การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม

Standards Development; Cyber Security of the Ministry of Defence

บทความวิชาการ

นางสาวศิวลีย์ สิริโรจน์บริรักษ์

ผู้ช่วยนักวิจัย ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

การศึกษาเรื่อง "การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม" มีวัตถุประสงค์เพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล และเพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานระดับสากล โดยการศึกษาครั้งนี้ใช้วิธีการสัมภาษณ์กลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) และการค้นคว้าข้อมูลจากเอกสารทางวิชาการต่าง ๆ ที่มีเนื้อหาเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. และมาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

ผลการศึกษา พบว่า ๑) กรอบนโยบาย ยุทธศาสตร์ และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ได้แก่ พ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของ กห. พ.ศ. ๒๕๕๑, นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กห. พ.ศ. ๒๕๕๔, ยุทธศาสตร์ กห. อิเล็กทรอนิกส์ (e-Defence), แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของ กห. ฉบับที่ ๓ พ.ศ. ๒๕๕๗ – ๒๕๖๑, การจัดตั้งศูนย์บัญชาการไซเบอร์ กห. ๒) มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 – 14, มาตรฐาน COBIT, และมาตรฐาน IT BPM ๓) แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานในระดับสากล **เชิงนโยบาย** ได้แก่ **ส่วนบังคับการ** ต้องเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร เพื่อดำเนินการตอบสนองต่อ

ปัญหา/เหตุการณ์บุกรุกระบบของหน่วยขึ้นตรงได้อย่างรวดเร็ว **ส่วนนโยบายและแผน** ต้องมีการบรรจุข้อกำหนดในกระบวนการจัดซื้อจัดจ้าง อุปกรณ์ฮาร์ดแวร์/ซอฟต์แวร์ เพื่อให้อุปกรณ์มีความปลอดภัยในระดับสากล **ส่วนปฏิบัติการไซเบอร์** จะต้องมีหน่วยปฏิบัติการเชิงรับสงครามข้อมูลข่าวสาร และหน่วยปฏิบัติการเชิงรุก สงครามข้อมูลข่าวสาร **ส่วนวิจัยและพัฒนาไซเบอร์** จะต้องจัดตั้งส่วนงาน Information Warfare System Research เพื่อพัฒนาระบบการรักษาความปลอดภัยของข้อมูลข่าวสารให้มีประสิทธิภาพมากยิ่งขึ้น และต้องบรรจุอัตราจเรทหารที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อดำเนินการตรวจสอบตามหลักการ ICT Audit **เชิงปฏิบัติ** ได้แก่ ๑) ควรจัดทำหลักสูตร Cyber Training เพื่ออบรมความรู้เกี่ยวกับการใช้งานซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งการให้ทุนการศึกษาต่อในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับ ๒) ควรมีการจัดการองค์ความรู้ด้านไซเบอร์ (Cyber Knowledge Management: KM) ในหน่วยงาน และควรนำ E-Document มาใช้ในการปฏิบัติราชการมากยิ่งขึ้น

คำสำคัญ: การรักษาความมั่นคงปลอดภัยไซเบอร์, มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Abstract

This work, “Standards Development; cyber security of the Ministry of Defence”, is to study the Ministry of Defence (MOD)’s cyber security policy, to study the international standards involved, and, to propose ways to enhance the MOD’s Standards to meet those international standards. The work conducted interviews with experts and key informants, also, studied academic research and important documents involved; especially, those documents involving with the MOD’s cyber security, also, the documents and standards with well recognized international levels within the matters.

This work studied the MOD’s documents involved; including the Acts of the year 2008, namely, “the MOD’s directives for Internet communications and technology”, the MOD’s policies and guidelines of the year 2011, the MOD’s e-Defence strategy for the year 2014-2018, and, the MOD’s cyber command establishments. This work also analyzed the international standards involved; including, the U.S. DoD’s security policy, ISO 27001: 2005, FIPS PUB 200, NIST 800-14, COBIT, IT BPM.

The results for ways to improve or enhance the MOD’s cyber security are, for the commanding structure to set up new ofcial positions for “the information warfare ofcers”, to enable effectiveness and fast operations, also, capabilities in effective/fast defensive or offensive operations involved, for policy and planning structure to set up regulations to ensure information security requirements since the beginning of procurements and acquisitions of any hardware or software involved, for the cyber security operational structure to set up new operational units for both offence and defence, and, for the cyber security research and development to set up new “Information Warfare System research” to develop or maintain secure information system to be most effective. Also, there should have expert inspectors who have sufcient expertise, knowledge, and skills to perform security audits upto information standards, or, military standards, to ensure secure deployment, usage, and maintenance of secure information system for the MOD, at all time.

In additions, there should be Cyber Security training courses for people involved at all levels, scholarship for higher education regarding Cyber Security, also, setting up Cyber Security knowledge management (KM) within each unit involved, and, implementing secure E- Document system in practices.

Keywords: Cyber Security, Operating Standards for Cyber Security.

