวข้องกับโลกดิจิทัล และออนไลน์ ซึ่งดูจะเป็นความหวัง ในการช่วยป้องกัน และช่วยลดความเสียหายที่จะเกิดขึ้นจากการโจรกรรมได้

5. การขาดแคลนบุคลากรทางด้านไอทีการขาดแคลนบุคลากรทางด้านไอทีนั้นถือเป็นปัญหาสำคัญสำหรับองค์กร และธุรกิจเพราะว่าบุคลากรในสาขานี้มีความเกี่ยวข้องกับปัญหาอาชญากรรมบนโลกไซเบอร์โดยตรง

6. กฎหมายทางไซเบอร์จะถูกนำมาใช้อย่างเคร่งครัดแม้ว่าจะมีกฎหมาย และกฎระเบียบที่บังคับใช้เกี่ยวกับความปลอดภัยบนโลกไซเบอร์ อยู่แล้ว แต่ในปี 2019 นี้คาดว่าจะมีการบังคับใช้กฎหมายที่เข้มงวดมากขึ้น รัฐบาลทั่วโลกต่างกำลังดำเนินการตามกฎหมายเพื่อตรวจสอบกิจกรรมที่ส่อความไม่ชอบมาพากลที่เกิดขึ้นบนโลกไซเบอร์ กฎหมายจึงถือว่าเป็นอีกปัจจัยสำคัญที่จะมีบทบาทอย่างจริงจังเพิ่มมากขึ้น

7. การติดตามผู้โจมตีบนโลกไซเบอร์จะทำได้ยากขึ้น กลุ่มอาชญากรทางไซเบอร์เป็นกลุ่มคนที่มีความเข้าใจเกี่ยวกับโลกไซเบอร์อย่างลึกซึ้ง ซึ่งทำให้การติดตามการกระทำผิดทางไซเบอร์จะทำได้ยากขึ้น เนื่องจากคนกลุ่มนี้รู้จักการหาทางหนีทีไล่ เพื่อหลีกเลี่ยงการติดตามจากเจ้าหน้าที่ ดังนั้นในปี 2019 นี้อาชญากรทางไซเบอร์อาจจะ “ล้ำหน้า” กว่าระบบการป้องกันการก่ออาชญากรรมได้

8. ผู้ดูแลระบบไอทีจะต้องเข้าใจระบบอย่างถ่องแท้ ผู้ที่รับผิดชอบทางด้าน Cyber Security ในองค์กร หรือธุรกิจ ต้องมีความเข้าใจในระบบไอทีของตัวเองอย่างถ่องแท้

มีการตรวจสอบระบบอยู่เสมอ เพราะบางครั้งความผิดพลาดอาจเกิดขึ้นจากบุคคลภายในองค์กรเอง หรือเกิดจากคนในองค์กรที่ทำการก่อการโจรกรรมทางไซเบอร์เพื่อหาผลประโยชน์จากช่องโหว่ที่เกิดขึ้นในระบบได้

9. การป้องกันการโจมตีบนโลกไซเบอร์ด้วย ปัญญาประดิษฐ์ หรือ AI (Artificial Intelligence) จะเป็นสิ่งที่ถูกใช้เพื่อเพิ่มการป้องกันการโจมตี เพราะไม่ใช่แค่เพียงประสิทธิภาพในการแจ้งล่วงหน้าว่าการโจมตีจะเกิดขึ้นเท่านั้น แต่ AI ยังสามารถระบุได้ว่าผู้ที่โจมตีมีวัตถุประสงค์ได้อีกด้วย

