ศูนย์ไซเบอร์กองทัพบก

อริย์ธัช แก้วเกาะสะบ้า
วิทยากรชำนาญการพิเศษ
กลุ่มงานบริการวิชาการ 1 สำนักวิชาการ

ความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสารได้ถูกนำมาใช้เป็นเครื่องมือเพื่อการพัฒนาประเทศโดยนำมาพัฒนาองค์กรให้มีความทันสมัยเพื่อเพิ่มศักยภาพ และการสร้างภาพลักษณ์หรือการยกระดับการพัฒนาให้องค์กรมีความเท่าเทียมกับองค์กรอื่น ๆ ซึ่งปัจจุบันได้นำเทคโนโลยีมาใช้ครอบคลุมในด้านต่าง ๆ เช่น ด้านเศรษฐกิจ ด้านการเมือง ด้านสังคมจิตวิทยา ด้านการทหาร และด้านการรักษาความมั่นคงภายในของประเทศ โดยเฉพาะการพัฒนาศักยภาพให้แก่กองทัพเพื่อให้มีความพร้อมรับมือต่อภัยคุกคามทางด้านไซเบอร์ ซึ่งเป็นภัยร้ายแรงที่ส่งผลต่อวิถีชีวิตของประชาชนในประเทศเพราะสังคมปัจจุบันมีการติดต่อสื่อสารกันระหว่างบุคคลอย่างสะดวกรวดเร็ว และการใช้อุปกรณ์การสื่อสารเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยมีการเชื่อมต่อสัญญาณอินเทอร์เน็ตซึ่งมีความเร็วสูงเข้าสู่ระบบคอมพิวเตอร์นับล้าน ๆ เครื่องทั่วโลก การนำระบบคอมพิวเตอร์มาใช้เป็นจำนวนมากภายในองค์กรเพื่อเพิ่มประสิทธิภาพในการทำงานและเชื่อมต่อกับองค์กรภายนอกไม่ว่าจะอยู่ในพื้นที่ใดในโลก ก็เป็นการเปิดช่องทางการเข้าถึงของผู้ที่ไม่หวังดีต่อองค์กรสามารถเข้ามาโจมตีระบบเครือข่ายคอมพิวเตอร์ซึ่งเรียกกันโดยทั่วไปว่าแฮกเกอร์ (Hacker) คือการเข้าโจมตีระบบเครือข่ายคอมพิวเตอร์จนทำให้ระบบล่มและไม่สามารถใช้งานได้ทำให้เกิดความเสียหายจนเสียระบบการควบคุม การโจมตีทางไซเบอร์ถือเป็นภัยคุกคามที่ร้ายแรงที่สร้างความเสียหายแก่ระบบการสื่อสารหรือระบบเครือข่ายคอมพิวเตอร์ได้อย่างมหาศาลโดยการโจมตีผ่านเครือข่ายอินเทอร์เน็ตจากส่วนหนึ่งส่วนใดในประเทศต่าง ๆ ในโลกนี้

การรักษาความปลอดภัยหรือป้องกันการโจมตีระบบคอมพิวเตอร์เป็นสิ่งที่ฝ่ายความมั่นคงได้ติดตามสถานการณ์ และได้เตรียมความพร้อมในการรับมือในสถานการณ์ฉุกเฉินอยู่ตลอดเวลา โดยเฉพาะกองทัพบกของไทยได้ตระหนักถึงภัยอันตรายจากการสื่อสารซึ่งเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตของระบบเครือข่ายคอมพิวเตอร์นับล้าน ๆ เครื่อง โดยได้เริ่มทำการศึกษาและเตรียมความพร้อมให้แก่กำลังพลเพื่อรับมือกับการโจมตีทางไซเบอร์ที่กองทัพบกโดย พลเอก ประยุทธ์ จันทร์โอชา อดีตผู้บัญชาการทหารบก ได้มีนโยบายและอนุมัติหลักการจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ขึ้นเพื่อปฏิบัติงานให้เป็นไปตามนโยบายของรัฐบาลโดยร่วมมือกับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security ; NCSC) โดยได้เริ่มทดลองปฏิบัติงานตั้งแต่ 1 ตุลาคม 2557 ซึ่งปฏิบัติไปพร้อมกับเหล่าทัพต่าง ๆ โดยมีกองบัญชาการกองทัพไทย กองทัพเรือ กองทัพอากาศ สำนักงานตำรวจแห่งชาติ และกระทรวงกลาโหมซึ่งเป็นองค์กรที่กำหนดนโยบายเพื่อเตรียมความพร้อมกับภัยคุกคามทางไซเบอร์ ซึ่งในระยะเริ่มแรกจัดตั้งขึ้นที่ศูนย์เทคโนโลยีทางทหาร (ศทท.) ได้ดำเนินการปรับปรุงภารกิจและโครงสร้างการจัดหน่วยโดยได้เพิ่มเติมภารกิจด้านการปฏิบัติการสงครามไซเบอร์และปรับสายการบังคับบัญชาจากเดิมขึ้นตรงต่อกรมการทหารสื่อสาร

มาเป็นหน่วยขึ้นตรงต่อกองทัพบก (นขต.ทบ.) เพื่อรองรับการปฏิบัติงานด้านความมั่นคงปลอดภัยทางด้านไซเบอร์ซึ่งกระทบต่อความมั่นคงของชาติทั้งภายในและภายนอกประเทศ โดยเน้นหนักไปที่ความมั่นคงทางทหาร และการรักษาความสงบเรียบร้อยภายในประเทศ รวมทั้งการทำงานที่สอดประสานกับหน่วยงานในเหล่าทัพ และกระทรวงกลาโหม รวมทั้งได้ร่วมมือกับหน่วยงานของภาครัฐและภาคเอกชน ตลอดจนการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations ; NCO) จากการเตรียมความพร้อมเรื่องความมั่นคงทางไซเบอร์มาโดยตลอดนั้น ต่อมาในปี 2559 ศูนย์เทคโนโลยีทางทหาร (ศทท.) ได้แปรสถานภาพหน่วยมาเป็นศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) มีฐานะเป็นหน่วยขึ้นตรงต่อกองทัพบกตั้งแต่ 1 ตุลาคม 2559 จนถึงปัจจุบัน

