บทความวิชาการ

การก่อการร้าย: ภัยคุกคามต่อโครงสร้างพื้นฐานที่สำคัญ

Terrorism Threat to Critical Infrastructure

พลตรี ปิยะ ศรีพลอย

กรมข่าวทหาร

127 กองบัญชาการกองทัพไทยซอย แจ้งวัฒนะ 7 ถนนแจ้งวัฒนะ

แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

Maj.Gen.Piya Sriploy

Directorate of Joint Intelligence

127 Thai Army Headquarters SoiChaengwattana 7, Chaengwattana Road

ThungsonghongLaksi, Bangkok 10210

E-mail: piya.s@rtarf.mi.th

วันที่รับบทความ : 10 ตุลาคม 2565

วันที่แก้ไขบทความ : 15 พฤศจิกายน 2565

วันที่ตอบรับบทความ : 2 ธันวาคม 2565

บทคัดย่อ

บทความนี้มีจุดประสงค์เพื่อศึกษาโครงการวิจัยทางการทหารภายใต้โครงการ ARPANET (Advanced Research Projects Agency Network) ซึ่งเป็นเครือข่ายสำนักงานโครงการวิจัยชั้นสูงมีวัตถุประสงค์หลัก เพื่อให้คอมพิวเตอร์สามารถเชื่อมต่อและมีปฏิสัมพันธ์เพื่อการสื่อสารและรับส่งข้อมูลด้วยมาตรการรักษาปลอดภัยที่ดีขึ้นโดยการส่งในลักษณะแพ็กเก็ต (TCP/IP Packet Switching: Packet) ระหว่างคอมพิวเตอร์กับตัวแสดงที่มิใช่รัฐ (Non-state Actor) อาทิ กลุ่มก่อการร้ายได้แสวงประโยชน์และเกาะอยู่บนคลื่นของการพัฒนา โดยการนำเทคโนโลยีเหล่านี้มาต่อยอดแนวความคิดเพื่อประยุกต์ใช้ให้เหมาะสมต่อภารกิจขององค์กร และพิสูจน์โครงสร้างพื้นฐานที่สำคัญด้านระบบสารสนเทศ (Critical Information Infrastructure: CII) เมื่อถูกโจมตีจะเกิดวิกฤติทั้งทางกายภาพและจิตวิทยาส่งผลกระทบต่อระบบการดำเนินงานโครงสร้างพื้นฐานที่สำคัญอื่นหรือไม่

จากการวิเคราะห์พบว่านับตั้งแต่สงครามเย็นกลุ่มก่อการร้ายเลือกใช้ สงครามนอกแบบผ่านการโจมตีในรูปแบบของสงครามกองโจร (Guerrilla Warfare) ที่เน้นการโจมตีจุดเปราะบาง (vulnerabilities) ที่มีการป้องกันด้วยประสิทธิภาพไม่สูงนักหรืออ่อนแอง่ายต่อการโจมตีทั้งทางตรงหรือทางอ้อม ขณะที่ กลุ่มก่อการร้าย ISIS กลุ่มก่อการร้าย Hamas และ กลุ่มก่อการร้าย Al Qaeda ยังคงเกาะคลื่นเทคโนโลยีเพื่อสนับสนุนภารกิจและขยายสนามรบเข้าสู่สมรภูมิบนโลกดิจิทัล ในการผลิตโฆษณาชวนเชื่อทั้งสื่อสิ่งพิมพ์และการถ่ายทอดสดรายการโทรทัศน์ผ่าน Internet นอกจากนี้ ยังพบว่า โครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure: CI) ตกเป็นเป้าหมายการโจมตีทางไซเบอร์อย่างต่อเนื่องทั่วโลกและแนวโน้มสถานการณ์ยังคงทวีความรุนแรงขึ้น โดยการโจมตีผ่านตัวแสดงที่หลากหลายแต่หากพิจารณาอย่างละเอียดพบว่าการดำเนินงานของระบบควบคุม CI ทั้งหมดจะต้องผ่านโครงสร้างพื้นฐานที่สำคัญด้านระบบสารสนเทศ (Critical Information Infrastructure: CII) เหตุนี้จึงเป็นเครื่องบ่งชี้ว่า CII คือ จุดศูนย์ดุลแห่งสงครามการก่อการร้ายในยุคดิจิทัลที่หากเพียงแค่ถูกระงับ ขัดขวางเพียงแค่ช่วงเวลาสั้น ๆ จะส่งผลให้ระบบโครงสร้างพื้นฐานที่สำคัญทั้งหมดถูกระงับขัดขวางตามไปด้วย

คำสำคัญ : การขัดขวางการก่อการร้าย, โครงสร้างพื้นฐานสำคัญทางสารสนเทศ, การก่อการร้ายทางไซเบอร์, การเปลี่ยนฉับพลันทางดิจิทัล, จุดอ่อน/จุดเปราะบาง

Abstract

This article is intended to study the military research project under the program Advanced Research Projects Agency Network (ARPANET) which is a network of the higher office of research project with the main purpose of connecting computers together and generate communications as well as sending and receiving information through a secure measure by using the TCP/IP Packet Switching: Packet between computers and Non-state Actor which are namely: terrorist organizations that are using the network signal for their benefits and development.They will incorporate these technologies along with the ideals to be suited for their organization and also to prove Critical Information Infrastructure: CII, when attacked will it cause a physical and psychological crisis, as well as affect other important basic infrastructures also?

After the research it was concluded that since the Cold War, terrorist organizations have chosen unconventional warfare as an attack method along with Guerrilla Warfare that is aimed at attacking vulnerabilities that have a low security protection measures or targets that are vulnerable towards a direct or indirect attack. Terrorist organizations such as ISIS, Hamas and Al Qaeda still continue to uses technology frequencies to support their mission and expand the battlefield into digital domain in producing printed and live broadcast propaganda through the Internet. Moreover, it was determined that Critical Infrastructure: (CI) was a popular target for cyber attacks worldwide and it is projected that the situation will increase in magnitude for the future. Attacks will be carried out through a variety of actors and after careful consideration, all CI are implemented through the Critical Infrastructure: (CII), which is an indication that CII is the Center off gravity for the digital war on terrorism, where if it is seized or temporarily obstructed will have an effect on the functioning of the whole basic infrastructure also.