๑. บทนำ

ภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ (Cyber Threat) เป็นประเด็นปัญหาที่ทำให้ประเทศต่าง ๆ ทั่วโลกเกิดการตื่นตัวและตระหนักถึงปัญหา ดังจะเห็นได้จากปรากฏการณ์ที่ก่อให้เกิดความเปลี่ยนแปลงในโลกอาหรับหรือที่รู้จักโดยทั่วไปว่าปรากฏการณ์ “Arab Spring” หรือแม้แต่กลุ่มก่อการร้าย ISIS ซึ่งใช้เครือข่ายสังคมออนไลน์ เช่น Twitter, Facebook ฯลฯ เป็นเครื่องมือสำคัญในการปลุกระดมมวลชน เป็นต้น จากรายงานของ World Economic Forum แสดงให้เห็นว่า ทั่วโลกกำลังวิตกกังวลกับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์เป็นอย่างมาก โดยภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ถูกจัดให้อยู่ในอันดับที่ ๔ ใน ๑๐ Trends ของโลก ประกอบกับผลการศึกษาของสถาบัน The Business Continuity Institute (BCI) ซึ่งเป็นสถาบันอันดับหนึ่งของโลกด้านการบริหารความต่อเนื่องทางธุรกิจ ยังแสดงให้เห็นว่า Cyber Attack เป็นประเด็นอันดับต้น ๆ ที่องค์กรให้ความสนใจมากที่สุด

ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA ๓ ประการ ได้แก่ การรักษาความลับของข้อมูล (Condentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

จึงกล่าวได้ว่าความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการเหล่านั้นได้ถูกกำหนดเอาไว้เป็นมาตรฐานที่เป็นที่ยอมรับ โดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ซึ่งองค์กรสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของตน และอาจเพิ่มเติมหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ

จากเหตุผลข้างต้น จึงนำมาสู่การศึกษาเรื่อง “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม” โดยมีวัตถุประสงค์เพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล เพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมให้ได้มาตรฐานระดับสากล อันจะเป็นไปตามยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม พ.ศ. ๒๕๕๕ ที่ว่า “กระทรวงกลาโหมต้องมีขีดความสามารถในการรับมือกับสงครามไซเบอร์ รวมทั้งมีขีดความสามารถในการปฏิบัติการสารสนเทศ สงครามอิเล็กทรอนิกส์ และสงครามจิตวิทยา เพื่อป้องกันการทำลายระบบควบคุมบังคับบัญชา ระบบสารสนเทศ และระบบข่าวกรอง รวมทั้งสามารถโจมตีฝ่ายตรงข้ามได้”

๒. วัตถุประสงค์ในการศึกษา

๒.๑ เพื่อศึกษานโยบาย ยุทธศาสตร์ และการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม

๒.๒ เพื่อศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

๒.๓ เพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมให้ได้มาตรฐานระดับสากล

๓. วิธีการศึกษา

๓.๑ ข้อมูลปฐมภูมิ (Primary Data) ดำเนินการศึกษาและเก็บรวบรวมข้อมูลภาคสนาม โดยใช้วิธีการสัมภาษณ์กับกลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) ได้แก่ กลุ่มแรก ผู้กำหนดนโยบาย หรือผู้บริหารระดับสูงที่มีบทบาทสำคัญในการกำหนดนโยบาย โดยอาศัยวิธีการสัมภาษณ์ข้อมูลเชิงลึก (In-depth Interview) กับหน่วยงานภายในกระทรวงกลาโหม กลุ่มที่สอง หน่วยปฏิบัติหรือบุคลากรที่มีหน้าที่ในการรับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปปฏิบัติ

๓.๒ ข้อมูลทุติยภูมิ (Secondary Data) เป็นการค้นคว้าข้อมูลจากเอกสารทางวิชาการต่าง ๆ ที่มีเนื้อหาเกี่ยวข้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม และมาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล เพื่อนำข้อมูลที่ได้มาสังเคราะห์เป็นต้นแบบหรือมาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมต่อไป

๔. ผลการศึกษา

๔.๑ กรอบนโยบาย ยุทธศาสตร์ และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์กระทรวงกลาโหม มีดังนี้

- **พ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม พ.ศ. ๒๕๕๑** กำหนดให้กระทรวงกลาโหมวางแผนพัฒนาและดำเนินการเกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการบริหารราชการทั่วไปของกระทรวงกลาโหม ให้สามารถติดต่อเชื่อมโยง แลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่าง ๆ ทั้งในประเทศและระหว่างประเทศ

- **นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ. ๒๕๕๔** กระทรวงกลาโหมได้กำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานต่อระบบสารสนเทศ ทรัพย์สินสารสนเทศ และข้อมูลสำคัญในการปฏิบัติภารกิจ โดยนโยบายนี้อาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ซึ่งอิงมาตรฐาน ISO 27001: 2005 เพื่อยึดเป็นแนวทางปฏิบัติในการลดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ

- **ยุทธศาสตร์กระทรวงกลาโหมอิเล็กทรอนิกส์ (e-Defence)** มียุทธศาสตร์ ๕ ด้าน ได้แก่ ๑) ด้านฝ่ายอำนวยการ ๒) ด้านการยุทธ์ ๓) ด้านการสนับสนุน ๔) ด้านการกำลังพล และ ๕) ด้านกิจการพิเศษ

- **แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม ฉบับที่ ๓ พ.ศ. ๒๕๕๗ – ๒๕๖๑** เพื่อมุ่งสู่หน่วยงานชั้นนำด้านความมั่นคงของรัฐและอาเซียน โดยกำหนดยุทธศาสตร์การพัฒนา ได้แก่ ๑) การพัฒนากำลังพลทุกระดับให้มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศและการสื่อสาร ๒) การพัฒนาการจัดหน่วย ระเบียบปฏิบัติ กฎ ข้อบังคับ คำสั่ง และมาตรฐานให้สอดคล้องและรองรับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ ๓) การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่พอเพียงและคุ้มค่า ๔) การพัฒนาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างชาญฉลาด และ ๕) การพัฒนาขีดความสามารถการปฏิบัติการไซเบอร์ และการรักษาความปลอดภัยสารสนเทศให้มีประสิทธิภาพ มุ่งสู่หน่วยงานด้านความมั่นคงหลักด้านไซเบอร์

▪ **ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม (Cyber Operations Center) และหน่วยปฏิบัติการไซเบอร์ของกองบัญชาการกองทัพไทย และเหล่าทัพ** โดยกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ เตรียมจัดตั้งหน่วยงานด้านไซเบอร์โดยตรง (Cyber Command) ขึ้นเพื่อรองรับการปฏิบัติงานความมั่นคงปลอดภัยของประเทศ จากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติ โดยศูนย์บัญชาการไซเบอร์ดังกล่าว จะมีหน้าที่ประสานงานกับหน่วยงานทั้งในประเทศและต่างประเทศในการรวมพลังของการปฏิบัติการไซเบอร์ การติดตามสถานการณ์ไซเบอร์ของประเทศ การพัฒนาบุคลากรในภาพรวมของกระทรวงกลาโหม การพัฒนาเทคโนโลยี กระบวนการทำงานและหลักนิยม การวิจัยพัฒนาด้านไซเบอร์ รวมถึงการป้องกันเครือข่ายกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

▪ **นโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ** ได้มีการจัดตั้ง “คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee: NCSC)” ซึ่งทำหน้าที่ในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามไซเบอร์ โดยหน่วยงานหลักในการขับเคลื่อน ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (ETDA), ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กระทรวงกลาโหม และสำนักงานตำรวจแห่งชาติ

๔.๒ มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

ตารางผลการสังเคราะห์เนื้อหาด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล

แนวทางปฏิบัติ		มาตรฐานสากล					
		U.S. DoD Standard	ISO 27001: 2005	FIPS PUB 200	NIST 800 – 14	COBIT	IT BPM
๑.	การกำหนดแผนกลยุทธ์ พันธกิจ นโยบาย และเป้าหมายการดำเนินงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ	✓	✓	✓		✓	
๒.	การกำหนดโครงสร้าง การบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และความสัมพันธ์กับหน่วยงานภายนอก	✓	✓		✓	✓	
๓.	การบริหาร และพัฒนาทรัพยากรบุคคลด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ	✓	✓	✓		✓	
๔.	การป้องกัน และการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อมจากภายในและภายนอกองค์กร	✓	✓	✓	✓		

๕.	การระบุ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ	✓	✓	✓		✓	
๖.	การวางแผน วิเคราะห์การลงทุน และการจัดการสินทรัพย์ทางเทคโนโลยีสารสนเทศ	✓	✓	✓	✓	✓	✓
๗.	การจัดหา พัฒนา และการบำรุงรักษาระบบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ	✓	✓	✓	✓	✓	✓
๘.	การบริหารความต่อเนื่อง การจัดการปัญหาและการเปลี่ยนแปลงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ	✓	✓		✓	✓	
๙.	การปฏิบัติตามข้อกำหนด ระเบียบ พระราชบัญญัติ กฎหมาย และบทลงโทษด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ	✓	✓		✓	✓	
๑๐.	การติดตามประเมิน และรับรองกระบวนการทำงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ	✓	✓		✓	✓	✓
๑๑.	มีการกำหนดมาตรฐานในกระบวนการประมูลจัดซื้อ หรือจัดจ้างสำหรับหน่วยงานภาครัฐ	✓					
๑๒.	กำหนดแนวทางในการออกแบบ พัฒนา ผลิต หรือทดสอบสำหรับผู้ผลิตเทคโนโลยีให้หน่วยงานภาครัฐ เพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้	✓					

