บทคัดย่อ

ผู้วิจัย พันเอก ชนกศ์ จรจำรัส
เรื่อง การพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหม
วันที่ 4 กรกฎาคม 2560 **จำนวนคำ:** 5,004 **จำนวนหน้า :** 14
คำสำคัญ ไซเบอร์ สงครามไซเบอร์ มาตรฐาน กระทรวงกลาโหม
ชั้นความลับ ไม่มีชั้นความลับ

การพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหม ยังมีข้อจำกัดที่สำคัญ ได้แก่ การใช้มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ยังไม่เหมาะสม โดยใช้มาตรฐาน ISO 27001 : 2005 ซึ่งมีหลักการออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ มากกว่าการนำมาใช้ในภารกิจด้านการทหาร ดังนั้นควรปรับใช้มาตรฐาน U.S. DoD ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของระบบคอมพิวเตอร์เพื่อความมีประสิทธิภาพของอุปกรณ์ รวมทั้งการแก้ไข เพิ่มเติม ให้เหมาะสมกับบริบทของกระทรวงกลาโหม แต่ยังคงเป็นไปตามมาตรฐานสากล ในส่วนการปฏิบัติภารกิจเชิงรุก ทั้งภายในและภายนอกประเทศ ปัจจุบันยังไม่มีกฎหมายรองรับการดำเนินการ แต่สามารถรวบรวมรายชื่อเจ้าหน้าที่ ที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ขออนุมัติแต่งตั้งเป็นพนักงานเจ้าหน้าที่ ต่อรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสามารถปฏิบัติภารกิจเชิงรุกได้เฉพาะภายในประเทศเท่านั้น ไม่ครอบคลุมการดำเนินการภายนอกประเทศ และในส่วนการทำสงครามไซเบอร์ยังขาดเอกภาพในการดำเนินการ ควรแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์กระทรวงกลาโหม และจัดตั้งศูนย์บัญชาการไซเบอร์กลาโหม ซึ่งจะส่งผลให้เกิดเอกภาพในการปฏิบัติ ลดภาระงานของศูนย์ปฏิบัติการไซเบอร์ ส่งผลต่อการเพิ่มประสิทธิภาพในการทำสงครามไซเบอร์

ABSTRACT

AUTHOR: COLONEL CHANOG JORNJUMRUS

TITLE: THE CYBER DEVELOPMENT OF THE MINISTRY OF DEFENCE

DATE: 4 JULY 2017 **WORDCOUNT:** 5,004 **PAGES :** 14

KEY TERMS: CYBER, CYBER WARFARE, STANDARDS, THE MINISTRY OF DEFENCE

CLASSIFICATION: Unclassified

The Cyber Development of the Ministry of Defence have the important limitation such as the operation standards of cyber security, referred ISO 27001: 2005, which is based on business processes rather than being used in military missions. Therefore, the Ministry of Defence should apply the U.S. DoD standard which cover a basis for the computer safety assessment process for the effectiveness of the equipment, including amendments to suit the context of the Ministry of Defense but still conform to international standards. Currently, the proactive mission for both inside and outside the country, there have operate without legal support. Therefore, Ministry of Defence should list the officers who have responsibility for cybersecurity functions for approval. However, there is not cover for operations outside the country. In addition, the cyber warfare capability of Ministry of Defence is still lack of unity in operation. Therefore, the cybersecurity board should be appointed by the Ministry of Defense. They should establish cyber defence command center which lead to unity in practice, reducing work load of cyber operation center and enhances the cyber warfare efficiency.

กิตติกรรมประกาศ

การวิจัยเรื่อง “การพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหม” ฉบับนี้ สำเร็จลุล่วงไปได้ด้วยความกรุณาจากผู้บังคับบัญชา ผู้ร่วมงานในกรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ที่ให้การสนับสนุนข้อมูลในการทำวิจัย

กราบขอบพระคุณเป็นอย่างยิ่ง พลตรี ชัยยศ ลิลิตวงษ์ ผู้อำนวยการศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ที่ได้กรุณาเป็นผู้ทรงคุณวุฒิที่ปรึกษาให้คำแนะนำแนวทาง ในการศึกษาสืบค้นแนวคิด ทฤษฎี และข้อกฎหมายที่เกี่ยวข้อง อันเป็นประโยชน์อย่างยิ่งต่อการศึกษาวิจัยในครั้งนี้

กราบขอบพระคุณ พันเอก ภรัถ เทียนทองดี ที่ได้กรุณาเป็นอาจารย์ที่ปรึกษาให้คำแนะนำเกี่ยวกับแนวทางการศึกษา ตลอดจนตรวจสอบ ปรับปรุงแก้ไข จนทำให้เอกสารวิจัยฉบับนี้เสร็จสมบูรณ์เป็นอย่างดี

การพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหม

ประเทศไทยมุ่งมั่นที่จะเดินหน้าสู่ยุคดิจิตอลด้วยการปรับใช้เทคโนโลยีที่ทันสมัยเพื่อพัฒนาศักยภาพทางด้านเศรษฐกิจของประเทศ ภายใต้โมเดล Thailand 4.0 ซึ่งมุ่งเน้นการสร้างสรรค์นวัตกรรมทางด้านเทคโนโลยีและการพัฒนาระบบดิจิตอล เพื่อปรับปรุงคุณภาพชีวิต กำลังการผลิต และประสิทธิภาพการทำงาน โดยมีการปรับใช้เทคโนโลยีดิจิตอลที่หลากหลาย เช่น Internet of Things (IoT), เทคโนโลยีคลาวด์ (Cloud), บิ๊กดาต้า (Big Data) และระบบวิเคราะห์ข้อมูลขั้นสูง (Analytics) [1] แต่ต้องระมัดระวังในเรื่องภัยคุกคามด้านไซเบอร์ เนื่องจากปัจจุบันการเติบโตและความสามารถในการเข้าถึงโครงข่ายไซเบอร์ของประชากรในประเทศไทยเพิ่มขึ้นอย่างก้าวกระโดด จึงทำให้ความเสี่ยงด้านภัยคุกคามไซเบอร์มีสูงขึ้นหลายเท่าตัวและจะเป็นภัยคุกคามที่จะถูกยกระดับในเชิงยุทธศาสตร์ของประเทศอย่างหลีกเลี่ยงไม่ได้ โดยภัยคุกคามรูปแบบใหม่นี้เป็นภัยคุกคามที่มีรูปแบบผสมที่ซับซ้อน ทั้งในมิติของสังคม เศรษฐกิจ การเมือง และการทหาร ดังนั้นการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง แต่ต้องสมดุลกับยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์(Cybersecurity) ที่เข้มแข็ง [2]