เมื่อวันที่ 1 พฤศจิกายน 2559 ได้มีการปรับปรุงยกระดับหน่วยอีกครั้งโดย พลเอก เฉลิมชัย สิทธิสาท ผู้บัญชาการทหารบกได้ทำการเปิดศูนย์ไซเบอร์กองทัพบกอย่างเป็นทางการซึ่งได้แบ่งโครงสร้างหน่วยเป็นสำนักงานผู้บังคับบัญชา กองธุรการ กองปฏิบัติการไซเบอร์ กองรักษาความปลอดภัยไซเบอร์ กองสนับสนุนปฏิบัติการข่าวไซเบอร์ สำหรับกองปฏิบัติการไซเบอร์ กองรักษาความปลอดภัยไซเบอร์ และกองสนับสนุนปฏิบัติการข่าวสารไซเบอร์มีอำนาจหน้าที่ ดังนี้

1. กองปฏิบัติการไซเบอร์ทำหน้าที่เป็นศูนย์ปฏิบัติการไซเบอร์ เพื่อเฝ้าระวัง แจ้งเตือน ป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์ การเผชิญเหตุฉุกเฉินด้านไซเบอร์ ตลอดจนการพัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุก เพื่อให้สามารถปฏิบัติการเชิงรุกและโต้ตอบโจมตีฝ่ายตรงข้ามได้ในกรณีจำเป็น

2. กองรักษาความมั่นคงปลอดภัยไซเบอร์ทำหน้าที่เสริมสร้างความรู้ ความเข้าใจ สร้างความตระหนัก ติดตาม กำกับดูแลการปฏิบัติของหน่วยตามมาตรการการรักษาความมั่งคงปลอดภัย รวมถึงการเฝ้าระวัง แจ้งเตือนภัยคุกคาม การติดตาม สืบค้น และตรวจสอบช่องโหว่ของระบบ โดยใช้เครื่องมือระบบตรวจหาการบุกรุก รวมถึงการกู้คืนสภาพเมื่อถูกโจมตี (Recovery) รวมถึงการดำเนินการพิสูจน์หลักฐานทางดิจิทัล

3. กองสนับสนุนการปฏิบัติการข่าวสารไซเบอร์ เพื่อให้การสนับสนุนการปฏิบัติการข่าวสารของกองทัพบกและหน่วยที่เกี่ยวข้อง โดยทำหน้าที่เฝ้าระวัง แจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ ที่ส่งผลกระทบต่อสถาบันและความมั่งคงของชาติ รวบรวม วิเคราะห์ ทิศทาง แนวโน้ม โครงข่ายความสัมพันธ์ของข้อมูลประเภทสื่อ และกลุ่มเป้าหมาย ติดตาม สืบค้น แหล่งที่มาและเป้าหมาย และกำหนดมาตรการป้องปราม ตอบโต้สกัดกั้น ตลอดจนพัฒนาโปรแกรมและเครื่องมือต่าง ๆ เพื่อรองรับงานด้านไซเบอร์ นอกจากนี้ ยังได้เตรียมการด้านการพัฒนาเทคโนโลยีและนวัตกรรมต่าง ๆ ด้านไซเบอร์โดยแสวงหาความร่วมมือกับหน่วยงานต่าง ๆ ทั้งภายในกองทัพบกและภาครัฐ และองค์กรเอกชนในด้านวิชาการ การวิจัยพัฒนา (R&D) การสัมมนาเชิงปฏิบัติการ (Workshop) และการฝึกปฏิบัติต่าง ๆ โดยเฉพาะการฝึกซ้อมแผนเผชิญเหตุด้านไซเบอร์ (Cyber Incident Action Plan Exercise) การฝึกซ้อมแผนฉุกเฉินด้านไซเบอร์ (Cyber Emergency) รวมถึงการประสานงานเพื่อดำเนินการตามกฎหมายกับผู้ที่โจมตีระบบเครือข่ายคอมพิวเตอร์

การจัดตั้งศูนย์ไซเบอร์กองทัพบกเพื่อพัฒนากองทัพให้ทันสมัยโดยสามารถทำงานให้สอดคล้องกับหน่วยงานภาครัฐอื่น ๆ โดยจะเน้นการปกป้องงานของกองทัพบกเพื่อป้องกันการถูกแทรกแซงจากแฮกเกอร์

