

บทบาทของผู้ประกอบการเชิงปทัสถานของสหรัฐฯ ในการเผยแพร่ ปทัสถานด้านความมั่นคงไซเบอร์ในเวทีระหว่างประเทศ¹

ธนาวิทย์ หวังภูษเคนทร์² และพงศ์พิสุทธิ์ บุชบาร์ตัน³

วันที่รับบทความ: 2 มีนาคม 2566

วันที่แก้ไขครั้งสุดท้าย: 6 มิถุนายน 2566

วันที่ตอบรับตีพิมพ์: 13 มิถุนายน 2566

บทคัดย่อ

บทความวิจัยชิ้นนี้ต้องการศึกษาแนวคิดเรื่องปทัสถานความมั่นคงไซเบอร์ซึ่งเป็นประเด็นถกเถียงในเวทีสากลมาตั้งแต่ปี ค.ศ. 1998 ทั้งนี้ ผู้เขียนมุ่งพิจารณาการเผยแพร่ปทัสถานแบบตะวันตกซึ่งสหรัฐฯ เป็นแกนกลางในการผลักดันผ่านการดำเนินการและยุทธศาสตร์ของตัวแสดงต่างๆ ของตนไม่ว่าจะเป็นรัฐบาล ผู้เชี่ยวชาญ และภาคเอกชน ซึ่งถือว่าเป็นผู้ประกอบการเชิงปทัสถานที่ทำกรเผยแพร่ปทัสถานไซเบอร์นี้ อย่างไรก็ตาม แม้ว่าผู้ประกอบการเชิงปทัสถานเหล่านี้จะพยายามอย่างต่อเนื่องในการโน้มน้าวประเทศต่างๆ แต่ยังไม่ประสบความสำเร็จมากนัก เห็นได้จากการถกเถียงอย่างต่อเนื่องในการประชุมสมัชชาใหญ่ของสหประชาชาติในวาระความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ผลการศึกษาชี้ให้เห็นถึงความท้าทายที่มักเกิดขึ้นจากการเผยแพร่ปทัสถานแบบตะวันตกในด้านการตีความปทัสถานโดยเฉพาะในประเด็นที่ว่า พื้นที่ไซเบอร์ควรเป็นอิสระหรือควรถูกควบคุมโดยรัฐ อันจะนำไปสู่แนวทางในการปฏิบัติภายในประเทศที่ต่างกัน นอกจากนี้ การแข่งขันระหว่างมหาอำนาจในช่วงทศวรรษที่ผ่านมาเป็นปัจจัยที่สำคัญเช่นกัน โดยเฉพาะรัสเซียและจีนในห้วงที่ผ่านมาที่ต่อต้านและท้าทายการยอมรับปทัสถานที่ขึ้นาโดยสหรัฐฯ มากขึ้น ทั้งยังเสนอทางเลือกในการตีความและตัวแบบของปทัสถานในด้านนี้เพื่อสร้างกรอบขอกถกเถียงในเวทีระหว่างประเทศต่อไป

คำสำคัญ ผู้ประกอบการเชิงปทัสถาน, ความมั่นคงไซเบอร์, วัฏจักรปทัสถาน, ปทัสถานไซเบอร์, สหรัฐฯ

¹ บทความนี้เป็นส่วนหนึ่งของวิทยานิพนธ์ เรื่อง การศึกษายุทธศาสตร์เส้นทางสายไหมดิจิทัลกับประเด็นความมั่นคงไซเบอร์ของไทย หลักสูตรรัฐศาสตรมหาบัณฑิต สาขาวิชาความสัมพันธ์ระหว่างประเทศ จุฬาลงกรณ์มหาวิทยาลัย

² นักศึกษาหลักสูตรรัฐศาสตรมหาบัณฑิต สาขาวิชาความสัมพันธ์ระหว่างประเทศ คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพฯ 10330 อีเมล: thanawit.wang@gmail.com

³ ผู้ช่วยศาสตราจารย์ ดร. คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพฯ 10330 อีเมล: pongphisoot.b@chula.ac.th

The Role of US Norm Entrepreneurs in Promoting Cybersecurity Norms in the International Stage

Thanawit Wangpuchakane⁴ and Pongphisoot Busbarat⁵

Received: 2 March 2023

Revised: 6 June 2023

Accepted: 13 June 2023

Abstract

This research article critically examines the concept of cybersecurity norms, which has become a subject of global contention since 1998. Specifically, the article focuses on the promotion of Western cyber norms by the United States and the strategies it employs as a norm entrepreneur for this promotion via its various agencies, including the US government, experts, and the private sector. However, despite the persistent efforts of the United States to influence other states, its endeavors have encountered significant obstacles. This is evident in the ongoing debates on information and communication technology security within the United Nations General Assembly. The study highlights the challenges in promoting Western cyber norms. The norms can be interpreted in several ways, including debates on whether cyber domains should be regulated by states, thus leading to various approaches to domestic adoption and practices. Furthermore, competition from other major powers in recent decades has become a considerable challenge. Such powers, most notably Russia and recently China, are increasingly opposing US-led norm acceptance and are also offering alternative interpretations and models to shape the international debate.

Keywords Norm Entrepreneurs, Cybersecurity, Norm Life Cycle, Cyber Norms, U.S.

⁴ Graduate student in International Relations, Faculty of Political Science, Chulalongkorn University, Bangkok 10330. E-mail: thanawit.wang@gmail.com

⁵ Assistant Professor, Ph.D., Faculty of Political Science, Chulalongkorn University, Bangkok 10330. E-mail: pongphisoot.b@chula.ac.th

1. บทนำ

ปัจจุบันเรื่องความมั่นคงไซเบอร์เป็นเรื่องใหม่ในเวทีความสัมพันธ์ระหว่างประเทศ หนึ่งในชุดคำถามที่สำคัญในการทำความเข้าใจปรากฏการณ์ดังกล่าว คือ ใครควรเป็นผู้ควบคุมและกำกับดูแลพื้นที่ไซเบอร์ (Cyberspace) ที่ผ่านมารัฐมหาอำนาจเป็นตัวแสดงที่มีบทบาทสำคัญในการออกแบบและกำกับดูแลพื้นที่ความมั่นคงไซเบอร์ ความพยายามเพื่อชิงบทบาทนำในการพัฒนา สนับสนุนหลักการ และกำหนดกฎเกณฑ์ในแบบของตัวเองเพื่อโน้มน้าวประชาคมระหว่างประเทศผ่านตัวแสดงในหลากหลายระดับ ทั้งในกรอบขององค์การระหว่างรัฐบาล องค์การเอกชน และระหว่างรัฐด้วยกันเอง การแข่งขันดังกล่าวจึงเป็นปัจจัยสำคัญซึ่งส่งผลกระทบต่อการศึกษาและการเปลี่ยนแปลงทางปทัสถาน ทั้งนี้ รัสเซีย และสหรัฐฯ คือหนึ่งในกลุ่มผู้เล่นที่สำคัญในการผลักดันปทัสถาน และพยายามโน้มน้าวให้นานาชาติยอมรับปทัสถานที่ฝ่ายตนเป็นผู้เสนอมาตั้งแต่ปี ค.ศ. 1998 โดยรัสเซียเป็นประเทศแรกที่เสนอจนถึงปี ค.ศ. 2018 ที่สหรัฐฯ เริ่มมีความพยายามเสนอปทัสถานชุดใหม่มาเพื่อแข่งขันกับรัสเซีย ซึ่งปรากฏอย่างชัดเจนในการเสนอผ่านเวทีสหประชาชาติ ความแตกต่างของจุดยืนที่สำคัญ คือ สหรัฐฯ โน้มน้าวให้พื้นที่ไซเบอร์มีอิสระ เปิดเผย และรัฐไม่ควรเข้ามาแทรกแซงการเคลื่อนไหวของข้อมูลเหล่านั้น ในขณะที่จุดยืนของรัสเซียได้เน้นย้ำถึงความสำคัญของบูรณภาพแห่งดินแดนในพื้นที่ไซเบอร์ซึ่งรัฐจำเป็นต้องมีบทบาทในการกำกับดูแลพื้นที่ไซเบอร์ของตน แสดงให้เห็นว่าปทัสถานความมั่นคงไซเบอร์ยังเป็นเรื่องใหม่ และยังเป็นที่ยกเถียงกันอยู่ในปัจจุบัน ส่งผลให้เกิดพื้นที่ว่างในการทำทาบปทัสถานความมั่นคงไซเบอร์ที่ดำรงอยู่ในแบบตะวันตกที่สหรัฐฯ มีบทบาทนำในปัจจุบัน

การศึกษาทฤษฎีทางปทัสถานจำนวนมากมีจุดร่วมเดียวกันในการมุ่งเน้นไปที่กระบวนการเกิดขึ้นของปทัสถาน การดำรงอยู่ และการเปลี่ยนแปลงอย่างมีพลวัตของปทัสถาน (Axelrod, 1997; Finnemore & Sikkink, 1998) ซึ่งหลักการทั่วไปเป็นที่ยอมรับอย่างกว้างขวางในสำนักสรรค์สร้างนิยม (Constructivist) ในทางความสัมพันธ์ระหว่างประเทศว่า รูปแบบวัฏจักรปทัสถาน (Norm Life Cycle) คือหนึ่งในงานศึกษาการศึกษาการเกิด และเปลี่ยนแปลงของปทัสถานที่สำคัญ ใจความหลักของงานศึกษาวัฏจักรปทัสถานมีข้อสรุปร่วมกันประการหนึ่งว่าปทัสถานถูกกำหนด และประกอบสร้างโดยพฤติกรรมของตัวแสดงในสังคม (Finnemore & Sikkink, 1998, p. 891) อย่างไรก็ตาม งานศึกษาจำนวนมากให้ความสนใจกับคำถามว่าผู้ประกอบการปทัสถาน (Norm Entrepreneurs) ในฐานะตัวแสดงที่มีบทบาทในการโน้มน้าวชักจูงใจรัฐบาลหรือตัวแสดงในสังคมให้ปรับเปลี่ยนพฤติกรรมได้อย่างไร (Finnemore & Sikkink, 1998, p. 897)

แม้ว่างานศึกษาผู้ประกอบการเชิงปทัสถาน และวัฏจักรปทัสถานจะถูกศึกษาอย่างกว้างขวาง แต่ยังคงมีข้อวิพากษ์จำนวนมากว่า กระบวนการเกิดและการเปลี่ยนแปลงปทัสถานไม่ใช่วงจรสมบูรณ์ที่เป็นสูตรสำเร็จของการเปลี่ยนผ่านทางปทัสถาน (Achaya, 2004) วัฏจักรปทัสถานของ Finnemore and Sikkink (1998) ไม่สามารถอธิบายได้อย่างชัดเจนถึงพลวัตที่ปทัสถานถูกนำไปปฏิบัติและเปลี่ยนแปลงพฤติกรรมของตัวแสดงต่างๆ ภายในรัฐแต่ละรัฐได้ หากการศึกษาปราศจากกระบวนการนำเอาปทัสถานของรัฐหรือตัวแสดงของรัฐยอมรับเพื่อนำมาปฏิบัติภายในประเทศ (Norm Internalization Process) ทั้งนี้ พลวัตภายในที่มีการนำปทัสถานแบบใหม่มาปฏิบัติใช้มีความเกี่ยวข้องกับผู้ประกอบการเชิงปทัสถานที่อาจจะตีความปทัสถานภายนอกเหล่านั้นตามเหตุผลและบริบทของตัวเอง

บทความนี้ต้องการศึกษาการเกิดและการเปลี่ยนแปลงของปทัสถานความมั่นคงไซเบอร์ ซึ่งเป็นปรากฏการณ์ใหม่ที่มหาอำนาจมีบทบาทในการพัฒนาเทคโนโลยีและพื้นที่ไซเบอร์เข้ามาแข่งขันในรูปแบบต่างๆ เพื่อกำหนดทิศทางของการพัฒนาปทัสถานโดยเฉพาะอย่างยิ่งการแข่งขันระหว่างปทัสถานในประเทศตะวันตกมีบทบาทนำในการเป็นผู้กำหนดปทัสถาน โดยเฉพาะอย่างยิ่งสหรัฐฯ ซึ่งในปัจจุบันพบว่าปทัสถานความมั่นคงไซเบอร์แบบโลกตะวันตกค่อนข้างเป็นที่ยอมรับมากกว่า ดังนั้น บทความนี้จึงต้องการศึกษาบทบาทผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์โดยเฉพาะอย่างยิ่งสหรัฐฯ องค์การระหว่างรัฐ องค์การเอกชนที่มีความสำคัญต่อการสนับสนุนปทัสถานทางไซเบอร์ที่มีอยู่ในปัจจุบัน และทำความเข้าใจว่า ผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ที่สำคัญของสหรัฐฯ คือใคร และมีบทบาทอย่างไรในช่วงวัฏจักรปทัสถาน โดยบทบาทของช่วงวัฏจักรนั้นทำให้เกิดอะไรในปทัสถานความมั่นคงไซเบอร์

ผู้เขียนได้แจกแจงโครงสร้างบทความไว้ดังนี้ 1) บทนำ 2) การทบทวนวรรณกรรมเพื่อแสดงให้เห็นถึงพัฒนาการของข้อถกเถียงวรรณกรรม และสร้างความเข้าใจเบื้องต้นถึงฐานความคิดทางทฤษฎีที่ถูกใช้ในงานเขียนชิ้นนี้ 3) กรอบแนวคิดและทฤษฎี เรื่อง วัฏจักรปทัสถานของ Finnemore and Sikkink (1998) 4) ผู้ประกอบการเชิงปทัสถานความมั่นคงไซเบอร์ของสหรัฐฯ เพื่ออธิบายว่า ตัวแสดงเชิงปทัสถานด้านความมั่นคงไซเบอร์คือใคร และมีบทบาทอย่างไรในการสร้างหรือเปลี่ยนแปลงปทัสถานทางไซเบอร์ 5) ประเมินความสำเร็จในการแพร่กระจายปทัสถานความมั่นคงไซเบอร์ของสหรัฐฯ และส่วนสุดท้ายสรุปเพื่อชี้ให้เห็นว่าปทัสถานความมั่นคงไซเบอร์ในแบบตะวันตกที่สหรัฐฯ มีบทบาทนำนั้นยังคงถูกตั้งคำถามและเป็นที่ถกเถียงโดยประชาคมโลกซึ่งเปิดช่องว่างให้มหาอำนาจอื่นเข้ามาท้าทายปทัสถานความมั่นคงไซเบอร์ที่ดำรงอยู่

2. การทบทวนวรรณกรรม

จากการศึกษาวรรณกรรมพบว่า คำว่า “ปทัสถานหรือบรรทัดฐาน” (Norms) ถูกกล่าวถึงในงานศึกษาที่เกี่ยวข้องกับรัฐศาสตร์และความสัมพันธ์ระหว่างประเทศอย่างกว้างขวาง นักวิชาการหลายสำนักคิดได้ศึกษานิยาม การตีความ และวิธีการนำไปใช้ในทางใดทางหนึ่งเพื่ออธิบายพฤติกรรมในตัวแสดงทุกระดับการเมือง Finnemore and Sikkink (1998) อธิบายว่า ปทัสถานเป็นรูปแบบของพฤติกรรมที่ถูกยอมรับโดยทั่วกัน และกระทำอย่างซ้ำๆ โดยตัวแสดงในสังคมซึ่งปทัสถานจะกำหนดพฤติกรรมของตัวแสดง (Agents) ในเวลาเดียวกัน เนื่องจากปทัสถานจะเป็นตัวกำหนดมาตรฐานหรือยุทธศาสตร์ของสังคมโดยส่วนใหญ่ ขณะเดียวกันสังคมโดยทั่วไปจะปฏิบัติตามมาตรฐานเหล่านั้นเพื่อรักษาเสถียรภาพของมาตรฐานที่ตอบรับความคาดหวังของตัวแสดงในสังคมนั้นร่วมกัน จากคำอธิบายข้างต้นชัดเจนว่าปทัสถานในสังคมจะเกิดการเสริมสร้างระหว่างตัวแสดงและสังคมอย่างมีนัยสำคัญ (Reinforcement) ปทัสถานที่สำคัญในปัจจุบัน เช่น ปทัสถานด้านสิทธิมนุษยชน ปทัสถานด้านเศรษฐกิจแบบทุนนิยม องค์การระหว่างประเทศ ปทัสถานทางไซเบอร์ เป็นต้น

อย่างไรก็ดี บทความนี้จะศึกษาปทัสถานความมั่นคงไซเบอร์เป็นประเด็นสำคัญ ซึ่งพบว่า ปทัสถานที่กำลังอยู่ในปัจจุบันจำนวนมากถูกกำหนดโดยชาติตะวันตกเป็นหลัก โดยเฉพาะอย่างยิ่งสหรัฐฯ ซึ่งผู้เขียนได้แจกแจงวรรณกรรมออกเป็น 2 กลุ่ม ได้แก่ 1) วรรณกรรมกลุ่มปทัสถานทางไซเบอร์ที่กำลังอยู่ในปัจจุบันซึ่งถูกกำหนดโดยชาติตะวันตก โดยเฉพาะอย่างยิ่งบทบาทของสหรัฐฯ ต่อการกำหนดปทัสดาดังกล่าว 2) วรรณกรรมกลุ่มการทำลายปทัสถานทางไซเบอร์ซึ่งถูกเสนอโดยเฉพาะอย่างยิ่งรัสเซีย และจีน ซึ่งวรรณกรรมทั้ง 2 กลุ่มจะแสดงให้เห็นถึงพัฒนาการของการปะทะทางปทัสถานทางไซเบอร์ซึ่งเป็นประเด็นที่สำคัญอย่างยิ่งในยุคเทคโนโลยีสมัยใหม่ แจกแจงไว้ดังนี้