10. Internet of Things ยังคงเป็นจุดอ่อน อุปกรณ์ เครื่องใช้ต่าง ๆ ที่สามารถเชื่อมต่อกับอินเทอร์เน็ตได้เหล่านี้มีอัตราการถูกโจมตีเพิ่มขึ้นตลอดเวลาด้วยเช่นกัน นั่นจึงเป็นสาเหตุที่ผู้เชี่ยวชาญพบว่าอุปกรณ์เหล่านี้เป็นจุดอ่อนที่ทำให้ผู้ใช้งานเสี่ยงต่อการถูกแฮก เพื่อใช้แสวงหาผลประโยชน์ในทางที่ผิดได้ ซึ่งในปี 2019 จะมีการโจรกรรมข้อมูลผ่านอุปกรณ์เหล่านี้เพิ่มขึ้น ผู้ใช้งานจึงควรเพิ่มความปลอดภัยให้กับการใช้งานโดยการป้องกันขั้นพื้นฐานคือ การตั้งค่ารหัสผ่านของระบบให้ปลอดภัยเพื่อยากต่อการโจมตีได้โดยง่าย [6]

การเปลี่ยนแปลงที่เกิดขึ้นบนโลกไซเบอร์ จะยิ่งทวีคูณความรวดเร็วขึ้นไปตามเวลา ดังนั้นการรักษาความปลอดภัยด้วยการเรียนรู้ ปรับตัว เพื่อรับมือ แก้ไข และป้องกัน จึงถือเป็นปัจจัยที่จะทำให้ธุรกิจปลอดภัยจากการจู่โจมบนโลกไซเบอร์ได้ หรืออย่างน้อยก็ช่วยทำให้เกิดความเสียหายต่อทรัพย์สินดิจิทัล (Internet of Things) ให้น้อยที่สุด

ด้านการเชื่อมโยงเครือข่ายรักษาความปลอดภัย และด้านออกแบบการรักษาความปลอดภัย วิเคราะห์ปรับปรุงเครือข่ายออกแบบใช้งานระบบความมั่นคงปลอดภัย เชื่อมโยงระบบของแต่ละหน่วยงานให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ จากสภาวะการแข่งขันและสภาวะแวดล้อมของธุรกิจที่เปลี่ยนไปในปัจจุบันระบบเครือข่ายคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศมีบทบาทสำคัญมากต่อองค์กรธุรกิจ ไม่ว่าองค์กรขนาดเล็ก กลาง หรือขนาดใหญ่ ล้วนมีความจำเป็นในการนำระบบเทคโนโลยีสารสนเทศมาใช้ เพื่อสนับสนุนการตัดสินใจและการดำเนินงานบริหารจัดการภายใน