ต่าง ๆ รวมทั้งงานที่เกี่ยวข้องกับด้านการข่าว โดยเน้นหนักไปในเรื่องการพัฒนากำลังคนและเครื่องมือ โดยเฉพาะที่กองทัพมีพื้นฐานรองรับงานต่าง ๆ ไว้แล้ว กองทัพบกได้มองเห็นปัญหาของภัยคุกคามทางไซเบอร์ ซึ่งมีการใช้เทคโนโลยีเข้ามาทำลายความมั่นคงของประเทศจึงได้เร่งพัฒนาเสริมศักยภาพของกองทัพไว้ให้พร้อมกับภัยที่กำลังเกิดขึ้น โดยเฉพาะประเทศไทยได้เรียนรู้จากประเทศที่เป็นมหาอำนาจทางทหาร ซึ่งประเทศเหล่านั้นได้กำหนดพลังอำนาจทางทหารไว้ 5 ด้าน หรือเรียกว่าเป็นโดเมน คือ 1) พื้นที่ปฏิบัติการบนดิน (Land Domain) 2) พื้นที่ปฏิบัติการในน้ำ (Sea Domain) 3) พื้นที่ปฏิบัติการในอากาศ (Air Domain) 4) พื้นที่ปฏิบัติการบนห้วงอวกาศ (Space Domain) และ 5) พื้นที่ปฏิบัติการด้านไซเบอร์โดเมน (Cyber Domain) ซึ่งโดเมนที่ 5 มีความสำคัญมาก เพราะประเทศที่มีกำลังทหารมากและมีอาวุธที่ทันสมัย แต่ถ้าหากไม่สามารถควบคุมไซเบอร์โดเมน (Cyber Domain) ซึ่งเป็นส่วนควบคุมหรือบังคับบัญชาได้ก็ไม่มีประโยชน์เพราะสงครามในยุคใหม่จะไม่เห็นภาพการเคลื่อนกำลังทหารในการรบ แต่จะมีการควบคุมสั่งการของกองทัพผ่านเครือข่ายคอมพิวเตอร์ ถ้าหากระบบควบคุมสั่งการของกองทัพได้ถูกทำลายไปและบิดเบือนข้อมูลต่าง ๆ ระบบบังคับบัญชาและระบบสั่งการใช้ไม่ได้กองทัพในยุคสมัยใหม่ก็จะพ่ายแพ้ในสมรภูมิรบ ในสังคมยุคไซเบอร์การเสริมสร้างกำลังทางทหารเพื่อการรบในพื้นที่ปฏิบัติการต่าง ๆ นั้นต้องใช้งบประมาณทางทหารเป็นจำนวนมาก เพราะงบประมาณทางทหารเป็นรายได้ที่จัดเก็บจากภาษีรายได้จากประชาชนทั้งประเทศ หากมีงบประมาณรายจ่ายทางทหารมากก็จะกลายเป็นภาระของประเทศทำให้หลายประเทศได้ตระหนักในเรื่องภัยคุกคามที่ร้ายแรง กองทัพของประเทศต่าง ๆ จึงพัฒนาปรับปรุงเพิ่มศักยภาพของกองทัพประเทศตนเองโดยการสร้างไซเบอร์ วอริเออร์ หรือเรียกว่านักรบไซเบอร์ ในความหมายของการรักษาความมั่นคงในปัจจุบันเรียกว่าอำนาจการรบที่ไร้ตัวตนขึ้นแทน (ฤทธี อินทราวุธ, ม.ป.ป. น. 1)

ภัยคุกคามทางด้านไซเบอร์ (Cyber Threats)

ภัยคุกคามทางด้านไซเบอร์ในวงการทหารถือว่าเป็นภัยที่คุกคามความมั่นคงของชาติซึ่งเชื่อมโยงไปสู่ด้านต่าง ๆ การกระทำทั้งหมดนั้นเป็นภัยที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในทางที่ผิดกฎหมาย รวมทั้งการละเมิดต่อศีลธรรมและความสงบสุขของสังคม เป็นภัยร้ายแรงอีกรูปแบบหนึ่งในด้านการทหาร ซึ่งภัยคุกคามทางด้านไซเบอร์มีหลายรูปแบบ ดังนี้

1. การโจมตีด้วยวิธีเจาะระบบ (Hacking) เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมแฮ็กหลากหลายรูปแบบที่สามารถดาว์นโหลดโปรแกรมแฮกมาใช้ได้ง่ายในโลกอินเทอร์เน็ต ไม่ต้องเป็นผู้เชี่ยวชาญก็สามารถเจาะระบบได้ ผู้ใช้งานอินเทอร์เน็ตจะต้องเฝ้าระวังและป้องกันตนเองให้ปลอดภัย แฮกเกอร์นั้นมีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการท้าทายโดยการเจาะระบบให้สำเร็จหรือมีจุดประสงค์เพื่อต้องการทำลายระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศเท่านั้น

2. การโจมตีโดยทำการฝังโปรมแกรมลับลอบโจรกรรมข้อมูล คือ การใช้สปายแวร์ (Spyware) หรือประตูหลัง (Back Door) ระบบคอมพิวเตอร์มีระบบรักษาความมั่นคง แต่ยังมีรูรั่วหรือช่องโหว่ของระบบรักษาความมั่นคงที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว้โดยเป็นกลไกลับทางซอฟต์แวร์หรือฮาดแวร์ จึงทำให้ผู้ไม่

ประสงค์ดีสามารถใช้ช่องโหว่นี้ผ่านระบบรักษาความมั่นคงเข้ามาในระบบและสร้างความเสียหายต่อระบบคอมพิวเตอร์ได้

3. การโจมตีด้วยโปรแกรมมัลแวร์ (Malware) หมายถึงซอฟแวร์ที่เขียนขึ้นที่มีวัตถุประสงค์ในทางร้ายหรือเป็นภัยคุกคามต่อระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ให้ไปทำความเสียหายต่อคอมพิวเตอร์ที่เจ้าของหรือผู้ใช้ไม่ได้อนุญาต โปรแกรมมัลแวร์จะส่งผลให้คอมพิวเตอร์เสียหาย คือ สูญเสียความลับทางข้อมูล สูญเสียข้อมูลที่ถูกเปลี่ยนแปลงแก้ไขโดยเฉพาะส่วนสำคัญที่เกี่ยวโยงกับระบบภายในระบบปฏิบัติการ และสูญเสียเสถียรภาพของระบบปฏิบัติการของคอมพิวเตอร์ โปรมแกรมมัลแวร์นั้นมีทั้งที่เป็นไวรัสคอมพิวเตอร์ และหนอนคอมพิวเตอร์

