แนวทางการปกป้องหน่วยงานโครงสร้างพื้นฐานสำคัญของชาติ
Guidelines for Protecting National Critical Infrastructure

บทความวิชาการ

จารุกฤษณ์ เรืองสุวรรณ[1] และ วรวรรณ ศรีศักดิ์[2]
Charukris Ruangsuwan and Worawan Srisak
โรงเรียนเสนาธิการทหารบก กรุงเทพฯ ประเทศไทย 10300[1]
Command and General Staff College, Bangkok, Thailand 10300
มหาวิทยาลัยรามคำแหง กรุงเทพ ประเทศไทย 10240[2]
Ramkhamhaeng University, Bangkok, Thailand 10240
E-mail: charukrisr@gmail.com[1] and worawansrisak@gmail.com[2]

บทคัดย่อ

การระบุหน่วยงานให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญนั้น เกิดขึ้นเพื่อเป็นมาตรการในการรับมือกับเหตุการณ์การก่อการร้ายและภัยคุกคามที่เปลี่ยนแปลง ไม่ว่าจะเป็นการป้องกัน เฝ้าระวัง ลดความเสี่ยง ลดความเสียหาย และช่วยเหลือในการกู้คืนจากการโจมตี สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น จะต้องมีการดำเนินการในการปกป้องควบคู่กันและไม่สามารถแบ่งแยกได้ การดำเนินการที่เริ่มจากการที่มีกฎหมายและหน่วยงานรับผิดชอบ การแบ่งมอบ Sectors และกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญ เพื่อให้เกิดการควบคุมและกำกับดูแล หลังจากนั้นจะเป็นกระบวนการในการปกป้องหน่วยงานโครงสร้างพื้นฐานสำคัญจะประกอบไปด้วย 5 ขั้นตอน ได้แก่ การระบุสินทรัพย์ในหน่วยงานโครงสร้างพื้นฐานสำคัญ การระบุความเสี่ยงและประเมินช่องโหว่ การทำให้เป็นมาตรฐาน วิเคราะห์ และจัดลำดับความสำคัญ การดำเนินการป้องกัน และการประเมินเพื่อวัดประสิทธิภาพ โดยหน่วยงานที่ถูกกำหนดให้เป็นโครงสร้างพื้นฐานสำคัญ จำเป็นต้องมีการดำเนินการในเรื่องของการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับมาตรฐานสากล เพื่อให้เกิดความปลอดภัยทันต่อสถานการณ์ทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว และพร้อมรับมือภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นในอนาคตได้อย่างมีประสิทธิภาพ

วันที่รับบทความ : 21 มี.ค. 67 วันที่แก้ไขบทความ : 23 พ.ค. 67 วันที่ตอบรับบทความ : 4 มิ.ย. 67

คำสำคัญ : หน่วยงานโครงสร้างพื้นฐานสำคัญ, ความมั่นคงปลอดภัยไซเบอร์, กระบวนการปกป้องหน่วยงานโครงสร้างพื้นฐานสำคัญ

Abstract

The identification of key infrastructure units as critical infrastructure agencies is established as a measure to deal with evolving threats and hazards, whether in preventing attacks, reducing risks, minimizing damage, or aiding in recovery. For both critical infrastructure and critical information infrastructure agencies, operations must be integrated and inseparable, starting from legal frameworks and responsible agencies, sectoral division, and designation of critical infrastructure agencies for control and oversight. Subsequently, the process involves five steps: identifying assets within critical infrastructure units, Risk identifying and assessing vulnerabilities, standardization, analysis, and prioritization, prevention operations, and performance evaluation. It is imperative that agencies designated as critical infrastructure must ensure that their cybersecurity measures align with international standards to effectively respond to rapidly changing cyber threats and be prepared to efficiently address future cyber threats.

Keywords: Critical Infrastructure, Cybersecurity, Critical Infrastructure Protection Process

บทนำ

"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing." - Frederick the Great, 1740-1786 (Quote Fancy, 2024)