“ความมั่นคงปลอดภัยไซเบอร์” (Cyber Security) คือ มาตรการและการดำเนินการที่กำหนดขึ้นเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศให้สามารถปกป้องป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศและความมั่นคงทางเศรษฐกิจ [3]

ในด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ยังคงถูกจัดลำดับ ในเรื่องไม่มีความมั่นคงปลอดภัยทางไซเบอร์ เช่น [4] เมื่อวันที่ 26 มิถุนายน 2557 รายงานจากเว็บไซต์บิสซิเนสอินไซเดอร์ สื่อวิเคราะห์ด้านธุรกิจและการเงินของประเทศสหรัฐอเมริกา เผยว่า บริษัทด้านการปกป้องข้อมูลคอมพิวเตอร์ นอร์ส (NORSE) เปิดเผยถึงสถิติการโจมตีเพื่อเจาะฐานข้อมูลเครือข่ายอินเทอร์เน็ต โดยพบว่าประเทศสหรัฐอเมริกา เป็นประเทศที่เป็นเป้าหมายถูกโจมตีมากที่สุดในโลก ด้วยสถิติ 5,840 ครั้ง ใน 45 นาที โดยมีประเทศไทยตามมาในอันดับที่สอง ด้วยสถิติการถูกโจมตีฐานข้อมูล 220 ครั้งในเวลาเท่า ๆ กัน [5] เมื่อวันที่ 29 กุมภาพันธ์ 2559 รายงานจากเว็บไซต์ผู้สื่อข่าวเอเชีย ว่าบริษัทด้านโปรแกรม

การรักษาความปลอดภัยไซเบอร์ บิทดีเฟนเดอร์ (BitDefender) เปิดเผยถึงสถิติพบว่าประเทศไทยมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์เป็นลำดับ 5 ในเอเชีย และเป็นลำดับ 11 ของโลก และติดลำดับ 25 ประเทศแรกที่ถูก มัลแวร์ (malware) โจมตีมากที่สุด จากการสำรวจ 200 ประเทศทั่วโลก

จากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนามาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ดังนั้นเพื่อให้ประเทศไทยสามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่าง ๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม มีการดำเนินการที่รวดเร็วและมีความเป็นเอกภาพ เป็นที่เชื่อถือและยอมรับในระดับสากล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้จัดทำ ร่างกรอบนโนบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้นเมื่อ พ.ศ.2556 ซึ่งมียุทธศาสตร์หลัก 3 ด้าน[6] ได้แก่ การบูรณาการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ และการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

ในส่วนกระทรวงกลาโหม ซึ่งมีภารกิจหลักด้านความมั่นคงของชาติ ได้มีการจัดทำยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.2558 [7] ขึ้นเพื่อเป็นกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง 4 ปี คือ พ.ศ. 2558 – 2562 โดยมีการกำหนดประเด็นยุทธศาสตร์ไว้ 3 ประเด็นคือ ป้องกัน ป้องปราม และผนึกกำลัง และได้จัดทำแผนแม่บท ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564 [8] รวมทั้งแต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม[9] เพื่อให้การดำเนินงานด้านไซเบอร์ในระดับกระทรวงกลาโหมเป็นไปด้วยความเรียบร้อย มีการกำหนดนโยบายและกรอบแนวทางการพัฒนางานด้านไซเบอร์ของกระทรวงกลาโหม

ที่ชัดเจน และมีการกำกับดูแลให้มีความสอดคล้อง ตามยุทธศาสตร์ไซเบอร์ป้องกันประเทศกระทรวงกลาโหม

ในระดับเหล่าทัพ กองบัญชาการกองทัพไทย ได้จัดทำยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ. 2558 [10] เช่นเดียวกัน เพื่อให้กองทัพไทยมีขีดความสามารถและมีเสรีในการปฏิบัติการบนมิติไซเบอร์ ทั้งเชิงรับและเชิงรุกตั้งแต่สภาวะปกติ ตลอดจนสามารถบูรณาการ และให้การสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ของประเทศไทยในภาพรวมได้อย่างมีประสิทธิภาพ โดยได้กำหนดประเด็นยุทธศาสตร์ทหารสำหรับการปฏิบัติการทางทหารในมิติไซเบอร์ เพื่อใช้เป็นกรอบแนวทางในการดำเนินการให้สามารถบรรลุวัตถุประสงค์ทางทหารที่ตั้งไว้แยกเป็น 3 ประเด็นยุทธศาสตร์ได้แก่ ยุทธศาสตร์การป้องกันเชิงรุก ยุทธศาสตร์การผนึกกำลังป้องกันประเทศและยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคง

กระทรวงกลาโหม กองบัญชาการกองทัพไทยและเหล่าทัพ ได้มีการจัดตั้งหน่วยงานด้านไซเบอร์เพื่อรองรับภารกิจการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นที่เรียบร้อย โดยแบ่งการดำเนินงานเป็น 2 ส่วนคือ ส่วนปฏิบัติกรด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) และส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security Incident Response Team : CSIRT) ซึ่งเป็นการพัฒนาศักยภาพทางไซเบอร์ของ กระทรวงกลาโหมในปัจจุบัน ดังนี้ [11]

ระดับ	**หน่วยงานไซเบอร์**	**CSOC (เชิงรับ)**	**CSIRT (เชิงรุก)**
สำนักงานปลัดกระทรวงกลาโหม(สป.)	กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (ทสอ.กห.)	กองเทคโนโลยีสารสนเทศ ทสอ.กห.	ศูนย์ไซเบอร์ ทสอ.กห.
กองบัญชาการกองทัพไทย (บก.ทท.)	ศูนย์ปฏิบัติการไซเบอร์ร่วม ทท.	กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร สส.ทหาร	กองสงครามเครือข่าย สปก.ยก.ทหาร

ระดับ	หน่วยงานไซเบอร์	CSOC (เชิงรับ)	CSIRT (เชิงรุก)
กองทัพบก	ศูนย์ไซเบอร์ ทบ. (ศซบ.ทบ.)	กองปฏิบัติการไซเบอร์ ศซบ.ทบ.	กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศซบ.ทบ.
กองทัพเรือ	กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (สสท.ทร.)	กองสงครามไซเบอร์ สำนักปฏิบัติการ สสท.ทร.	กองสงครามไซเบอร์ สำนักปฏิบัติการ สสท.ทร.
กองทัพอากาศ	กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.)	ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ	กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม ทสส.ทอ.