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

5. การโจมตีด้วยหนอนคอมพิวเตอร์ (Computer Worm) หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้ โดยมากจะคัดลอกและกระจายตัวของหนอนคอมพิวเตอร์เองในเครือข่ายและข้ามเครือข่ายได้ สามารถทำลายข้อมูลและสร้างความเสียหายให้กับคอมพิวเตอร์ได้

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

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

8. การโจมตีโดยใช้หุ่นยนต์ (Botnet) เป็นภัยคุกคามด้านสารสนเทศที่เกิดกลับกลุ่มของเครื่องคอมพิวเตอร์ที่มีโปรแกรมไม่พึงประสงค์ติดตั้งอยู่ ซึ่งโปรแกรมไม่พึงประสงค์นั้นจะทำการรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ต โดยอาจจะเป็นคำสั่งที่ให้ทำการโจมตีระบบเครือข่ายหรือส่งสแปม และโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์นั้น

9. การโจมตีแบบ (DoS/DDos) การโจมตีสภาพพร้อมใช้งานของระบบคอมพิวเตอร์ โดยมีการโจมตีมาจากหลายที่โดยแต่ละที่จะโจมตีเป้าหมายเดียวกันภายในเวลาเดียวกัน เพื่อทำให้บริการต่าง ๆ ของระบบคอมพิวเตอร์ไม่สามารถให้บริการได้ตามปกติมีผลกระทบต่อการให้บริการและเกิดความล่าช้าในการตอบสนองของผู้รับบริการจนกระทั่งระบบไม่สามารถให้บริการได้ต่อไปและทำให้เกิดเว็บไซต์ล่มในที่สุด

10. การโจมตีด้วย (Ransomware) คือ มัลแวร์เรียกค่าไถ่เป็นซอฟต์แวร์ที่ได้รับการพัฒนาขึ้นเพื่อเข้ารหัสลับไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ หรือปิดกั้นไม่ให้ผู้ใช้เข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ได้โดยเรียกร้องให้เหยื่อจ่ายเงินเพื่อจะได้รับกุญแจถอดรหัสไฟล์หรือปลดล็อกการใช้งานเครื่องคอมพิวเตอร์ซึ่งปัจจุบันจะมีภัยคุกคามลักษณะนี้เพิ่มมากขึ้น

การกำหนดระดับภัยคุกคามทางด้านไซเบอร์ของประเทศสหรัฐอเมริกา

ภัยคุกคามทางด้านไซเบอร์ถือว่าเป็นอันตรายต่อความมั่นคงของชาติ เป็นภัยร้ายแรงสร้างความเสียหายในวงกว้างกระทบต่อพลเมืองเป็นจำนวนมาก หน่วยรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber security and Integration Center: NCCIC) ของประเทศสหรัฐอเมริกา ได้กำหนดระดับภัยคุกคามด้านไซเบอร์ไว้ 5 ระดับ ดังนี้

1. ภัยคุกคามในระดับรัฐบาลแห่งชาติ คือภัยที่เป็นอันตรายต่อประเทศชาติเป็นการปล่อยข่าวที่ไม่น่าเชื่อถือ การเข้าไปโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ในหน่วยงานของรัฐ หรือการเจาะระบบของโครงสร้างพื้นฐานที่เป็นระบบการเงินการธนาคาร และระบบสาธารณูปโภค เช่น ระบบไฟฟ้า ระบบประปา ซึ่งให้บริการกับประชาชนในประเทศ

2. ภัยจากการก่อการร้ายสากล โดยเฉพาะกลุ่มก่อการร้ายต้องการโจมตีต่อประเทศคู่ขัดแย้งทางการเมือง มุ่งทำลายผลประโยชน์ทางการเมือง เพื่อสร้างความหวาดกลัวไปยังประชาชนในประเทศนั้น ๆ

3. ภัยจากสายลับหรือพวกจารกรรมข้อมูลในภาคอุตสาหกรรม และองค์กรเครือข่ายอาชญากรรม ซึ่งภัยด้านนี้จะกำหนดให้เป็นภัยคุกคามระดับกลางของประเทศ

4. ภัยจากกลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ ซึ่งเกิดจากการรวมกลุ่มของพวกแฮกเกอร์กลุ่มเล็ก ๆ โดยรวมกลุ่มกันโจมตีเว็บไซต์ของรัฐบาลโดยมีแรงจูงใจจากอุดมการณ์ทางการเมืองหรือความคิดเห็นที่แตกต่างทางการเมืองเพราะกลุ่มแฮ็กเกอร์เหล่านั้นเห็นว่ารัฐหรือหัวหน้ารัฐบาลในประเทศนั้น ๆ ได้ดำเนินนโยบายที่ขัดต่อสิทธิเสรีภาพในการแสดงออกหรือลิดรอนสิทธิเสรีภาพของบุคคล และการปิดกั้นสิทธิเสรีภาพทางการเมืองของประชาชน

5. ภัยจากกลุ่มแฮ็กเกอร์มือสมัครเล่น โดยกลุ่มแฮ็กเกอร์จะประชาสัมพันธ์ทางเว็บไซต์เพื่อรวบรวมพวกมือสมัครเล่นให้ร่วมกันโจมตีเว็บไซต์ของหน่วยงานภาครัฐและภาคเอกชน และส่งผลกระทบอย่างกว้างขวางจนสร้างความเสียหายในระยะยาวให้กับโครงสร้างพื้นฐานในระดับชาติที่ถูกโจมตีได้อย่างมหาศาล ภัยคุกคามทางไซเบอร์ทั้ง 5 ประการจะเกิดขึ้นในประเทศมหาอำนาจทางทหาร คือ สหรัฐอเมริกาและประเทศในยุโรปที่มีความก้าวหน้าทางเทคโนโลยีสารสนเทศอย่างมาก แต่ภัยเหล่านี้ยังสามารถนำมาเป็นบทเรียนให้แก่ประเทศเล็ก ๆ เช่น ประเทศไทยได้ซึ่งต้องการยกระดับเพิ่มศักยภาพในการรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์