องค์กร หรือแม้แต่สร้างความแตกต่างสำหรับบริการใหม่ๆ ให้กับลูกค้า เพราะว่าข้อดีของการนำระบบไอทีมาใช้ก็คือช่วยให้ระบบการทำงานต่างๆมีความคล่องตัว รวดเร็ว ประหยัดเวลา ลดความซ้ำซ้อนของระบบงานลง จึงกล่าวได้ว่าระบบเครือข่ายมีความสำคัญมากเพราะว่าระบบเครือข่ายไม่ได้ทำแค่หน้าที่เชื่อมโยงอุปกรณ์ต่างๆให้เป็นระบบเดียวกันเท่านั้น แต่ระบบเครือข่ายทำหน้าที่เสมือนโครงสร้างพื้นฐานของระบบเทคโนโลยีสารสนเทศในการสร้างโซลูชั่นหรือแอพพลิเคชั่นสำหรับบริหารจัดการธุรกิจและเพิ่มขีดความสามารถในการแข่งขันขององค์กร ดังนั้นการรับส่งข้อมูลในระบบเครือข่ายจะสามารถทำงานได้ต่อเนื่อง ถูกต้อง รวดเร็ว และมีประสิทธิภาพได้นั้น ระบบเครือข่ายนั้นจะต้องได้รับการออกแบบที่ดี เหมาะสมกับธุรกิจ และต้องไม่ใช้เงินลงทุนมากเกินไป อย่างไรก็ตาม อีกเรื่องหนึ่งที่มีความสำคัญมากในปัจจุบัน ทั้งเจ้าของธุรกิจเองและผู้ออกแบบระบบเครือข่ายหรือระบบไอทีจะมองข้ามไปไม่ได้เลย นั่นก็คือเรื่องความมั่นคงปลอดภัย เนื่องจากทุกวันนี้ระบบเครือข่ายมีความหลากหลายและสลับซับซ้อนมากกว่าแต่ก่อนจากที่เคยใช้เฉพาะภายในองค์กรหรือเฉพาะหน่วยงานในสมัยก่อน แต่ปัจจุบันมีการติดต่อแลกเปลี่ยนข้อมูลข่าวสารกับองค์กรภายนอกหรือกับคู่ค้าทางธุรกิจมากขึ้น มีการแชร์ข้อมูลบางระบบให้บุคคลภายนอกเข้ามาใช้งานและมีการเข้าไปใช้ข้อมูลจากระบบเครือข่ายภายนอกองค์กรด้วยเหมือนกัน จะเห็นได้ว่าระบบเครือข่ายและระบบไอทีทุกวันนี้มีความต้องการการใช้งานที่หลากหลาย และผู้เข้าใช้งานระบบเองก็มีหลายกลุ่ม เช่น พนักงาน ผู้บริหาร ที่ปรึกษาแขกผู้มาติดต่อเป็นครั้งคราว รวมทั้งบริษัทคู่ค้าด้วย และพฤติกรรมของผู้ใช้งานระบบเองก็เปลี่ยนไปจากที่เคยใช้งานอยู่กับที่กับโต๊ะทำงานเท่านั้น แต่ทุกวันนี้ความต้องการใช้งานก็เปลี่ยนไปเป็นต้องการใช้งานจากที่ไหนเวลาไหนก็ได้ ทุกๆที่ทุกๆเวลา ตัวอย่างเช่น ผู้บริหารต้องการเช็คอีเมล์จากโทรศัพท์มือถือเมื่ออยู่ข้างนอก พนักงานเองก็อยากทำงานจากส่วนไหนของออฟฟิศก็ได้เช่น ในห้องน้ำ ห้องทานกาแฟ ห้องประชุม หรือจากที่บ้านด้วยก็ได้ดังนั้นความต้องการระบบเครือข่ายในปัจจุบันนอกจากต้องการเครือข่ายที่ดีมีประสิทธิภาพแล้ว ยังไม่เพียงพอต่อความต้องการในปัจจุบัน เรื่องความมั่นคงปลอดภัยในระบบเครือข่ายก็เป็นความต้องการอีกเรื่องหนึ่งที่มีความสำคัญมากที่จะไม่มีไม่ได้ เพราะข้อมูลขององค์กรบางอย่างเป็นความลับถือว่ามีความสำคัญมาก ถ้ามีผู้ไม่ประสงค์ดีสามารถลักลอบเข้ามาในระบบได้แล้วเอาข้อมูลความลับนั้นไปเผยแพร่หรือเอาไปขายให้กับองค์กรที่เป็นคู่แข่งก็จะเกิดความเสียหายกับองค์กรอย่างมาก [7]

ตัวอย่างโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต (Cyber Scout) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อรณรงค์ส่งเสริมให้เด็ก เยาวชน และประชาชนทั่วไป ใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตอย่างมีคุณธรรม จริยธรรม มีความถูกต้องเหมาะสม โดยมีการออกแบบ พัฒนาและนำเนื้อหาหลักสูตรสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ตไปฝึกอบรมเผยแพร่สู่แกนนำ ลูกเสือ ครู/อาจารย์ และบุคคลทั่วไป รวมทั้งมีการสร้างเป็นเครือข่ายสังคมออนไลน์ในภาคประชาชนเพื่อการกำจัดข้อความ สื่อ บทความที่เป็นอันตราย ตลอดจนมีการพัฒนาบทบาทหน้าที่ของลูกเสือไซเบอร์ในมิติของการพัฒนาศักยภาพและการขยายผลเครือข่ายอาสาสมัครในการช่วยสอดส่องดูแลเพื่อการเพิ่มจำนวนให้ได้ในปริมาณที่รวดเร็วขึ้น อีกทั้งกระทรวงฯ ยังได้จัดทำโปรแกรม ICT House Keeper ซึ่งเป็นโปรแกรมสำเร็จรูปเพื่อช่วยให้ครู อาจารย์ และผู้ปกครองสามารถใช้เป็นเครื่องมือป้องกันเว็บไซต์และกำหนดเวลาการเล่นเกมออนไลน์ของเด็กและเยาวชนได้ทั้งที่บ้านและโรงเรียน[8] นับเป็นโครงการตัวอย่างด้านการเชื่อมโยงเครือข่ายระบบรักษาความปลอดภัยที่ดี ซึ่งสามารถบูรณาการกับกำลังสำรองประเภทนักศึกษาวิชาทหารได้