๔. บทวิเคราะห์

จากการสังเคราะห์เนื้อหาดังกล่าว พบว่า แต่ละมาตรฐานมีแนวทางในการปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ที่แตกต่างกันออกไปโดย **มาตรฐาน U.S. DoD** เป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของระบบคอมพิวเตอร์เพื่อความมีประสิทธิภาพของอุปกรณ์ตั้งแต่ขั้นตอนแรก คือ กระบวนการประมูลจัดซื้อหรือจัดจ้างสำหรับหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางในการออกแบบ พัฒนา ผลิต หรือทดสอบสำหรับผู้ผลิตเทคโนโลยี หรือภาคเอกชนได้ปฏิบัติตาม เพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้

มาตรฐาน ISO 27001: 2005 เป็นมาตรฐานที่มีแนวทางปฏิบัติที่ได้รับการยอมรับ และนำไปใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรทั่วโลก ทั้งนี้จากรายงานของ ISMS (Information Security Management System) พบว่า มีองค์กรมากกว่า ๗,๓๔๖ แห่ง นำมาตรฐานนี้ไปใช้ และในประเทศไทยมีองค์กรที่ผ่านการรับรองจากมาตรฐานนี้แล้ว ๔๑ แห่ง ในขณะที่ **มาตรฐาน COBIT** เป็นมาตรฐานที่มีจำนวนแนวทางปฏิบัติที่ใกล้เคียงกับ ISO 27001: 2005 ยกเว้นแนวทางการป้องกันและการ

สร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อมจากภายในและภายนอกองค์กร และมาตรฐานที่มีแนวทางปฏิบัติน้อยที่สุด ได้แก่ **มาตรฐาน IT BPM** เนื่องจากมาตรฐานนี้เป็นการกำหนดมาตรฐานขั้นต่ำที่องค์กรควรจะปฏิบัติ โดยเฉพาะระบบสารสนเทศที่มีใช้ในองค์กร เช่น ระบบสารสนเทศบุคลากร ระบบการสื่อสารด้วยจดหมายอิเล็กทรอนิกส์ เป็นต้น

สำหรับประเทศไทย กรอบนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถูกกำหนดโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยได้กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศไว้ใน "พ.ร.ฎ. ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓" รวมทั้ง "แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ ๒๕๕๓" โดยอ้างอิงตามมาตรฐาน ISO 27001: 2005 และ **สำหรับกระทรวงกลาโหม** ได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติ โดยได้กำหนดไว้ใน "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.๒๕๕๔" อย่างไรก็ตาม จากการทบทวนวรรณกรรม พบว่า มาตรฐาน ISO 27001: 2005 หรือมาตรฐาน NIST 800 มีหลักการที่ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ โดยเฉพาะการปกป้องข้อมูลและทรัพย์สินจากภัยคุกคามทางไซเบอร์ที่มาในรูปแบบต่าง ๆ เช่น ความเสี่ยงจากการใช้งานอินเทอร์เน็ต ภัยจากการทำธุรกรรมทางธนาคารหรือการซื้อขายออนไลน์ การโจรกรรมพาสเวิร์ด การจู่โจมด้วยการส่งโปรแกรมดักจับข้อมูลทางคอมพิวเตอร์ เป็นต้น ซึ่งมาตรฐานเหล่านี้จึงอาจมีความเหมาะสมในสภาวะแวดล้อมทางธุรกิจมากกว่า

แต่สำหรับหน่วยงานด้านความมั่นคง ที่ภารกิจต่าง ๆ ล้วนเกี่ยวข้องและมีความสำคัญอย่างมากต่ออธิปไตยของชาติ จึงจำเป็นจะต้องมีระบบป้องกันความปลอดภัยไซเบอร์ที่เฉพาะเจาะจง และควรให้ความสำคัญตั้งแต่ขั้นตอนแรก ได้แก่ ความปลอดภัยของอุปกรณ์และเครื่องมือที่ใช้งานด้านไซเบอร์ ซึ่งจากการทบทวนวรรณกรรม พบว่า กระทรวงกลาโหมสหรัฐฯ ได้มีการกำหนดมาตรฐานในกระบวนการประเมินอุปกรณ์และเครื่องมือที่ใช้งานด้านความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ โดยมาตรฐานดังกล่าวจะมีมาตรวัดความปลอดภัยของอุปกรณ์หรือเครื่องมือที่ใช้เพื่อประมวลผลข้อมูลที่มีระดับชั้นความลับต่าง ๆ ได้อย่างถูกต้องเที่ยงตรง จึงกล่าวได้ว่า มาตรฐาน U.S. DoD อาจจะเหมาะสมกับภารกิจด้านความมั่นคงและเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้มากกว่ามาตรฐาน ISO 27001: 2005 ซึ่งเป็นมาตรฐานทางธุรกิจ จึงนำเสนอข้อมูลเพื่อรับการพิจารณาอีกทางเลือกหนึ่ง ซึ่งสอดคล้องกับบทสัมภาษณ์ที่ว่า...