การกำหนดระดับภัยคุกคามทางด้านไซเบอร์ของประเทศไทย

กรณีประเทศไทยภัยคุกคามทางด้านไซเบอร์นั้น ได้กำหนดระดับความปลอดภัยเช่นเดียวกับประเทศสหรัฐอเมริกา แต่ระดับความรุนแรงของประเทศไทยไม่มากเหมือนประเทศมหาอำนาจ ส่วนใหญ่จะมีเพียงภัยคุกคามทางไซเบอร์ในระดับของการปล่อยไวรัสคอมพิวเตอร์ และการปล่อยมัลแวร์ รวมทั้งการแฮก

หน้าเว็บไซต์หรือเปลี่ยนแปลงรูปหน้าเว็บไซต์ ซึ่งศูนย์ไซเบอร์กองทัพบกได้ตระหนักในภัยคุกคามดังกล่าว โดยได้เฝ้าระวัง ตรวจสอบ พร้อมทั้งการฝึกกำลังพลให้สามารถแก้ไขหรือตอบโต้ได้ในกรณีที่ถูกโจมตีทางไซเบอร์ และกำหนดให้การรักษาความมั่นคงทางด้านไซเบอร์เป็นภารกิจที่สำคัญในด้านความมั่นคงของชาติ และได้กำหนดระดับภัยคุกคามทางด้านไซเบอร์เป็น 4 ด้าน ดังนี้

1. ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ เป็นภัยคุกคามในระดับประเทศหรือระดับชาติ ผู้ที่ก่อภัยคุกคามอาจใช้วิธีนำข่าวสารเหล่านั้นลงเผยแพร่ในเว็บไซต์ของประเทศตนเองเพื่อให้ข่าวสารเหล่านั้นเผยแพร่เข้ามาสู่ประเทศไทยจนส่งผลกระทบต่อความมั่นคงภายในประเทศไทย และทำให้เกิดความได้เปรียบทางการเมืองหรือด้านความมั่นคง รวมทั้งการเผยแพร่ข้อมูลความลับของประเทศไทย และการแพร่กระจายโปรแกรมไม่พึงประสงค์สำหรับการทำลายเครือข่ายระบบคอมพิวเตอร์

2. ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.) เป็นการใช้ไซเบอร์ที่เป็นภัยคุกคามต่อความมั่นคงของชาติในการเผยแพร่ข่าวสารของผู้ก่อความไม่สงบ เช่น การเผยแพร่ข่าวลือ ข่าวที่ไม่เป็นจริง โดยการกล่าวหาว่าเจ้าหน้าที่ของรัฐทำการละเมิดสิทธิมนุษยชน เพื่อให้สื่อมวลชนกระแสหลักนำข่าวไปเผยแพร่ต่อเพื่อต้องการให้ประชาชนทั่วไปหวาดกลัวจนทำให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่รัฐถือเป็นการปฏิบัติการข่าวสาร (Information Operation) ที่เป็นการปฏิบัติการจิตวิทยาอย่างหนึ่ง นอกจากนั้นยังมีการเผยแพร่ผลงานของผู้ก่อความไม่สงบที่อาจจะส่งผลกระทบทำให้เกิดแนวร่วมของผู้ก่อความไม่สงบเพิ่มมากขึ้น

3. ภัยคุกคามที่ส่งผลกระทบต่อสถาบันของชาติ เป็นสิ่งที่กระทำได้ง่ายและยากต่อการดำเนินคดีต่อผู้กระทำผิดคือการเผยแพร่ภาพที่หมิ่นสถาบันพระมหากษัตริย์ การวิจารณ์สถาบันในทางเสื่อมเสีย ซึ่งเจ้าหน้าที่ของรัฐบาลไทยไม่สามารถดำเนินการตามกฎหมายไทยได้เพราะส่วนหนึ่งของผู้กระทำความผิดไม่ได้อยู่ในประเทศไทยแต่ได้ใช้เว็บไซต์หรือสื่อโซเชียลในต่างประเทศเผยแพร่ข่าวสารเข้ามายังประเทศไทย

4. ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพไทย ทำให้ภาพลักษณ์ของผู้นำกองทัพไทยเสียหายหรือลดความน่าเชื่อถือในสังคมไทย รวมทั้งลดความเชื่อมั่นของประชาชนต่อการปกป้องประเทศไทย และการบังคับบัญชาของเหล่าทัพ ซึ่งส่งผลกระทบต่อการพิทักษ์อธิปไตยของชาติไทย (ฤทธี อินทราวุธ, 2558. น. 1-5)