จากภัยคุกคามด้านไซเบอร์ที่แตกต่างของแต่ละองค์กร ระบบรักษาความปลอดภัยด้านไซเบอร์ ทั้งด้านการรักษาระบบ ฮาร์ดแวร์ ,ซอฟท์แวร์ ซึ่งแต่ละองค์กรย่อมมีวิธีการและกระบวนการที่แตกต่างกันเพื่อให้การทำงานการให้บริการสามารถดำเนินการไปได้ตามปกติ สิ่งหนึ่งในยุทธศาสตร์ชาติคือ “...บูรณาการให้มีความพร้อมและเพียงพอต่อการป้องกันภัยคุกคามทุกมิติ ทุกรูปแบบ และทุกระดับความรุนแรง...” ผู้ที่มีความสามารถด้านนี้ส่วนใหญ่คือวิศวกรจบการการศึกษาวิศวกรรมศาสตร์บัณฑิต สาขาคอมพิวเตอร์รวมถึงผู้ที่ชอบค้นคว้าด้านคอมพิวเตอร์ซึ่งมีความรู้ความสามารถในการเชื่อมโยงเครือข่ายการรักษาความปลอดภัย

ข้อพิจารณาจากข้อมูลคุณลักษณะแต่ละด้าน จากการศึกษาข้อมูลที่ค้นพบ บุคลากรที่จะทำงานด้านไซเบอร์ได้ดีต้องมีความสามารถทั้ง เชิงรุก(โจมตี) และ เชิงรับ(ป้องกัน) มีลักษณะนิสัยชอบการค้นคว้าด้านไอที กระตือรือร้น ตื่นตัว มีความสามารถในการเชื่อมโยงข้อมูลที่ค้นพบในระบบ ค้นหาและตอบโต้ภัยคุกคามได้รวดเร็ว มีความคิดเชิงบวก เป็นนักสร้างสรรค์พัฒนาความรู้ด้านไอที ไม่หยุดนิ่ง เข้าใจรูปแบบระบบการรักษาความ

ปลอดภัยด้านไซเบอร์ขององค์กรอย่างถ่องแท้ สามารถทำวิจัยโครงการเกี่ยวกับการออกแบบระบบการรักษาความปลอดภัยขององค์กรได้

ข้อเสนอแนะคุณลักษณะอันพึงประสงค์ ของกำลังสำรองซึ่งเชี่ยวชาญงานด้านไซเบอร์ที่เหมาะสมกับการบรรจุเพื่อสนับสนุนการป้องกันภัยคุกคามด้านไซเบอร์ของกองทัพบก

ที่ผ่านมาหน่วยต่างๆ ในกองทัพบกมีอัตราการจัดยุทโธปกรณ์เป็นอัตราลด โดยบรรจุกำลังพลสำรองไว้ในบัญชีที่ได้จัดทำไว้ให้ครบ 100 เปอร์เซ็นต์ตามอัตราการจัด ซึ่งจะมีการเรียกมาฝึกตามแผนป้องกันประเทศตามกฎหมายเดิมเป็นการฝึกการรบตามแบบ ปัจจุบันจะเป็นการเรียกกำลังพลสำรองเพื่อรับราชการ ตามพระราชบัญญัติกำลังพลสำรองปี 2558 โดยจะเรียกเข้ามารับราชการทหารตามกำหนดเวลา หากหน่วยระดับกองพันขึ้นไปสามารถบรรจุกำลังพลสำรองที่มีความเชี่ยวชาญทางด้านไซเบอร์ไว้ในบัญชีของหน่วย ก็จะสามารถเรียกเข้ามาเพื่อรับราชการ และใช้ประโยชน์จากความสามารถของกำลังพลสำรองแต่ละคนได้