วรรณกรรมกลุ่มที่หนึ่งซึ่งศึกษาปทัสถานทางไซเบอร์ที่กำลังอยู่ในปัจจุบันโดยเฉพาะอย่างยิ่งบทบาทของสหรัฐฯ และชาติพันธมิตรตะวันตก งานศึกษาจำนวนมากมีจุดเริ่มต้นเดียวกัน คือ การศึกษาพัฒนาการของอินเทอร์เน็ตและเวิลด์ไวด์เว็บ (World Wide Web) ซึ่งถูกพิจารณาว่าเป็นโครงสร้างพื้นฐานที่สำคัญที่สุดของการสร้างสังคมและการจัดการผู้มีส่วนได้ส่วนเสียในพื้นที่ไซเบอร์ (Adler, 1997; Mueller, Mathiason, & Klein, 2007; Yau, 2019) นักวิชาการตะวันตกจำนวนมากให้นิยามปทัสถานที่ทำให้บทบาทของตัวแสดงหลายตัวที่เกี่ยวข้องมีส่วนร่วมในการกำกับดูแลทางไซเบอร์ซึ่งไม่จำกัดเพียงรัฐ แต่ควรหมายรวมถึงปัจเจกบุคคล ภาคธุรกิจ องค์กรที่ไม่ใช่รัฐ และผู้เกี่ยวข้องว่าเป็นการกำกับดูแลพื้นที่ไซเบอร์แบบผู้มีส่วนได้ส่วนเสียหลายฝ่าย (Multistakeholder Governance) (Gleckman, 2018)

ในขณะเดียวกัน นักวิชาการจำนวนหนึ่งได้พิจารณาถึงข้อพึงระวังในพื้นที่ไซเบอร์ว่า ในความเป็นจริงแล้วนั้นมีหลายพื้นที่ที่ยังไม่สามารถเข้าถึงการใช้งานอินเทอร์เน็ตได้ โดยมีข้อเสนอถึงแนวคิดของ “Wild West Web” แนวคิดซึ่งเน้นย้ำถึงความไร้ระเบียบในพื้นที่ไซเบอร์เพื่อชี้ให้เห็นถึงความสำคัญของการพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ และการออกแบบกฎระเบียบเพื่อรักษาความมั่นคงที่ไม่ใช่เพียงแค่เรื่องไซเบอร์เท่านั้น (Arquilla & Ronfeldt, 1997, p. 242) อย่างไรก็ตาม นักวิชาการตะวันตกโดยเฉพาะอย่างยิ่งสหรัฐฯ จำนวนหนึ่งให้การสนับสนุนปทัสถานการกำกับดูแลโดยผู้มีส่วนได้ส่วนเสียหลายฝ่าย เสนอว่า รัฐบาลไม่ควรควบคุมพื้นที่ไซเบอร์เพียงลำพัง เนื่องจากโครงสร้างพื้นฐานในโลกไซเบอร์นั้น ถูกออกแบบ ควบคุม ดำเนินการ และบำรุงรักษาร่วมกันโดยตัวแสดงอื่นโดยเฉพาะอย่างยิ่ง ภาคเอกชน (Lu, 2014)

ในทางหนึ่ง การศึกษาปทัสถานซึ่งเกี่ยวข้องกับตัวแสดงที่หลากหลายเสนอว่า ตัวแสดงที่เกี่ยวข้อง และมีส่วนร่วมในการออกแบบปทัสถานความมั่นคงไซเบอร์แบบผู้มีส่วนได้ส่วนเสียหลายฝ่าย คือ ตัวแสดงที่สนับสนุนและเสริมสร้างความแข็งแกร่งให้กับปทัสถานดังกล่าว (Finnemore, 2017; Ostrom, 2000) นักวิชาการสำนักสรรค์สร้างนิยมนิยามตัวแสดงดังกล่าวว่าเป็นตัวกระทำการ (Agency) ที่มีฐานะเป็นผู้ประกอบการเชิงปทัสถานซึ่งมีบทบาทสำคัญในการเผยแพร่ โน้มน้าวปทัสถานหนึ่งๆ ในบริบทเช่นนี้การมีผู้ประกอบการเชิงปทัสถานจำนวนมากย่อมหมายความว่า ปทัสถานดังกล่าวถูกเชื่อมโยงและเกี่ยวพันโดยตัวแสดงที่เกี่ยวข้องจำนวนมาก ส่งผลให้ปทัสถานในแบบตะวันตกวันมีความเข้มแข็งและเป็นที่ยอมรับอยู่ในปัจจุบัน (Mueller, 2009, pp. 74-75)

อย่างไรก็ตาม วรรณกรรมทุกชิ้นในกลุ่มผู้สนับสนุนปทัสถานซึ่งกำกับดูแลโดยผู้มีส่วนได้ส่วนเสียหลายฝ่ายมีข้อสรุปในลักษณะเดียวกันว่า เทคโนโลยีนั้นเติบโตและมีการแข่งขันกันอยู่ตลอดเวลา ดังนั้น สหรัฐฯ อาจไม่สามารถรักษาอิทธิพลนำในฐานะผู้กำหนดปทัสถานที่สำคัญในอนาคตได้ เนื่องจากเทคโนโลยีที่ล้ำสมัยและทรัพยากรที่เพิ่มมากขึ้นโดยเฉพาะอย่างยิ่งในโลกของข้อมูลและคลังความรู้ (Think Tanks) ที่เชื่อมโยงกันในปัจจุบัน

อีกด้านหนึ่ง วรรณกรรมกลุ่มที่สองกล่าวถึงปทัสถานทางไซเบอร์ที่ถูกเสนอโดยรัสเซียและจีนในฐานะรัฐแกนนำที่สำคัญ (Critical State) ซึ่งท้าทายปทัสถานดังกล่าวที่ดำรงอยู่ในแบบตะวันตก นักวิชาการจำนวนหนึ่งมีข้อสรุปร่วมกันว่า ปทัสถานทางไซเบอร์ที่ถูกเสนอโดยรัฐอำนาจนิยมมักมีลักษณะที่รัฐเป็นศูนย์กลาง (State-Centric) (Badescu, 2011) การศึกษาจำนวนมากโดยเฉพาะนักวิชาการสหรัฐฯ ตั้งข้อสังเกตว่า รัฐบาลรัสเซีย และจีนสนับสนุนยุทธศาสตร์ระดับโลกในการควบคุมพื้นที่ไซเบอร์ ซึ่งเน้นย้ำถึงความจำเป็นในการมีส่วนร่วมของรัฐบาลและบทบาทของสหประชาชาติ (United Nations: UN) ในฐานะองค์กรที่มีอำนาจโดย

ขอบด้วยกฎหมาย (Gold, 2021; Mueller et al., 2007, pp. 238-239) นักวิชาการส่วนหนึ่งเสนอว่า หลักการของจีนจะทำให้รัฐบาลต่างๆ สามารถควบคุมอธิปไตยและความมั่นคงแห่งดินแดนของตนเองได้มากขึ้น (Kolton, 2017) และโต้แย้งว่า ปทัสถานการกำกับดูแลโดยผู้มีส่วนได้ส่วนเสียหลายฝ่ายแบบตะวันตกส่งผลให้การพัฒนาและการออกแบบสถาปัตยกรรมอินเทอร์เน็ต (Internet Architecture) ถูกกระจายและแบ่งส่วน (De-Centralize) ซึ่งอาจเป็นภัยคุกคามต่ออำนาจอธิปไตยของรัฐ (Hobbs, 2020) ดังนั้น ประเด็นเรื่อง “อำนาจอธิปไตยทางไซเบอร์” (Cyber Sovereignty) จึงควรถูกพิจารณาและตีความใหม่ กล่าวอีกนัยหนึ่งว่า พื้นที่ไซเบอร์และอินเทอร์เน็ตควรเป็นเรื่องระหว่างรัฐกับรัฐ (State-To-State) ซึ่งทุกรัฐควรทำงานร่วมกันเพื่อผลประโยชน์ร่วมอย่างเท่าเทียม (Cai, 2018, p. 67; Li, 2019, pp. 109-114) ประเด็นดังกล่าวยังเสนออีกว่า การกำกับดูแลพื้นที่ไซเบอร์จำเป็นต้องพิจารณาครอบคลุมถึงประเด็นทางสังคมและนโยบายโครงสร้างพื้นฐานด้านเทคโนโลยี-สารสนเทศรวมถึงเทคโนโลยีที่เกี่ยวข้องด้วย (Streubz, 2021)

การศึกษาจำนวนหนึ่งได้อธิบายถึงลักษณะของปทัสถานทางไซเบอร์ของจีนว่า รัฐบาลจีน และรัสเซียใช้กลไกระหว่างประเทศและภูมิภาคที่นำโดยรัฐ (State-Led) เพื่อเสนอปทัสถานความมั่นคงไซเบอร์ในแบบของตัวเอง ผู้เขียนพิจารณาเบื้องต้นว่า ทั้งสองประเทศได้วางตัวเองให้มีบทบาทเป็นผู้ประกอบการเชิงปทัสถานซึ่งมีบทบาทในการโน้มน้าวรัฐบาลอื่นให้ยอมรับปทัสถานของตน นักวิชาการจำนวนมากอธิบายว่า ปทัสถานของจีนถูกผลักดันผ่านข้อริเริ่มแถบและทาง (Belt and Road Initiative) โดยมียุทธศาสตร์เป็นการเฉพาะในเรื่องการสร้างเครือข่ายเชื่อมโยงด้านดิจิทัลที่เรียกว่า เส้นทางสายไหมดิจิทัล (Digital Silk Road) นอกจากนี้ นักวิชาการโดยเฉพาะจีนยืนยันว่า ประเทศที่มีลักษณะเป็นประชาธิปไตยนั้นสามารถอยู่ร่วมกับกรอบปทัสถานของรัฐซึ่งจะมีการปกครองแบบอำนาจนิยมเป็นผู้กำหนดได้ (Yeli, 2017) โดยอ้างว่า การนำประชาธิปไตยไปใช้ในความเป็นจริงนั้นไม่ควรถูกจำกัดไว้อย่างเข้มงวดเพียงแบบเดียวดังที่ชาติตะวันตกส่วนใหญ่กล่าวอ้าง และเสนอต่อว่า ประเทศจีนก็มีรูปแบบการปกครองแบบประชาธิปไตยอยู่ด้วยในบางแง่มุมเช่นกัน ในขณะที่รัฐบาลจีน และรัฐอำนาจนิยมหลายรัฐมีระบบการให้ความสำคัญกับผู้นำพรรคอยู่นั้นก็มีกลไกซึ่งให้พรรคหรือบุคคลที่ไม่ใช่พรรคร่วมรัฐบาลมีบทบาทสำคัญในการให้คำปรึกษาหารือและกำกับดูแลกิจการของรัฐด้วย (Jiayi, 2021)

ในขณะเดียวกัน งานศึกษาจำนวนหนึ่งในกรอบแนวคิดหลังอาณานิคม (Post-Colonialism) ได้เสนอในอีกแง่มุมว่า ปทัสถานความมั่นคงทางไซเบอร์ไม่ต่างอะไรจากการล่าอาณานิคมในยุคหนึ่ง ต่างเพียงบริบทซึ่งเป็นการขูดรีดและแย่งชิงทางข้อมูลเพียงเท่านั้น (Arora, 2019) อย่างไรก็ตาม นักวิชาการจำนวนมากได้เสนอว่า ลัทธิอาณานิคมนั้นไม่ได้จำกัดเฉพาะการล่าอาณานิคมโดยชาติตะวันตกเพียงอย่างเดียว แต่แนวคิดดังกล่าวยังสามารถ

ผสมผสานและกลายเป็นเครื่องมือของทั้งระบบเสรีทุนนิยมและระบอบเผด็จการได้ด้วย ซึ่งเป็นคำอธิบายที่ถูกใช้โดยเฉพาะในลัทธิอาณานิคมทางดิจิทัล ส่งผลกระทบต่อโครงสร้างพื้นฐานไซเบอร์ซึ่งไม่จำกัดเพียงชาติตะวันตกเป็นผู้กระทำเท่านั้น แต่ยังหมายรวมถึงชาติอำนาจนิยมอย่างรัสเซีย และจีน (Greenwood, 2020)

อย่างไรก็ดี วรรณกรรมทั้งสองกลุ่มได้ฉายให้เห็นถึงบริบทของการแข่งขันทางปทัสถานทางไซเบอร์ที่ดำรงอยู่ซึ่งถูกกำหนดโดยชาติตะวันตกโดยเฉพาะอย่างยิ่งสหรัฐฯ ในฐานะผู้มีบทบาทนำในการกำหนดปทัสถานเป็นที่ยอมรับในปัจจุบัน และปทัสถานใหม่ที่กำลังท้าทายอยู่ การแข่งขันดังกล่าวได้สร้างความขัดแย้งต่อการตีความและการกำหนดปทัสถานที่จะเกิดขึ้นในอนาคต เนื่องจากการขยายขอบเขตของการตีความในเรื่องอำนาจอธิปไตยทางไซเบอร์และบูรณาภาพแห่งดินแดน ซึ่งแนวปฏิบัติของปทัสถานดังกล่าวถูกนักวิชาการจำนวนหนึ่งพิจารณาว่าเป็น “อำนาจนิยมทางดิจิทัล” (Digital Authoritarianism) รัฐบาลสามารถใช้ข้ออ้างด้านความมั่นคงในการควบคุมและจำกัดพื้นที่ไซเบอร์ในการจำกัดเสรีภาพในการแสดงออก รวมถึงสิทธิมนุษยชนด้านอื่นๆ (Khalil, 2020; Sherman, 2021)

งานศึกษาชิ้นนี้มีจุดมุ่งหมายสำคัญเพื่อสนับสนุนกลุ่มสรรค์สร้างนิยมในเรื่องผู้ประกอบการเชิงปทัสถาน เนื่องจากการศึกษาตัวแสดงต่างๆ ในฐานะตัวกระทำที่สำคัญในกระบวนการเกิด เปลี่ยนแปลง และแพร่กระจายปทัสถานทางไซเบอร์ยังมีช่องว่าง (Gap) การศึกษาปทัสถานทางไซเบอร์จำนวนมากมักมุ่งเน้นไปที่ผลลัพธ์ และผลกระทบของการถกเถียงทางปทัสถานในเวทีสากล ซึ่งการศึกษามุมมองที่และความสามารถของตัวกระทำที่สำคัญในฐานะผู้ประกอบการเชิงปทัสถานทางไซเบอร์จะทำให้สามารถทำความเข้าใจกระบวนการเปลี่ยนแปลงเชิงปทัสถานได้ชัดเจนขึ้น จากผลการศึกษาผู้เขียนได้นำเสนอเพิ่มเติมในชุดความคิดวิถักรปทัสถาน และชี้ให้เห็นข้อเท็จจริงจากกรณีศึกษาที่เกิดขึ้นโดยเฉพาะอย่างยิ่งในกรอบปทัสถานความมั่นคงไซเบอร์แบบตะวันตกซึ่งมีสหรัฐฯ เป็นผู้มียบทบาทนำในฐานะผู้กำหนดปทัสถาน เพื่ออธิบายว่า การเกิดขึ้นของปทัสถานทางความมั่นคงไซเบอร์เป็นเช่นไร เพื่อเสนอว่า ตัวแสดงใดเป็นผู้ประกอบการเชิงปทัสถานของสหรัฐฯ และผู้ประกอบการเชิงปทัสถานเหล่านั้นมีบทบาทอย่างไรในช่วงวิถักรต่างๆ ผ่านกรณีศึกษาปทัสถานความมั่นคงไซเบอร์ตะวันตกซึ่งได้รับการยอมรับอย่างกว้างขวางในปัจจุบัน ภายใต้บริบทการแข่งขันทางปทัสถานไซเบอร์ในโลกตะวันตกระหว่างสหรัฐฯ และรัสเซียในฐานะรัฐแกนนำที่สำคัญ ทั้งนี้ การศึกษาจะช่วยเติมเต็มช่องว่างของการศึกษามุมมองผู้ประกอบการเชิงปทัสถานทางไซเบอร์ โดยเฉพาะอย่างยิ่งสหรัฐฯ และเป็นแนวทางสำคัญต่อการศึกษาตัวแสดงในกรณีประเทศอื่นๆ

3. กระบวนการสร้างปทัสถานระหว่างประเทศ แนวคิดเรื่อง วัฏจักรปทัสถาน

การทำความเข้าใจกระบวนการเกิดปทัสถาน พลวัต และการเปลี่ยนแปลงทางปทัสถาน คือ ชุดคำถามสำคัญในงานศึกษาปทัสถานต่างๆ ในบทความชิ้นนี้ผู้เขียนเลือกใช้แนวคิดวัฏจักรปทัสถานของสำนักสรรค์สร้างนิยมตามตัวของ Martha Finnemore และ Kathryn Sikkink (1998) ในการทำความเข้าใจการแพร่กระจายของปทัสถาน เนื่องจากแนวคิดดังกล่าวพยายามตอบคำถามสำคัญถึงการเกิดขึ้นและกลไกในการอธิบายการเปลี่ยนแปลงของปทัสถานในเชิงวิวัฒนาการ โดยเฉพาะอย่างยิ่งมีการให้การพิจารณาบทบาทของผู้กระทำ การซึ่งถูกเรียกว่าผู้ประกอบการเชิงปทัสถานซึ่งเป็นตัวแสดงสำคัญในการสร้าง การเปลี่ยนแปลง และการแพร่กระจายของปทัสถาน ทั้งนี้ แนวคิดวัฏจักรปทัสถานดังกล่าว ประกอบด้วย 3 ระยะที่สำคัญ ได้แก่