การทำสงครามตั้งแต่ในอดีตนั้นไม่ได้มีการกำหนดกฎเกณฑ์หรือมีกติกาที่ตายตัว ทุกฝ่ายล้วนแต่ต้องการหาจุดอ่อน เพื่อบรรลุเป้าหมายในการเอาชนะของฝ่ายตรงข้าม ยกตัวอย่างเช่น ในสมัยกรีกโบราณ Lysander หนึ่งในหัวหน้านักรบของสปาร์ตาได้ทำการโจมตีโดยยึด Hellespont ที่เป็นแหล่งธัญพืชหลักสำหรับส่งเข้าสู่เมืองเอเธนส์ เป็นการวางกลยุทธ์เพื่อทำให้ชาวเมืองเอเธนส์ขาดแคลนอาหารและยอมจำนนต่อสปาร์ตา แม้ว่าต่อมาชาวเมืองเอเธนส์ที่อ่อนแอจะพยายามต่อสู้ แต่ต้องพ่ายแพ้อย่างเด็ดขาดในสงคราม Aegospotami หรือแม้กระทั่งในช่วงสงครามโลกครั้งที่ 2 ในปี ค.ศ. 1943 ฝ่ายสัมพันธมิตรได้ออกคำสั่งคาซาบลังกา (Casablanca Directive) ให้ทิ้งระเบิดที่ตำแหน่งทางยุทธศาสตร์ของเยอรมัน ทั้งอุตสาหกรรมป้องกันประเทศ การคมนาคมขนส่ง และโรงกลั่นน้ำมัน เพื่อหยุดยั้งความก้าวหน้าและบั่นทอนขวัญกำลังใจของชาวเยอรมัน จนไปถึงการโจมตีระบบรถไฟของเยอรมนีหลังจากวันดีเดย์ในปี ค.ศ. 1944 ทำให้ระบบการส่งสินค้าชะลอตัวลงและส่งผลให้เศรษฐกิจของเยอรมันเข้าสู่ภาวะล่มสลาย หรือแม้กระทั่งเหตุวินาศกรรม 9/11 ที่อาคารเพนตากอนและอาคารรัฐสภาสหรัฐอเมริกา เป็นเป้าหมายในการโจมตี (Brown, 2006, p.14-16) จากเหตุการณ์ที่ยกตัวอย่างมาจะเห็นได้ว่า ท่ามกลางสงครามหรือความขัดแย้ง หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่มีส่วนขับเคลื่อนประเทศ

มักจะเป็นเป้าหมายของการโจมตีทางทหารอยู่เสมอ โดยเฉพาะอย่างยิ่งในสถานการณ์ปัจจุบันที่มีการพัฒนาทางเทคโนโลยีอย่างรวดเร็ว ทำให้หน่วยงานโครงสร้างพื้นฐานมีการใช้งานระบบเทคโนโลยีสารสนเทศในการควบคุมการดำเนินการและให้บริการประชาชน ส่งผลให้ระบบเหล่านี้ตกเป็นเป้าหมายของการโจมตีทางไซเบอร์จากผู้ไม่หวังดีด้วย จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการศึกษาความเป็นมา ความหมายการกำหนดด้าน (Sectors) และหน่วยงานโครงสร้างพื้นฐานสำคัญ และแนวทางการปกป้องหน่วยงานโครงสร้างพื้นฐานสำคัญ โดยเฉพาะอย่างยิ่งจากการโจมตีทางไซเบอร์ในปัจจุบันทั้งของไทยและต่างประเทศ เพื่อเป็นข้อเสนอแนวทางในการปกป้องโครงสร้างพื้นฐานสำคัญให้เกิดความมั่นคงปลอดภัยต่อไป

ความเป็นมาของหน่วยงานโครงสร้างพื้นฐานสำคัญ

ในกรณีของสหรัฐฯ เมื่อ ค.ศ. 1995 หลังจากเหตุการณ์ระเบิดในโอคลาโฮมาซิตี (Oklahoma City Bombing) ประธานาธิบดี บิล คลินตัน ของสหรัฐฯ ออกคำสั่ง Presidential Decision Directives (PDD) เลขที่ PDD-39 ว่าด้วยการต่อต้านการก่อการร้ายต่อพลเมืองและสมบัติของชาติ (The White House, 1995) และเป็นผลให้ออกคำสั่ง Executive Order เลขที่ EO-13010 เมื่อ 15 กรกฎาคม ค.ศ. 1996 เรื่อง การป้องกันโครงสร้างพื้นฐานที่สำคัญ (The White House, 1996) เหตุผลและความจำเป็นเนื่องจากโครงสร้างพื้นฐานระดับชาติมีความสำคัญมาก หากหยุดดำเนินการหรือถูกทำลายจะส่งผลกระทบต่อความมั่นคงหรือเศรษฐกิจของสหรัฐฯ โดยได้กำหนดภัยคุกคามต่อโครงสร้างพื้นฐานที่สำคัญออกเป็น 2 ประเภท คือ ภัยคุกคามทางกายภาพต่อทรัพย์สินที่จับต้องได้ (Physical Threats) และภัยคุกคามทางอิเล็กทรอนิกส์ คลื่นความถี่วิทยุ หรือการโจมตีทางคอมพิวเตอร์ต่อส่วนประกอบข้อมูลหรือการสื่อสารที่ควบคุมโครงสร้างพื้นฐานที่สำคัญ (Cyber Threats) โครงสร้างพื้นฐานสำคัญเหล่านี้ส่วนใหญ่มีเอกชนเป็นเจ้าของดำเนินการ จึงจำเป็นอย่างยิ่งที่รัฐและเอกชนจะต้องทำงานร่วมกันเพื่อพัฒนากลยุทธ์ในการปกป้องและรับประกันการดำเนินงานอย่างต่อเนื่อง จึงมีคำสั่งให้จัดตั้ง Infrastructure Protection Task Force (IPTF) เพื่อรับมือและแก้ไขปัญหา รวมทั้งแต่งตั้งคณะกรรมการ President's Commission on Critical Infrastructure Protection (PCCIP) โดยมี โรเบิร์ต ทอม มาร์ช (Robert "Tom" Marsh) เป็นประธานและมีผู้เชี่ยวชาญเป็นกรรมาธิการจากหน่วยงาน 5 ด้าน (Sectors) ได้แก่ ด้านสารสนเทศและการสื่อสาร ด้านคมนาคม ด้านพลังงาน ด้านธนาคารและการเงิน และด้านสาธารณสุขและสาธารณูปโภค ทำหน้าที่จัดทำรายงานให้ประธานาธิบดี ในตุลาคม ค.ศ. 1997 PCCIP ได้ออกรายงาน *"Critical Foundations: Protecting America's Infrastructures"* (President's Commission on Critical Infrastructure Protection [PCCIP], 1997) รายงานฉบับนี้ กล่าวถึงความสำคัญของโครงสร้างพื้นฐานสำคัญ แนวโน้มภัยคุกคามที่เกิดขึ้น และการรับผิดชอบร่วมกันระหว่างรัฐและเอกชน เพื่อให้แน่ใจว่าหน่วยงานโครงสร้างพื้นฐานสำคัญมีการดำเนินการประเมินช่องโหว่และความเสี่ยง เพื่อแก้ไขและประกันความปลอดภัยได้ในอนาคต (OODA LLC, n.d.)