จากการค้นคว้าข้อมูลด้านไซเบอร์และไอที ของผู้วิจัย ทำให้ทราบถึงความอันตรายของภัยคุกคามด้านไซเบอร์ของ กองทัพบก ซึ่งมีผลต่อพลังอำนาจของชาติทุกด้าน การโจมตีระบบฐานข้อมูลของกองทัพบก หรือหน่วยในกองทัพบก วัตถุประสงค์เพื่อ ทำให้ระบบการทำงานช้าลง หรือขโมยข้อมูลเพื่อนำไปใช้ประโยชน์ในทางลบ เช่น รบกวนให้เกิดความล่าช้า ลดความน่าเชื่อถือ บ่อนทำลายสร้างความแตกแยก จากฝ่ายที่ไม่เห็นด้วยกับกองทัพและรัฐบาล และมักจะได้รับการยอมรับจาก ฝ่ายเป็นกลาง ข้อจำกัดของกองทัพบกคือกำลังพลที่บรรจุและรับราชการอยู่ในปัจจุบัน ยังขาดขีดความสามารถในการตอบโต้สื่อเชิงลบต่างๆ ในโลกโซเชียล แต่ยังมีกำลังพลสำรองอยู่เป็นจำนวนมากที่มีขีดความสามารถด้านไอทีที่สามารถชดเชยข้อจำกัดนี้ ทั้งนี้ต้องมีการคัดกรองที่เหมาะสม

ข้อเสนอแนะของงานวิจัย

กำลังสำรองซึ่งเชี่ยวชาญด้านไซเบอร์เพื่อสนับสนุนการป้องกันภัยคุกคามด้านไซเบอร์ของกองทัพบก คุณลักษณะที่เหมาะสมได้แก่

1. บุคลากรที่จบการศึกษาด้านคอมพิวเตอร์ ผู้สนใจศึกษาค้นคว้าด้านไอที เช่น ผู้ประกอบการร้านอินเตอร์เน็ต ร้านรับลงโปรแกรม หรือขายแผ่นโปรแกรมต่างๆ
2. มีความรู้ความสามารถในการเขียนโครงการวิจัยเกี่ยวกับระบบการรักษาความปลอดภัยด้านไซเบอร์เพื่อเป็นต้นแบบให้กับกองทัพบกนำไปเผยแพร่ให้กับหน่วยต่างๆ และบูรณาการร่วมกับองค์กรต่างๆ ด้วยการเชื่อมโยงเครือข่ายระบบการรักษาความปลอดภัยด้านไซเบอร์
3. มีความสามารถในการ ค้นหา ตรวจสอบ ป้องกัน ลดผลกระทบ ฟื้นฟู ความเสียหายของระบบที่เกิดจากการโจมตีทางไซเบอร์
4. มีอุดมการณ์ ยึดผลประโยชน์ของชาติในการทำงาน ยึดมั่นในสถาบันหลักของชาติเป็นสิ่งสำคัญ กองทัพบกต้องสร้างแรงจูงใจและมีสิ่งตอบแทนที่เหมาะสม เนื่องจากกำลังสำรองเหล่านี้ส่วนใหญ่จะมี ตำแหน่งหน้าที่ในองค์กรเอกชนหรือภาครัฐ

ตามพระราชบัญญัติกำลังพลสำรอง ปี 2558 กำลังสำรองเหล่านี้ มีที่มาจาก ทหารกองเกินที่จับใบดำ นักศึกษาวิชาทหาร หรือทหารกองประจำการที่ปลดประจำการ ถ้าหน่วยระดับกองพันขึ้นไป สามารถนำมาบรรจุในบัญชีบรรจุกำลังพลสำรองของหน่วยเพื่อใช้งานด้านไซเบอร์หรือไอทีของหน่วยได้