- 1) การเกิดขึ้นของปทัสถาน (Norm Emergence)
- 2) การแพร่กระจายของปทัสถาน (Norm Cascade)
- 3) การนำปทัสถานภายนอกมาปฏิบัติภายในประเทศ (Norm Internalization)

3.1 ระยะที่หนึ่ง การเกิดขึ้นของปทัสถาน

จากการศึกษาพบว่า ในจุดกำเนิดของปทัสถานนั้นงานศึกษาจำนวนมากพบว่าผู้ประกอบการเชิงปทัสถาน คือ ส่วนสำคัญซึ่งเป็นตัวแสดงที่จะโน้มน้าว (Persuade) มวลชนที่สำคัญให้สนับสนุนปทัสถานใหม่เพื่อเปลี่ยนแปลงปทัสถานที่มีอยู่ทำให้เกิดการเปลี่ยนแปลงพฤติกรรมที่ผู้ประกอบการปทัสถานพึงประสงค์ให้รัฐหรือสังคมปฏิบัติ อย่างไรก็ตาม หน้าที่ของผู้ประกอบการเชิงปทัสถานนั้นเป็นเรื่องยากในความเป็นจริง กล่าวคือ การเสนอปทัสถานใหม่นั้นหมายถึงการแข่งขันกับบริบททางสังคม หนึ่งคือ ผู้ประกอบการเชิงปทัสถานต้องแข่งขันและท้าทายกับสถานะภาพของปทัสถานเดิมที่ดำรงอยู่ในสังคม เปรียบได้เช่นการเสนอขายสินค้าชนิดหนึ่งให้กับบริษัทที่ผูกสัณฐานใช้สินค้าชนิดเดียวกันอยู่แล้วเป็นประจำซึ่งหมายความว่าผู้ประกอบการเชิงปทัสถานเหล่านั้นต้องพร้อมที่จะปะทะกับการแข่งขันเชิงปทัสถานและความขัดแย้งด้านผลประโยชน์ภายในบริบทเฉพาะทางสังคมแต่ละสังคม

การเกิดขึ้นของปทัสถานในบริบทของความสัมพันธ์ระหว่างประเทศ Finnemore and Sikkink (1998) อธิบายว่า ผู้ประกอบการเชิงปทัสถานจะดำเนินการอยู่ภายในองค์กร เช่น องค์กรระหว่างประเทศ องค์กรที่ไม่ใช่รัฐ เป็นต้น โดยเชื่อว่าการดำเนินการอยู่ในระดับดังกล่าวจะส่งเสริมและอำนวยความสะดวกในการเข้าถึงมวลชนภายในเป้าหมายได้ เมื่อผู้ประกอบการเชิงปทัสถานสามารถโน้มน้าวรัฐให้ยอมรับปทัสถานจนถึงจุดสูงสุดได้ (Tipping Point) เมื่อนั้นปทัสถานจะเกิดขึ้นในความสัมพันธ์ระหว่างประเทศ การศึกษาเดียวกันเสนอว่า มติ 1 ใน 3

(One-Third) ของสมาชิกในองค์การระหว่างประเทศ สามารถตีความได้ว่า ปทัสถานหนึ่งได้ถูกสร้างขึ้น

3.2 ระยะที่สอง การแพร่กระจายของปทัสถาน

เมื่อปทัสถานถูกสร้างขึ้นมาระยะเวลาหนึ่งจนมีผู้ให้ความสนใจและสนับสนุนเป็นจำนวนมากจะเกิดกระแสที่เป็น “ปกติ” ขึ้น เมื่อนั้นกระบวนการแพร่กระจายของปทัสถานจะเริ่มขึ้น กล่าวคือ เมื่อผู้ประกอบการเชิงปทัสถานโน้มน้าวตัวแสดงที่เกี่ยวข้องจนเกิดอัตราการยอมรับปทัสถานใหม่ระหว่างตัวแสดงไปจนถึงจุดสูงสุด ส่งผลให้การยอมรับปทัสถานใหม่นั้นจะเพิ่มขึ้นอย่างรวดเร็ว เนื่องจากเกิดกลไกการขัดเกลาทงสังคม (Socialization) ตัวแสดงจะดำเนินการโน้มน้าวเชิงปทัสถานด้วยตัวเองเพื่อให้ผู้อื่นยอมรับปทัสถานบางอย่าง ในทางหนึ่ง ตัวแสดงในสังคมจะได้รับแรงกดดันจากผู้กระทำการรอบข้างในฐานะที่ผู้กระทำการจำนวนมากเหล่านั้นกระทำพฤติกรรมบางอย่างซึ่งพิจารณาแล้วว่าเหมาะสม ส่งผลในเชิงจิตวิทยาให้เกิดสภาพกดดันตัวแสดงอื่นภายนอกปทัสถานให้เกิดความคล้อยตามทางใดทางหนึ่ง กล่าวอีกนัยหนึ่งในกรณีของรัฐในฐานะสมาชิกองค์การระหว่างประเทศจะได้รับแรงกดดันจากสมาชิกภายในเสมอ โดยเฉพาะอย่างยิ่งเมื่อความต้องการเพิ่มความชอบธรรมทั้งภายในและระหว่างประเทศสูงขึ้น ส่งผลให้เกิดแรงกดดันเพื่อสร้างบทบาทนำของสมาชิกหนึ่ง บ่อยครั้งบีบบังคับให้รัฐต้องเลือกคล้อยตามเพื่อลดปัญหาที่อาจเกิดกับรัฐสมาชิกที่มีอำนาจนำปทัสถานนั้นอยู่ ทั้งนี้รัฐที่เป็นแกนนำที่สำคัญในการเมืองระหว่างประเทศ มีบทบาทในการทำให้เกิดการขัดเกลาทงสังคมเพื่อให้รัฐอื่นคล้อยตามปทัสถานที่ฝ่ายตนเสนอ (Norm Conformity)

คำถามสำคัญ คือ จะใช้เกณฑ์หรือตัวชี้วัดใดในการพิจารณาว่าปทัสถานใหม่เป็นที่ยอมรับอย่างกว้างขวางจนเข้าสู่กระบวนการแพร่กระจายของปทัสถานในระยะที่ 2 ทั้งนี้ Hoffmann (2003) มีข้อเสนอว่า จุดสูงสุดของการยอมรับปทัสถานใหม่สามารถพิจารณาได้จากการยอมรับโดยตัวแสดงในสังคม Hoffmann ศึกษากระบวนการเปลี่ยนผ่านปทัสถานโดยใช้รูปแบบวัฏจักรปทัสถานของ Finnemore และ Sikkink มีข้อสรุปว่า กระบวนการแพร่กระจายในระยะที่ 2 ของวัฏจักรปทัสถานจะเกิดขึ้นได้เมื่อจำนวนตัวแสดงที่ยอมรับปทัสถานใหม่เพิ่มจำนวนมากขึ้นอย่างรวดเร็ว โดยวัดจากเมื่อตัวแสดงยอมรับปทัสถานดังกล่าวร้อยละ 60-70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบในที่ประชุมหนึ่งๆ และมีแนวโน้มจะเพิ่มขึ้นอย่างต่อเนื่อง อีกนัยหนึ่งหมายถึง 2 ใน 3 (two-third) ของเสียงมติจากที่ประชุมขององค์กร (Hoffmann, 2003)

ในบริบทปทัสถานความมั่นคงไซเบอร์เริ่มมีการแข่งขันเข้มข้น และมีประเทศต่างๆ เริ่มคล้อยตามกับข้อเสนอที่สหรัฐฯ เสนอมากขึ้นตามไปด้วย อย่างไรก็ตาม ระยะของการ

แพร่กระจายของปัทสถานที่น่าโดยสหรัฐฯ ยังไม่ได้รับการยอมรับอย่างกว้างขวาง ทำให้การ
แข่งขันเสนอปัทสถานในระยะนี้ยังคงดำเนินต่อไป

3.3 ระยะที่สาม การนำปัทสถานที่ยอมรับมาปฏิบัติภายในประเทศ

อนึ่ง เมื่อปัทสถานที่ถูกสร้างขึ้นดำเนินอยู่ภายในสังคมโดยมีตัวแสดงยอมรับและปฏิบัติ
ตามแนวคิดทางปัทสถานเหล่านั้นแล้ว เมื่อถึงจุดนั้นจะเกิดกระบวนการนำเอาปัทสถานที่รัฐหรือ
ตัวแสดงของรัฐยอมรับเพื่อนำมาปฏิบัติภายในประเทศ ปัทสถานจะถูกทำให้กลายเป็นเรื่อง
ภายในประเทศ หมายความว่า ปัทสถานดังกล่าวจะไม่ถูกตั้งคำถามหรือถูกตั้งข้อสงสัยในสังคม
น้อยลงอย่างมาก ในเชิงรูปธรรมนั้นรัฐบาลอาจประกาศเป็นข้อกำหนดหรือกฎหมายเพื่อให้เกิด
เป็นที่ยอมรับโดยทั่วกัน เป็นต้น อย่างไรก็ตาม ผู้เขียนตั้งข้อสังเกตบางประการว่า รัฐบาลอาจกำหนด
เป็นแนวนโยบายซึ่งจะส่งผลต่อการตีความและการดำเนินกิจกรรมของตัวแสดงภายในรัฐ
กล่าวคือ เนื้อหาสาระของปัทสถานเหล่านั้นเป็นเรื่องของอัตวิสัย (Subjective) อาจส่งผลต่อ
ความเข้าใจร่วมของตัวแสดง นำไปสู่ความไม่เป็นหนึ่งเดียวกันของปัทสถานในสังคม

อย่างไรก็ตาม แนวคิดวิภาษวิธีของปัทสถานของสำนักสรรค์สร้างนิยมดังกล่าว ถูกวิพากษ์ว่า
เมื่อเกิดสภาพความล้มเหลวของวิภาษวิธีปัทสถานขึ้น ผู้ประกอบการเชิงปัทสถานจะถูกพิจารณา
ว่ามีส่วนสร้างและเปลี่ยนแปลงผลลัพธ์ดังกล่าว (Achaya, 2004) ผู้เขียนมีข้อเสนอว่า
ข้อเท็จจริงเชิงประจักษ์ที่เกิดขึ้นในแต่ละประเทศไม่ได้ถูกพิจารณาอย่างแท้จริงว่า
ผู้ประกอบการเชิงปัทสถานสามารถมีอิทธิพลต่อผลลัพธ์ที่เกิดขึ้นจากปฏิสัมพันธ์ระหว่าง
ตัวแสดงที่แตกต่างกัน และพึ่งพาซึ่งกันและกันได้อย่างไร ส่งผลให้แนวคิด วิภาษวิธีปัทสถาน
ไม่สามารถอธิบายในลักษณะเหมารวมได้ (Stereotype) เมื่อถึงจุดที่พิจารณาถึงข้อเท็จจริง
เชิงประจักษ์ภายในรัฐแล้ว สิ่งที่ต้องพิจารณาต่อ คือ เงื่อนไขของผู้ประกอบการเชิง
ปัทสถานที่เป็นตัวเร่งปฏิกิริยาการเกิดและเปลี่ยนแปลงทางปัทสถาน กล่าวคือ ผู้ประกอบการ
เชิงปัทสถานมีอิทธิพลต่อการเกิดปัทสถานใหม่ได้เพียงใด เมื่อพิจารณาถึงสมมติฐานที่ว่า
ผู้ประกอบการเชิงปัทสถานสามารถมีอิทธิพลต่อการเกิดและเปลี่ยนแปลงปัทสถานได้แม้ว่า
ตัวแสดงดังกล่าวจะเข้าถึงประชาชนเพียงส่วนน้อยก็ตาม (Hoffmann, 2003) ดังนั้น ในส่วน
ต่อไปจึงมีจุดมุ่งหมายเพื่อชี้แจงสภาพการณ์ดังกล่าวโดยนำเสนอผ่านกรณีศึกษาปัทสถานด้าน
ความมั่นคงไซเบอร์โดยเฉพาะอย่างยิ่งกรณีของสหรัฐฯ

4. ตัวแสดงในฐานะผู้ประกอบการเชิงปัทสถานความมั่นคงไซเบอร์ของสหรัฐฯ

ในส่วนนี้ผู้เขียนจะนำกรณีศึกษาของความพยายามในการก่อสร้างและเปลี่ยนแปลง
ปัทสถานที่เกิดขึ้นโดยใช้ข้อมูลเชิงประจักษ์ในกรณีศึกษาปัทสถานความมั่นคงไซเบอร์ในแบบ

ตะวันตกโดยเฉพาะสหรัฐฯ ซึ่งถือเป็นรัฐแกนนำที่สำคัญตัวหนึ่ง เพื่ออธิบายถึงตัวแสดงซึ่งเป็นผู้ประกอบการเชิงปทัสถานนั้นมีหน้าที่ และอิทธิพลต่อการสร้างและการเปลี่ยนแปลงปทัสถานได้อย่างไร โดยใช้กรอบรูปแบบการศึกษาวิจัยจักรปทัสถานเพื่อแสดงให้เห็นถึงพลวัตที่เกิดขึ้นในบริบทความสัมพันธ์ระหว่างประเทศ ผู้เขียนแจกแจงลักษณะตัวแสดงที่เป็นผู้ประกอบการเชิงปทัสถานไว้ 3 ตัวแสดง ดังนี้ 1) สหรัฐฯ ในฐานะตัวกระทำการ 2) ผู้เชี่ยวชาญทางเทคนิค (Expert) 3) ตัวแสดงภาคเอกชน (Private Sector)

4.1 ตัวแสดงที่หนึ่ง บทบาทของสหรัฐฯ ในฐานะตัวกระทำการ

สหรัฐฯ ในฐานะรัฐแกนนำที่สำคัญ แม้ว่าจะไม่ใช่ผู้เสนอร่างปทัสถานความมั่นคงไซเบอร์เข้าสู่เวทีสหประชาชาติเป็นชาติแรก แต่สหรัฐฯ มีจุดยืนที่ชัดเจนในการแสดงความคิดเห็นต่อปทัสถานความมั่นคงไซเบอร์ที่รัสเซียเป็นผู้เสนอมาตั้งแต่ปี ค.ศ. 1998 ในชื่อ “Developments in the field of information and telecommunications in the context of international security”⁶ ซึ่งชื่อเรื่องดังกล่าวถูกใช้เป็นชื่อระเบียบวาระการประชุม (Agenda) ในสมัชชาใหญ่แห่งสหประชาชาติในหัวข้อซึ่งเกี่ยวกับความมั่นคงทางไซเบอร์มาจนถึงปัจจุบัน ในความหมายนี้ ชาติอื่นสามารถเสนอร่างต่อที่ประชุมสมัชชาใหญ่ในชื่ออื่นได้ แต่จะอยู่ในระเบียบวาระการประชุมในชื่อข้างต้นซึ่งสหรัฐฯ เป็นชาติแรกที่เสนอในชื่อที่แตกต่างกับรัสเซียเสนออย่างมีนัยสำคัญ

ข้อถกเถียงเกี่ยวกับประเด็นความมั่นคงไซเบอร์ถูกถกเถียงมาตั้งแต่ปี ค.ศ. 1998 จนถึง 2004 จุดเริ่มต้นที่น่าสนใจเมื่อรัสเซียเสนอร่างอย่างแข็งขันเพื่อเสนอให้ลงมติเห็นชอบต่อที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติในปี ค.ศ. 2005 แม้ผลการประชุมจะแสดงให้เห็นว่าร่างดังกล่าวของรัสเซียเป็นที่ยอมรับในเวลานั้น แต่สหรัฐฯ เป็นเพียงชาติเดียวที่โหวตไม่เห็นชอบซึ่งผู้เขียนจะอธิบายต่อไปในส่วนที่ 5 ทั้งนี้ สะท้อนให้เห็นจุดยืนที่น่าสนใจอย่างมากของสหรัฐฯ อนึ่ง ใจความสำคัญของร่างดังกล่าวของรัสเซีย คือ การตีความขอบเขตของอำนาจทางไซเบอร์ และการตีความว่าขอบเขตของการป้องกันทางไซเบอร์ควรมีเพียงใด (United Nations General Assembly, 1998)

⁶ ร่างของรัสเซียถูกเสนอต่อโดยตรงมาจาก เรื่อง “Role of science and technology in the context of security, disarmament and other related fields” ใจความสำคัญกล่าวถึง การสร้างความมั่นคงทางวิทยาศาสตร์ และ เทคโนโลยีในเชิงกายภาพ ดูใน A/53/576: Report / 1st Committee (United Nations General Assembly, 1998) ผู้เขียนตั้งข้อสังเกตว่า ข้อถกเถียงเรื่องดังกล่าวในสหประชาชาติสามารถพิจารณาได้ว่า เป็นปทัสถานเดิมที่ดำรงอยู่ซึ่งถูกท้าทายโดยรัสเซียได้เช่นเดียวกัน