ในปี ค.ศ. 1998 ประธานาธิบดีสหรัฐฯ ออกคำสั่งเลขที่ PDD-63 เรื่อง การปกป้องโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Protection) (The White House, 1998) มีการให้ขอบเขตของโครงสร้างพื้นฐานสำคัญ เป็นระบบทางกายภาพและทางไซเบอร์ที่จำเป็นต่อการดำเนินงานขั้นต่ำทางเศรษฐกิจและการบริหารงานของรัฐบาล รวมถึงการให้บริการสำคัญด้านอื่น ๆ ที่กำหนดทั้งของรัฐและเอกชน ในอดีตระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญมีการแยกระบบทางกายภาพ

และทางไซเบอร์โดยมีความเกี่ยวข้องกันเพียงเล็กน้อย แต่จากความก้าวหน้าทางเทคโนโลยีสารสนเทศและความจำเป็นในการปรับปรุงประสิทธิภาพ โครงสร้างพื้นฐานสำคัญเหล่านี้จึงกลายเป็นระบบอัตโนมัติและเชื่อมโยงกันมากขึ้น ก่อให้เกิดช่องโหว่ใหม่ ๆ ทั้งจากความล้มเหลวของอุปกรณ์ ความผิดพลาดของมนุษย์ สภาพอากาศ และภัยพิบัติทางธรรมชาติ รวมไปถึงการโจมตีทางกายภาพและทางไซเบอร์ การจัดการกับช่องโหว่เหล่านี้จำเป็นต้องอาศัยแนวทางที่อ่อนตัวและปรับปรุงให้ทันสมัยตลอดเวลา โดยมีขอบเขตครอบคลุมทั้งรัฐและเอกชน เพื่อปกป้องความมั่นคงทั้งในประเทศและระหว่างประเทศ คำสั่งฉบับนี้กล่าวถึงกลไกในการดำเนินการปกป้องโครงสร้างพื้นฐานสำคัญ การกำหนดลักษณะของหน่วยงานแต่ละประเภท การมอบหน้าที่ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) รับหน้าที่ในการปกป้องโครงสร้างพื้นฐานสำคัญ การวิเคราะห์ช่องโหว่ จัดทำแผนการแก้ไข แจ้งเตือน รับมือ การฟื้นฟู การสร้างความตระหนักรู้ การวิจัยและพัฒนา ข่าวกรอง ความร่วมมือระหว่างประเทศ รวมถึงข้อกำหนดด้านกฎหมายและงบประมาณ

หลังจากเหตุการณ์ 9/11 ในปี ค.ศ. 2001 ภัยคุกคามจากการก่อการร้ายและการพัฒนาของระบบสารสนเทศส่งผลให้รูปแบบการปกป้องโครงสร้างพื้นฐานสำคัญเปลี่ยนไป สหรัฐฯ ได้ออกกฎหมาย The Homeland Security Act of 2002 (2002) จัดตั้งกระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐฯ (Department of Homeland Security: DHS) จากการรวมตัวของหน่วยงานโครงสร้างพื้นฐานสำคัญ เพื่อช่วยป้องกัน การโจมตี ลดความเสี่ยง ลดความเสียหาย และช่วยเหลือในการกู้คืนจากการโจมตีของผู้ก่อการร้าย ด้วยการแบ่งปันข้อมูลระหว่างหน่วยงานตนเองและกับหน่วยงานรัฐบาลกลางอื่น ๆ รัฐบาลของรัฐและท้องถิ่น ภาคเอกชน และอื่น ๆ โดยหนึ่งในภารกิจสำคัญของ DHS คือ การดำเนินการตามแผน National Infrastructure Protection Plan (NIPP) ในปี ค.ศ. 2007 ได้มีการก่อตั้งหน่วยงาน National Protection and Programs Directorate (NPPD) เป็นส่วนหนึ่งของ DHS รับผิดชอบการดำเนินการสร้างความมั่นคงของประเทศด้วยการลดและขจัดภัยคุกคามต่อโครงสร้างพื้นฐานทางกายภาพและทางไซเบอร์ที่สำคัญของสหรัฐฯ ต่อมาในปี ค.ศ. 2018 มีการประกาศกฎหมาย Cybersecurity and Infrastructure Security Agency Act of 2018 NPPD จึงถูกแยกออกมาเป็นหน่วยงานชื่อว่า Cybersecurity and Infrastructure Security Agency (CISA) ทำหน้าที่ช่วยเหลือหน่วยงานรัฐและเอกชนในการแก้ไขปัญหาความปลอดภัยทางไซเบอร์ (Homeland Security, 2018) จนถึงปัจจุบัน