จากการศึกษาค้นคว้า ข้อมูลจากหน่วยงานที่เกี่ยวข้อง รวมทั้งพิจารณามาตรฐาน ข้อกฎหมาย งานวิจัย และเอกสารทางวิชาการต่างๆ พบว่าการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหม ยังมีข้อจำกัดที่สำคัญดังนี้

การใช้มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กล่าวได้ว่าความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการเหล่านั้นได้ถูกกำหนดเอาไว้เป็นมาตรฐานที่เป็นที่ยอมรับ โดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ซึ่งองค์กรสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของตน และอาจเพิ่มเติมหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ

สำหรับมาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 – 14, มาตรฐาน COBIT, และ มาตรฐาน IT BPM [12] โดยมาตรฐาน U.S. DoD เป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม

สหรัฐอเมริกา ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของระบบคอมพิวเตอร์เพื่อความมีประสิทธิภาพของอุปกรณ์ตั้งแต่ขั้นตอนแรก คือ กระบวนการประมูลจัดซื้อหรือจัดจ้างสำหรับหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางในการออกแบบ พัฒนา ผลิต หรือทดสอบสำหรับผู้ผลิตเทคโนโลยี หรือภาคเอกชนได้ปฏิบัติตามเพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้

มีการกำกับคุณภาพของคนโดยมีใบรับรอง IT Certificate ทางด้าน Cyber Security ทำให้ได้เจ้าหน้าที่ ที่เหมาะสมเข้ามาทำงานด้านนี้ นอกจากนี้ยังให้ความสำคัญกับหลักการประกันความมั่นคงปลอดภัยสารสนเทศ (Informational Assurance: IA) โดยมีมาตรฐานในการประเมิน และมี IT Audit team ในการกำกับควบคุม ทำให้การนำนโยบายด้านไซเบอร์มาสู่การปฏิบัติ มีประสิทธิภาพมากยิ่งขึ้น

มาตรฐาน ISO 27001 : 2005 เป็นมาตรฐานที่มีแนวทางปฏิบัติที่ได้รับการยอมรับและนำไปใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรทั่วโลก ในขณะที่มาตรฐาน COBIT เป็นมาตรฐานที่มีจำนวนแนวทางปฏิบัติใกล้เคียงกับ ISO 27001 : 2005 ยกเว้นแนวทางการป้องกันและการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อม จากภายในและภายนอกองค์กรและมาตรฐานที่มีแนวทางปฏิบัติน้อยที่สุดได้แก่ มาตรฐาน IT BMP เนื่องจากมาตรฐานนี้เป็นการกำหนดมาตรฐานขั้นต่ำที่องค์กรควรจะปฏิบัติ

แนวทางในการดำเนินการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหมสู่มาตรฐานสากลนั้นจะต้องดำเนินการตามกฎหมาย คือพระราชกฤษฎีกาว่าด้วย วิธีการแบบปลอดภัย ในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 ที่เกี่ยวข้องคือให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด [13]

โดยตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 ได้ออกประกาศกำหนดหลักเกณฑ์ และรายละเอียดของมาตรฐาน การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับชั้น ซึ่งมาตรฐานดังกล่าว จะครอบคลุมการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องความครบถ้วน

(Integrity) และ การสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ และให้ความสำคัญกับการดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ [14]

กระทรวงกลาโหม ซึ่งเป็นหน่วยงานของรัฐ ต้องดำเนินการตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 ซึ่งอ้างอิงตามมาตรฐาน ISO 27001 : 2005 ซึ่งมีหลักการที่ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ[15]

โดยเฉพาะการปกป้องข้อมูลและทรัพย์สินจากภัยคุกคามทางไซเบอร์ที่มาในรูปแบบต่างๆ เช่น ความเสี่ยงจากการใช้งานอินเทอร์เน็ต ภัยจากการทำธุรกรรมทางธนาคารหรือการซื้อขายออนไลน์ การโจรกรรมพาสเวิร์ด การจู่โจมด้วยการส่งโปรแกรมดักจับข้อมูลทางคอมพิวเตอร์เป็นต้น จึงเป็นมาตรฐานที่เหมาะสม ในสภาวะแวดล้อมทางธุรกิจ มากกว่าการนำมาใช้ในงานด้านการทหาร งานด้านความมั่นคง ที่ภารกิจต่าง ๆ ล้วนเกี่ยวข้องและมีความสำคัญอย่างมากต่ออธิปไตยของชาติ จึงเป็นข้อจำกัดที่สำคัญ

ข้อจำกัดดังกล่าวย่อมส่งผลต่อกระบวนการจัดซื้อ – จัดจ้าง ที่ใช้ในงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ทั้งในส่วนฮาร์ดแวร์ และซอร์ฟแวร์ ที่ต้องใช้งานเฉพาะเจาะจง ตามภารกิจหลักของเหล่าทัพที่ไม่เหมือนกัน รวมทั้งในภารกิจด้านความมั่นคง ซึ่งอาจถูกร้องเรียนว่าเกินกว่ามาตรฐานที่ใช้งาน และมีราคาสูงเกินกว่าเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดไว้อีกด้วย

ดังนั้นกระทรวงกลาโหมจึงควรพัฒนามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมขึ้นมาใช้เอง โดยการปรับใช้ มาตรฐาน U.S. DoD ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของระบบคอมพิวเตอร์เพื่อความมีประสิทธิภาพของอุปกรณ์ตั้งแต่ขั้นตอนแรก คือ กระบวนการประมูลจัดซื้อหรือจัดจ้างสำหรับหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางในการออกแบบ พัฒนา ผลิต หรือทดสอบสำหรับผู้ผลิตเทคโนโลยี หรือภาคเอกชนได้ปฏิบัติตาม เพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้ รวมทั้งการแก้ไข เพิ่มเติม ให้เหมาะสมกับบริบทของกระทรวงกลาโหมแต่ยังคงเป็นไปตามมาตรฐานสากล