"กห. ควรจะกำหนดมาตรฐานการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมสำหรับ กห. เอง เพราะภารกิจด้านความมั่นคง เป็นสิ่งที่เฉพาะเจาะจง แม้กระทรวง ICT จะกำหนดมาตรฐาน ISO 27001: 2005 มาให้เราใช้ มาเป็นแนวทางให้เราปฏิบัติ แต่การจะปรับใช้มาตรฐานที่ทำมาให้เหมาะสมกับทางธุรกิจ การเงิน และการธนาคารก็ดูจะไม่เอื้อต่อภารกิจด้านการทหารเท่าไรนัก"

"การปรับใช้มาตรฐาน ISO 27001: 2005 ให้เข้ากับวัฒนธรรมองค์กรก็พอจะทำได้ แต่ถ้าจะใช้วัฒนธรรมของหน่วยงานทหารด้วยกัน ก็จะดำเนินการปรับใช้ได้ง่ายกว่า"

"U.S. DoD Standard ดีตรงที่ถือว่าการใช้ข้อมูลทั้งหมดก็เพื่อหลวงเท่านั้น ทรัพย์สินทุกอย่างถือว่าเป็นของหลวงหมด ก่อนจะปฏิบัติงานเราต้องมาทำสัญญา มาเขียนสัญญากันก่อนว่า การกระทำหรือการใช้คอมพิวเตอร์ทุกอย่าง หลวงสามารถควบคุมได้ เช่น การห้ามเล่น Facebook หรือ YouTube ในที่ทำงาน ซึ่งเหมือนเป็นการสร้างจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงาน แต่ตอนนี้เรายังทำไม่ได้ และมาตรฐาน ISO 27001: 2005

ไม่ได้ระบุโทษไว้"

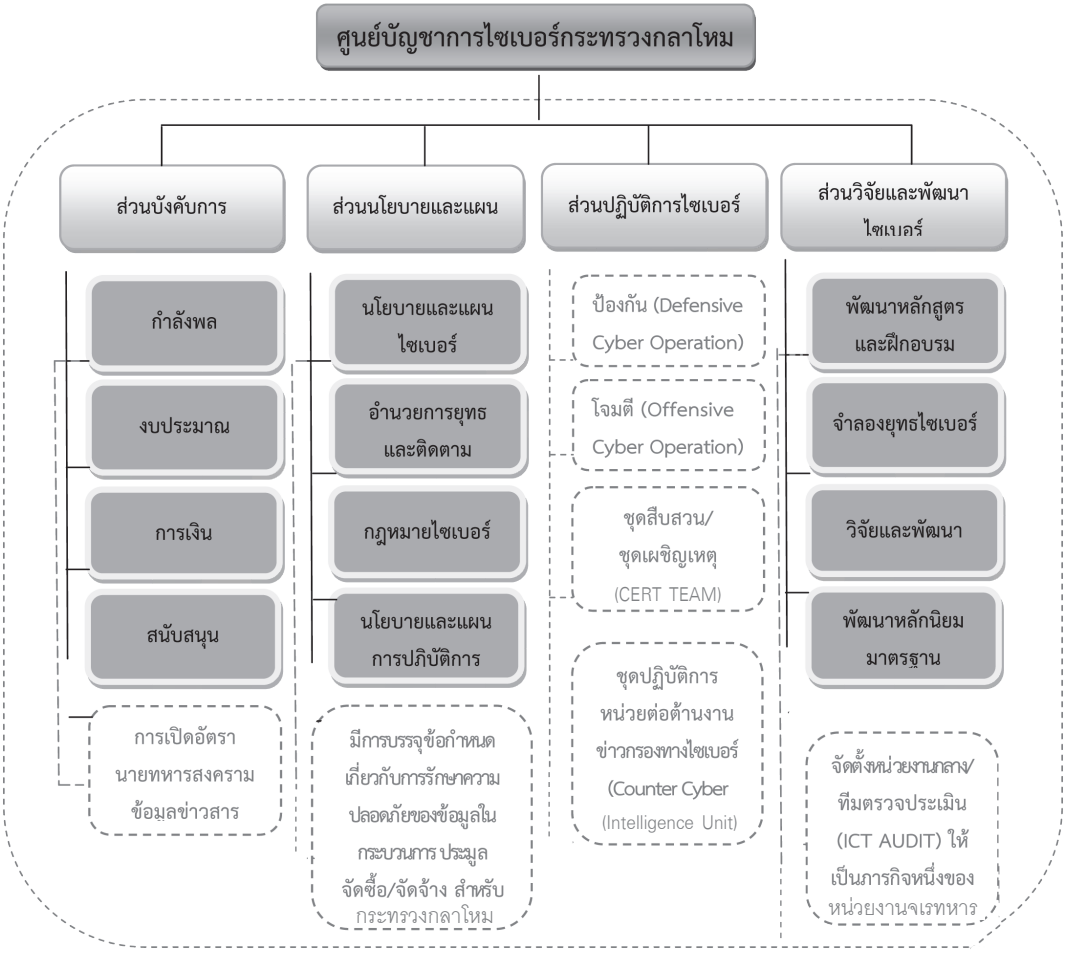
"U.S. DoD Standard มีการกำกับคุณภาพของคน โดยมีใบรับรอง IT Certificate ทางด้าน Cyber Security ซึ่งจะเป็นการดีหากได้คนที่เหมาะสมเข้ามาทำงานด้านนี้"