สำหรับประเทศไทย ไม่มีการระบุคำว่า โครงสร้างพื้นฐานสำคัญที่ชัดเจน แต่มีคำใกล้เคียงกำหนดอยู่ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 56 โดยมีการกำหนดคำว่า *“สาธารณูปโภคขั้นพื้นฐาน”* ในทางความมั่นคงจะมีกำหนดในหน่วยงานที่มีความสำคัญตามแผนการเตรียมพร้อมแห่งชาติแผนบริหารวิกฤตการณ์ (กระทรวงกลาโหมและสำนักงานสภาความมั่นคงแห่งชาติ, 2559) และในทางเศรษฐกิจจะมีการกำหนดหน่วยงานในพระราชบัญญัติ การร่วมลงทุนระหว่างรัฐและเอกชน พ.ศ. 2562 แต่ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562 มีการระบุคำว่า *“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ”* และระบุให้หน่วยงานที่มีลักษณะดังกล่าวต้องมีการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ ต่อระบบโครงสร้างสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานกำกับดูแลตามกฎหมายฉบับนี้ (พิธุวรรณ กิติคุณ, 2558)

จะเห็นได้ว่า ในกรณีของสหรัฐฯ จุดเริ่มต้นของการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญเกิดจากเหตุการณ์การก่อการร้ายและภัยคุกคามที่เปลี่ยนแปลงไปที่กระทำต่อหน่วยงานโครงสร้างพื้นฐานสำคัญและกระทบต่อความมั่นคงของชาติ ทำให้สหรัฐฯ ต้องมีการออกคำสั่งจัดตั้งคณะทำงานเพื่อกำหนดประเภทหน่วยงาน แนวทางในการปกป้องหน่วยงานจัดตั้งหน่วยงานรับผิดชอบ ทีมแก้ไขปัญหา รวมถึงผู้รับผิดชอบในแต่ละหน่วยงานในการป้องกัน ลดความเสี่ยง ลดความเสียหายและช่วยเหลือในการกู้คืนจากการโจมตี แต่ของไทยเกิดจากภัยคุกคามทางไซเบอร์และกฎหมายที่ให้กำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศขึ้น

ความหมายของโครงสร้างพื้นฐานสำคัญและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

สำหรับความหมายของโครงสร้างพื้นฐานสำคัญและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แต่ละประเทศได้ให้ความหมายที่แตกต่างกันไป โดย Organization for Economic Co-operation and Development (OECD) ของสหภาพยุโรป ได้ทำการเปรียบเทียบความหมายในแต่ละประเทศไว้ดังนี้

ตารางที่ 1 ความหมายของโครงสร้างพื้นฐานสำคัญ

ประเทศ	ความหมายของ Critical Infrastructure (CI)
สหรัฐอเมริกา	ระบบและทรัพย์สิน ไม่ว่าจะเป็นทางกายภาพหรือเสมือน ซึ่งมีความสำคัญอย่างยิ่งต่อสหรัฐฯ หากถูกทำให้ไร้ความสามารถหรือถูกทำลายระบบและทรัพย์สินดังกล่าว จะมีผลกระทบต่อความมั่นคง ความมั่นคงทางเศรษฐกิจของประเทศ สาธารณสุขหรือความปลอดภัยของประเทศ หรือเรื่องใด ๆ รวมกัน
ออสเตรเลีย	สิ่งอำนวยความสะดวกทางกายภาพ ห่วงโซ่อุปทาน เทคโนโลยีสารสนเทศ และเครือข่ายการสื่อสาร ซึ่งหากถูกทำลาย ลดระดับ หรือไม่สามารถใช้งานได้เป็นระยะเวลานาน อาจส่งผลกระทบอย่างมีนัยสำคัญต่อความเป็นอยู่ทางสังคมหรือเศรษฐกิจของประเทศ หรือส่งผลกระทบต่อออสเตรเลีย ความสามารถในการป้องกันประเทศและประกันความมั่นคงของชาติ
สหภาพยุโรป	ทรัพย์สิน ระบบ หรือส่วนหนึ่งส่วนใดของระบบที่ตั้งอยู่ในรัฐสมาชิกที่จำเป็นต่อการบำรุงรักษาเพื่อให้บริการสำคัญแก่สังคม สุขภาพ ความปลอดภัย ความมั่นคง ความอยู่ดีมีสุขทางเศรษฐกิจหรือสังคมของประชาชน และการหยุดชะงักหรือการทำลายล้างอาจส่งผลกระทบสำคัญต่อประเทศสมาชิกอันเป็นผลมาจากความล้มเหลวในการรักษาหน้าที่เหล่านั้น