Keywords: Antiterrorism, Critical Information Infrastructure, Cyber-terrorism, Digital Disruption, Vulnerabilities

บทนำ

จากการศึกษาพบว่านับตั้งแต่ช่วงสงครามเย็น (Cold War 1947-1991) เพื่อนำไปสู่มหาอำนาจทางการทหาร ตัวแสดงที่เป็นรัฐ (State Actor) ได้เร่งเพิ่มศักยภาพในการวิจัยและพัฒนาเทคโนโลยีเพื่อให้มีขีดความสามารถเหนือกว่าฝ่ายตรงข้ามโดยนวัตกรรมที่คิดค้นเป็นไปในลักษณะการเติบโตแบบก้าวกระโดด (Exponential Growth) ซึ่งสิ่งอุปกรณ์เดิมที่ในยุคที่ผ่านมาจะถูกทดแทนด้วยสิ่งอุปกรณ์ใหม่ที่มีประสิทธิภาพและโดยหนึ่งในนวัตกรรมนั้นคือ อินเทอร์เน็ต (ค.ศ. 1969/พ.ศ. 2512) ที่กระทรวงกลาโหมสหรัฐฯ ได้ริเริ่มพัฒนามาจากโครงการวิจัยทางการทหารภายใต้โครงการ ARPANET (Advanced Research Projects Agency Network) ซึ่งเป็นเครือข่ายสำนักงานโครงการวิจัยชั้นสูงซึ่งมีวัตถุประสงค์หลัก เพื่อให้คอมพิวเตอร์สามารถเชื่อมต่อและมีปฏิสัมพันธ์เพื่อการสื่อสารและรับส่งข้อมูลด้วยมาตรการรักษาปลอดภัยที่ดีขึ้น โดยการส่งในลักษณะ แพ็กเก็ต (TCP/IP Packet Switching: Packet) ระหว่างคอมพิวเตอร์กับตัวแสดงที่มิใช่รัฐ (Non-state Actor) อาทิ กลุ่มก่อการร้ายได้แสวงประโยชน์และเกาะอยู่บนคลื่นของการพัฒนา โดยการนำเทคโนโลยีเหล่านี้มาต่อยอดแนวความคิดเพื่อประยุกต์ใช้ให้เหมาะสมต่อภารกิจขององค์กร จากการวิเคราะห์พบว่านับตั้งแต่สงครามเย็นกลุ่มก่อการร้ายเลือกใช้ สงครามนอกแบบผ่านการโจมตีในรูปแบบของสงครามกองโจร (Guerrilla Warfare) ที่เน้นการโจมตีจุดเปราะบาง (Vulnerabilities) ที่มีการป้องกันด้วยประสิทธิภาพไม่สูงนักหรืออ่อนแอง่ายต่อการโจมตีทั้งทางตรงหรือทางอ้อมในลักษณะบรรลุผลลัพธ์ให้แตกหักหรือส่วนที่สำคัญโดยวัตถุประสงค์คือการสร้างความหวาดกลัวในหมู่ประชาชน ทั้งนี้กลุ่มก่อการร้ายชั้นนำ อาทิ กลุ่มก่อการร้าย ISIS, กลุ่มก่อการร้าย Hamas และ กลุ่มก่อการร้าย Al Qaeda ยังคงเกาะคลื่นเทคโนโลยีเพื่อสนับสนุนภารกิจและได้ขยายสนามรบเข้าสู่สมรภูมิบนโลกดิจิทัล โดยมีการใช้ทั้งอำนาจด้านการใช้อำนาจละมุน (Soft PowerPersuasive Power) และการใช้อำนาจแข็ง (Hard Power: Coercive Power) เพื่อใช้ประโยชน์ทั้ง 2 มิติ โดยในช่วงที่ผ่านมาประสบความสำเร็จด้าน Soft Power ที่ได้มีการใช้เทคโนโลยีในการผลิตโฆษณาชวนเชื่อทั้งสื่อสิ่งพิมพ์และการถ่ายทอดสดรายการโทรทัศน์ผ่าน Internet (จุลชีพ 2015, p.50-51, 186-187; Byman, 2015, p.26-27, 57-58, 80, 108; Mazanec& Whyte, 2019, p.70-71, 184-185; Mullins, 2016, p.265-270) แต่ประเด็นที่น่าศึกษาคือการใช้ Hard Power ที่แม้ว่ายังไม่ปรากฏอย่างชัดเจนว่ากลุ่มก่อการร้ายมีขีดความสามารถในการทำสงครามไซเบอร์บนสมรภูมิดิจิทัลแต่นั้นมิได้หมายถึงไม่ได้อยู่ระหว่างสะสมสรรพกำลังเพื่อก่อเหตุบทความนี้จะวิเคราะห์ประเด็นที่สำคัญต่อสงครามต่อต้านการก่อการร้ายในยุคปัจจุบันคือ การก่อการร้ายทางไซเบอร์ที่มุ่งโจมตีต่อโครงสร้างพื้นฐานที่สำคัญเป็นภัยคุกคามความมั่นคงหรือไม่

จากการศึกษาพบว่าโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure: CI) ตกเป็นเป้าหมายการโจมตีทางไซเบอร์อย่างต่อเนื่องทั่วโลกและแนวโน้มสถานการณ์ยังคงทวีความรุนแรงขึ้นโดยการโจมตีผ่านตัวแสดงที่หลากหลายแต่หากพิจารณาอย่างละเอียดพบว่าการดำเนินงานของระบบควบคุม CI ทั้งหมดจะต้องผ่านโครงสร้างพื้นฐานที่สำคัญด้านระบบสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งบทความนี้มุ่งที่จะศึกษาเพื่อพิสูจน์ว่า CII นั้น นับว่าเป็นจุดศูนย์ดุล (Center of Gravity: CG) ที่เมื่อถูกโจมตีจะเกิดวิกฤติทั้งทางกายภาพและจิตวิทยาส่งผลกระทบต่อระบบการดำเนินงานโครงสร้างพื้นฐานที่สำคัญอื่นหรือไม่และภัยคุกคามจากการก่อการร้ายบนสมรภูมิดิจิทัลจะโจมตีด้วยวิธีใดที่สามารถนำไปสู่การหยุด/ระงับขัดขวางการดำเนินงาน (Disruption) เพื่อนำไปสู่การเพิ่มเติมการเตรียมการป้องกันต่อไป

ประเด็นที่ 1: การก่อการร้ายทางไซเบอร์ที่มุ่งโจมตีต่อโครงสร้างพื้นฐานที่สำคัญเป็นภัยคุกคามความมั่นคงหรือไม่

"Terrorism and the threat to Critical Infrastructure"

"I talked about the proposition that certain critical infrastructure should be off-limits to attack, period, by cyber or any other means, of 16 entities — 16 defined as critical infrastructure, from the energy sector to our water systems."