"U.S. DoD Standard ให้ความสำคัญกับหลักการประกันความมั่นคงปลอดภัยสารสนเทศ (Informational Assurance: IA) โดยมีมาตรฐานในการประเมิน และมี IT Audit team ในการกำกับควบคุมทำให้การนำนโยบายด้านไซเบอร์มาสู่การปฏิบัติได้มีประสิทธิภาพมากยิ่งขึ้น"

อย่างไรก็ตาม มาตรฐาน ISO 27001: 2005 ถือเป็นมาตรฐานที่กระทรวงกลาโหมไทยรับจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติ จึงกล่าวได้ว่ามาตรฐานดังกล่าวเป็นมาตรฐานกลางที่เหล่าทัพต่าง ๆ ยึดถือปฏิบัติร่วมกัน

๔.๓ แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมให้ได้มาตรฐานในระดับสากล

จากการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงได้นำเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเสนอแนะปรับปรุงโครงสร้างการจัดตั้งศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม สามารถอธิบายได้ ดังนี้



ส่วนบังคับการ ต้องบรรจุอัตรานายทหารสงครามข้อมูลข่าวสารเข้าไปในโครงสร้างองค์กร ซึ่งตำแหน่งนี้จะต่างจากนายทหารรักษาความปลอดภัยคอมพิวเตอร์ กล่าวคือ นายทหารสงครามข้อมูลข่าวสารจะต้องมีคุณสมบัติในการทำงานในเชิงรุกมากกว่านายทหารรักษาความปลอดภัยคอมพิวเตอร์ และจะต้องเป็นทีม "MOD CERT" ในการดำเนินการตอบสนองต่อปัญหา/เหตุการณ์บุกรุกระบบของหน่วยขึ้นตรงกระทรวงกลาโหมได้อย่างรวดเร็ว ต้องมีความสามารถในการล้วงความลับข้อมูล/ โจมตีฝ่ายตรงข้าม มีความสามารถในการปกป้องตนเองจากการถูกล้วงข้อมูล และการเสาะหาข้อมูลต่าง ๆ ในโลกออนไลน์ตามที่ได้รับมอบหมายจากกองทัพ ตลอดจนเป็นที่ปรึกษาเพื่อแก้ไขปัญหาด้านการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศให้แก่ผู้บริหารระดับสูงของหน่วยงานได้

ส่วนนโยบายและแผน ต้องมีการบรรจุข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล หรือมีการออกระเบียบ กห. มาบังคับใช้ในกระบวนการจัดซื้อจัดจ้างเพื่อบ่งบอกถึงระดับความปลอดภัย และจะต้องจัดทำข้อระบุดังกล่าวให้เป็นไปตามมาตรฐานสากล

ส่วนปฏิบัติการไซเบอร์ จะต้องมีดำเนินงานลักษณะเชิงรับ (Defensive) และ เชิงรุก (Offensive) ดังนี้

• หน่วยปฏิบัติการเชิงรับสงครามข้อมูลข่าวสาร (Defensive Cyber Operation) มีหน้าที่ในการปกป้องเฝ้าระวังป้องกันระบบฐานข้อมูล มีการดูแลระบบคอมพิวเตอร์และระบบเครือข่าย การปฏิบัติการเพื่อตรวจจับ การวิเคราะห์การต่อต้าน และการลดภัยคุกคามและจุดอ่อน เพื่อให้ได้เปรียบศัตรูที่กำลังจะรุกราน และขณะเดียวกันก็ปกป้องความสามารถในการปฏิบัติการอย่างเสรีในโลกไซเบอร์

• หน่วยปฏิบัติการเชิงรุกสงครามข้อมูลข่าวสาร (Offensive Cyber Operation) ควรมีขีดความสามารถในการโจมตีทางไซเบอร์มีความสามารถในการรบกวนการใช้งานระบบสารสนเทศของฝ่ายตรงข้าม หรือการเจาะระบบ การล้วงความลับผ่านเครือข่าย หรือมีขีดความสามารถในการเจาะระบบของฝ่ายตรงข้ามได้ อนึ่ง การดำเนินการเชิงรุกดังกล่าวนี้ ปัจจุบันยังไม่มีกฎหมายรองรับ และการตีความในกฎหมายระดับนานาชาติยังไม่ชัดเจน ดังนั้นกระทรวงกลาโหมจึงควรจะศึกษาในประเด็นดังกล่าวให้ชัดเจนมากยิ่งขึ้น