อย่างไรก็ดี อีกกว่าทศวรรษนับตั้งแต่ร่างข้อมติที่เสนอโดยรัสเซียตั้งแต่ปี ค.ศ. 1998 สหรัฐฯ ได้ลงมติไม่เห็นชอบร่างของรัสเซียทั้งหมด 4 ครั้ง กระทั่งในปี ค.ศ. 2016 สหรัฐฯ ได้ออกเสียงเห็นชอบร่างดังกล่าวของรัสเซีย เนื่องจากสหรัฐฯ ในฐานะรัฐแกนนำที่สำคัญ ผ่านที่ประชุมระหว่างรัฐบาลในประเด็นเฉพาะด้านภายใต้สหประชาชาติ (United Nations Group of Governmental Experts: UNGGE)⁷ สามารถผลักดันให้ประเด็นความมั่นคงไซเบอร์ตีความในเรื่องความมั่นคงให้สอดคล้องกับกฎบัตรสหประชาชาติ (U.N. Charter) ในขอบเขตที่ครอบคลุมถึงการสร้างความมั่นคงและสงบสุขในขอบเขตของเทคโนโลยีสารสนเทศ (United Nations General Assembly, 2013, 2015) นอกจากนี้ ร่างฉบับดังกล่าวยังเป็นครั้งแรกที่สิทธิมนุษยชนถูกระบุเข้าเป็นส่วนหนึ่งของการตีความด้านความมั่นคงไซเบอร์ ซึ่งก่อนหน้านี้กล่าวถึงขอบเขตเพียงอาชญากรรมและการก่อการร้ายเท่านั้น สะท้อนให้เห็นถึงนัยสำคัญอีกชุดหนึ่งของสหรัฐฯ ในความพยายามแสดงบทบาทนำของค่านิยมด้านสิทธิมนุษยชน

ในขณะเดียวกัน ประเด็นความมั่นคงไซเบอร์ได้สร้างความคลุมเครือหลายประการในการตีความเพื่อนำไปใช้โดยเฉพาะอย่างยิ่งในมาตรการป้องกันตนเองของรัฐ ประการแรก มาตรา 2 วรรค 4 กล่าวถึง การห้ามคุกคามหรือการใช้กำลังต่อบุรณภาพแห่งดินแดนของรัฐใดๆ อย่างชัดเจน ยกเว้นเพื่อวัตถุประสงค์ในการป้องกันตนเองหรือเมื่อได้รับอนุญาตจากคณะมนตรีความมั่นคง ประการที่สอง กรณีสถาปัตยกรรมระหว่างประเทศ (International Court of Justice) ใช้กฎหมายจารีตระหว่างประเทศในการใช้กำลังอันชอบด้วยกฎหมาย กล่าวคือ จะต้องมีการโจมตีด้วยอาวุธหรือเทียบเท่ากับการโจมตีด้วยอาวุธ การโจมตีนั้นต้องมีเป้าหมายและสามารถระบุที่มาได้ เมื่อคุณลักษณะข้างต้นปรากฏ การใช้กำลังจะต้องเป็นทางเลือกสุดท้ายโดยพึงเล็งเห็นว่าจะประสบความสำเร็จในการป้องกัน และความเสียหายที่ก่อจะต้องได้สัดส่วนกับความเสียหายที่ได้รับ (United Nations, 2024, Article 2, Paragraph 4; O'Connell & Arimatsu, 2012) โจทย์สำคัญคือ การโจมตีทางไซเบอร์ (Cyber Attack) เป็นการใช้อำนาจหรือไม่ ซึ่งประเด็นดังกล่าวไม่มีการกล่าวถึงเป็นฉันทามติอย่างชัดเจน (Lotrionte, 2018) ส่งผลให้มาตรา 2 วรรค 4 ในกฎบัตรสหประชาชาติสามารถตีความได้ว่า กิจกรรมทางไซเบอร์ที่ส่งผลให้เกิดการสูญเสียชีวิต การบาดเจ็บหรือการทำลายล้างอย่างมีนัยสำคัญอาจถูก

⁷ UNGGE ถูกเสนอครั้งแรกโดยรัสเซียต่อที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติปี 2001 เพื่อร้องขอให้จัดการประชุมระหว่างรัฐบาลในประเด็นเฉพาะเรื่องการตีความด้านความมั่นคงไซเบอร์ซึ่งข้อสรุปของ UNGGE จะถูกเสนอต่อที่ประชุม UNGA ปี 2014 และ/หรือ ตามวาระที่ร้องขอ

พิจารณาได้ว่าเป็นการใช้กำลัง ประเทศต่างๆ มีสิทธิ์ตอบโต้การโจมตีทางไซเบอร์ตามมาตรการป้องกันตนเอง

ในปี ค.ศ. 2018 สหรัฐฯ พยายามมีเข้ามามีบทบาทนำมากขึ้นผ่านการเสนอร่างปทัสถานความมั่นคงของตัวเองภายใต้วาระการประชุมเดียวกัน แต่ในชื่อร่างที่แตกต่าง คือ “Advancing responsible State behavior in cyberspace in the context of international security” ร่างดังกล่าวของสหรัฐฯ มีความคล้ายคลึงร่างของรัสเซียดังนี้ ประการแรก สหรัฐฯ นำข้อสรุปที่ประชุม UNGGE 2013 เข้ามาประกอบใช้ภายในร่าง โดยสาระสำคัญ คือ การตีความให้สอดคล้องกับกฎบัตรสหประชาชาติ (United Nations General Assembly, 2013) ประการที่สอง สหรัฐฯ นำข้อสรุปที่ประชุม UNGGE 2015 เข้ามาประกอบใช้ภายในร่าง โดยสาระสำคัญ คือ การกำหนดพฤติกรรมและความรับผิดชอบของรัฐว่า สิ่งที่รัฐพึงกระทำและสิ่งที่รัฐไม่พึงกระทำ

ทั้งนี้ สหรัฐฯ สนับสนุนพฤติกรรมและความรับผิดชอบของรัฐ 8 ประการหลัก คือ

- 1) รัฐควรร่วมมือกันในการพัฒนาและใช้มาตรการเพื่อส่งเสริมเสถียรภาพและความปลอดภัยในการใช้เทคโนโลยีสารสนเทศเพื่อป้องกันเทคโนโลยีสารสนเทศที่เป็นอันตรายต่อระบบข้อมูล
- 2) รัฐควรใช้มาตรการที่เหมาะสมในการปกป้องโครงสร้างพื้นฐานที่สำคัญของตน
- 3) รัฐควรดำเนินการตามสมควรเพื่อให้มั่นใจถึงความต่อเนื่องของห่วงโซ่อุปทาน (Supply Chain)
- 4) รัฐควรร่วมมือกันในการดำเนินคดีการใช้เทคโนโลยีสารสนเทศของผู้ก่อการร้ายและอาชญากร
- 5) รัฐไม่ควรดำเนินการหรือสนับสนุนกิจกรรมที่เป็นอันตรายต่อระบบข้อมูลของหน่วยงานฉุกเฉินที่มีอำนาจรับผิดชอบ
- 6) รัฐไม่ควรใช้ทีมตอบโต้เหตุฉุกเฉินที่ได้รับอนุญาตในข้อ 5) เพื่อมีส่วนร่วมในกิจกรรมระหว่างประเทศที่เป็นอันตราย
- 7) รัฐไม่ควรยินยอมให้เขตแดนของรัฐถูกฟ้องในข้อหากระทำการโดยมิชอบโดยเจตนาจากการใช้เทคโนโลยีสารสนเทศ และควรตอบสนองเพื่อลดหรือยุติกิจกรรมทางเทคโนโลยีที่เป็นอันตรายดังกล่าว
- 8) รัฐไม่ควรดำเนินการหรือสนับสนุนกิจกรรมเทคโนโลยีสารสนเทศที่จงใจทำลายโครงสร้างพื้นฐานที่สำคัญ

ทั้งนี้ รัฐบาลสามารถกำหนด และนิยามว่าสิ่งใดอาจเป็นอันตราย หรือเป็นภัยต่อระบบข้อมูลของตนตามคำนิยามข้างต้นเองได้ เนื่องจากแนวปฏิบัติดังกล่าวเป็นเพียงคำแนะนำซึ่งไม่มีข้อบังคับทางกฎหมายระหว่างประเทศผูกมัด จึงเกิดเป็นคำถามว่า รัฐจะนำแนวทางเหล่านี้ไปปฏิบัติใช้ทางกฎหมายอย่างไร (United Nations General Assembly, 2015)

ในทางตรงกันข้าม ความแตกต่างอย่างชัดเจนของร่างที่สหรัฐฯ เสนอ ประการแรก มีการกล่าวถึงความร่วมมือระหว่างรัฐ (State Cooperation) และการดำเนินการร่วมกัน (Collective Action) ขึ้นเป็นครั้งแรก ประการที่สอง องค์กรภาคเอกชน องค์กรระหว่างประเทศ องค์กรการศึกษา และภาคประชาสังคมถูกระบุเข้ามาเป็นหนึ่งในผู้เกี่ยวข้องกับ

ปทัสถานความมั่นคงไซเบอร์ อาจกล่าวอีกนัยหนึ่งได้ว่า ตัวแสดงซึ่งเป็นผู้มีส่วนได้ส่วนเสียหลายฝ่าย (Multi-Stakeholder) ได้ถูกระบุเข้ามาในร่างปทัสถานความมั่นคงไซเบอร์เป็นครั้งแรกอย่างชัดเจน

ในขณะเดียวกัน รัสเซียได้เสนอต่อคณะกรรมการที่หนึ่งแห่งสหประชาชาติในปี ค.ศ. 2018 (UN First Committee) คณะกรรมการซึ่งเกี่ยวข้องกับการจำกัดอาวุธและความมั่นคงระหว่างประเทศของสหประชาชาติให้มีการจัดตั้งคณะทำงานปลายเปิด (Open-Ended Working Group: OEWG) เพื่อการตีความ และทำงานในด้านปทัสถานทางไซเบอร์ใหม่ (New Cyber Norms) ซึ่งแตกต่างจากที่ประชุม UNGGE เนื่องจาก OEWG ใหม่นี้จะเปิดให้ทุกสมาชิกในสหประชาชาติเข้ามามีส่วนร่วมในการประชุม สอดคล้องกับมติสมัชชาใหญ่แห่งสหประชาชาติในเรื่องความเป็นประชาธิปไตย การมีส่วนร่วม และความโปร่งใสที่มากขึ้น (United Nations General Assembly, 2018b) กลไก OEWG ดังกล่าวยังมีข้อเสนอให้เกิดการหารือเชิงสถาบันกับองค์กรที่เกี่ยวข้องซึ่งอาจมีข้อเสนอหรืออธิบายรายละเอียดเพิ่มเติมเกี่ยวกับความเปลี่ยนแปลงที่เกิดขึ้นในระดับจุลภาคในแต่ละพื้นที่ได้ (United Nations General Assembly, 2018a)

อย่างไรก็ตาม สหรัฐฯ ได้ระบุให้มีการจัดการประชุมแบบไม่เป็นทางการในการปรึกษาหารือขึ้น (Informal Consultative) ล่วงหน้า 2 วัน ก่อนที่จะมีการประชุมคณะทำงานปลายเปิดทุกครั้งในประเด็นดังกล่าว เพื่อตรวจสอบว่านานาชาติมีการนำกรอบความมั่นคงไซเบอร์ไปปรับใช้ภายในประเทศอย่างไร (United Nations General Assembly, 2018b) ซึ่งพิจารณาได้ว่า กลไกดังกล่าวที่สหรัฐฯ เสนอในร่างเป็นการต่อต้าน และตรวจสอบการทำงานของรัสเซีย อย่างไรก็ตาม การแบ่งแยกกระบวนการและกลไกซึ่งเป็นเรื่องเดียวกันจะทำให้เกิดความซับซ้อนและความขัดแย้งกันมากขึ้น

อย่างไรก็ตาม หนึ่งในคำถามชุดใหญ่ที่ตามมาหลังจากการกำหนดปทัสถานความมั่นคงไซเบอร์ดังกล่าวเกิดขึ้น คือ กฎหมายระหว่างประเทศควรจะต้องบังคับใช้อย่างไรกับการใช้เทคโนโลยีสารสนเทศของรัฐ แม้ว่าการประชุม UNGA 2016 จะสร้างความเชื่อมโยงทางกฎหมายระหว่างประเทศที่มากขึ้นจากการตีความให้สอดคล้องกับกฎบัตรสหประชาชาติ และดูเหมือนจะเกิดเป็นแนวทางเชิงรูปธรรมมากขึ้นถึงการกำหนดพฤติกรรมของรัฐจากข้อสรุปที่ประชุม UNGGE 2015 แล้วก็ตาม แต่ไม่ได้ระบุถึงวิธีการนำมาใช้แต่อย่างใด

ผู้เขียนจะยกกรณีที่ถูกกล่าวถึงบ่อยครั้งในงานศึกษาพัฒนาการปทัสถานทางไซเบอร์ คือ มาตรา 51 แห่งกฎบัตรสหประชาชาติ เรื่องการตีความเรื่องสิทธิการป้องกันตนเอง (Self-Defense) จากการถูกโจมตีด้วยอาวุธ (Armed Attack) สหรัฐฯ มีข้อเสนอว่า กฎบัตรมาตรา 51 ดังกล่าวควรนำมาปรับใช้และชี้เฉพาะในกรณีพื้นที่ไซเบอร์รวมถึงสิทธิในการตอบโต้ด้วย

มาตรการตอบโต้ที่เกี่ยวข้องกับข้อบัญญัติดังกล่าว และนัยเชื่อมโยงเกี่ยวกับกฎหมายสิทธิมนุษยชน (Sukumar, 2017) อย่างไรก็ตาม รัฐสมาชิกอื่นโดยเฉพาะอย่างยิ่งคิวบาให้ความเห็นขัดแย้งว่า ข้อเสนอของสหรัฐฯ ไม่อาจยอมรับได้เนื่องจากเมื่อพิจารณาถึง “การโจมตีด้วยอาวุธ” ในขอบเขตของเทคโนโลยีสารสนเทศแล้วนั้นจะเกิดความอสมมาตรขึ้นในพื้นที่ไซเบอร์ กล่าวคือ ความกลัวต่อสิทธิของการป้องกันตนเองจะเกิดขึ้นอย่างอสมมาตรต่อตัวแสดงที่มีอำนาจที่เหนือกว่าศัตรูในพื้นที่ไซเบอร์ (Rodriguez, 2017) ผู้เขียนตั้งข้อสังเกตว่า ความกังวลดังกล่าวเกิดขึ้นเนื่องจากชาติตะวันตกมีบทบาทนำในการประกอบสร้างปทัสสถานและควบคุมทางไซเบอร์จำนวนมากโดยเฉพาะอย่างยิ่งสหรัฐฯ และชาติพันธมิตร นอกจากนี้ ความพยายามในการบังคับใช้กฎหมายสิทธิมนุษยชนระหว่างประเทศกับพื้นที่ไซเบอร์เป็นประเด็นขัดแย้งเช่นเดียวกัน เนื่องจากบรรทัดฐานของการทำสงครามในอนุสัญญาเจนีวา 1949 (International Committee of the Red Cross, 1949) กำหนดให้มีการแบ่งแยกระหว่าง พลเรือนและกำลังรบ (Combatants) ว่า พลเรือนไม่ควรเป็นเป้าหมายของการโจมตี ซึ่งในใจความนี้นำไปใช้กับเรื่องพื้นที่ไซเบอร์ได้ยากเนื่องจากโครงสร้างพื้นฐานทางไซเบอร์โดยเฉพาะอย่างยิ่งเมื่ออินเทอร์เน็ตสามารถนำไปใช้ได้ทั้งวัตถุประสงค์ทางทหารและพลเรือน

จากข้อถกเถียงข้างต้นสะท้อนให้เห็นถึงข้อจำกัดเรื่องค่านิยม (Value) และผลประโยชน์ ซึ่งสะท้อนให้เห็นว่าประเด็นความมั่นคงไซเบอร์ไม่ใช่เพียงเรื่องความมั่นคงเพียงอย่างเดียว แต่ยังควรพิจารณาไปถึงวิธีการควบคุมการใช้งานอินเทอร์เน็ตโดยทั่วไปด้วย เนื่องจากประชาชนมีส่วนเกี่ยวข้องอย่างมีนัยสำคัญ

สหรัฐฯ พยายามแสดงบทบาทอย่างแข็งขันผ่านที่ประชุมสมัชชาสหประชาชาติ รวมถึง UNGGE และ OEWG ซึ่งเป็นกลไกในการปรึกษาหารือระหว่างผู้เชี่ยวชาญและรัฐบาล และผ่านการผลักดันให้มีมติเห็นชอบในที่ประชุม UNGA ทั้งปี ค.ศ. 2019, 2020 และ 2022 ทั้งนี้ การลงมติทั้ง 3 ครั้งดังกล่าวมีสมาชิกลงมติเห็นชอบมากกว่าร่างของรัสเซียเรื่อยมา โดยเฉพาะอย่างยิ่งรัสเซียสูญเสียพื้นที่ในการแสดงบทบาทในฐานะรัฐแกนนำอย่างมีนัยสำคัญ ซึ่งจะกล่าวต่อไปในส่วนที่ 5