President Biden: Press Conference 17th June 2021 (Phillips, 2021; Walsh, 2021)

เมื่อ 16 มิ.ย. 64 ประธานาธิบดีไบเดน แห่งสหรัฐฯ และประธานาธิบดีปูติน แห่งรัสเซีย ได้จัดการประชุม US-Russia Summit ณ กรุงเจนีวา โดยสามารถสรุปประเด็นที่สำคัญคือ (จากข้อความข้างต้น) การโจมตีด้วยเครื่องมือทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure: CI) นั้นเป็นสิ่งที่ห้ามอย่างเด็ดขาด (off-limits) และการกระทำลักษณะดังกล่าวนับว่ามีความผิดฐานการก่อการร้ายทางไซเบอร์ (Cyber-Terrorism) โดยเป้าหมายที่กล่าวถึงแบ่งออกเป็น 16 ประเภท ประกอบด้วย ระบบเทคโนโลยีสารสนเทศ ระบบการสื่อสาร ระบบการขนส่งและคมนาคม ระบบการเงินการธนาคาร ระบบควบคุมโรงงานอุตสาหกรรม ระบบการบริการด้านสาธารณสุข ระบบการป้องกันประเทศ ระบบควบคุมพลังงาน ระบบฉุกเฉิน ระบบนิวเคลียร์ ระบบเคมี ระบบน้ำประปา ระบบเขื่อน ระบบอาหาร ระบบงานภาครัฐ ระบบควบคุมธุรกรรม (Mazanec& Whyte, 2019, p.118; Phillips, 2021; Walsh, 2021) จากการประชุมครั้งนี้เป็นเครื่องบ่งชี้ว่าภัยคุกคามจากการก่อการร้ายทางไซเบอร์ได้เดินทางมาถึงจุดที่มีความเสี่ยงสูงสุดต่อระดับความมั่นคงของประเทศ (National Security Level) ที่ส่งผลให้ประเทศมหาอำนาจด้านความมั่นคงและด้านเทคโนโลยีต้องหยิบประเด็นมาวางบนโต๊ะเพื่อกำหนดทิศทาง/สร้างความร่วมมือเป็นการจำกัดผลกระทบที่กำลังขยายออกไปอย่างรวดเร็วในฐานะนายทหารฝ่ายข่าว (สธ.2) ซึ่งมีหน้าที่วิเคราะห์แนวคิดเสมือนประหนึ่งว่าตนเองคือข้าศึก (ฝ่ายแดง) โดยหน้าที่จะต้องกำหนดให้ได้ว่าข้าศึกกำหนดเป้าหมายโจมตีที่คุ้มค่าซึ่งต้องเริ่มจากการหาเป้าหมายที่เป็นจุดศูนย์ดุล (Center of Gravity: CG)–ศูนย์รวมของพลังอำนาจโดยหากถูกยึดหรือทำลายจะส่งผลให้ส่งผลกระทบอย่างรุนแรงหรือพ่ายแพ้ทั้งทางกายภาพและด้านจิตวิทยา (รร.เสธ.ทบ., 2013, p.2 จ-1)–แม้ว่า CI ทั้ง 16 ประเภทล้วนมีความสำคัญอย่างมากต่อการดำรงชีวิตในยุคดิจิทัลแต่จากการประเมินพบว่า โครงสร้างพื้นฐานด้านระบบเทคโนโลยีสารสนเทศ (CII) ที่หากถูกโจมตีจะส่งผลกระทบต่อ CI อื่น ๆ ในลักษณะที่ทางรัฐศาสตร์เรียกว่า วิกฤตระลอกคลื่น "Ripple Effect" ซึ่งเป็นปรากฏการณ์ที่เมื่อเกิดผลกระทบจากจุดเล็ก ๆ ผลจากจุดกระทบนั้นจะกลายเป็นคลื่นที่สามารถส่งผลต่อด้านอื่น ๆ ขยายวงกว้างออกไปเรื่อย ๆ

จากคำกล่าวของประธานาธิบดีโจ ไบเดน พอสรุปประเด็นที่ฝ่ายความมั่นคงทั่วโลกจะต้องติดตามและนำไปปรับยุทธศาสตร์ด้านความมั่นคงคือ คำจำกัดความว่าด้วยการก่อการร้ายนั้นได้มีการเปลี่ยนแปลงขึ้นแล้ว โดยตัวแสดง (Actor) ที่มีขีดความสามารถในการโจมตีทางไซเบอร์ต่อ CI ที่ครอบคลุมทุกตัวแสดงทั้งที่เป็นรัฐ (State Actor), ตัวแทนแห่งรัฐ (Proxies), ตัวแสดงที่มิใช่รัฐ (Non-State Actor) นั้นล้วนเป็นผู้ก่อการร้ายทางไซเบอร์ทั้งสิ้น โดยในเอกสารนี้มุ่งเน้นไปการศึกษา Non-State Actor ซึ่งเจาะลึกลงไปที่กลุ่มก่อการร้ายในยุคดิจิทัลโดยจากการศึกษางานวิจัยของ Mockaitis (2008, p.56-57, 96-97) และ Mullins (2016, p.196-197) ต่างเห็นพ้องว่ากลุ่มก่อการร้าย เช่น Al Qaeda และกลุ่มก่อการร้าย ISIS ได้เกาะอยู่บนคลื่นอินเทอร์เน็ตเพื่อแสวงประโยชน์ในการใช้งานเครื่องมือทางไซเบอร์โดยเฉพาะด้าน Soft Power เพื่อใช้ในการปลูกฝังอุดมการณ์รุนแรงแบบสุดโต่ง "Online Jihadist" ซึ่งประสบความสำเร็จอย่างมากในการแสวงหาแนวร่วมจากหลายพื้นที่ที่โลกและประเด็นที่จะส่งผลให้เกิดปัญหาในอนาคตอันใกล้คือการแสวงประโยชน์ด้าน Hard Power เพื่อดำเนินการโจมตี CI ด้วยอาวุธที่ใช้เฉพาะบนดิจิทัลแพลตฟอร์มที่เรียนรู้ได้ง่ายและราคาไม่สูงซึ่งได้แก่มัลแวร์ (Malicious Software: Malware) ซึ่งเป็นอาวุธทางไซเบอร์ที่จะทำการค้นหาจุดอ่อน/จุดเปราะบาง (Vulnerabilities)