• กระทรวงกลาโหมจะต้องเพิ่มบทบาท "Ministry of Defence Computer Emergency Response Team (MOD CERT)" โดยเพิ่มขอบเขตของการปฏิบัติงานให้กว้างขวางและเพียงพอเพื่อประสานข้อมูลอย่างเป็นรูปธรรมอย่างแท้จริง กล่าวคือ ในส่วนของ **การปฏิบัติการ** กระทรวงกลาโหมจะต้องพัฒนาให้ MOD CERT ทำหน้าที่หลักในการตอบสนองและจัดการกับเหตุการณ์ความปลอดภัยคอมพิวเตอร์อย่างมีประสิทธิภาพ ในส่วนของ **การวิจัยและพัฒนา** MOD CERT จะมีหน้าที่ทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความปลอดภัยในการใช้คอมพิวเตอร์และเครือข่าย ตลอดจนจัดทำฐานข้อมูลในการแก้ไขไวรัส เพื่อให้เป็นประโยชน์แก่หน่วยขึ้นตรงและหน่วยงานอื่น ๆ ไว้เป็นฐานข้อมูลในการป้องกันภัยทางไซเบอร์

ส่วนวิจัยและพัฒนาไซเบอร์ : จะต้องจัดตั้งส่วนงาน Information Warfare System Research เพื่อพัฒนาระบบการรักษาความปลอดภัยของข้อมูลข่าวสาร ซึ่งส่วนงานนี้จะมีหน้าที่ในการฝึกอบรม วิจัยและพัฒนานายทหารสงครามข้อมูลข่าวสาร เพื่อให้มีความเชี่ยวชาญในการปฏิบัติภารกิจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งเชิงรับและเชิงรุก

อีกทั้ง กห. จะต้องเพิ่มอัตราหรือบรรจุใหม่ **หน่วยงานจเรทหาร** ที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะ เพื่อดำเนินการตรวจสอบตามหลักการ ICT Audit ที่มีคุณลักษณะเฉพาะ ได้แก่ ๑) การดำเนินการให้สอดคล้องตามข้อกำหนดทางกฎหมาย ๒) การดำเนินการให้สอดคล้องตามนโยบายความมั่นคงปลอดภัย มาตรฐาน และข้อกำหนดทางเทคนิค และ ๓) การดำเนินการตรวจประเมินระบบสารสนเทศ และจะต้องมีการกำหนด

แนวทางในการดำเนินการขององค์กรเพื่อให้สอดคล้องตามข้อกำหนดต่าง ๆ ซึ่งแนวทางการพัฒนาดังกล่าวจะทำให้กระทรวงกลาโหมมีมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีมาตรฐานในระดับสากลมากยิ่งขึ้น

๖. ข้อเสนอแนะ

<u>เชิงนโยบาย</u>

๑) กระทรวงกลาโหมควรเร่งดำเนินการปรับปรุงโครงสร้าง ภารกิจการจัดองค์กร และแนวทางการบรรจุอัตรากำลังพลในระดับเหล่าทัพ ได้แก่ การเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร และควรออกกฎระเบียบหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยที่เป็นมาตรฐานในกระบวนการประมูลจัดซื้อ/จัดจ้างที่มีความชัดเจน รวมทั้งควรกำหนดแนวทางในการออกแบบ พัฒนา ผลิต หรือทดสอบระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศสำหรับผู้ผลิตเทคโนโลยีให้กับกระทรวงกลาโหม เพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้

๒) กระทรวงกลาโหมควรจัดตั้งหน่วยงานกลาง/ทีมตรวจประเมิน (ICT AUDIT) ให้เป็นภารกิจหนึ่งของหน่วยงานจเรทหารในการตรวจประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศหน่วยงาน

<u>เชิงปฏิบัติ</u>

๑) กระทรวงกลาโหมควรให้ความสำคัญกับโครงการฝึกอบรม โดยการจัดทำหลักสูตร Cyber Training การอบรมความรู้เกี่ยวกับการใช้ซอฟท์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งการให้ทุนการศึกษาต่อในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมถึงบุคลากรทุกระดับ

๒) กระทรวงกลาโหมควรมีการจัดการองค์ความรู้ด้านไซเบอร์ (Cyber Knowledge Management: KM) ในหน่วยงาน เช่น สถานการณ์ด้านไซเบอร์ในปัจจุบัน วิธีการในการกำจัดไวรัสในตัวเครื่อง เป็นต้น เพื่อเป็นฐานข้อมูลให้หน่วยขึ้นตรงต่าง ๆ ได้นำข้อมูลไปใช้ และควรให้ความสำคัญกับการนำ E-Document มาใช้ในการปฏิบัติราชการ เช่น การรายงานต่าง ๆ การทำหนังสือเชิญประชุม หรือบันทึกการประชุม เป็นต้น