อนึ่ง ในปี ค.ศ. 2020 เป็นต้นมา ร่างปทัสสถานความมั่นคงไซเบอร์ของสหรัฐฯ ได้เน้นย้ำถึงขอบเขตของพื้นที่ทางไซเบอร์ในยุคโควิด 19 (COVID-19) (United Nations General Assembly, 2020) อย่างไรก็ตาม ในปี ค.ศ. 2022 ถึงแม้ว่าสหรัฐฯ จะไม่ได้เสนอร่างข้อมติใหม่ของตนอย่างชัดเจน แต่ก็ได้แสดงบทบาทสำคัญต่อการผลักดันในนามของสหรัฐฯ (On Behalf) ต่อร่างข้อมติของพันธมิตรอย่างฝรั่งเศสเพื่อเสนอร่างในปี ค.ศ. 2022 ต่อที่ประชุม UNGA ในชื่อ “Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international

security” เพื่อผลักดันเรื่องความหลากหลายทางเพศ “gender digital divide” โดยเฉพาะบทบาทของสตรีในฐานะตัวแสดงในกระบวนการตัดสินใจทางนโยบายเกี่ยวกับไซเบอร์ (Decision-Making Processes) (United Nations General Assembly, 2022)

จะเห็นได้ว่า สหรัฐฯ ได้แสดงบทบาทในฐานะรัฐแกนนำที่สำคัญภายใต้องค์การระหว่างประเทศ โดยพยายามกำหนดแนวปฏิบัติขึ้นให้แก่รัฐสมาชิก ซึ่ง Margaret and Sikkink (1998) อธิบายว่า รัฐแกนนำดังกล่าวมีความสำคัญอย่างมากในการเสนอที่สถานใหม่เข้าสู่องค์การระหว่างรัฐเพื่อให้เกิดข้อถกเถียงทางที่สถานขึ้น และนำไปสู่ข้อตกลงในแนวทางปฏิบัติแบบใหม่ร่วมกัน ซึ่งกระบวนการนี้ คือ กระบวนการเกิดขึ้นของที่สถานในความสัมพันธ์ระหว่างประเทศ อย่างไรก็ตาม นักคิดสำนักสรรค์สร้างนิยมอธิบายไว้ว่า การเปลี่ยนแปลงของที่สถานระหว่างประเทศจะถูกพิจารณาโดยรัฐในฐานะตัวแสดงที่มีเหตุผลเนื่องจากรัฐจะเลือกปฏิบัติตามที่สถานที่ตนเห็นว่าเหมาะสม สิ่งใดที่ตนไม่ยอมรับแนวปฏิบัติเหล่านั้นก็จะถูกกีดขวางและสูญสลายไป (Katzenstein, 1996; Kratochwil, 1989)

4.2 ตัวแสดงที่สอง ผู้ประกอบการเชิงที่สถานที่เป็นผู้เชี่ยวชาญทางเทคนิค โดยเฉพาะอย่างยิ่งด้านเทคโนโลยีสารสนเทศ และอินเทอร์เน็ต

ในส่วนนี้จะกล่าวถึงองค์กรด้านเทคนิคของสหรัฐฯ ซึ่งเป็นส่วนหนึ่งของที่สถานทางไซเบอร์แบบผู้มีส่วนได้ส่วนเสียหลายฝ่าย องค์กรซึ่งดำรงอยู่เพื่อเสริมสร้างอินเทอร์เน็ตในฐานะโครงสร้างพื้นฐานสำคัญทางไซเบอร์ หนึ่ง องค์กรคณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (Internet Engineering Task Force: IETF) องค์กรรัฐบาลกลางแห่งสหรัฐฯ ซึ่งมีหน้าที่กำหนดมาตรฐานโพรโทคอล (Protocol) สำหรับการทำงานของอินเทอร์เน็ต เช่น IP address (Internet Protocol Address) หรือที่รู้จักว่าเป็นหมายเลขประจำเครื่องคอมพิวเตอร์ เป็นต้น หนึ่ง องค์กร IETF มีหน้าที่ทำให้อินเทอร์เน็ตทำงานได้ดีขึ้นโดยการผลิตเอกสารทางเทคนิคระดับสูงที่เกี่ยวข้องซึ่งมีอิทธิพลต่อวิธีที่ผู้คนหรือวิศวกรใช้ออกแบบและจัดการอินเทอร์เน็ต (Internet Engineering Task Force, 2023) เช่นเดียวกับสถาบันวิชาชีพวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers) โดยในส่วนที่รับผิดชอบอย่างกว้างขวาง คือ ผู้สถาบันผู้กำหนดมาตรฐานสำหรับ Wi-Fi และเวิลด์ไวด์เว็บคอนซอร์เทียม (World Wide Web Consortium: W3C) ซึ่งรับผิดชอบในการพัฒนามาตรฐานทางเทคนิคสำหรับเว็บไซต์

แม้องค์กรดังกล่าวข้างต้นอาจยากต่อการทำความเข้าใจในคำอธิบายเชิงเทคนิค และอาจจะมีบทบาทไม่มากนักในกระบวนการสร้างที่สถาน อย่างไรก็ตาม นักวิชาการได้อธิบายไว้ว่า การแข่งขันกันเพื่อให้ได้มาซึ่งการควบคุมข้อมูลออนไลน์นั้นมักเกิดขึ้นในระดับของโครงสร้าง

พื้นฐานของอินเทอร์เน็ต ซึ่งการแจกแจงและจัดสรรโครงสร้างทางเทคนิคเหล่านั้นก็ถือเป็นการจัดสรรทางอำนาจด้วย (Denardis, 2012, p. 720) กล่าวอีกนัยหนึ่ง การตัดสินใจของวิศวกรเกี่ยวกับอินเทอร์เน็ตย่อมส่งผลโดยตรงนโยบายทางสังคม เศรษฐกิจ และความมั่นคงของรัฐ เช่น วิศวกรสามารถเลือกได้ว่าจะออกแบบสถาปัตยกรรมทางอินเทอร์เน็ตให้ระบบการป้องกันข้อมูลส่วนบุคคลหรือไม่ก็ได้ อาทิ การเข้ารหัส ซึ่งผลลัพธ์ดังกล่าวส่งผลต่อความปลอดภัยในงานออกแบบส่งผลกระทบต่อมาตรฐานในการออกแบบและนโยบายประเทศผู้ใช้สถาปัตยกรรมทางอินเทอร์เน็ตนั้น อาจกล่าวได้ว่า มาตรฐานทางเทคนิคที่วิศวกรกำหนดสามารถส่งผลกระทบต่อสมดุลทางอำนาจระหว่างประชาชนและรัฐบาลได้ กล่าวคือ หากวิศวกรมีข้อกำหนดทางเทคนิคที่สนับสนุนขีดความสามารถของรัฐบาลในการปิดกั้น ตรวจสอบ ปลอมแปลงหรือสามารถสอดส่องความเคลื่อนไหวของข้อมูลสาธารณะได้ เช่นนั้นย่อมส่งผลกระทบต่อกระแสทางการเมืองอย่างมีนัยสำคัญ นอกจากนี้ โครงสร้างขององค์กร แหล่งทุน และผู้มีอิทธิพลในองค์กรของหน่วยงานด้านเทคนิคเหล่านี้ยังสะท้อนถึงค่านิยมเฉพาะด้วย กล่าวคือ หลักการสำคัญขององค์กร IETF คือ เป็นองค์กรเปิด หมายความว่า เป็นองค์กรที่เปิดกว้างสำหรับทุกคนในการตรวจสอบ โปร่งใส กระบวนทัศน์ดังกล่าวส่งผลต่อภาพลักษณ์ของมาตรฐานอินเทอร์เน็ต คือ การทำงานร่วมกันของผู้มีส่วนได้ส่วนเสียหลายฝ่ายจากล่างขึ้นบน ในทางตรงกันข้ามเมื่อองค์กรผู้กำหนดมาตรฐานทางเทคนิคมีลักษณะไม่โปร่งใส ปิดกั้นข้อมูลหรือควบคุมทางเทคนิคโดยตัวแสดงหรือกลุ่มตัวแสดงใดตัวแสดงหนึ่ง ย่อมสะท้อนถึงกระบวนทัศน์ของการกำกับควบคุมโดยไม่เน้นกิจกรรมที่มีส่วนร่วมจากส่วนล่างแต่เป็นลักษณะของบนลงล่าง

นอกจากนี้ ตัวอย่างสำคัญที่นักวิชาการด้านความมั่นคงไซเบอร์มักกล่าวถึง คือ คู่มือทาลลินน์ (Tallinn Manuals) ในปี ค.ศ. 2013 และ 2017 ถูกออกแบบโดยกลุ่มผู้เชี่ยวชาญทางเทคนิคระหว่างประเทศในนามของ NATO (Schmitt, 2013, 2017) สำคัญของคู่มือนี้เพื่อเป็นข้อเสนอทางกฎหมายระหว่างประเทศในพื้นที่ไซเบอร์ต่อองค์กรที่เกี่ยวข้องทางด้านความมั่นคงไซเบอร์ ประเด็นแรก อธิบายการบังคับใช้กฎหมายระหว่างประเทศกับพื้นที่ไซเบอร์ในช่วงที่เกิดความขัดแย้งขึ้น ประเด็นที่สอง อธิบายถึงการปฏิบัติทางไซเบอร์โดยทั่วไปซึ่งไม่ได้ถึงระดับการใช้กำลัง คู่มือทาลลินน์ระบุชัดเจนว่า การดำเนินการทางไซเบอร์ไม่ได้เกิดขึ้นมาอย่างไรกฎหมายควบคุม หรืออย่างน้อยที่สุดเพื่อเน้นย้ำว่า กฎหมายระหว่างประเทศที่มีอยู่สามารถ/และควรนำไปใช้กับพื้นที่ไซเบอร์ เช่น คู่มือทาลลินน์ 2.0 (Tallinn Manual 2.0) ซึ่งอ้างอิงสนธิสัญญาและกฎหมายกรณีต่างๆ หลายฉบับมาปรับใช้ในประเด็นความมั่นคงไซเบอร์เนื้อหาสำคัญโดยเฉพาะความสอดคล้องกับ กฎบัตรสหประชาชาติมาตรา 4 ว่าด้วยหลักการไม่รุกรานโดยล่อกับกฎบัตรสหประชาชาติว่า รัฐต้องไม่ดำเนินการทางไซเบอร์ที่ละเมิดอำนาจอธิปไตยของอีกรัฐหนึ่ง (Schmitt, 2017)

กล่าวโดยสรุป ผู้ประกอบการเชิงปทัสสถานที่เป็นผู้เชี่ยวชาญที่ไม่ใช่รัฐ นัยหนึ่งอาจกล่าวได้ว่าเป็นวิศวกรผู้รับผิดชอบงานออกแบบทางเทคนิค ผู้เขียนใคร่ย้ำว่า ตัวแสดงดังกล่าวถูกพิจารณาว่าเป็นผู้ประกอบการเชิงปทัสสถาน เนื่องจากปทัสสถานทางไซเบอร์ที่ดำรงอยู่ในปัจจุบันให้ความสำคัญกับตัวแสดงที่มีส่วนได้ส่วนเสียหลายฝ่าย ดังนั้น ตัวแสดงในฐานะผู้ให้คำปรึกษาทางเทคนิคจึงถูกพิจารณาว่าเป็นผู้ประกอบการเชิงปทัสสถานซึ่งผู้ประกอบการเชิงปทัสสถานที่เป็นผู้เชี่ยวชาญเหล่านี้มีบทบาทต่อการถกเถียงทางปทัสสถาน กล่าวคือ ควบคู่ไปกับการถกเถียงระหว่างตัวแสดงในองค์การระหว่างรัฐซึ่งผู้เชี่ยวชาญจะโน้มน้าวตัวแสดงซึ่งเป็นสมาชิกในองค์การระหว่างรัฐเพื่อให้ข้อมูลประกอบการตัดสินใจ ดังตัวอย่างข้างต้น หากผู้เชี่ยวชาญเสนอให้สถาปัตยกรรมทางอินเทอร์เน็ตใดเป็นภัยต่อความมั่นคง สถาปัตยกรรมนั้นก็จะถูกรัฐพิจารณาว่า อาจเป็นภัยหากรัฐเชื่อตามคำโน้มน้าวดังกล่าวของผู้เชี่ยวชาญ ขณะเดียวกัน ปทัสสถานที่ถูกยอมรับจนเข้าสู่ระยะที่ 2 การแพร่กระจายของปทัสสถาน ปทัสสถานซึ่งไม่ถูกตั้งคำถามหรือถูกตั้งคำถามน้อยนั้นผู้เชี่ยวชาญก็จะเป็นตัวแสดงที่สำคัญในการทำทายทางปทัสสถาน เช่น ความเชื่อเรื่องโลกแบนซึ่งแพร่กระจายอยู่ในยุคเก่านั้นได้ถูกตั้งคำถามด้วยเหตุผลทางวิทยาศาสตร์ ส่งผลให้เกิดข้อเสนอว่าโลกกลมนำไปสู่ความพยายามในการศึกษาและพิสูจน์เพื่อโน้มน้าวให้เกิดความเชื่อต่อข้อเสนอของนักวิชาการในยุคนั้นว่าโลกนั้นกลมในเวลาต่อมา เป็นต้น แสดงให้เห็นว่า การโน้มน้าวของผู้ประกอบการเชิงปทัสสถานที่เป็นผู้เชี่ยวชาญที่ไม่ใช่รัฐนั้นมีอิทธิพลอย่างมากต่อกระบวนการเกิดและการเปลี่ยนแปลงปทัสสถานในระยะที่ 2 ของวัฏจักรปทัสสถาน

4.3 ตัวแสดงที่สาม ผู้ประกอบการเชิงปทัสสถานที่เป็นตัวแสดงภาคเอกชน

ตัวแสดงภาคเอกชนมีความเกี่ยวข้องอย่างมากในฐานะผู้ประกอบการเชิงปทัสสถานที่มีบทบาทสำคัญในการสร้างและเปลี่ยนแปลงปทัสสถานโดยเฉพาะอย่างยิ่งปทัสสถานด้านความมั่นคงไซเบอร์ บริษัทผู้ให้บริการพื้นฐานทางเทคโนโลยี เช่น เครื่องมือค้นหาออนไลน์ต่างๆ (Search Engines) โซเชียลมีเดีย อีคอมเมิร์ซ (E-Commerce) เป็นต้น อย่างไรก็ตาม บริษัทเอกชนของสหรัฐฯ ที่เกี่ยวข้องดังกล่าวจำนวนมากล้มเหลวในการปกป้องข้อมูลและผลประโยชน์ของผู้บริโภค ตั้งแต่การละเมิดข้อมูลส่วนตัวของผู้ใช้ไปจนถึงการเผยแพร่ข่าวเท็จหรือปล่อยให้ตกเป็นเครื่องมือของรัฐใช้เพื่อจุดประสงค์ในการสอดแนมแม่ในประเทศที่มีรูปแบบการปกครองแบบประชาธิปไตย เช่น กรณีโครงการ PRISM ซึ่งดำเนินงานอย่างผิดกฎหมายโดยสำนักงานความมั่นคงแห่งชาติสหรัฐฯ (U.S. National Security Agency: NSA) ซึ่งถูกเปิดเผยโดย เอ็ดเวิร์ด สโนว์เดน (Edward Snowden) เป็นต้น

อย่างไรก็ตาม ข้อเท็จจริงเหล่านี้แสดงให้เห็นถึงความไม่สอดคล้องกันของพฤติกรรมในทางปฏิบัติกับการแพร่กระจายปทัสถานทางไซเบอร์ในกรอบเสรี มีอิสระ เปิดเผย และรัฐไม่ควรเข้ามาแทรกแซงการเคลื่อนไหวของข้อมูล ซึ่งสิ่งนี้อาจทำให้การแพร่กระจายปทัสถานของสหรัฐฯ ไม่ประสบความสำเร็จ เนื่องจาก ผู้ประกอบการเชิงปทัสถานควรเป็นแบบอย่างที่ดีในการปฏิบัติตามปทัสถานที่ตนเองเป็นผู้สนับสนุน ดังเช่นที่ John Braithwaite (1994) อธิบายว่า การแพร่กระจายปทัสถานจะมีประสิทธิภาพ และมีพลังอำนาจในการโน้มน้าวได้ ผู้ประกอบการเชิงปทัสถานควรเป็นตัวแทนที่ดี (Modelling) เพื่อแสดงให้เห็นถึงความสำเร็จทางปทัสถาน