เพื่อทำการโจมตีและจะทำการขยายการเจาะต่อไปด้วยระบบอัตโนมัติหรือการสั่งการระบบทางไกลตัวอย่างเหตุการณ์ที่เป็น Ripple Effect คือ Malware Wanna Cry Attack 2017 ที่มีความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติผ่านช่องโหว่ระบบ SMB (Server Message Block) ของ Window ซึ่งการโจมตีจากมัลแวร์นี้ส่งผลกระทบต่อคอมพิวเตอร์ที่อยู่ใน Block-chain เดียวกันมากกว่า 200,000 เครื่อง จาก 112 ประเทศ (Shackelford, 2020, p.100)

สรุป/ข้อเสนอแนะ

จากการประกาศที่ชัดเจนของประธานาธิบดีไบเดนเป็นสิ่งยืนยันได้ว่าการก่อการร้ายทางไซเบอร์ที่มุ่งโจมตีต่อโครงสร้างพื้นฐานที่สำคัญนั้นได้กลายเป็นภัยคุกคามความมั่นคงในยุคดิจิทัลแล้ว ดังนั้นมาตรการ/แนวทางการป้องกันการก่อการร้ายจะต้องมีการเปลี่ยนแปลงที่มุ่งไปสู่การต่อต้านการก่อการร้ายทางไซเบอร์ที่จะต้องเป็นการป้องกันไม่ให้เกิด Ripple Effect โดยในเบื้องต้นจะต้องดำเนินการค้นหาจุดอ่อน/จุดเปราะบาง (Vulnerabilities) เพื่อนำไปสู่การวางยุทธศาสตร์ “การเสริมเกราะป้องกันเป้าหมาย” (Target hardening) ที่มีความสำคัญเป็นอย่างยิ่งซึ่งสงครามต่อต้านการก่อการร้ายในยุคดิจิทัลนั้นการป้องกันทางกายภาพ เช่น การวางกำลังตามจุดที่สำคัญ การตั้งเครื่องตรวจอาวุธตามอาคารที่เป็นอาคารบริวารของโครงสร้างพื้นฐานที่สำคัญนั้นยังคงมีความสำคัญแต่ไม่เพียงพออีกต่อไป โดยแผนการรับมือจะต้องเพิ่มเติมเรื่องการป้องกันระบบ/เครือข่ายคอมพิวเตอร์จากภัยคุกคามทางไซเบอร์ทั้งจากการถูก Hack เพื่อการจารกรรมข้อมูลหรือการปล่อย Malware เพื่อการขัดขวางการดำเนินงานของระบบ/เครือข่ายคอมพิวเตอร์

ประเด็นที่ 2: โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ นั้นนับว่าเป็นจุดศูนย์ดุลหรือไม่

Critical Information Infrastructure (CII) as Center of Gravity (CG)

“Information technology (IT) is central to our Nation’s security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent on IT Sector functions and services as are all other critical infrastructure sectors’ products and services.”

US Department of Homeland Security 2007

“เทคโนโลยีสารสนเทศ (IT) คือจุดศูนย์ดุลของประเทศ (สหรัฐฯ) ทั้งทางด้านเศรษฐกิจ ด้านความมั่นคง ด้านสาธารณสุข โดยโครงสร้างพื้นฐานที่สำคัญทุกภาคส่วนจะต้องเพิ่มการพึงพาระบบ IT เพื่อการดำเนินงานมากยิ่งขึ้น”

(คำแปล: ผู้เขียน)

จากการศึกษาพบว่าประชาคมโลกนั้นได้ตระหนักถึงความสำคัญถึงการก่อการร้ายทางไซเบอร์ที่ได้แสดงขีดความสามารถด้วยโจมตีโครงสร้างพื้นฐานที่สำคัญด้วย Malware ในรูปแบบของซอฟต์แวร์ที่ฝังตัวมากับอุปกรณ์สื่อสารและ/หรือระบบคอมพิวเตอร์ได้หลายเป้าหมายทั่วโลกจึงได้สร้างกรอบความร่วมมือผ่าน คณะมนตรีความมั่นคงแห่งสหประชาชาติ (United Nation Security Council: UNSC) ภายใต้ข้อมติว่าด้วยยุทธศาสตร์ “การต่อต้านการก่อการร้ายระดับโลก” (Global Counter-Terrorism Strategy; 8th September 2006) เพื่อหามาตรการป้องกันและขัดขวาง (Antiterrorism) เพื่อเป็นแนวทางไปสู่การบัญญัติกฎหมาย ข้อบังคับ เพื่อเป็นการบูรณาการด้านการป้องกันรับมือ/ขัดขวางภัยคุกคามจากการก่อการร้ายทางไซเบอร์โดยเมื่อปี 2007 กระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐได้ประกาศอย่างชัดเจนว่าโครงสร้างพื้นฐานที่สำคัญด้านระบบสารสนเทศ (CII) นั้น เปรียบ