ที่มา : Organization for Economic Co-operation and Development [OECD], 2008, p.4

ตารางที่ 2 ความหมายของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ประเทศ	ความหมายของ Critical Information Infrastructure (CII)
สิงคโปร์	ระบบคอมพิวเตอร์ที่เกี่ยวข้องโดยตรงในการให้บริการที่จำเป็น การโจมตีทางไซเบอร์ต่อ CII อาจส่งผลกระทบต่อเศรษฐกิจและสังคม
ไทย	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

ที่มา : 1. Cyber Security Agency of Singapore, 2018

2. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2562, เล่ม 136

จากตารางที่ 1 และตารางที่ 2 จะเห็นได้ว่าทั้ง 2 คำ คือ โครงสร้างพื้นฐานสำคัญ (CI) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) มีส่วนที่เหมือนกัน คือ ระบบหรือทรัพย์สินหากถูกทำลายจะมีผลกระทบต่อความมั่นคงของประเทศ เมื่อพิจารณาในส่วนที่แตกต่างในส่วนของโครงสร้างพื้นฐานสำคัญ จะหมายรวมถึงระบบและทรัพย์สินทั้งทางกายภาพและเสมือน และถูกทำลายด้วยวิธีการใด ๆ ในขณะที่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะเน้นไปที่ระบบและทรัพย์สินทางสารสนเทศและเน้นที่การโจมตีทางไซเบอร์เป็นหลัก ซึ่งอาจกล่าวได้ว่าโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นส่วนหนึ่งของโครงสร้างพื้นฐานสำคัญ แต่อย่างไรก็ตาม Centre for European Policy Studies (CEPS) ให้ความเห็นว่าปัจจุบันความเสียหายทางกายภาพสามารถกระทำได้ผ่านการโจมตีทางไซเบอร์ แต่ในขณะเดียวกันหน่วยงานโครงสร้างพื้นฐานส่วนใหญ่ยังมุ่งเน้นในการปกป้องทางกายภาพมากกว่าการปกป้องทางไซเบอร์ แนวโน้มในอนาคตหากโครงสร้างพื้นฐานสำคัญพึ่งพาระบบสารสนเทศในการดำเนินการ เช่น ระบบเครือข่าย ระบบคลาวด์ หรือแม้กระทั่ง ระบบ SCADA จะส่งผลทำให้การปกป้องโครงสร้างพื้นฐานสำคัญและโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีการดำเนินการควบคู่กัน (Centre for European Policy Studies [CEPS], 2010, p.23-28) รวมทั้ง แนวโน้มที่โครงสร้างพื้นฐานสำคัญของประเทศส่วนใหญ่จะมีลักษณะเดียวกันกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และอาจกลายเป็นจุดศูนย์ดุลแห่งสงครามการก่อการร้ายในอนาคตด้วย (ปิยะ ศรีพลอย, 2565, p.87-97) อย่างไรก็ตาม ในแต่ละประเทศจะมีการกำหนดคำและแนวทางที่แตกต่างกันตามบริบทและตามอำนาจทางกฎหมายที่บังคับใช้กับหน่วยงานโครงสร้างพื้นฐานสำคัญ

การกำหนดด้าน (Sectors) และกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญ

แต่ละประเทศจะมีแนวทางในการแบ่งด้าน (Sectors) ของโครงสร้างพื้นฐานสำคัญและโครงสร้างพื้นฐานสำคัญทางสารสนเทศแตกต่างกัน สหรัฐฯ กำหนด Sectors ตามเอกสารที่มีชื่อว่า Homeland Security Presidential Directive (HSPD) ฉบับที่ HSPD-7 (The White House, 2003, p.36) ครั้งแรก สหรัฐฯ แบ่ง Sectors ออกตามหน่วยงานภาครัฐที่เป็นเจ้าภาพ

ใน Sectors ที่รับผิดชอบ แต่ต่อมา มีการยกเลิกและมีการแบ่งหน่วยงานตามคำสั่งเลขที่ PPD-21 (The White House, 2013, p.10-11) แบ่งออกเป็น 16 Sectors ตามภารกิจหลักที่กำหนด ในขณะที่แนวคิดของออสเตรเลีย สหภาพยุโรป และสิงคโปร์ มีการแบ่งตามภารกิจหลักเป็น 11 Sectors และประเทศไทยแบ่งภารกิจหลักเป็น 7 Sectors และด้านอื่น ๆ รวม 8 Sectors มีรายละเอียดตามตารางที่ 3

ตารางที่ 3 เปรียบเทียบ Sector ของหน่วยงานโครงสร้างพื้นฐานสำคัญของไทยและต่างประเทศ