การเตรียมความพร้อมรับมือกับภัยคุกคามทางด้านไซเบอร์

ประเทศไทยมีภัยคุกคามทางด้านไซเบอร์เป็นจำนวนมาก ระบบคอมพิวเตอร์ของไทยถูกใช้เป็นฐานในการโจมตีไปยังประเทศอื่นด้วย ทำให้เกิดความเสียหายเป็นวงกว้าง หรือเสียหายต่อทรัพยากร ภาพลักษณ์ และความเชื่อมั่นต่อประเทศ การโจมตีเป็นการเข้าไปเปลี่ยนแปลงหน้าเว็บเพจของหน่วยงานภาครัฐซึ่งเกิดเหตุขึ้นบ่อยครั้ง ฝ่ายความมั่นคงโดยเฉพาะกองทัพบกจึงต้องมีการดำเนินการจัดตั้งศูนย์ไซเบอร์กองทัพบก เนื่องจากมีกลุ่มผู้ไม่หวังดีใช้เครือข่ายมุ่งโจมตีหน่วยงานของรัฐ หรือการเผยแพร่ข่าวสารอันเป็นเท็จที่ส่งผลกระทบต่อความมั่นคงของชาติ การรักษาความปลอดภัยทางไซเบอร์ของกองทัพบกจะเน้นความร่วมมือกับหน่วยงานภาครัฐและองค์กรภาคเอกชนโดยร่วมมือทั้งเรื่ององค์ความรู้ และการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ที่เป็นภัยคุกคามร้ายแรงต่อระบบเครือข่ายคอมพิวเตอร์โดยฝึกผู้เชี่ยวชาญด้านไซเบอร์โดยเน้นในเรื่องการรักษาความปลอดภัยทางไซเบอร์ 3 ประการ ดังนี้

1. การป้องกัน (Identify & Protect) โดยการตรวจสอบช่องโหว่ที่มีในระบบ การทดสอบการเจาะการเข้าสู่ระบบ หากตรวจพบช่องโหว่ในระบบจะได้ดำเนินการแก้ไขให้มีความปลอดภัยเพิ่มขึ้น

2. การเฝ้าระวังแบบเรียลไทม์ (Detect) ต้องทำการตรวจสอบ วิเคราะห์ภัยคุกคามทางด้านไซเบอร์ขั้นสูง การรวบรวมและศึกษาข่าวกรอง และการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ที่จะเกิดขึ้น

3. การสนองตอบภัยคุกคามแบบเรียลไทม์ (Repond) โดยจัดทำแผนตอบสนองต่อภัยคุกคามตามขั้นตอนที่ได้กำหนดไว้ คือการสืบสวนสอบสวนทางดิจิทัลและนิติวิทยาศาสตร์ การวิเคราะห์หาสาเหตุของภัยคุกคามที่เกิดขึ้น รวมถึงการประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อดำเนินงานตามขั้นตอนของกฎหมาย

ศูนย์ไซเบอร์กองทัพบกมีเป้าหมายในการพัฒนาขีดความสามารถของกองทัพบกให้ทันสมัยและรองรับภัยคุกคามทางไซเบอร์ได้หลากหลายรูปแบบ ซึ่งกระทรวงกลาโหมนั้นได้กำหนดให้ภัยคุกคามทางไซเบอร์เป็นภยันตรายต่อความมั่นคงของชาติ และกำหนดให้ภัยคุกคามทางไซเบอร์ดังกล่าวเป็นภารกิจของกระทรวงกลาโหม กองบัญชาการกองทัพไทย กองทัพเรือ กองทัพอากาศ สำนักงานตำรวจแห่งชาติ ดังนั้น ศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) ในฐานะที่เป็นหน่วยรับผิดชอบงานด้านไซเบอร์ยังได้เพิ่มการพัฒนาโดยการฝึกอบรมกำลังพลของกองทัพบกซึ่งเป็นนายทหารสัญญาบัตรและชั้นประทวนประจำปี 2560 ขึ้นอีก 7 หลักสูตร ดังนี้

หลักสูตรที่ 1 คือการปฏิบัติการด้านไซเบอร์เบื้องต้น ประกอบไปด้วยการปฏิบัติการไซเบอร์ (Kali Linux) การเจาะระบบเบื้องต้น องค์ประกอบพื้นฐานของ Information Security ประเภทภัยคุกคาม (Threat) ขั้นตอนการโจมตี Ethical Hacker 9 ขั้นตอน Network Mapping และการทำ Scanning เบื้องต้น

หลักสูตรที่ 2 การปฏิบัติการไซเบอร์ขั้นสูง ศึกษาช่องโหว่ระบบปฏิบัติการต่าง ๆ ขั้นตอนการทดสอบการเจาะระบบข้อมูลของผู้ทดสอบเจาะระบบ โปรมแกรมทดสอบการเจาะระบบ (Metasploit Framework) การโจมตี Web Application

หลักสูตรที่ 3-4 การรักษาความปลอดภัยทางไซเบอร์ (Cyber Security) สำหรับนายทหารสัญญาบัตรและนายทหารชั้นประทวน การติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายให้ปลอดภัย การรักษาความปลอดภัย Intrusion Detection System (IDS) ระบบตรวจจับการบุกรุกเป็นระบบที่ใช้สำหรับการเฝ้าระวังและแจ้งเตือนภัยถ้ามีการบุกรุก Internet Service Provider (ISP) ระบบการเชื่อมต่อเครือข่ายอินเทอร์เน็ตเพื่อเปิดใช้งานกับเว็บไซต์ต่าง ๆ Intrusion Prevention System (IPS) การหยุดการบุกรุกจะใช้หลักการที่เรียกว่า “Inline” หรือที่เรียกว่า “Gateway IDS” ซึ่งก็คือ การนำ IPS ไปกั้นกลางบนเส้นทางการส่งข้อมูลโดยไม่ต้องมีการกำหนดหมายเลขไอพีให้กับ IDS/IPS เป็นระบบรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์เพื่อเป็นเครื่องมือสำหรับการสืบสวนบุคคลที่โจมตี บุกรุก เก็บสถิติเกี่ยวกับการโจมตี และนำข้อมูลไปวิเคราะห์ภัยคุกคามและเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัย เช่น ไฟร์วอล เป็นต้น Firewall, Virus, Malware, Ransomware และการป้องกันการโจมตี Web Application กฎหมายอาชญากรรมทางไซเบอร์