เสมือนจุดศูนย์ดุล (CG) ของโครงสร้างพื้นฐานที่สำคัญอื่น ๆ ทั้งด้านความมั่นคง ด้านเศรษฐกิจ ด้านสาธารณสุข เนื่องจาก CI อื่นจะต้องใช้ระบบเทคโนโลยีสารสนเทศที่เปรียบเสมือนแกนกลางในการกระจาย การเก็บ การประสานความสอดคล้องของข้อมูลและระบบงานทั้งหมด ซึ่งอีก 10 ปีถัดมา องค์การตำรวจอาชญากรรมระหว่างประเทศ (International Criminal Police Organization: Interpol) ยังคงยืนยันถึงความสำคัญสูงสุดในการป้องกัน CII เพื่อมิให้ถูกโจมตีซึ่งจะนำไปสู่เกิดเหตุการณ์ Ripple Effect โดย INTERPOL Secretary General Jürgen Stock ได้กล่าวว่า “One (cyber) attack on a single point of failure could disrupt or destroy multiple vital systems in the country directly affected, causing a ripple effect worldwide...” ซึ่งในปีเดียวกัน UNSC ได้ทบทวนหลักการในการเตรียมการป้องกัน/รับมือกับการก่อการร้ายรูปแบบใหม่เพื่อให้สอดคล้องต่อการเปลี่ยนแปลงด้านเทคโนโลยีจึงได้ออกแนวทางปฏิบัติ ผ่าน UNSC ข้อมติ 2341 (2017) (S/RES/2341: 2017) ที่รัฐสมาชิกต่างลงนามโดยเห็นพ้องว่า 1) กลุ่มก่อการร้ายได้พัฒนาขีดความสามารถทางสงครามไซเบอร์เพื่อการระงับขัดขวางการทำงานของระบบควบคุม (disrupt) และการเจาะเพื่อจารกรรมข้อมูลสำคัญขององค์กร (Espionage) โดยเป้าหมายการโจมตีที่เป็นโครงสร้างพื้นฐานที่สำคัญที่ประกอบด้วย โครงสร้างพื้นฐานที่สำคัญด้านระบบสารสนเทศ (CII) โครงสร้างพื้นฐานด้านการขนส่งและโลจิสติกส์ โครงสร้างพื้นฐานด้านการเงินการธนาคาร โครงสร้างพื้นฐานด้านพลังงาน โดยทั้งหมดต้องดำเนินการทำงานด้วยระบบเทคโนโลยีสารสนเทศและอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) ที่จะทำการสื่อสารระหว่างกันแบบอัตโนมัติ 2) การป้องกันกลุ่มก่อการร้ายยุคดิจิทัลต้องเป็นความร่วมมือทั้งภาครัฐและภาคเอกชน เนื่องจากการสื่อสารระหว่างเครื่องจักร/ระบบคอมพิวเตอร์ซึ่งหากมีจุดเปราะบางที่ใดนั้นย่อมหมายถึงสิ่งอุปกรณ์ที่อยู่ในระบบห่วงโซ่จะต้องได้รับผลกระทบต่อความสัมพันธ์ (Node) ของระบบของโครงสร้างพื้นที่สำคัญอื่น ๆ อย่างหลีกเลี่ยงไม่ได้

โดยตัวอย่างเหตุการณ์โจมตีด้วย Malware ที่ส่งผลกระทบต่อ CI ด้วยวิธีการขัดขวางการเข้าถึงระบบและข้อมูล อาทิ การโจมตีระบบการบริการด้านสาธารณสุขโดยเมื่อ 9 ก.ย. 2563 โรงพยาบาลสระบุรี ออกแถลงข่าวระบบสารสนเทศของโรงพยาบาลถูกไวรัสโจมตีเรียกค่าไถ่ Voidcrypt/Spade ส่งผลให้ จนท.รพ.ไม่สามารถเข้าสู่ระบบการจัดการและรักษาพยาบาลเนื่องจากถูกขัดขวางการเข้าถึงข้อมูล (Disrupt) อีกทั้งฐานข้อมูลส่วนบุคคลของคนไข้ได้ถูกจารกรรมไปด้วย ในปีต่อมาเมื่อ 8 ก.ค. 64 เกิดเหตุการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานระบบการขนส่งและคมนาคมของ Iran ซึ่งเป็นการเจาะระบบการควบคุมรถไฟ ส่งผลให้ระบบเบรก ระบบฉุกเฉิน ไม่ทำงาน ส่งผลให้รถไฟในประเทศหลายร้อยขบวนถูกยกเลิกกระทันหัน โดยเหตุการณ์ต่อมาคือ แฮกเกอร์ได้ดำเนินการโพสต์เบอร์โทรศัพท์ผู้นำอิหร่านบน Social Media เพื่อสำหรับเป็นเบอร์สอบถามข้อมูล อีกเพียงไม่กี่สัปดาห์ต่อมาเมื่อ 22 ก.ค. 64 มีเหตุการณ์โจมตีโทรศัพท์เคลื่อนที่สมาร์ทโฟนจำนวนกว่า 50,000 เครื่อง (รวมถึง นายมาครง ปธน.ฝรั่งเศส) ด้วย Spyware ชนิด Pegasus ของอิสราเอล โดย Malware ชนิดนี้สามารถเปิด-เปิดกล้องของโทรศัพท์รวมถึงสามารถปฏิบัติภารกิจ COMINT เพื่อการจารกรรมข้อมูลในระหว่างการสนทนา (BBC 2021) จากทั้ง 3 เหตุการณ์เป็นที่ประจักษ์แล้วว่าการก่อการร้ายทางไซเบอร์นั้น มิได้มีขีดจำกัดในเรื่องของกฎการปะทะ (ROE) จึงสามารถเลือกเป้าหมายและเครื่องมือในการโจมตีได้อย่างเสรีดังนั้นมาตรการรับมือทางไซเบอร์ยังคงจะต้องทำการยกระดับขึ้นไปรวมทั้งหน่วยงานที่เกี่ยวข้องยังคงต้องค้นหาจุดเปราะบางต่อการถูกโจมตีอย่างต่อเนื่องอีกทั้งเหตุการณ์เหล่านี้เป็นเครื่องบ่งชี้ว่าการก่อการร้ายทางไซเบอร์ได้ทำการโจมตีโครงสร้างพื้นฐานที่สำคัญอย่างกว้างขวางที่แม้ว่ายังไม่ปรากฏเหตุการณ์การโจมตี CII แต่นั้นสามารถตีความได้ 2 ลักษณะคือ กลุ่มก่อการร้ายยังอยู่ในระหว่างการพัฒนาขีดความสามารถเพื่อโจมตี CG หรือการโจมตีนั้นได้เกิดขึ้นแล้วหากแต่มาตรการรับมือยังอยู่ในระดับที่ดีเพียงพอแต่ทั้งนี้จะต้องตระหนักว่าการโจมตี CI อื่น ๆ นั้นอาจส่งผล Ripple Effect ให้ย้อนกลับเพื่อสร้างความเสียหายต่อ CII ได้เช่นกัน