ส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security Incident Response Team : CSIRT) ซึ่งมีภารกิจเชิงรุก ทั้งภายในและภายนอกประเทศ

การปฏิบัติการเชิงรุก สามารถใช้เป็นกำลังอำนาจที่ไม่มีตัวตน ในการปฏิบัติการบนโลกไซเบอร์ เป็นที่ทราบกันดีว่า ภัยคุกคามด้านไซเบอร์ (Cyber Threats) ถูกนำมาใช้เป็นเครื่องมือทางการทหาร ไม่ว่าจะเป็นการเจาะระบบ (Hack /Crack) การฝังโปรแกรมลักลอบโจรกรรมข้อมูล เช่น สปายแวร์ (Spyware) หรือ ประตูหลัง (Back Door) การโจมตีด้วยโปรแกรมมัลแวร์ (Malware) อาทิเช่น ไวรัสคอมพิวเตอร์ (Computer Virus) , หนอนคอมพิวเตอร์ (Computer Worm) หรือ ม้าโทรจัน (Trojan Horse) , การใช้โปรแกรมตั้งเวลาทำงานเพื่อการทำลาย (Logic Bomb) การโจมตีแบบ DoS/DDos การใช้โปรแกรมหุ่นยนต์โจมตีเพื่อเป็นฐานโจมตีอุปกรณ์คอมพิวเตอร์บนเครือข่ายสารสนเทศ (BOTNET / Robot Network) การสร้างข้อมูลขยะ (Spam) เป็นต้น [16]

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ยก (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ขึ้น [17] เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่างๆ อันครอบคลุมถึง ความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม มีการดำเนินการที่รวดเร็วและมีความเป็นเอกภาพ โดยมีสาระสำคัญที่เกี่ยวข้อง ได้แก่ “พนักงานเจ้าหน้าที่” หมายความว่าผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้ มาตรา 6 ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กปช.” และให้ใช้ชื่อภาษาอังกฤษว่า “National Cyber Security Committee” เรียกโดยย่อว่า “NCSC” โดยมี รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

มาตรา 7 ให้ กปช. มีอำนาจหน้าที่ โดยที่เกี่ยวข้องคือ กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ ความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรืออย่าง

ร้ายแรง เพื่อให้เป็นศูนย์กลางการดำเนินการเมื่อมีเหตุการณ์หรือสถานการณ์ความมั่นคงปลอดภัยได้อย่างทันท่วงที มีความเป็นเอกภาพ เว้นแต่ภัยคุกคามทางไซเบอร์นั้นเป็นภัยที่กระทบต่อความมั่นคงทางทหาร ซึ่งเป็นอำนาจของสภากลาโหมหรือสภาความมั่นคงแห่งชาติ

มาตรา 35 เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ มีอำนาจดังต่อไปนี้

(1) มีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติการตามพระราชบัญญัตินี้

(2) มีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช.

(3) เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

การดำเนินการตาม (3) ให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะรัฐมนตรีกำหนด

มาตรา 37 การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญเกี่ยวกับระบบคอมพิวเตอร์หรือการรักษาความมั่นคงปลอดภัยสารสนเทศและมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา 38 เพื่อประโยชน์ในการประสานงานหรือการปฏิบัติการ ให้เจ้าหน้าที่ของกระทรวงกลาโหมที่ได้รับมอบหมายในการปฏิบัติภารกิจเพื่อตอบสนองและรับมือกับภัยคุกคามไซเบอร์ที่กระทบต่อความมั่นคงทางทหาร เป็นพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

พบว่า ปัจจุบัน (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ยังมิได้ประกาศใช้ ดังนั้น การปฏิบัติภารกิจเชิงรุก ทั้งภายในและภายนอกประเทศ ของส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security Incident Response Team : CSIRT) จึงไม่มีข้อกฎหมาย รองรับการดำเนินการในปัจจุบันซึ่งเป็นข้อจำกัดที่สำคัญ

เมื่อ (ร่าง) พระราชบัญญัติฉบับนี้ ได้ประกาศใช้ จะมีประโยชน์ต่อการดำเนินงานรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมเป็นอย่างมาก การปฏิบัติภารกิจเชิงรุกทั้งภายในและภายนอกประเทศ จะมีข้อกฎหมาย รองรับการดำเนินการ โดยเจ้าหน้าที่ที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จะเป็นพนักงานเจ้าหน้าที่ตามมาตรา 38 ของ(ร่าง) พระราชบัญญัติฉบับนี้ ซึ่งสามารถปฏิบัติภารกิจเชิงรุกภายในประเทศได้ ในส่วนการปฏิบัติภารกิจเชิงรุกภายนอกประเทศ สามารถดำเนินการตามมาตรา 7 ซึ่งเป็นอำนาจของสภากลาโหม โดยเห็นควรให้คณะอนุกรรมการไซเบอร์กระทรวงกลาโหม จัดทำแนวทางและมาตรการตอบสนอง เพื่อขอความเห็นชอบจากสภากลาโหมต่อไป ดังนั้นกระทรวงกลาโหมควรเร่งผลักดัน (ร่าง) พระราชบัญญัติฉบับนี้ ให้ประกาศใช้โดยเร็ว

และตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งได้ประกาศในราชกิจจานุเบกษา เมื่อ มกราคม 2560 [18] โดยในมาตรา 4 ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รักษาการตาม พระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้

พบว่า การปฏิบัติภารกิจเชิงรุก ทั้งภายในและภายนอกประเทศ ของส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security Incident Response Team : CSIRT) เจ้าหน้าที่ผู้ปฏิบัติงานมิได้เป็นเจ้าหน้าที่ตามพระราชบัญญัติฉบับนี้ จึงไม่มีข้อกฎหมาย รองรับการดำเนินการในปัจจุบันซึ่งเป็นข้อจำกัดที่สำคัญ