หลักสูตรที่ 5-6 นายทหารรักษาความปลอดภัยไซเบอร์และเจ้าหน้าที่รักษาความปลอดภัยของนายทหารชั้นประทวน ฝึกอบรมความตะหนักและการรักษาความปลอดภัยทางด้านไซเบอร์ คอมพิวเตอร์และระบบปฏิบัติการ ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) VA and Penetration Tesing, Vulnerability Scaning, Penetration Testing, Log Analysis

หลักสูตรที่ 7 การบริหารจัดการข่าวสารทางไซเบอร์ของนายทหารระดับชั้นสัญญาบัตร และนายทหารชั้นประทวน โดยฝึกอบรมพื้นฐานด้านการข่าวและวงรอบข่าวกรอง หลักการประชาสัมพันธ์และการสื่อสารมวลชน กฎหมายที่เกี่ยวข้องกับพระราชบัญญัติคอมพิวเตอร์ และพระราชบัญญัติลิขสิทธิ์ เทคนิคการโฆษณาประชาสัมพันธ์ทางอินเทอร์เน็ตรูปแบบต่าง ๆ

ศูนย์ไซเบอร์กองทัพบกได้เตรียมความพร้อมเพื่อเผชิญกับภัยคุกคามทางด้านไซเบอร์โดยการจัดหลักสูตรฝึกอบรมเพื่อพัฒนาเพิ่มศักยภาพให้กำลังพลของกองทัพบกให้มีความรู้ความเชี่ยวชาญในการป้องกันระบบคอมพิวเตอร์ของหน่วยงานทางด้านความมั่นคง ปกป้องภาพลักษณ์ของผู้นำกองทัพ หรือผู้นำประเทศและสถาบันหลักของชาติ เพื่อเพิ่มความเชื่อมั่นต่อระบบการสื่อสารและสารสนเทศที่ปลอดภัย การทำงานของศูนย์ไซเบอร์กองทัพบกก็ทำตามนโยบายของรัฐบาลและกองทัพ ปัจจุบันรัฐบาลมีเป้าหมายเพื่อพัฒนาประเทศเข้าสู่ระบบเศรษฐกิจดิจิทัล ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นผู้นำในการขับเคลื่อนงานของรัฐบาลให้บรรลุเป้าหมาย รวมทั้งได้ปรับปรุงและพัฒนาวิธีการทำงานเพื่อให้สอดคล้องกับโลกปัจจุบัน ถ้าหากหน่วยงานของรัฐไม่ได้เตรียมความพร้อมเรื่องการรักษาความปลอดภัยทางไซเบอร์ไว้ ความเสียหายซึ่งเกิดจากภัยคุกคามทางไซเบอร์จะส่งผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์ ดังนั้น ผู้เชี่ยวชาญได้กล่าวว่าผู้ใช้งานเทคโนโลยีควรจะมีการบริหารจัดการที่ดี ซึ่งเทคโนโลยีสารสนเทศและการสื่อสารจะมีอิทธิพลต่อการทำธุรกิจสมัยใหม่ ซึ่งเป็นการทำธุรกิจไร้พรมแดนภายใต้เทคโนโลยีดิจิทัลที่ทันสมัยก็ยังมีอันตรายที่แอบแฝงอยู่ถือเป็นอาชญากรรมทางคอมพิวเตอร์ ซึ่งทำให้การก่ออาชญากรรมต่าง ๆ เช่น การโจมตีเว็บไซต์ของหน่วยงานต่าง ๆ มีต้นทุนที่ต่ำลง แต่สามารถสร้างความเสียหายอย่างมหาศาลและกว้างขวาง ศูนย์ไซเบอร์กองทัพบกจะเน้นไปในด้านความมั่นคงทางด้านไซเบอร์ ความมั่นคงทางด้านทหาร ความมั่นคงของชาติเป็นภารกิจที่สำคัญ และได้ทำงานประสานกับหน่วยงานรัฐอื่น ๆ อีก เช่น หน่วยงานไทยเซิร์ตซึ่งเป็นหน่วยงานสำคัญของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เป็นองค์การมหาชน สังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีหน้าที่สำคัญในการรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์ต่าง ๆ เพื่อให้การทำธุรกรรมทางออนไลน์มีความมั่นคงปลอดภัย ซึ่งปัจจุบันนี้ภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มมากขึ้นในประเทศไทยและมีความซับซ้อน สังคมไทยจึงต้องตื่นตัวเฝ้าระวังและหาทางรับมือกับภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้น

บทสรุปและข้อเสนอแนะของผู้ศึกษา

การปฏิบัติงานในองค์กรหรือการติดต่อสื่อสารในชีวิตปัจจุบันของประชาชนทั่วไปมีการติดต่อสื่อสารระหว่างบุคคลได้รวดเร็ว ทันสมัย ทั้งระบบภาพและเสียงผ่านอุปกรณ์คอมพิวเตอร์ สมาร์ทโฟน โทรศัพท์ โดยผ่านช่องทางสังคมออนไลน์โดยการใช้เครือข่ายคอมพิวเตอร์หรือการทำงานบนระบบอินเทอร์เน็ตเข้ามาเกี่ยวข้องกับชีวิตประจำวันมากขึ้น การติดต่อสื่อสารเพื่อการทำงานหรือการสื่อสารระหว่างบุคคล