บริบทเหล่านี้ทำให้เกิดความคาดหวังที่เพิ่มขึ้นของรัฐบาลเกี่ยวกับความรับผิดชอบของตัวแสดงภาคเอกชนส่งผลให้บางบริษัทต้องรับหน้าที่ที่มากขึ้นในพื้นที่ไซเบอร์ อย่างไรก็ตาม ตัวแสดงภาคเอกชนเหล่านี้มีแรงจูงใจของตนเองในการทำหน้าที่เป็นผู้ประกอบการเชิงปทัสถานเนื่องจากผลประโยชน์ทางธุรกิจ กล่าวคือ การละเมิดความปลอดภัยและการคุ้มครองข้อมูลส่วนตัวที่มีการเผยแพร่ นั้นอาจส่งผลเสียต่อความเชื่อมั่นและชื่อเสียงของบริษัทซึ่งส่งผลต่อการตลาดและผลกำไร Deitelhoff and Wolf (2013) อธิบายว่า ชุดความคิดของผู้ประกอบการเชิงปทัสถานที่เป็นเอกชนมักถูกขับเคลื่อนโดยการคำนวณอย่างมีเหตุผลในกรอบของผลประโยชน์ทางธุรกิจ ประเด็นสำคัญประการหนึ่ง คือ ตัวแสดงเอกชนมักจะแสวงหาความชอบธรรมในการดำเนินกิจกรรมทางปทัสถาน กล่าวคือ ผู้ประกอบการเชิงปทัสถานโดยเฉพาะภาคเอกชนมักโน้มน้าวและส่งออกแนวคิดทางปทัสถานหนึ่งโดยคำนึงถึงผลประโยชน์เชิงธุรกิจมากกว่าการโน้มน้าวให้เกิดการเปลี่ยนแปลงทางปทัสถานที่มีนัยโดยตรง ตัวแสดงดังกล่าวจะมีกระบวนการปรับปรุง (Modification Process) สารของปทัสถานเพื่อให้สามารถเป็นที่ยอมรับได้ง่ายในสังคมที่ตนดำรงอยู่ด้วยเหตุผลทางธุรกิจ เช่น Microsoft ได้มีส่วนเกี่ยวข้องโดยตรงกับการสร้างปทัสถานซึ่งจะเป็นบริษัทแรกที่มีบทบาทในฐานะตัวแสดงทางการเมืองและการทูต (Hurel & Lobato, 2018) จากกรณี NSA ที่ได้กล่าวไปข้างต้น Microsoft ซึ่งเป็นคู่เจรจายแรกกับ NSA ในโครงการ PRISM ส่งผลให้บริษัท Microsoft ถูกวิจารณ์อย่างหนักในฐานะผู้เกี่ยวข้องโดยตรง ก่อให้เกิดแรงจูงใจอย่างมากที่จะผลักดันปทัสถานความมั่นคงทางไซเบอร์ที่เข้มงวดมากขึ้นเพื่อหยุดข้อวิพากษ์วิจารณ์และสร้างความเชื่อมั่นให้แก่บริษัทอีกครั้งหนึ่ง

บทบาทสำคัญของบริษัทผู้นำทางเทคโนโลยีอย่าง Microsoft ของสหรัฐฯ โดดเด่นอย่างมากในการแพร่กระจายปทัสถานทางไซเบอร์อย่างมีนัยสำคัญ ข้อเท็จจริงจากที่ประชุมธุรกิจด้านความมั่นคงระหว่างประเทศปี ค.ศ. 2017 บริษัท Microsoft ได้กล่าวสาระสำคัญถึงความจำเป็นที่รัฐบาลทั่วโลกจะต้องรวมตัวกันเพื่อจัดทำอนุสัญญาเจเนวาสำหรับดิจิทัล

(the Digital Geneva Convention) เพื่อปกป้องพลเรือนบนพื้นที่อินเทอร์เน็ต (Smith, 2017) ส่งผลให้ในปีต่อมาแนวคิดนี้ถูกกล่าวยกขึ้นมาเป็นประเด็นสำคัญในข้อตกลงเพื่อความมั่นคงโลกไซเบอร์ร่วมกัน (Cybersecurity Tech Accord, 2023) ซึ่งเป็นการลงนามโดยบริษัทเทคโนโลยีชั้นนำระดับโลกในข้อตกลงเรื่องการปรับปรุงความมั่นคงไซเบอร์ เช่น Apple, Google, Twitter, Facebook, Cisco และ Microsoft เป็นต้น

นอกจากนี้ ผู้ประกอบการเชิงปทัสสถานที่เป็นตัวแสดงภาคเอกชนอาจถูกพิจารณาอีกนัยหนึ่งว่า เป็นตัวแสดงเชิงปทัสสถานที่เป็นผู้เชี่ยวชาญได้เช่นเดียวกัน แต่หากเพียงดำเนินการในฐานะตัวแสดงที่เป็นองค์กรเอกชน กล่าวคือ เป็นกลุ่มก้อนของผู้เชี่ยวชาญเพื่อเพิ่มความเชื่อถือให้กับการโน้มน้าวของผู้เชี่ยวชาญเหล่านั้นโดยจะดำเนินการในฐานะองค์กร เช่นเดียวกับตัวแสดงที่เป็นผู้เชี่ยวชาญซึ่งมีบทบาทและอิทธิพลต่อการเกิดและเปลี่ยนแปลงปทัสสถานจากการโน้มน้าวตัวแสดงที่มีอำนาจโดยเฉพาะอย่างยิ่งรัฐ อย่างไรก็ตาม การศึกษาของ Acharya (2004) ชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสสถานที่เป็นตัวแสดงภาคเอกชนมีความสำคัญอย่างมากในวัฏจักรปทัสสถานระยะที่ 3 กระบวนการนำเอาปทัสสถานของรัฐหรือตัวแสดงของรัฐยอมรับเพื่อนำมาปฏิบัติภายในประเทศ ซึ่งตัวแสดงภาคเอกชนเป็นตัวแสดงหลักสำคัญในการโน้มน้าวรัฐและประชาชนภายในรัฐให้ยอมรับการปฏิบัติปทัสสถานนั้น ผู้เขียนตั้งข้อสังเกตว่า หากปทัสสถานที่เกิดขึ้นในระยะที่ 1 ของวัฏจักรปทัสสถานไม่สามารถเปลี่ยนเข้าสู่ระยะที่ 2 ในการนี้อาจทำให้เกิดช่องว่างของกระบวนการนำเอาปทัสสถานมาปฏิบัติภายในประเทศและนำไปสู่ความล้มเหลวในทางปฏิบัติที่สอดคล้องกับปทัสสถานที่ถูกสร้างขึ้นภายนอกประเทศ (องค์การระหว่างประเทศ)

จะเห็นได้ว่าผู้ประกอบการเชิงปทัสสถานมีความพยายามในการสร้างปทัสสถานความมั่นคงไซเบอร์ซ้อนทับอยู่หลายระดับ อย่างไรก็ตาม ในระยะการเกิดขึ้นของปทัสสถานเป็นสิ่งที่เกิดขึ้นได้ไม่ยากเมื่อเทียบกับระยะที่ 2 และ 3 ในวัฏจักรปทัสสถาน และเป็นการยากที่จะตรวจสอบว่าปทัสสถานหนึ่งมาถึงจุดเปลี่ยนทางปทัสสถานในระยะที่ 2 ได้อย่างไร Deitelhoff and Zimmermann (2019) อธิบายว่า ปทัสสถานที่เกิดขึ้นใหม่นั้นถูกสร้างขึ้นจากบริบทการแข่งขันเชิงปทัสสถานที่สูง ไม่ใช่เกิดขึ้นมาจากสุญญากาศซึ่งปทัสสถานใหม่เหล่านั้นสามารถอ่อนกำลังลงได้จากการถูกตั้งคำถามโดยปทัสสถานที่ดำรงอยู่ว่า ปทัสสถานใหม่นั้นชอบธรรมหรือไม่ เมื่อพิจารณาถึงการเกิดขึ้นและเปลี่ยนแปลงเชิงปทัสสถานความมั่นคงไซเบอร์ข้างต้นจะเห็นได้ว่าปทัสสถานยังคงอยู่ในระยะที่ 1 ระยะของการเกิดขึ้นของปทัสสถานซึ่งมีลักษณะสำคัญคือ การถกเถียงกันระหว่างตัวแสดงถึงความชอบธรรม ผู้ประกอบการเชิงปทัสสถานหลายกลุ่มพยายามโน้มน้าวและนำเสนอปทัสสถานให้กับตัวแสดงในเวทีระหว่างประเทศเพื่อให้เกิดจุดเปลี่ยนและเกิดกระบวนการนำเข้าสู่ระยะที่ 3 ให้เป็นเรื่องภายใน คำอธิบายในส่วนนี้ข้างต้น

ผู้เขียนต้องการแสดงให้เห็นว่า ปทัสถานความมั่นคงไซเบอร์ยังคงเป็นที่ถกเถียงและยังไม่เป็นที่ยอมรับโดยทั่วกันอย่างแท้จริง หรืออย่างน้อยที่สุดก็เป็นเพียงกระแสปกติที่มีนัยสำคัญบางประการซึ่งนำโดยชาติตะวันตก เมื่อปทัสถานถูกสร้างขึ้นและเกิดการถกเถียงแต่ยังไม่เกิดข้อสรุปหรือตกลง ย่อมส่งผลต่อวัฏจักรในระยะที่ 2 และ 3 ซึ่งก่อให้เกิดช่องว่างในการตีความทางปทัสถานให้กับตัวแสดงภายในประเทศสำหรับการทำให้เป็นเรื่องภายในประเทศ

5. ประเมินความสำเร็จในการแพร่กระจายปทัสถานความมั่นคงไซเบอร์ของสหรัฐฯ

ปทัสถานความมั่นคงไซเบอร์และผู้ประกอบการเชิงปทัสถานที่ผู้เขียนได้แจกแจงไว้ข้างต้นนั้น แสดงให้เห็นว่า ปทัสถานทางไซเบอร์ดังกล่าวยังคงเป็นที่ถกเถียงกันอย่างกว้างขวางทั้งในองค์การระหว่างประเทศ ในหมู่ผู้เชี่ยวชาญด้านเทคนิค และในองค์กรภาคเอกชน ผู้เขียนมีข้อสรุปว่า ปทัสถานความมั่นคงทางไซเบอร์นั้นยังคงดำเนินอยู่ในวัฏจักรปทัสถานในระยะที่ 1 คือ ช่วงการเกิดขึ้นของปทัสถาน เนื่องจากปทัสถานใหม่นี้ไม่ถูกยอมรับโดยทั่วไปหรือเกิดเป็นกระแสปกติอันเป็นที่ยอมรับอย่างกว้างขวางเพื่อเข้าสู่กระบวนการในระยะการแพร่กระจายของปทัสถานตามรูปแบบของ Finnemore and Sikkink (1998) อย่างไรก็ตาม ปทัสถานความมั่นคงทางไซเบอร์ก็ถูกยอมรับในบางส่วนดังที่ยกตัวอย่างถึงการประชุมต่างๆ ในระดับองค์การระหว่างรัฐบาล คำถามสำคัญ คือ จะใช้เกณฑ์หรือตัวชี้วัดใดในการพิจารณาว่าปทัสถานใหม่ (ความมั่นคงไซเบอร์) เป็นที่ยอมรับอย่างกว้างขวางจนเข้าสู่กระบวนการแพร่กระจายของปทัสถานในระยะที่ 2

ในส่วนของผู้พื้นที่ไซเบอร์นั้นมีความพยายามโดยรัสเซียในการเสนอมาตรฐานเรื่อง การพัฒนาด้านข้อมูลและโทรคมนาคมในบริบทของความมั่นคงระหว่างประเทศ (Developments in the field of information and telecommunications in the context of international security) ตั้งแต่ปี ค.ศ. 1998 ซึ่งถือได้ว่า ปทัสถานใหม่เริ่มกลายมาเป็นประเด็นที่ได้รับความสนใจในเวทีระหว่างประเทศ จนถึงปี ค.ศ. 2005 รัสเซียมีความแข่งขันในการผลักดันมาตรฐานที่ตนเองเสนอมาโดยตลอดผ่านเวทีสหประชาชาติ ซึ่งมีการลงประชามติ 9 ครั้ง โดย 4 ครั้งแรกสหรัฐฯ ลงมติไม่เห็นชอบ แต่ในปี ค.ศ. 2016 เริ่มมีความเห็นสอดคล้องในประเด็นสิทธิมนุษยชน และคำแนะนำสำหรับกำหนดพฤติกรรมของรัฐบาลว่า สิ่งใดควรหรือไม่ควรทำ อย่างไรก็ตาม ในปี ค.ศ. 2018 สหรัฐฯ ได้มีความพยายามแสดงบทบาทนำมากขึ้นผ่านการเสนอร่างมติฉบับใหม่จนถึงปี ค.ศ. 2022 ซึ่งเป็นข้อมติล่าสุดที่มีการลงคะแนนในสหประชาชาติดังข้อมูลในตารางที่ 1

ตารางที่ 1 สรุปมติการประชุมสมัชชาใหญ่แห่งสหประชาชาติ เรื่อง “Developments in the field of information and telecommunications in the context of international security”

Year	Title	Voting summary					
		Yes / (70%)	No	Abstentions	Non-voting	Total voting	US position
2005	Agenda (1)	177 / (133)	1	-	13	191	No
2006	Agenda (1)	176 / (134)	1	-	15	192	No
2007	Agenda (1)	179 / (134)	1	-	12	192	No
2008	Agenda (1)	178 / (134)	1	-	13	192	No
2016	Agenda (1)	181 / (135)	-	1	11	193	Yes
2018	Agenda (1)	119 / (135)	46	14	14	193	No
	Agenda (2)	138 / (135)	12	16	27	193	Yes
2019	Agenda (2)	163 / (135)	10	6	14	193	Yes
	Agenda (1)	129 / (135)	6	45	13	193	No
2020	Agenda (2)	163 / (135)	10	7	13	193	Yes
	Agenda (1)	92 / (135)	50	21	30	193	No
2022	Agenda (3)	156 / (135)	7	14	16	193	Yes
	Agenda (1)	112 / (135)	52	8	21	193	No

ที่มา: เรียบเรียงโดยผู้เขียน (United Nations General Assembly, 2005, 2006, 2007, 2008, 2016, 2018a, 2019, 2020, 2022)

หมายเหตุ:

Agenda (1) Developments in the field of information and telecommunications in the context of international security

Agenda (2) Advancing responsible State behavior in cyberspace in the context of international security

Agenda (3) Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security

อย่างไรก็ตาม เมื่อพิจารณาถึงหลักเกณฑ์ที่ Hoffmann เสนอดังกล่าว จะพบว่า ปทัสถานที่รัสเซียเสนอในระยะแรกแม้จะถูกผลักดันเข้าสู่เวทีระหว่างประเทศและเป็นที่ยอมรับ

ในระยะหนึ่ง แต่รัฐแกนนำที่สำคัญแสดงความไม่เห็นด้วยดังเห็นได้จากตารางที่ 2 จะเห็นว่าสหรัฐฯ ลงมติไม่เห็นชอบกับข้อเสนอของรัสเซียซึ่งเป็นรัฐแกนนำที่สำคัญในการเสนอร่างปทัสถานความมั่นคงไซเบอร์เข้าสู่เวทีสหประชาชาติมาตั้งแต่ปี ค.ศ. 1998 อย่างต่อเนื่อง โดยสหรัฐฯ ลงมติเห็นชอบร่างของรัสเซียเพียง 1 ครั้ง จากทั้งหมด 9 ครั้ง คือ การประชุม UNGA 2016 ซึ่งเป็นครั้งแรกที่มีการกล่าวถึงประเด็นด้านสิทธิมนุษยชนอยู่ในร่างที่ห้ามตีเห็นชอบอย่างใดก็ตาม จากการลงมติเห็นชอบร่างในครั้งนั้น สหรัฐฯ ไม่ได้ลงมติเห็นชอบอีกเลย แต่ได้พยายามมีบทบาทนำที่มากขึ้นผ่านการเสนอร่างของตนเองตั้งแต่ปี ค.ศ. 2018 เป็นต้นมา

ตารางที่ 2 สรุปข้อโต้แย้งหรือข้อถกเถียงหลักที่โดดเด่นในมติการประชุมสมัชชาใหญ่แห่งสหประชาชาติ เรื่อง “Developments in the field of information and telecommunications in the context of international security” โดยตัวกระทำกระทำการของสหรัฐฯ เป็นผู้ผลักดัน

UNGA	ข้อโต้แย้งหรือข้อถกเถียงหลัก / ข้อเสนอ
2016	<ol style="list-style-type: none"> 1) ตีความเรื่องความมั่นคงให้สอดคล้องกับกฎบัตรสหประชาชาติ 2) ตีความสิทธิมนุษยชนว่า เป็นส่วนหนึ่งของการตีความด้านความมั่นคงไซเบอร์ 3) นำข้อสรุป UNGGE 2015 เรื่อง การกำหนดพฤติกรรมและความรับผิดชอบของรัฐมาปรับใช้
2018	<ol style="list-style-type: none"> 1) นำเรื่องการตีความ และหลักการกำหนดพฤติกรรมและความรับผิดชอบของรัฐมาตามมติ UNGA 2016 มาปรับใช้ 2) ระบุถึงความร่วมมือระหว่างรัฐ (State Cooperation) และการดำเนินการร่วมกัน (Collective Action) เป็นครั้งแรก 3) ระบุตัวแสดงอื่นที่ผู้มีส่วนได้ส่วนเสียหลายฝ่าย (Multi-Stakeholder) เข้ามาในร่าง 4) เสนอให้มีการหารือแบบไม่เป็นทางการขึ้นทุกครั้งก่อนการประชุม OEWG 2 วัน ด้วยเหตุผลเพื่อการความโปร่งใสในการทำงานของที่ประชุม OEWG
2020	<ol style="list-style-type: none"> 1) เน้นย้ำถึงขอบเขตของพื้นที่ทางไซเบอร์ในยุคโควิด 19
2022	<ol style="list-style-type: none"> 1) ระบุประเด็นความหลากหลายทางเพศเข้ามาในร่าง (Gender Digital Divide) 2) เน้นย้ำความสำคัญของบทบาทสตรีในฐานะตัวแสดงในกระบวนการตัดสินใจทางนโยบายที่เกี่ยวกับไซเบอร์ (Decision-Making Processes)

ที่มา: เรียบเรียงโดยผู้เขียน (United Nations General Assembly, 2016, 2018a, 2018b, 2020, 2022)

หมายเหตุ: การลงมติปี ค.ศ. 2016-2022 คือ ปีที่สหรัฐฯ ให้การเห็นชอบในร่างใดร่างหนึ่ง