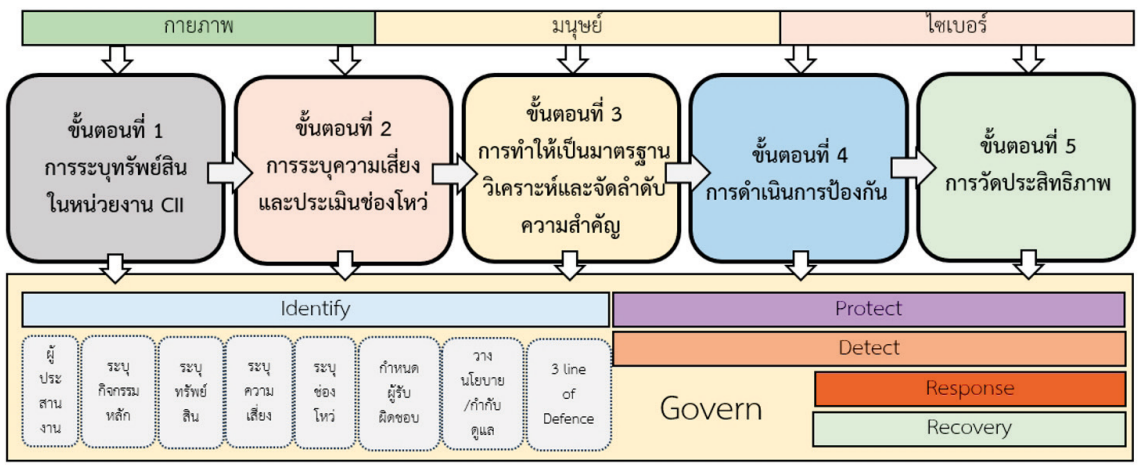
Sectors/ประเทศ	สหรัฐฯ	ออสเตรเลีย	สหภาพยุโรป	สิงคโปร์	ไทย
พลังงาน	●	●	●	●	●
การเงิน	●	●	●	●	●
สาธารณสุข	●	●	●	●	●
ขนส่งและคมนาคม	●	●	●	● (บก)	●
โทรคมนาคม	●	●	●	●	●
เทคโนโลยีสารสนเทศ	●	●			
น้ำและระบบบำบัด	●	●	●	●	-
อาหารและเกษตร	●	●	●	-	-
บริการภาครัฐ	●	-	-	●	●
บริการฉุกเฉิน	●	-	-	●	-
ความมั่นคง					●
อื่น ๆ	- อุตสาหกรรมป้องกันประเทศ - เคมีภัณฑ์ - สิ่งอำนวยความสะดวก - การผลิตที่สำคัญ - เขื่อน - นิวเคลียร์	- อุตสาหกรรมป้องกันประเทศ - ศึกษา/วิจัย - อวกาศ	- เคมีภัณฑ์ - นิวเคลียร์ - อวกาศ - สื่อ	- ขนส่งทางน้ำ - ขนส่งทางอากาศ - สื่อ	- อื่น ๆ
รวม (Sectors)	16	11	11	11	7

ที่มา : 1. The White House, 2013
2. Australia Government, 2018
3. European Commission, 2006
4. Cyber Security Agency of Singapore, 2018
5. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2562, เล่ม 136

ในกรณีของประเทศไทยจากข้อมูลในตารางหน่วยงานอื่น ๆ ที่ไม่อยู่ภายใต้ 7 Sectors อาจถูกแบ่งตามความเหมาะสม เช่น หน่วยงานด้านน้ำจะอยู่ในด้านพลังงาน บางภารกิจอาจอยู่ในความควบคุมของหน่วยงานความมั่นคง และภารกิจอื่น ๆ อาจพิจารณาเพิ่มเติม เป็นด้านใหม่ในอนาคต สำหรับขั้นตอนการกำหนดหน่วยงาน หน่วยงานสำคัญใน 7 Sectors จะถูกมอบหมายให้เป็นหน่วยงานควบคุมหรือกำกับดูแล (Regulator) มีหน้าที่กำหนดให้หน่วยงานภายใต้กำกับตามภารกิจของตนเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับดูแล โดยแนวทางการพิจารณามี 5 ขั้นตอน ได้แก่ การระบุกระบวนการที่สำคัญ (Determine Critical Processes/Services) การพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการที่สำคัญ (Identify Outage Impacts) การประเมินเวลาการหยุดชะงักที่ยอมรับได้ (Estimated Downtime) เลือกกระบวนการที่สำคัญและการระบุทรัพย์สินสารสนเทศ (System Resource/Component) และการระบุหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Determine Critical Infrastructure) หลังจากที่ถูกกำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแล้ว จะมีการส่งข้อมูลกระบวนการที่สำคัญกำหนดผู้ประสานงาน และดำเนินการตามมาตรฐานที่เกี่ยวข้องต่อไป

แนวทางการปกป้องหน่วยงานโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Protection Process: CIPP)

สำหรับ CIPP เป็นแนวคิดที่เกี่ยวข้องกับการเตรียมพร้อมและการตอบสนองต่อเหตุการณ์ร้ายแรงที่เกี่ยวข้องกับโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยอ้างอิงจากแนวทางตามคำสั่ง PDD-63 ของสหรัฐฯ ซึ่งเมื่อทำการเปรียบเทียบกับข้อกำหนดตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานของไทยที่ สกมช. กำหนด (ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564, 2564, เล่ม 138) และสอดคล้องกับมาตรฐานสากล NIST CSF มีกระบวนการดำเนินการสรุปได้ 5 ขั้นตอน ดังนี้