ในแบบปกติทั่วไปไม่ได้สร้างปัญหาแต่อย่างใด แต่ที่สร้างปัญหาหรือภัยคุกคามต่างๆ เพราะยังมีบุคคลหรือกลุ่มบุคคลที่ต้องการสร้างความเสียหายหรือการพยายามแฮกเว็บไซต์เพื่อสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบอินเทอร์เน็ต ซึ่งการกระทำดังกล่าวก่อให้เกิดความเสียหายและมีผลกระทบต่อสังคมอย่างกว้างขว้างและเป็นภัยคุกคามทางไซเบอร์ที่ร้ายแรงในด้านการทหาร ความมั่นคง เศรษฐกิจ และความสงบสุขของประชาชน การคุกคามทางด้านไซเบอร์ที่กระทบในสังคมจะมีการเข้าไปทำลายระบบการให้บริการทางการเงินของระบบธนาคารหรือการให้บริการสาธารณูปโภค คือ โจมตีระบบการให้บริการประปา ระบบไฟฟ้า ศูนย์ไซเบอร์กองทัพบกต้องมีการมอนิเตอร์ เฝ้าระวัง ข้อมูลข่าวสาร เนื้อหาต่าง ๆ ที่มีความเกี่ยวข้อง และสร้างผลกระทบต่อภาพลักษณ์ของสถาบันหลักของชาติ รวมทั้งภาพลักษณ์ของประเทศไทย เพื่อสร้างความเชื่อมั่นให้แก่ประเทศ ภัยคุกคามทางไซเบอร์ที่สามารถป้องกันและตอบโต้ได้ภายใต้กฎหมายก็จะมีการตอบโต้ โดยการชี้แจงและสร้างความเข้าใจในเนื้อหาของข่าวสารที่ถูกต้องให้แก่ประชาชนในประเทศ และถ้ามีผลกระทบที่รุนแรงก็ต้องประสานกับหน่วยงานของรัฐหรือภาคเอกชนเพื่อแก้ไขข่าวสารที่สร้างความเสียหาย การดำเนินการตามกฎหมายนั้นมีสำนักงานตำรวจแห่งชาติทำการบังคับใช้ให้เป็นไปตามกฎหมายหรือติดตามข่าวกรองทางด้านไซเบอร์ ส่วนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งได้พัฒนาศักยภาพเพื่อให้สามารถรองรับกับระบบเศรษฐกิจยุคใหม่มากขึ้น ดังนั้น ความมั่นคงปลอดภัยทางด้านไซเบอร์ก็ต้องเพิ่มศักยภาพและป้องกันให้มีความปลอดภัยมากขึ้นเพื่อให้เกิดความเชื่อมั่น ซึ่งประเทศไทยนั้นมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย และยังมีไทยเซิร์ตซึ่งอยู่ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ซึ่งเป็นองค์การมหาชนเป็นหน่วยงานที่มีศักยภาพในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่มีผลต่อเศรษฐกิจและสังคมไทยได้ เพราะไทยเซิร์ตได้พัฒนาบุคลากร องค์ความรู้ และการใช้เทคโนโลยีและเทคนิคต่าง ๆ ในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ เพื่อต้องการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัลที่มั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ

บรรณานุกรม

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2559). **รายงานประจำปีไทยเซิร์ต 2558.** กรุงเทพฯ: ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งประเทศไทย.

ความมั่นคงและความปลอดภัยของข้อมูล. (2555). สืบค้น 15 มีนาคม 2560 จาก www.chanthaburi.buu.ac.th/-phaitoon/courses/2555/icm/firewall_and_IDS.ppt

ความหมายของ ISP. (2554). สืบค้น 16 มีนาคม 2560 จาก http://supaporn711.blogspot.com /2011/09/isp.html

เฉลิมชัย สิทธิสาท. ผู้บัญชาการทหารบก, ณ ศูนย์ไซเบอร์ ทบ. (1 พฤศจิกายน 2559). **สัมภาษณ์.**

ชรัติ อุ่มสัมฤทธิ์. (2556). ข้ออภิปรายพลังอำนาจแห่งชาติและพลังอำนาจรูปแบบใหม่. **นิตยสารยุทธโกษ,** 121 (3), 32-38.

ไทยเสี่ยงภัยไซเบอร์ด้วยการใช้เทคโนโลยี. (2559). **นิตยสาร digital Age,** 18 (211), 38-40.

ภัยจากการทำลายหรือก่อกวนระบบคอมพิวเตอร์. (2555). สืบค้น 7 กุมภาพันธ์ 2560 จาก http://foh9.blogspot.com/2012/04/blog-post_06.html

ภัยคุกคามในระบบสารสนเทศ. (2557). สืบค้น 3 กุมภาพันธ์ 2560 จาก www.rtna.ac.th/download /cyber / Threat-information -system1.pdf

ริชาร์ด เอ.คลาร์ก., โรเบิร์ต คเนค (6 เมษายน 2555). **สงครามไซเบอร์** (ไพรัตน์ พงศ์พานิชย์, ผู้แปล). กรุงเทพฯ: มติชน.

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม. **วารสารสถาบันวิชาการป้องกันประเทศ,** 6(3), 19-29.

ศูนย์ไซเบอร์กองทัพบก. (2559). สืบค้น 2 กุมภาพันธ์ 2560 จาก http://cyber.rta.mi.th//about.php

ฤทธี อินทราวุธ. **กองทัพบกกับความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ.** (2556). สืบค้น 1 กุมภาพันธ์ 2560 จาก http://www.ilc2012.org/moodle/file.php/52/cyber.pdf

_____. **“หน่วยรบไซเบอร์” เมื่อเทคโนโลยีทรงพลังกว่าการถือปืน.** (2558). สืบค้น 17 กุมภาพันธ์ 2560 จาก http://www.posttoday.com/analysis/report/389038

_____. **“หน่วยรบไซเบอร์” อำนาจกำลังรบไร้ตัวตน.** (2558). สืบค้น 9 กุมภาพันธ์ 2560 จาก http://rittee1834.blogspot.com/2015/09/blog-post.html