สรุป/ข้อเสนอแนะ

จากคำถามที่ว่าโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (CII) นับว่าเป็น Center of Gravity (CG) หรือไม่ ซึ่งคำตอบค่อนข้างชัดเจนว่าใช่อย่างแน่นอน ซึ่งข้อสรุปนั้นได้มาจากการรายงานจากหน่วยงานด้านความมั่นคงที่ได้ยืนยันมากว่า 20 ปี อีกทั้งได้มีการพัฒนาขีดความสามารถในการป้องกันจนนำไปสู่การขับเคลื่อนด้านกฎหมาย/กฎระเบียบจนมีผลบังคับใช้ ซึ่งองค์ประกอบเหล่านี้ย่อมเป็นเครื่องบ่งชี้ว่า CII นั้นเป็น CG ของระบบ/เครือข่าย CI อื่น ๆ ในส่วนการรับมือสงครามต่อต้านการก่อการร้ายยุคดิจิทัลนั้นเมื่อสามารถกำหนด CG ได้จะส่งผลให้สามารถนำไปสู่การวิเคราะห์เพื่อกำหนดจุดอ่อน/จุดเปราะบางที่จะทำให้เกิดความเสียหายที่เด็ดขาดต่อ CG และวางมาตรการป้องกันต่อไปโดยขั้นตอนมีความคล้ายกับการก่อการร้ายในยุคก่อนสามารถแบ่งเป็น 3 กลุ่มงาน ประกอบด้วย 1) การต่อต้านการก่อการร้ายที่เป็นมาตรการป้องกันการถูกโจมตี 2) การตอบโต้การก่อการร้าย ซึ่งเป็นการปฏิบัติการเชิงรุกทั้งทางด้านกฎหมายและทางทหารในการค้นหาและทำลายเป้าหมายเมื่อถูกโจมตี 3) การบริหารการจัดการหลังเกิดเหตุคือการเตรียมการตั้งแต่ระดับประเทศถึงระดับยุทธวิธีในการแก้ไขสภาวะวิกฤต (Antiterrorism, Counterterrorism, Consequence Management) (Mockaitis, 2008, p. 92-95; พิศาล 2021)

ประเด็นที่ 3: ยุทธวิธีโจมตีโครงสร้างพื้นฐานที่สำคัญ

"มาตรา 60 การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์...โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ...หรือความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้"

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (ไทย)

ในบทนี้มีวัตถุประสงค์ที่จะวิเคราะห์เป้าหมายและวิธีการที่กลุ่มก่อการร้ายยุคดิจิทัลที่สามารถเลือกใช้เพื่อให้เกิดการหยุด/ระงับขัดขวางการดำเนินงาน (Disruption) ของระบบโครงสร้างพื้นฐานที่สำคัญเพื่อนำไปสู่การกำหนดแนวทางและมาตรการในการเตรียมการป้องกันต่อไป หากพิจารณาตามข้อตกลง US-Russia 2021 พอสรุปได้ว่าการก่อเหตุโจมตี CI ด้วยเครื่องมือทางไซเบอร์นั้นเป็นลักษณะของการก่อการร้าย (ไซเบอร์) โดยจากการศึกษาพบว่าการโจมตีที่มีประสิทธิภาพซึ่งส่งผลกระทบในลักษณะ Disruption เรียกว่า "Cyber Blockade" ที่การโจมตีมีวัตุประสงค์ที่ให้การทำงาน/ระบบต้องหยุดลงในช่วงเวลาใดเวลาหนึ่ง ณ พื้นที่หรือบริเวณใดบริเวณหนึ่ง (Disruption Operations) โดยจะประกอบด้วย 2 ยุทธวิธีหลัก คือ Cyber Vandal (Vandalism) ซึ่งเป็นวิธีที่ง่ายด้วยการเจาะเข้าสู่ Website ของหน่วยงาน/องค์กร และเข้าไปแก้ไขลบข้อมูลที่มีอยู่เดิม และ Cyber Blockades ซึ่งเป็นวิธีการที่ผู้ก่อการร้ายนิยมใช้มากที่สุด ได้แก่ การโจมตีโดยปฏิเสธการให้บริการ (Distribute Denial of Service: DDOS) โดยเป็นเทคนิคการโจมตีแบบ Brute Force โดย Hacker จะทำการยึดอุปกรณ์บนเครือข่ายอินเทอร์เน็ตทั้ง Computer และ IoTs ต่อมาจะส่งข้อมูลจำนวนมากที่เกี่ยวข้องและอาจจะไม่ได้เกี่ยวข้องกับการปฏิบัติงานที่แท้จริงด้วยการใช้ช่องโหว่ของ DNS Server เพื่อให้ระบบของปลายทางต้องทำการรับ/ส่งและประมวล/ประเมินข้อมูลที่เกินขีดความสามารถ จนทำให้เครื่องหรือทรัพยากรเครือข่ายการดำเนินการเกิดการหยุดชะงักลงจนไม่สามารถให้บริการได้ แม้ว่าการโจมตีอาจพุ่งเป้าไปที่สิ่งอุปกรณ์ที่อาจเป็น IoTs ที่เป็นฟันเฟืองขนาดเล็กใน Blockchain แต่ต้องดำเนินการควบคุมผ่าน CII อาทิ ระบบการยิงต่อสู้อากาศยานในระดับกรมที่อาจมิได้พัฒนา Software เป็นระยะเวลานาน หรือ Website ของหน่วยงานราชการที่มิได้มีการ Update ระบบการป้องกัน (Firewall) ซึ่งการโจมตีแบ่งออกเป็น 2 รูปแบบได้แก่ 1) การโจมตีในระดับ Layer 3/4 หรือ Volumetric Attack และ 2) การโจมตีในระดับ Layer 7 หรือ Application Attack จะเน้นโจมตีไปยังเว็บเซิร์ฟเวอร์ (Mazanec & Whyte, 2019. p.100-101, 118, 122, 131)