ภาพ Critical Infrastructure Protection Process

ที่มา : ปรับปรุงจาก Wade, 2016, p.5-9

ขั้นตอนที่ 1 การระบุสินทรัพย์ในหน่วยงานโครงสร้างพื้นฐานสำคัญ คือ การระบุทรัพย์สินที่สำคัญที่อยู่ในขอบเขตความรับผิดชอบของหน่วยงาน เริ่มต้นจากการทบทวนภารกิจ จัดลำดับความสำคัญ ภารกิจและข้อจำกัดของหน่วยเหนือ วิเคราะห์ทรัพย์สินที่มีความสำคัญยิ่งต่อการบรรลุภารกิจ เมื่อเปรียบเทียบกับของไทย คือ การวิเคราะห์ผลกระทบทางธุรกิจ และการจัดการทรัพย์สิน

ขั้นตอนที่ 2 ระบุความเสี่ยงและประเมินช่องโหว่ ดำเนินการกับรายการทรัพย์สินที่ระบุไว้ในขั้นตอนที่ 1 จำเป็นต้องระบุความเสี่ยง จุดอ่อนและช่องโหว่ที่เป็นไปได้ ตลอดจน มาตรการป้องกันที่จำเป็นเพื่อบรรเทาช่องโหว่ การระบุความต้องการสนับสนุนที่จำเป็น และการประเมินช่องโหว่ เมื่อเปรียบเทียบกับของไทย คือ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง และการประเมินช่องโหว่และการทดสอบเจาะระบบ

ขั้นตอนที่ 3 การทำให้เป็นมาตรฐาน วิเคราะห์และจัดลำดับความสำคัญ ทำการรวบรวมผลการประเมินความเสี่ยงและช่องโหว่ โดยจัดเรียงให้เป็นมาตรฐาน จัดลำดับความสำคัญกับสินทรัพย์ทั้งหมดที่หน่วยงานรับผิดชอบ เพื่อที่จะระบุว่า ทรัพย์สินใดมีความเสี่ยงมากที่สุดและได้รับประโยชน์สูงสุดจากมาตรการป้องกัน เมื่อเปรียบเทียบกับของไทย คือ การจัดการความเสี่ยง

ขั้นตอนที่ 4 การดำเนินการป้องกัน ข้อมูลที่รวบรวมระหว่างกระบวนการจะช่วยในการพัฒนาและดำเนินการตามแผนเพื่อกำหนดผู้รับผิดชอบ วางนโยบาย กำกับดูแล เพื่อป้องกันหรือลดความเสียหายให้กับโครงสร้างพื้นฐาน และสามารถประสานงานกับหน่วยงานที่ให้ความช่วยเหลือได้ เมื่อเปรียบเทียบกับของไทย คือ การจัดการผู้ให้บริการภายนอก การควบคุมการเข้าถึง การทำให้ระบบมีความแข็งแกร่ง การควบคุมการเชื่อมต่อระยะไกล การควบคุมสื่อเก็บข้อมูลแบบถอดได้ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ และนโยบายและแผนการรับมือภัยคุกคามทางไซเบอร์

ขั้นตอนที่ 5 วัดประสิทธิภาพ คือ การกำหนดตัวชี้วัดสำหรับมาตรการป้องกันแต่ละอย่างเพื่อให้แน่ใจว่ามีการดำเนินการอย่างสม่ำเสมอ ยั่งยืน และมีประสิทธิภาพ การทบทวนตัวชี้วัดอย่างต่อเนื่องจะส่งผลให้เกิดการปรับปรุงกรอบการทำงานและแผนการป้องกัน เมื่อเปรียบเทียบกับของไทย คือ การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ การแบ่งปันข้อมูล การฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์ การฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ และการฝึกซ้อมการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

สรุปผลการศึกษา

จากแนวคิดเริ่มต้นของการดำเนินการที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญของสหรัฐฯ ในการรับมือกับเหตุการณ์การก่อการร้ายและภัยคุกคามที่เปลี่ยนแปลง จนนำไปสู่แนวทางในการปกป้องโครงสร้างพื้นฐานสำคัญด้วยการออกกฎหมาย การจัดตั้งหน่วยงานรับผิดชอบในการป้องกันการโจมตี ลดความเสี่ยง ลดความเสียหาย และช่วยเหลือในการกู้คืนจากการโจมตีต่อหน่วยงานโครงสร้างพื้นฐานสำคัญ โดยขอบเขตความหมายของโครงสร้างพื้นฐานสำคัญ หมายถึง ระบบหรือทรัพย์สิน หากถูกทำลายจะมีผลกระทบต่อความมั่นคงของประเทศ ในขณะที่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งเป็นส่วนย่อยของโครงสร้างพื้นฐานสำคัญ หมายถึง ระบบและทรัพย์สินทางสารสนเทศ และเน้นที่การโจมตีทางไซเบอร์เป็นหลัก การกำหนดความหมายและหน่วยงานจะมีความแตกต่างตามบริบทและกฎหมายแต่ละประเทศ อย่างไรก็ตาม การดำเนินการในปัจจุบันมีแนวโน้มที่โครงสร้างพื้นฐานสำคัญและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะต้องมีการดำเนินการปกป้องควบคู่กันอย่างไม่สามารถแบ่งแยกได้ การดำเนินการที่สำคัญต้อง