ทั้งนี้ ประเด็นถกเถียงหรือข้อโต้แย้งหลักที่เกิดขึ้นในการลงมติการประชุม UNGA ในแต่ละครั้งของสหรัฐฯ ส่งผลต่อการยอมรับปทัสถานทางไซเบอร์เช่นกัน ดังที่ได้กล่าวไว้ใน ส่วนที่ 4 ซึ่งสังเกตได้ว่า ในการลงมติที่ประชุม UNGA 2016 ได้รับการเห็นชอบจากที่ประชุม กว่า 181 เสียงจากทั้งหมด 193 เสียง โดยถือเป็นครั้งแรกที่มีการยอมรับปทัสถานทางไซเบอร์ มากที่สุดแม้จะเป็นร่างของรัสเซีย แต่ข้อถกเถียงสำคัญที่เกิดขึ้นในครั้งนี้ คือ การตีความเรื่อง ความมั่นคงให้สอดคล้องกับกฎบัตรสหประชาชาติในขอบเขตที่ครอบคลุมถึงการสร้างความมั่นคงและสงบสุขในขอบเขตของเทคโนโลยีสารสนเทศ ซึ่งประเด็นนี้ตีความครอบคลุม ถึงเรื่องสิทธิมนุษยชนซึ่งแตกต่างจากมติครั้งก่อนที่กล่าวถึงขอบเขตเพียงอาชญากรรมและการก่อการร้ายเท่านั้น นอกจากนี้ ข้อถกเถียงหลักที่สหรัฐฯ เป็นผู้ผลักดันตั้งข้อมูลในตารางที่ 2 อาจส่งผลต่อการแพร่กระจายปทัสถานไซเบอร์ของสหรัฐฯ อย่างมีนัยสำคัญ สังเกตได้จากร่าง ปทัสถานไซเบอร์ของสหรัฐฯ นับจากปี ค.ศ. 2016 เป็นต้นมาได้รับความเห็นชอบเกินกว่า ร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบมาโดยตลอดตั้งข้อมูลในตารางที่ 1

ตารางที่ 3 พัฒนาการมติการประชุมสมัชชาใหญ่แห่งสหประชาชาติตั้งแต่ปี ค.ศ. 1998 - 2022 เรื่อง “Developments in the field of information and telecommunications in the context of international security”

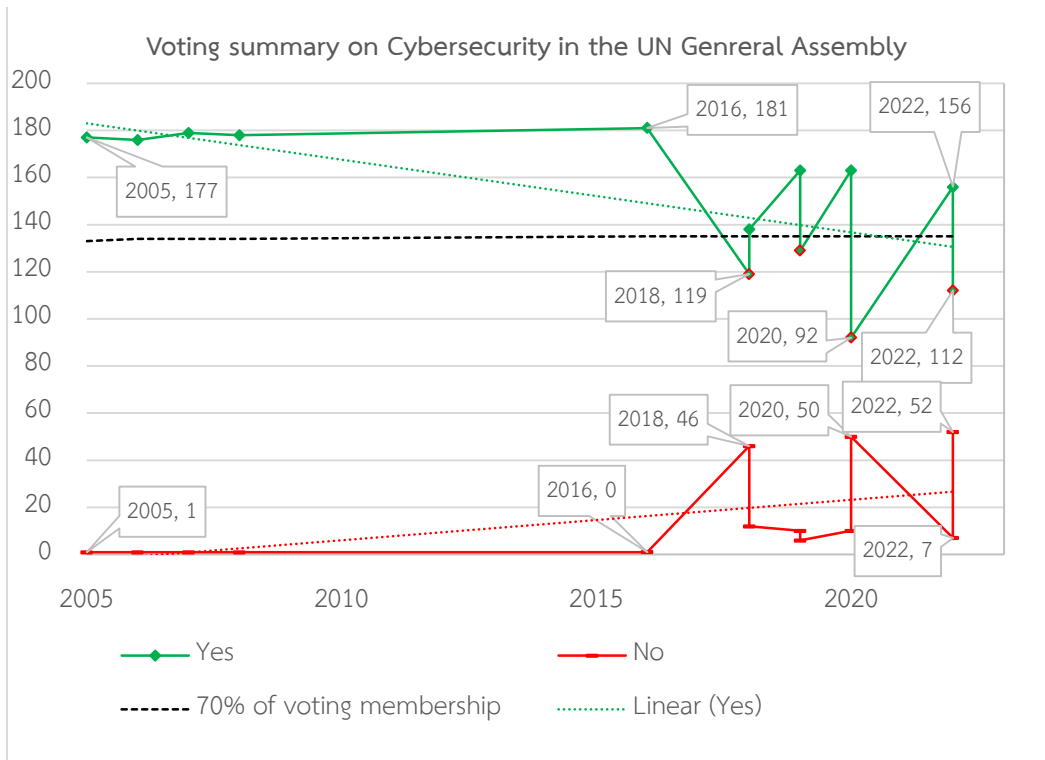
Year	Agenda(s)	Voting summary			
		Yes / (70%)	No	Total voting	US position
1998	(1) — Russia Draft	Adopted without vote			
1999	(1) — Russia Draft	Adopted without vote			
2000	(1) — Russia Draft	Adopted without vote			
2001	(1) — Russia Draft	Adopted without vote			
2002	(1) — Russia Draft	Adopted without vote			
2003	(1) — Russia Draft	Adopted without vote			
2004	(1) — Russia Draft	Adopted without vote			
2005	(1) — Russia Draft	177 / (133)	1	191	No
2006	(1) — Russia Draft	176 / (134)	1	192	No
2007	(1) — Russia Draft	179 / (134)	1	192	No
2008	(1) — Russia Draft	178 / (134)	1	192	No

Year	Agenda(s)	Voting summary			
		Yes / (70%)	No	Total voting	US position
2009	(1) — Russia Draft	Adopted without vote			
2010	(1) — Russia Draft	Adopted without vote			
2011	(1) — Russia Draft	Adopted without vote			
2012	(1) — Russia Draft	Adopted without vote			
2013	(1) — Russia Draft	Adopted without vote			
2014	(1) — Russia Draft	Adopted without vote			
2015	(1) — Russia Draft	Adopted without vote			
2016	(1) — Russia Draft	181 / (135)	-	193	Yes
2018	(1) — Russia Draft	119 / (135)	46	193	No
	(2) — US Draft	138 / (135)	12	193	Yes
2019	(2) — US Draft	163 / (135)	10	193	Yes
	(1) — Russia Draft	129 / (135)	6	193	No
2020	(2) — US Draft	163 / (135)	10	193	Yes
	(1) — Russia Draft	92 / (135)	50	193	No
2021	(1) — Russia and US Draft	Adopted without vote			
2022	(3) — France Draft	156 / (135)	7	193	Yes
	(1) — Russia Draft	112 / (135)	52	193	No

ที่มา: เรียบเรียงโดยผู้เขียน (United Nations General Assembly, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2018a, 2019, 2020, 2021, 2022)

นัยสำคัญอีกประการหนึ่ง คือ หลังจากที่สหรัฐฯ เสนอร่างของตนก็ได้รับความเห็นชอบจากที่ประชุมเกินกว่าร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบมาโดยตลอดจนถึงมติปีล่าสุด ค.ศ. 2022 ขณะที่ร่างในเรื่องเดียวกันของรัสเซียซึ่งเสนอมาโดยตลอดนั้นได้รับความเห็นชอบที่ลดลงอย่างมากจนต่ำกว่าระดับร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบดังปรากฏในตารางที่ 3 แสดงให้เห็นว่าสหรัฐฯ ได้เข้ามามีบทบาทหน้าที่มากขึ้นในการเป็นรัฐแกนนำที่สำคัญเพื่อกำหนดและผลักดันปทัสสถานความมั่นคงไซเบอร์ในเวทีสหประชาชาติ

แผนภาพที่ 1 แผนภูมิเส้นแสดงพลวัตการประชุมสมัชชาใหญ่แห่งสหประชาชาติ เรื่อง
“Developments in the field of information and telecommunications
in the context of international security”



ที่มา: เรียบเรียงโดยผู้เขียน (United Nations General Assembly, 2005, 2006, 2007, 2008, 2016, 2018a, 2019, 2020, 2022)

จากแผนภาพที่ 4 จะสังเกตได้ว่า หลังจากที่สหรัฐฯ ได้เสนอร่างปทัสถานความมั่นคงไซเบอร์ของตนเข้าสู่ที่ประชุม UNGA ปี 2018, 2019, 2020 ในฐานะผู้เสนอร่าง และปี ค.ศ. 2022 ในฐานะผู้สนับสนุนร่างในนามของสหรัฐฯ (on behalf of) ต่อร่างของฝรั่งเศส ซึ่งได้รับมติเห็นชอบจากที่ประชุมสูงกว่าร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบทั้งสิ้น ในขณะที่ร่างปทัสถานเดียวกันซึ่งถูกเสนอโดยรัสเซียกลับได้รับมติเห็นชอบจากที่ประชุมไม่ถึงร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบในปีเดียวกันแม้แต่ครั้งเดียว แม้ว่าในความเป็นจริงนั้นร่างดังกล่าวของรัสเซียจะถูกยอมรับที่ประชุมด้วยหลักการเสียงส่วนใหญ่ (มากกว่าร้อยละ 50 ของสมาชิกที่มีสิทธิ์ลงมติเห็นชอบ) ก็ตาม แต่นัยสำคัญต่อการพิจารณาในกรอบวัฏจักรปทัสถานแสดงให้เห็นว่า ปทัสถานของสหรัฐฯ กำลังมีแนวโน้มที่เพิ่มสูงขึ้นในระดับที่อาจ

เข้าสู่ระยะที่ 2 การแพร่กระจายปทัสถานดังแผนที่ภาพที่ 4 ซึ่งแสดงให้เห็นเส้นความก้าวหน้าของปทัสถานความมั่นคงไซเบอร์ซึ่งถูกเสนอโดยสหรัฐฯ ที่สูงกว่าร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบโดยกราฟพุ่งขึ้นอย่างต่อเนื่อง ในขณะที่แผนภาพได้แสดงให้เห็นเส้นความก้าวหน้าของปทัสถานที่รัสเซียเสนอในลักษณะที่ถดถอย กล่าวคือ อยู่ในระดับที่ต่ำกว่าร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบอย่างตื้นเนื่อง

อย่างไรก็ตาม ผู้เขียนตั้งข้อสังเกตว่า ผลการแสดงความเห็นชอบจากที่ประชุมเพียง 4 ครั้งของสหรัฐฯ ในฐานะตัวกระทำที่สำคัญ อาจยังไม่เพียงพอต่อการคาดคะเนแนวโน้มการยอมรับปทัสถานความมั่นคงไซเบอร์อย่างแท้จริงว่า เข้าสู่ระยะที่ 2 การแพร่กระจาย แม้ว่าปทัสถานใหม่ที่สหรัฐฯ เสนอจะเข้าสู่จุดยอมรับปทัสถานโดยทั่วกันในความหมายของ Hoffmann ที่ร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบ เมื่อเทียบกับรัสเซียซึ่งมีทั้งหมด 9 ครั้ง แต่อาจกล่าวได้ว่า สหรัฐฯ ได้เข้ามามีบทบาทนำที่มากขึ้นในการเป็นผู้กำหนดปทัสถานความมั่นคงไซเบอร์ในช่วงครึ่งทศวรรษที่ผ่านมา

อีกประการหนึ่งที่สำคัญ คือ ถึงแม้ว่าสหรัฐฯ จะแสดงบทบาทในฐานะผู้ประกอบการเชิงปทัสถานที่พยายามโน้มน้าวให้รัฐอื่นเห็นชอบกับข้อเสนอของตนจนเป็นที่ยอมรับของประชาคมระหว่างประเทศ ดังที่ Hoffmann อธิบายไว้ แต่จำนวนรัฐที่ยอมรับข้อเสนอเหล่านั้นมีความผันผวน ไม่ได้มีจำนวนยอมรับเพิ่มขึ้นอย่างรวดเร็วและต่อเนื่อง ดังแผนที่ภาพที่ 4 จึงไม่สามารถบอกได้ว่า ปทัสถานความมั่นคงไซเบอร์เข้าสู่ระยะที่ 2 ซึ่งเป็นระยะของการแพร่กระจายปทัสถานในวัฏจักรอย่างสมบูรณ์ อาจกล่าวได้ว่า พัฒนาการของการยอมรับปทัสถานความมั่นคงไซเบอร์ยังคงเป็นที่ถกเถียงและปรับเปลี่ยนอยู่ตลอดเวลาในปัจจุบัน แสดงให้เห็นว่า ตัวแสดงจะเลือกยอมรับ และ/หรือ ปฏิเสธปทัสถานออกไปอย่างมีเหตุผลตามความสนใจของตน (Katzenstain, 1996)

จะเห็นได้ว่า ยังคงมีรัฐสมาชิกอีกจำนวนกว่าร้อยละ 30 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบ ซึ่งไม่ยอมรับปทัสถานดังกล่าวของสหรัฐฯ โดยเฉพาะอย่างยิ่งรัฐอำนาจนิยม หรือคู่แข่งชั้นของสหรัฐฯ เช่น รัสเซีย จีน เกาหลีเหนือ เป็นต้น จึงพิจารณาได้ว่า ผู้ประกอบการเชิงปทัสถานของสหรัฐฯ ยังไม่สามารถโน้มน้าวตัวแสดงบางตัวให้เห็นพ้องกับปทัสถานของตนได้ ในขณะเดียวกัน ปทัสถานความมั่นคงไซเบอร์ซึ่งสหรัฐฯ เป็นผู้เสนอนั้นอาจถูกตั้งคำถามโดยตัวแสดงที่ไม่พอใจต่อข้อเสนอของสหรัฐฯ ว่า การที่ชาติมหาอำนาจอย่างสหรัฐฯ โดยเฉพาะอย่างยิ่งมหาอำนาจทางเทคโนโลยีจะส่งผลให้เกิดผลประโยชน์ และความอสมมาตรทางอำนาจในพื้นที่ไซเบอร์ ซึ่งจะนำมาสู่การทำลายปทัสถานด้วยข้อเสนอปทัสถานที่แตกต่างกัน (Norm Divergence) โดยตัวแสดงเดิมอย่างรัสเซีย และโดยเฉพาะอย่างยิ่งจีนในฐานะรัฐแกนนำที่สำคัญซึ่งกำลังมีบทบาททำลายปทัสถานทางไซเบอร์ในปัจจุบันในการปฏิรูปโครงสร้าง

พื้นฐานอินเทอร์เน็ตให้รัฐเข้ามามีบทบาทหลักในการควบคุมและเรื่องอำนาจอธิปไตยทางไซเบอร์ แม้ในปัจจุบันจะยังไม่มีปรากฏว่า รัฐบาลจีนได้เสนอร่างปทัสถานความมั่นคงเป็นของตนเองอย่างชัดเจน แต่ก็แสดงให้เห็นอย่างแข็งขันถึงมุมมอง และความยึดมั่นของการนำเสนอปทัสถานความมั่นคงไซเบอร์ในแบบของตนในเรื่อง “อธิปไตยทางไซเบอร์”

กล่าวโดยสรุป พัฒนาการของการเกิดปทัสถานความมั่นคงไซเบอร์ของสหรัฐฯ ในเวลานี้ยังหยุดอยู่ในช่วงเปลี่ยนผ่านของระยะที่ 1 สู่ระยะที่ 2 เมื่อพิจารณาตามรูปแบบวัฏจักรปทัสถานของ Finnemore and Sikkink (1998) ซึ่งอยู่ในระยะของการยอมรับปทัสถาน โดยทั่วกันโดยรัฐก่อนจะเข้าสู่ระยะของการแพร่กระจายและอัตราการยอมรับปทัสถานเพิ่มขึ้นสูงอย่างต่อเนื่อง หรือพิจารณาตามเกณฑ์ของ Hoffmann แล้วสามารถไปสู่จุดสูงสุดของการยอมรับปทัสถานใหม่เพื่อเข้าสู่ระยะที่ 2 การแพร่กระจายของปทัสถานได้ อีกนัยหนึ่ง คือ ปทัสถานถูกยอมรับโดยสมาชิกในที่ประชุมกว่ากว่าร้อยละ 70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบ และมีแนวโน้มจะเพิ่มขึ้นอย่างต่อเนื่อง อย่างไรก็ตาม ปทัสถานความมั่นคงไซเบอร์ ก็ถูกยอมรับในบางส่วนจนเกิดเป็นมติจากที่ประชุมในองค์การระหว่างประเทศเพื่อใช้เป็นแนวทางในการปฏิบัติภายในประเทศโดยผู้ประกอบการเชิงปทัสถานในระดับอื่น ผู้เขียนตั้งข้อสังเกตว่า การไม่สามารถมีข้อสรุปถึงการปฏิบัติของปทัสถานได้นั้นจะทำให้เกิดช่องว่างของการตีความปทัสถานขึ้นซึ่งจะส่งผลต่อการตีความของผู้ประกอบการเชิงปทัสถานภายในประเทศ ทำให้วัฏจักรปทัสถานในระยะที่ 3 กระบวนการรับปทัสถานที่ยอมรับจากภายนอกไปปฏิบัติภายในประเทศนั้นเกิดขึ้นได้ยาก