จากรายงานของ (The Australian Cyber Security Center (ACSC)) พบว่าช่วงระยะเวลาเพียง 9 เดือนของปี 2021 มีการโจมตีทางไซเบอร์ต่อจุดอ่อน/จุดเปราะบางของโครงสร้างพื้นฐานที่สำคัญถึง 67,500 ครั้ง (เพิ่มขึ้น 15 % จากปี 2020) หรือคิดเป็น 8 ครั้ง/นาทีโดยเป็นการใช้ Malware มีวัตถุประสงค์หลักเพื่อทำการจารกรรมข้อมูลลับและการทำให้ระบบหยุดทำงานซึ่งจากปริมาณความถี่ที่เพิ่มขึ้นอย่างมีนัยยะเป็นเครื่องบ่งชี้ว่าการก่อการร้ายทางไซเบอร์มีแนวโน้มที่จะทวีความรุนแรงยิ่งขึ้นต่อไปในอนาคต (Guardian 2021) กลุ่มก่อการร้ายจะมุ่งเป้าโจมตีไปที่ระบบควบคุมการทำงานแบบระยะไกล Supervisory Control and Data Acquisition (SCADA) ซึ่งเป็นหัวใจของการทำงานของระบบตรวจสอบและวิเคราะห์ข้อมูลแบบ Real-time ที่ใช้ในการตรวจสอบสถานะตลอดจนถึงควบคุมการทำงานของระบบควบคุมในอุตสาหกรรมและงานวิศวกรรมต่าง ๆ โดยระบบจะประกอบด้วย 4 กลุ่มงาน คือ Data Acquisition, Networked Data Communication, Data Presentation และ Control โดยระบบจะประมวลข้อมูลเพื่อออกคำสั่งให้ AI ดำเนินการทำงานผ่าน Communication Network ที่ควบคุมจากศูนย์กลางของระบบเชื่อมต่อการสื่อสารซึ่งนั้นคือ โครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ จึงแน่นอนว่าจะมีการเตรียมการป้องกันการโดยโจมตีเป็นอย่างดีแต่อย่างไรก็ตามจากรายงานของ ACSC พบว่าจำนวนการโจมตีกลับเพิ่มขึ้นอย่างมีนัยยะซึ่งเนื่องจากจากการทำงานเป็นแบบ real-time ดังนั้นหากมีการส่ง Data ที่มีจำนวนมาก (Volumetric Attack) จนเกินขีดความสามารถของระบบย่อมส่งผลให้เกิดการติดสภาวะคอขวดที่จะระงับ/ขัดขวางการทำงานของระบบอื่น ๆ ที่อยู่บนแพลตฟอร์มเดียวกัน จากการประเมินพบว่ายุทธวิธีที่เป็นไปได้มากที่สุดคือผู้ก่อการร้ายจะดำเนินการโจมตีในลักษณะทางอ้อมโดยตั้งเป้าหมายไปที่ อุปกรณ์ IoTs และเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีการเชื่อมต่อและมีทำการร่วมกับ SCADA แต่มีการป้องกันในระดับที่ต่ำและง่ายต่อการถูกHack โดยจะปล่อย malware เพื่อทำการควบคุมอุปกรณ์ฯ และจากนั้นจึงใช้การโจมตีทางไซเบอร์ด้วยยุทธวิธี DDOS เพื่อเข้าควบคุม SCADA ต่อไป

สรุป/ข้อเสนอแนะ

ปัจจุบันโลกได้ขับเคลื่อนเข้าสู่ยุคดิจิทัลเป็นที่เรียบร้อยแล้วซึ่งองค์กร/หน่วยงานที่ควบคุมโครงสร้างพื้นฐานที่สำคัญได้ทำขัดขวาง/ระงับตนเอง (Disruption) เพื่อให้เกิดการเปลี่ยนที่ทันต่อการเปลี่ยนแปลงและได้ขับเคลื่อนองคาพยพไปสู่ Digital Organization การพึงพาระบบเครือข่ายและคอมพิวเตอร์ในการดำเนินกิจกรรมนั้นมีความจำเป็นอย่างหลีกเลี่ยงไม่ได้ซึ่งการกระจายคลื่นความถี่เหล่านี้ล้วนมาจากโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (CII) นั้น ย่อมหมายถึง CII คือจุดศูนย์ดุลของโครงสร้างพื้นฐานที่สำคัญทั้งหมดซึ่งหากถูกโจมตี CI อื่น ๆ ย่อมถูก disrupt ไปโดยปริยาย ดังนั้นการนำองค์กรไปสู่ยุคดิจิทัลจึงจำเป็นต้องลดความเสี่ยงต่อการถูกโจมตีในการเตรียมการป้องกันจากการศึกษาเหตุการณ์ที่ผ่านมาพบว่าการก่อการร้ายด้วยลักษณะ DDOS นั้นเกิดขึ้นอย่างต่อเนื่องนำไปสู่การหยุด/ระงับขัดขวางการดำเนินงานของ CI (Disruption) วิธีการขั้นพื้นฐานที่องค์กร/หน่วยควรดำเนินการให้เป็น ระเบียบปฏิบัติประจำคือ 1. การต่อต้านการก่อการร้าย คือ มาตรการระวังป้องกันก่อนการถูกโจมตีในระดับ Layer 3/4 อาทิ การบันทึกและเก็บข้อมูลการใช้งาน Bandwidth Usage ทั้ง Incoming และ Outgoing Trafficและ การโจมตีในระดับ Layer 7 อาทิ การบันทึกและเก็บข้อมูลปริมาณ HTTP Request/Sec, Session/Sec, Log/Sec 2.การบริหารการจัดการหลังเกิดเหตุคือมาตรการเตรียมการรับมือเมื่อถูกโจมตีองค์กรควรจะต้องให้ผู้ใช้งานในระบบได้รับผลกระทบน้อยที่สุดซึ่งเป็นการพิจารณาว่าระบบป้องกันที่ใช้ในปัจจุบัน รองรับการโจมตีชนิดใดได้บ้าง Malware สามารถ Bypass การป้องกันได้หรือไม่ และสำคัญที่สุดคือ สามารถป้องกัน Volumetric Attack ได้ในระดับใดและสุดท้ายคือการ Test ความพร้อมของระบบเมื่อถูกโจมตี

สรุป

คำนิยามของการก่อการร้ายได้มีการเปลี่ยนแปลงทั้งตัวแสดง (Actor) และยุทธวิธี โดยด้านตัวแสดงซึ่งมีการขยายขอบเขตตัวแสดงที่ครอบคลุมทุกตัวแสดงทั้งที่เป็นรัฐ (State Actor), ตัวแทนแห่งรัฐ (Proxies), ตัวแสดงที่มิใช่