๗. บทสรุป

จากความแพร่หลายของการใช้อินเทอร์เน็ตในโลกปัจจุบัน และการเชื่อมต่อกันเป็นระบบเครือข่ายคอมพิวเตอร์ภายในและระหว่างองค์กรต่าง ๆ ก่อให้เกิดการติดต่อสื่อสารกันระหว่างผู้คนผ่านระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะอยู่ที่ใดในโลก การเชื่อมต่อนี้เปิดโอกาสให้ผู้ไม่ประสงค์ดีหรือ Hacker เข้ามาโจมตีระบบได้ เช่น การจารกรรมข้อมูล การทำให้ระบบเครือข่ายคอมพิวเตอร์ไม่สามารถใช้การได้ หรือการควบคุมและสั่งการไปยังเครื่องอื่น เป็นต้น

ทั้งนี้ “โลกเสมือน (Cyber Space)” เป็นพื้นที่ที่ไม่มีเขตแดนที่ชัดเจน มีลักษณะการเชื่อมต่อที่สมบูรณ์และเป็นสาธารณะ ซึ่งสามารถเชื่อมต่อได้ทุกสถานที่ ทุกเวลาและเปิดกว้างสำหรับผู้ใช้บริการทุกคน สิ่งเหล่านี้ก่อให้เกิดลักษณะการทำสงครามแบบ “อสมมาตร (Asymmetric Warfare)” คือ ผู้ก่อการร้ายไม่จำเป็นต้องมีกำลังคนมาก ยุทโธปกรณ์ครบครัน หรือเป็นองค์กรที่มีขนาดใหญ่อีกต่อไป แต่สามารถใช้กำลังคนเพียงคนเดียวกับความสามารถในการเข้าถึงระบบอินเทอร์เน็ตได้เท่านั้น ก็เพียงพอต่อการก่อการร้ายผ่านโลกไซเบอร์ได้

จากผลการศึกษา จะเห็นได้ว่ากระทรวงกลาโหมได้ตระหนักถึงความสำคัญของการป้องกันภัยทางไซเบอร์และการพัฒนาเทคโนโลยีสารสนเทศ เพื่อนำไปประยุกต์ใช้ในงานด้านต่าง ๆ ของกระทรวงกลาโหม ทั้งในงานด้านการบริหารจัดการทั่วไปจนถึงงานด้านการป้องกันประเทศ ซึ่งในการรับมือกับภัยคุกคามไซเบอร์ในขั้นแรกนั้น กระทรวงกลาโหมจะต้องพัฒนามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของตนเองเสียก่อน เพื่อเป็นกรอบหรือเป็นแนวทางการปฏิบัติให้หน่วยขึ้นตรงซึ่งประกอบด้วย หน่วยขึ้นตรงกระทรวงกลาโหม หน่วยขึ้นตรงสำนักงานปลัดกระทรวง

กลาโหม หน่วยขึ้นตรงกองบัญชาการกองทัพไทย เหล่าทัพ และองค์การรัฐวิสาหกิจในความควบคุมของกระทรวงกลาโหม ได้ปฏิบัติตาม เพื่อลดช่องโหว่และข้อผิดพลาดของงานด้านความมั่นคงปลอดภัยไซเบอร์ และเพื่อรับมือกับภัยคุกคามด้านนี้ที่อาจจะเกิดขึ้นในอนาคต

บรรณานุกรม

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (๒๕๕๒). *แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ ๒) พ.ศ. ๒๕๕๒-๒๕๕๖*. กรุงเทพฯ: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. แนวทางการพัฒนากองทัพไทย ในอนาคตต่อการรองรับภัยคุกคามรูปแบบใหม่. *การประชุมเชิงสัมมนาทางวิชาการศูนย์อาเซียนศึกษาฯ* ครั้งที่ ๔/๒๕๕๗. กรุงเทพฯ: ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ.

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. “Cyber Security: ภัยคุกคามความมั่นคงรูปแบบใหม่. *การสัมมนาปัญหายุทธศาสตร์* ครั้งที่ ๖/๒๕๕๖. กรุงเทพฯ: ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ.

ธวัชชัย ชมศิริ. (๒๕๕๓). ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์. กรุงเทพฯ : โปรวิชั่น.

นิวัติ เนียมพลอย. ไซเบอร์กับการรักษาความปลอดภัยและการปฏิบัติการ (Cyber with Security and Operations). from http://nniwat.wordpress.com.

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์. มาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ. from http://www.thaicert.or.th.

อมร ชมเชย. (๒๕๕๗). การประชุมเชิงปฏิบัติการด้านความมั่นคง ครั้งที่ ๓/๒๕๕๗. *“กองทัพกับยุทธศาสตร์ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของอาเซียน.”* 8 กรกฎาคม 2557 ณ โรงแรมทาวน์ อิน ทาวน์. กรุงเทพฯ: ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ.

Business Contituity Institute. แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยที่องค์กรทั่วโลกตระหนักปี ๒๐๑๔ (Threats and horizon scanning 2014). from http://www.thebci.org.

Global Agenda. แนวโน้มภัยคุกคามไซเบอร์ทั่วโลกประจำปี 2014. from http://www.weforum.org.

The United States Department of Defense. Trusted computer system evaluation criteria. from http://www.Defanse.gov.