6. สรุป

จากการศึกษาแสดงให้เห็นว่า ปทัสถานความมั่นคงไซเบอร์ยังคงเป็นปทัสถานใหม่ซึ่งยังเป็นที่ยกเถียงถึงการกำหนดแนวทาง การตีความ และการบังคับใช้ทางการกฎหมายระหว่างประเทศ เพื่อเป็นแนวทางในการให้รัฐต่างๆ นำไปปฏิบัติใช้ภายในประเทศ ส่งผลให้เกิดการไม่ตกลงหลักทางปทัสถาน แม้ว่ามติที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติว่าด้วยเรื่องความมั่นคงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และการสื่อสารจะชี้ให้เห็นว่า ปทัสถานความมั่นคงไซเบอร์จะผ่านพ้นระยะที่ 1 เป็นปทัสถานที่เกิดขึ้น และมีตัวตนอยู่ในความสัมพันธ์ระหว่างประเทศตามวัฏจักรปทัสถาน ซึ่งผลการศึกษาได้ชี้ให้เห็นว่า ปทัสถานความมั่นคงไซเบอร์ที่ดำรงอยู่ในปัจจุบันในแบบของตะวันตกโดยมีสหรัฐฯ เป็นผู้มีบทบาทสำคัญในการกำหนดหลักการต่างๆ ยังไม่สามารถเข้าสู่ระยะที่ 2 การแพร่กระจายของปทัสถานได้ เพราะเมื่อพิจารณาถึงจุดสูงสุดของระดับการแพร่กระจายซึ่งถูกนิยามว่า เป็นจุดที่ทำให้ปทัสถานเป็นที่

ยอมรับโดยทั่วกันจนไม่ถูกตั้งคำถามหรือถูกตั้งคำถามน้อยลงตามคำอธิบายของ Hoffmann (2003) ซึ่งอ้างถึงผลลัพธ์ของมติที่ประชุมที่ยอมรับปทัสถานสูงกว่าระดับร้อยละ 60-70 ของสมาชิกที่มีสิทธิ์แสดงมติเห็นชอบและสูงขึ้นอย่างสม่ำเสมอ พบว่า ผลลัพธ์ของมติที่ประชุมสมาชิกใหญ่แห่งสหประชาชาติมีความผันผวนซึ่งไม่เป็นไปตามเงื่อนไขของการยอมรับปทัสถานระดับที่เข้าสู่ระยะการแพร่กระจายของวัฏจักรปทัสถาน ส่งผลให้เกิดพื้นที่ของการตีความและท้าทายปทัสถานของตัวแสดงอื่นโดยเฉพาะอย่างยิ่งปทัสถานที่จีนเป็นผู้เสนอ

ดังนั้น ในการจะทำให้ปทัสถานความมั่นคงไซเบอร์เข้าสู่วัฏจักรปทัสถานในระยะที่ 3 การรับปทัสถานที่ยอมรับจากภายนอกไปปฏิบัติภายในประเทศนั้นเป็นสิ่งท้าทายอย่างยิ่ง เนื่องจากเป็นเรื่องภายในประเทศ โดยปกติแล้วผู้ประกอบการเชิงปทัสถานจะมุ่งโน้มน้าวตัวแสดงเป็นเป้าหมายหลักเพื่อให้เกิดการเปลี่ยนแปลงพฤติกรรม แต่ในความเป็นจริงนั้น ตัวแสดงภายในมักตีความปทัสถานด้วยตัวเองอีกครั้งหนึ่ง (Reinterpretation) ซึ่งส่งผลต่อการนำไปปฏิบัติภายในประเทศ Risse, Ropp and Sikkink (1999) อธิบายว่า กระบวนการทำปทัสถานให้เป็นภายในและการเปลี่ยนแปลงภายในนั้นจำเป็นต้องพิจารณาถึงบริบทสังคมภายใน ตัวแสดง เครือข่ายที่เชื่อมโยงภายในประเทศ และระเบียบระหว่างประเทศเป็นสำคัญ ส่งผลให้ในการทำปทัสถานให้เป็นภายในนั้นจำเป็นต้องพิจารณาถึงข้อมูลเชิงประจักษ์ซึ่งแต่ละประเทศนั้นแตกต่างกัน

อย่างไรก็ตาม เมื่อพิจารณาถึงค่านิยมและคุณลักษณะของรัฐที่หลากหลายข้างต้นสามารถพิจารณาได้ว่า ปทัสถานความมั่นคงไซเบอร์ในปัจจุบันแบบการกำกับดูแลโดยผู้มีส่วนได้ส่วนเสียหลายฝ่ายซึ่งชาติตะวันตกมีบทบาทนำโดยเฉพาะสหรัฐฯ อาจถูกยอมรับจากภายในได้ง่ายในกลุ่มประเทศตะวันตกด้วยกันเนื่องจากลักษณะการปกครอง สภาพแวดล้อมทางสังคม การเมือง มีความคล้ายคลึงและสอดคล้องกันทำให้ปทัสถานไซเบอร์แบบตะวันตกนั้นถูกยอมรับได้ง่าย ขณะเดียวกัน บางประเทศที่บริบทดังกล่าวไม่สอดคล้องหรือไม่เห็นด้วยกับการเป็นพันธมิตรชาติตะวันตกก็อาจจะทำให้ปทัสถานความมั่นคงไซเบอร์ซึ่งถูกออกแบบโดยชาติตะวันตกโดยเฉพาะอย่างยิ่งสหรัฐฯ ไม่เป็นที่ยอมรับหรือยอมรับได้ยาก โดยเฉพาะอย่างยิ่งในบางประเทศที่มีบทบาทในลักษณะขัดขวางข้ามทางอำนาจหรืออุดมการณ์ คู่แข่งขัน เช่น จีน รัสเซีย เกาหลีเหนือ ก็อาจจะทำให้เกิดความแตกแยกทางปทัสถานขึ้นได้ ดังเช่นที่จีนพยายามเสนอปทัสถานใหม่ เรื่อง อธิปไตยทางไซเบอร์เพื่อท้าทายปทัสถานเดิม อย่างไรก็ตาม สงครามความขัดแย้งเหนือดินแดนระหว่างรัสเซีย และยูเครนอาจส่งผลต่อภาพลักษณ์ของประเทศอำนาจนิยมในการเป็นภาพสะท้อนรูปแบบหนึ่งของแนวคิดเรื่อง “บูรณภาพแห่งดินแดน” ซึ่งในปัจจุบันประเด็นดังกล่าวกำลังได้รับความสนใจอย่างมากในปทัสถานทางไซเบอร์

ภูมิทัศน์ของการแข่งขันทางแพลตฟอร์มทางไซเบอร์ของสหรัฐฯ และจีนแสดงให้เห็นถึงมุมมองและทิศทางของนโยบายในแบบของตนเอง ในทางหนึ่ง สหรัฐฯ สนับสนุนลักษณะของอินเทอร์เน็ตที่มีอิสระ และปลอดภัยจากการควบคุมโดยรัฐซึ่งกล่าวหาว่ารัฐบาลจีนว่ามึนโยบายทางไซเบอร์ที่คุกคามและปิดกั้นทางข้อมูล ในขณะเดียวกัน จีนให้ความสำคัญกับอำนาจอธิปไตยทางไซเบอร์และความมั่นคงของรัฐเป็นสำคัญ ทำให้เกิดการออกแบบระเบียบในการควบคุมข้อมูลอย่างเข้มงวด มุมมองที่ขัดแย้งดังกล่าวนำไปสู่ความตึงเครียดระหว่างสองประเทศในการแข่งขันการชิงบทบาทในฐานะผู้พัฒนาและผู้กำหนดแพลตฟอร์มระหว่างประเทศขึ้น บริบทการทำนายเชิงแพลตฟอร์มดังกล่าว ส่งผลให้แพลตฟอร์มทางไซเบอร์เกิดการปะทะ และแข่งขันกันมากขึ้นอย่างมีนัยสำคัญต่อการเมืองระหว่างประเทศซึ่งยังทำให้การศึกษาผู้ประกอบการเชิงแพลตฟอร์ม และแพลตฟอร์มความมั่นคงไซเบอร์มีความสำคัญมากขึ้นในปัจจุบัน

เอกสารอ้างอิง

ภาษาอังกฤษ

- Acharya, A. (2004). How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism. *International Organization*, 58(2), 239-275.
- Adler, E. (1997). Seizing the Middle Ground: Constructivism in World Politics. *European Journal of International Relations*, 3(3), 319-363.
- Arora, P. (2019). Politics of Algorithms, Indian Citizenship, and the Colonial Legacy. In Punathambekar, A., & Mohan, S. (Eds.). *Global Digital Cultures: Perspectives from South Asia* (pp. 37-52). N.P.: University of Michigan Press.
- Arquilla, J., & Ronfeldt, D. (Eds.). (1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: Rand Corporation.
- Axelrod, R. (1997). *The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration*. Princeton: Princeton University Press.
- Badescu, C. G. (2011). *Humanitarian Intervention and the Responsibility to Protect: Security and Human Rights*. New York: Routledge.
- Braithwaite, J. (1994). A Sociology of Modelling and the Politics of Empowerment. *British Journal of Sociology*, 45(3), 445-479.

- Cai, C. (2018). Global Cyber Governance: China's Contribution and Approach. *China Quarterly of International Strategic Studies*, 4(1), 55-76.
- Cybersecurity Tech Accord. (2023). *Signatories*. Retrieved June 4, 2023, from <https://cybertechaccord.org/signatories/>
- Deitelhoff, N., & Wolf, K. (2013). Business and Human Rights: How Corporate Norm Violators Become Norm Entrepreneurs. In Risse, T., Sikkink, K., & Ropp, C. S. (Eds.). *The Persistent Power of Human Rights: From Commitment to Compliance* (pp. 222-238). Cambridge: Cambridge University Press.
- Deitelhoff, N., & Zimmermann, L. (2019). Norms Under Challenge: Unpacking the Dynamics of Norm Robustness. *Journal of Global Security Studies*, 4(1), 2-17.
- DeNardis, L. (2012). Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance. *Information, Communication & Society*, 15(5), 720-738.
- Finnemore, M. (2017). *Cybersecurity and the Concept of Norms*. Retrieved February 4, 2023, from <https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870>
- Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, 50(4), 887-918.
- Gleckman, H. (2018). *Multistakeholder Governance and Democracy: A Global Challenge*. New York: Routledge.
- Gold, J. (2021). Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?. Retrieved February 4, 2023, from <https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what>
- Greenwood, F. (2020). Data Colonialism, Surveillance Capitalism and Drones. In Specht, D. (Ed.). *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping* (pp. 89-118). University of London Press.
- Hobbs, C. (Ed.). (2020). *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry*. N.P.: European Council on Foreign Relations.

- Hoffmann, M. (2003). *Entrepreneurs and Norm Dynamics: An Agent-based Model of the Norm Life Cycle*. Retrieved February 4, 2023, from http://www.polisci.upenn.edu/ps-i/Pamla/Hoffmann_norms.doc
- Hurel, L. M., & Lobato, C. L. (2018). Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs. *Journal of Cyber Policy*, 3(1), 61-76.
- International Committee of the Red Cross. (1949). *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)*, 12 August 1949, 75 UNTS 287. Retrieved February 4, 2023, from <https://www.refworld.org/docid/3ae6b36d2.html>
- Internet Engineering Task Force. (2023). *Mission and Principles*. Retrieved February 4, 2023, from <https://www.ietf.org/about/introduction/>
- Jiayi, L. (2021). *The Qualities and Strengths of Consultative Democracy Practiced Through the Chinese People's Political Consultative Conference*. Retrieved February 4, 2023, from http://en.qstheory.cn/2022-01/18/c_699097.htm
- Katzenstein, P. (Ed.). (1996). *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press.
- Khalil, L. (2020). *Digital Authoritarianism, China and COVID*. (Research report). N.P.: Lowy Institute for International Policy.
- Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*, 2(1), 119-154.
- Kratochwil, F. (1989). *Rules, Norms, and Decisions*. Cambridge: Cambridge University Press.
- Li, Y. (2019). Global Cyberspace Governance: State Actors and the China-US Cyber Relationship. *Contemporary International Relations*, 29(2), 105-124.
- Lotrionte, C. (2018). Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations under International Law. *The Cyber Defense Review*, 3(2), 73-114.
- Lu, W. (2014). *Cyber Sovereignty Must Rule Global Internet*. Retrieved February 4, 2023, from https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060

- Margaret, K., & Sikkink, K. (1998). *Activists Beyond Borders: Transnational Advocacy Networks in International Politics*. Ithaca: Cornell University Press.
- Mueller, M. (2009). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.
- Mueller, M., Mathiason, J., & Klein, H. (2007). The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance: A Review of Multilateralism and International Organizations*, 13(2), 237-254.
- O'Connell, E. M., & Arimatsu, L. (2012). *Cyber Security and International Law*. Retrieved February 4, 2023, from <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf>
- Ostrom, E. (2000). Collective Action and the Evolution of Social Norms. *Journal of Economic Perspectives*, 14(3), 137-158.
- Risse, T., Ropp, S., & Sikkink, K. (Eds.). (1999). *The Power of Human Rights: International Norms and Domestic Change*. Cambridge: Cambridge University Press.
- Rodriguez, M. (2017). *Declaration by the Representative of Cuba at the Final Session of the Group of Governmental Experts*. Retrieved February 4, 2023, from <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf>
- Schmitt, N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press.
- Schmitt, N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press.
- Sherman, J. (2021). Digital Authoritarianism and Implications for US National Security. *The Cyber Defense Review*, 6(1), 107–118.
- Smith, B. (2017). *The Need for a Digital Geneva Convention*. Retrieved June 4, 2023, from <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>
- Streinz, T. (2021). *RCEP's Contribution to Global Data Governance*. Retrieved February 4, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826217

- Sukumar, A. M. (2017). *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*. Retrieved February 4, 2023, from <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>
- United Nations General Assembly. (1998). *Report of the 1st Committee: Role of Science and Technology in the Context of International Security, Disarmament and Other Related Fields*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/264457?ln=en>
- United Nations General Assembly. (1999). *Report of the 1st Committee: General Assembly, 54th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/351558?ln=en&v=pdf>
- United Nations General Assembly. (2000). *Report of the 1st Committee: General Assembly, 55th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/427170?ln=en&v=pdf>
- United Nations General Assembly. (2001). *Report of the 1st Committee: General Assembly, 56th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/452991?ln=en&v=pdf>
- United Nations General Assembly. (2002). *Report of the 1st Committee: General Assembly, 57th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/478670?ln=en&v=pdf>
- United Nations General Assembly. (2003). *Report of the 1st Committee: General Assembly, 58th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved

- February 23, 2023, from <https://digitallibrary.un.org/record/506848?ln=en&v=pdf>
- United Nations General Assembly. (2004). *Report of the 1st Committee: General Assembly, 59th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from https://digitallibrary.un.org/record/535822/files/A_59_454-EN.pdf
- United Nations General Assembly. (2005). *Report of the 1st Committee: General Assembly, 60th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/561130?ln=en&v=pdf>
- United Nations General Assembly. (2006). *Report of the 1st Committee: General Assembly, 61st session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/587060?ln=en&v=pdf>
- United Nations General Assembly. (2007). *Report of the 1st Committee: General Assembly, 62nd session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/612351?ln=en&v=pdf>
- United Nations General Assembly. (2008). *Report of the 1st Committee: General Assembly, 63rd session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/641397?ln=en&v=pdf>
- United Nations General Assembly. (2009). *Report of the 1st Committee: General Assembly, 64th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/671471?ln=en&v=pdf>

- United Nations General Assembly. (2010). *Report of the 1st Committee: General Assembly, 65th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/693819?ln=en&v=pdf>
- United Nations General Assembly. (2011). *Report of the 1st Committee: General Assembly, 66th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/715997?ln=en&v=pdf>
- United Nations General Assembly. (2012). *Report of the 1st Committee: General Assembly, 67th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/738631?ln=en&v=pdf>
- United Nations General Assembly. (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 4, 2023, from <https://digitallibrary.un.org/record/753055>
- United Nations General Assembly. (2014). *Report of the 1st Committee: General Assembly, 69th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/782912?ln=en&v=pdf>
- United Nations General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 4, 2023, from <https://digitallibrary.un.org/record/799853>
- United Nations General Assembly. (2016). *Report of the 1st Committee: General Assembly, 71st session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/848219?ln=en&v=pdf>
- United Nations General Assembly. (2018a). *Report of the 1st Committee: General Assembly, 73rd session, Developments in the Field of Information and*

- Telecommunications in the Context of International Security*. Retrieved February 4, 2023, from <https://digitallibrary.un.org/record/1654007?ln=en>
- United Nations General Assembly. (2018b). *UN Resolution 73/27*. Retrieved February 4, 2023, from <https://undocs.org/en/A/RES/73/27>
- United Nations General Assembly. (2019). *Report of the 1st Committee: General Assembly, 74th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/3836338?ln=en&v=pdf>
- United Nations General Assembly. (2020). *Report of the General Assembly, Advancing Responsible State Behavior in Cyberspace in the Context of International Security*. Retrieved February 17, 2023, from <https://digitallibrary.un.org/record/3893847?ln=en>
- United Nations General Assembly. (2021). *Report of the 1st Committee: General Assembly, 76th session, Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved February 23, 2023, from <https://digitallibrary.un.org/record/3948700?ln=en&v=pdf>
- United Nations General Assembly. (2022). *Report of the General Assembly, Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security*. Retrieved February 17, 2023, from <https://digitallibrary.un.org/record/3996919?ln=en>
- United Nations. (2024). *Charter of the United Nations*. Retrieved March 5, 2024, from <https://www.un.org/en/sections/un-charter/un-charter-full-text>
- Yau, H. (2019). An Assessment of Cyberpower Within the Triangular Relations of Taiwan-US-China and Its Implications. *International Journal of Taiwan Studies*, 2(2), 264-291.
- Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *PRISM*, 7(2), 108-115.