รัฐ (Non-State Actor) ทางด้านยุทธวิธีนั้นมิได้จำกัดแค่เพียงการโจมตีทางกายภาพ (Physical Attack) แต่ได้ครอบคลุมไปถึงสงครามบนโลกเสมือนจริง (Virtual Attack) ซึ่งด้านการใช้ Hard Power ต่อเป้าหมายของการโจมตีแตกต่างจากการก่อการร้ายในยุค 1990s ที่ต้องการทำลายสิ่งอุปกรณ์/สิ่งก่อสร้างทางกายภาพหากแต่ในสงครามการก่อการร้ายในยุคดิจิทัลเป้าหมายที่สำคัญคือการขัดขวางทำงาน (Disrupt) โครงสร้างพื้นฐานที่สำคัญทางเทคโนโลยีสารสนเทศที่ควบคุมการทำงานระบบ/เครือข่ายอินเทอร์เน็ตคอมพิวเตอร์และ IoTs ซึ่งการโจมตีลักษณะนี้เรียกว่า “Cyber Blockade” ในภาพรวมแผนการเตรียมการรับมือและแผนการทำสงครามต่อต้านการก่อการร้ายในยุคดิจิทัลนั้นมิได้แตกต่างจากในยุค 1990s โดยยังคงไว้ซึ่งมี 3 องค์ประกอบคือ 1) การต่อต้านการก่อการร้าย คือมาตรการป้องกันการถูกโจมตี 2) การตอบโต้การก่อการร้าย คือ การปฏิบัติการเชิงรุกทั้งทางด้านกฎหมายและทางทหารในการค้นหาและทำลายเป้าหมายเมื่อถูกโจมตี 3) การบริหารการจัดการหลังเกิดเหตุคือการเตรียมการตั้งแต่ระดับประเทศถึงระดับยุทธวิธีในการแก้ไขสภาวะวิกฤต แต่สิ่งที่แตกต่างที่ต้องยกระดับความสำคัญคือมาตรการป้องกันและขัดขวาง (Antiterrorism) เนื่องจากหากโครงสร้างพื้นฐานที่สำคัญทางเทคโนโลยีสารสนเทศถูกโจมตีนั้น หมายถึงโครงสร้างพื้นฐานที่สำคัญอื่นจะต้องได้รับผลกระทบ (Ripple Effect) และนี่คือเครื่องบ่งชี้ว่า CII คือจุดศูนย์ดุลแห่งสงครามการก่อการร้ายในยุคดิจิทัลที่หากเพียงแค่ถูกระงับ/ขัดขวางเพียงแค่ช่วงเวลาสั้น ๆ ระบบโครงสร้างพื้นฐานที่สำคัญทั้งหมดจะต้องหยุดชะงักตามไปด้วยในทันทีซึ่งนับจากนี้ฝ่ายความมั่นคงโดยเฉพาะนายทหารด้านการข่าวจะต้องปรับกลยุทธ์อย่างเร่งด่วนและจะต้องวิเคราะห์ให้ชัดเจนว่าจุดศูนย์ดุลและจุดอ่อน/จุดเปราะบางของ CII บนสงครามการก่อการร้ายบนสมรภูมิดิจิทัลเพื่อนำไปสู่การวางมาตรการรับมือต่อไป

ทั้งนี้ประเด็นที่หน่วยงานในกองทัพจะต้องตระหนักถึงความสำคัญในการมีส่วนร่วมในการป้องกันโครงสร้างพื้นฐานที่สำคัญโดยตีความตาม พรบ. ไซเบอร์ พ.ศ. 2562 มาตรา 9 กองทัพไทยมีหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยจากการโจมตีทางไซเบอร์ของภาครัฐและภาคเอกชนที่กำหนดให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DES) เป็นประธานคณะกรรมการกำกับดูแล และผู้บัญชาการทหารสูงสุดเป็นหนึ่งในกรรมการฯ โดยตำแหน่งนั้นย่อมแสดงถึงกองทัพเป็นกลไกที่สำคัญในการต่อสู้และการป้องกันบนสมรภูมิใหม่แห่งสงครามบนโลกเสมือนจริง

บรรณานุกรม

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560” ราชกิจจานุเบกษา.เล่ม 134 ตอนที่ 10, 24 มกราคม 2560.

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562”.ราชกิจจานุเบกษา.เล่ม 136 ตอนที่ 69, 27 พฤษภาคม 2562.

จุลชีพ ชินวรรโณ (2015). โลกในศตวรรษที่ 21: กรอบวิเคราะห์ความสัมพันธ์ระหว่างประเทศ,กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย

โรงเรียนเสนาธิการทหารบก (2013).”แนวสอน 100-9: การประมาณสถานการณ์ของกองบัญชาการ”, เอกสารประกอบการสอน.

สมบูรณ์เสงี่ยมบุตร, (2013).กฎหมายอาญาระหว่างประเทศ.กรุงเทพฯ: โรงพิมพ์เพิ่มทรัพย์การพิมพ์.

พิศาล อมรรัตนานุภาพ (2021). สงครามยุคที่ 5: การก่อการร้ายไซเบอร์.บทความวิชาการสถาบันวิชาการป้องกันประเทศ, กรุงเทพฯ

Byman, D. (2017). Al Qaeda, The Islamic State, and The Global Jihadist Movement: What Everyone Needs to Know, London: Oxford University Press.

Courtney, S & Riley, M (2021). “Biden Rushes to Protect Power Grid as Hacking Threats Grow, Bloomberg”.Cybersecurity, 14th Apr, viewed 6th May 2021, Retrieved October 12 2021 from <https://www.bloomberg.com/news/articles/2021-04-14/biden-rushes-to-protect-the-power-grid-as-hacking-threats-grow>.

Guardian 2021, “Significant Threat’: Cyber Attacks Increasingly Targeting Australian’s Critical Infrastructure”, Retrieved October 12 2021 from https://www.theguardian.com/technology/2021/sep/15/significant-threat-cyber-attacks-increasingly-targeting-australias-critical-infrastructure

INTERPOL 2017 (2017). UN Resolution Highlights INTERPOL’s Role in Protecting Critical Infrastructure from Terrorists, Retrieved June, 23 2021 from https://www.interpol.int/News-and-Events/News/2017/UN-Resolution-highlights-INTERPOL-s-role-in-protecting-critical-infrastructure-from-terrorists

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic & International Studies (CSIS), Retrieved June, 17 2021 from https://csis-website-prod.s3.amazonaws.com/s3fs public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lewis, J. A. (2021). Securing the Information and Communications Technology and Services Supply Chain, Center for Strategic & International Studies (CSIS), Retrieved June, 17 2021 from https://www.csis.org/analysis/securing-information-and-communications-technology-and-services-supply-chain

Mazanec, B. & Whyte, C. (2019).Understanding Cyber Warfare: Politics, Policy and Strategy, New York: Routledge