เริ่มจากการมีกฎหมายและหน่วยงานรับผิดชอบ การแบ่งมอบ Sectors และกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญ เพื่อให้เกิดการควบคุมและกำกับดูแล หลังจากนั้นจะเป็นแนวทางในการปกป้องหน่วยงานโครงสร้างพื้นฐานสำคัญ จะประกอบไปด้วย 5 ขั้นตอน ได้แก่ การระบุสินทรัพย์ในหน่วยงานโครงสร้างพื้นฐานสำคัญ การระบุความเสี่ยงและประเมินช่องโหว่ การทำให้เป็นมาตรฐาน วิเคราะห์ และจัดลำดับความสำคัญ การดำเนินการป้องกัน และการประเมินเพื่อวัดประสิทธิภาพโดยหน่วยงานที่ถูกกำหนดให้เป็นโครงสร้างพื้นฐานสำคัญจำเป็นต้องมีการดำเนินการในเรื่องของการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับมาตรฐานสากล เพื่อให้เกิดความปลอดภัยทันต่อสถานการณ์ทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว และพร้อมรับมือภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นในอนาคตได้อย่างมีประสิทธิภาพ เพื่อให้เกิดความความมั่นคง เสถียรภาพทางเศรษฐกิจ และปกป้องการดำเนินการวิถีชีวิตของประชาชนในชาติให้สามารถดำเนินกิจกรรมอย่างเป็นปกติต่อไป

เอกสารอ้างอิง

กระทรวงกลาโหมและสำนักงานสภาความมั่นคงแห่งชาติ. (2559). *แผนผนึกกำลังและทรัพยากรในการป้องกันประเทศ.* นนทบุรี: กรมสรรพกำลังกลาโหม กระทรวงกลาโหม.

ปิยะ ศรีพลอย. (2565). การก่อการร้าย : ภัยคุกคามต่อโครงสร้างพื้นฐานที่สำคัญ. *วารสารรัฐฐาภิรักษ์. 64*(3), 87-97.

“ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564” (2564, 6 กันยายน). *ราชกิจจานุเบกษา*. เล่ม 138 ตอนพิเศษ 208 ง. หน้า 9-15.

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562” (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา.* เล่ม 136 ตอนที่ 69 ก. หน้า 21.

พิธุวรรณ กิติคุณ. (2558). *การจัดทำโครงสร้างพื้นฐานและบริการสาธารณะตามพระราชบัญญัติการร่วมลงทุนระหว่างรัฐและเอกชน พ.ศ. 2562.* Retrieved March, 15 2024 from https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=57152&filename=house2558

Australia Government. (2018). *Security of Critical Infrastructure Act 2018 (SOCI).* Retrieved March, 15 2024 from https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018

Brown, K. A. (2006). *Critical Path : a brief history of critical infrastructure protection in the United States.* Virginia: Spectrum Publishing Group.

Centre for European Policy Studies. (2010). *Protecting Critical Infrastructure in the EU.* Retrieved March, 15 2024 from https://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf

Cyber Security Agency of Singapore. (2018). *Cybersecurity Act.* Retrieved March, 15 2024 from http://www.csa.gov.sg/legislation/Cybersecurity-Act

European Commission. (2006). *The European Programme for Critical Infrastructure Protection (EPCIP).* Retrieved March, 15 2024 from https://ec.europa.eu/commission/presscorner/detail/en/MEMO_06_477

Homeland Security. (2018). *Congress Passes Legislation Standing Up Cybersecurity Agency in DHS.* Retrieved March, 15 2024 from https://www.dhs.gov/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs

Homeland Security Act of 2002. (2002, 25 November). Public Law 296 U.S. Stat. 116. §§ 2135-2321. Retrieved from https://www.dhs.gov/sites/default/files/2023-11/03_0116_hr_5005_enr.pdf

OODA LLC. (n.d.). *PCCIP History and Background.* Retrieved March, 15 2024 from https://www.oodaloop.com/documents/Legacy/pccip/PCCIP_index.htm

Organization for Economic Co-operation and Development. (2008). *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security.* Retrieved March, 15 2024 from https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations Protecting America's Infrastructures.* Retrieved March, 15 2024 from https://apps.dtic.mil/sti/citations/tr/ADA331523

Quote Fancy. (2024). *Top 50 Frederick the Great Quotes.* Retrieved March, 15 2024 from https://quotefancy.com/frederick-the-great-quotes

The White House. (1995). *U.S. Policy on Counterterrorism.* Retrieved March, 15 2024 from https://irp.fas.org/offdocs/pdd39.htm

_____. (1996). *Executive Order EO-13010 Critical Infrastructure Protection.* Retrieved March, 15 2024 from https://irp.fas.org/offdocs/eo13010.htm

_____. (1998). *Critical Infrastructure Protection.* Retrieved March, 15 2024 from https://irp.fas.org/offdocs/pdd/pdd-63.htm

_____. (2003). *Homeland Security Presidential Directive-7 Critical Infrastructure Identification, Prioritization, and Protection.* Retrieved March, 15 2024 from https://irp.fas.org/offdocs/nspd/hspd-7.html

_____. (2013). *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience (PPD-21).* Retrieved March, 15 2024 from https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

Wade, M.N. (2016). *Counter terrorism, WMD & Hybrid Threat SMARTbook.* Florida: The Lightning Press.