ถึงแม้เจ้าหน้าที่ผู้ปฏิบัติงานมิได้เป็นเจ้าหน้าที่ตามพระราชบัญญัติฉบับนี้ แต่ก็ได้เปิดช่องไว้ใน มาตรา 4 ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่ได้ จึงเห็นควรให้กระทรวงกลาโหมรวบรวมรายชื่อเจ้าหน้าที่ที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ขออนุมัติแต่งตั้งเป็นพนักงานเจ้าหน้าที่ต่อรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมต่อไป แต่ก็จะยังมีข้อจำกัด โดยสามารถปฏิบัติภารกิจเชิงรุกได้เฉพาะภายในประเทศเท่านั้น ไม่ครอบคลุมการดำเนินการภายนอกประเทศ

การดำเนินการด้านไซเบอร์ของกระทรวงกลาโหมในปัจจุบัน ยังมีข้อจำกัด ต่อการทำสงครามไซเบอร์

สงครามไซเบอร์ (Cyberwarfare) เป็นคำที่นิยามขึ้นมาโดย ผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลที่ชื่อ ริชาร์ด เอ. คลาร์ก ในหนังสือที่ชื่อ Cyber War (พฤษภาคม 2010) โดยนิยามว่า "เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก" [19]

สงครามไซเบอร์มีการโจมตีกันหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด อาทิ การโจมตีเว็บ หรือบล็อกเว็บ, การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเทอร์เน็ต, การเจาะข้อมูลลับ โดยแฮ็กเกอร์ที่นอกจากได้ข้อมูลลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้, การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้ หรือทำงานไม่แม่นยำ, การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก สงครามไซเบอร์เป็นการปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้าม และต้องทำให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา [20]สงครามไซเบอร์ได้อุบัติขึ้นแล้วในหลายประเทศซึ่งมีทั้งประเภทชัดเจน เปิดเผย และซุ่มเงียบ ตัวอย่างเช่น

ในช่วงสงครามอ่าวที่สหรัฐโจมตีอิรัก และสงครามอิรักครั้งที่สอง สิ่งที่สหรัฐต้องทำก่อนอื่นคือ ทำลายเครือข่ายคอมพิวเตอร์และอิเล็กทรอนิกส์ของอิรักที่ใช้ควบคุมระบบการยิงของอาวุธ ไม่เพียงแต่กรณีสงครามอิรักเท่านั้น ในการสู้รบปัจจุบัน แต่ละฝ่ายต้องหาทางทำลายระบบคอมพิวเตอร์และอิเล็กทรอนิกส์ ที่ควบคุมการยิงของอาวุธก่อน ในวันที่ 17 พฤษภาคม 2550 ประเทศเอสโตเนียถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะรัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่างๆ จนข้อมูลเสียหายพังยับเยิน เมื่อต้นเดือนกันยายน 2550 ตึกเพนตากอน กระทรวงกลาโหม สหรัฐอเมริกา และที่ทำการรัฐบาลของฝรั่งเศส เยอรมนี และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหายอย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา [21]

สำนักข่าวเอเอฟพีรายงานเมื่อวันที่ 29 กุมภาพันธ์ 2559 ว่า กระทรวงกลาโหมสหรัฐอเมริกา ยกระดับ สงครามไซเบอร์ โจมตีเครือข่ายคอมพิวเตอร์ของ กลุ่มรัฐอิสลาม (ไอเอส) อย่างจริงจัง โดยใช้ทางเทคนิคที่พัฒนาขึ้นเอง ส่งผลให้ระบบคอมพิวเตอร์ของ

ไอเอสโอเวอร์โหลดจนทำงานไม่ได้ ซึ่งเป็นการขัดขวางไม่ให้แกนนำไอเอส สามารถบัญชาการนักรบ ได้อย่างสะดวก [22]

เมื่อปลายเดือนกันยายน 2559 รัฐบาลเกาหลีใต้ได้รายงานว่า แฮ็กเกอร์ได้เจาะระบบเซิร์ฟเวอร์กลางของศูนย์บัญชาการกองกำลังทางไซเบอร์เกาหลีใต้ โดยตัวเซิร์ฟเวอร์ดังกล่าวทำหน้าที่เป็นช่องทางในการเชื่อมต่ออินเทอร์เน็ตและใช้วิเคราะห์ทราฟฟิกของคอมพิวเตอร์ในกองทัพกว่า 20,000 เครื่องเพื่อตรวจจับการโจมตี โดยแฮ๊กเกอร์ได้เจาะระบบผ่านช่องโหว่ของเซิร์ฟเวอร์และฝังมัลแวร์ได้ [23]

การดำเนินงานของ หน่วยบัญชาการไซเบอร์สหรัฐอเมริกา

จะเห็นได้ว่าการโจมตีโดยใช้สงครามไซเบอร์ เป็นสงครามรูปแบบใหม่ที่มีผลกระทบในระดับยุทธศาสตร์ ประเทศมหาอำนาจเช่น สหรัฐอเมริกา รัสเซีย จีน ให้ความสำคัญและเชื่อว่าเมื่อเกิดความขัดแย้งจะเริ่มรุกด้วยสงครามไซเบอร์ก่อน สหรัฐอเมริกาจึงได้มีการปรับเปลี่ยนแนวคิดทางทหารใหม่ เป็นการแบ่งมอบงานไซเบอร์หลักๆ ให้กรมฝ่ายเสนาธิการร่วม รับผิดชอบอย่างสอดคล้องกัน ตามภารกิจ วิสัยทัศน์ ภายใต้ยุทธศาสตร์ของหน่วยบัญชาการไซเบอร์สหรัฐอเมริกา โดยสรุปสาระสำคัญคือ [24]

ด้านการรับรู้สถานการณ์ไซเบอร์ทั่วโลกบนเครือข่ายทั้งปวง เป็นภาระหน้าที่ของกรมยุทธการทหาร (Directorate of Operation : J3) กรมข่าวทหาร (Directorate of Intelligence: J2)

ด้านการฝึกอบรมและการสร้างความพร้อมทีมงานไซเบอร์ เป็นภาระหน้าที่ของ กรมพัฒนาแผนยุทธการและกองกำลังรบร่วม (Directorate of Operational Planning and Joint Force Development: J7)

ด้านการสร้างสถาปัตยกรรมไซเบอร์ซึ่งป้องกันได้มากยิ่งขึ้น เป็นภาระหน้าที่ของกรมบังคับบัญชาควบคุม สื่อสาร และคอมพิวเตอร์ (Directorate of Command, Control, Communication, and Computer : J6)

ด้านการพัฒนาผู้มีอำนาจในกระทรวงกลาโหม กระทรวงความมั่นคงแห่งมาตุภูมิ และสำนักงานสอบสวนกลาง เกี่ยวกับบทบาทและความรับผิดชอบ เพื่อการป้องกันประเทศ

เป็นภาระหน้าที่ของ กรมนโยบายและแผนยุทธศาสตร์ (Directorate of Strategic Plans and Policy : J5)

และด้านการสร้างกระบวนการสั่งการและการควบคุมที่มีประสิทธิภาพ ตลอดจนแนวความคิดการปฏิบัติการไซเบอร์ เป็นภาระหน้าที่ของ กรมบังคับบัญชา ควบคุม สื่อสาร และคอมพิวเตอร์ (Directorate of Command , Control , Communication , and Computer : J6)

การดำเนินงานของ กระทรวงกลาโหม

รัฐมนตรีว่าการกระทรวงกลาโหม ได้อนุมัติหลักการ แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์กระทรวงกลาโหม[25] ซึ่งมีแนวความคิดควรจัดคณะกรรมการประกอบด้วยผู้แทนกรมฝ่ายเสนาธิการ ตามการมอบหมายงานไซเบอร์หลักๆ โดยมีหน่วยบัญชาการไซเบอร์สหรัฐอเมริกา เป็นแม่แบบดังนี้ [26]

การมอบหมายงานไซเบอร์หลักๆ กับกรมฝ่ายเสนาธิการ

กรมฝ่ายเสนาธิการ	**ขั้นปกติ**	**ขั้นตอบโต้**	**ขั้นป้องกันประเทศ**
ฝสธ.2,3	การรับรู้สถานการณ์ไซเบอร์บนเครือข่ายทั่วโลก		
ฝสธ.5,7	การฝึกอบรมสร้างความพร้อมกำลังพลไซเบอร์		
ฝสธ.6	การสร้างสถาปัตยกรรมไซเบอร์ ปกป้องเครือข่าย		
ฝสธ.5,7	การพัฒนาผู้มีอำนาจฝ่ายความมั่นคงของประเทศ		
ฝสธ.6	การสร้างระบบควบคุมบังคับบัญชาไซเบอร์		
ฝสธ.3,6	การปฏิบัติการไซเบอร์		
ฝสธ.5,6	การพัฒนาหลักนิยมไซเบอร์		

โดย ฝสธ.2 ข่าว, ฝสธ.3 ยุทธการ, ฝสธ.5 แผน, ฝสธ.6 สารสนเทศและสื่อสาร, ฝสธ.7 กิจการพลเรือน หมายถึง กรมฝ่ายเสนาธิการในส่วนของ หน่วยขึ้นตรงกระทรวงกลาโหมและเหล่าทัพ

พบว่าปัจจุบันยังมิได้แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์กระทรวงกลาโหม แต่ได้มีการแต่งตั้ง คณะอนุกรรมการไซเบอร์กระทรวงกลาโหม [27] โดยมีเจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหมเป็นประธาน มีผู้อำนวยการศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหมเป็นเลขานุการ มีอำนาจหน้าที่ ที่สำคัญคือ ดำเนินการจัดทำร่างนโยบาย ยุทธศาสตร์ แผนแม่บท ระเบียบ ข้อบังคับ คู่มือด้านไซเบอร์ ระดับกระทรวงกลาโหมและเอกสารด้านไซเบอร์ที่มีผลบังคับใช้ในภาพรวม ของระทรวงกลาโหม เสนอต่อคณะกรรมการ เทคโนโลยีสารสนเทศและการสื่อสารกระทรวงกลาโหม ที่มีปลัดกระทรวงกลาโหม เป็นประธาน และมีเจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม เป็นเลขานุการ

การแต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม โดยที่มิได้แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์กระทรวงกลาโหมจะทำให้เกิดข้อจำกัด คือ คณะอนุกรรมการจัดจาก กรมยุทธการ (ฝสธ.3) และหน่วยงานไซเบอร์ ในส่วนของสำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทยและเหล่าทัพ เป็นหลัก มิได้มี ฝสธ.2 ข่าว, ฝสธ.5 แผน , ฝสธ.6 สารสนเทศและสื่อสาร, ฝสธ.7 กิจการพลเรือน ซึ่งมีความสำคัญในการมอบหมายงานไซเบอร์หลักๆ กับกรมฝ่ายเสนาธิการ เมื่อต้องการข้อมูลและการดำเนินการจำต้องเสียเวลาในการประสานงาน และการดำเนินการ รวมทั้งต้องเสนอต่อ คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารกระทรวงกลาโหมเพื่อพิจารณาอนุมัติ ทำให้ขาดเอกภาพในการดำเนินการ ย่อมส่งผลต่อประสิทธิภาพในการทำสงครามไซเบอร์

ดังนั้น เมื่อมีความพร้อมควรเร่งจัดตั้ง รวมทั้งสมควรให้ กระทรวงการต่างประเทศ กรมพระธรรมนูญ หน่วยงานด้านความมั่นคงในสภาความมั่นคงแห่งชาติ และหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศต้องร่วมมืออย่างใกล้ชิด ในการพัฒนาหลักนิยมไซเบอร์ การปฏิบัติการไซเบอร์ และการจัดทำกฎการใช้กำลังไซเบอร์ ให้ถูกต้องชอบธรรมตามกฎหมายภายในประเทศ และกฎหมายระหว่างประเทศ ครอบคลุมทุกการปฏิบัติการทางทหารของหน่วยขึ้นตรงกระทรวงกลาโหมและเหล่าทัพ

รัฐมนตรีว่าการกระทรวงกลาโหม ยังได้อนุมัติหลักการจัดตั้งหน่วยรับผิดชอบด้านไซเบอร์ของกระทรวงกลาโหม ในลักษณะหน่วยบัญชาการไซเบอร์ (Cyber Command) ให้มี

เอกภาพงานด้านไซเบอร์ในกระทรวงกลาโหม [28] โดยมีโครงสร้างศูนย์บัญชาการไซเบอร์กลาโหมประกอบด้วย [29] ส่วนบังคับบัญชา แบ่งเป็น กำลังพล งบประมาณ การเงิน ธุรการ ส่วนแผนและยุทธศาสตร์ แบ่งเป็น แผนและยุทธศาสตร์ไซเบอร์ ติดตามสถานการณ์และอำนวยการยุทธ์ กฎหมายไซเบอร์ ปฏิบัติการข่าวสารไซเบอร์ ส่วนปฏิบัติการไซเบอร์ แบ่งเป็น ป้องกัน โจมตีและแทรกซึม สืบสวน ชุดเผชิญเหตุ และส่วนพัฒนาไซเบอร์ แบ่งเป็น พัฒนาหลักสูตรและฝึกอบรม จำลองยุทธไซเบอร์ วิจัยและพัฒนาไซเบอร์ พัฒนาหลักนิยม ระเบียบปฏิบัติ มาตรฐาน

หน้าที่ศูนย์บัญชาการไซเบอร์กลาโหม ได้แก่ ปรับปรุงการแจ้งเตือนเหตุการณ์ไซเบอร์ให้ครอบคลุมเครือข่ายทั้งหมด สร้างแบบฝึกและกองกำลังไซเบอร์พร้อมปฏิบัติการ สร้างสถาปัตยกรรมไซเบอร์ที่มีศักยภาพเชิงป้องกันให้ดียิ่งขึ้น การพัฒนาหน่วยงานโครงสร้างสำคัญในบทบาทและความรับผิดชอบเพื่อการป้องกันประเทศ เสริมสร้างระบบควบคุมบังคับบัญชาและการปฏิบัติการไซเบอร์ และเป็นหน่วยปฏิบัติรองรับมติคณะกรรมการความมั่นคงปลอดภัยไซเบอร์กระทรวงกลาโหม

พบว่าปัจจุบัน ยังมิได้มีการจัดตั้ง ศูนย์บัญชาการไซเบอร์กลาโหม โดยจะทำให้เกิดข้อจำกัด คือ จากการที่ศูนย์ปฏิบัติการไซเบอร์ในส่วนของ สำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ยังอยู่ในระยะเริ่มแรกของการจัดตั้ง ปัญหาสำคัญที่ต้องเร่งดำเนินการ คือ การขาดองค์ความรู้ไซเบอร์และขาดกำลังพลไซเบอร์ ที่มีความเชี่ยวชาญและเพียงพอ ต่อการทำสงครามไซเบอร์ และจำต้องรับภาระงานอื่นๆ ที่จำเป็นต้องปฏิบัติ ย่อมส่งผลต่อประสิทธิภาพในการทำสงครามไซเบอร์

ดังนั้นพื่อให้กำลังพลไซเบอร์ มีความชำนาญและเพียงพอ ต่อการทำสงครามไซเบอร์ในระดับหนึ่ง เห็นควรจัดตั้งศูนย์บัญชาการไซเบอร์กลาโหม ซึ่งจะส่งผลให้เกิดเอกภาพในการปฏิบัติ ลดภาระงานของศูนย์ปฏิบัติการไซเบอร์ ส่งผลต่อการเพิ่มประสิทธิภาพในการทำสงครามไซเบอร์ นอกจากนั้น ต้องเชื่อมโยงความสัมพันธ์ด้านนโยบายและยุทธศาสตร์ไปถึงศูนย์ปฏิบัติการไซเบอร์ทั้งในส่วนของ กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ซึ่งต้องดำเนินการปรับโครงสร้างให้สอดคล้องตามภารกิจหน้าที่ต่อไป

บทสรุป

ถึงแม้ในปัจจุบันกระทรวงกลาโหมได้มี ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม เพื่อใช้เป็นกรอบในการดำเนินงานด้านไซเบอร์ ได้แต่งตั้งคณะอนุกรรมการไซเบอร์ กระทรวงกลาโหม รวมทั้งได้จัดตั้งหน่วยงานด้านไซเบอร์ที่ดูแลรับผิดชอบ เรียบร้อยแล้วก็ตาม แต่ก็เป็นเพียงระยะเริ่มแรกของการดำเนินงานขับเคลื่อนอย่างเป็นรูปธรรมเท่านั้น

การพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหม ยังมีข้อจำกัดที่สำคัญ ได้แก่ การใช้มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ยังไม่เหมาะสม ในส่วนการปฏิบัติภารกิจเชิงรุก ทั้งภายในและภายนอกประเทศ ปัจจุบันยังไม่มีกฎหมายรองรับการดำเนินการ และในส่วนการทำสงครามไซเบอร์ ยังขาดเอกภาพในการดำเนินการ ทั้งนี้สิ่งสำคัญลำดับแรกสำหรับการพัฒนาก็คือ องค์ความรู้ไซเบอร์และกำลังพลไซเบอร์ที่เพียงพอ ต่อการทำสงครามไซเบอร์ ซึ่งจะเป็นรากฐานที่สำคัญในการพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหมต่อไป

เอกสารอ้างอิง

[1] Cyber Security สำคัญอย่างยิ่งต่อความสำเร็จของ ”Thailand 4.0” ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://www.techtalkthai.com/cyber-security-for-thailand-4-0

[2] Thailand 4.0 กับภัยคุกคามด้านอาชญากรรมไซเบอร์ ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://www.it24hrs.com/2016/thailand-4-0-cybersecurity

[3] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-cyber-security-protection-act

[4] สถิติการโจมตีเครือข่ายอินเทอร์เน็ต. บิสซิเนส อินไซเดอร์ ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก http://www.businessinsider.com/norse-hacking-map-shows-us-getting-hammered-2014-6

[5] ประเทศไทยมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์เป็นลำดับ 5 ในเอเชีย.ผู้สื่อข่าวเอเชีย ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://asiancorrespondent.com/2016/02/thailand-faces-5th-highest-risk-for-cybersecurity-threats-in-asia-bitdefender/#5sGyKpwVKR6uKa1A.99

[6] ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://thainetizen.org/wp-content/uploads/2015/01/cybersecurity-bill-cabinet-approved-20150106.pdf

[7] ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม; 2558

[8] แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม; 2560 – 2564

[9] คำสั่งคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงกลาโหม(เฉพาะ) ที่ 10/60 เรื่อง แต่งตั้งคณะอนุกรรมการไซเบอร์ กระทรวงกลาโหม ลงวันที่ 9 กุมภาพันธ์ 2560

[10] สุทธิศักดิ์ สลักคำ , พลตรี. ยุทธศาสตร์การป้องกันไซเบอร์ กระทรวงกลาโหม [เอกสารวิจัยส่วนบุคคล]. กรุงเทพฯ: วิทยาลัยป้องกันราชอาณาจักร; 2558

[11] คณะทำงานด้านเทคโนโลยีสารสนเทศและสถานีโทรทัศน์ดิจิตอลเพื่อความมั่นคงของกระทรวงกลาโหม. สรุปผลการดำเนินงานประจำปีเรื่อง แนวคิดในการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหม.2559

[12] ศิวลีย์ สิริโรจน์บริรักษ์ , การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CYBER SECURITY) ของกระทรวงกลาโหม ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก http://www.tci-thaijo.org/index.php/ndsijournal/article/view/39369

[13] พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ; เข้าถึงเมื่อ 18 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://ictlawcenter.etda.or.th

[14] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์.มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 ; เข้าถึงเมื่อ 19 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://ictlawcenter.etda.or.th

[15] ศิวลีย์ สิริโรจน์บริรักษ์ , การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CYBER SECURITY) ของกระทรวงกลาโหม ; เข้าถึงเมื่อ 10 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก http://www.tci-thaijo.org/index.php/ndsijournal/article/view/39369

[16] กองทัพบกกับความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ ; เข้าถึงเมื่อ 19 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก http://www.kpjhospital.com/images/ PDF_File/km/km1/km11.pdf

[17] ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ;เข้าถึงเมื่อ 19 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-cyber-security-protection-act

[18] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ;เข้าถึงเมื่อ 20 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://ictlawcenter .etda.or.th/laws -2560

[19] Wikipedia . สงครามไซเบอร์ ; เข้าถึงเมื่อ 21 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://th.wikipedia.org/สงครามไซเบอร์

[20] สงครามไซเบอร์. หนังสือพิมพ์ไทยโพสต์ ; เข้าถึงเมื่อ 21 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก http://www.ryt9.com/s/tpd/2577187

[21] รุ่งธรรม บัวแตง , นาวาอากาศเอก. สงครามไซเบอร์คืออะไร ; เข้าถึงเมื่อ 21 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก http://www.dstd.mi.th/ กรมวิทยาศาสตร์และเทคโนโลยีกลาโหม

[22] เพนตากอนยกระดับ “สงครามไซเบอร์” โจมตีเครือข่ายคอมพิวเตอร์ของ IS. หนังสือพิมพ์ผู้จัดการ ; เข้าถึงเมื่อ 21 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก http://www.manager.co.th/Sport/ViewNews.aspx?NewsID=9590000021811

[23] ศูนย์บัญชาการกองกำลังทางไซเบอร์เกาหลีใต้ถูกแฮกเซิร์ฟเวอร์ที่ใช้ตรวจจับการโจมตี. ข่าวสั้น ไทยเซิร์ต ; เข้าถึงเมื่อ 22 กุมภาพันธ์ 2560 ; เข้าถึงได้จาก https://www.thaicert.or.th/newsbite/2016-10-04-01.html

[24] ชัยยศ ลิลิตวงษ์ , พลตรี. การเสริมสร้างศักยภาพไซเบอร์ ในระดับกระทรวงกลาโหม [เอกสารวิจัยส่วนบุคคล]. กรุงเทพฯ: วิทยาลัยการทัพเรือ; 2557

[25] หนังสือ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ด่วนมาก ที่ กห 0217/850 ลงวันที่ 6 มิถุนายน 2556 เรื่อง การหารือเตรียมการประชุมคณะกรรมการ ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีนายกรัฐมนตรีเป็นประธาน (ผนวก ค)

[26] ชัยยศ ลิลิตวงษ์ , พลตรี. การเสริมสร้างศักยภาพไซเบอร์ ในระดับกระทรวงกลาโหม [เอกสารวิจัยส่วนบุคคล]. กรุงเทพฯ: วิทยาลัยการทัพเรือ; 2557

[27] คำสั่งคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารกระทรวงกลาโหม(เฉพาะ) ที่ 10/60 ลงวันที่ 9 กุมภาพันธ์ 2560 เรื่อง แต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม

[28] ตามหนังสือ สำนักงานปลัดกระทรวงกลาโหม ที่ ต่อ กห 0217/945 ลง 9 กรกฎาคม 2556 เรื่อง สรุปสาระสำคัญการประชุมคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee) ครั้งที่ 1/2556 ที่มีนายกรัฐมนตรีเป็นประธาน (ผนวก ข)

[29] ชัยยศ ลิลิตวงษ์ , พลตรี. การเสริมสร้างศักยภาพไซเบอร์ ในระดับกระทรวงกลาโหม [เอกสารวิจัยส่วนบุคคล]. กรุงเทพฯ: วิทยาลัยการทัพเรือ; 2557

ประวัติย่อผู้วิจัย

ยศ ชื่อ พันเอก ชนกศ์ จรจำรัส

วัน เดือน ปี เกิด 16 มีนาคม 2513

ประวัติสำเร็จการศึกษา

พ.ศ.2537	วิทยาศาสตรบัณฑิต โรงเรียนนายร้อยพระจุลจอมเกล้า
พ.ศ.2544	วิศวกรรมศาสตรมหาบัณฑิต มหาวิทยาลัยเกษตรศาสตร์

ประวัติการทำงาน

พ.ศ.2544	หัวหน้าหมวดซ่อมเรดาร์ กองซ่อมเครื่องสื่อสารและอิเล็กทรอนิกส์
พ.ศ.2548	อาจารย์ส่วนวิชาทหาร โรงเรียนนายร้อยพระจุลจอมเกล้า
พ.ศ.2552	หัวหน้าแผนกแผนและโครงการ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม
พ.ศ.2556	รองผู้อำนวยการ กองแผนและวิศวกรรม กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม
พ.ศ.2557	รองผู้อำนวยการ กองการสื่อสาร กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม
พ.ศ.2558	หัวหน้าส่วนกิจการวิทยุกระจายเสียง สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมกระทรวงกลาโหม

ตำแหน่งปัจจุบัน

พ.ศ.2559 – 2560	ที่ปรึกษาทางเทคนิค กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม