# การศึกษายุทธศาสตร์เส้นทางสายไหมดิจิทัลกับปทัสถานด้านความมั่นคงไซเบอร์ของไทย

นายธนาวิทย์ หวังภุชเคนทร์



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญารัฐศาสตรมหาบัณฑิต
สาขาวิชาความสัมพันธ์ระหว่างประเทศ ภาควิชาความสัมพันธ์ระหว่างประเทศ
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

# China's Digital Silk Road and Cybersecurity Norms in Thailand

Mr. Thanawit Wangpuchakane



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Arts in International Relations
Department of International Relations
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2022

| | |
|---|---|
| หัวข้อวิทยานิพนธ์ | การศึกษายุทธศาสตร์เส้นทางสายไหมดิจิทัลกับปทัสถานด้านความมั่นคงไซเบอร์ของไทย |
| โดย | นายธนาวิทย์ หวังภุชเคนทร์ |
| สาขาวิชา | ความสัมพันธ์ระหว่างประเทศ |
| อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก | ผู้ช่วยศาสตราจารย์ ดร.พงศ์พิสุทธิ์ บุษบารัตน์ |

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญารัฐศาสตรมหาบัณฑิต

..... คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.ปกรณ์ ศิริประกอบ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ธีวินท์ สุพุทธิกุล)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.พงศ์พิสุทธิ์ บุษบารัตน์)

..... กรรมการภายนอกมหาวิทยาลัย
(ศาสตราจารย์ ดร.สิทธิพล เครือรัฐติกาล)

ธนาวิทย์ หวังภุชเคนทร์ : การศึกษายุทธศาสตร์เส้นทางสายไหมดิจิทัลกับปทัสถานด้านความมั่นคงไซเบอร์ของไทย. ( China’s Digital Silk Road and Cybersecurity Norms in Thailand) อ.ที่ปรึกษาหลัก : ผศ. ดร.พงศ์พิสุทธิ์ บุษบารัตน์

วิทยานิพนธ์นี้วิเคราะห์การรับรู้ของหน่วยงานและตัวแสดงที่เกี่ยวข้องในไทยเกี่ยวกับปทัสถานทางไซเบอร์ของจีนที่เผยแพร่ผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัล ความเข้าใจของตัวกระทำการเหล่านี้อาจแตกต่างกันไป ซึ่งส่งผลต่อมุมมองของประเทศไทยเกี่ยวกับความมั่นคงไซเบอร์ ปัจจุบันงานศึกษาจำนวนมากให้ความสำคัญกับประเด็นที่เกี่ยวข้องด้านข้อมูล เทคโนโลยีสารสนเทศ และการสื่อสารโทรคมนาคมในความสัมพันธ์ระหว่างประเทศโดยเฉพาะอย่างยิ่งการศึกษาความมั่นคงไซเบอร์ อย่างไรก็ตาม แม้จะมีการวิจัยอย่างครอบคลุมเกี่ยวกับกลยุทธ์เส้นทางสายไหมดิจิทัลและมิติด้านความมั่นคงไซเบอร์ แต่การศึกษาการมีส่วนร่วมของไทย โดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับปทัสถานไซเบอร์ของจีนยังคงมีจำกัด ดังนั้น งานวิจัยนี้จึงกำหนดขอบเขตภายในกรอบการศึกษาผู้ประกอบการเชิงปทัสถาน โดยเน้นที่ยุทธศาสตร์เส้นทางสายไหมดิจิทัลซึ่งเป็นยุทธศาสตร์ที่สำคัญในการแพร่กระจายปทัสถานทางไซเบอร์ของจีน เพื่อตรวจสอบบทบาทของตัวแสดงทั้งจากภาครัฐและเอกชนของไทยในฐานะผู้ประกอบการเชิงปทัสถานที่มีส่วนร่วมในการเผยแพร่และอิทธิพลของปทัสถานไซเบอร์ของจีน การศึกษาชี้ให้เห็นว่ายุทธศาสตร์เส้นทางสายไหมดิจิทัลมีอิทธิพลต่อมุมมองด้านความปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐและเอกชนในประเทศไทย ซึ่งนำไปสู่การยอมรับเทคโนโลยีและปทัสถานด้านความมั่นคงไซเบอร์ของจีนหลายประการเพื่อวัตถุประสงค์ทางธุรกิจและการพัฒนา โดยเฉพาะอย่างยิ่ง "อำนาจอธิปไตยทางไซเบอร์" กลายเป็นประเด็นสำคัญของการถกเถียงเกี่ยวกับปทัสถานทางไซเบอร์ของจีนในเวทีโลก



| | | |
|---|---|---|
| สาขาวิชา | ความสัมพันธ์ระหว่างประเทศ | ลายมือชื่อนิสิต ..... |
| ปีการศึกษา | 2565 | ลายมือชื่อ อ.ที่ปรึกษาหลัก ..... |

# # 6280051324 : MAJOR INTERNATIONAL RELATIONS

KEYWORD: Digital Silk Road, norm entrepreneur, cybersecurity, cyber norms, norm diffusion

Thanawit Wangpuchakane : China’s Digital Silk Road and Cybersecurity Norms in Thailand. Advisor: Asst. Prof. PONGPHISOOT BUSBARAT, Ph.D.

This thesis analyzes the perceptions of relevant agencies and actors in Thailand regarding the propagation of China's cyber norms through the Digital Silk Road Strategy. The understanding of these actors may vary, thereby influencing Thailand's perspective on cybersecurity. Currently, numerous research endeavors focus on examining information-related issues, particularly within the domains of information technology, telecommunications, and cybersecurity studies in the context of international relations. However, the study of Thailand's involvement, specifically concerning China's cyber norms, remains limited despite extensive research on the Digital Silk Road strategy and various dimensions of cybersecurity. Thus, this research establishes boundaries within the framework of norm entrepreneur study, with a specific focus on the Digital Silk Road strategy as a significant approach for spreading China's cyber norms. The intention is to investigate the role played by actors in Thailand's public and private sectors as norm entrepreneurs, contributing to the dissemination and influence of China's cyber norms. The study reveals that the Digital Silk Road Strategy has influenced the cybersecurity perspectives of actors in Thailand's public and private sectors, resulting in the adoption of several Chinese cybersecurity technologies and norms for business and developmental purposes. Notably, the concept of "cyber sovereignty" emerges as a prominent point of debate surrounding China's cyber norms on the global stage.



| | | |
|---|---|---|
| Field of Study: | International Relations | Student's Signature ..... |
| Academic Year: | 2022 | Advisor's Signature ..... |

# กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยความพยายาม ความตั้งใจ และความใส่ใจของผู้เขียนและผู้มีพระคุณทั้งหลายที่ทำให้วิทยานิพนธ์ฉบับนี้สำเร็จเป็นอย่างดี

ผู้เขียนขอขอบคุณ ผู้ช่วยศาสตราจารย์ ดร. พงศ์พิสุทธิ์ บุษบารัตน์ อาจารย์ที่ปรึกษาประจำวิทยานิพนธ์ที่กรุณาสละเวลาอันมีค่าคอยชี้แนะ ใส่ใจ และให้กำลังใจผู้เขียนเป็นอย่างดียิ่ง

ผู้เขียนขอขอบคุณ ผู้ช่วยศาสตราจารย์ ดร. ธีวินท์ สุพุทธิกุล ที่ได้กรุณารับเป็นประธานกรรมการสอบวิทยานิพนธ์ และศาสตราจารย์ ดร. สิทธิพล เครือรัฐติกาล ที่ได้กรุณารับเป็นกรรมการสอบวิทยานิพนธ์ภายนอก ซึ่งทั้งสองท่านได้ให้คำชี้แนะ ใส่ใจ และให้ความร่วมมือในฐานะประธานและกรรมการได้อย่างดียิ่ง

ผู้เขียนขอขอบคุณ คุณมฤษฎา คำสิทธิ มิตรใกล้ชิดซึ่งเป็นที่ยึดเหนี่ยวจิตใจสำหรับผู้เขียนมาโดยตลอด รวมถึงมิตรสนิทท่านอื่นที่ไม่ได้เอ่ยนามมาทั้งหมดเช่นกัน

ผู้เขียนขอขอบคุณ ครอบครัวและญาติสนิททุกท่านที่เป็นกำลังใจ และสนับสนุนผู้เขียนตลอดการเขียน

รวมทั้งขอขอบคุณ คณาจารย์ท่านอื่นทั้ง อาจารย์ภาณุภัทร จิตเที่ยง อาจารย์ณัฐนันท์ คุณมาศ คณาจารย์ท่านอื่นที่ไม่ได้เอ่ยนามมาทั้งหมด และเจ้าหน้าที่คณะทุกท่านสำหรับการสั่งสอนและสนับสนุนผู้เขียนเป็นอย่างดี

ท้ายที่สุด ผู้เขียนยินดีอย่างยิ่งหากงานชิ้นนี้จะเป็นคุณประโยชน์ต่อแวดวงวิชาการทางใดทางหนึ่ง หากงานชิ้นนี้มีข้อบกพร่องประการใด ผู้เขียนจะขอรับความบกพร่องเหล่านั้นไว้ ณ ที่นี้



ธนาวิทย์ หวังภุชเคนทร์

# สารบัญ

**หน้า**

# บทที่ 1

# บทนำ

## ที่มาและความสำคัญ

เส้นทางสายไหมใหม่ หรือเส้นทางสายไหมแห่งศตวรรษที่ 21 ที่รู้จักกันในชื่อ “ข้อริเริ่มแถบและทาง (Belt and Road Initiative: BRI)” ซึ่งถูกประกาศครั้งแรกโดยประธานาธิบดีสี จิ้นผิง ในปี ค.ศ. 2013 เส้นทางดังกล่าวเชื่อมโยงการค้าระหว่างจีนและเปอร์เซียในอดีต โดยเส้นทางสายไหมนั้นแรกเริ่มถูกกล่าวถึงเฉพาะว่าเป็นเส้นทางขนส่งทางบก แต่ในเวลาต่อมาได้มีการขยายเส้นทางสู่การขนส่งทางทะเลด้วย เพื่อเป็นการสร้างความปลอดภัยในการเดินทาง ณ ขณะนั้น ส่งผลให้เกิดความสัมพันธ์ทางเศรษฐกิจและการค้าในแถบมหาสมุทรอินเดียขึ้นอย่างต่อเนื่อง เกิดการสร้างเมืองท่าเพื่อตอบสนองต่อความทะเยอทะยานของจีนในขยายตลาดออกนอกภูมิภาค การพัฒนาความร่วมมือทางโครงสร้างพื้นฐานในภูมิภาค เป็นความพยายามของจีนในการเชื่อมโยงพรมแดนระหว่างรัฐด้วยการพัฒนาโครงสร้างทางคมนาคม โดยเฉพาะอย่างยิ่ง การสร้างทางรถไฟ สนามบิน และเมืองท่า รวมถึงการบูรณาการทางเศรษฐกิจครอบคลุมทั้งทวีปเอเชีย ยุโรปและตะวันออกกลาง โดยรัฐบาลจีนเชื่อว่ายุทธศาสตร์นี้จะเปิดโอกาสให้ได้รับผลประโยชน์ร่วมกันตลอดเส้นทาง ส่งเสริมให้เกิดความร่วมมือทางเศรษฐกิจ การค้าและการลงทุนข้ามพรมแดน ก่อให้เกิดการเชื่อมโยงระหว่างนักลงทุน ตลาด การเกิดติดต่อกันระหว่างนักท่องเที่ยวชาวจีนกับชาติอื่น ๆ ความริเริ่มในยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทาง

อย่างไรก็ตามนอกจากการพัฒนาโครงสร้างพื้นฐานเชิงกายภาพแล้วนั้น หนึ่งในยุทธศาสตร์ที่สำคัญภายใต้กรอบการริเริ่มยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทาง คือ ยุทธศาสตร์เส้นทางสายไหมดิจิทัล (Digital Silk Road: DSR) เพื่อเสริมสร้างความเชื่อมโยงระหว่างรัฐ ไม่เพียงเฉพาะโครงสร้างพื้นฐานทางกายภาพ (physical infrastructure) แต่รวมถึงการพัฒนาโครงสร้างพื้นฐานทางดิจิทัลด้วย (digital infrastructure) กล่าวคือ เป็นการบูรณาการนำเทคโนโลยีและระบบเครือข่ายไร้สายหรืออินเทอร์เน็ตเข้ามาผนวกกับการพัฒนาโครงการพื้นฐานที่เกี่ยวข้องกับยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทาง เพื่อความสอดคล้องกับการพัฒนาด้านอุตสาหกรรมภายในของประเทศจีน รัฐบาลจีนเชื่อว่าประเทศผู้เกี่ยวข้องจะได้รับการเสริมสร้างการวางโครงข่ายอินเทอร์เน็ตและความเชื่อมโยงระหว่างรัฐด้วยเทคโนโลยีสารสนเทศที่มากขึ้น เช่น เกิดการแลกเปลี่ยนข้อมูลทางสถิติ การเข้าถึงคลังข้อมูลที่ถูกเก็บรักษาไว้ในโครงข่ายอินเทอร์เน็ต หรือคลาวด์ สามารถเข้าถึงระบบประมวลผล คาดการณ์และจัดการเหตุผ่านระบบปัญญาประดิษฐ์ ความร่วมมือในการจัดการพัฒนาแพลตฟอร์มทางการค้าระหว่างจีน เป็นต้น

นโยบายการพัฒนาด้านอุตสาหกรรมของประเทศจีนมีแนวโน้มสามประการ ซึ่งเกี่ยวข้องกับยุทธศาสตร์เส้นทางสายไหมดิจิทัล ประการแรก นโยบายอุตสาหกรรมที่ให้ความสำคัญกับการพัฒนาเทคโนโลยีที่เน้นการใช้ปัญญาประดิษฐ์มากขึ้น การโทรคมนาคมด้วยเทคโนโลยีเครือข่าย 5Gและเครือข่ายอัจฉริยะ ประการที่สอง ลักษณะการดำเนินนโยบายภายใต้บริษัทเอกชนเป็นลักษณะของการที่รัฐบาลจีนมีบทบาทนำบริษัทเหล่านั้น กล่าวคือ บริษัทเอกชนที่เกี่ยวข้องนั้นมีความร่วมมือที่ใกล้ชิดกับรัฐบาลอย่างมาก เช่น Alibaba, Baiduและ Tencent เป็นต้น ประการที่สาม นโยบายระดับภูมิภาคโดยเฉพาะอย่างยิ่งนโยบายที่มีลักษณะการพัฒนาโครงสร้างพื้นฐาน ได้แก่ เส้นทางรถไฟ เมืองท่า ท่าอากาศยาน รวมไปถึงโครงข่ายเทคโนโลยีไร้สาย เพื่อสร้างกลุ่มเมืองกระจายทั่วภูมิภาค โดยมีประเทศจีนเป็นศูนย์กลางโครงการริเริ่มหนึ่งแถบหนึ่งเส้นทาง เป็นโครงการหลักที่สำคัญภายใต้ยุทธศาสตร์จีน ซึ่งเป็นโครงการสนับสนุนการพัฒนาโครงสร้างพื้นฐานที่รัฐบาลจีนออกแบบมาเพื่อผูกมัดประเทศจีนกับประเทศคู่เจรจาให้มีความใกล้ชิดกันมากขึ้น ด้วยเหตุดังกล่าวประเด็นการพัฒนาโครงสร้างพื้นฐานในลักษณะดิจิทัล (digital infrastructure) จึงกลายเป็นประเด็นสำคัญซึ่งถือเป็นส่วนหนึ่งการเชื่อมโยงระหว่างรัฐในโครงการริเริ่มหนึ่งแถบหนึ่งเส้นทาง

อย่างไรก็ดี สำหรับประเทศผู้เกี่ยวข้องจำเป็นต้องพิจารณายุทธศาสตร์ขนาดใหญ่ดังกล่าวอย่างรอบคอบ บริษัทจีนซึ่งขยายตัวเข้าไปมีส่วนในการพัฒนาเครือข่ายการสื่อสารโทรคมนาคมในชาติที่เกี่ยวข้องนั้น อาทิ ทั้งการวางโครงสร้างพื้นฐานกายภาพการเดินเครือข่ายอินเทอร์เน็ต ในรูปแบบดิจิทัลผ่านการพัฒนาแอปพลิเคชัน เป็นต้น ปฏิเสธไม่ได้ว่ายุทธศาสตร์เส้นทางสายไหมดิจิทัลนั้นส่งผลให้เกิดการเชื่อมโยงที่ใกล้ชิดกันในการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร ดังนั้นประเทศผู้เกี่ยวข้องควรมีความตระหนักถึงความเสี่ยงในมิติความมั่นคงทางไซเบอร์ที่อาจเกิดขึ้นจากยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน



ประเทศไทยเป็นหนึ่งในประเทศที่มีความเกี่ยวข้องและสำคัญอย่างมากต่อการดำเนินยุทธศาสตร์เส้นทางสายไหมศตวรรษที่ 21 ซึ่งมีความเชื่อมโยงกับการพัฒนาเส้นทางสายไหมทางทะเล เส้นทางสายไหมทางบกและเส้นทางสายไหมดิจิทัล กล่าวคือ ประเทศไทยเป็นหนึ่งในประเทศที่มีความเชื่อมโยงกับโครงการระเบียงเศรษฐกิจ (Eastern Economic Corridor: EEC) ซึ่งเป็นพื้นที่พิจารณาสำคัญที่สามารถเชื่อมโยงเข้าเป็นส่วนหนึ่งของระเบียงเศรษฐกิจภายใต้ยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทางได้ โดยในปี 2019 สำนักงาน Economic Corridor Office of Thailand (EECO) ทำข้อตกลงกับบริษัท Alibaba ให้มีบทบาทในการพัฒนาธุรกิจ E-commerce platform เพื่อสนับสนุนการท่องเที่ยวและใช้เทคโนโลยีดิจิทัล อาจกล่าวได้ว่าเป็นการบูรณาการในแบบ Smart Infrastructure ภายใต้ยุทธศาสตร์ดิจิทัลของจีน เพื่อกระตุ้นสินค้าไทยสู่ผู้บริโภคชาวจีนผ่านการ

ให้บริการซื้อขายออนไลน์ ทั้งนี้แนวนโยบายและการพัฒนาความร่วมมือภายใต้ยุทธศาสตร์ดังกล่าวสอดคล้องกับแนวทางตามแผนยุทธศาสตร์ชาติ 20 ปีของไทย

อนึ่ง ในแผนยุทธศาสตร์ชาติ 20 ปี ระบุไว้ว่าไทยมีความพยายามที่จะส่งเสริมขีดความสามารถในการแข่งขันของประเทศ โดยการเชื่อมโยงโครงข่ายคมนาคมไร้รอยต่อ เชื่อมโยงโครงข่ายคมนาคมในภูมิภาคโดยมีไทยเป็นจุดเชื่อมหลักของการคมนาคมให้เป็นระเบียงเศรษฐกิจแห่งเอเชีย หรือเป็นศูนย์กลางทางการคมนาคมเพื่อการค้า การลงทุนและการท่องเที่ยวของภูมิภาค ด้วยเหตุนี้ ประเทศไทยจำเป็นต้องยกระดับโครงสร้างพื้นฐานทางเศรษฐกิจของประเทศให้มีขีดความสามารถที่สูงขึ้น อาทิ การลงทุนเพื่อพัฒนาระบบรางหรือทางรถไฟ เพื่อลดต้นทุนด้านขนส่ง การสร้างความเชื่อมโยงระหว่างการเดินทางทางอากาศและการขนส่งสินค้าทางเรือ เข้ากับระบบราง เพื่อให้ไทยเป็นจุดเชื่อมโยงที่สำคัญภายในภูมิภาคที่เชื่อมโยงกับประเทศจีน ก่อให้เกิดการดึงดูดการลงทุนจากต่างประเทศและการพัฒนาเครื่องมือในรูปแบบดิจิทัล เพื่อเป็นเครื่องมือในการบูรณาการเข้ากับการพัฒนาในทุกภาคส่วนของประเทศ เป็นต้น

อย่างไรก็ตามภายใต้ยุทธศาสตร์ของจีนนั้นเกิดข้อถกเถียงซึ่งสร้างความกังวลให้กับประเทศผู้เกี่ยวข้องหลายประเด็น โดยเฉพาะอย่างยิ่งประเด็นด้านความมั่นคงในหลากหลายมิติ เช่น ความมั่นคงทางเศรษฐกิจ การเมืองจากการทูตกับดักหนี้ (dept-trap diplomacy) ความมั่นคงทางเศรษฐกิจ การลงทุนจากการผูกขาด ข้อผูกมัดในการลงทุนที่มีจีนเป็นผู้กำหนด รวมถึงความไม่ชัดเจนของการดำเนินกิจกรรมที่เกิดขึ้นในโครงการที่จีน ความมั่นคงด้านข้อมูลทางไซเบอร์และเทคโนโลยีสารสนเทศจากการพัฒนาโครงข่ายอินเทอร์เน็ต เป็นต้น

เส้นทางสายไหมดิจิทัลก่อให้เกิดความกังวลต่อสถานการณ์การแข่งขันและสภาพความขัดแย้งระหว่างจีนและสหรัฐฯ ในภาพใหญ่ กล่าวคือ เส้นทางสายไหมดิจิทัลก่อให้เกิดการเติบโตของการแข่งขันในด้านดังกล่าวระหว่างสหรัฐฯ และจีน ซึ่งส่งผลต่อการพัฒนาเทคโนโลยีสารสนเทศของโลก ความมั่นคงของระบบเศรษฐกิจโดยเฉพาะในด้านเทคโนโลยีก่อให้เกิดการแบ่งออกเป็น 2 ภาคส่วน คือ กลุ่มพันธมิตรของสหรัฐฯ โดยเฉพาะประเทศกลุ่มเสรีนิยมประชาธิปไตย อีกกลุ่ม คือ กลุ่มประเทศที่พึ่งพาข้อมูลและเทคโนโลยีสารสนเทศที่มีฐานความเชื่อมโยงโดยจีน (Chinese-based) การแข่งขันดังกล่าวส่งผลต่อบริษัทโทรคมนาคม รวมถึงระบบห่วงโซ่อุปทานทั้งในระดับโลกและระดับภูมิภาค ในขณะที่การแข่งขันระหว่าง 2 ค่ายในเวทีโลกยังคงเติบโตขึ้น ยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีนได้เพิ่มความตรึงเครียดในการแข่งขันมากขึ้น อีกทั้งยังสร้างแรงกดดันให้กับประเทศเกี่ยวข้อง โดยเฉพาะอย่างยิ่งในหลายประเทศที่ต้องพึ่งพาข้อมูล เทคโนโลยีสารสนเทศจากทั้ง 2 ค่าย ก่อให้เกิดทางแพ่งของทางเลือก (dilemma) ในการตัดสินใจด้านนโยบาย โดยอย่างน้อยที่สุดประเทศที่เกี่ยวข้องดังกล่าวอาจต้องดำเนินยุทธศาสตร์เพื่อความมั่นคงทางเศรษฐกิจและเทคโนโลยีตาม

มาตรการของแต่ละค่าย หรืออย่างเลวร้ายผู้มีอำนาจตัดสินใจทางนโยบายอาจต้องตัดสินใจเลือกในทางแพ่งนี้ว่าค่ายใดสำคัญกว่า

หากกล่าวถึงประเด็นด้านข้อมูล เทคโนโลยีสารสนเทศและโทรคมนาคมแล้ว มิติความมั่นคงทางไซเบอร์เป็นหนึ่งในประเด็นที่ไม่อาจมองข้ามได้ อย่างไรก็ดี การศึกษาในปัจจุบันในเรื่องความมั่นคงและการป้องกันของการบูรณาการเทคโนโลยีสารสนเทศของจีนเข้ากับระบบดิจิทัลระดับชาตินั้นมีนัยสำคัญเกี่ยวข้องกับภัยคุกคามที่อาจเกิดขึ้นจากความร่วมมือด้านข่าวกรองและความร่วมมือในการป้องกันประเทศ อย่างไรก็ตามความหมายของ “ระบบนิเวศ (ecosystem)” ในด้านดิจิทัลของจีนสำหรับการศึกษาด้านความมั่นคงไซเบอร์ในอุตสาหกรรมตะวันตกและกลุ่มประเทศที่มีความเชื่อมโยงภายใต้อุตสาหกรรมดังกล่าวนั้น ยังคงไม่ได้ถูกศึกษาอย่างชัดเจน ซึ่งสมควรได้รับความสนใจมากขึ้น

ประเทศไทยต้องเผชิญความท้าทายภายใต้ความกังวล 2 ประการ ได้แก่ ประการแรก ข้อกังวลต่อเศรษฐกิจของไทยซึ่งตกอยู่ในกับดักรายได้ปานกลาง (middle trap income) ประการที่สอง ข้อกังวลต่อความมั่นคงและความเสี่ยงที่อาจเกิดขึ้นจากยุทธศาสตร์เส้นทางสายไหมดิจิทัล ซึ่งไทยต้องพิจารณาข้อกังวลทั้งสอง ประการข้างต้น โดยในบริบทของไทยอยู่ในฐานะที่เป็นประเทศที่มีส่วนเกี่ยวข้องกับยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทางและภายใต้การบูรณาการทางเทคโนโลยีตามยุทธศาสตร์เส้นทางสายไหมดิจิทัล นอกจากนี้ไทยยังเป็นประเทศที่ต้องพึ่งพาข้อมูลและเทคโนโลยีจากทั้ง 2 ค่าย ผลที่ตามมาอาจนำมาสู่ความลักลั่นในการตัดสินใจกำหนดนโยบายในประเด็นดังกล่าว ในขณะเดียวกันรัฐบาลต้องตระหนักถึงภัยคุกคามที่อาจเกิดขึ้นทางไซเบอร์เป็นสำคัญ

เมื่อพิจารณาประเด็นความมั่นคงทางไซเบอร์และความเสี่ยงที่อาจเกิดขึ้นกับประเทศที่เกี่ยวข้องโดยมียุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีนเป็นบริบทแวดล้อมที่เกิดขึ้นในภูมิภาค ประกอบกับเงื่อนไขของไทยซึ่งมีความต้องการในการยกระดับขีดความสามารถในการแข่งขันของประเทศตามแผนยุทธศาสตร์ชาติ 20 ปี ข้างต้น ก่อให้เกิดคำถามเชิงคาดการณ์ 4 ข้อ ประการแรก อะไรคือความเสี่ยงที่อาจเกิดขึ้นของโครงสร้างพื้นฐานดิจิทัลของจีน ต่อความมั่นคง อุตสาหกรรมและเศรษฐกิจของรัฐ ประการที่สอง การบูรณาการทางเทคโนโลยีสารสนเทศของจีนและโครงสร้างพื้นฐานดิจิทัล สร้างความท้าทายทางข้อมูลของผู้เกี่ยวข้องและความร่วมมือด้านการป้องกันในระดับใด ประการที่สาม การบูรณาการระดับใดที่ควรพิจารณาว่ามีนัยสำคัญต่อความมั่นคงและความร่วมมือด้านความมั่นคง (เช่น การนำเข้า-ส่งออกอาวุธ) จะได้รับผลกระทบอย่างไร ประการที่สี่ ตัวแสดงทั้งภาครัฐและเอกชนของไทยมีมุมมองและความตระหนักต่อประเด็นความมั่นคงทาง ไซเบอร์อย่างไร

อย่างไรก็ตามโครงการขนาดใหญ่ดังกล่าวของจีนนั้น เมื่อพิจารณาถึงความหลากหลายทั้งสภาพภูมิรัฐศาสตร์ สภาพแวดล้อมทางการเมือง เศรษฐกิจและสังคมแล้วนั้น ประเด็นสำคัญที่ไม่อาจมองข้ามได้ คือ ความเข้าใจที่สอดคล้องกันของการตีความตัวนโยบายหนึ่งแถบหนึ่งเส้นทางของจีน ทั้ง

จากหน่วยงานภาครัฐ ภาคเอกชน เพื่อให้เกิดความเป็นหนึ่งเดียวกัน (unity) ของการดำเนินนโยบายและกิจกรรม หากตัวแสดงที่เกี่ยวข้องเหล่านั้นมีความเข้าใจที่สอดคล้อง หรือเป็นไปในทำนองเดียวกันจะส่งผลให้การออกแบบกิจกรรมมีความชัดเจน เป็นหนึ่งเดียวกันขององค์กรภายในประเทศมากยิ่งขึ้น จะส่งผลในเชิงบวกต่อการปรับตัวสอดรับกับยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน ซึ่งเป็นผลดีต่อการดำเนินนโยบายต่างประเทศระหว่างไทยและจีนอย่างมาก

ด้วยเหตุนี้งานวิจัยชิ้นนี้จึงพยายามศึกษาเพื่อเติมเต็มคำถามข้างต้น ในการวิเคราะห์ในปัจจุบันโดยสรุปความเสี่ยงที่อาจเกิดขึ้นจากการลงทุนด้านดิจิทัลและเทคโนโลยีทั้งในระดับภูมิภาคและระดับโลกของจีน รวมถึงการวิเคราะห์ขอบเขตของกิจกรรมภายใต้เส้นทางสายไหมดิจิทัลของจีนในไทย จุดมุ่งหมายเพื่อก่อให้เกิดข้อมูลเชิงลึกมากขึ้นเกี่ยวกับการตัดสินใจของรัฐบาลในการกำหนดแนวทางนโยบายในอนาคต

**คำถามวิจัย**

หน่วยงานหรือตัวแสดงที่เกี่ยวข้องในประเทศไทยมีความเข้าใจปทัสถานของจีนผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัลมากน้อยเพียงใด ความเข้าใจนั้นสอดคล้องหรือแตกต่างกันอย่างไร และตัวแสดงที่เกี่ยวข้องเหล่านั้นในประเทศไทยมีมุมมอง ต่อประเด็นความมั่นคงทางไซเบอร์อย่างไร มุมมองเหล่านั้นมีความตระหนักร่วมกันหรือแตกต่างกันหรือไม่ อย่างไร

**ข้อถกเถียง**

ผู้วิจัยได้พิจารณาและตั้งข้อสังเกตเพื่อสอดคล้องกับการศึกษาชิ้นนี้ นำมาซึ่งสมมติฐานเบื้องต้นว่า

1) ตัวแสดงเชิงปทัสถานที่เกี่ยวข้องในไทยมีความหลากหลายอย่างมาก ส่งผลให้มุมมองและความเข้าใจของตัวแสดงเหล่านั้นไม่มีความเป็นหนึ่งเดียวกัน
2) ตัวแสดงเชิงปทัสถานที่เกี่ยวข้องในไทยมีความตระหนักในประเด็นความมั่นคงไซเบอร์ต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัล แต่ใช้เครื่องมือในการรับและแพร่กระจายปทัสถานเพื่อให้สอดคล้องกับบริบทภายในประเทศ ส่งผลให้ความกังวลต่อปทัสถานไซเบอร์ของจีนถูกบิดเบือนไปอย่างมีนัยสำคัญ

**วัตถุประสงค์การศึกษา**

1. เพื่อศึกษาและวิเคราะห์หลักการ การตีความยุทธศาสตร์เส้นทางสายไหมแห่งศตวรรษที่ 21 ในกรอบยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน
2. เพื่อศึกษาและวิเคราะห์การตีความ การตอบสนอง นำไปใช้ของผู้ประกอบการเชิงปทัสถานในประเทศไทยทั้งภาครัฐและเอกชนต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน

3. เพื่อศึกษาและวิเคราะห์มุมมองด้านความมั่นคงไซเบอร์ของตัวแสดงที่เกี่ยวข้องในประเทศไทยทั้งภาครัฐและเอกชนต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน

**การทบทวนวรรณกรรมที่เกี่ยวข้อง**

การศึกษายุทธศาสตร์เส้นทางสายไหมสายดิจิทัลในปัจจุบันถูกให้ความสนใจอย่างมาก โดยเฉพาะอย่างยิ่งในสังคมตะวันตก ปฏิเสธไม่ได้ว่าประเด็นที่เกี่ยวกับข้อมูล เทคโนโลยีสารสนเทศและโทรคมนาคมเป็นประเด็นที่น่าสนใจและมีความสำคัญในการศึกษาทางวิชาการในสมัยใหม่ จากการศึกษาเอกสารและบทความทางวิชาการเพื่อใช้ในการจำแนกกลุ่มการศึกษา ผู้เขียนพบว่าวรรณกรรมในประเด็นดังกล่าวได้ถูกแจกแจงไว้เป็น 4 กลุ่ม <u>กลุ่มที่หนึ่ง</u> กล่าวถึงภาพรวมของยุทธศาสตร์เส้นทางสายไหมดิจิทัล ซึ่งอธิบายถึงที่มาและบทบาทของเส้นทางสายไหมดิจิทัล โดยอธิบายย้อนไปถึงยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทางและแนวทางการกำหนดนโยบายด้านอุตสาหกรรมของจีนในช่วงทศวรรษก่อน <u>กลุ่มที่สอง</u> ให้ความสนใจอย่างเจาะจงในเรื่องความมั่นคงในยุคสมัยใหม่ โดยเฉพาะอย่างยิ่งความมั่นคงหลังจากที่จีนได้ประกาศยุทธศาสตร์เชิงบูรณาการ ซึ่งอธิบายถึงความกังวลที่อาจเกิดขึ้นจากยุทธศาสตร์เหล่านั้น <u>กลุ่มที่สาม</u> พบว่างานศึกษาจำนวนมากในช่วงทศวรรษที่ผ่านมาให้ความสนใจประเด็นทางเทคโนโลยี โดยเฉพาะอย่างยิ่งความมั่นคงในโลกสมัยใหม่ ประเด็นเรื่องเทคโนโลยีสารสนเทศและโทรคมนาคม ซึ่งอธิบายถึงความเสี่ยงที่อาจเกิดขึ้นและมาตรการป้องกันความเสี่ยงเหล่านั้น <u>กลุ่มสุดท้าย</u> วรรณกรรมซึ่งกล่าวถึงช่วงเวลาในปัจจุบัน โดยเฉพาะอย่างยิ่งการศึกษาเพื่อคาดการณ์แนวโน้มที่อาจจะเกิดขึ้นในยุคหลังการแพร่ระบาดของโรคโควิด 19

<u>กลุ่มที่หนึ่ง</u> งานศึกษาซึ่งกล่าวถึงภาพรวมของยุทธศาสตร์เส้นทางสายไหมดิจิทัล ซึ่งนำประเด็นเทคโนโลยีมาบูรณาการเข้ากับยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทาง งานศึกษาจำนวนหนึ่งให้ความสำคัญกับการศึกษาทางประวัติศาสตร์ของจีน เพื่อชี้ให้เห็นถึงพัฒนาการของการดำเนินนโยบายภายในของจีน งานศึกษาจำนวนมากอธิบายว่า หนึ่งในแรงจูงใจที่สำคัญประการหนึ่งของยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทาง คือปัญหาในการล้นของตลาดอุตสาหกรรม (industrial overcapacity) ขีดความสามารถในการผลิตส่วนเกินที่เรื้อดังกล่าวมาพร้อมกับการรวมตัวกันของการลงทุนโดยตรงจากประเทศอื่น ซึ่งการลงทุนเหล่านั้นขับเคลื่อนและมุ่งเน้นโดยเฉพาะการส่งออกเข้ากับระบบทุนนิยมโลกตั้งแต่ปลายทศวรรษที่ 1970 นักวิชาการจำนวนหนึ่งอธิบายรูปแบบอุตสาหกรรมของจีนมีลักษณะรวมกำลังการผลิตส่วนเกิน เป็นสิ่งที่เกิดขึ้นมาแต่เดิมนับตั้งแต่ปี ค.ศ. 1978และได้กลับมาได้รับความสำคัญใหม่อีกครั้งภายใต้การบริหารของรัฐบาลสี จิ้นผิง เนื่องจากเศรษฐกิจจีนชะลอตัวลง ในปี ค.ศ. 2013 สภาแห่งชาติได้ออกหนังสือ “guiding opinion” ซึ่งเป็นความเห็นชี้นำต่อปัญหาของการล้นตลาดของประเทศจีน เกิดข้อเสนอให้มีการจัดการประเด็นดังกล่าว ด้วยการขยายตลาดสู่ภายนอก “actively expand the external market” (Naughton, Chen, & Barry, 2016)

ในขณะที่รัฐบาลจีนคาดหวังว่ายุทธศาสตร์หนึ่งแถบหนึ่งเส้นทางจะมีบทบาทสำคัญในการแก้ไขปัญหาดังกล่าว นักวิชาการจีนอธิบายวิธีการดังกล่าวสามารถเกิดขึ้นได้ผ่าน 2 วิธีหลัก ประการแรก จัดการให้เกิดการดูดซับกำลังการผลิตส่วนเกินของจีนผ่านการสร้างโครงสร้างพื้นฐานขนาดใหญ่ทั้งในพื้นที่ที่มีการพัฒนาน้อยและในต่างประเทศ ประการที่สอง โดยการอำนวยความสะดวกในการส่งออกสินค้าและอุปกรณ์ส่วนเกินของจีนผ่านการขยาย เพื่อปรับโครงสร้างเครือข่ายการผลิตและการค้าระหว่างประเทศ (Cai, Jun, & Yang, 2009) Guo (2017) ชี้ว่าการบูรณาการด้านเทคโนโลยีเข้ามาเป็นส่วนหนึ่งกับการพัฒนาโครงสร้างพื้นฐานดังเช่นยุทธศาสตร์เส้นทางสายไหมดิจิทัล จะส่งผลให้เกิดความเชื่อมโยงระหว่างรัฐมากขึ้น อีกทั้งยังสามารถยกระดับให้ตลาดเทคโนโลยีของจีนกลายเป็น “ผู้บุกเบิก” และสร้าง “มาตรฐาน” ให้กับอุตสาหกรรมทางเทคโนโลยีได้อีก (Sadasivam, Samudrala, & Yang, 2005)

การศึกษายุทธเส้นทางสายไหมดิจิทัลกับมิติความมั่นคงเป็นอีกกลุ่มวรรณกรรมที่ถูกให้ความสำคัญ โดยเฉพาะอย่างยิ่งในประเด็นที่มีความเกี่ยวข้องกับความมั่นคงรูปแบบใหม่ การศึกษาจำนวนมากอธิบายว่า จีนดำเนินนโยบายเชิงรุกอย่างมากในการดำเนินยุทธศาสตร์ทางเศรษฐกิจระหว่างรัฐและต่อการพัฒนาทางเทคโนโลยี ซึ่งก่อให้เกิดความตึงเครียดในบรรยากาศการแข่งขันทางการค้ากับสหรัฐฯ (Conley, Hillman, McCalpin, & Ruy, 2020) การแข่งขันทางการค้าและการพัฒนาทางเทคโนโลยีส่งผลต่อห่วงโซ่การผลิตในภาพกว้าง Le Corre (2018) อธิบายว่าการพัฒนาเทคโนโลยี 5G เป็นสัญญาณสำคัญของความพยายามเข้ามามีบทบาทนำในบทบาทของผู้นำทางเทคโนโลยีโลก นำมาซึ่งมาตรการตอบโต้ของสหรัฐฯ และการกดดันเพื่อไม่ให้เกิดการนำเทคโนโลยี 5G ซึ่งถูกพัฒนาโดยจีน มาตรการกดดันและการห้ามใช้เทคโนโลยีของจีนส่งผลให้เกิดทาง 2 แพ่งในการดำเนินนโยบาย เกิดตัวเลือกระหว่างเทคโนโลยีโลกตะวันตกและเทคโนโลยีโลกตะวันออก นักวิชาการจำนวนหนึ่งอธิบายว่า ปัญหาห่วงโซ่อุปทานที่เกิดจากมาตรการการห้ามใช้เทคโนโลยีจีนในโลกเสรีนั้นส่งผลกระทบอย่างชัดเจนโดยเฉพาะอย่างยิ่งประเทศที่ 3 ซึ่งเป็นฐานการผลิตชิ้นส่วนอิเล็กทรอนิกส์ (Conley et al., 2020) Tugendhat and Voo (2021) ได้ยกตัวอย่างสถานการณ์ไว้ 2 รูปแบบ ที่อาจเกิดขึ้นในประเทศที่ 3 ซึ่งเป็นฐานการผลิตและเป็นประเทศที่ต้องพึ่งพาข้อมูล เทคโนโลยีจากทั้ง 2 ค่าย ซึ่งอาจก่อให้เกิดทางเลือกที่ลักลั่น จนอาจนำไปสู่การตัดสินใจที่ส่งผลกระทบต่อเศรษฐกิจและความสัมพันธ์ระหว่างประเทศในระยะยาวได้

กลุ่มที่สาม งานศึกษาที่ให้ความสนใจเฉพาะเจาะจงในเรื่องความมั่นคงไซเบอร์ พบว่างานศึกษาจำนวนมากในช่วงทศวรรษที่ผ่านมาให้ความสนใจประเด็นทางเทคโนโลยี โดยเฉพาะอย่างยิ่งความมั่นคงในโลกสมัยใหม่ งานศึกษาจำนวนมากให้ความกังวลต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัลในความมั่นคงของข้อมูลเป็นอย่างมาก โดยเส้นทางสายไหมดิจิทัลมีวัตถุประสงค์ในการเชื่อมโยง

ประเทศทางทะเลและเส้นทางของยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทาง ผ่านเครือข่ายโทรคมนาคม ซึ่งเป็นอีกหนึ่งเครื่องมือที่จะทำให้จีนมีผลประโยชน์เหนือผู้เกี่ยวข้อง (Dekker & Okano-Heijmans, 2020) Khalil (2020) อธิบายถึงรูปแบบดิจิทัลภายใต้การระบอบการปกครองแบบอำนาจนิยมของจีน (Authoritarianism) ในช่วงการแพร่ระบาดของโควิดไว้อย่างน่าสนใจว่า หนึ่งในตัวอย่างที่สำคัญของการใช้ดิจิทัลในจีนภายใต้ระบอบดังกล่าวนั้น รัฐบาลจีนมีอำนาจเด็ดขาดในการควบคุมข้อมูลข่าวสาร Khalil ชี้ให้เห็นว่ารัฐบาลจีนปิดกั้นข้อมูลข่าวสาร รวมถึงให้ข้อมูลเท็จต่อประชาคมถึงการแพร่ระบาดโควิด 19 ในช่วงแรก อันส่งผลให้เกิดผลกระทบทางเศรษฐกิจและการเมืองระหว่างประเทศ Hurley, Morris, and Portelance (2019) ชี้ให้เห็นในลักษณะเดียวกันว่า รัฐบาลจีนมีความพยายามในการแทรกแซงและโน้มนำทางการเมือง ในงานศึกษาชี้ตัวอย่างเกิดขึ้นจากกรณีบริษัท Huawei ซึ่งเป็นบริษัททางเทคโนโลยีสัญชาติจีนที่มีบทบาทสำคัญในหลายประเทศ มีอิทธิพลและมีอำนาจโน้มนำทางผลประโยชน์เนื่องจากมีความผูกติดกับโครงสร้างพื้นฐานทางเทคโนโลยีโดยเฉพาะเป็นผู้ให้บริการ 5G ในประเทศซึ่งพึ่งพาเทคโนโลยีจากจีนเป็นหลัก กรณีศึกษาดังกล่าวพบเช่นเดียวกันในประเทศเกาหลีใต้ (Lee, Rasser, Fitt & Goldberg, 2020) อย่างไรก็ตามต้องตระหนักไว้เสมอว่า เครือข่ายการทำงานของอินเทอร์เน็ตในประเทศจีนนั้นมีความแตกต่างและแยกตัวออกมาจากเครือข่ายทางเทคโนโลยีของโลกเสรีอยู่ในหลายระบบ ในขณะเดียวกัน นักวิชาการจำนวนหนึ่งอธิบายว่า เครือข่ายที่แยกตัว แตกต่างกันของการทำงานและการเก็บข้อมูลอาจก่อให้เกิดความเสี่ยงในการควบคุมข้อมูลอยู่ที่รัฐบาลจีนฝ่ายเดียว ซึ่งเป็นที่ชัดเจนแล้วว่านานาประเทศให้ความตระหนักและกังวลต่อความพยายามของจีนในการเข้ามาเป็นผู้นำทางเทคโนโลยีของโลก (Lee, Rasser, Fitt, & Goldberg, 2020)

<u>กลุ่มสุดท้าย</u> งานศึกษาซึ่งกล่าวถึงช่วงเวลาในปัจจุบันโดยเฉพาะอย่างยิ่งการศึกษาเพื่อคาดการณ์แนวโน้มที่อาจจะเกิดขึ้นในยุคหลังการแพร่ระบาดของโรคโควิด 19 นักวิชาการจำนวนมากได้อธิบายในบริบทปัจจุบัน (2021) ว่า สถานการณ์การระบาดของโรคโควิด 19 ส่งผลอย่างมากต่อการลงทุนในการพัฒนาอุตสาหกรรมโครงสร้างพื้นฐานหนัก (hard infrastructure) เช่น ธุรกิจอสังหาริมทรัพย์และระบุว่าโควิด 19 เป็นหัวใจสำคัญของการเติบโตด้านดิจิทัลแพลตฟอร์ม โดยชี้ให้เห็นว่า สภาวการณ์ในปัจจุบันก่อให้เกิดการพังทลายลงของหลายธุรกิจที่จำเป็นต้องพึ่งพาการใช้บริการทางกายภาพของผู้บริโภค เช่น การท่องเที่ยว การโรงแรม โดยเสนอว่าสิ่งเหล่านี้จะกระตุ้นการเติบโตและเป็นโอกาสสำหรับผู้ประกอบการในการนำธุรกิจเข้าสู่ดิจิทัล (digitization) ในภาคธุรกิจมากขึ้น (Horgan et al., 2020) อย่างไรก็ตาม การปรับตัวของภาคธุรกิจที่กลายเป็นธุรกิจภาคดิจิทัลมากขึ้น ส่งผลให้ประเทศที่มีความต้องการที่จะพัฒนาเหล่านั้นมีความต้องการในการได้รับการสนับสนุนทางด้านเทคโนโลยี ซึ่งเป็นโอกาสของจีนในการสนับสนุนยุทธศาสตร์เส้นทางสายไหมดิจิทัลที่มาเป็นแพ็กเกจ (package) เดียวกัน

แม้จะมีการศึกษาเกี่ยวกับยุทธศาสตร์เส้นทางสายไหมดิจิทัลและมิติความมั่นคงทางไซเบอร์จำนวนมาก แต่สิ่งสำคัญคือ ต้องสังเกตว่าจำนวนสิ่งพิมพ์ในหัวข้อนี้ในไทยนั้นมีจำนวนน้อยอย่างมาก หรือไม่มีปรากฏอย่างชัดเจน หรือเปิดเผยต่อสาธารณะในช่วงทศวรรษที่ผ่านมา ในขณะที่สิ่งพิมพ์และงานศึกษาโดยนานาประเทศทั้งสถาบันตะวันตกและตะวันออกมีปรากฏและถูกให้ความสำคัญจนเกิดการศึกษาเป็นจำนวนมาก นอกจากนี้จีนมีความสัมพันธ์ทางเศรษฐกิจ การค้าและการลงทุน อย่างมากกับไทย ดังนั้นงานศึกษานี้จึงหวังที่จะเติมเต็มช่องว่างดังกล่าวในการให้ข้อมูลเชิงลึกใหม่เกี่ยวกับยุทธศาสตร์เส้นทางสายไหมดิจิทัลและความสัมพันธ์ในมิติความมั่นคงไซเบอร์ซึ่งเป็นประเด็นที่นานาประเทศให้ความสนใจในยุคสมัยใหม่ เพื่อให้ผู้เกี่ยวข้องและผู้กำหนดนโยบายเกิดความเข้าใจและตระหนักถึงความเสี่ยงด้านความมั่นคงที่อาจเกิดขึ้นและใช้เป็นแนวทางในการกำหนดนโยบายของไทยในอนาคต

**กรอบการวิเคราะห์**

งานวิจัยชิ้นนี้ อาศัยแนวคิดในกรอบ “ผู้ประกอบการทางปทัสถาน” (norm entrepreneurs) เพื่อพิจารณาตัวแสดงที่เกี่ยวข้องกับยุทธศาสตร์เส้นทางสายไหมดิจิทัลในฐานะผู้ประกอบการที่มีอำนาจการกำหนดนโยบายและกิจกรรมโดยปทัสถานของตน เพื่อทำความเข้าใจเหตุจูงใจว่า ทำไม ตัวแสดงที่เกี่ยวข้องเหล่านั้นถึงมีกระบวนการตัดสินใจและพฤติกรรมในการดำเนินกิจกรรมเช่นปรากฏ

John Muller อธิบายว่า ผู้ประกอบการเชิงปทัสถานโดยทั่วไป คือ บุคคลหรือองค์กรที่มุ่งมั่นที่จะเปลี่ยนแปลงพฤติกรรมของตัวแสดงอื่น ๆ (Florini, 1996) การนิยามเบื้องต้นเช่นนี้ของ Muller อาจเรียกได้ว่าเป็นการนิยามที่ค่อนข้างกว้าง เนื่องจาก ผู้ประกอบการเชิงปทัสถานสามารถเป็นได้ทั้งตัวแสดงระดับปัจเจกและตัวแสดงที่เป็นกลุ่มก้อน ทั้งนี้ นักวิชาการผู้ได้รับการอ้างอิงอย่างมากในการศึกษาปทัสถาน ผลงานของ Martha Finnemoreและ Kathryn Sikkink (1998) ได้อธิบายว่า ในการทำความเข้าใจกระบวนการ สร้างและแพร่กระจายของปทัสถาน สามารถศึกษาได้จากพฤติกรรมของตัวกระทำการที่สำคัญในระดับต่าง ๆ โดยเฉพาะอย่างยิ่งมีการให้การพิจารณาบทบาทของตัวกระทำการ (agent) ซึ่งถูกเรียกว่าผู้ประกอบการเชิงปทัสถานซึ่งเป็นตัวแสดงสำคัญในการสร้าง การเปลี่ยนแปลงและการแพร่กระจายของปทัสถาน

งานศึกษาจำนวนมากพบว่าผู้ประกอบการเชิงปทัสถาน คือ ส่วนสำคัญซึ่งเป็นตัวแสดงที่จะโน้มน้าว (persuade) มวลชนที่สำคัญให้สนับสนุนปทัสถานใหม่ เพื่อสร้างหรือเปลี่ยนแปลงปทัสถานที่มีอยู่ทำให้เกิดการเปลี่ยนแปลงพฤติกรรมที่ผู้ประกอบการปทัสถานพึงประสงค์ให้รัฐหรือสังคมปฏิบัติ อย่างไรก็ตาม ในความเป็นจริงนั้นหน้าที่ของผู้ประกอบการเชิงปทัสถานเป็นสิ่งที่ทำให้เกิดผลสำเร็จยาก เนื่องจาก การแพร่กระจายปทัสถานใหม่ที่ตนสนับสนุนนั้นหมายถึงการแข่งขันกับบริบท

ทางสังคม ในทางหนึ่งผู้ประกอบการเชิงปทัสถานต้องท้าทายกับปทัสถานที่ดำรงอยู่แล้วในสังคมซึ่งอาจนำไปสู่การปะทะของความขัดแย้งด้านผลประโยชน์ภายในบริบทเฉพาะทางสังคม

ทั้งนี้ เมื่อปทัสถานใหม่ถูกสร้างขึ้นมาระยะเวลาหนึ่งจนได้รับการสนับสนุนและการยอมรับจำนวนมากจากสังคม กระบวนการแพร่กระจายของปทัสถานจะเกิดการหลากอย่างรวดเร็วขึ้น (norm cascade) กล่าวคือ จะเกิดกลไกการขัดเกลาทางสังคม (socialization) ขึ้นในสังคม โดยที่ตัวแสดงอื่น ๆ จะดำเนินการโน้มน้าวเชิงปทัสถานที่ตนสนับสนุนให้ผู้อื่นยอมรับ เพื่อสร้างความเป็นปกติขึ้นแก่ปทัสถานนั้น ส่งผลให้ ปทัสถานใหม่จะไม่ถูกตั้งคำถาม หรือถูกท้าทายลดลงโดยตัวแสดงอื่น ๆ ในสังคม อาจกล่าวอีกนัยหนึ่งว่า การโน้มน้าวทางปทัสถานของตัวกระทำการที่สำคัญเหล่านั้นสร้างแรงกดดันเชิงจิตวิทยาให้เกิดสภาพการคล้อยตามทางปทัสถานทางใดทางหนึ่ง (norm conformity)

นอกจากนี้ ผู้ประกอบการเชิงปทัสถานยังบทบาทสำคัญอย่างมากในกระบวนการนำเอาปทัสถานที่รัฐหรือตัวแสดงของรัฐยอมรับเพื่อนำมาปฏิบัติภายในประเทศ (norm internalization process) (Acharya, 2004) ผู้ประกอบการเชิงปทัสถานภายในประเทศจะรับเอาปทัสถานภายนอกประเทศมาปรับใช้ให้เข้ากับบริบทภายในประเทศด้วยเครื่องมือที่แตกต่างกันเพื่อวัตถุประสงค์ให้เกิดการยอมรับปทัสถานที่ตนสนับสนุน ในเชิงรูปธรรมนั้นรัฐบาลอาจประกาศเป็นกฎหมายเพื่อให้ตัวแสดงในสังคมเกิดการยอมรับ อย่างไรก็ดี การรับและแพร่กระจายปทัสถานโดยผู้ประกอบการเชิงปทัสถานเหล่านั้นเป็นเรื่องของอัตวิสัย (subjective) ซึ่งส่งผลต่อกระบวนการรับปทัสถานของตัวแสดงเหล่านั้นซึ่งอาจแปล ตีความ เปลี่ยนแปลงและปรับเนื้อหาของปทัสถานให้สอดคล้องกับบริบทของตนและเพื่อให้ง่ายต่อการแพร่กระจายปทัสถาน (Keck & Sikkink, 1998)

ในงานวิจัยชิ้นนี้ ผู้วิจัยได้กำหนดขอบเขตในกรอบการศึกษาผู้ประกอบการเชิงปทัสถาน โดยวางกรอบการพิจารณายุทธศาสตร์หนึ่งแถบหนึ่งเส้นทางและยุทธศาสตร์เส้นทางสายไหมดิจิทัลในฐานะที่เป็นนโยบายที่ประเทศจีนต้องการส่งออก ผ่านตัวแสดงที่สนับสนุนแนวนโยบายดังกล่าวของจีน ซึ่งเป็นตัวแสดงที่เกี่ยวข้องทั้งภาครัฐและเอกชนภายในประเทศไทย ในฐานะที่เป็นผู้ประกอบการเชิงปทัสถานซึ่งมีบทบาทในการประชาสัมพันธ์ โน้มน้าวนโยบายดังกล่าวของจีนเข้าสู่ประเทศไทย ซึ่งผู้เขียนเชื่อว่ายุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน ส่งผลและทำให้เกิดการเปลี่ยนแปลงต่อมุมมองด้านความมั่นคงไซเบอร์ของตัวแสดงที่เกี่ยวข้องทั้งภาครัฐและเอกชนในประเทศไทย โดยขอบเขตการศึกษาภายใต้กรอบผู้ประกอบการเชิงปทัสถานดังกล่าว ผู้วิจัยใคร่พิจารณาว่า ตัวแสดงที่เกี่ยวข้องในยุทธศาสตร์เส้นทางสายไหมดิจิทัลทั้งภาครัฐและเอกชนเข้าใจว่าหน้าที่ หรือสิ่งที่พึงกระทำในฐานะผู้เกี่ยวข้องคืออะไร มีมุมมองที่ตระหนักถึงความมั่นคงไซเบอร์ต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัลหรือไม่และหากตัวแสดงเหล่านั้นมีความตระหนักในเรื่องความมั่นคงไซเบอร์ มุมมองเหล่านั้นมี

ความตระหนักร่วมกันหรือต่างกันอย่างไรและเหตุใดแม้มีความตระหนักถึงประเด็นความมั่นคงไซเบอร์แต่ยังคงดำเนินกิจกรรมในความเสี่ยงนั้นอยู่ อะไรเป็นเหตุที่ทำให้ไม่สามารถต้านทานได้

**วิธีการดำเนินการวิจัยและการออกแบบการวิจัย**

งานวิจัยชิ้นนี้เป็นการศึกษาเชิงคุณภาพ โดยผู้วิจัยแบ่งการศึกษาออกเป็น 2 กระบวนการ

<u>กระบวนการที่หนึ่ง</u> เพื่ออธิบายและหาคำตอบว่า ยุทธศาสตร์เส้นทางสายไหมดิจิทัล ภายใต้ยุทธศาสตร์เส้นทางสายไหมแห่งศตวรรษที่ 21 ซึ่งเป็นยุทธศาสตร์หลัก มีหลักการ แนวความคิดและการให้การจำกัดความ ภายใต้วัตถุประสงค์อย่างไรและยุทธศาสตร์นี้จะส่งผลกระทบต่อประเทศผู้เกี่ยวข้องอย่างไร โดยเอกสารสำคัญในการศึกษาจะเน้นเป็นเอกสารที่มาจากหลายแหล่ง เบื้องต้นได้แก่เอกสารจากทางการของรัฐบาลจีน เอกสารจากสถาบันเอกชนทั้งของจีนและประเทศอื่น เอกสารจากสถาบันวิจัยและนักวิชาการ โดยเฉพาะเอกสารที่ถูกตีพิมพ์เป็นภาษาอังกฤษ หรือได้รับการแปลเป็นหลัก

การศึกษาเอกสารตั้งต้นที่เกี่ยวกับยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทางจะเป็นเอกสารโดยรัฐบาลจีนทั้งหมด เพราะ ยุทธศาสตร์นี้ของจีนในช่วงประกาศมีความไม่แน่นอนและขาดเนื้อหาที่เป็นรูปธรรม ส่งผลให้งานศึกษาต่าง ๆ ที่ไม่ได้มาจากเอกสารทางการ จะส่งผลต่อความน่าเชื่อถือของการอ้างอิง ดังนั้นเอกสารอื่นที่ไม่ได้มาจากรัฐบาลจีนที่ใช้ในการอ้างอิง จะเน้นศึกษาตั้งแต่ปี ค.ศ. 2015 เป็นต้นไป

เอกสารที่จะมุ่งศึกษาเป็นภาษาอังกฤษ หรือเอกสารแปลภาษาอังกฤษ เพราะ ผู้ศึกษาไม่มีทักษะภาษาจีน เพื่อเป็นการตรวจสอบความน่าเชื่อถือของเอกสารแปล ผู้วิจัยจะใช้เอกสารตั้งต้นที่ถูกตีพิมพ์เป็นภาษาอังกฤษโดยไม่ผ่านการแปลเป็นการตรวจสอบความน่าเชื่อถือ นอกจากนี้เอกสารไทยที่มีการศึกษาที่เป็นงานวิจัย สามารถแบ่งออกเป็นสองกลุ่มอย่างเห็นได้ชัด คือ เอกสารที่ศึกษาวิจัยโดยภาครัฐจะมีเนื้อหาให้ การสนับสนุนยุทธศาสตร์ ในขณะที่เอกสารที่ศึกษาวิจัยโดยภาคเอกชน จะมีเนื้อหาส่วนใหญ่เป็นการตั้งคำถามและท้าทายยุทธศาสตร์ ซึ่งเมื่อใช้ข้อมูลอื่นประกอบ สามารถใช้กระบวนการ triangulate ในการตรวจสอบข้อมูลได้ดี

<u>กระบวนการที่สอง</u> เพื่อศึกษากิจกรรมและความเข้าใจต่อตัวยุทธศาสตร์และโครงการต่าง ๆ ภายใต้ยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน ในประเทศไทย ผู้วิจัยจะแบ่งช่วงการศึกษาออกเป็น 2 ช่วงระยะเวลา

ช่วงการสืบค้นเอกสาร ผู้วิจัยจะศึกษานโยบายภายในประเทศที่สอดคล้องกับยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทางและยุทธศาสตร์เส้นทางสายไหมดิจิทัลเป็นการเจาะจง เอกสารสาธารณะจาก

หน่วยงานของภาครัฐและเอกชนของไทย สื่อมัลติมีเดีย ข่าว ที่มีการนำเสนอกิจกรรมที่มีลักษณะสอดคล้องกับการดำเนินกิจกรรมภายใต้ยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน ตลอดจนแถลงการณ์และบทสัมภาษณ์จากผู้เกี่ยวข้องจากการดำเนินกิจกรรม เพื่อใช้ในการพิจารณาเบื้องต้นเกี่ยวกับความเข้าใจของตัวแสดงที่เกี่ยวข้องในประเทศไทยต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัล

ช่วงการเก็บข้อมูลจากผู้เข้าร่วมการวิจัย ซึ่งผู้วิจัยจะลงพื้นที่ศึกษา โดยใช้วิธีการสัมภาษณ์ตัวแสดงที่เกี่ยวข้องกับการศึกษา โดยมีเกณฑ์การคัดเลือกผู้มีส่วนร่วมในการวิจัยและเกณฑ์พิจารณาให้ผู้มีส่วนร่วมในการวิจัยออกจากโครงการ ดังนี้ ผู้เข้าร่วมในการวิจัยมีจะต้องเป็นผู้มีความรู้ความชำนาญที่เกี่ยวข้องกับหัวข้อในการศึกษา โดยเฉพาะอย่างยิ่งประเด็นเกี่ยวกับ ความมั่นคงไซเบอร์ ความมั่นคงสมัยใหม่ นโยบายต่างประเทศของไทย ยุทธศาสตร์เส้นทางสายไหมสายดิจิทัลและยุทธศาสตร์การต่างประเทศของจีน อย่างน้อยหนึ่งประเด็น ซึ่งผู้มีส่วนร่วมในการวิจัยสามารถออกจากโครงการได้ตลอดการศึกษา เมื่อผู้เข้าร่วมรู้สึกว่าการศึกษาจะเป็นภัย หรืออันตรายต่อผู้เข้าร่วม โดยไม่จำเป็นต้องแจ้งเหตุผลแก่ผู้วิจัย แต่ต้องแจ้งให้ผู้วิจัยทราบถึงความประสงค์ในการออกจากการมีส่วนร่วมในการวิจัย เพื่อผู้วิจัยจะดำเนินการคุ้มครองผู้เข้าร่วม ด้วยการทำลายข้อมูลที่เก็บจากผู้เข้าร่วมทั้งสิ้น ได้แก่ ไฟล์บันทึกเสียงสัมภาษณ์ ตลอดจนบันทึกมือและข้อมูลในระบบที่เกี่ยวข้องทั้งหมด

ผู้วิจัยได้แจกแจงหน่วยงานต่าง ๆ เพื่อให้สอดคล้องกับการศึกษา 3 ประเภท ได้แก่ หน่วยงานที่มีบทบาทหน้าที่ในด้านนโยบาย หน่วยงานที่มีบทบาทหน้าที่ในการปฏิบัติตามแนวนโยบายและหน่วยงานรัฐที่เชื่อมโยงกับภาคประชาชน โดยมีรายละเอียดดังนี้

ประเภทที่หนึ่ง หน่วยงานที่มีบทบาทหน้าที่ในด้านนโยบาย ได้แก่ 1) สำนักงานสภาความมั่นคงแห่งชาติ มีหน้าที่จัดทำนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติเสนอต่อคณะรัฐมนตรีเพื่อพิจารณา รวมถึงเสนอแนะและให้ความเห็นในการกำหนดยุทธศาสตร์ชาติในมิติความมั่นคง หรือประเด็นเกี่ยวกับความมั่นคงแห่งชาติ พิจารณากำหนดยุทธศาสตร์หรือแผนที่เกี่ยวข้องกับความมั่นคงแห่งชาติ นอกจากนี้ยังมีหน้าที่ประเมิน วิเคราะห์สถานการณ์ กำกับและติดตามภาพรวมในเชิงยุทธศาสตร์อันเป็นภัยต่อความมั่นคงแห่งชาติ 2) สำนักข่าวกรองแห่งชาติ มีหน้าที่ครอบคลุมที่เกี่ยวข้องกับกิจการข่าวกรอง การต่อต้านข่าวกรองทั้งภายในและต่างประเทศ ข่าวกรองทางการสื่อสาร เทคนิคและเครือข่าย รวมถึงการรักษาความปลอดภัยฝ่ายพลเรือน

ประเภทที่สอง หน่วยงานที่มีบทบาทหน้าที่ในการปฏิบัติตามแนวนโยบาย ได้แก่ 1) กองทัพไทย มีหน้าที่หลักสำคัญในการรักษาความมั่นคงของชาติในทางกายภาพ 2) กองบัญชาการตำรวจสืบสวนสอบสวน อาชญากรรมทางเทคโนโลยี มีหน้าที่ให้คำแนะนำ เสนอแนะการปฏิบัติงานให้กับหน่วยงานในสังกัด เพื่อดำเนินการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี สนับสนุนการพัฒนาบุคลากรด้านการสืบสวนสอบสวนของสำนักงานตำรวจแห่งชาติให้มีความรู้ในการสืบสวน

สอบสวนคดีอาชญากรรมทางเทคโนโลยี รวมทั้งประสานความร่วมมือกับหน่วยงานของรัฐ หรือองค์กรอื่นที่เกี่ยวข้องกับงานป้องกัน ปราบปรามและงานสืบสวนอาชญากรรมทางเทคโนโลยีทั้งในและนอกประเทศ

ประเภทที่สาม หน่วยงานรัฐที่เชื่อมโยงกับภาคประชาชน ได้แก่ 1) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีหน้าที่ในการจัดการและพัฒนาทางด้านเทคโนโลยีสารสนเทศ โดยเฉพาะธุรกิจการค้าและการลงทุนในแพลตฟอร์มออนไลน์ 2) กระทรวงพาณิชย์ มีหน้าที่ในการจัดการดูแลสินค้าและผู้บริโภค มีภารกิจในการเจรจาการค้าระหว่างประเทศ จัดระเบียบและบริหารงานนำเข้าส่งออกต่าง ๆ ส่งเสริมการพัฒนาธุรกิจสินค้าและบริการ

ทั้งนี้ผู้วิจัยจะใช้วิธีการติดต่อและวิธีการเข้าถึงผู้มีส่วนร่วมในการวิจัย ในกรณีเจ้าหน้าที่ระดับสูง หรือผู้ชำนาญการที่สังกัดหน่วยงาน ผู้วิจัยจะติดต่อและประสานการออกหนังสือ บันทึกผ่านคณะรัฐศาสตร์ ภาคความสัมพันธ์ระหว่างประเทศ จุฬาลงกรณ์มหาวิทยาลัย อย่างไรก็ดีผู้มีส่วนร่วมสามารถแสดงความจำนงในการติดต่อส่วนตัวได้โดยไม่ต้องติดต่อผ่านหน่วยงานหากผู้มีส่วนร่วมยินยอม ทั้งนี้ผู้วิจัยอาจใช้วิธีการสุ่มตัวอย่างแบบอ้างอิง (snowball sampling) ในการติดต่อผู้มีส่วนร่วมรายอื่นต่อไป

โดยผู้วิจัยได้ให้ความสำคัญกับการพิทักษ์สิทธิ ป้องกันความเสี่ยง รักษาความลับของผู้มีส่วนร่วมในการวิจัยและความยินยอมในการให้การสัมภาษณ์อย่างที่สุด ในการสัมภาษณ์ผู้เข้าร่วมวิจัยจำเป็นต้องให้การยินยอมในการเก็บและบันทึกข้อมูลทุกครั้งทั้งอย่างเป็นลายลักษณ์อักษร หรือในกรณีผู้เข้าร่วม ไม่สามารถลงลายลักษณ์อักษรได้นั้น ให้กระทำการยินยอมด้วยวาจา ซึ่งผู้วิจัยจะขอความยินยอมสองครั้ง คือ ก่อนการสัมภาษณ์และหลังจากการสัมภาษณ์สิ้นสุด ซึ่งจะสอบถามครอบคลุมไปถึงประเด็นความเป็นส่วนตัวในความจำนงที่จะปิดบังข้อมูลส่วนตัว ซึ่งผู้วิจัยจะใช้นามสมมติในการศึกษาต่อไป ทั้งนี้ผู้มีส่วนร่วมมีสิทธิในการถอนตัวออกจากกระบวนการสัมภาษณ์ตลอดการเก็บข้อมูลโดยไม่ต้องแจ้งเหตุผลให้ผู้วิจัยทราบ ผู้วิจัยสามารถขอหยุด หรือตัดทอนบางส่วนของการบันทึกข้อมูลที่ไม่อาจเปิดเผย ตลอดจนสิ้นสุดการเก็บข้อมูลผู้มีส่วนร่วมมีสิทธิในการแสดงความประสงค์ที่จะออกจากการมีส่วนร่วมในการวิจัย หากผู้วิจัยรู้สึกว่าการศึกษาอาจเป็นภัย หรืออันตรายต่อผู้เข้าร่วมโดยไม่ต้องแจ้งเหตุผล แต่ต้องแจ้งให้ผู้วิจัยทราบถึงความจำนงในการถอนตัว เพื่อผู้วิจัยจะดำเนินการทำลายเอกสาร ตลอดจนไฟล์บันทึกทั้งหมดที่เกี่ยวข้องกับผู้วิจัยต่อไป

อย่างไรก็ตาม เนื่องจากสถานการณ์การแพร่ระบาดของโรคโควิด 19 ที่ยังคงแพร่ระบาดอยู่ในขณะนี้ ผู้วิจัยคาดการว่า การสัมภาษณ์จะเกิดขึ้นผ่านทางโทรศัพท์ หรือระบบออนไลน์เป็นหลัก เว้นแต่ในกรณีที่ผู้ให้สัมภาษณ์มีความประสงค์จะให้สัมภาษณ์ในลักษณะอื่น ซึ่งผู้วิจัยตระหนักและคำนึงถึงหลักการเว้นระยะห่างทางกายภาพเป็นสำคัญตลอดการดำเนินการศึกษา โดยใช้การสัมภาษณ์

ในลักษณะกึ่งโครงสร้าง กล่าวคือ ผู้วิจัยจะจัดเตรียมชุดคำถามในลักษณะปลายเปิดไว้ล่วงหน้า เพื่อให้บทสนทนานำมาซึ่งความเข้าใจประเด็นอื่น ที่เกี่ยวข้อง เนื่องจากวัตถุประสงค์ของการศึกษาให้ความสนใจต่อทรรศนะและความเข้าใจของผู้เข้าร่วมเป็นสำคัญ นอกจากนี้การสัมภาษณ์บุคคลหนึ่งนั้น อาจเกิดขึ้นมากกว่าหนึ่งครั้ง ในกรณีซึ่งผู้วิจัยเห็นว่าข้อมูลที่ได้รับจากการสัมภาษณ์นั้นยังไม่เพียงพอ หรือมีความจำเป็นต้องการขยายความเพิ่มเติมในประเด็นใด ๆ ภายหลัง

# บทที่ 2

# ยุทธศาสตร์การพัฒนาเทคโนโลยีและดิจิทัลของจีน

## ความนำ

การกล่าวถึงจีนในช่วงทศวรรษที่ผ่านมาปฏิเสธไม่ได้ว่าจีนเป็นตัวแสดงที่โดดเด่นและมีความสำคัญในฐานะมหานาจในเวทีระหว่างประเทศอย่างมากโดยเฉพาะเมื่อ บทบาทและยุทธศาสตร์ของจีนคือ “ข้อริเริ่มแถบและทาง หรือ Belt and Road Initiative (BRI)” ได้ขยายขอบเขตเข้าสู่ดิจิทัลอย่างเด่นชัดจากการเปิดตัวกรอบยุทธศาสตร์ในชื่อ “Digital Silk Road (DSR) หรือเส้นทางสายไหมดิจิทัล” ในปี 2015 ซึ่งเป็นส่วนหนึ่งของ BRI เกิดจุดเปลี่ยนที่เห็นได้ชัดทางนโยบายและกิจกรรมในต่างประเทศของจีนซึ่งได้เปลี่ยนจากโครงสร้างพื้นฐานด้านการขนส่งและเครือข่ายการค้าไปสู่การเร่งขยายตัวทางด้านเทคโนโลยีของจีนทั่วโลก ตั้งแต่เครือข่ายโทรคมนาคมและเมืองอัจฉริยะไปจนถึง E-commerceและความพยายามในการวางระบบดาวเทียมใหม่ของจีน โดยมีเป้าหมายสำคัญเพื่อให้จีนสามารถพึ่งพาตนเองได้ในด้านวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม

นอกจากนี้ เพื่อที่จะเสริมสร้างกลยุทธ์ทางยุทธศาสตร์ในการพัฒนาเศรษฐกิจภายในประเทศภายใต้ยุทธศาสตร์ “Made in China 2025” วัตถุประสงค์สำคัญประการหนึ่งเพื่อตั้งเป้าหมายให้จีนเป็นผู้นำระดับโลกในด้านเทคโนโลยีขั้นสูง โดยรัฐบาลจีนได้เผยแพร่แนวนโยบายเรื่อง “Internet Plus” ขึ้นในปี 2015และได้เปิดตัวกรอบ “China Standards 2035” ในปี 2020 ซึ่งเป็นแผนการพัฒนาในระยะ 15 ปี ที่มุ่งหวังที่จะกำหนดมาตรฐานระดับโลกในด้านเทคโนโลยีรุ่นต่อไป ซึ่งรวมถึงเทคโนโลยี 5G ปัญญาประดิษฐ์ (AI) และ Internet of Things (IoT) ดังนั้นยุทธศาสตร์ DSR จึงเป็นยุทธศาสตร์ที่รวมการผลักดันจากภายในประเทศเพื่อส่งออกเทคโนโลยีของจีนที่พัฒนาจากนโยบายทางด้านอุตสาหกรรมในทศวรรษที่ผ่านมา โดยมีวาระและเนื้อหาที่กว้างขึ้นเพื่อยกระดับขีดความสามารถในการทำงานร่วมกันระหว่างเครือข่ายเทคโนโลยีของจีนกับต่างประเทศภายใต้แนวทางยุทธศาสตร์ของจีน

อย่างไรก็ตาม ประเด็นเรื่องเส้นทางสายไหมดิจิทัลเริ่มดึงดูดความสนใจจากนานาชาติมากขึ้นในช่วง 5 ปีที่ผ่านมา โดยเฉพาะประเด็นของบริษัท Huawei ซึ่งเป็นผู้ให้บริการเครือข่ายโทรคมนาคม 5G ที่น่าเชื่อถือบริษัทหนึ่ง ได้ถูกตั้งคำถามจากรัฐบาลสหรัฐฯ จนเป็นที่ถูกจับตามองในเวทีนานาชาติเนื่องจากความกังวลด้านความปลอดภัยและมั่นคงทางดิจิทัล (security and digital concern) ประเด็นถกเถียงดังกล่าวมีความเกี่ยวโยงกับประเด็นอภิปรายที่เกิดขึ้นในยุโรปเรื่อง แนวทางที่รัฐบาลจีนใช้ควบคุมและกำกับดูแลอินเทอร์เน็ตภายในของจีน ซึ่งสหภาพโทรคมนาคมระหว่างประเทศ (the

International Telecommunications Union: ITU) ได้ชี้ให้เห็นถึงกิจกรรมที่แฝงไปด้วยความทะเยอทะยานของรัฐบาลจีนในช่วงที่ผ่านมา

พฤติกรรมของจีนในระยะที่ผ่านมาโดยเฉพาะในเรื่องดิจิทัลนั้นถูกจับตามองมากยิ่งขึ้น ด้านหนึ่งเนื่องจากความกังวลด้านความยั่งยืนในยุโรปเกี่ยวกับกรอบอธิปไตยด้านดิจิทัล ประเด็นเรื่องการขับเคลื่อนของข้อมูลข่าวสารภายในสังคม ประเด็นความเป็นส่วนตัวของแต่ละบุคคลและประเด็นของการไหลของข้อมูลอย่างเป็นอิสระ (free flows of data) โดยเฉพาะอย่างยิ่งสถานการณ์การแพร่ระบาดของ COVID-19 ทำให้ความกังวลดังกล่าวถูกยกระดับความสำคัญมากขึ้น เนื่องจากก่อให้เกิดการผลักดันสังคมให้เข้าสู่สังคมดิจิทัลในทันที โดยเฉพาะอย่างยิ่ง รัฐบาลทั่วโลกที่กำลังใช้เครื่องมือดิจิทัลซึ่งรวมถึงการติดตามและเฝ้าระวังผู้ติดเชื้อทางดิจิทัล เพื่อตรวจสอบและป้องกันการแพร่กระจายของไวรัสดังกล่าว

**จากข้อริเริ่มแถบและทางสู่การบูรณาการทางเทคโนโลยี**

นับตั้งแต่การประกาศแนวยุทธศาสตร์ข้อริเริ่มแถบและทาง ขึ้นในปี 2013 อย่างเป็นทางการ รัฐบาลจีนได้รวบรวมเป้าหมายของตนเพื่อที่จะนิยามและกำหนดซึ่งใช้ทัศนะของตนเป็นตัวกำหนดกรอบโลกาภิวัตน์และกรอบพหุภาคีขึ้นอีกครั้งเพื่อให้สอดคล้องกับผลประโยชน์ของจีน ในขณะที่โลกกำลังเข้าสู่ช่วงการยกระดับทางเทคโนโลยีและความเชื่อมโยงทางดิจิทัลซึ่งเห็นได้ชัดเจนในช่วงทศวรรษที่ผ่านมา การรวมองค์ประกอบทางด้านดิจิทัลเข้ามาเป็นส่วนประกอบของ BRI อย่างเป็นทางการนั้นเป็นการเน้นย้ำถึงความสำคัญของบทบาทและแนวยุทธศาสตร์ที่จีนกำลังวางตำแหน่งแห่งหนของตนในเวทีระหว่างประเทศยุคปัจจุบัน ความร่วมมือของ BRI กับประเทศอื่น ๆ ประธานาธิบดี จีน สี จิ้นผิง ได้เรียกร้องให้มีการแสวงการพัฒนาที่ขับเคลื่อนด้วยนวัตกรรมและความร่วมมือที่มากขึ้นในพื้นที่ชายแดน เช่น เศรษฐกิจแบบดิจิทัล (the digital economy) ปัญญาประดิษฐ์ (AI) นาโนเทคโนโลยี (nanotechnology) และเทคโนโลยีกลุ่มควอนตัมคอมพิวเตอร์ (quantum computing) การพัฒนา big data รวมไปถึงการจัดเก็บข้อมูลบนระบบคลาวด์ (cloud) และเมืองอัจฉริยะ (smart cities) ดังนั้นการนิยามยุทธศาสตร์เส้นทางสายไหมดิจิทัลอย่างกว้างจึงกล่าวได้ว่า เป็นการบูรณาการทางด้านเทคโนโลยีโดยนำดิจิทัลเทคโนโลยีที่ล้ำสมัยเข้ามาใช้งานและพัฒนารูปแบบธุรกิจเพื่อพัฒนายกระดับและปรับปรุงการเชื่อมต่อข้ามชาติ

รัฐบาลจีนได้กล่าวถึงยุทธศาสตร์ข้อริเริ่มแถบและทาง ผ่านสำนักข่าว Xinhua News Agency ซึ่งเป็นสื่อสำนักข่าวทางการของจีนถึงการนิยามและกำหนดให้การเชื่อมโยงของข้อริเริ่มแถบและทางเป็น “ห้าความเชื่อมโยงและสามประชาคม” ซึ่งประกอบไปด้วย ความเชื่อมโยง 5 ประการ ได้แก่ ความเชื่อมโยงในโครงสร้างพื้นฐาน (infrastructure) ความเชื่อมโยงด้านการค้า (trade) ความ

เชื่อมโยงด้านการเงิน (finance) ความเชื่อมโยงของผู้คน หรือ “หัวใจของผู้คน” (people’s hearts) และความเชื่อมโยงด้านนโยบาย (policy) และประชาคมทั้ง 3 ได้แก่ ประชาคมที่มีผลประโยชน์ร่วมกัน (the community of interest) ประชาคมที่มีชะตากรรมร่วมกัน (the community of destiny) และประชาคมที่มีความรับผิดชอบร่วมกัน (the community of responsibility)

อนึ่ง ยุทธศาสตร์เส้นทางสายไหมดิจิทัล มีจุดประสงค์หลัก 3 ประการ ได้แก่ ประการที่หนึ่ง เพื่อพัฒนาการเชื่อมโยงในระดับภูมิภาคและระดับนานาชาติในห้าด้าน ได้แก่ ด้านโครงสร้างพื้นฐาน ด้านการค้า ด้านการเงิน ด้านผู้คนและด้านนโยบาย ห้าประเด็นดังกล่าวข้างต้นได้รับการอ้างอิงจาก สถาบัน the Digital Belt and Road Center ของมหาวิทยาลัยฟูตัน (Fudan University) (Dekker, Okano-Heijmans, & Zhang, 2020) ซึ่งเป็นหนึ่งในสถาบันหลักของจีนที่ศึกษาในหัวข้อดังกล่าว ประการที่สอง เพื่อส่งเสริมและยกระดับนวัตกรรมของอุตสาหกรรมแบบดั้งเดิมและการจ้างงานในประเทศที่เกี่ยวข้องกับยุทธศาสตร์ข้อริเริ่มแถบและทาง เพื่อเป็นการขยายและเปิดตลาดจีนที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล ควบคู่ไปกับการกระตุ้นการพัฒนา BRI ในประเทศที่เกี่ยวข้อง รัฐบาลจีนเชื่อว่าผลลัพธ์ส่วนใหญ่ที่ประเทศผู้เกี่ยวข้องในยุทธศาสตร์จะได้รับนั้นมาจากการกระตุ้นนวัตกรรม การยกระดับอุตสาหกรรมและการจ้างงาน ซึ่งจะก่อให้เกิดการพึ่งพาทางเศรษฐกิจแบบดิจิทัลของจีนมากขึ้น ประการที่สาม อ้างอิงจากผู้เชี่ยวชาญจีนจำนวนหนึ่งได้กล่าวในลักษณะเดียวกันว่า DSR มีวัตถุประสงค์เพื่อยกระดับประสิทธิภาพของอุตสาหกรรมในระดับภูมิภาคและเพื่อสร้างพื้นฐานของประชาคมในภูมิภาคที่มีประโยชน์ทางเศรษฐกิจร่วมกัน นำไปสู่การสร้างห่วงโซ่มูลค่าโลก (the global value chain) ที่มีจีนเป็นผู้นำแทนที่ชาติตะวันตก ประเด็นดังกล่าวนี้ชี้ให้เห็นถึงการบูรณาการที่สำคัญระหว่างเครือข่ายทางเทคโนโลยีของจีนกับประเทศในภูมิภาคใกล้เคียงโดยเฉพาะอย่างยิ่งในเอเชียตะวันออกเฉียงใต้และประเทศอื่น ๆ ในปัจจุบัน



นอกจากนี้ รัฐบาลจีนได้วางแผนยุทธศาสตร์ในการทำให้ทันสมัย (modernize) และปฏิรูปในส่วนโครงสร้างพื้นฐานภายในประเทศโดยปรากฏชัดอยู่ในแผนยุทธศาสตร์ “Made in China 2025 (MiC2025)” ที่ประกาศในปี 2015 ยุทธศาสตร์ดังกล่าวมีประเด็นสำคัญอยู่ที่นโยบายด้านอุตสาหกรรม วัตถุประสงค์เพื่อเปลี่ยนเศรษฐกิจของจีนจากโมเดลที่เน้นการผลิตในระดับล่างที่ใช้แรงงานจำนวนมาก ให้กลายเป็นเศรษฐกิจที่ขับเคลื่อนด้วยเทคโนโลยีและนวัตกรรม ด้วยเหตุนี้จีนจึงพยายามจัดวางตำแหน่งของบริษัทสัญชาติจีนเพื่อให้อยู่ในแนวหน้าของนวัตกรรมโลก โดยการเปลี่ยนจุดความสนใจของโลกมาที่ประเทศจีน รัฐบาลจีนพยายามที่จะก้าวเข้ามารับบทผู้นำทางเทคโนโลยีของโลก ดังนั้นยุทธศาสตร์ MiC2025 จึงกลายเป็นกุญแจสำคัญที่ส่งผลให้เกิดการเปลี่ยนแปลงบทบาทความสัมพันธ์ระหว่างประเทศโดยเฉพาะอย่างยิ่ง ความสัมพันธ์ระหว่างจีนและสหรัฐฯ จากความร่วมมือทั่วไปกลายเป็นประเด็นความขัดแย้ง

ในขณะเดียวกัน ยุทธศาสตร์เส้นทางสายไหมดิจิทัลเป็นการเพิ่มมิติให้กับข้อริเริ่มแถบและทางของจีนและชี้ให้เห็นถึงความทะเยอทะยานของจีนในการก้าวเข้ามาเป็นผู้นำการปฏิวัติอุตสาหกรรมครั้งที่ 4 อย่างเต็มรูปแบบ (Dekker, Okano-Heijmans, & Zhang, 2020) จากความสำเร็จของยุทธศาสตร์ด้านอุตสาหกรรมภายในประเทศของจีน จีนได้ส่งเสริมการดำเนินการและใช้เทคโนโลยีของจีนในประเทศที่เกี่ยวข้องกับข้อริเริ่มแถบและทาง ทั้งนี้ พฤติกรรมดังกล่าวของจีนสะท้อนให้เห็นถึงความพยายามในการสร้างมาตรฐานของตนเองในประเทศอื่น โดยเฉพาะอย่างยิ่งด้านโครงสร้างพื้นฐานอัจฉริยะ (smart infrastructure) ฮาร์ดแวร์และซอฟต์แวร์ 5G โดยมี Huawei บริษัทด้านดิจิทัลเทคโนโลยีขนาดใหญ่ของจีนเป็นศูนย์กลาง นอกจากนี้จีนกำลังผลักดันวาระของตนในเรื่องเมืองและอวกาศอัจฉริยะด้วยการแนะนำทางเลือกของตนเองควบคู่กับการพัฒนาระบบนำทางผ่านดาวเทียม หรือ GPSและให้การช่วยเหลือประเทศต่าง ๆ ในการปล่อยดาวเทียมของสัญชาติจีน รัฐบาลจีนกำลังก้าวสู่บทบาทสำคัญจากการเปิดตัวแผน “China Standards 2035” ในปี 2020 ซึ่งเป็นความพยายามในการผลักดันมาตรฐานด้านดิจิทัลที่มีลักษณะแบบจีนทั้งในและต่างประเทศ ส่งผลให้รัฐบาลจีนและบริษัทจีนมีกิจกรรมและลักษณะกิจกรรมในเชิงเสริมสร้างสถานะของตนในองค์การระหว่างประเทศมากขึ้นในปัจจุบัน อย่างไรก็ตามในประเด็นด้านธุรกิจนั้นรัฐบาลจีนมุ่งเน้นไปที่รากฐานของกลุ่มธุรกิจของเศรษฐกิจแบบดิจิทัลมากขึ้น กล่าวคือ ให้ความสำคัญกับการลงทุนในเรื่อง E-commerceและการซื้อขายธุรกรรมออนไลน์อย่างมาก เพื่อให้เกิดพฤติกรรมที่ใช้ในชีวิตประจำวัน อาทิ ส่งเสริมให้แพลตฟอร์มการซื้อขายออนไลน์ที่บริษัทเป็นเจ้าของกลายเป็นทางเลือกหลักของประชาชน การใช้จ่ายประจำวันของประชาชนในรูปแบบ “สังคมไร้เงินสด” (cashless society) โดยผู้ให้บริการที่เป็นบริษัทจีน เป็นต้น

อย่างไรก็ตาม บริษัทจีนและรัฐบาลจีนก้าวเข้ามามีบทบาทและอิทธิพลที่เพิ่มขึ้นอย่างมาก รวมถึงความเชื่อมโยงและการผสมผสานทางเทคโนโลยี ส่งผลให้เกิดความกังวลต่ออำนาจอธิปไตย โดยเฉพาะอย่างยิ่งความท้าทายทางเศรษฐกิจ จริยธรรมและความมั่นคง ในขณะเดียวกันกลุ่มประเทศที่เกี่ยวข้องหลายกลุ่มก็พยายามร่วมมือกับจีนในด้านดิจิทัลก่อให้เกิดความซับซ้อนมากขึ้น เพื่อตอบสนองความต้องการทางตลาด ปฏิเสธไม่ได้ว่าเทคโนโลยีของจีนมีบทบาทอย่างมากในตลาดเศรษฐกิจและกำลังพัฒนาสถานะที่แข็งแกร่งมากขึ้นและเป็นผู้บุกเบิกกลุ่มแรกๆ ในประเทศกำลังพัฒนาและประเทศเศรษฐกิจเกิดใหม่ โดยเฉพาะอย่างยิ่งในเอเชียใต้ เอเชียตะวันออกเฉียงใต้และแอฟริกา ปัจจุบันจีนได้ผลักดันวิสัยทัศน์ด้านการบริหารจัดการไซเบอร์อย่างแข็งขันยิ่งขึ้น ทั้งในประเทศพันธมิตร BRIและในสถาบันระหว่างประเทศ กว่าทศวรรษที่ผ่านมานโยบายและแนวยุทธศาสตร์ต่าง ๆ ของจีน รวมถึงแนวทางในอนาคตของจีน อาทิ แผน “Made in China 2025” แผน “Internet Plus” แผน “Digital Silk Road” และแผน “China Standards 2035” ต่าง

สะท้อนให้เห็นว่ารัฐบาลจีนปรารถนาที่จะยกระดับตัวเองจากสถานะผู้ทำตามกฎ (rule-taker) เป็นผู้กำหนดกฎเกณฑ์ (rule-maker) ในการกำหนดมาตรฐานทางด้านเทคโนโลยีในยุคสมัยหน้า

ท่ามกลางการแข่งขันทางเทคโนโลยีระหว่างจีนและสหรัฐฯ กลุ่มประเทศที่เกี่ยวข้องในเอเชียตะวันออกเฉียงใต้ โดยเฉพาะไทยเองต้องมีความเข้มแข็งมากขึ้นในการปกป้องผลประโยชน์ทางเศรษฐกิจและยุทธศาสตร์ของตนเองและให้ความสำคัญกับประเด็นด้านความมั่นคงของประเทศที่อาจเกิดขึ้น โดยเฉพาะอย่างยิ่งประเด็นความมั่นคงไซเบอร์ซึ่งเป็นประเด็นสำคัญที่มักถูกท้าทายและตั้งคำถามในนานาประเทศเมื่อกล่าวถึงการพัฒนาและความเกี่ยวโยงทางด้านเทคโนโลยีกับจีน

**ประเด็นสำคัญของเส้นทางสายไหมดิจิทัลของจีน**

ประการที่หนึ่ง โครงสร้างพื้นฐานภายใต้กรอบยุทธศาสตร์เส้นทางสายไหมดิจิทัล หรืออีกนัยหนึ่งว่าเป็นโครงสร้างพื้นฐานอัจฉริยะ อาทิ เครือข่ายโทรคมนาคม โครงสร้างพื้นฐานด้านปัญญาประดิษฐ์ ระบบนำทาง เป็นต้น โครงสร้างพื้นฐานดังกล่าวดำเนินการโดยบริษัทเทคโนโลยีขนาดใหญ่ของจีน เช่น Huaweiและ ZTE เป็นต้น ปัจจุบันบริษัทจีนเป็นผู้นำในการสร้างโครงสร้างพื้นฐานดิจิทัลทั่วโลกซึ่งรวมถึงเครือข่ายโทรคมนาคมด้วยเทคโนโลยี 5G การเดินสายเคเบิลใต้น้ำ เมืองอัจฉริยะ ระบบดาวเทียมและระบบจัดการข้อมูลบนคลาวด์ (cloud) ในแง่ของส่วนแบ่งตลาดอุปกรณ์โทรคมนาคม 5G ทั่วโลก ข้อมูลเมื่อปี 2021 (Triolo, 2020) เปิดเผยว่าบริษัท Huawei เป็นผู้นำโลกในเทคโนโลยีด้านดังกล่าวอยู่ที่ร้อยละ 23.18 ของส่วนแบ่งตลาดอุปกรณ์โทรคมนาคม 5G ขณะที่บริษัท ZTE อยู่ในอันดับที่ 6 ด้วยร้อยละ 5.37 ของส่วนแบ่งตลาดดังกล่าว เมื่อเทียบกับ Ericsson และ Nokia ของยุโรปอยู่ที่ร้อยละ 18.83-14.61 ของส่วนแบ่งตลาดอุปกรณ์โทรคมนาคม 5G ตามลำดับ บริษัทจีนยังคงเป็นผู้นำในจำนวนสิทธิบัตร 5G โดยที่ Huawei มีสิทธิบัตรประกาศกว่า 3,325 รายการ เมื่อเทียบกับ 2,038 รายการสำหรับ Nokiaและ 1,423 รายการสำหรับ Ericsson นอกจากนี้จากข้อมูลที่เปิดเผยเมื่อปี 2019 (*Microwave Journal*, 2019) ในเอเชียตะวันออกเฉียงใต้ บริษัทจีนยังครองตลาดสมาร์ตโฟนด้วยร้อยละ 60 ของส่วนแบ่งตลาดสมาร์ตโฟนในประเทศอาเซียน 5 ประเทศ ได้แก่ อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ สิงคโปร์และไทย

นอกจากนี้ ประเด็นเมืองอัจฉริยะก็เป็นอีกหนึ่งส่วนสำคัญของกรอบยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีนเช่นเดียวกัน อาจกล่าวได้ว่ากรอบแนวคิดดังกล่าวเป็นการนิยามรูปแบบใหม่ของวิถีทางของการทำให้เป็นเมืองด้วยการนำเทคโนโลยีดิจิทัลมาบูรณาการ เช่น ปัญญาประดิษฐ์ เครือข่ายโทรคมนาคม 5Gและ Internet of Things (IoT) ซึ่งช่วยอำนวยความสะดวกในการพัฒนาอุตสาหกรรมและสนับสนุน กระตุ้นให้เกิดการปฏิวัติทางดิจิทัล บริษัทจีนเป็นผู้นำในการพัฒนาเมืองอัจฉริยะในหลายส่วนของโลก รวมถึงในเอเชียกลางและรัสเซีย แอฟริกา ตะวันออกกลาง สหภาพ

ยุโรป โดยเฉพาะอย่างยิ่งในเอเชียตะวันออกเฉียงใต้ รัฐบาลจีนและบริษัทเอกชนดำเนินการประสานกัน ขณะที่รัฐบาลระดับชาติและระดับท้องถิ่นช่วยเหลือบริษัทต่าง ๆ ให้อยู่รอดและขยายขอบเขตโครงข่ายทั่วโลกในรูปแบบต่าง ๆ ทั้งด้วยเงินอุดหนุนภาษี เงินกู้พิเศษ เงินช่วยเหลือและราคาซื้อขายที่เอื้ออำนวยต่อการดำเนินกิจกรรม

อย่างไรก็ดีในช่วงครึ่งทศวรรษที่ผ่านมาจีนแสดงออกอย่างชัดเจนถึงความทะเยอทะทานมากขึ้นด้วยการพัฒนาด้านอวกาศที่มีความโดดเด่นมากขึ้นหลังจากที่วาระการประชุมประเด็นเรื่องยุทธศาสตร์เส้นทางสายไหมดิจิทัล ถูกประกาศอย่างเป็นทางการ รัฐบาลจีนได้สร้างทางเลือกใหม่ให้กับระบบกำหนดตำแหน่งบนโลกของสหรัฐฯ (Global Positioning System: GPS) ระบบดาวเทียมนำทางทั่วโลกของรัสเซีย (Global Navigation Satellite System: GLONASS) และระบบกาลิเลโอของสหภาพยุโรป ซึ่งระบบดังกล่าวข้างต้นเป็นระบบนำทางผ่านดาวเทียมที่ถูกใช้อยู่อย่างเป็นทางการในปัจจุบัน รัฐบาลจีนเสนอทางเลือกใหม่ด้วยระบบดาวเทียมนำทาง BeiDou ซึ่งถูกกำหนดให้เป็นระบบอิสระเต็มรูปแบบในบริการด้านภาพ การสื่อสารและการระบุตำแหน่งทางภูมิศาสตร์ ซึ่งรัฐบาลจีนได้เสนอบริการดังกล่าวเหล่านั้นของ BeiDou แก่ประเทศอื่นเช่นเดียวกัน

นอกจากนี้ รัฐบาลจีนยังสนับสนุนในการริเริ่มด้านอวกาศระหว่างประเทศ เช่น PakSat Multi-Mission Satellite ซึ่งเป็นการพัฒนาและเปิดตัวร่วมกันของโครงการดาวเทียมโดยจีนและปากีสถานและระบบ AfghanSat 2 ที่กำลังเริ่มดำเนินการขึ้นในอัฟกานิสถานในปี 2019 (Ministry of Communications & IT, India, 2019) ซึ่งบริษัทจีนได้ให้ความช่วยเหลือทางเทคนิคและการเงินที่สำคัญ ขณะเดียวกันในระดับพหุภาคียังมีองค์การความร่วมมือด้านอวกาศแห่งเอเชีย-แปซิฟิก (Asia–Pacific Space Cooperation Organization: APSCO) ซึ่งนำโดยจีนนั้นส่งผลให้จีนสามารถถ่ายทอดความรู้ด้านเทคนิคและอุปกรณ์ไปยังตลาดเป้าหมายได้



แม้ว่ายุทธศาสตร์เส้นทางสายไหมดิจิทัลจะเป็นความคิดริเริ่มที่นำโดยรัฐเป็นส่วนใหญ่ แต่ปฏิเสธไม่ได้ว่า ตัวแสดงซึ่งเป็นกุญแจสำคัญของการพัฒนาดังกล่าวของจีน คือ บริษัทด้านเทคโนโลยีของจีน ที่ได้รับการส่งเสริมจากภายในทั้งการวิจัยและนวัตกรรม รวมถึงเงินลงทุนจำนวนมหาศาล การผลักด้านทางการเมืองที่ส่งเสริมและกระตุ้นให้บริษัทจีนเหล่านั้นเกิดแรงจูงใจในการพัฒนา จนนำไปสู่ความสามารถในการส่งออกและปรับใช้เทคโนโลยีดิจิทัล ขณะเดียวกันตลาดภายในของจีนก็ได้รับประโยชน์มากมายจากการพัฒนาด้านดิจิทัลและ E-commerce ในประเทศที่ยุทธศาสตร์เส้นทางสายไหมดิจิทัลเข้าไปมีบทบาทและวางโครงสร้างเพื่อยึดโยงบริษัทจีนเข้ากับโครงสร้างพื้นฐานดิจิทัลของประเทศอื่น ๆ ที่เข้าไปลงทุน ซึ่งสามารถกล่าวได้อีกนัยหนึ่งว่าโครงสร้างพื้นฐานดิจิทัลนี้เป็นฐานที่ธุรกิจอิเล็กทรอนิกส์จำเป็นต้องดำเนินการจนสำเร็จในระยะยาว สะท้อนให้เห็นถึงความ

ทะเยอทะยานและความพยายามในการวางตำแหน่งแห่งที่ของจีนในฐานะผู้กำหนดมาตรฐานในระดับโลก ผ่านความยึดโยงที่เหนียวแน่นและซับซ้อนของบริษัทจีนเหล่านั้น

ประการที่สอง รัฐบาลจีนได้ให้ความสำคัญกับความเชื่อมโยงในมิติทางการค้า การเงินและผู้คน ผ่านนโยบาย Internet Plus ในปี 2015 ซึ่งเชื่อมโยงกับยุทธศาสตร์ Made in China 2025 โดยนโยบายดังกล่าวกำหนดขึ้นเพื่อบูรณาการอินเทอร์เน็ตเข้ากับอุตสาหกรรมแบบดั้งเดิม ผลลัพธ์ที่ชัดเจนที่สุด คือ การเกิดขึ้นของตลาด E-commerceและการธนาคารทางอินเทอร์เน็ตซึ่งกลายมาเป็นเครื่องมือสำคัญสำหรับการเติบโตทางเศรษฐกิจของจีน แนวนโยบายของยุทธศาสตร์เส้นทางสายไหมดิจิทัล ได้เปิดตลาดใหม่สำหรับบริษัทเหล่านี้ โดยหนึ่งในจุดแข็งที่สุดของบริษัท E-commerce ของจีน คือ การเสนอทางเลือกที่มีราคาและต้นทุนค่าใช้จ่ายในการดำเนินการถูกกว่าสำหรับสินค้าและบริการ ซึ่งถูกกว่าเมื่อเทียบกับตลาดเดียวกันในยุโรปและสหรัฐฯ บริษัทผู้นำ E-commerce รายใหญ่ของจีน ได้แก่ Baidu, Alibabaและ Tencent หรือที่มักถูกเรียกรวมกันว่า “BAT” เป็นหนึ่งในเสาหลักสำคัญทางเศรษฐกิจของประเทศจีนโดยเฉพาะอย่างยิ่งในต่างประเทศ

อย่างไรก็ดี เมื่อกล่าวถึงธุรกิจ E-commerce ย่อมเลี่ยงไม่ได้ที่จะต้องทำความเข้าใจเบื้องต้นว่าธุรกิจดังกล่าวนั้นขับเคลื่อนและมีการทำงานหน้าร้านส่วนใหญ่อยู่บนการให้บริการแพลตฟอร์มดิจิทัล ดังนั้นการแข่งขันส่วนแบ่งทางตลาดในกลุ่มผู้ให้บริการแพลตฟอร์มต่าง ๆ จึงมุ่งเน้นไปที่ความสะดวกสบายและความหลากหลายของลักษณะการทำงาน โดยแบ่งเป็นประเภทต่าง ๆ ดังนี้ แพลตฟอร์มให้บริการด้านการเงิน (Pay, PayPal, etc.) แพลตฟอร์มให้บริการด้านสังคมและการติดต่อสื่อสาร (Skype, twitter, facebook, TikTok, etc.) แพลตฟอร์มให้บริการด้านคลังและการจัดหมวดหมู่ (YouTube, GitHub, Spotify, etc.) แพลตฟอร์มให้บริการด้านการค้นหาข้อมูล (Google, Bing, Baidu, etc.) และแพลตฟอร์มให้บริการทางการตลาด (UBER, amazon, ebay, AliExpress, etc.) ซึ่งสหรัฐฯ ในปัจจุบันครอบครองส่วนแบ่งการตลาดที่โดดเด่นในหลายภูมิภาค โดยเฉพาะอย่างยิ่งตลาดยุโรป อย่างไรก็ตาม ผู้เชี่ยวชาญได้คาดการว่าบริษัท E-commerceและอินเทอร์เน็ตของจีนนั้นกำลังเติบโตขึ้นอย่างรวดเร็วและมีแนวโน้มว่าบริษัทเหล่านี้ของจีนจะครองตลาดในประเทศกำลังพัฒนาในช่วงทศวรรษหน้านี้ เนื่องจากได้รับการผลักดันอย่างต่อเนื่องในการพัฒนาจากรัฐบาลจีนซึ่งจีนได้ให้ความสำคัญกับการพัฒนาด้านเทคโนโลยีโดยถือเป็นวาระสำคัญอย่างมากประการหนึ่ง ทั้งยังสอดรับกับแนวยุทธศาสตร์ที่จีนวางไว้ในอนาคตเรื่องการผลักดันทางเทคโนโลยีที่นำโดยรัฐบาลจีน

นอกจากนี้กระแสและค่านิยมทางสังคมในที่ยอมการใช้งานปัญญาประดิษฐ์ภายในจีน มีความแตกแตกต่างจากโลกตะวันตก โดยเฉพาะอย่างยิ่งในโลกเสรีประชาธิปไตย กล่าวคือ ความละเอียดอ่อนและความอ่อนไหวในการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้งานในชีวิตประจำวันในโลกเสรี ส่งผลต่อความรู้สึกไม่ปลอดภัยและการละเมิดความเป็นส่วนตัว (privacy) โดยเฉพาะอย่างยิ่ง

กรณีของแพลตฟอร์มออนไลน์ที่มีการบันทึกข้อมูลและตรวจจับการทำงานของผู้ใช้งาน เพื่อบันทึกเป็นข้อมูลในลักษณะอัลกอริทึมซึ่งเป็นส่วนหนึ่งของการทำงานของปัญญาประดิษฐ์ นำไปสู่คลังประมวลผลแบบ Big Data จึงกล่าวได้ว่า ปรากฏการณ์ดังกล่าวส่งผลให้กลุ่มโลกตะวันตก โดยเฉพาะอย่างยิ่งกลุ่มผู้นำโลกเสรีมีความเชื่อมั่นต่อการใช้งานปัญญาประดิษฐ์ในระดับต่ำ เมื่อเทียบกับจีนที่มีความเชื่อมั่นในการใช้งานปัญญาประดิษฐ์ในชีวิตประจำวัน ซึ่งเป็นหนึ่งในจุดแข็งของการพัฒนาทางเทคโนโลยีของจีนในปัจจุบัน

จากประเด็นข้างต้นเมื่อพิจารณาประกอบกับการส่งออกโครงสร้างพื้นฐานทางดิจิทัล บริษัทแพลตฟอร์มของจีนยังสามารถช่วยเหลือประเทศกำลังพัฒนาให้ก้าวกระโดดไปสู่การพัฒนาในขั้นต่อไป เช่น การเชื่อมโยงเข้ากับเศรษฐกิจอิเล็กทรอนิกส์ทั่วโลก ดังนั้นอาจกล่าวได้ว่ายุทธศาสตร์เส้นทางสายไหมดิจิทัล เป็นกลไกสำคัญในการส่งเสริมการค้า E-commerce ในส่วนต่าง ๆ ของโลก ปัจจุบันที่การใช้จ่ายเงินจริงและการไหลของข้อมูลเป็นเรื่องยาก

แม้ว่าแพลตฟอร์มดิจิทัลของจีนจำนวนมากจะเพิ่งเกิดใหม่และยังตามหลังส่วนแบ่งการตลาดกับบริษัทตะวันตกอยู่บ้าง โดยเฉพาะอย่างยิ่งในประเทศกลุ่มเป้าหมายที่เป็นประเทศเศรษฐกิจเกิดใหม่และประเทศกำลังพัฒนา ผู้เชี่ยวชาญชี้ว่าในอนาคตอันใกล้ หรือทศวรรษข้างหน้าบริษัทจะที่ให้บริการด้านแพลตฟอร์มดิจิทัลจะครองส่วนแบ่งการตลาดที่มากกว่า หรือเทียบเท่าบริษัทสัญชาติตะวันตกอย่างสหรัฐฯ และยุโรปโดยเฉพาะอย่างยิ่งในประเทศกลุ่มเป้าหมายหลักอย่างประเทศเศรษฐกิจเกิดใหม่และประเทศกำลังพัฒนา เนื่องจากการมีอยู่ของบริษัทจีนที่ควบคู่ไปกับโครงการเส้นทางสายไหมดิจิทัลจะสร้างภาพลักษณ์ของบริษัทจีนเหล่านั้นให้ถูกใจผู้คนได้มากขึ้น ส่งผลให้เมื่อบริษัทจีนกลายเป็นผู้นำตลาดในประเทศเหล่านั้น บริษัทจีนดังกล่าวจะกลายเป็นผู้กำหนดมาตรฐานทางตลาดซึ่งจะได้รับประโยชน์จากการผูกขาดและ/หรือ ข้อได้เปรียบในการเข้าถึงและผูกมัดลูกค้าส่วนใหญ่ไว้ อนึ่ง ลักษณะเช่นว่านี้คล้ายคลึงกันกับวิธีที่บริษัทตะวันตก โดยเฉพาะสหรัฐฯ ทำกำไรมาตลอดหลายทศวรรษ นอกจากนี้บริษัทจีนดังกล่าวที่ได้ความช่วยเหลือจากรัฐบาลจีน (ผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัลและอื่น ๆ) จะมีอิทธิพลและอยู่ในตำแหน่งที่จะสามารถอำนวยและผลักดันให้มีการนำมาตรฐานทางเทคนิคของจีนไปใช้ในหน่วยงานกำหนดมาตรฐานอื่น ๆ

บริษัท E-commerce จึงมีบทบาทสำคัญในฐานะเป็นเครื่องมือในการเชื่อมโยงและชนะใจประชาชน เนื่องจากผู้บริโภคและผู้ใช้บริการหลัก คือ ประชาชนโดยทั่วไป ที่จะเข้าถึงการใช้บริการแพลตฟอร์มในลักษณะต่าง ๆ ในชีวิตประจำวัน อาทิ ซื้อขายและทำธุรกรรมออนไลน์ หรือพื้นที่แลกเปลี่ยนชุมชนออนไลน์ต่าง ๆ เป็นต้น ด้วยเหตุนี้ E-commerce จึงเป็นเครื่องมือที่มีลักษณะเป็นอำนาจอ่อน หรือ soft power ทางการทูตสาธารณะ ในกรณีดังกล่าวบริษัทจีนซึ่งได้รับการสนับสนุนจากรัฐบาลจีนผ่านทางการเมืองและการเงินนั้น จึงมีเป้าหมายสำคัญในการเข้าถึงประเทศโลกใต้

(Global South) เพื่อตอบสนองความต้องการและเสนอทางเลือกหลักให้กับประเทศเศรษฐกิจเกิดใหม่และประเทศกำลังพัฒนาที่ยังไม่บรรลุการเชื่อมต่อทางดิจิทัล รวมถึงโครงการด้านการศึกษา โครงการด้านสุขภาพและสาธารณสุขและโครงการที่เกี่ยวข้องกับโครงสร้างพื้นฐานดิจิทัลเพื่อเชื่อมต่อพื้นที่ดังกล่าวกับโลก

นอกจากนี้การเงินก็เป็นอีกส่วนสำคัญของการเชื่อมต่อในยุทธศาสตร์เส้นทางสายไหมดิจิทัลเช่นเดียวกัน นอกจากจะสามารถอำนวยความสะดวกในโครงการทางการค้าและโครงสร้างพื้นฐานแล้ว ยังรวมถึงการปรับปรุงให้ดีขึ้นของโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ (IT) และการสร้างระบบรวมการชำระเงินที่รองรับการทำธุรกรรมของประชากรส่วนใหญ่ ช่วยเพิ่มโอกาสทางธุรกิจในภาคการลงทุนอื่น ๆ ในส่วนของบริษัททางการเงินนั้น การสร้างความร่วมมือกับบริษัทท้องถิ่น คือกุญแจสำคัญในการขยายบทบาทและสร้างอิทธิพลในภูมิภาคและในโลก เช่น บริษัททางการเงิน AntFinancial ในเครืออาลีบาบาได้ขยายกิจกรรมทางธุรกิจส่วนใหญ่ในเอเชียตะวันออกเฉียงใต้ด้วยการสร้างความร่วมมือกับบริษัทพันธมิตรในท้องถิ่น เช่น PayTM ในอินเดียและ Touch’n Go ในมาเลเซีย เป็นต้น

ในมิติทางด้านนโยบาย จีนมุ่งเน้นที่การเปลี่ยนแปลงจากอุตสาหกรรมหนักไปสู่การลงทุนโครงสร้างพื้นฐานดิจิทัล ควบคู่ไปกับการส่งออกอุปกรณ์เทคโนโลยีโดยบริษัทจีน เพื่อให้เกิดการพึ่งพาตนเองในด้านวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม เพื่อวางตำแหน่งและบทบาทของตัวเองในเวทีโลกด้วยการกำหนดมาตรฐานสากล กล่าวคือ รัฐบาลจีนมีความพยายามที่จะเปลี่ยนตัวเองจากผู้ทำตามกฎมาเป็นผู้กำหนดกฎเกณฑ์ หรือมาตรฐาน เพื่อชี้นำแนวทางของเทคโนโลยีใหม่ๆ ว่า เทคโนโลยีใหม่ๆ เหล่านั้นควรนำไปใช้ในเชิงพาณิชย์ได้อย่างไรในโลกอนาคต

ข้อมูลดิจิทัล คือ ตัวแปรสำคัญของความสำเร็จของบริษัท กล่าวคือ บริษัทที่สามารถเข้าถึงข้อมูลและมีทักษะการวิเคราะห์ข้อมูลที่มีประสิทธิภาพ ทั้งจากคลังความคิด (think tank) หรือ small-big data จะกลายเป็นตัวแปรสำคัญสู่ความสำเร็จเหนือบริษัทอื่น ๆ ในตลาดเดียวกัน โจทย์ที่ตามมา คือ บริษัทเหล่านั้นจะเก็บรวบรวมข้อมูล จัดการ จัดเก็บและถ่ายโอนข้อมูลทั้งในส่วนของบุคคลและข้อมูลอุตสาหกรรมได้อย่างไร ส่งผลให้สิ่งที่เรียกว่า “พื้นที่ทางไซเบอร์ (cyberspace)” มีความโดดเด่นและเป็นสิ่งที่ควรได้รับความสนใจยิ่งขึ้น เนื่องจากจะนำไปสู่พรมแดนทาง “กายภาพ” ที่ไม่ชัดเจนระหว่างรัฐในแง่ของธุรกิจและการค้า ดังนั้น บรรทัดฐาน กฎเกณฑ์และมาตรฐานที่ตกลงโดยทั่วไปจึงเป็นสิ่งจำเป็นเพื่อให้แน่ใจว่าพื้นที่ไซเบอร์มีความเปิดกว้างและที่สำคัญ คือ ปลอดภัยมั่นคงในการเชื่อมต่อดิจิทัลข้ามพรมแดน

อย่างไรก็ตาม ความพยายามที่จะกำหนดมาตรฐานและบรรทัดฐานระดับโลกเป็นส่วนหนึ่งขององค์ประกอบทางด้านนโยบายของยุทธศาสตร์เส้นทางสายไหมดิจิทัลของจีน ดังนั้น จีนจึงเป็น

คู่แข่งที่มีความทะเยอทะยานและท้าทายสหรัฐฯ มากขึ้น โดยเฉพาะอย่างยิ่งในการสร้างมาตรฐานทางเทคโนโลยีและอุตสาหกรรมระดับสากล เนื่องจากความสามารถในการกำหนดมาตรฐานเหล่านั้นนำมาซึ่งผลประโยชน์เชิงพาณิชย์ เชิงบรรทัดฐานและรวมไปถึงอำนาจเชิงเปรียบเทียบ โดยเฉพาะอย่างยิ่งในปัจจุบันที่พรมแดนของรัฐมีความซับซ้อนและไม่ชัดเจนมากยิ่งขึ้นในโลกไซเบอร์

กระนั้นผู้เขียนได้แจกแจงยุทธศาสตร์ แนวนโยบายและการเคลื่อนไหวของรัฐบาลจีนที่มีความชัดเจน 3 ประการ ที่บ่งชี้ถึงจุดยืนและความตั้งใจของจีนในเวทีโลก ดังนี้ ประการที่หนึ่ง การผลักดันความสามารถในการกำหนดมาตรฐานตามหลักการของ “China Standards 2035” ประการที่สอง แนวนโยบายและกฎระเบียบทางไซเบอร์ภายในประเทศของจีนซึ่งส่งผลกระทบต่อการทำงานของบริษัทจีนและบริษัทต่างชาติในจีนและการกำหนดจุดยืนของจีนในการถกเถียงในระดับนานาชาติในประเด็นเรื่องข้อมูลและการกำกับดูแลในโลกไซเบอร์ ประการที่สาม การเคลื่อนไหวและท่าทีของจีนที่ปรากฏอย่างชัดเจนในสถาบันและเครือข่ายระหว่างประเทศสะท้อนถึงความทะเยอทะยานของจีนที่เพิ่มขึ้น

**การกำหนดมาตรฐานตามหลักการของ China Standards 2035**

เส้นทางสายไหมดิจิทัลของจีนในฐานะเป็นยุทธศาสตร์และนโยบายระดับนานาชาติ ผนวกกับบทบาทของบริษัทจีนที่ดำเนินการอยู่ทั่วโลกนั้นส่งเสริมให้จีนมีโอกาสและความสามารถที่จะเข้ามาเป็นผู้กำหนดมาตรฐานทางด้านเทคโนโลยีเกิดใหม่ อย่างไรก็ตามสิ่งที่เป็นกุญแจสำคัญประการหนึ่งคือ ขีดความสามารถของบริษัทและนวัตกรรมที่เริ่มต้นจาก “ภายใน” ประเทศจีน ดังนั้น สิ่งที่เกิดตามมาต่อยุทธศาสตร์ “Made in China 2025” คือ ยุทธศาสตร์ “China Standards 2035” ที่ประกาศในปี 2020 เพื่อเป็นในแผนการกำหนดมาตรฐานอุตสาหกรรมภายในประเทศโดยมีเป้าหมายเพื่อทำให้มาตรฐานดังกล่าวเป็นมาตรฐานระดับสากลในที่สุด

อย่างไรก็ดี การกล่าวถึงการพัฒนาโครงสร้างพื้นฐานดิจิทัลทั้งในลักษณะที่เป็นกายภาพจับต้องได้และลักษณะที่เป็น “อัจฉริยะ” หรือจับต้องไม่ได้ อาทิ เครือข่ายอินเทอร์เน็ต แพลตฟอร์มให้บริการต่าง ๆ เป็นต้น ประเทศที่เลือกให้บริษัทที่รับผิดชอบเป็นการเจาะจงในด้านดังกล่าวจะต้องเผชิญกับผลกระทบลักษณะที่ถูก “ผูกติด” ในระยะยาว เนื่องจากการเปลี่ยนไปใช้บริษัทอื่นเป็นเรื่องที่ทำได้ยาก เพราะโครงสร้างพื้นฐานดิจิทัลในลักษณะดังกล่าวมีค่าใช้จ่ายเพิ่มเติมที่เกี่ยวข้องสูงและสิ่งสำคัญคือความเข้ากันได้ทางเทคนิคซึ่งเทคโนโลยีบางอย่างไม่สามารถใช้งานร่วมกันได้ หากไม่ได้มาจากบริษัทเดียวกัน หรือมาจาก “ผู้ผลิต” เดียวกัน ยกตัวอย่าง ระบบปฏิบัติการของ Apple ที่มีลักษณะเป็น iOS ซึ่งไม่สามารถทำงานร่วมกันกับระบบ Android ของ Microsoft ได้ เป็นต้น ซึ่งหมายความว่าประเทศคู่ค้าในยุทธศาสตร์เส้นทางสายไหมดิจิทัล เมื่อเวลาผ่านไปประเทศเหล่านั้นจะ

กลายเป็นส่วนที่สร้างผลประโยชน์และสนับสนุนความสำเร็จของบริษัทจีน ทำนองเดียวกันบริษัทจีนดังกล่าวก็ผลักดันยุทธศาสตร์จีนให้ประสบความสำเร็จเช่นเดียวกัน ทั้งนี้เนื่องจากบริษัทจีนเหล่านั้นเป็นผู้ขับเคลื่อนรายแรก หรือเป็น “หัวหอก (spearhead)” ด้านเทคโนโลยีในประเทศคู่ค้า ดังนั้นบริษัทจีนโดยเฉพาะอย่างยิ่งในเอเชียตะวันออกเฉียงใต้และในแอฟริกาซึ่งจีนมีอิทธิพลในภูมิภาคทั้งสองอย่างมาก จะเป็นภูมิภาคที่สำคัญที่ทำให้ยุทธศาสตร์ “China Standards 2035” ของจีนประสบความสำเร็จ

**ผลกระทบของนโยบายและระเบียบการกำกับดูแลทางไซเบอร์ของจีนต่อบริษัทข้ามชาติภายในประเทศจีน**

รัฐบาลจีนตระหนักว่า ข้อมูลเป็นทรัพยากรที่สำคัญ ดังปรากฏชัดเจนในประกาศการพัฒนา “ยุทธศาสตร์สารสนเทศแห่งชาติ (the National Informatization Strategy) ปี 2016-2020” ในขณะเดียวกัน รัฐบาลจีนมีความกังวลเกี่ยวกับความเสี่ยง หรืออันตรายที่อาจเกิดขึ้นทางด้านความมั่นคงไซเบอร์ของจีนเนื่องจากการไหลเข้าออกของข้อมูลภายในจีนไปยังต่างประเทศ ข้อกังวลดังกล่าวนำมาซึ่ง “กฎหมายความมั่นคงไซเบอร์ของจีนในปี 2017 (the Cybersecurity Law of China)” ซึ่งกำหนดกฎระเบียบด้านการคุ้มครองความเป็นส่วนตัวโดยมีแม่แบบมาจากยุโรป ระเบียบว่าด้วยเรื่องมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation: GDPR) กฎหมายความมั่นคงไซเบอร์ของจีนมีความเหมือนระเบียบ GDPR ในเรื่องภาระหน้าที่ทางกฎหมายทั่วไปในการขอรับความยินยอมก่อนที่จะได้รับข้อมูล

อย่างไรก็ตามกฎหมายความมั่นคงไซเบอร์ของจีนมีความแตกต่างจากระเบียบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ในเรื่อง ความเข้มงวดในการบังคับใช้มาตรฐานการควบคุมเฉพาะพื้นที่ (localization rules) โดยทั่วไปแล้วแต่ละประเทศจะมักมาตรฐานและแนวทางในการกำกับดูแลทางข้อมูลเป็นของตัวเองเพื่อให้สอดคล้องกับกฎหมายภายในและสังคม เพื่อป้องกันอาชญากรรมทางไซเบอร์ ตลอดจนส่งเสริมโอกาสทางเศรษฐกิจ อย่างไรก็ตามสิ่งเหล่านี้มักนำมาซึ่งคำถามสำคัญว่า รัฐมีอำนาจทางกฎหมายเพียงใดในการเข้าถึงข้อมูล

การศึกษากฎหมายไซเบอร์จำนวนมากบ่งชี้ไปในทางเดียวกันว่า รัฐบาลจีนมีการบังคับใช้มาตรฐานการควบคุมในพื้นที่อย่างเข้มข้น อาจกล่าวอีกนัยหนึ่งว่า กฎหมายภายในประเทศของจีนให้อำนาจรัฐบาลจีนในการเข้าถึงข้อมูลส่วนบุคคลและข้อมูลที่สำคัญหากพิจารณาแล้วว่า ข้อมูลเหล่านั้นมีความเสี่ยงเป็นภัยคุกคามต่อความมั่นคง นอกจากนี้ยังมีความคลุมเครือเนื่องจากความมั่นคงสำหรับจีนนั้นมักถูกพิจารณาในลักษณะที่กว้างทั้งความมั่นคงของชาติ ประชาชน พรรคคอมมิวนิสต์และตัวผู้นำ (Dekker, Okano-Heijmans, & Zhang, 2020) เช่นเดียวกับการบังคับใช้ที่มีความแตกต่างกับ

มาตรฐาน GDPR ซึ่งจะถูกบังคับใช้โดยหน่วยงานคุ้มครองข้อมูล (the Data Protection Authorities: DPAs) ซึ่งเป็นหน่วยงานอิสระ แต่หน่วยงานที่บังคับใช้กฎหมายความมั่นคงไซเบอร์ของจีนนั้นเป็นหน่วยงานของรัฐ จึงทำให้เกิดคำถามว่า กฎหมายความมั่นคงไซเบอร์ของจีนจะคุ้มครองบุคคลจากรัฐได้ด้วยหรือไม่

กฎหมายความมั่นคงไซเบอร์ของจีนส่งผลกระทบต่อธุรกิจต่างชาติที่ประกอบธุรกิจในจีนหลายประการ (Mochinaga, 2021) ประการที่หนึ่ง คือ ข้อบังคับของการส่งผ่านข้อมูลข้ามพรมแดนของจีนนั้นเข้มงวดกว่าระเบียบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ซึ่งก่อให้เกิดความไม่สมดุลขึ้นต่อบริษัทจีนอย่างมาก กล่าวคือ ธุรกิจต่างชาติที่ดำเนินกิจการในจีนถูกบังคับให้แปลข้อมูลต่าง ๆ เป็นภาษาจีน โดยเฉพาะข้อมูลที่สำคัญ ในขณะที่บริษัทจีนที่ดำเนินงานในต่างประเทศสามารถถ่ายโอนข้อมูลประเภทเดียวกันข้ามพรมแดนได้โดยไม่มีข้อจำกัด ประการที่สอง คือ ข้อกำหนดทางกฎหมายที่ใช้ในกฎหมายความมั่นคงไซเบอร์ของจีนนั้นคลุมเครือ ส่งผลให้การตีความกฎหมายส่วนใหญ่ต้องบังคับใช้อย่างคลุมเครือซึ่งสร้างความกังวลและความไม่แน่นอนให้แก่ธุรกิจต่างชาติที่เข้ามาลงทุนในจีน ประการที่สาม จากปัญหาทั้งสองประการข้างต้นส่งผลเสียต่อเนื่องทั้งบริษัทจีนและต่างชาติ เนื่องจากข้อมูลเป็นทรัพยากรที่สำคัญอย่างมากสำหรับกิจกรรมทางเศรษฐกิจและเมื่อเกิดข้อจำกัดของการเคลื่อนย้าย หรือโอนถ่ายข้อมูลย่อมส่งผลกระทบเชิงลบต่อประสิทธิภาพ หรืออาจขัดขวางธุรกิจและการค้าอย่างเลี่ยงไม่ได้

นอกจากนี้ “กฎหมายข่าวกรองแห่งชาติของจีน (the National Intelligence Law of China)” (NPC Observer, 2017) ซึ่งประกาศใช้เมื่อปี 2017 ก่อให้เกิดคำถามและความกังวลเกี่ยวกับความน่าเชื่อถือของบริษัทโทรคมนาคมของจีนที่ดำเนินงานในต่างประเทศว่า รัฐบาลจีนอาจมีอำนาจในการควบคุมบริษัทโทรคมนาคมเหล่านี้มากเกินไป กล่าวคือ ในมาตรา 7 ของกฎหมายดังกล่าวระบุว่า “องค์กรและประชาชนมีหน้าที่ในการสนับสนุน ช่วยเหลือและร่วมมือกับหน่วยข่าวกรอง” และมาตรา 14 ใจความสำคัญระบุว่า อนุญาตให้หน่วยงานข่าวกรองมีอำนาจร้องขอความร่วมมือจากสถาบัน องค์กรและประชาชน โดยกฎหมายข่าวกรองแห่งชาติของจีนเตือนว่า หากบริษัทโทรคมนาคมของจีนปฏิเสธไม่ให้ความช่วยเหลือทางข้อมูลตามที่ร้องขอจะถือเป็นความผิดตามกฎหมาย



**การกำกับดูแลพื้นที่ไซเบอร์โลก (Global cyber governance) และการแพร่กระจายทางเทคโนโลยีของจีนในภูมิภาคเอเชียตะวันออกเฉียงใต้**

แพลตฟอร์มระหว่างประเทศที่เป็นกุญแจและมีบทบาทสำคัญในการกำหนดมาตรฐานทางเทคโนโลยี ดูแลและควบคุม คือ สหภาพโทรคมนาคมระหว่างประเทศ (International

Telecommunication Union: ITU) ซึ่งเป็นองค์การในระดับพหุภาคีภายใต้สหประชาชาติ องค์กรความร่วมมือด้านการจัดสรรชื่อและหมายเลขทางอินเทอร์เน็ต (Internet Corporation for Assigned Names and Numbers: ICAAN) ซึ่งเป็น NGO ที่ริเริ่มโดยสหรัฐฯ และ World Internet Conference (WIC หรือ Wuzhen Summit) ซึ่งริเริ่มโดยจีน

อนึ่ง ประเทศจีนเป็นสมาชิกเก่าแก่ในสหภาพโทรคมนาคมระหว่างประเทศมาอย่างยาวนาน ซึ่งก่อตั้งขึ้นเมื่อปี 1865 มีภาระหน้าที่เพื่อจัดการมาตรฐานโทรเลขและต่อมากลายเป็นการเชื่อมต่อโทรศัพท์และสัญญาณวิทยุ การเปลี่ยนแปลงครั้งสำคัญเมื่อปี 1947 ITU เข้ามาเป็นส่วนหนึ่งขององค์การสหประชาชาติในฐานะองค์กรเฉพาะทาง เพื่อสนับสนุนการพัฒนาและการกำหนดนโยบายระหว่างประเทศด้านการสื่อสารโทรคมนาคม โดยเฉพาะในปี 2015 เป็นปีที่รัฐบาลจีนมีบทบาทอย่างมากใน ITU เนื่องจากเลขาธิการ ITU ในครั้งนั้นเป็นชาวจีน รัฐบาลจีนแสดงจุดยืนในการสนับสนุนอธิปไตยในโลกไซเบอร์อย่างแข็งขัน แสดงจุดยืนว่าพื้นที่ทางไซเบอร์ (cyberspace) ถือเป็นการขยายอาณาเขตทางกายภาพของรัฐ อีกทั้งจีนได้ผลักดันมาตรฐานสากลใหม่ในเรื่องเทคโนโลยีการจดจำใบหน้าและการเฝ้าระวังเพื่อสร้างเทคโนโลยีที่สอดคล้องกันในระดับสากล รัฐบาลจีนมีข้อเสนอในการปรับเปลี่ยนการเชื่อมต่ออินเทอร์เน็ต โดยเชื่อว่าเพื่อให้มีขอบเขตที่กว้างขึ้นและมีทางเลือกมากขึ้นด้วยแนวคิด “New” Internet Protocol (IP) อย่างไรก็ดี การเสนอทางเลือกดังกล่าวให้กับระบบ Internet Protocol (IP) ที่ใช้อยู่ในปัจจุบัน อาจนำไปสู่การทำให้ระบบอินเทอร์เน็ตขาดเอกภาพ หรือเกิดการแยกตัวออกจากกันหากจีนสามารถออกแบบและนำระบบใหม่ดังกล่าวมาใช้ได้จริง

นอกเหนือจากสหภาพโทรคมนาคมระหว่างประเทศแล้ว สหรัฐฯ ได้ผลักดันให้จัดตั้งองค์กรความร่วมมือด้านการจัดสรรชื่อและหมายเลขทางอินเทอร์เน็ต (ICAAN) ขึ้นในปี 1998 ซึ่งเป็นองค์กรไม่แสวงหาผลกำไรโดยมีคณะกรรมการกำกับดูแลที่ประกอบไปด้วยผู้ให้บริการอินเทอร์เน็ตและคณะกรรมการที่ปรึกษาของรัฐบาลจำนวน 112 คนและดำเนินการภายใต้การกำกับดูแลของกระทรวงการค้าของสหรัฐฯ อย่างไรก็ตาม ICAAN มักถูกตั้งคำถามและถูกวิพากษ์วิจารณ์ถึงความเป็นศูนย์กลางโดยสหรัฐฯ ที่มากเกิน ซึ่งปรากฏชัดเจนในมาตรการการคว่ำบาตรจีนขององค์กรในช่วงปี 2001–2009 (Dekker, Okano-Heijmans, & Zhang, 2020) ส่งผลให้เกิดการเปลี่ยนผ่านในปี 2016 สู่แนวทางที่ผู้มีส่วนได้ส่วนเสียมีบทบาทภายในองค์กรมากขึ้นและปัจจุบันยังรวมถึงกลุ่มสิทธิมนุษยชนและบริษัทต่าง ๆ แม้ว่าบริษัทเหล่านั้นส่วนใหญ่จะเป็นบริษัทสัญชาติสหรัฐฯ ก็ตาม (Zhao, Shi, & Yao, 2021)

เมื่อกล่าวถึงองค์กรเอกชนในด้านสิทธิมนุษยชนดิจิทัล (digital human rights) รวมถึงการคุ้มครองผู้บริโภค ข้อมูลและเสรีภาพทางดิจิทัล ซึ่งกำลังมีบทบาทและถูกให้ความสำคัญมากขึ้นในปัจจุบัน เนื่องจากเทคโนโลยีได้เข้ามามีความเชื่อมโยงและเกี่ยวข้องกับชีวิตประจำวันมากขึ้น อย่างไร

ก็ตามสหภาพโทรคมนาคมระหว่างประเทศยังคงเป็นองค์การทางเทคนิคที่บริษัทโทรคมนาคมเข้าร่วมการประชุมในฐานะสมาชิกที่ไม่มีอำนาจในการออกเสียง (non-voting sector members) โดยมีหน้าที่ในการนำเสนอร่างรายงาน หรือมาตรฐานใหม่ ๆ ซึ่งมีรัฐบาลเพียงไม่กี่รัฐบาลที่จะมีศักยภาพเพียงพอในการผลักดันวาระของบริษัทตนเองให้เป็นที่สนใจต่อที่ประชุมได้ เนื่องจากวาระด้านเทคโนโลยีนั้นมีปัญหาในเชิงเปรียบเทียบในเรื่องความก้าวหน้า ศักยภาพและนวัตกรรม ซึ่งเห็นได้ชัดว่าสิ่งนี้เป็นประโยชน์ต่อจีน เนื่องจากบริษัทจีนมีความก้าวหน้าทางด้านเทคโนโลยีมากขึ้นและได้รับส่วนแบ่งการตลาดในกลุ่มที่สำคัญในปัจจุบัน

อย่างไรก็ตามรัฐบาลจีนได้ดำเนินการตามแนวทางของตนเองด้วยในเวลาเดียวกัน การประชุมอินเทอร์เน็ตโลก (WIC) ตั้งแต่ปี 2014 จัดทำโดยฝ่ายบริหารพื้นที่ไซเบอร์ของจีน (the Cyberspace Administration of China) เพื่อจัดแจงตำแหน่งผู้มีบทบาทและเกี่ยวข้องในการกำกับดูแลพื้นที่ไซเบอร์ทั่วโลก เป็นการประชุมเพื่อเฉลิมฉลองความก้าวหน้าทางเทคโนโลยี การค้าของจีนและเป็นการสำรวจบรรทัดฐานในการดำเนินการของรัฐต่าง ๆ ต่อโลกไซเบอร์ (Dekker & Okano-Heijmans, 2020) รัฐบาลจีนใช้ประโยชน์จากความสำคัญของตลาดจีนและห่วงโซ่การผลิต ซึ่งทำให้การประชุม Wuzhen ประสบความสำเร็จในการดึงดูดผู้นำทางธุรกิจ อาทิ บริษัท Appleและ Google รวมถึงตัวแทนของรัฐบาลที่เป็นพันธมิตรกับจีน เช่น รัสเซียและหลายประเทศในเอเชียกลาง รวมถึงตัวแทนจาก ITU อย่างไรก็ตาม รัฐบาลตะวันตกไม่เห็นด้วยกับข้อเสนอในการปิดกั้นข้อมูลของจีนและไม่ได้ส่งผู้แทนระดับสูงเข้าร่วมอีกเลยนับแต่การประชุมครั้งแรกปี 2014 ดังกล่าว เมื่อผู้จัดงานพยายามที่จะผลักดันแถลงการณ์เพื่อสนับสนุนความคิดริเริ่มและนโยบายที่จีนปกป้อง (Leswing, 2017)

เมื่อกล่าวถึงกลไก หรือเครื่องมือที่ทำหน้าที่เป็นผู้ผสานความเชื่อมโยงระหว่างหน่วยงานและระหว่างรัฐบาลในเอเชียตะวันออกเฉียงใต้ภายใต้กรอบยุทธศาสตร์เส้นทางสายไหมดิจิทัล ตัวแสดงที่สำคัญดังกล่าวไว้ในตอนต้น คือ บริษัทด้านเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทสำคัญในการอำนวยความสะดวกและการประสานงานด้านนโยบายเกี่ยวกับยุทธศาสตร์เส้นทางสายไหมดิจิทัลระหว่างจีนและประเทศหุ้นส่วนที่เอเชียตะวันออกเฉียงใต้ เพื่อพัฒนากลไกความร่วมมือพหุภาคีและทวิภาคีในภูมิภาคโดยการจัดเวทีการประชุม การเจรจาบันทึกความเข้าใจ (MoU) รวมถึงการให้ความสนับสนุนในการแบ่งปันข้อมูลในกรอบดิจิทัล อย่างไรก็ดี กระทรวงอุตสาหกรรมและเทคโนโลยีสารสนเทศของจีน (Ministry of Industry and Information Technology: MIIT) ได้ประกาศใช้แผนการก่อสร้างโครงสร้างพื้นฐานในประเทศเพื่อนบ้าน (the Infrastructure Construction Plan for Neighboring Countries) ในปี 2014 ซึ่งเป็นแผนเพื่อเสนอมาตรฐานของข้อมูลระหว่างจีนและเอเชียตะวันออกเฉียงใต้ ต่อมาในปี 2016 รัฐบาลจีนได้อนุมัติแผนการก่อสร้างศูนย์ความร่วมมือด้านข้อมูลข่าวสารจีน-อาเซียน (the Construction Plan of China-ASEAN Information Harbor) และพัฒนาเป็นแผน

แม่บทของศูนย์ความร่วมมือด้านข้อมูลข่าวสารจีน-อาเซียน (the Masterplan of China-ASEAN Information Harbor) ในปี 2019 โดยศูนย์ความร่วมมือด้านข้อมูลดังกล่าวมีวัตถุประสงค์เพื่อที่จะเป็นศูนย์กลางสำคัญเพื่อยกระดับเครือข่ายอินเทอร์เน็ตและการเชื่อมต่อระหว่างข้อมูลในเอเชียตะวันออกเฉียงใต้ เพื่อให้สอดคล้องกับหลักการเส้นทางสายไหมดิจิทัล

จีนได้ริเริ่มความร่วมมือแบบทวิภาคีในการประสานงานและความร่วมมือด้านภาษี การตรวจสอบและกักกันสินค้า ความมั่นคงของเครือข่าย ไปจนถึงการจัดเก็บและการส่งข้อมูล จีนและไทยได้จัดตั้งเวทีการเจรจาระดับรัฐมนตรีเพื่อความร่วมมือทางเศรษฐกิจดิจิทัล (Ministerial-level Dialogue for Digital Economic Cooperation) ในปี 2019 เพื่อหารือเกี่ยวกับเมืองอัจฉริยะ เทคโนโลยี 5G ความมั่นคงไซเบอร์และปัญญาประดิษฐ์ (Ministry of Foreign Affairs, the People's Republic of China, 2022) อย่างไรก็ตาม ในปัจจุบันการประสานงานด้านนโยบายส่วนใหญ่เกิดขึ้นในระดับทวิภาคีและระดับระหว่างรัฐ ในขณะที่การมีส่วนร่วมของภาคเอกชนยังคงมีความจำกัด กล่าวคือ บริษัทข้ามชาติหลายแห่งต้องเผชิญกับอุปสรรคในการดำเนินธุรกิจท่ามกลางระบบเศรษฐกิจแบบดิจิทัล ดังนั้น รัฐบาลที่มุ่งมั่นที่จะเชื่อมต่อกับยุทธศาสตร์เส้นทางสายไหมดิจิทัลควรส่งเสริมให้มีการเจรจาและการแบ่งปันความรู้มากขึ้นเกี่ยวกับสิ่งที่บริษัทต้องการเพื่อทำธุรกิจดิจิทัล

นอกจากนี้บริษัทเอกชนของจีนที่มีความใกล้ชิดกับรัฐบาลจีนอย่างมาก อาทิ Huaweiและ Alibaba กำลังเป็นผู้นำในการสร้างโครงสร้างพื้นฐานดิจิทัลและจัดวางศูนย์กลางธุรกิจทั่วเอเชียตะวันออกเฉียงใต้ ดังเช่นกรณีของประเทศไทยในปี 2017 บริษัท Huawei ซึ่งผลิตอุปกรณ์โทรคมนาคมและสมาร์ตโฟนได้จัดตั้ง “OpenLab” ขึ้นที่สำนักงานใหญ่ระดับภูมิภาคในกรุงเทพฯ ซึ่งเป็นส่วนหนึ่งของโครงการริเริ่ม “Thailand 4.0” (Lee, Rasser, Fitt, & Goldberg, 2020) ซึ่งเป็นแพลตฟอร์มพื้นฐานด้านสารสนเทศแบบครบวงจรสำหรับองค์กรต่าง ๆ เช่น การเป็นศูนย์การนำเสนอข้อมูลเพื่อใช้ใน Internet of Things (IoT) Big Dataและการจัดการข้อมูลบนระบบคลาวด์ (cloud) รวมถึงเป็นแพลตฟอร์มเพื่อช่วยในการทดสอบนวัตกรรมและฝึกอบรมด้านสารสนเทศแก่ลูกค้าและผู้ประกอบการภายในไทยและเอเชียตะวันออกเฉียงใต้ นอกจากนี้ บริษัท Huawei ยังได้เปิดตัวเทคโนโลยี 5G เป็นแห่งแรกในไทยเมื่อปี 2020 อีกด้วย อย่างไรก็ดีบริษัทด้านสารสนเทศของจีนรายใหญ่ เช่น Alibabaและ Tencent ได้แสดงความสนใจอย่างมากต่อยุทธศาสตร์ระเบียงเศรษฐกิจภาคตะวันออก (Eastern Economic Corridor: EEC) ของไทย ที่มุ่งหวังจะเปลี่ยนพื้นที่ส่วนใหญ่ในจังหวัดฉะเชิงเทรา ชลบุรีและระยองให้เป็นเขตอุตสาหกรรมในการผลิตและให้บริการทางด้านเทคโนโลยี (Eastern Economic Corridor, 2022)

บริษัท Alibaba ได้ก่อตั้งศูนย์กลางด้านดิจิทัลในไทยเพื่อเชื่อมโยงกับยุทธศาสตร์ระเบียงเศรษฐกิจภาคตะวันออกของไทยและเพื่อเป็นแพลตฟอร์มที่สำคัญในการช่วยให้ SMEs สามารถ

เปลี่ยนผ่านเป็นดิจิทัลได้ อำนวยความสะดวกด้านการค้าและการท่องเที่ยว รวมถึงฝึกอบรวมความรู้ด้าน E-commerce แก่ผู้ประกอบการในไทย ในปี 2019 สำนักงาน EEC ของไทยได้บรรลุข้อตกลงกับบริษัท Alibaba ในการใช้ E-commerceและเทคโนโลยีดิจิทัลในการส่งเสริมสินค้าไทย กับลูกค้าชาวจีน โดยเครือข่ายจีนดังกล่าวซึ่งจัดการด้วยระบบโลจิสติกส์อัจฉริยะ (smart logistics) ที่ควบคุมโดยบริษัท Alibaba ได้สร้างช่องทางที่รวดเร็วในการขนส่งสินค้า โดยเฉพาะอย่างยิ่งสินค้าเกษตร เช่น ทุเรียน เพื่อเข้าถึงจีนโดยส่งตรงจากฐานการผลิตในไทยภายในระยะเวลาอันสั้น นอกจากนี้บริษัท Alibaba ยังได้เสนอแนวคิดของ “Taobao Village Model” ซึ่งเป็นโมเดลเมืองอัจฉริยะโดยบริษัท Alibaba ให้กับไทยเพื่อช่วยแก้ไขปัญหาความยากจนและเพิ่มรายได้ของชุมชนผ่าน E-commerce และเทคโนโลยีดิจิทัล

อย่างไรก็ตาม กิจกรรมในกรอบยุทธศาสตร์เส้นทางสายไหมดิจิทัลที่เพิ่มขึ้นอย่างต่อเนื่องในปัจจุบันนั้นซึ่งมีการเคลื่อนย้ายของข้อมูลข้ามพรมแดนอยู่ตลอด ส่งผลให้เกิดความกังวลและความท้าทายด้านนโยบายใหม่ในด้านความเป็นส่วนตัว การแข่งขัน โดยเฉพาะอย่างยิ่งในด้านความมั่นคง ปัญหาดังกล่าวจะต้องได้รับความร่วมมือระหว่างรัฐบาลจีนและรัฐบาลที่เกี่ยวข้องเช่นเดียวกับไทย ในการทำงานและสร้างความเข้าใจร่วมกัน เพื่อก่อให้เกิดความไว้ใจและความเชื่อมั่นให้กับเศรษฐกิจที่ยั่งยืนในโลกดิจิทัล

# บทที่ 3

# แนวคิดและพลวัตทางปทัสถานของพื้นที่ไซเบอร์ในระดับสากล

## ความนำ

ในปี 2003 ประเด็นความมั่นคงไซเบอร์ในยุทธศาสตร์แห่งชาติของสหรัฐฯ ระบุว่า “พื้นที่ทางไซเบอร์” (cyberspace) เป็นพื้นที่เชื่อมโยงระหว่างเครือข่ายคอมพิวเตอร์ (computers) เซิร์ฟเวอร์ (servers) เราเตอร์ (routers) สวิตช์ (switches) และสายเคเบิลใยแก้วนำแสง (optical cable) ที่เชื่อมต่อกัน ซึ่งช่วยให้โครงสร้างพื้นฐานที่สำคัญต่าง ๆ ทำงานได้อย่างมีประสิทธิภาพ สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้นิยามเกี่ยวกับพื้นที่ทางไซเบอร์ทั้งในลักษณะทางกายภาพและไม่เป็นกายภาพ โดยมีองค์ประกอบทั้งหมดหรือบางส่วนซึ่งประกอบไปด้วย คอมพิวเตอร์และระบบการทำงานของเครื่อง (systems) เครือข่าย (networks) ซอฟต์แวร์ (software) ข้อมูล (data) และผู้ใช้ (users) ประเด็นสำคัญคือ การมี “ปฏิสัมพันธ์” จากมนุษย์ (human *interaction*) และ “การแลกเปลี่ยน” ข้อมูล (*exchange* of information) ประเด็นข้างต้นถูกเน้นย้ำในการให้คำจำกัดความของพื้นที่ทางไซเบอร์ที่เผยแพร่ในแผนยุทธศาสตร์ความมั่นคงไซเบอร์ของอังกฤษในปี 2011 ฉะนั้นพื้นที่ทางไซเบอร์จึงหมายรวมถึงความเชื่อมโยงของเครือข่ายต่าง ๆ อาทิ เครือข่ายบริการด้านการสื่อสาร เครือข่ายทางทหาร เครือข่ายทางอุตสาหกรรม เครือข่ายทางการเกษตรและอื่น ๆ ซึ่งเชื่อมโยงและสร้างความต่อเนื่องสอดคล้องกับพื้นที่ทางกายภาพ (physical space)

พื้นที่ทางไซเบอร์ถูกใช้เป็นเครื่องมือในการทำความเข้าใจและเปลี่ยนแปลงพื้นที่ทางกายภาพ หลังการก่อตั้งเครือข่ายขององค์กรภายใต้กระทรวงกลาโหมสหรัฐฯ คือ สำนักโครงการวิจัยขั้นสูงด้านกลาโหม (The Defense Advanced Research Projects Agency: DARPA) ในช่วงสงครามโลกครั้งที่ 2 พื้นที่ทางไซเบอร์ได้มีการบูรณาการและมีพลวัตผ่านเครือข่ายในหลายระดับ โดยนักวิชาการจำนวนหนึ่งได้แบ่งขอบเขตของความเกี่ยวพันของพื้นที่ทางไซเบอร์ไว้ดังนี้ ระดับที่หนึ่ง พื้นที่ทางไซเบอร์ที่เกี่ยวพันกับเครือข่ายการสื่อสาร ระดับที่สอง พื้นที่ทางไซเบอร์ที่เกี่ยวพันกับเครือข่ายข้อมูล และ ระดับที่สาม พื้นที่ทางไซเบอร์ที่เกี่ยวพันกับเครือข่ายคอมพิวเตอร์ (Chang, 2023) กล่าวได้ว่าความเกี่ยวพันกับเครือข่ายในระดับแรกนั้นมีจุดเริ่มต้นมาจากจากความต้องการขั้นพื้นฐานของระบบการสื่อสาร ในขณะที่ในระดับที่สองมีความเกี่ยวพันกับเครือข่ายข้อมูลนั้น มิได้หมายถึงเพียงความเกี่ยวพันของผู้ให้บริการด้านข้อมูลเพียงอย่างเดียว แต่หมายรวมถึงแพลตฟอร์มที่หลากหลาย ทั้งด้านธุรกิจ การค้า โซเชียลเน็ตเวิร์ค (social network) การเรียน การเงิน สงคราม ซึ่งอาจกล่าวได้ว่าประเด็นใดก็ตามที่สามารถขับเคลื่อนได้ผ่านอินเทอร์เน็ต หรือที่เรียกว่า “Internet+” สิ่งเหล่านั้นอยู่

ในขอบเขตของระดับความเกี่ยวพันในระดับที่สองทั้งสิ้น อย่างไรก็ดี ขอบเขตความเกี่ยวพันในระดับที่สาม ขับเคลื่อนจากกระบวนการเปลี่ยนแปลงของการทำให้เป็นข้อมูล (informatization) ในระดับที่สอง เข้าสู่การขัดเกลาทางสังคม (socialization) และการทำให้เป็นหน่วยขับเคลื่อนหรือองค์กรที่มีขนาดย่อย/เล็กลง (molecularization) ได้แก่ big data ปัญญาประดิษฐ์ (AI) Internet of Things (IoT) และการจัดการข้อมูลบนระบบคลาวด์ (cloud) สิ่งเหล่านี้กลายเป็นเทคโนโลยีหลักที่สำคัญในทำให้เกิดข้อมูลยุคใหม่ ด้วยเหตุนี้การบูรณาการของระบบซึ่งมีความซับซ้อนและมีขนาดใหญ่ดังกล่าวจะถูกขับเคลื่อนโดยปัญญาประดิษฐ์ที่ถูกสร้างขึ้น ซึ่งอาจกล่าวได้ว่าในอนาคตทิศทางของพัฒนาการของพื้นที่ทางไซเบอร์จะเกิดสิ่งที่เรียกว่า “พื้นที่กายภาพทางไซเบอร์” (cyber-physical space) หรืออย่างน้อยที่สุดพื้นที่ทางไซเบอร์และพื้นที่ทางกายภาพจะมีความแนบชิด ซับซ้อนและเชื่อมโยงกันมากขึ้น จนยากที่จะแยกเป็น 2 พื้นที่อย่างชัดเจน

**แนวคิดการกำกับดูแลพื้นที่ทางไซเบอร์สากล**

การกล่าวถึงการกำกับดูแลพื้นที่ไซเบอร์ (cyberspace governance) อาจไม่สามารถอธิบายได้อย่างชัดเจนว่า สิ่งใดคือนิยามที่ถูกที่สุดสำหรับประเด็นดังกล่าว กระนั้นผู้เขียนได้พยายามแจกแจงเพื่อให้เกิดความเข้าใจที่มากขึ้นว่า การกำกับดูแลพื้นที่ไซเบอร์ หมายถึง กิจกรรมการประสานงานและความร่วมมือระหว่างประเทศที่ดำเนินการโดยผู้มีส่วนได้ส่วนเสียทั้งหมดในประชาคมระหว่างประเทศ ทั้งรัฐบาลระดับชาติ ภาคเอกชน ภาคประชาสังคมและแม้กระทั่งผู้ใช้งานในเครือข่าย (users) เพื่อส่งเสริมการพัฒนาพื้นที่ไซเบอร์อย่างเป็นระเบียบและอย่างมีประสิทธิภาพ ซึ่งจะพิจารณาผลกระทบสำคัญ 2 ด้านร่วมกัน คือ ผลกระทบทางเทคโนโลยีและผลกระทบทางสังคม อนึ่ง การกำกับดูแลพื้นที่ไซเบอร์ สามารถแจกแจงได้เป็น 2 ระดับ คือ ระดับชาติ (national governance) และ ระดับโลก (global governance) ซึ่งทั้งสองลักษณะดังกล่าวไม่ควรแยกออกจากกันโดยสิ้นเชิง หรืออีกนัยหนึ่ง ตัวกระทำการ (agent) ควรทำความเข้าใจโครงสร้างพื้นฐานของการกำกับดูแลพื้นที่ไซเบอร์ทั้ง 2 ระดับ

ทั้งนี้ โครงสร้างของการกำกับดูแลพื้นที่ไซเบอร์ในปัจจุบันได้ถูกแจกแจงพื้นฐานไว้ 3 ลำดับชั้น ซึ่งเป็นรากฐานสำคัญของการกำกับดูแลทางอินเทอร์เน็ต (internet governance) ที่ถูกเสนอโดยองค์การความร่วมมือด้านการจัดสรรชื่อและหมายเลขทางอินเทอร์เน็ต (Internet Corporation for Assigned Names and Numbers: ICANN) ได้แก่ ชั้นโครงสร้างพื้นฐาน (infrastructure layer) ชั้นตรรกะ (logical layer) และชั้นเศรษฐกิจและสังคม (economic and social layer) (Cui & Liu, 2020) กล่าวคือ ชั้นโครงสร้างพื้นฐานเป็นชั้นที่กล่าวถึง ศูนย์ควบคุมทางอินเทอร์เน็ตต่าง ๆ สายเคเบิลภาคพื้นดิน สายเคเบิลใต้น้ำ ดาวเทียม ระบบไร้สาย (wireless systems) ชั้นตรรกะเป็นชั้นที่กล่าวถึงการแก้ปัญหาของเซิร์ฟเวอร์ (servers) ชื่อโดเมน (domain name) Internet Protocol

address (IP address) และมาตรวัดโปรโตคอล (protocol parameters) ชั้นที่สามระดับเศรษฐกิจและสังคมกล่าวถึงเรื่อง ผู้ใช้บริการ (application layer) ซึ่งใช้สำหรับการเผยแพร่ข้อมูล สิทธิสังคม และบริการของประชาชนเป็นสำคัญ

อย่างไรก็ตามการกำกับดูแลพื้นที่ไซเบอร์ในปัจจุบันทั้งสองระดับนั้นมีพัฒนาการอยู่ตลอดเวลา ซึ่งผู้เขียนได้แจกแจงปทัสถานการกำกับดูพื้นที่ไซเบอร์ในทางปฏิบัติออกเป็น 2 ลักษณะ ได้แก่ ลักษณะพหุภาคีนิยม (multilateralism) โดยมีรัฐเป็นตัวกระทำการที่มีบทบาทนำในการกำกับดูแลและลักษณะพหุภาคีแบบผู้มีส่วนได้ส่วนเสีย (multistakeholderism) โดยมีรัฐและองค์กรที่เกี่ยวข้องเป็นตัวแสดงที่มีบทบาทในการกำกับดูแลและร่วมกัน พัฒนาปทัสถานทางไซเบอร์ อนึ่ง ในอดีตมีใจความสำคัญมุ่งเน้นไปที่อธิปไตยของชาติ ซึ่งนำโดยรัฐบาลและกลุ่มอื่น ๆ ที่มีส่วนร่วมในความร่วมมือ เพื่อแก้ปัญหาที่เกี่ยวข้องกับพื้นที่ทางไซเบอร์และออกแบบยุทธศาสตร์การพัฒนาทางไซเบอร์ภายใต้กรอบขององค์การสหประชาชาติ (Moritz & Vytautas, 2019) ในเวลาต่อมาพัฒนาการของพื้นที่ไซเบอร์ ได้รับอิทธิพลจากชาติตะวันตกมากขึ้น ส่งผลให้เกิดการมุ่งเน้นที่ความต้องการของผู้มีส่วนได้ส่วนเสียหลายฝ่าย ในนิยามข้างต้นทำให้อำนาจอธิปไตยของชาติในมิติดังกล่าวอ่อนแอลง และทำให้เกิดการสนับสนุนความเท่าเทียมกันในการมีส่วนร่วม เพื่อส่งเสริมกลไกการตัดสินใจจากล่างขึ้นบน อาจกล่าวในเบื้องต้นได้ว่า ความแตกต่างระหว่างสองพัฒนาการดังกล่าวข้างต้นนั้นสะท้อนภาพของการแข่งขันระหว่างกลไกการตัดสินใจจากบนลงล่างและจากล่างขึ้นบน

อย่างไรก็ดี เมื่อพิจารณาในทางปฏิบัติดูเหมือนว่า ปทัสถานของโลกตะวันตกนั้นจะมีสหรัฐฯ เป็นผู้มีบทบาทนำ ซึ่งมีแนวปฏิบัติแบบพหุภาคี ผนวกกับข้อได้เปรียบอย่างมากในฐานะผู้ริเริ่ม ในการนี้อาจเรียกได้ว่าเป็นพหุภาคีที่มีความ “พิเศษ” เนื่องจากสถานะภาพในฐานะผู้ริเริ่มนั้นมีมิติของอำนาจอย่างมีนัยสำคัญ ผู้เขียนได้ตั้งข้อสังเกตว่า ความเป็นจริงในทางปฏิบัติของอำนาจการจัดการและควบคุมระบบ (พื้นที่ไซเบอร์) ดูเหมือนรัฐบาลจะมีอำนาจในการกำกับดูแลระบบมากกว่าจะเป็นภาพขององค์การที่เกี่ยวข้องคอยกำกับดูแลร่วมกัน ประเด็นดังกล่าวชี้ให้เห็นว่า ความร่วมมือในลักษณะพหุภาคีนั้นถูกท้าทายด้วยตัวของมันเอง กล่าวคือ ภายในความร่วมมือพหุภาคีในสภาพเช่นว่านั้นมีมิติของระเบียบที่มีลำดับชั้น (hierarchy order) แฝงอยู่ภายในความร่วมมืออย่างมีนัยสำคัญ ดังนั้น หลักความร่วมมือพหุภาคีโดยทั่วไปและแนวพหุภาคีที่มีความพิเศษดังกล่าวอาจไม่เพียงพอต่อการบรรลุหลักการกำกับดูแลพื้นที่ไซเบอร์ที่ควรเป็น ในลักษณะที่ทุกฝ่ายมีส่วนร่วมอย่างเท่าเทียม

**ตัวแบบปทัสถานทางไซเบอร์โดยผู้มีส่วนได้ส่วนเสียหลายฝ่าย (multi-stakeholder model) กับการนำไปใช้**

สหรัฐฯ เป็นมหาอำนาจพื้นที่ทางไซเบอร์ ซึ่งได้ยกระดับประเด็นพื้นที่ทางไซเบอร์ให้เป็นหนึ่งในประเด็นยุทธศาสตร์ของชาติ โดยลักษณะและรูปแบบการกำกับดูแลจะขึ้นอยู่กับผู้มีส่วนได้ส่วนเสียหลายฝ่าย (multi-stakeholder model) ด้านหนึ่ง สหรัฐฯ ให้ความสำคัญกับการพัฒนาองค์กรที่เกี่ยวข้องทางด้านเทคโนโลยีและการปกป้องข้อมูลส่วนตัว (personal privacy data) อาทิ สหรัฐฯ มีการจัดทำเอกสารทางกฎหมายที่เข้มงวด รวมถึงระบบตรวจสอบความปลอดภัยของเครือข่าย เป็นต้น ในขณะเดียวกันด้านเนื้อหาและขอบเขตของการกำกับดูแลพื้นที่ทางไซเบอร์ สหรัฐฯ มีความพยายามในการบูรณาการประเด็นทางทหารและปฏิบัติการทางทหารเข้ามาเกี่ยวข้องอย่างต่อเนื่อง (Zhao, Shi, & Yao, 2021) ซึ่งชี้ให้เห็นว่า การพัฒนาพื้นที่ทางไซเบอร์ดังกล่าวไม่ควรถูกเพิกเฉย หรือละเลย นอกจากนี้สหรัฐฯ ได้เน้นย้ำถึงการให้คำมั่นต่อการพัฒนานวัตกรรมทางเทคโนโลยีมาโดยตลอด ตั้งแต่การฝึกอบรมผู้มีความสามารถไปจนถึงการลงทุนในภาคอุตสาหกรรมซึ่งเป็นหนึ่งในประเด็นที่นานาชาติให้ความสนใจอยู่เสมอ

หนึ่งในประเทศซึ่งมีความน่าสนใจต่อตัวแบบดังกล่าว คือ สิงคโปร์ หนึ่งในประเทศที่มีฐานข้อมูลทางไซเบอร์จำนวนมาก โดยเฉพาะอย่างยิ่งการเป็นชุมทางทางไซเบอร์ในพื้นที่เอเชียตะวันออกเฉียงใต้ สิงคโปร์ได้จัดตั้งระบบการจัดการองค์กร ระบบนโยบายและระบบกฎหมายที่ดีในการบริหารจัดการพื้นที่ทางไซเบอร์ ในปี 2015 รัฐบาลสิงคโปร์ได้ก่อตั้งหน่วยงานความมั่นคงทางไซเบอร์แห่งสิงคโปร์ (Cyber Security Agency of Singapore: CSA) มีวัตถุประสงค์เพื่อประสานงานด้านการกำกับดูแลทางไซเบอร์โดยเฉพาะในประเด็นที่เกี่ยวกับความมั่นคง สิงคโปร์ได้นำประเด็นเรื่องความมั่นคงไซเบอร์เข้ามาเป็นส่วนหนึ่งของประเด็นทางนโยบาย ส่งผลให้เกิดการพัฒนาระบบนิเวศทางไซเบอร์ภายในสิงคโปร์ ตลอดจนการเสริมสร้างความร่วมมือระหว่างประเทศในพื้นที่ทางไซเบอร์และด้านอื่น ๆ โดยเฉพาะในปี 2017 ถือเป็นปีที่สำคัญสำหรับสิงคโปร์ในด้านพัฒนาการทางด้านความมั่นคงไซเบอร์ สิงคโปร์ได้จัดทำร่างกฎหมายความมั่นคงทางไซเบอร์ฉบับใหม่และกฎหมายต่าง ๆ รวมถึงกฎหมายว่าด้วยความมั่นคงภายในประเทศที่เกี่ยวข้อง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและพระราชบัญญัติการใช้คอมพิวเตอร์และความมั่นคงทางไซเบอร์ในทางที่ผิด (Abuse of Computer and Cybersecurity Act) วัตถุประสงค์จัดตั้งขึ้นเพื่อควบคุมระเบียบในพื้นที่ทางไซเบอร์ อย่างไรก็ดีนักวิชาการจำนวนหนึ่งมีทัศนะต่อการกำกับดูแลพื้นที่ทางไซเบอร์ของสิงคโปร์ว่าพัฒนาการต่าง ๆ ที่เกิดขึ้นในปี 2017 ถือเป็นพลวัตที่สร้างความเปลี่ยนแปลงภายในของพื้นที่ไซเบอร์ในสิงคโปร์ เนื่องจากบทบาทหน้าที่ของรัฐบาลไม่ได้เป็นแบบ “รอบด้าน (all-round)” แต่มีลักษณะของ “ความร่วมมือ (cooperation)” ที่มากขึ้น (Wang, 2018) กล่าวคือ รัฐบาลสิงคโปร์ได้ลด

บทบาทของตัวเองในการควบคุมระเบียบพื้นที่ทางไซเบอร์ โดยหันไปเน้นการบูรการและสร้างความร่วมมือกับหน่วยงานภายนอกประเทศมากขึ้น ประการแรก สิงคโปร์ผลักดันและเสริมสร้างความตระหนักรู้เรื่องพื้นที่ทางไซเบอร์เข้าสู่อาเซียน เพื่อสนับสนุนความร่วมมือกับสมาชิกในอาเซียนและประเทศอื่น ๆ ภายนอก ประการที่สอง สิงคโปร์พยายามที่จะร่วมมือกับองค์กรและมหาวิทยาลัยทั้งภายในและภายนอกที่มีเทคโนโลยีขั้นสูง เพื่อซึมซับเทคโนโลยีและองค์ความรู้ที่ทันสมัยกว่าด้วยวิธีการฝึกอบรมบุคลากรที่มีความเชี่ยวชาญพิเศษ ประการที่สาม สิงคโปร์ได้ทำการสำรวจการมีส่วนร่วมของคนภายในประเทศ เพื่อสร้างความมีส่วนร่วมของคนในชาติในการกำกับดูแลความมั่นคงในพื้นที่ทางไซเบอร์ (Zhao, Shi, & Yao, 2021)

นอกจากสิงคโปร์ ประเทศญี่ปุ่นเป็นอีกหนึ่งประเทศที่มีลักษณะการกำกับดูแลพื้นที่ทางไซเบอร์ที่น่าสนใจ กล่าวคือ ลักษณะของการกำกับดูแลพื้นที่ทางไซเบอร์ในประเทศญี่ปุ่นยุคใหม่ ผู้เขียนได้แจกแจงการอธิบายไว้ 3 มุมมอง ประการที่หนึ่ง การพิจารณาพื้นที่ทางไซเบอร์จากมุมมองทางเศรษฐกิจ กล่าวคือ ญี่ปุ่นให้ความสำคัญอย่างยิ่งในการพัฒนาพื้นที่ไซเบอร์สำหรับการใช้งานในชีวิตประจำวันโดยเฉพาะในชั้นผู้ใช้บริการ (application layer) โดยสอดคล้องกับการพัฒนาเทคโนโลยีด้านดิจิทัลในประเทศ สำนักงานใหญ่ยุทธศาสตร์ความมั่นคงไซเบอร์ของญี่ปุ่น (Cyber Security Strategy Headquarters) ได้ประกาศใช้กฎหมายว่าด้วยเรื่องกิจการทางดิจิทัล (Digital Procedure Law) ในปี 2019และได้กำหนดโครงร่างนโยบายทางเทคโนโลยีสารสนเทศใหม่สำหรับยุคดิจิทัลในปีเดียวกัน นอกจากนี้ญี่ปุ่นให้การยอมรับการนำข้อมูลส่วนตัวมาใช้ในอุตสาหกรรมในปี 2018 โดยได้ริเริ่มอุตสาหกรรมทางด้านข้อมูลในลักษณะของ “ธนาคารข้อมูล (information banking)” เกิดเป็นองค์กรแห่งแรกของโมเดลธุรกิจที่ใช้ข้อมูลส่วนบุคคลเพื่อสร้างมูลค่าทั่วโลก (Ding, 2020) ประการที่สอง การพิจารณาพื้นที่ทางไซเบอร์จากมุมมองความมั่นคง ประเทศญี่ปุ่นได้เข้าสู่ยุคของการพัฒนาเครือข่ายความมั่นคงขั้นสูงอย่างเป็นทางการในปี 2013 โดยเกิดเอกสารที่เกี่ยวข้องกับนโยบายและหน่วยงานด้านไซเบอร์เพิ่มมากขึ้น ซึ่งชี้ให้เห็นว่า รัฐบาลญี่ปุ่นตื่นตัวและให้ความสำคัญกับสังคมดิจิทัลโดยเฉพาะพื้นที่ทางไซเบอร์ ประการที่สาม การพิจารณาพื้นที่ทางไซเบอร์จากมุมมองของการบูรณาการทั้งสองมุมมองข้างต้น ในปี 2020 รัฐบาลญี่ปุ่นได้นำยุทธศาสตร์เครือข่ายความมั่นคงปี 2018 มาปรับปรุง เพื่อเสนอยุทธศาสตร์ของการสร้าง ระบบนิเวศความมั่นคงทางไซเบอร์ (cyber security ecosystem) ซึ่งเป็นแนวคิดในการสร้างกลไกการประสานงานนโยบายระหว่างประเทศของญี่ปุ่น ในทางหนึ่งเพื่อเป็นการบังคับตัวเองให้พัฒนากลไกในทางปฏิบัติให้เกิดขึ้น ซึ่งไม่เพียงแต่ก่อให้เกิดการสนับสนุนพัฒนาการการกำกับดูแลพื้นที่ทางไซเบอร์ในญี่ปุ่น แต่ยังสอดคล้องกับปทัสถานของการพื้นที่ทางไซเบอร์สากลอีกด้วย นอกจากนี้ ในปี 2021 รัฐสภาแห่งชาติญี่ปุ่น (National Diet) ได้ผ่านกฎหมายที่สำคัญในการผลักดันเรื่อง สังคมดิจิทัล (digital society) อย่างไรก็ดี ผู้เขียนเชื่อว่าพัฒนาการดังกล่าวถูกกระตุ้นให้เกิดขึ้นเนื่องจากสถานการณ์การแพร่ระบาดของเชื้อ

โควิด 19 (COVID-19) ส่งผลให้พื้นที่ทางไซเบอร์กับชีวิตจริงมีความแนบชิดกันมากขึ้น สอดคล้องกับแนวนโยบายที่นายกรัฐมนตรี Yoshihide Suga (2020-2021) ประกาศในเรื่อง “realization of a digitalized society” ซึ่งเป็นความพยายามในการลดกระบวนการที่หลากหลายของภาครัฐต่อประชาชน โดยสรุปใจความของถ้อยแถลงดังกล่าวได้ความว่า เพื่อลดกระบวนการและขั้นตอนของภาครัฐแก่ประชาชนในการติดต่อกับภาครัฐ เพื่อให้ประชาชนไม่จำเป็นต้องมาสถานที่ทำการทางราชการในการติดต่อ โดยเฉพาะการผลักดันกลุ่มคนที่อาศัยนอกเขตเมือง เพื่อให้สามารถเข้าถึงบริการทางแพทย์ (อาทิ วัคซีน การกักตัว การรักษา ในช่วงเวลานั้น) และการศึกษาในระดับเดียวกับประชาชนในเขตเมือง (Japan Cybersecurity Innovation Committee [JCIC], 2020) ส่งผลให้เกิดการสนับสนุนสังคมดิจิทัลขึ้นอย่างรวดเร็วภายในญี่ปุ่นในสภาพบังคับภายใต้เงื่อนไขทางสังคมและสถานการณ์การแพร่ระบาดของโรคติดต่อ สะท้อนให้เห็นถึงพัฒนาการที่สำคัญของพื้นที่ทาง ไซเบอร์ในประเทศญี่ปุ่น

จากการยกตัวอย่าง 3 ประเทศข้างต้นจะเห็นได้ถึงแนวทางในการพัฒนาพื้นที่ทางไซเบอร์ประเทศที่มุ่งพัฒนาการกำกับการดูแลพื้นที่ทางไซเบอร์ภายใต้กรอบปทัสถานลักษณะของการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียหลายฝ่ายในการกำกับดูแลร่วมกับรัฐ (multi-stakeholder governance) สรุปได้ดังนี้ ขั้นแรก รัฐควรสร้างกลไกการเพื่อรับรองสถาบันให้มีประสิทธิภาพ รวมถึงการจัดองค์กรและกำหนดตำแหน่งขององค์กรการจัดการที่ชัดเจน ร่างกฎหมายและระเบียบข้อบังคับรวมถึงเอกสารทางนโยบายที่เกี่ยวข้องเพื่อเป็นกรอบสำหรับองค์กรและหน่วยงานที่เกี่ยวข้อง ประการที่สอง คือ การให้ความสนใจกับการพัฒนาและการประยุกต์ใช้ชั้นผู้ใช้บริการ (application layer) ในพื้นที่ทางไซเบอร์เพื่อสร้างระบบนิเวศของพื้นที่ทางไซเบอร์ กล่าวคือ บูรณาการพื้นที่ทางไซเบอร์เข้าสู่ชีวิตประจำวัน อาจกล่าวในลักษณะของการทำให้เป็นดิจิทัล (digitalization) ได้เช่นเดียวกัน อนึ่งเพื่อสนับสนุนให้ประชาชนมีส่วนร่วมและเกี่ยวข้องกับพื้นที่ทางไซเบอร์มากขึ้น ประการที่สาม ยกระดับยุทธศาสตร์พื้นที่ทางไซเบอร์ให้เป็นยุทธศาสตร์ระดับชาติ ประการที่สี่ รัฐบาลควรทำงานร่วมกับองค์กรและประชาชนเพื่อพัฒนาแผนยุทธศาสตร์การกำกับดูแลพื้นที่ทางไซเบอร์

นอกจากนี้ เทคโนโลยีทางอินเทอร์เน็ตเป็นพื้นฐานสำคัญของพื้นที่ทางไซเบอร์และเป็นแรงผลักดันที่สำคัญในการพัฒนาประเทศ จากการศึกษาพบว่า การลงทุนในโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศและการสื่อสาร มีความสัมพันธ์อย่างมากกับการเติบโตทางเศรษฐกิจ (Global Connectivity Index, 2020) กล่าวคือ การพัฒนาในทุกด้านที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารจะทำให้มูลค่าผลิตภัณฑ์มวลรวมของประเทศสูงขึ้น (Gross Domestic Product: GDP) ดังนั้นเมื่อกล่าวถึงกลไกการกำกับดูแลพื้นที่ทางไซเบอร์ สิ่งแรกที่ต้องพิจารณา คือ การพัฒนาขีดความสามารถของนวัตกรรมทางเทคโนโลยีอินเทอร์เน็ต ซึ่งเป็นแนวปฏิบัติที่สหรัฐฯ ให้ความสำคัญ

(*Xinhuanet*, 2020a) ในทางหนึ่ง เราอาจอ้างอิงจากแนวปฏิบัติของสิงคโปร์ในประเด็นเรื่องการซึมซับความแข็งแกร่งทางเทคนิคและประสบการณ์การฝึกอบรมความเชี่ยวชาญเฉพาะทางจากประเทศที่พัฒนาแล้วมาประกอบการดำเนินนโยบาย เพื่อนำมาพัฒนาทางเทคโนโลยี ปรับปรุงจุดด้อยและพัฒนาข้อได้เปรียบ นำไปสู่การริเริ่มทางนวัตกรรมด้านเทคโนโลยี หรือในอีกทางหนึ่ง ในมิติของการพัฒนาทางเศรษฐกิจ เราอาจอ้างอิงแนวปฏิบัติในการประยุกต์ใช้และการจัดการความมั่นคงของพื้นที่ทางไซเบอร์จากญี่ปุ่น ในลักษณะของการกระชับความร่วมมือกับชาติอื่น ๆ ดำเนินความร่วมมือข้ามชาติบนพื้นฐานของความไว้วางใจ ส่งเสริมการแลกเปลี่ยนประสบการณ์และการปรึกษาหารือในเวทีระหว่างประเทศในกรอบของกฎหมายระหว่างประเทศและร่วมกันออกแบบ สร้างชุมชนแห่งการแบ่งปันในพื้นที่ทางไซเบอร์ในอนาคต

อย่างไรก็ตาม ผู้เขียนต้องการเสนอว่า กระบวนของการกำกับการดูแลพื้นที่ทางไซเบอร์ภายใต้ปทัสถานที่ผู้มีส่วนได้ส่วนเสียหลายฝ่ายสิ่งสำคัญที่ควรตระหนัก คือ อำนาจสาธารณะ (public power) เช่นเดียวกับตัวแสดงอื่นที่ไม่ใช่รัฐควรได้มีบทบาทในการริเริ่มการออกแบบการกำกับการดูแลพื้นที่ทางไซเบอร์ อย่างไรก็ดี องค์กรที่จะสามารถใช้อำนาจสาธารณะดังกล่าวนั้นควรมีลักษณะสำคัญบางประการดังนี้ องค์กรที่มีอำนาจการจัดการไม่เพียงแต่จะต้องกำกับดูแลพื้นที่ทางไซเบอร์เท่านั้น แต่ยังหมายรวมถึงการริเริ่มด้วย นอกจากนี้องค์กรควรเป็นกำลังสำคัญในการประสานงานการมีส่วนร่วมระหว่างองค์กร สนับสนุนประชาธิปไตย ภาคประชาสังคมและตัวแสดงอื่น ๆ ด้วย

**จีนกับการกำหนดปทัสถานทางเทคโนโลยีและยุทธศาสตร์วงจรคู่ขนาด (dual circulation)**

ในปี 2020 คณะกรรมการกลางพรรคคอมมิวนิสต์จีน (Chinese Communist Party: CCP) ได้เผยแพร่แผนยุทธศาสตร์ 5 ปี สำหรับการจัดทำแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 14 (2021–2025) และเป้าหมายระยะยาวเพื่อให้สอดคล้องกับยุทธศาสตร์การพัฒนาปี 2035 (*Xinhuanet*, 2016) แผนยุทธศาสตร์ดังกล่าวของจีน แสดงให้เห็นถึงความทะเยอทะยานของจีนที่จะทำให้ระบบการพัฒนาเป็นที่ยอมรับในสากล โดยเฉพาะในประเด็นเรื่องการรวมความสามารถทางเศรษฐกิจและเทคโนโลยีของประเทศไว้ภายใต้การควบคุมโดยส่วนกลาง รัฐบาลจีนเชื่อว่าการปฏิวัติทางวิทยาศาสตร์และเทคโนโลยีที่เกิดขึ้นภายในจีนจะเป็นกำลังสำคัญในการทำให้จีนสามารถผลักดันการพึ่งพาตนเองทางเศรษฐกิจและเทคโนโลยีและเป็นพลังที่จะช่วยให้จีนกลายเป็นมหาอำนาจชั้นนำระดับโลก

ในส่วนหนึ่งของแผนยุทธศาสตร์ 5 ปี ฉบับที่ 14 รัฐบาลจีนพยายามยกระดับการพัฒนาด้านเทคโนโลยีเพื่อให้เพียงพอต่อการพึ่งพาตนเอง โดยเฉพาะอย่างยิ่งด้านเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรัฐบาลจีนมีความหวาดระแวงในการที่จะถูกตัดขาดจากเทคโนโลยีต่างประเทศที่มีโลก

ตะวันตกนำ หรืออาจกล่าวอีกนัยหนึ่งได้ว่า เป็นเทคโนโลยีที่มีสหรัฐฯ เป็นผู้นำ ประธานาธิบดีจีน สี จิ้นผิง กล่าวย้ำเสมอถึงความหวั่นเกรงดังกล่าวส่วนหนึ่งใจความว่า “ความจริงที่ว่าเทคโนโลยีหลักถูกควบคุมโดยผู้อื่น คือ อันตรายที่ซ่อนอยู่ที่สุดของเรา (จีน)” (Mochinaga, 2021) สะท้อนให้เห็นว่า สี จิ้นผิงและพรรคคอมมิวนิสต์จีนให้ความสำคัญต่อเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในฐานะของการเป็นกิจการภายใน ความมั่นคงแห่งชาติและอิทธิพลในเวทีโลก อนึ่ง ยุทธศาสตร์ข้อริเริ่มแถบและทาง (Belt and Road Initiative: BRI) และโดยเฉพาะยุทธศาสตร์เส้นทางสายไหมดิจิทัล (Digital Silk Road: DSR) ถือได้ว่าเป็นยุทธศาสตร์ที่มีนัยของการสนับสนุนระบบนิเวศทางดิจิทัลภายในของจีนให้กลายเป็นสากล ซึ่งประกอบด้วยเทคโนโลยี โครงสร้างพื้นฐาน แพลตฟอร์มการให้บริการด้านต่าง ๆและกฎหมาย

ยุทธศาสตร์เส้นทางสายไหมดิจิทัลแสดงให้เห็นว่าแนวคิดทางยุทธศาสตร์ในแบบ “วงจรคู่ขนาน” (dual circulation) เป็นองค์ประกอบสำคัญของการพัฒนาของจีน ซึ่งจีนจะได้รับผลตอบแทนจากการลงทุน ยุทธศาสตร์วงจรคู่ขนานประกอบด้วยวงจรทางเศรษฐกิจภายในประเทศและระหว่างประเทศ เมื่อพิจารณาจากมุมมองทางเทคโนโลยี โครงการหลักอย่างข้อริเริ่มแถบและทางของจีนมีส่วนสนับสนุนในการส่งออกเทคโนโลยีจีนที่พัฒนาภายในประเทศ ไปสู่ภายนอก กล่าวคือ ในขณะที่ประเทศที่เป็นส่วนหนึ่งของยุทธศาสตร์แถบและทางจะได้รับการพัฒนาโครงสร้างพื้นฐานที่เชื่อมโยงผู้คน สินค้าและเงินเข้าไปกับเทคโนโลยีเพื่อการพัฒนาเศรษฐกิจ อุตสาหกรรมของจีน ส่งผลให้เกิดเป็นวงจรหมุนเวียนของการลงทุนของอุตสาหกรรมจีนอย่างมีนัยสำคัญ หมายถึง ความช่วยเหลือภายใต้แผนยุทธศาสตร์ดังกล่าวของจีนภายใต้เงื่อนไขและข้อตกลงของจีนนั้น มีข้อผูกมัดบางประการที่สำคัญในเรื่องการต้องยอมรับสินค้า การค้า ผลิตภัณฑ์และผู้คนที่มาจากบริษัทจีน ส่งผลให้โครงการภายใต้ชื่อยุทธศาสตร์เหล่านี้ได้ยกระดับการพึ่งพาอาศัยกันทางเศรษฐกิจและเทคโนโลยีระหว่างประเทศจีนและกลุ่มประเทศผู้เกี่ยวข้อง

กรอบกลยุทธ์ทางเศรษฐกิจแบบวงจรคู่ขนานของจีนมีจุดมุ่งหมายเพื่อส่งเสริมนวัตกรรมบริษัทเทคโนโลยีภายในประเทศจีนและทำให้บริษัทเหล่านั้นของจีนมีขีดความสามารถในการแข่งขันได้ทั่วโลก โดยขั้นตอนที่หนึ่งจากการหมุนเวียนการลงทุน การพัฒนาและการนำเทคโนโลยีไปใช้ภายในประเทศโดยได้รับการสนับสนุนจากรัฐบาล รัฐบาลจีนได้สนับสนุนการวิจัยและการพัฒนาเทคโนโลยีใหม่ เช่น การสื่อสารทางโทรศัพท์ อี-คอมเมิร์ซ เมืองอัจฉริยะ เป็นต้น การสนับสนุนจากรัฐบาลในประเด็นดังกล่าวส่งผลให้บริษัทจีนยกระดับห่วงโซ่คุณค่า (value chain) และเตรียมความพร้อมสำหรับการแข่งขันในระดับโลก ขณะเดียวกันการพัฒนาเทคโนโลยีในภาคเอกชนของบริษัทจีนได้รับความช่วยเหลือจากรัฐบาลจีน จากการอำนวยในการออกใบอนุญาตและการอนุมัติด้านกฎหมาย ซึ่งรัฐบาลจีนมีมาตรการที่เข้มงวดในการออกใบอนุญาตและการอนุมัติด้านกฎหมายภายในของจีนต่อ

บริษัทต่างประเทศ (Lin & MinMin, 2020) ทั้งนี้ ส่งผลให้สินค้าจากต่างประเทศเข้าสู่ตลาดจีนได้ยาก

ขั้นตอนที่สอง รัฐบาลจีนได้ผลักดันบริษัทจีนเพื่อทำให้เทคโนโลยีของจีนมีความเป็นสากลและสามารถจูงใจประเทศอื่น ๆ ให้ต้อนรับการลงทุนและเทคโนโลยีของจีน ดังนั้น การกำหนดมาตรฐาน (standardization) เป็นกุญแจสำคัญในการทำให้เป็นสากล กล่าวคือ ทำให้ประเทศอื่นต้องพึ่งพาบริษัทและเทคโนโลยีจากจีน อุตสาหกรรมของจีนมีความพยายามในการกำหนดมาตรฐานทางเทคโนโลยีเข้าสู่องค์การระหว่างประเทศผ่านการสนับสนุนจากรัฐบาลจีน พฤติกรรมดังกล่าวของจีนนับเป็นหัวใจสำคัญสำหรับอุตสาหกรรมต่าง ๆ ของจีน เพื่อแข่งขันกับผู้เล่นที่โดดเด่นซึ่งกำหนดมาตรฐานเทคโนโลยีระดับโลกมาเป็นเวลาหลายทศวรรษ

ยุทธศาสตร์การริเริ่มแถบและทางและเส้นทางสายไหมดิจิทัล คือ เครื่องมือในการสนับสนุนการทำให้เทคโนโลยีจีนมีความเป็นสากลผ่านการเจรจาระหว่างรัฐบาล โครงการต่าง ๆ ภายใต้ยุทธศาสตร์แถบและทาง กล่าวคือ เกิดการส่งออกระบบที่ประกอบด้วยเทคโนโลยีที่ถูกทดสอบและเป็นมาตรฐานที่จีนเป็นผู้กำหนด ทั้งด้านประสิทธิภาพ โดยเฉพาะต้นทุนซึ่งมักจะถูกกว่ารัฐคู่แข่งทางเทคโนโลยี เช่น ญี่ปุ่น เกาหลีใต้ รัฐในยุโรป โดยเฉพาะสหรัฐฯ เพื่อใช้เป็นสิ่งดึงดูดรัฐผู้รับโครงการ

นอกจากนี้ ข้อริเริ่มแถบและทางยังเข้ากันได้กับระบอบการปกครองแบบอำนาจนิยมและเผด็จการ ซึ่งเป็นลักษณะของรัฐบาลที่ตั้งใจจะใช้อำนาจแบบรวมศูนย์เพื่อควบคุมพลเมืองของตนด้วยเทคโนโลยี อนึ่ง ระบบทุนนิยมที่มีรัฐนำแบบจีนนั้นง่ายและสอดรับกันได้ดีกับรัฐที่ปกครองแบบอำนาจนิยมในการจัดตั้งโครงการที่ถูกควบคุมโดยกลุ่มชนชั้นนำ ในขณะที่เทคโนโลยีของจีนบางอย่างยังช่วยแก้ปัญหาให้กับรัฐในพื้นที่เอเชียตะวันออกเฉียงใต้ที่ต้องการบรรลุความมั่นคงของชาติ การพัฒนาเศรษฐกิจและการสร้างเสถียรภาพของระบอบในลักษณะอำนาจนิยม หรือเผด็จการ เช่น กรณีสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (The Association of Southeast Asian Nations: ASEAN) ในปี 2019 จีนมีความพยายามในการผลักดันโครงการเมืองอัจฉริยะเพื่อการพัฒนาที่ขับเคลื่อนด้วยนวัตกรรม ส่งผลให้ในปีต่อมารัฐบาลเมียนมาร์ได้เปิดตัวการใช้ระบบกล้องวงจรปิดของ Huawei ที่มีความสามารถในการจดจำใบหน้าในเมืองหลวงเนปิดอว์ (Association of Southeast Asian Nations, 2019) แสดงให้เห็นว่า แม้ระบบการเมืองของเมียนมาร์ในสมัยออองซานซูจีขณะนั้นจะมีความเป็นประชาธิปไตยอยู่บ้าง แต่ปฏิเสธไม่ได้ว่า กลุ่มผลประโยชน์ที่ยังคงขับเคลื่อนทางการเมืองเมียนมาร์ยังคงเป็นกลุ่มชนชั้นนำ โดยเฉพาะอย่างยิ่งกลุ่มที่มีอิทธิพลในกองทัพ เป็นต้น

ในขั้นตอนท้ายสุดท้ายของกลยุทธ์แบบวงจรคู่ขนานของจีน คือ การใช้อิทธิพล “เหนือ” กลุ่มประเทศภายใต้โครงการแถบและทางและโดยเฉพาะอย่างยิ่งโครงการที่มีลักษณะของการบูรณาการทางเทคโนโลยี ซึ่งจะมีลักษณะเป็นดังการ *ติดตั้ง (install)* ยุทธศาสตร์ที่จะนำมาซึ่งผลตอบแทนทางเศรษฐกิจให้กับจีน ตัวอย่างเช่น ค่าธรรมเนียมสิทธิบัตรจากผู้ประกอบการโทรคมนาคมและผู้ผลิตใน

ประเทศต่าง ๆ เป็นประโยชน์ต่ออุตสาหกรรมจีนและบริษัทจีน กล่าวคือ บริษัทจีนเหล่านั้นได้รับค่าลิขสิทธิ์หรือค่าธรรมเนียมจากใบอนุญาตของสิทธิบัตรที่จำเป็นต้องมีมาตรฐาน (standard essential patents: SEPs) ที่ต้องใช้เพื่อปฏิบัติตามมาตรฐานทางเทคนิค ในขณะเดียวกัน หนึ่งในประเด็นที่สำคัญของการพัฒนาโครงสร้างพื้นฐานทั้งทางกายภาพและโดยเฉพาะอย่างยิ่งในแบบดิจิทัลนั้นมีลักษณะของการผูกติดกับผู้กำหนดมาตรฐาน ซึ่งจำเป็นต้องมีการดำเนินการและบำรุงรักษา ส่งผลให้เป็นเรื่องยากสำหรับประเทศต่าง ๆ ที่จะถอด/ถอนเทคโนโลยีออกเมื่อฝังอยู่ในโครงข่ายไฟฟ้า เครือข่ายโทรคมนาคมและองค์ประกอบสำคัญอื่น ๆ ของสังคม อย่างไรก็ดี ในความเป็นจริงนั้นอาจเลวร้ายกว่าที่คาดการณ์สำหรับประเทศที่พึ่งพาเทคโนโลยีของจีนมากขึ้นเรื่อย ๆ ธุรกิจของจีนจะได้เปรียบในการได้รับสัญญาการดำเนินการและบำรุงรักษา เนื่องจากธุรกิจเหล่านั้นคุ้นเคยกับการใช้งานและการบำรุงรักษาเทคโนโลยี ส่งผลให้บริษัทจีนเข้าถึงข้อมูลทางภูมิศาสตร์ โดยเฉพาะอย่างยิ่งโครงสร้างกายภาพของจุดยุทธศาสตร์ที่สำคัญของรัฐ อาจนำไปสู่ประเด็นด้านความมั่นคงได้

ยกตัวอย่างกรณีโครงสร้างพื้นฐานของลาวซึ่งต้องพึ่งพาเทคโนโลยีของจีนเป็นอย่างมาก กล่าวคือ Huawei ได้รับการสนับสนุนในการก่อสร้างโครงสร้างพื้นฐานโทรคมนาคมภายในประเทศลาวซึ่งบูรณาการเข้ากับทางหลวงและทางรถไฟ ขณะที่ Huawei ได้เสนอแพลตฟอร์มทางเทคโนโลยีสารสนเทศและระบบการจัดการสำหรับโครงการทางด่วนอัจฉริยะ (smart highway) อันเป็นส่วนหนึ่งของโครงการทางด่วนจีน-ลาว ซึ่งจะรวมเข้ากับโครงสร้างพื้นฐานการสื่อสารเคลื่อนที่ 5G ในอีกด้านหนึ่งจีนกำลังดำเนินโครงการทางรถไฟที่เดินทางจากประตูพรมแดนจีน-ลาวไปยังเวียงจันทร์ ดังนั้นทางเชื่อมคุนหมิง-เวียงจันทร์นี้ในที่สุดจะเชื่อมต่อกับเส้นทางรถไฟที่มุ่งไปยังกรุงเทพฯ และทางตอนใต้คาบสมุทรมาเลย์แม้ว่าสัญญาที่มอบให้กับบริษัทจีนในการดำเนินการและการบำรุงรักษาทางรถไฟจะมีจำนวนไม่มาก (*Huawei,* 2020) แต่ประเทศลาวก็จะถูกผูกติดอยู่กับเทคโนโลยีของจีนไปกว่าทศวรรษตามสัญญา



นอกจากนี้ อิทธิพลของจีนในลักษณะดังกล่าวอาจจำมาสู่การวางท่าทีกดดันรัฐที่ร่วมโครงการแถบและทาง หรือรัฐที่มีส่วนเกี่ยวข้องในยุทธศาสตร์เส้นทางสายไหมดิจิทัลซึ่งต้องพึ่งพาการลงทุนและเทคโนโลยีของจีนมากขึ้นเรื่อย ๆ ให้เข้าข้างจีนในประเด็นที่มีความสำคัญทางการทูต ประเด็นสำคัญซึ่งจีนได้เสนอปทัสถานใหม่เกี่ยวกับการกำกับดูแลพื้นที่ทางไซเบอร์ระดับโลกและความมั่นคงด้านข้อมูล โดยท้ายที่สุดรัฐบาลจีนอาจผลักดันประเทศต่าง ๆ ที่พึ่งพาโครงการแถบและทางและเส้นทางสายไหมดิจิทัลให้เข้าร่วมปทัสถานใหม่ของจีนในการกำกับดูแลพื้นที่ทางไซเบอร์และความมั่นคงด้านข้อมูลในที่สุด

กล่าวโดยสรุป สิ่งที่เป็นกุญแจสำคัญในกลยุทธ์แบบวงจรคู่ขนาดของจีน คือ การสร้างมาตรฐาน ซึ่งประเทศจีนมุ่งเน้นและมีความพยายามกับการสร้างมาตรฐานให้เกิดเป็นพฤตินัย หรือ

ในทางปฏิบัติในเวทีระหว่างประเทศและในองค์การระหว่างประเทศมาโดยตลอด เพื่อโน้มน้าว (convincing) ให้ประเทศอื่น ๆ นำมาตรฐานเหล่านั้นไปปรับใช้

**โครงสร้างพื้นฐานและแพลตฟอร์มดิจิทัลกับการพึ่งพาทางเศรษฐกิจของจีน**

ประเทศจีนใช้ประโยชน์จากการพัฒนาโครงสร้างพื้นฐานและแพลตฟอร์มดิจิทัลเพื่อสร้างมาตรฐานระดับโลกในทางปฏิบัติโดยเฉพาะระบบอีคอมเมิร์ซและระบบการชำระเงินออนไลน์ กล่าวคือ โครงสร้างพื้นฐานด้านโทรคมนาคมได้เชื่อมโยงผู้คนและตลาดของประเทศในโครงการแถบและทางเข้ากับบริษัทจีน ซึ่งบริษัทจีนเหล่านั้นเป็นเจ้าของแพลตฟอร์มอีคอมเมิร์ซและระบบการชำระเงินออนไลน์ ในขณะเดียวกันผู้ให้บริการด้านเครือข่ายมือถือช่วยให้สามารถเข้าถึงอินเทอร์เน็ตและสายเคเบิลใยแก้วนำแสงเชื่อมต่อข้อมูลที่กระจายอยู่ทั่วโลก

อย่างไรก็ดีอีคอมเมิร์ซและระบบการชำระเงินดิจิทัลเป็นระบบที่ค่อนข้างใหม่และมีกฎระเบียบน้อยกว่าธนาคารและสถาบันการเงินในแบบเดิมอื่น ๆ กฎระเบียบที่น้อยลง ส่งผลให้เกิดการนำเทคโนโลยีจีนไปใช้ง่ายขึ้นในโครงสร้างพื้นฐานด้านเทคโนโลยีทางการเงินของประเทศต่าง ๆ รวมถึงในเอเชียตะวันออกเฉียงใต้

ในขณะเดียวกัน การส่งออกโครงสร้างพื้นฐานและแพลตฟอร์ม ก่อให้เกิดการพึ่งพาทางเศรษฐกิจและเทคโนโลยีของจีนในภูมิภาคที่มากขึ้น ธุรกิจจีนกลายเป็นผู้เล่นหลักในอีคอมเมิร์ซและการชำระเงินออนไลน์ในเอเชียตะวันออกเฉียงใต้ ตัวอย่างในกรณีของ บริษัทอาลีบาบาได้รับประโยชน์จากการเป็น “ผู้ที่เคลื่อนไหวรายแรก (the first-mover)” ในการให้บริการ ส่งผลให้บริษัทอาลีบาบาได้รับความนิยมในลักษณะที่เป็น *ทางลัด* กล่าวคือ บริษัทอาลีบาบาเลือกใช้วิธีการเข้าซื้อกิจการ หรือการลงทุนในหุ้นของผู้ค้าปลีกออนไลน์รายใหญ่ของประเทศในเอเชียตะวันออกเฉียงใต้ แทนที่จะสร้างบริการของตนเองในท้องถิ่นตั้งแต่เริ่มต้น ส่งผลให้ผู้ให้บริการเครือข่ายโทรคมนาคมรายใหญ่ในแต่ละประเทศในภูมิภาคนำผลิตภัณฑ์ของจีนมาใช้เพื่อสร้างโครงสร้างพื้นฐานใหม่ เช่น โครงสร้างพื้นฐานการสื่อสารเคลื่อนที่ เป็นต้น

อาจกล่าวได้ว่า อีคอมเมิร์ซและการชำระเงินออนไลน์ คือ เครื่องมือสำคัญของจีนในการกำหนดพฤติกรรม หรือสร้างพื้นฐานของพฤติกรรมของประชาชนอย่างแนบเนียน ซึ่งทั้งสองสิ่งนี้จำเป็นต้องดำเนินการผ่านการเข้าถึงอินเทอร์เน็ตซึ่งกลายเป็นส่วนหนึ่งของชีวิตประจำวัน ทำให้ยากต่อการละทิ้ง ดังนั้น การให้บริการด้านอินเทอร์เน็ตจึงเป็นสิ่งจำเป็นสำหรับการเชื่อมต่อลูกค้า กับศูนย์ร่วมรวมข้อมูลและเพื่อรักษาการให้บริการที่มีคุณภาพในด้านความน่าเชื่อถือและประสบการณ์การใช้งานของลูกค้า ค่าธรรมเนียมสำหรับบริการเหล่านี้จึงเป็นสิ่งสำคัญในการจูงใจผู้คนให้ใช้บริการ ทั้งนี้ค่าการบริการโดยทั่วไปถูกคำนวณจากองค์ประกอบต่าง ๆ เช่น อุปกรณ์ สิ่งอำนวยความสะดวก การ

สื่อสารและค่าใช้จ่ายในการดำเนินการ ดังเช่นในกรณีของ Huawei บริษัทจีนซึ่งมีส่วนในโครงสร้างพื้นฐานการสื่อสารเคลื่อนที่ มักเสนออุปกรณ์เครือข่าย 5G ที่มีราคาถูกกว่าบริษัทคู่แข่งชาติอื่น ๆ ดังนั้น ประเทศต่าง ๆ อาจถูกชักจูงให้เข้าสู่แพลตฟอร์มและโครงสร้างพื้นฐานที่รองรับเส้นทางสายไหมดิจิทัลอย่างแนบเนียนและค่อยเป็นค่อยไป เนื่องจากผลประโยชน์ทางเศรษฐกิจของเศรษฐกิจแบบดิจิทัลอาจลดลงหากเปลี่ยนไปใช้อุปกรณ์อื่น ๆ อย่างไรก็ดี ถึงแม้ว่า Huawei จะเป็นหนึ่งในบริษัทชั้นนำที่เกี่ยวข้องซึ่งมีมูลค่าตลาดกว่า 1 แสนล้านเหรียญสหรัฐฯ (Daniel, 2023) ก็ตาม แต่บางประเทศเลือกที่จะไม่ใช้เทคโนโลยีของจีน เช่น ผู้ให้บริการโทรคมนาคมในเวียดนามตัดสินใจไม่ใช้อุปกรณ์ของ Huawei หรือในกรณีของผู้ให้บริการโทรคมนาคมในสิงคโปร์เลือกใช้ Ericssonและ Nokia แทน Huawei ในการสร้างโครงสร้างพื้นฐาน 5G ของประเทศ

ในขณะเดียวกัน สหรัฐฯ ได้กดดันชาติพันธมิตร เช่น อังกฤษ ออสเตรเลีย นิวซีแลนด์และญี่ปุ่น ไม่ให้ซื้อผลิตภัณฑ์ Huawei จากจีน แรงกดดันดังกล่าวส่งผลให้ญี่ปุ่นหยุดซื้ออุปกรณ์เครือข่ายจาก Huaweiและ ZTE ในหน่วยงานราชการและกองกำลังทหาร อีกด้านหนึ่ง ออสเตรเลียและนิวซีแลนด์ไม่อนุญาตให้ Huawei มีส่วนร่วมในการสร้างเครือข่าย 5G ของประเทศ แต่ในทางหนึ่งนั้นรัฐบาลอังกฤษแม้จะเป็นพันธมิตรของสหรัฐฯ ซึ่งเป็นหนึ่งในประเทศที่มีระบบการเฝ้าระวังเข้มงวดที่สุดในโลกและเป็นหนึ่งในสมาชิกของหน่วยข่าวกรองระดับโลกในชื่อ Five Eyes ซึ่งประกอบไปด้วยสหรัฐฯ แคนาดา ออสเตรเลีย นิวซีแลนด์และอังกฤษ ในปัจจุบันได้อนุญาตให้โครงการจาก Huawei ติดตั้งโครงสร้างพื้นฐาน 5G ภายในประเทศ นอกจากนี้กว่า 45 ประเทศตลอดเส้นทาง ได้อนุมัติโครงการให้ Huawei ดำเนินการติดตั้งเครือข่าย 5G ในประเทศของตน มีเพียง 4 ประเทศเท่านั้นที่ไม่อนุมัติการดำเนินการของ Huawei (Triolo, 2020)



อย่างไรก็ตาม รัฐบาลจีนได้ท้าทายชาติตะวันตกซึ่งปรากฏชัดจากแสดงออกถึงความพยายามที่จะครอบงำทางเทคโนโลยีภายใต้โลกเสรีอย่างชัดเจน หนึ่งในยุทธศาสตร์ที่เด่นชัดอย่างยิ่ง คือ การออกเครื่องหมายรับรองภาคบังคับของจีน China Compulsory Certificate (CCC) ในปี 2009 เป็นเครื่องหมายความปลอดภัยภาคบังคับสำหรับผลิตภัณฑ์จำนวนมากที่เข้ามาจำหน่าย หรือใช้ในตลาดและอุตสาหกรรมของจีน โดยเฉพาะอย่างยิ่งสินค้าทางด้านเทคโนโลยี ซึ่ง CCC ดังกล่าวกำหนดให้ต้องเปิดเผยพิมพ์เขียวและรหัสต้นทาง (source code) ของผลิตภัณฑ์ด้านเทคโนโลยีสารสนเทศเพื่อจำหน่ายในประเทศจีน อย่างไรก็ตามประเทศญี่ปุ่น สหรัฐฯ และสหภาพยุโรปแสดงท่าทีคัดค้านข้อกำหนดดังกล่าว เนื่องจากรายการเหล่านี้มีความลับทางการค้าที่เป็นแก่นของความได้เปรียบทางเทคโนโลยี ด้วยเหตุนี้ จีนจึงดำเนินการตามมาตรการควบคุมอื่น ๆ ซึ่งข้อกำหนดดังกล่าวมีผลเฉพาะกับการจัดซื้อจัดจ้างของรัฐบาลเท่านั้น (*Xinhuanet*, 2018)

นอกจากนี้ รัฐบาลจีนมีบทบาทในเชิงรุกอย่างมากในการส่งผู้แทน หรือผู้เข้าร่วมไปยังองค์การผู้กำหนดมาตรฐานสากลในปัจจุบันและร่วมเวลาการอภิปรายจำนวนมาก เช่น สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) และองค์กรกำหนดมาตรฐานที่สำคัญ คือ The 3rd Generation Partnership Project (3GPP) เป็นต้น โดยมีจุดมุ่งหมายเพื่อพัฒนาบุคลากรที่มีความเชี่ยวชาญและสร้างเครือข่ายในกระบวนการการกำหนดมาตรฐานและรวบรวมข้อมูลเกี่ยวกับเทคโนโลยีที่ทันสมัย การส่งผู้เข้าร่วมเหล่านี้เข้าสู่องค์การสำคัญดังกล่าวส่งเสริมให้ความสามารถของจีนในการพัฒนาผู้เชี่ยวชาญด้านมาตรฐานภายในประเทศสูงขึ้น ประเด็นสำคัญ เมื่อจีนได้ที่นั่งในตำแหน่งผู้นำองค์กรกำหนดมาตรฐานดังกล่าว เช่น ตำแหน่งคณะกรรมการใด ๆ ผู้แทนเหล่านั้นจะสามารถร่างมาตรฐานซึ่งเป็นข้อเสนอใหม่เสนอต่อคณะกรรมการได้ ผลที่พึงเกิดขึ้น คือ ผู้แทนจีนจะได้รับความคิดเห็นของผู้เข้าร่วมซึ่งเป็นตัวแทนชั้นนำและเป็นผู้เชี่ยวชาญด้านมาตรฐานสากลคนอื่น ๆ กลับมา สิ่งสำคัญ คือ ผู้แทนจีนอาจได้รับข้อมูลทางเทคนิคที่แนบมาพร้อมกับความเห็นเหล่านั้นด้วย ส่งผลให้รัฐบาลจีนได้รับข้อมูลทางเทคนิคที่สำคัญและความคิดเห็นสำหรับการปรับปรุงยุทธศาสตร์การกำหนดมาตรฐานสากลต่อไป

**ปทัสถานทางเทคโนโลยีและความมั่นคงไซเบอร์ของจีน**

ปทัสถานทางทางเทคโนโลยีและความมั่นคงไซเบอร์ของจีนที่พยายามเผยแพร่ให้ประชาคมทั้งอย่างชัดเจนและอย่างแยบยลผ่านกรอบการบูรณาการทางเทคโนโลยีโดยเฉพาะอย่างยิ่งเส้นทางสายไหมดิจิทัลซึ่ง สามารถแจกแจงได้ 3 ลักษณะ ได้แก่ การกำกับดูแลพื้นที่ไซเบอร์ในแบบของจีน อธิปไตยทางไซเบอร์ (cyber sovereignty) และการกำหนดมาตรฐานทางเทคโนโลยีจากการใช้ผลิตภัณฑ์และเทคโนโลยีจากจีน ซึ่งสามารถแจกแจงได้ดังนี้

ประการที่หนึ่ง การกำกับดูแลพื้นที่ไซเบอร์ในแบบของจีนมีสาระสำคัญอยู่ที่การควบคุมและบริหารจัดการระบบและพื้นที่ไซเบอร์โดยรัฐบาล องค์ประกอบที่สำคัญที่สุดคือ การกำหนดกฎเกณฑ์สำหรับรัฐบาลในการควบคุมข้อมูลและการเคลื่อนย้ายข้อมูลข้ามพรมแดนดังเช่นที่ปรากฏในเอกสารปกขาว (white paper) ของจีนเมื่อเดือนมีนาคม 2023 (The State Council Information Office, The People's Republic of China, 2023) ในชื่อ “China’s Law-Based Cyberspace Governance in the New Era” ซึ่งแสดงให้เส้นว่า ปทัสถานทางไซเบอร์ของจีนในเวลานี้ได้อยู่ในจุดของการกำหนดกฎเกณฑ์เพื่อให้สอดคล้องกับกฎหมายของจีน

ประการที่สอง อธิปไตยทางไซเบอร์ (cyber sovereignty) ภายในเอกสารปกขาวฉบับเดียวกันนั้นมีการกล่าวถึง การเคารพอธิปไตยทางไซเบอร์ของรัฐ โดยเฉพาะการกล่าวถึงความร่วมมือในการสร้างประชาคมพื้นที่ไซเบอร์ที่มีอนาคตร่วมกันและปรากฏในเอกสารปกขาวในปี 2022 เรื่อง “Jointly Build a Community with a Shared Future in Cyberspace” (The State Council

Information Office, The People's Republic of China, 2022) สาระสำคัญของเอกสารปกขาวทั้งสองฉบับที่กล่าวอ้างถึงกันนั้น ได้ให้ความสำคัญกับการเคารพอธิปไตยทางไซเบอร์ระหว่างรัฐ โดยเฉพาะมีการอ้างถึงกฎบัตรสหประชาชาติในมาตรา 2 (Charter of the United Nations, (n.d.), Article 1(1)-(5)) ซึ่งเอกสารปกขาวเน้นย้ำถึงหลักการความเสมอภาคของอธิปไตยที่บัญญัติไว้ในกฎบัตรสหประชาชาติเป็นบรรทัดฐานพื้นฐานที่ควบคุมความสัมพันธ์ระหว่างประเทศ โดยเฉพาะเรื่องความสัมพันธ์ที่เท่าเทียมกันระหว่างรัฐต่อรัฐและสิ่งนี้เองควรนำไปใช้กับพื้นที่ไซเบอร์ด้วยเช่นเดียวกัน (SCIO, The People's Republic of China, 2023)

ประการที่สาม การกำหนดมาตรฐานทางเทคโนโลยีจากการใช้ผลิตภัณฑ์และเทคโนโลยีจากจีน ดังเช่นที่ได้กล่าวไว้ในบทที่ 2 เรื่องยุทธศาสตร์ “China Standard 2035” ซึ่งแสดงให้เห็นถึงความพยายามในการเปลี่ยนผ่านตำแหน่งแห่งที่ของรัฐบาลจีน โดยเฉพาะอย่างยิ่งในฐานะเป็นผู้กำหนดมาตรฐานทางเทคโนโลยี เพื่อสร้างความเชื่อมโยงทางห่วงโซ่อุปทานและการพึ่งพาทางเทคโนโลยีจีนอย่างแยบยล (Sheehan, Blumenthal, & Nelson, 2021)

**ความท้าทายทางไซเบอร์ที่เกิดจากปทัสถานการกำกับดูแลพื้นที่ไซเบอร์ของจีน**

การกำกับดูแลพื้นที่ทางไซเบอร์ของจีนกำลังท้าทายทั้งภายในประเทศและระเบียบระหว่างประเทศ ผู้เขียนแจกแจงประเด็นซึ่งสร้างความท้าทายสังคมระหว่างประเทศได้ 3 ประเด็น ได้แก่ ประการที่หนึ่ง ความท้าทายต่อสภาพแวดล้อมระหว่างประเทศ (international environment) ประการที่สอง ขนาดของประชากรอินเทอร์เน็ตที่เพิ่มขึ้น (netizens) และ ประการที่สาม สภาวะความไร้บรรทัดฐานทางไซเบอร์ (cyber anomie) ซึ่งแจกแจงไว้ดังนี้



ประการที่หนึ่ง การกำกับดูแลพื้นที่ทางไซเบอร์ของจีนสร้างความท้าทายต่อสภาพแวดล้อมระหว่างประเทศ กล่าวคือ ปทัสถานทางไซเบอร์และเครือข่ายการกำกับดูแลพื้นที่ทางไซเบอร์ส่งผลต่ออำนาจอธิปไตยกับประเทศที่เกี่ยวข้องกับยุทธศาสตร์ของจีน โดยเฉพาะอย่างยิ่งยุทธศาสตร์การพัฒนาโครงสร้างพื้นฐานซึ่งสร้างเชื่อมโยงระหว่างประเทศกับจีนในลักษณะที่ผูกติด ความท้าทายดังกล่าวสอดรับกันอย่างมีนัยสำคัญต่อการเติบโตของผู้ใช้อินเทอร์เน็ตโดยเฉพาะอย่างยิ่งในประเทศกำลังพัฒนาและประเทศโลกใต้ (global south) อนึ่ง ผลการศึกษาชี้ให้เห็นว่า ระหว่างปี 2000–2009 อัตราการเติบโตของผู้ใช้อินเทอร์เน็ตอันดับต้น ๆ ไม่ปรากฏในประเทศที่พัฒนาแล้วแต่ปรากฏในแอฟริกา ลาตินอเมริกาและภูมิภาคอื่น ๆ (Li, 2019) แสดงให้เห็นว่าอัตราของตัวแสดงในพื้นที่ทางไซเบอร์มีจำนวนเพิ่มมากในกลุ่มประเทศดังกล่าวอย่างเห็นได้ชัด ซึ่งประเทศเหล่านั้นจำนวนมากต่างเป็นส่วนหนึ่งและ/หรือมีส่วนได้ส่วนเสียกับยุทธศาสตร์เส้นทางสายไหมดิจิทัล (Digital Silk Road)

การเพิ่มขึ้นของตัวแสดงในพื้นที่ทางไซเบอร์กลายเป็นหน่วย (unit) ที่สำคัญซึ่งสร้างความเชื่อมโยงทางเศรษฐกิจ ความมั่นคง วัฒนธรรมและอำนาจส่วนบุคคลของตัวแสดงของจีนให้สูงมากยิ่งขึ้นอย่างมีนัยสำคัญ ส่งผลให้อิทธิพลของจีนแผ่ขยายสู่ภายในประเทศอย่างแนบเนียนผ่านผู้ใช้งานอินเทอร์เน็ตซึ่งเป็นหน่วยที่สำคัญของยุทธศาสตร์ นอกจากนี้ในด้านจิตวิทยา การที่ผู้ใช้งานอินเทอร์เน็ตในประเทศดังกล่าวถูกแวดล้อมด้วยเครือข่ายและเครื่องมือต่าง ๆ ของจีน เช่น ผู้ให้บริการ ผู้ผลิตและผู้จำหน่ายสินค้าทางไซเบอร์จากจีนเป็นสินค้าครองตลาดในประเทศแอปพลิเคชันในชีวิตประจำวันจากจีน เป็นต้น เครื่องมือเหล่านี้สร้างบรรยากาศแวดล้อมให้กับประชากรภายในประเทศต้นทางให้เกิดความคุ้นชิน โดยเฉพาะอย่างยิ่งสร้างความยึดโยงในชีวิตประจำวัน

ดังนั้น ความต้องการการพัฒนาทางเทคโนโลยี โดยเฉพาะอย่างยิ่งโครงสร้างพื้นฐานทางเทคโนโลยีในประเทศกำลังพัฒนาและประเทศโลกใต้จึงกลายเป็นบริบทและหมุดหมายสำคัญของยุทธศาสตร์จีน ในขณะเดียวกันการเพิ่มขึ้นของผู้ใช้งานอินเทอร์เน็ตกลายเป็นอีกตัวแปรหนึ่งที่สำคัญในยุทธศาสตร์ทางไซเบอร์ของจีนในฐานะหน่วย (unit) ที่เชื่อมโยงประเด็นสำคัญของจีนในมิติอื่นในทางหนึ่งนั้นสะท้อนความพยายามของจีนในการกำหนดมาตรฐาน (standard setting) ผ่านพฤติกรรมของผู้ใช้งานอินเทอร์เน็ต ขณะเดียวกันบทบาทของตัวแสดงข้างต้นและยุทธศาสตร์ของจีนได้สร้างความเชื่อมโยงในระดับโครงสร้าง ซึ่งส่งผลให้อิทธิพลและอำนาจของจีนสูงขึ้นอย่างมีนัยสำคัญจึงเกิดเป็นคำถามและเป็นที่ถกเถียงถึงอำนาจอธิปไตยของประเทศเหล่านั้น

<u>ประการที่สอง</u> การเพิ่มขึ้นของขนาดประชากรอินเทอร์เน็ต (netizen) กลายเป็นประเด็นท้าทายทั้งภายในและระหว่างประเทศ กล่าวคือ การเพิ่มขึ้นของประชากรอินเทอร์เน็ตนั้นสอดคล้องกับการพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ ยุทธศาสตร์การพัฒนาโครงสร้างพื้นฐานของจีนโดยเฉพาะอย่างยิ่งข้อริเริ่มแถบและทางนำมาซึ่ง การบูรณาการทางเทคโนโลยีภายใต้กรอบเส้นทางสายไหมดิจิทัล ดังนั้น ขนาดของประชากรอินเทอร์เน็ตและจำนวนผู้เข้าถึงอินเทอร์เน็ตในประเทศที่เกี่ยวข้องกับยุทธศาสตร์ดังกล่าวของจีนจะมีจำนวนเพิ่มขึ้น โดยเฉพาะอย่างยิ่งประเทศกำลังพัฒนาและประเทศโลกใต้ ชัดเจนที่สุดในแอฟริกาและเอเชียซึ่งเป็นเส้นทางสำคัญภายใต้ยุทธศาสตร์แถบและทาง อนึ่ง ตัวเลขของประชากรอินเทอร์เน็ตนั้นไม่ใช่ตัวเลขเดียวกับจำนวนผู้เข้าถึงอินเทอร์เน็ต โดยอัตราการเข้าถึงอินเทอร์เน็ตของประชากรโดยทั่วไปจะน้อยกว่าขนาดของประชากรอินเทอร์เน็ตเนื่องจากปัจจัยโครงสร้างพื้นฐานภายในประเทศที่ไม่เพียงพอและพลวัตพฤติกรรมของผู้ใช้ ปัจจัยดังกล่าวจึงสะท้อนในทางหนึ่งว่า ช่องว่างระหว่างขนาดของประชากรอินเทอร์เน็ตกับจำนวนผู้เข้าถึงอินเทอร์เน็ตในประเทศพัฒนาแล้วจะมีขนาดเล็กกว่าเนื่องจากมีการพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ที่เพียงพอหรือมากกว่าเมื่อเทียบกับประเทศกำลังพัฒนา หรือประเทศโลกใต้

อย่างไรก็ตามการเพิ่มขึ้นของประชากรอินเทอร์เน็ตส่งผลต่อการกระจายของผู้ใช้เครือข่ายในแง่ของอายุ อาชีพและเพศ ซึ่งมีลักษณะแตกต่างกัน รวมถึงวิธีการเข้าถึงเครือข่ายที่มีความหลากหลายมากขึ้น ผู้ใช้อินเทอร์เน็ตจำนวนมากและโครงสร้างที่หลากหลายก่อให้เกิดข้อมูลที่มากขึ้นส่งผลต่อการกำกับดูแลพื้นที่ทางไซเบอร์ของประเทศ โดยเฉพาะอย่างยิ่งในประเทศโลกใต้ซึ่งอาจเผชิญกับปัญหาในการวางบรรทัดฐาน กฎหมาย ข้อบังคับในการควบคุมปัญหาที่อาจเกิดขึ้นจากการเติบโตของพื้นที่ทางไซเบอร์อย่างรวดเร็ว หรืออาจจะกล่าวได้ว่า เป็นการพัฒนาอย่างไม่เป็นพลวัต ส่งผลให้เกิดเป็นความท้าทายทั้งภายในและระหว่างประเทศในประเด็นต่อไป

ประการที่สาม สภาวะความไร้บรรทัดฐานทางไซเบอร์ (cyber anomie) ก่อให้เกิดปัญหาทางไซเบอร์ เช่น การฉ้อโกงทางไซเบอร์ (scammer) การโจมตีทางไซเบอร์ (cyberattack) การรั่วไหลของข้อมูลทางไซเบอร์ (cyber data leakage) ปัญหาการละเมิดความเป็นส่วนตัวทางไซเบอร์ (privacy) เป็นต้น ดังนั้น การกำหนดบรรทัดฐาน กฎหมายและข้อบังคับเพื่อจำกัดและควบคุมดูแลพื้นที่ทางไซเบอร์จึงเป็นสิ่งสำคัญอย่างยิ่ง อย่างไรก็ตาม คำถามสำคัญ คือ อะไรเป็นปัจจัยเอื้อให้เกิดสภาวะดังกล่าว ปทัสถานทางไซเบอร์ภายใต้การนำของจีนและรูปแบบการจัดการพื้นที่ทางไซเบอร์ของจีนมีส่วนเกี่ยวข้องกับการเกิดขึ้นของสภาวะดังกล่าวมากน้อยเพียงใด

ผู้เขียนพิจารณาและเชื่อว่าสภาวะดังกล่าวเป็นสภาวะที่เกิดโดยทั่วไปไม่จำกัดเฉพาะเพียงภายใต้ปทัสถานทางไซเบอร์ของจีนเพียงอย่างเดียว แต่รวมถึงปทัสถานเดิมภายใต้การนำของตะวันตกเช่นเดียวกัน อย่างไรก็ดี ปทัสถานทางไซเบอร์ของจีนมีปัจจัยเอื้อแตกต่างกันออกไป ซึ่งผู้เขียนได้แจกแจงประเด็นไว้ดังนี้

ปทัสถานใหม่ทางไซเบอร์ของจีนถูกมองในแง่ลบในฐานะเป็นผู้ท้าทายปทัสถานเดิม กล่าวคือ การออกกฎหมาย หรือข้อบังคับเพื่อควบคุมพื้นที่ทางไซเบอร์อาจทำได้ยาก เนื่องจากปทัสถานของจีนถูกมองว่าเป็นแนวคิดใหม่ที่ยังขาดความน่าเชื่อถือในเรื่องวิธีการและความโปร่งใส ประกอบกับภาพลักษณ์ในทางลบภายใต้ระเบียบระหว่างประเทศที่องค์การต่าง ๆ ที่รับผิดชอบด้านไซเบอร์ขับเคลื่อนด้วยแนวคิดของโลกเสรี การกำกับดูแลทางไซเบอร์ในลักษณะการควบคุมโดยรัฐบาลในแบบข้อเสนอของจีนจึงมีความขัดแย้งกับกรอบปทัสถานระหว่างประเทศอยู่ในเวลาเดียวกัน

อุปกรณ์การเข้าถึงอินเทอร์เน็ตของจีนมีราคาถูกอย่างมากซึ่งเป็นจุดเด่นสำคัญ โดยเฉพาะอย่างยิ่งอุปกรณ์ในลักษณะ *all-in-one*และ *ready-to-use* อย่างสมาร์ตโฟน มักถูกใช้เป็นเครื่องมือในการก่อความผิดปกติทางไซเบอร์ เช่น การฉ้อโกง การโจมตีทางไซเบอร์ การเผยแพร่ข้อมูลและการคุกคาม เป็นต้น กล่าวคือ โทรศัพท์มือถือเป็นเครื่องมือสำคัญและเข้าถึงง่ายที่สุดสำหรับการเข้าถึงพื้นที่ทางไซเบอร์ในราคาเริ่มต้นเพียงหลักร้อยบาท สิ่งที่เกิดขึ้น คือ โทรศัพท์มือถือเมื่อถูกใช้ก่อเหตุเพื่อเป็นการกำจัดและลดร่องรอยดิจิทัล (digital footprint) จึงจำเป็นต้องทำลาย หรือแม้แต่การมี

โทรศัพท์มือถือจำนวนมากในชีวิตประจำวันก็เป็นความพยายามในการลดร่องรอยดิจิทัลเช่นเดียวกัน ดังนั้น ค่าใช้จ่ายจากกระบวนการดังกล่าวจึงเป็นสิ่งที่ต้องพิจารณา อาจกล่าวได้ว่าการเข้าถึงอินเทอร์เน็ตสามารถเข้าถึงได้ง่ายในราคาเพียงหลักร้อยบาท ประเด็นนี้ย่อมส่งผลให้เกิดความเสี่ยงต่อปัญหาทางไซเบอร์ข้างต้นทั้งสิ้น

การพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ของประเทศอย่างไม่เป็นพลวัตส่งผลให้เกิดปัญหาทางไซเบอร์ กล่าวคือ ในบางประเทศโดยเฉพาะประเทศโลกใต้ยังขาดความพร้อม การศึกษาและการตระหนักถึงผลกระทบของการพัฒนาทางเทคโนโลยียุคปัจจุบัน เนื่องจากช่องว่างระหว่างการพัฒนามีมาก การข้าม หรือลัดพลวัตของการพัฒนาภายในประเทศอาจนำไปสู่ความไม่เข้าใจ หรือการขาดการเตรียมความพร้อมอย่างรอบคอบของประเทศเหล่านั้น ดังนั้น การศึกษา การกำหนดแนวกฎหมายหรือข้อบังคับอย่างรอบคอบไว้ก่อนการรับเทคโนโลยีเข้ามาเป็นส่วนหนึ่งของประเทศจึงเป็นสิ่งสำคัญอย่างยิ่งในการลดความเสี่ยงปัญหาการควบคุมทางไซเบอร์

**ความท้าทายปทัสถานทางไซเบอร์ของจีนในระดับสากล**

รัฐบาลจีนแสดงออกอย่างแข็งขันถึงความต้องการในการกำหนดมาตรฐานทางเทคโนโลยี ความทะเยอทะยานหนึ่งที่ชัดเจนที่สุดของจีนในการสร้างมาตรฐาน คือ การสร้างมาตรฐาน 5G ซึ่งเริ่มต้นในปี 2013 กระทรวงอุตสาหกรรมและเทคโนโลยีสารสนเทศ (Ministry of Industry and Information Technology: MIIT) ร่วมกับคณะกรรมการปฏิรูปและการพัฒนาแห่งชาติจีน (National Development and Reform Commission: NDRC) และกระทรวงวิทยาศาสตร์และเทคโนโลยี (Ministry of Science and Technology: MOST) ร่วมกันก่อตั้งกลุ่มส่งเสริม 5G นอกจากรัฐบาล ผู้ประกอบการด้านโทรคมนาคมและผู้ขายต่างร่วมมือกันก็มีส่วนสำคัญในส่งเสริมมาตรฐาน 5G ของจีนให้เกิดเป็นมาตรฐานสากล ขณะเดียวกันรัฐบาลจีนได้มุ่งดำเนินยุทธศาสตร์ของจีนเพื่อให้บรรลุตามเป้าหมายยุทธศาสตร์จีนปี 2035 โดยเฉพาะอย่างยิ่งแผนปฏิบัติภายใต้ยุทธศาสตร์ข้อริเริ่มแถบและทาง จะทำให้เกิดความเชื่อมโยงกับประเทศที่เกี่ยวข้องกับโครงการซึ่งจะอำนวยและส่งเสริมการสร้างมาตรฐานของจีน สะท้อนให้เห็นว่ารัฐบาลจีนได้เริ่มขั้นตอนที่สามของกลยุทธ์แบบวงจรคู่ขนานของจีนซึ่งได้กล่าวไว้ในตอนต้น คือ การใช้อิทธิพลเหนือกลุ่มประเทศภายใต้ยุทธศาสตร์แถบและทาง

ตัวอย่างเช่น รัฐบาลจีนได้ดำเนินการผลักดันแนวคิดอธิปไตยในพื้นที่ทางไซเบอร์โดยใช้ประสบการณ์จากการเซนเซอร์อินเทอร์เน็ต (internet censorship) และกฎระเบียบภายในประเทศ รัฐบาลจีนได้ออกแบบเครื่องมือเพื่อใช้กรอง (filter) ในอินเทอร์เน็ตในปี 2002 ต่อมาถูกพัฒนาเป็น “Great Firewall” ซึ่งในปี 2016 กฎหมายความมั่นคงทางไซเบอร์ของจีนได้กำหนดหลักการของ

อำนาจอธิปไตยในพื้นที่ไซเบอร์ การปกป้องข้อมูล การเซนเซอร์เนื้อหาที่ผิดกฎหมายและการแทรกแซงของรัฐบาลเพื่อความปลอดภัยของสาธารณะ (Zittrain & Edelman, 2003) รัฐบาลจีนเชื่อว่าแนวคิดการกำกับดูแลพื้นที่ทางไซเบอร์มีศักยภาพที่จะขยายอิทธิพลของจีนได้ นอกจากนี้ ร่างกฎหมายว่าด้วยการรักษาความปลอดภัยของข้อมูลยังมีบทบัญญัติเกี่ยวกับกิจกรรมนอกอาณาเขต ซึ่งได้กำหนดความผิดของกิจกรรมที่เกี่ยวกับการประมวลผลข้อมูลภายนอกประเทศจีนหากกิจกรรมดังกล่าวมีความเกี่ยวข้องกับความมั่นคงของชาติ ผลประโยชน์สาธารณะ หรือสิทธิและผลประโยชน์ที่ชอบด้วยกฎหมายของพลเมืองของจีน (National People's Congress of the People's Republic of China, 2016) ส่งผลให้รัฐบาลจีนอาจสามารถควบคุมบริษัทข้ามชาติที่ดำเนินการในประเทศจีนได้และครอบครองข้อมูลจากศูนย์ข้อมูลในต่างประเทศโดยการบังคับใช้กฎหมายดังกล่าว

ขณะที่รัฐบาลจีนใช้ระบบการกำกับดูแลพื้นที่ทางไซเบอร์ภายในประเทศ เวลาเดียวกันนั้นก็ยังพยายามเผยแพร่แนวคิดดังกล่าวในการควบคุมพื้นที่ทางไซเบอร์สู่เวทีโลก ในปี 2015 รัฐบาลจีนเป็นเจ้าภาพการประชุมอินเทอร์เน็ตโลกครั้งที่ 2 (Second World Internet Conference: WIC) ได้เสนอให้มีการสร้างชุมชนที่มีอนาคตร่วมกันในโลกไซเบอร์ขึ้นที่งานประชุม ข้อเสนอดังกล่าวเรียกร้องให้เกิดการเข้าร่วมกับชุมชนและสนับสนุนแนวคิดการกำกับดูแลพื้นที่ทางไซเบอร์ของจีน (Chinese Ministry of Foreign Affairs, 2015) การประชุมมีจุดมุ่งหมายเพื่อสร้างเครือข่ายระดับโลกและศึกษาติดตามประเทศอื่น ๆ ว่า มีแนวคิด หรือมีการกำหนดบรรทัดฐานระดับโลกอย่างไร

ในงานประชุมอินเทอร์เน็ตโลกครั้งที่ 6 ปี 2019 สถาบันความสัมพันธ์ระหว่างประเทศร่วมสมัยของจีน (China Institutes of Contemporary International Relations: CICIR) องค์กรซึ่งเป็นคลังความคิด (think tank) ร่วมกับกระทรวงความมั่นคงแห่งชาติ (Ministry of State Security) สถาบันสังคมศาสตร์เซี่ยงไฮ้ (Shanghai Academy of Social Sciences) และมหาวิทยาลัยหวู่ฮั่น (Wuhan University) ได้เผยแพร่เอกสารสำคัญชื่อ "Network Sovereignty: Theory and Practice" ซึ่งนำเสนอแนวคิดเกี่ยวกับอำนาจอธิปไตยในพื้นที่ทางไซเบอร์ นอกจากนี้ในปี 2020 ได้มีการปรับปรุงแนวคิดโดยรวมสถาบันต่าง ๆ เช่น หน่วยงานกำกับดูแลบริหารพื้นที่ทางไซเบอร์ของจีน (Cyberspace Administration of China: CAC) และมหาวิทยาลัยอื่น ๆ เป็นต้น

ผู้เขียนเชื่อว่า รัฐบาลจีนตั้งเป้าที่จะทำให้ระบบการกำกับดูแลพื้นที่ทางไซเบอร์ของตนเป็นมาตรฐานอย่างน้อยที่สุดเชิงพฤตินัยในระดับภูมิภาคที่ซึ่งจีนมีอิทธิพลสูง อนึ่ง หน่วยงานกำกับดูแลบริหารพื้นที่ทางไซเบอร์ของจีนเชื่อว่า กฎหมายความมั่นคงทางไซเบอร์เป็นแนวทางการแก้ไขปัญหาและทางออกสำหรับการควบคุม ดูแลพื้นที่ทางไซเบอร์ในระดับโลก (Cyberspace Administration of China, 2020) หากประเทศต่าง ๆ นำระบบการบริหารจัดการของตนมาใช้ก็จะสามารถออกแบบ

แนวทางการดำเนินการร่วมกันเพื่อกำหนดรูปแบบและพูดคุยกันเกี่ยวกับพฤติกรรมของรัฐในพื้นที่ทางไซเบอร์ได้

นอกจากนี้ จีนกำลังเตรียมความพร้อมในการเปลี่ยนผ่านและเข้าร่วมการอภิปรายอย่างต่อเนื่องเกี่ยวกับการกำหนดกฎเกณฑ์ (rule-making) สำหรับพื้นที่ทางไซเบอร์ กระแสการถกเถียงกันเกี่ยวกับพื้นที่ทางไซเบอร์ในประเด็นเรื่องความเป็นส่วนตัว (privacy) กำลังถูกพูดถึงอย่างกว้างขวางในชุมชนทั่วโลก การปกป้องข้อมูล ทรัพย์สินทางปัญญา ตัวอย่างเช่น ในการประชุม G20 (Group of Twenty) ประจำปี 2019 ญี่ปุ่นมีเป้าหมายที่จะเป็นผู้นำในการกำหนดกฎเกณฑ์ทางเศรษฐกิจแบบดิจิทัล (digital economy) และแนวคิดอินโด-แปซิฟิกที่เสรีและเปิดกว้าง (Free and Open Indo-Pacific: FOIP) รวมถึงยุทธศาสตร์การจัดการด้านข้อมูลในชื่อ “Osaka Track” และ “Data Free Flow with Trust (DFFT)” ซึ่งเป็นแนวคิดที่ถูกเสนอโดยญี่ปุ่นเพื่อการดูแลจัดการและขนส่งข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคลข้ามพรมแดนไปมาอย่างอิสระ (Japanese Ministry of Foreign Affairs, 2019) เป็นต้น

แม้ว่ารัฐบาลจีนจะไม่มีท่าทีตอบโต้ข้อเสนอแนะของญี่ปุ่นในทันที แต่ได้มีการจัดทำข้อเสนอเกี่ยวกับการกำหนดกฎเกณฑ์สำหรับการกำกับดูแลพื้นที่ทางไซเบอร์ขึ้นในภายหลัง โดยกระทรวงการต่างประเทศจีน (Ministry of Foreign Affairs) ได้เผยแพร่แนวคิดเกี่ยวกับการจัดการความมั่นคงของข้อมูลในแบบของตนในชื่อแผน “Global Initiative on Data Security (GIDS)” ในเดือนกันยายน 2020 (Chinese Ministry of Foreign Affairs, 2020) เพื่อเรียกร้องนานาชาติให้ใช้แนวทางเพื่อสร้างความสมดุลต่อความก้าวหน้าทางเทคโนโลยี การพัฒนาเศรษฐกิจและการปกป้องความมั่นคงแห่งชาติและผลประโยชน์สาธารณะ อย่างไรก็ตาม GIDS ปฏิบัติตามและยึดหลักการของจีนในการกำกับดูแลข้อมูลและอธิปไตย ซึ่งแตกต่างจากกรอบแนวคิดของ FOIPและ DFFT



รัฐบาลจีนได้ผลักดันอย่างจริงจังให้ประเทศอื่น ๆ สนับสนุนแนวคิด GIDS เพื่อที่จะได้ตำแหน่งนำในเวทีพูดคุยที่เกี่ยวกับเรื่องการกำกับดูแลข้อมูล รัฐมนตรีต่างประเทศของจีนได้นำเสนอ (advocate) ข้อริเริ่มดังกล่าวต่อเวทีการประชุมทวิภาคีตลอดมานับตั้งแต่มีการเผยแพร่ ซึ่งเมียนมาร์และกัมพูชาให้การตอบรับและสนับสนุนข้อริเริ่มดังกล่าวของจีน (Chinese Ministry of Foreign Affairs, 2022) อย่างไรก็ตาม ประเทศอื่น ๆ เช่น ฟิลิปปินส์และปากีสถาน ที่ซึ่งจีนได้ลงทุนภายใต้ยุทธศาสตร์แถบและทางและยุทธศาสตร์เส้นทางสายไหมสายดิจิทัล ทั้งสองประเทศมีท่าทียินดีกับหลักการดังกล่าวแต่ไม่สนับสนุนข้อเสนอนี้ (*Xinhuanet,* 2020b) ดังนั้น สิ่งเหล่านี้จึงเป็นสัญญาณที่สะท้อนให้เห็นว่า ความพยายามของจีนในการขึ้นเป็นผู้นำการดำเนินการกำกับดูแลพื้นที่ทางไซเบอร์อาจยังไม่สำเร็จอย่างเต็มที่ จีนต้องใช้เวลามากขึ้นเพื่อใช้อิทธิพลเหนือกลุ่มประเทศผู้เกี่ยวข้องกับ

ยุทธศาสตร์แถบและทางให้แสดงออกไปในทิศทางเดียวกันกับจีน จากที่กล่าวมานั้นชี้ให้เห็นว่า รัฐบาลจีนกำลังเข้าสู่แผนระยะที่สามของกลยุทธ์แบบวงจรคู่ขนานอย่างเต็มรูปแบบ

**ความท้าทายปทัสถานทางไซเบอร์ของจีนในระดับภูมิภาค**

จีนกำลังได้รับความสนใจทางด้านเทคโนโลยีในเอเชียตะวันออกเฉียงใต้ โดยให้ความสำคัญต่อภูมิรัฐศาสตร์และศักยภาพการเติบโตทางเศรษฐกิจ ประเด็นเหล่านี้ผลักดันให้จีนเข้ามามีส่วนร่วมในภูมิภาคนี้มากขึ้นโดยเป็นหนึ่งในหมุดหมายแรกของยุทธศาสตร์แถบและทางและเส้นทางสายไหมสายดิจิทัล

เอเชียตะวันออกเฉียงใต้เป็นภูมิภาคที่สำคัญในแผนการพัฒนาโครงสร้างพื้นฐานดิจิทัลของจีน เนื่องจากเป็นจุดยุทธศาสตร์ทางภูมิรัฐศาสตร์ที่สำคัญสำหรับจีนในการเชื่อมโยงกับภูมิภาคอื่น กล่าวคือ เส้นทางสายไหมดิจิทัลได้เชื่อมโยงประเทศในยุทธศาสตร์แถบและทางผ่านการแนวสายเคเบิลใยแก้ว (fiber-optic) ทั้งภาคพื้นดินและใต้น้ำ ซึ่งรัฐบาลจีนได้เน้นย้ำการสร้างสายเคเบิลเหล่านี้ไปยังเอเชียใต้ เอเชียตะวันออกเฉียงใต้ แปซิฟิกและจะเชื่อมต่อไปยังแอฟริกา โครงสร้างพื้นฐานด้านโทรคมนาคมการสื่อสารที่จีนสร้างขึ้นในเอเชียตะวันออกเฉียงใต้มีเป้าหมายที่จะขยายแนวเคเบิลใต้น้ำที่เชื่อมต่อภูมิภาคกับแนวชายฝั่งของจีน เพื่อเชื่อมต่อกับสายเคเบิลในพื้นที่ฝั่งตะวันตกของประเทศจีน อนึ่ง บริษัท China Unicorn เป็นบริษัทด้านโทรคมนาคมการสื่อสารของจีนได้สร้าง โครงการเดินสายเคเบิลใต้น้ำ ซึ่งปัจจุบันเป็นแนวเส้นทางเคเบิลที่สั้นที่สุดระหว่างเอเชียกับยุโรป แนวเคเบิลดังกล่าว เอเชีย-แอฟริกา-ยุโรป 1 (Asia-Africa-Europe 1: AAE-1) คือ แนวเคเบิลใต้น้ำใหม่ระยะทาง 25,000 กิโลเมตร ซึ่งจะติดตั้งจากฮ่องกงไปยังฝรั่งเศสและยังเชื่อมต่อจีนกับเอเชียตะวันออกเฉียงใต้ เอเชียใต้ บางส่วนของแอฟริกา ตะวันออกกลางและยุโรป ตลอดแนวเคเบิลอีกด้วย (AAE-1, 2022)



ยิ่งกว่านั้น จากการที่รัฐบาลจีนกำลังสร้างสายเคเบิลภาคพื้นดินและใต้น้ำเพื่อขยายการเชื่อมโยงใยแก้วนำแสงระหว่างจีนกับส่วนต่าง ๆ ของยูเรเซีย เห็นได้ชัดว่าในบางกรณีรัฐบาลจีนกำลังสร้างเส้นทางเชื่อมต่อที่ซ้ำแนวเดิม ส่งผลให้เครือข่ายของจีนไปยังประเทศอื่นมีความยืดหยุ่น เพราะการเชื่อมต่อที่ซ้ำซ้อนเหล่านี้ทำเกิดทางเลือกอื่นแก่ผู้ให้บริการด้านโทรคมนาคมในจีนเมื่อสายเคเบิลมีปัญหาในการสื่อสาร

อย่างไรก็ดี เอเชียตะวันออกเฉียงใต้ไม่เพียงมีความสำคัญทางภูมิศาสตร์สำหรับจีนเท่านั้น แต่ยังมีอัตราการเติบโตทางเศรษฐกิจสูงและเป็นตลาดที่มีศักยภาพที่สำคัญต่อบริษัทจีนในด้านเทคโนโลยีสารสนเทศและบริการด้านดิจิทัล อนึ่ง ในแง่ของศักยภาพทางเศรษฐกิจ การค้าและบริการที่เปิดใช้งานแบบดิจิทัลในตลาดเอเชียตะวันออกเฉียงใต้เพิ่มขึ้นกว่าเท่าตัวในระหว่างปี 2011-2019 (United Nations Conference on Trade and Development, 2022) เช่น แอปพลิเคชันในการสื่อสารของ

จีน แพลตฟอร์มอีคอมเมิร์ซและบริษัทชำระเงิน เป็นต้น ทั้งหมดต่างขยายตัวอย่างรวดเร็วในเอเชียตะวันออกเฉียงใต้ บริษัทผู้ลงทุนชาวจีน อาทิ Alibabaและ JD.com ต่างเป็นผู้ลงทุนรายใหญ่ในบริษัทในเอเชียตะวันออกเฉียงใต้โดยเฉพาะอย่างยิ่งบริษัทแพลตฟอร์มอีคอมเมิร์ซ เช่น Lazadaและ Grab-hailing เป็นต้น

แม้จะมีการลงทุนจำนวนมากเกิดขึ้นในเอเชียตะวันออกเฉียงใต้ แต่โครงสร้างพื้นฐานดิจิทัลของภูมิภาคนี้ยังคงค่อนข้างด้อยพัฒนา โดยเฉพาะอย่างยิ่งในประเทศที่รายได้ต่ำ เช่น กัมพูชา ลาว และเมียนมาร์ จึงเป็นปกติที่รัฐบาลในภูมิภาคจะให้ความสำคัญกับการพัฒนาและมีความสนใจในโครงสร้างพื้นฐานที่มีต้นทุนต่ำและได้มาตรฐานของจีน รัฐในเอเชียตะวันออกเฉียงใต้หลายแห่งไม่มีกฎหมายและนโยบายความเป็นส่วนตัว (privacy) ความมั่นคงทางไซเบอร์ หรือการคุ้มครองข้อมูลที่ครอบคลุม ดังนั้น รัฐเหล่านั้นจึงอาจไม่กังวลอย่างที่สุดว่าการลงทุนของจีนอาจส่งผลต่อความเป็นส่วนตัวและความมั่นคงทานด้านข้อมูลในพื้นที่ ซึ่งอาจนำไปสู่สภาวะการไร้บรรทัดฐานทางไซเบอร์ (cyber anomie) ดังที่กล่าวไว้ได้

นอกจากนี้ในมิติทางเศรษฐกิจและการเงิน จีนมีความพยายามในการแสดงตนทางเทคโนโลยีในภาคการเงินของภูมิ โดยยุทธศาสตร์เส้นทางสายไหมสายดิจิทัลจะทำให้ประเทศต่าง ๆ มีการเชื่อมต่ออินเทอร์เน็ตและการขนส่งที่เป็นรากฐานของการชำระเงินดิจิทัลและบริการทางด้านการเงินอื่น ๆ อุตสาหกรรมบริการทางการเงินเป็นอุตสาหกรรมที่ต้องการเครือข่ายการประมวลผลที่มีประสิทธิภาพสูง เชื่อถือได้และรวดเร็ว ขณะเดียวกันอุตสาหกรรมของจีนได้ลงทุนในเทคโนโลยีในด้านดังกล่าวเช่นกัน โดยหวังจะเป็นผู้นำด้าน Fintech

ตัวอย่างกรณีบริษัท Ant Group หนึ่งในบริษัทอีคอมเมิร์ซสัญชาติจีนในเครือของ Alibaba Group Holding ประสบความสำเร็จภายในประเทศจีนมากขึ้นและยังขยายระบบการชำระเงินผ่านมือถือในประเทศแถบเอเชียตะวันออกเฉียงใต้ เช่น อินโดนีเซีย เมียนมาร์ ฟิลิปปินส์ สิงคโปร์และไทย (Iwamoto, 2020) โดยบริษัทได้ลงทุนร่วมกับบริษัทในพื้นที่เพื่อจัดหาเทคโนโลยีและแบ่งปันองค์ความรู้ด้าน Fintech ที่ได้รับในตลาดจีนให้ เช่น แนวทางการให้คะแนนเครดิต (credit-scoring) ของ Zhima Credit ซึ่งเป็นของ Ant Financial โดยผ่านการใช้งานจริงมาตั้งแต่ปี 2015 ในประเทศจีน ซึ่งรัฐบาลจีนเชื่อว่ามีประสิทธิภาพเพียงพอที่จะนำไปใช้ในเอเชียตะวันออกเฉียงใต้ได้เช่นกัน (Consulate General of The People's Republic of China in Chicago, 2015)

อย่างไรก็ตาม ระบบการให้คะแนนเครดิต (credit-scoring) จะเป็นเครื่องมือสำคัญอย่างหนึ่งในการควบคุมข้อมูลส่วนบุคคลของรัฐบาลจีน กล่าวคือ ข้อมูลที่รวบรวมในระบบการให้คะแนนเครดิตอาจส่งผลให้รัฐบาลจีนมีความสามารถในการควบคุมทางการเมืองมากขึ้น ซึ่งไม่เพียงแต่ประชาชนภายในจีนเท่านั้น แต่ยังหมายรวมถึงผู้ใช้บริการจากประเทศอื่น ๆ ผู้ให้บริการทางการเงินดังกล่าวของ

จีนอาจต้องให้ข้อมูลของลูกค้าซึ่งรวมทั้งลูกค้าจากภายในและภายนอกประเทศหากรัฐบาลจีนร้องขอ ดังนั้น หากรัฐบาลจีนต้องการที่จะโน้มน้าวประเทศอื่น ๆ เช่น ประเทศในเอเชียตะวันออกเฉียงใต้ซึ่งเป็นพื้นที่สำคัญหลักของระบบการจัดการคะแนนเครดิตดังกล่าว การควบคุมข้อมูลส่วนบุคคลข้างต้นจะเป็นเครื่องมือที่มีนัยสำคัญในการต่อรองของรัฐบาลจีนอย่างมาก

นอกจากนี้ จีนได้ผลักดันให้ธนาคารของตนใช้ระบบการชำระเงินหยวน ซึ่งจะแยกออกจากเครือข่ายธุรกรรมทางการเงินทั่วโลก ธนาคารกลางของจีนได้เสนอระบบการชำระเงินข้ามพรมแดนระหว่างธนาคาร (Cross-Border Interbank Payment System: CIPS) ซึ่งเป็นระบบการหักบัญชีและการชำระเงินผ่านบัญชีที่ใช้สกุลเงินหยวนของจีนเป็นหลักในปี 2015 (Congressional Research Service, 2021) ให้กับธนาคารต่าง ๆและแพร่กระจายไปยัง 96 ประเทศและภูมิภาค ซึ่งรวมถึงสหรัฐฯ และญี่ปุ่นด้วยในปี 2020 ทั้งนี้ รัฐบาลจีนเชื่อว่า การพึ่งพาเงินดอลลาร์สหรัฐและเครือข่ายทางการเงินระหว่างประเทศของสมาคมเพื่อการโทรคมนาคมทางการเงินระหว่างธนาคารทั่วโลก (Society for Worldwide Interbank Financial Telecommunication: SWIFT) เพียงทางเดียวอาจมีความเสี่ยง โดยเฉพาะอย่างยิ่งหากสหรัฐฯ พยายาม SWIFT เป็นเครื่องมือในการกดดันสถานการณ์ทางการเงินและโดยเฉพาะอย่างยิ่งในการต่อสู้กับรัฐบาลจีน เช่น กรณีการคว่ำบาตรทางเศรษฐกิจของสหรัฐฯ ต่ออิหร่าน โดยการนำอิหร่านออกจากเครือข่ายของ SWIFT ส่งผลให้อิหร่านถูกแยกตัวออกจากระบบเศรษฐกิจโลก (Job.banks.am, 2022) และกรณีความขัดแย้งระหว่างรัสเซีย-ยูเครนในปี 2022 โดยการตัดธนาคารรัสเซียออกจากเครือข่ายของ SWIFT ซึ่งจากทั้งสองกรณีดังกล่าวได้เพิ่มความหวาดระแวงของจีนในการพึ่งพาเครือข่าย SWIFT เพียงทางเดียว ดังนั้น รัฐบาลจีนจึงเชื่อว่า วิธีการชำระเงินทางเลือกจะมีความสำคัญต่อความมั่นคงทางเศรษฐกิจของจีนและต่อประเทศอื่น ๆ



อย่างไรก็ตาม จีนยังคงมีความล้าหลังมาตรฐานระดับโลกในระบบการจัดการทางการเงิน รายงานจากคณะกรรมการกำกับดูแลการธนาคารและการประกันภัยแห่งประเทศจีน (China Banking and Insurance Regulatory Commission: CBIRC) ประจำปี 2018 ชี้ให้เห็นว่า จีนกำลังเผชิญกับปัญหาการขาดแคลนเทคโนโลยีสำคัญ เช่น ชิป ระบบปฏิบัติการและฐานข้อมูลการทำธุรกรรม จากรายงานดังกล่าวแสดงให้เห็นว่าแนวปฏิบัติของรัฐบาลจีนปี 2014 ยังไม่สมบูรณ์ในการลดการพึ่งพาเทคโนโลยีจากต่างประเทศและแนะนำให้เปลี่ยนโมเดลคอมพิวเตอร์ภายในประเทศเป็นโมเดลที่ผลิตในประเทศจีน เพื่อกระตุ้นศักยภาพในการพึ่งพาตนเองให้สูงยิ่งขึ้น (Mochinaga, 2021)

กล่าวโดยสรุป กรอบแนวคิดทางอำนาจและสถานะภาพเดิม (status quo) คือ พื้นฐานทางความคิดที่สำคัญในการทำความเข้าใจเบื้องต้นถึงความพยายามในการเปลี่ยนผ่านตำแหน่งแห่งที่ในเวทีโลกระหว่างสหรัฐฯ และจีน กล่าวคือ รัฐบาลจีนทะเยอทะยานมุ่งสร้างอิทธิพลและขยายอำนาจ

ทางเทคโนโลยีให้เป็นที่ยอมรับ เพื่อท้าทายสถานะภาพเดิมที่เป็นอยู่ที่ซึ่งสหรัฐฯ และชาติตะวันตกจำนวนหนึ่งมีบทบาทสำคัญในฐานะเป็นผู้กำหนดกฎเกณฑ์ (rule-maker) ภายใต้ปทัสถานทางเทคโนโลยีและพื้นที่ทางไซเบอร์ในปัจจุบัน ดังนั้น จีนจึงต้องแสวงหาอำนาจในการโน้มน้าว หรือกดดันประชาคมเพื่อการเปลี่ยนผ่านตำแหน่งผู้กำหนดกฎเกณฑ์

อย่างไรก็ตาม ผู้เขียนเชื่อว่า การพึ่งพาอาศัยกันทางเศรษฐกิจระหว่างสหรัฐฯ และจีนเป็นสิ่งสำคัญต่อความพึงพอใจของจีนที่มีต่อสหรัฐฯ เมื่อจีนมีการพึ่งพาอาศัยทางเศรษฐกิจกับสหรัฐฯ มากขึ้นเท่าใด ระดับความพึงพอใจของจีนที่มีต่อระบบและสถานะภาพเดิมที่เป็นอยู่จะมากขึ้นเท่านั้นและสหรัฐฯ ก็จะยิ่งสามารถยับยั้งความไม่พอใจของจีนได้มากขึ้นเช่นเดียวกัน แต่ในความเป็นจริงที่ปรากฏนั้น การพึ่งพาอาศัยกันทางเศรษฐกิจระหว่างสหรัฐฯ และจีนยังไม่เพียงพอที่จะทำให้จีนเกิดความพึงพอใจมากขึ้นที่จะไม่ท้าทายระบบ แต่กลับเป็นตัวกระตุ้นความไม่พอใจของจีน เนื่องจาก ตำแหน่งแห่งที่ของสหรัฐฯ ในฐานะผู้กำหนดกฎเกณฑ์บ่อยครั้งที่สหรัฐฯ แสดงอิทธิพลเหนือและดำเนินกิจกรรมในการแทรกแซงดังที่ยกตัวอย่างไว้จำนวนหนึ่งในตอนต้น อีกทั้งข้อจำกัดที่สหรัฐฯ สร้างต่อความทะเยอทะยานของจีนในการที่จะรับบทบาทผู้นำอาจส่งผลต่อความไม่พอใจของจีนต่อระบบได้เช่นเดียวกัน

กล่าวอีกนัยหนึ่งได้ว่า ปัจจัยทางอำนาจทำให้เราเข้าใจว่าจีนกำลังเดินหน้ายุทธศาสตร์วงจรคู่ขนานตามวัตถุประสงค์นโยบายของตนเองผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัลได้อย่างไร ความสามารถในการโน้มน้าว โน้มนำ ชักจูง รวมถึงการกดดัน แสดงออกถึงอำนาจที่มีอิทธิพลเหนือกว่า เพื่อให้ประเทศต่าง ๆ ยอมรับโครงสร้างพื้นฐานทางเทคโนโลยีของจีน แม้ว่าสหรัฐฯ จะกดดันให้นานาชาติและหน่วยงานอื่น ๆ ไม่ให้ยอมรับโครงการทางเทคโนโลยีของจีน อย่างไรก็ดี สถานการณ์ระหว่างประเทศในปัจจุบันสะท้อนให้เห็นว่า จีนได้ท้าทายต่อการดำเนินการของสหรัฐฯ ในระบบระหว่างประเทศและรูปแบบทางเศรษฐกิจ นำไปสู่การมุ่งสู่กลุ่มประเทศใหม่ ทั้งนี้ สหรัฐฯ เชื่อว่า มาตรฐานที่เกี่ยวข้องกับการใช้เครือข่ายปัญญาประดิษฐ์และ 5G ที่พัฒนาโดยจีนก่อให้เกิดความกังวลเกี่ยวกับการจารกรรมข้อมูลทางไซเบอร์และได้พยายามยับยั้งการแพร่กระจายของโครงสร้างพื้นฐานด้านเทคโนโลยีของจีน เช่น Huawei อย่างไรก็ตาม แม้ว่าสหรัฐฯ จะพยายามห้ามพันธมิตรที่เข้มแข็งข้างต้นของตนไม่ให้ยอมรับเทคโนโลยีของจีน แต่ในความเป็นจริงนั้นสหรัฐฯ ล้มเหลว มีเพียง 3 ประเทศเท่านั้นที่ยินยอมทำตามที่สหรัฐฯ เรียกร้อง แม้แต่อังกฤษ ซึ่งเป็นพันธมิตรที่เข้มแข็งของสหรัฐฯ ก็ยอมให้ Huawei ดำเนินการภายในประเทศของตน

**ประเทศไทยกับความมั่นคงไซเบอร์**

รัฐบาลไทยตื่นตัวในการผลักดันประเด็นความมั่นคงไซเบอร์ในช่วงปีที่ผ่านมา โดยเฉพาะอย่างยิ่งเมื่อเกิดการลงนามในบันทึกความเข้าใจระหว่างหน่วยงานซึ่งรับผิดชอบด้านความมั่นคงไซเบอร์กับบริษัท Huawei ของจีนในปี 2022 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมร่วมกับหน่วยงานด้านความมั่นคงไซเบอร์ของไทยและบริษัท Huawei ได้จัดตั้ง E-Lab ขึ้นเพื่อเป็นแพลตฟอร์มการอบรมทักษะสำหรับบุคลากรไทยทางเทคโนโลยีโดยความร่วมมือกับบริษัทด้านเทคโนโลยีของจีน (*Bangkok Post*, 2022) ในขณะเดียวกันสอดคล้องกับความตั้งใจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency: NCSA) ในการตั้งเป้าขยายความร่วมมือระหว่างหน่วยงานเพื่อยกระดับการควบคุมและเฝ้าระวังพื้นที่ไซเบอร์เพื่อยกระดับความมั่นคงไซเบอร์ของไทย (Sharon, 2022) นอกจากนี้ รัฐบาลไทยยังได้ลงนามในบันทึกความเข้าใจกับหน่วยงานของสหรัฐฯ เพื่อยกระดับการป้องกันอาชญากรรมไซเบอร์โดยเฉพาะเรื่องที่เกี่ยวกับเด็ก (*ไทยรัฐออนไลน์*, 2565) ซึ่งเป็นอีกหนึ่งตัวอย่างที่แสดงให้เห็นถึงการตื่นตัวของไทยต่อประเด็นการพัฒนาความมั่นคงไซเบอร์ของไทย

ตัวอย่างข้างต้นสะท้อนให้เห็นเบื้องต้นว่า มุมมองด้านความมั่นคงไซเบอร์ของไทยของไทยสอดคล้องกับปทัสถานทางไซเบอร์ของจีนโดยเฉพาะในเรื่องการยกระดับการเฝ้าระวังและการควบคุมไซเบอร์ของรัฐดังที่ได้กล่าวไว้ในตอนต้น อีกทั้งยังอาจพิจารณาได้อีกว่า ประชาชนมีความใกล้ชิดกับเทคโนโลยีของจีน โดยเฉพาะอย่างยิ่งเมื่อผู้ให้บริการทางอินเทอร์เน็ตของไทยได้ลงนามทำสัญญาให้ Huawei เป็นแกนในการพัฒนาเทคโนโลยี 5G ภายในไทย (Huawei Technologies, 2022) ซึ่งอาจกล่าวได้ยอมรับปทัสถานทางไซเบอร์ของจีนมาจำนวนหนึ่งแล้วไม่ว่าจะด้วยความตั้งใจหรือไม่ก็ตาม อย่างไรก็ดี ในลักษณะเช่นนี้อาจเป็นให้ความสำคัญกับความเชื่อมโยงหรือผลประโยชน์ทางเศรษฐกิจมากกว่าเป็นการให้ความสนใจกับปทัสถานด้านความมั่นคงดังเช่นที่ได้กล่าวไว้ในลักษณะเดียวกันกับการยอมรับผลิตภัณฑ์ของจีนในประเทศสิงคโปร์ ญี่ปุ่น สหราชอาณาจักร สหรัฐฯ และอื่น ๆ ในตอนต้น อีกทั้งยังเป็นอีกหนึ่งสัญญาณสำคัญสำหรับความพยายามในการเข้ามาเป็นผู้กำหนดมาตรฐานทางเทคโนโลยีในประเทศไทยด้วย

เห็นได้ชัดว่าเส้นทางสายไหมดิจิทัล (Digital Silk Road) ของจีนในทางหนึ่ง ประสบความสำเร็จในการดำเนินตามวัตถุประสงค์ของนโยบายโดยการเปลี่ยนแปลงนโยบายของประเทศอื่นในขณะที่สหรัฐฯ ได้ลดอิทธิพลของตนที่มีต่อประเทศอื่น ๆ จากการแสวงหาเป้าหมายด้านนโยบายที่แคบลง ส่งผลให้จีนมีศักยภาพมากขึ้นในการวิเคราะห์ความสามารถและความต้องการของประเทศอื่น ๆและสร้างผลิตภัณฑ์ทางเลือกและอาจเหนือกว่า ซึ่งเป็นที่ต้องการของประเทศอื่น ๆ มากกว่าข้อเสนอจากสหรัฐฯ ประกอบกับความไม่พอใจที่มีต่อสหรัฐฯ ในฐานะผู้กำหนดกฎเกณฑ์ที่สำคัญ

ภายใต้ปทัสถานที่เป็นอยู่ นอกจากนี้ ยุทธศาสตร์เส้นทางสายไหมดิจิทัลได้ส่งเสริมผลประโยชน์ของจีนไปพร้อมกับที่ส่งเสริมโลกาภิวัตน์ผ่านความเชื่อมโยงของโครงสร้างพื้นฐานด้านเทคโนโลยีที่พัฒนาขึ้น อีกทั้งรัฐบาลจีนได้พยายามสร้างความสัมพันธ์อันดีกับมหาอำนาจขนาดกลางและขนาดเล็กอื่น ๆ เพื่อดึงชาติเหล่านั้นเข้าเป็นส่วนหนึ่งของโครงการขนาดใหญ่ ส่งผลให้หลายประเทศเริ่มมีความใกล้ชิดและเข้าใกล้จีนมากขึ้น กล่าวอีกนัยหนึ่ง ยุทธศาสตร์เส้นทางสายไหมดิจิทัลได้ลดทอนการครอบงำของสหรัฐฯ ในระบบสากล ขณะเดียวกันก็เพิ่มศักยภาพของจีนในการเปลี่ยนผ่านจากการเป็นผู้ทำตามกฎ (rule-taker) มาเป็นผู้กำหนดกฎเกณฑ์ (rule-maker)

จากที่กล่าวมาข้างต้น สรุปได้ว่ายุทธศาสตร์เส้นทางสายไหมดิจิทัลประสบความสำเร็จในการให้ทางเลือกอื่น ๆ แก่นานาชาติซึ่งมีความไม่พอใจบางประการต่อระบบระหว่างประเทศที่นำโดยสหรัฐฯ แม้ว่าจะไม่ได้แทนที่ตำแหน่งที่โดดเด่นของสหรัฐฯ ในระบบสากลอย่างสมบูรณ์ แต่การครอบงำนั้นลดลงอย่างเห็นได้ชัด ซึ่งยุทธศาสตร์เส้นทางสายไหมดิจิทัล คือ ปัจจัยสำคัญของเทคโนโลยีดิจิทัลในโลกปัจจุบัน อนึ่ง สหรัฐฯ ควรแก้ไขมุมมองและนโยบายที่แทรกแซงจนสร้างความไม่พอใจและหวาดระแวงให้แก่นานาชาติ หากต้องการขัดขวางการผงาดขึ้นของจีนโดยไม่ก่อให้เกิดสงครามแย่งชิงเทคโนโลยีกับจีนในอนาคต

# บทที่ 4

# ปทัสถานความมั่นคงไซเบอร์และผู้ประกอบการเชิงปทัสถานในประเทศไทย

## ความนำ

การศึกษาในบทที่ 2และ 3 ปทัสถานความมั่นคงไซเบอร์ของจีนอาจสรุปได้ว่า การกำกับดูแลพื้นที่ไซเบอร์ในแบบของจีนให้ความสำคัญกับรัฐในการกำหนดกฎเกณฑ์และควบคุมการเคลื่อนย้ายของข้อมูล ทั้งยังสอดคล้องกับเรื่อง อธิปไตยทางไซเบอร์ (cyber sovereignty) ดังปรากฏในเอกสารปกขาวซึ่งกล่าวถึงความมั่นคงไซเบอร์ทั้งสองฉบับในการเคารพอธิปไตยทางไซเบอร์ของรัฐ ซึ่งเน้นย้ำถึงหลักการความเสมอภาคของอธิปไตยที่บัญญัติไว้ในกฎบัตรสหประชาชาติ (The State Council Information Office, The People's Republic of China, 2022) และประการสุดท้าย การกำหนดมาตรฐานทางเทคโนโลยีจากการใช้ผลิตภัณฑ์และเทคโนโลยีจากจีน “China Standard 2035” ซึ่งแสดงให้เห็นถึงความพยายามในการวางตัวเป็นผู้กำหนดมาตรฐานทางเทคโนโลยี เพื่อสร้างความเชื่อมโยงเทคโนโลยีและสร้างการพึ่งพาทางเทคโนโลยีจีน (Sheehan, Blumenthal, & Nelson, 2021)

ประเทศไทยในฐานะหนึ่งในประเทศผู้มีส่วนได้ส่วนเสียในข้อริเริ่มแถบและทาง ดังนั้นยุทธศาสตร์เส้นทางสายไหมดิจิทัลจึงส่งผลอย่างมีนัยสำคัญทั้งทางตรงและทางอ้อม ดังได้กล่าวไว้ในบทที่ 3 ถึงความกังวลด้านความมั่นคงไซเบอร์ที่เกิดขึ้นต่อยุทธศาสตร์ดังกล่าวของจีน เช่น ปัญหาการผูกติดและพึ่งพาทางเทคโนโลยีจากจีนอย่างแนบชิด สภาวะความไร้บรรทัดฐานทางไซเบอร์ ปัญหาผูกขาดทางเทคโนโลยีจากจีน รวมถึงปัญหาการครอบงำผ่านเทคโนโลยี เป็นต้น เมื่อพิจารณาถึงข้อกังวลดังกล่าวซึ่งเป็นที่ถกเถียงอยู่ภายนอกประเทศแล้ว คำถามสำคัญ คือ ประเทศไทยมีมุมมอง หรือความกังวลสอดคล้อง หรือแตกต่างจากข้อถกเถียงภายนอกหรือไม่ ดังนั้น ผู้เขียนได้เลือกใช้แนวคิดเรื่องผู้ประกอบการเชิงปทัสถาน (norm entrepreneur) เพื่อพิจารณาถึงบทบาทของผู้ประกอบการเชิงปทัสถานซึ่งทำหน้าที่โน้มน้าวให้ตัวแสดงภายในไทยยอมรับยุทธศาสตร์เส้นทางสายไหมดิจิทัลในฐานะปทัสถานด้านไซเบอร์ใหม่จากจีน

บทบาทของผู้ประกอบการเชิงปทัสถานในฐานะตัวกระทำการ (agent) ที่สำคัญ คือ การสนับสนุนและเผยแพร่การนำไปใช้ของแนวคิดความมั่นคงไซเบอร์ใหม่ของจีน ทั้งนี้ การนำปทัสถานความมั่นคงไซเบอร์จากภายนอกมาปฏิบัติใช้ภายในประเทศของไทยเกิดขึ้นใน 2 ระดับ คือ ระดับระหว่างประเทศและระดับภายในประเทศ กล่าวคือ ในระดับโครงสร้างระหว่างประเทศเกิดจากการบังคับใช้ หรือกดดันจากมหาอำนาจและการขัดเกลาทางสังคม (socialization) ภายในองค์การ

ระหว่างประเทศซึ่งอาจมีอิทธิพลต่อการยอมรับปทัสถานความมั่นคงทางไซเบอร์ใหม่ ในอีกลักษณะหนึ่งเกิดขึ้นในระดับภายในประเทศ เช่น ระบบการเมืองและวัฒนธรรมที่อาจส่งผลกระทบต่อการยอมรับและการดำเนินการตามปทัสถานความมั่นคงไซเบอร์ของประเทศ

ทั้งนี้ ผู้ประกอบการเชิงปทัสถานในระดับข้ามชาติสามารถทำงานร่วมกับกลุ่มผู้สนับสนุนปทัสถานภายในประเทศเพื่อส่งเสริมปทัสถานความมั่นคงไซเบอร์ใหม่ในฐานะตัวกระทำการที่สำคัญที่จะส่งเสริมศักยภาพในการนำไปใช้ ในขณะเดียวกันผู้ประกอบการเชิงปทัสถานโดยเฉพาะอย่างยิ่งตัวกระทำการที่เป็นภาครัฐสามารถนำเสนอแนวทางซึ่งอาจเรียกได้ว่าเป็น “นวัตกรรมใหม่” เมื่อปทัสถานหนึ่งยังคงมีช่องว่าง หรือเปิดให้มีการตีความด้วยตัวเอง โดยเฉพาะอย่างยิ่งปทัสถานไซเบอร์ของจีนซึ่งกล่าวถึงเรื่อง อธิปไตยทางไซเบอร์ (cyber sovereignty) ซึ่งชัดเจนว่าอำนาจอธิปไตยเป็นเรื่องภายในของแต่ละประเทศ ดังนั้นปทัสถานความมั่นคงไซเบอร์ในแบบของจีนจึงอาจเรียกได้ว่าเป็นปทัสถานซึ่งสร้างแรงผลักดัน (motivate) ให้ไทยใช้เป็นแม่แบบในการแก้ปัญหามากกว่าการกล่าวอ้างเชิงศีลธรรม (moral claim) (Becker, 1963) อย่างไรก็ตาม ผู้เขียนตั้งข้อสังเกตว่า ตัวกระทำการภายในไทยโดยเฉพาะอย่างยิ่งตัวกระทำการที่เป็นภาครัฐมีลักษณะเป็นผู้ประกอบการเชิงศีลธรรม (moral entrepreneur) ซึ่งกล่าวอ้างการนำปทัสถานไปใช้เชิงศีลธรรมมากกว่าการเผยแพร่ปทัสถานอย่างตรงไปตรงมา ซึ่งเห็นได้จากกรณีการอ้างถึงความถูกต้องเชิงศีลธรรมจากการตีความกฎหมายซึ่งเกี่ยวข้องกับการแสดงความคิดเห็นบนอินเทอร์เน็ตในกรณีของกฎหมายมาตรา 112 เพื่อปกป้องความสงบเรียบร้อยของราชอาณาจักร (*BBC News ไทย*, 2564) โดยผู้เขียนจะอธิบายต่อไปในส่วนผู้ประกอบการเชิงปทัสถานที่เป็นภาครัฐภายในประเทศไทย

นอกจากนี้ ช่องว่างทางปทัสถานที่ได้กล่าวไปข้างต้นจะส่งผลต่อกระบวนการนำปทัสถานภายนอกมาปฏิบัติใช้ภายในประเทศ (norm internalization process) อย่างมีนัยสำคัญว่า การตีความและการดำเนินกิจกรรมของตัวแสดงภายในรัฐจะเกิดการตีความใหม่ (reinterpretation) (Acharya, 2004) กล่าวคือ เนื้อหาสาระของปทัสถานเหล่านั้นเป็นเรื่องของอัตวิสัย (subjective) อาจส่งผลต่อความเข้าใจร่วมของตัวแสดง ซึ่งอาจนำไปสู่ความไม่เป็นหนึ่งเดียวกันของการตีความและปฏิบัติของตัวแสดงในสังคม ดังนั้น ในบทนี้ผู้เขียนจะอธิบายถึงตัวกระทำการ (agent) ภายในไทยที่มีบทบาทเป็นผู้ประกอบการเชิงปทัสถานในการโน้มน้าวตัวแสดงต่าง ๆ ในสังคมให้ยอมรับปทัสถานความมั่นคงไซเบอร์ของจีนโดยเฉพาะผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัล เพื่อตอบคำถามสำคัญดังนี้ 1) ใครคือตัวกระทำการในฐานะผู้ประกอบการเชิงปทัสถานที่โน้มน้าวให้เกิดการยอมรับยุทธศาสตร์ของจีนในไทย 2) ผู้ประกอบการเชิงปทัสถานมีอิทธิพลต่อตัวแสดงในสังคมเพียงใด 3) ผู้ประกอบการเชิงปทัสถานในไทยมีวิธีการทำงานหรือนำเครื่องมือใดมาใช้ในการแพร่กระจายปทัสถานทางไซเบอร์ของจีนจากกรอบยุทธศาสตร์เส้นทางสายไหมดิจิทัล คำถามเหล่านี้มุ่งชี้ให้เห็นถึง

ผลลัพธ์ของบทบาทของผู้ประกอบการเชิงปทัสถานในไทยว่า ส่งผลอย่างไรต่อนโยบาย หรือการปฏิบัติของตัวแสดงภายในประเทศในประเด็นที่เกี่ยวข้อง

**ตัวแสดงในฐานะผู้ประกอบการเชิงปทัสถานความมั่นคงไซเบอร์ของไทย**

ตัวกระทำการ (agent) ในฐานะผู้ประกอบการเชิงปทัสถานในไทยโดยเฉพาะตัวกระทำการที่มีส่วนเกี่ยวข้องกับความมั่นคงไซเบอร์สามารถเป็นได้ทั้งตัวแสดงที่เป็นปัจเจก หรือองค์กรซึ่งสนับสนุนในการแพร่กระจายและนำปทัสถานไปปฏิบัติ ซึ่งตัวกระทำการสามารถเป็นตัวแสดงที่ไม่ใช่รัฐได้ (Finnemore & Sikkink, 1998) อย่างไรก็ตาม คุณลักษณะประการหนึ่งที่สำคัญของไทย คือ ตัวแสดงที่ไม่ใช่รัฐเหล่านั้นควรเป็นตัวแสดงที่สามารถเข้าถึงโครงสร้างทางการเมืองเพื่อจะสนับสนุนปทัสถานเข้าสู่แนวนโยบายได้อย่างมีประสิทธิภาพ อนึ่ง ผู้ประกอบการเชิงปทัสถานทั่วไปในเรื่องความมั่นคงไซเบอร์ซึ่งเป็นหน่วยงานภาครัฐ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency: NCSA) ซึ่งทำหน้าที่ในการพัฒนาและดำเนินการตามนโยบายและยุทธศาสตร์ด้านความมั่นคงไซเบอร์ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [สกมช.], ม.ป.) ซึ่งการทำงานของ NCSA โดนเด่นในเรื่องการจัดตั้งหน่วยปฏิบัติการร่วมทางไซเบอร์ในประเด็นต่าง ๆ รวมถึงการจัดอบรมและการให้ความรู้แก่บุคลากรในหลายระดับที่เกี่ยวข้องทั้งในหน่วยงานภาครัฐและเอกชน (สกมช., 2566) รวมถึงองค์กรที่ไม่ใช่รัฐ (NGOs) และกลุ่มประชาสังคมในฐานะผู้ประกอบการเชิงปทัสถานทำหน้าที่สำคัญในการสนับสนุนให้เกิดการยอมรับปทัสถานความมั่นคงไซเบอร์ใหม่ รวมถึงสร้างความตระหนักเกี่ยวกับประเด็นด้านความมั่นคงไซเบอร์ให้กับตัวแสดงภายในประเทศ เช่น กรณีของการจัดอบรมด้านความมั่นคงไซเบอร์โดย สกมช. เพื่อยกระดับบุคลากรรัฐ (*BrandInside*, 2065) หรือในกรณีของกลุ่ม True ซึ่งเปิดตัวบริการครบวงจรด้านความมั่นคงไซเบอร์ในชื่อ ทรูดิจิทัล ไซเบอร์ ซิเคียวริตี้ เพื่อบริหารจัดการความปลอดภัยไซเบอร์แบบครบวงจร (*สำนักข่าวอินโฟเควสท์*, 2565) เป็นต้น

นอกจากนี้ ตัวกระทำการที่เป็นตัวแสดงภาคเอกชน เช่น บริษัทเทคโนโลยี บริษัทด้านความมั่นคงไซเบอร์ รวมถึงผู้เชี่ยวชาญด้านเทคนิค ยังสามารถทำหน้าที่เป็นผู้ประกอบการเชิงปทัสถานได้ด้วยการพัฒนาและส่งเสริมเทคโนโลยี รวมถึงเสนอแนวทางด้านความมั่นคงไซเบอร์ใหม่ ๆ ตัวแสดงเหล่านี้สามารถทำงานร่วมกับรัฐบาลและผู้มีส่วนได้ส่วนเสียอื่น ๆ เพื่อส่งเสริมการยอมรับปทัสถานและมาตรฐานความมั่นคงไซเบอร์ใหม่ในเวลาเดียวกัน ดังกรณีของ ทรูดิจิทัล ไซเบอร์ ซิเคียวริตี้ซึ่งได้กล่าวในข้างต้นนั้นจับมือร่วมกับบริษัทเอกชนชั้นนำผู้ให้คำปรึกษาด้านเทคโนโลยีอย่างบริษัท คลาวด์สไตร์ท อินคอร์พอเรชั่น บริษัทให้คำปรึกษาทางเทคโนโลยีโดยเฉพาะเรื่องการป้องกันและตรวจจับภัยคุกคามทางด้านการโจมตีทางไซเบอร์ ร่วมกับบริษัท ซี-สเกเลอร์ ประเทศไทย บริษัทผู้ให้คำปรึกษาด้านการป้องกันข้อมูลแบบชนิดต้องตรวจสอบสิทธิ์ก่อนการเข้าถึงระบบเครือข่าย (Zero Trust

Architecture) และบริษัท อิมเพอว่าร์ ประเทศไทย ด้านการตรวจสอบการใช้งานเว็บแอปพลิเคชันและโปรแกรมการเข้าถึงฐานข้อมูลภายใน (*ผู้จัดการออนไลน์*, 2566)

ในส่วนนี้ผู้เขียนจะอธิบายถึงตัวแสดงซึ่งเป็นผู้ประกอบการเชิงปทัสถานว่ามีหน้าที่และอิทธิพลต่อการสร้าง การเปลี่ยนแปลงและการนำปทัสถานภายนอกประเทศมาปรับใช้ภายในประเทศได้อย่างไร เพื่อแสดงให้เห็นว่าตัวกระทำการในฐานะผู้ประกอบการเชิงปทัสถานในไทยใช้เครื่องมือใดในการแพร่กระจายปทัสถานความมั่นคงไซเบอร์และผลลัพธ์ของแพร่กระจายปทัสถานเหล่านั้นเป็นเช่นไร ผู้เขียนแจกแจงลักษณะตัวแสดงที่เป็นผู้ประกอบการเชิงปทัสถานไว้ 3 ตัวแสดง ดังนี้ 1) รัฐบาลไทยและหน่วยงานภาครัฐในฐานะตัวกระทำการ (agent) 2) ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชน (private sector) 3) ผู้ประกอบการเชิงปทัสถานในบทบาทผู้เชี่ยวชาญทางเทคนิคโดยเฉพาะอย่างยิ่งด้านเทคโนโลยีสารสนเทศและอินเทอร์เน็ต (expert)

**ตัวแสดงที่หนึ่ง บทบาทของรัฐบาลไทยและหน่วยงานภาครัฐในฐานะตัวกระทำการ (agent)**

จากการศึกษาพบว่า ในบริบทด้านความมั่นคงไซเบอร์ของไทยองค์กรหรือหน่วยงานภาครัฐมีบทบาทในการขับเคลื่อน หรือแพร่กระจายทางปทัสถานความมั่นคงไซเบอร์โดยทั่วไปน้อยกว่าเมื่อเทียบกับตัวแสดงที่เป็นกลุ่มนักเคลื่อนไหวทางสังคม เครือข่ายการเคลื่อนไหวทางสังคมและองค์กรพัฒนาเอกชนที่ดำเนินงานในระดับนานาชาติซึ่งมีบทบาทสำคัญในการส่งเสริมปทัสถานและนโยบายใหม่ที่เกี่ยวข้องกับความมั่นคงไซเบอร์ (เจ้าหน้าที่หน่วยงานความมั่นคงของรัฐ, การสื่อสารส่วนบุคคล, 2566) เช่น ความเป็นส่วนตัวของข้อมูล (data privacy) การป้องกันการโจมตีทางไซเบอร์และการกำหนดกฎหมายในการควบคุมอาชญากรรมทางไซเบอร์ ดังปรากฏให้เห็นชัดเจนจากนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) (ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ, 2565) โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นต้นนอกจากนี้ หน่วยงานภาครัฐของไทยได้ดำเนินการเพื่อปรับปรุงความมั่นคงปลอดภัยทางไซเบอร์ เช่น การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency: NCSA) (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562, น. 23-26) และการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ซึ่งเป็นหน่วยงานของรัฐที่รับผิดชอบด้านการส่งเสริมการพัฒนาธุรกรรมอิเล็กทรอนิกส์และอีคอมเมิร์ซในประเทศไทย (พระราชบัญญัติสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์, 2562) เป็นต้น ตัวแสดงที่มีบทบาทเหล่านี้สามารถสร้างความตระหนักรู้เกี่ยวกับปัญหาความมั่นคงไซเบอร์ สนับสนุนการยอมรับปทัสถานและนโยบายใหม่และกำหนดให้รัฐบาลกลางรับผิดชอบต่อการกระทำที่เกี่ยวข้องกับความมั่นคง อย่างไรก็ดี การยอมรับปทัสถานใหม่ที่เกี่ยวข้องกับความมั่นคงไซเบอร์จะสามารถไปถึงจุดสูงสุด

ของการเปลี่ยนผ่านได้ (tipping point) จำเป็นต้องได้รับการยินยอมจากรัฐบาลและหน่วยงานภาครัฐในการรับรองและส่งเสริมปทัสถานใหม่ที่เกี่ยวข้องเสียก่อน (Acharya, 2004) อย่างน้อยที่สุดควรได้รับการยอมรับจากตัวแสดงที่มีความสำคัญ (critical actor) เพื่อรับและส่งต่อนโยบายที่เป็นเรื่องปทัสถานทางไซเบอร์ซึ่งจีนเป็นผู้เผยแพร่ผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัล

**ตัวแสดงที่สอง ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชน**

ตัวกระทำการที่สำคัญในฐานะผู้ประกอบการเชิงปทัสถานซึ่งเกี่ยวข้องกับการเชื่อมต่อทางดิจิทัลและความร่วมมือในบริบทของยุทธศาสตร์เส้นทางสายไหมดิจิทัลและมีบทบาทสำคัญในการกำหนดพฤติกรรมของตัวแสดงในภาคอุตสาหกรรมดิจิทัล ตัวกระทำการเหล่านี้อาจมาจากหลากหลายภาคส่วนทั้งภาคเอกชน อุตสาหกรรม บริษัทผู้ให้บริการอินเทอร์เน็ต โดยเฉพาะอย่างยิ่งภาคธุรกิจ

ผู้ประกอบการเชิงปทัสถานด้านไซเบอร์ซึ่งหมายรวมถึงผู้บริหารและผู้นำของบริษัทที่เกี่ยวข้องกับอุตสาหกรรมดิจิทัลในไทย บุคคลเหล่านี้สามารถใช้อิทธิพลและเครือข่ายเพื่อส่งเสริมการยอมรับปทัสถานใหม่ที่เกี่ยวข้องกับการเชื่อมต่อดิจิทัลและความร่วมมือระหว่างบริษัทอื่น ๆ ในอุตสาหกรรม เห็นได้ชัดจากกรณีของการรวมตัวหน่วยงานด้านเทคโนโลยีเอกชนร่วมกับภาครัฐอย่าง สกมช. เพื่อความร่วมมือป้องกันภัยคุกคามไซเบอร์ ซึ่งทำให้เกิดการพัฒนาและการวิจัย (R&D) ที่มากขึ้น (*มติชนออนไลน์*, 2566) นอกจากนี้ ตัวแสดงเหล่านี้ยังสามารถใช้ความเชี่ยวชาญ ความรู้และโดยเฉพาะอย่างยิ่งความสัมพันธ์ซึ่งเกี่ยวข้องระหว่างตัวแทน หรือตัวผู้นำบริษัทซึ่งเป็นลักษณะเฉพาะที่เด่นชัดอย่างมากระหว่างผู้ประกอบการไทยและจีน เช่น ความสัมพันธ์เชิงเครือญาติ ความสัมพันธ์เชิงชาติพันธุ์ ดังกรณีของบริษัท SAIC Motor หนึ่งในบริษัทด้านเทคโนโลยียานยนต์ของจีนในเครือ CP หนึ่งในทุนเครือใหญ่ในไทยที่มีความเชื่อมโยงระหว่างบริษัทจีนอย่างมาก ในชื่อเต็มบริษัท เอสเอไอซี มอร์เตอร์-ซีพี จำกัด (SAIC Motor-CP Co. Ltd.) ซึ่งมีความคาดหวังว่าจะนำเข้ารถยนต์ไฟฟ้าจากค่ายจีนเข้ามาตีตลาดเป็นผู้นำตลาดยานยนต์ไฟฟ้าของไทยภายในปี 2030 (*Post Today*, 2564) เป็นต้น เพื่อใช้ในการพัฒนาแนวปฏิบัติให้เกิดการนำปทัสถานไปใช้ หรืออย่างน้อยที่สุด คือ สร้างการรับรู้ทางปทัสถานของจีนสู่สาธารณะ จนนำไปสู่การยอมรับทางปทัสถานใหม่อย่างแยบยล อาจกล่าวได้ว่า ตัวกระทำการในฐานะผู้ประกอบการเชิงปทัสถานด้านไซเบอร์ของไทยที่ส่งเสริมการนำปทัสถานของจีนที่เกี่ยวข้องกับการเชื่อมต่อทางดิจิทัลและความร่วมมือในยุทธศาสตร์เส้นทางสายไหมดิจิทัล จะต้องเป็นตัวกระทำการที่มีส่วนสำคัญในการกำหนดพฤติกรรมของตัวแสดงของตัวแสดงในอุตสาหกรรมดิจิทัลทางใดทางหนึ่ง

ผู้บริหารหรือผู้นำของบริษัทผู้ให้บริการอินเทอร์เน็ตในประเทศไทย คือ หนึ่งในตัวกระทำการที่สำคัญดังกล่าว ตัวกระทำการเหล่านี้สามารถใช้อิทธิพลและเครือข่ายเพื่อส่งเสริมการยอมรับ

ปทัสถานใหม่ของจีนที่เกี่ยวข้องกับการเชื่อมต่อดิจิทัลและความร่วมมือระหว่างบริษัทอื่น ๆ ในอุตสาหกรรม ดังที่บริษัท TRUE หนึ่งในผู้ให้บริการอินเทอร์เน็ตรายใหญ่ของไทยได้ควบรวมกิจการบริษัท DTAC ซึ่งเป็นหนึ่งในผู้ให้บริการทางอินเทอร์เน็ตและโทรคมนาคมไร้สายรายใหญ่ของไทยเช่นเดียวกัน (ประลองยุทธ ผงงอย, 2566) อย่างไรก็ดี บริษัท TRUE คือ ตัวแทนจำหน่ายโทรศัพท์ HUAWEI ที่รองรับเทคโนโลยี 5G ของจีนได้เป็นรายแรกและอันดับ 1 ของไทย (*Ture.th*, 2563) ซึ่งแสดงให้เห็นว่า บริษัทผู้ให้บริการด้านอินเทอร์เน็ตอย่าง TRUE มีศักยภาพเพียงพอที่จะสร้างอิทธิพลต่อตลาดดิจิทัลในไทยและโดยเฉพาะอย่างยิ่งเมื่อเกิดการควบรวมกิจการของบริษัท DTAC ส่งผลให้ศักยภาพในการรับและแพร่กระจายโครงสร้างพื้นฐานด้านอินเทอร์เน็ต เช่น การให้บริการอินเทอร์เน็ต การติดตั้งสายไฟเบอร์ การจำหน่ายโทรศัพท์ซึ่งจีนเป็นผู้ผลิตอย่าง HUAWEI เป็นต้น ซึ่งโครงสร้างพื้นฐานด้านอินเทอร์เน็ตเหล่านี้ คือ ส่วนสำคัญของยุทธศาสตร์เส้นทางสายไหมดิจิทัลในเรื่องโครงสร้างพื้นฐานอัจฉริยะของจีน นอกจากนี้ยังสามารถทำงานร่วมกับรัฐบาลและผู้มีส่วนได้ส่วนเสียอื่น ๆ เพื่อพัฒนาแนวทางและการปฏิบัติ รวมถึงการอำนวยเพื่อให้เกิดการยอมรับปทัสถานดังกล่าวของจีนผ่านการให้ความรู้แก่ลูกค้าและผู้ใช้เกี่ยวกับผลประโยชน์ของปทัสถานทางไซเบอร์ของจีนและกระตุ้นให้พวกเขานำไปใช้ในธุรกิจและแนวทางปฏิบัติของตนเอง

อีกตัวอย่างจากกรณี บริษัทซึ่งผู้ให้บริการอินเทอร์เน็ตสามารถให้การฝึกอบรมและการสนับสนุนแก่ลูกค้าและผู้ใช้เพื่อช่วยให้พวกเขายอมรับปทัสถานใหม่ที่เกี่ยวข้องกับการเชื่อมต่อและความร่วมมือทางดิจิทัล นอกจากนี้ยังสามารถให้สิ่งจูงใจและรางวัลแก่ลูกค้าและผู้ใช้ที่ใช้ปทัสถานใหม่ เช่น สิทธิพิเศษจากการซื้อโทรศัพท์ HUAWEI หรือการเปิดใช้บริการครั้งแรกกับบริษัทที่เกี่ยวข้อง การให้สิทธิประโยชน์ในการเข้าถึงบริการทางอินเทอร์เน็ตและเทคโนโลยี 5G เป็นกลุ่มแรก (*ผู้จัดการออนไลน์*, 2563) เป็นต้น



ในขณะเดียวกันสิทธิประโยชน์ รวมถึงต้นทุนที่ต่ำซึ่งเป็นจุดเด่นของโครงสร้างพื้นฐานดิจิทัลของจีน บ่อยครั้งมักกระตุ้นให้ภาคธุรกิจ โดยเฉพาะอย่างยิ่งบริษัทผู้ให้คำปรึกษาและการจัดการโดยเฉพาะด้านเทคโนโลยีหันมาให้ความสนใจกับโครงสร้างพื้นฐานเหล่านั้นเพื่อลดต้นทุนและผลประโยชน์ทางธุรกิจ (ที่ปรึกษาด้านธุรกิจบริษัทเอกชน, การสื่อสารส่วนบุคคล, 2565) อย่างไรก็ตามแรงจูงใจดังกล่าวของกลุ่มธุรกิจโดยเฉพาะบริษัทผู้ให้คำปรึกษาด้านเทคโนโลยีบ่อยครั้งไม่ได้ให้ความสำคัญ หรือเข้าใจถึงชุดความคิด หรือคุณค่าทางปทัสถานแม้แต่น้อย ทั้งปทัสถานทางไซเบอร์ในแบบตะวันตก หรือปทัสถานใหม่ซึ่งถูกเสนอโดยจีน ตัวกระทำการเหล่านั้นมักให้ความสำคัญกับผลประโยชน์ด้านธุรกิจเพียงอย่างเดียว (วิศวกรฝ่ายจัดการระบบ หน่วยงานผู้ให้บริการอินเทอร์เน็ต, การสื่อสารส่วนบุคคล, 2565) การตีความ การรับรู้และความเข้าใจด้านปทัสถานอื่นที่เกี่ยวข้องจะถูกเบี่ยงเบน หรือแม้แต่เกิดการตีความใหม่ (reinterpretation) เพื่อให้สามารถเสนอขายธุรกิจของตนได้

ซึ่งผู้เขียนจะอธิบายอีกครั้งในส่วนของเครื่องมือที่ผู้ประกอบการเชิงปทัสถานใช้ในการเผยแพร่ปทัสถาน

**ตัวแสดงที่สาม ผู้ประกอบการเชิงปทัสถานในบทบาทผู้เชี่ยวชาญทางเทคนิคโดยเฉพาะอย่างยิ่งด้านเทคโนโลยีสารสนเทศและอินเทอร์เน็ต**

ผู้เชี่ยวชาญและบุคลากรทางเทคนิค คือ ตัวกระทำการในระดับ “ปัจเจก” ที่สำคัญในฐานะผู้ประกอบการเชิงปทัสถานความมั่นคงไซเบอร์ซึ่งมีบทบาทในการสนับสนุนให้เกิดการเชื่อมโยงกับองค์กร หรือสถาบันที่น่าเชื่อถือ เช่น เจ้าหน้าที่ในองค์การระหว่างประเทศ สถาบันการศึกษา หรือบริษัทเทคโนโลยี โดยผู้เชี่ยวชาญด้านเทคนิคเหล่านั้นสามารถดำเนินการตามความสามารถของแต่ละคนและโดยทั่วไปแล้วพวกเขาจะเป็นผู้ที่ได้รับความเคารพนับถือในบางประเด็นหรือมีอำนาจในการพูดโดยเฉพาะอย่างยิ่งนักวิชาการและผู้เชี่ยวชาญทางเทคนิคดังเช่นที่อาจารย์ปวีร์ เจนวีระนนท์ นักวิชาการด้านกฎหมายได้ให้คำแนะนำแก่รัฐบาลในการสร้างความเชื่อมั่นด้วยแนวนโยบายป้องกันภัยไซเบอร์ (ปวีร์ เจนวีระนนท์, 2566) อนึ่ง โดยทั่วไปแล้วผู้เชี่ยวชาญและบุคคลทางเทคนิคที่มีความรู้และประสบการณ์อย่างกว้างขวางในด้านความมั่นคงไซเบอร์สามารถทำหน้าที่เป็นผู้ประกอบการเชิงปทัสถานได้โดยสนับสนุนให้มีการยอมรับปทัสถานทางไซเบอร์ได้

อย่างไรก็ตาม ตัวกระทำการที่เป็นผู้เชี่ยวชาญและบุคลากรทางเทคนิคอาจมีความซับซ้อนในการทำความเข้าใจและอาจสร้างความสับสนกับตัวแสดงในระดับองค์กร เนื่องจากผู้เชี่ยวชาญและบุคลากรทางเทคนิคจำนวนมากกระทำการในนามหรือภายใต้องค์ใดองค์กรหนึ่งทั้งที่เป็นภาครัฐและภาคเอกชน ผู้เขียนใคร่อธิบายว่า ตัวกระทำการที่เป็นผู้เชี่ยวชาญและบุคลากรทางเทคนิคเป็นตัวแสดงในลักษณะปัจเจกที่มีอัตวิสัยโดยตัวเอง ซึ่งบางครั้งใช้วิธีการโน้มน้าวและนำเสนอปทัสถานแตกต่างจากตัวกระทำการในระดับองค์กร แม้ท้ายที่สุดตัวแสดงระดับปัจเจกเหล่านี้อาจตัดสินใจไปในทิศทางเดียวกันกับองค์กรที่ตนสังกัดก็ตาม แต่ระหว่างกระบวนการโน้มน้าวและนำเสนอปทัสถานหรือชุดความคิด บ่อยครั้งที่ตัวแสดงในระดับปัจเจกนี้มีความคิดเห็นและโน้มน้าวที่แตกต่างจากองค์กร (ที่ปรึกษาด้านธุรกิจบริษัทเอกชน, การสื่อสารส่วนบุคคล, 2566)

กรณีที่พบเห็นบ่อยครั้งจากการศึกษาให้ข้อมูลในลักษณะเดียวกันว่า “...บ่อยครั้งที่มีการเตือนฝ่ายบริหารถึงความเสี่ยงทางเทคนิคของข้อมูลและความเป็นส่วนตัวของผู้ใช้บริการในเครือข่าย... แต่มักถูกปัดตกจากฝ่ายบริหาร เนื่องจากความเสี่ยงเหล่านั้นเล็กน้อยกว่าสิ่งที่บริษัทจะได้รับ (กำไรและเครือข่ายทุน)” (วิศวกรฝ่ายจัดการระบบ หน่วยงานผู้ให้บริการอินเทอร์เน็ต, การสื่อสารส่วนบุคคล, 2565) ในลักษณะเดียวกัน ผู้ให้บริการด้านคำปรึกษาและการจัดการในด้านเทคโนโลยี (digital consultations) ให้ข้อมูลที่สอดคล้องกันว่า “แทบทุกครั้งในแต่ละโครงการที่เราจะต้องปรับเปลี่ยน

แผนการขายเพื่อให้ ‘ลูกค้า’ พอใจกับข้อเสนอ...” (ที่ปรึกษาด้านธุรกิจบริษัทเอกชน, การสื่อสารส่วนบุคคล, 2565) ในกรณีนี้การขายสามารถหมายรวมถึง การนำเสนอความเสี่ยง การเตือนถึงภัยที่อาจจะเกิดขึ้นในระบบหากดำเนินการด้วยเงื่อนไขบางอย่าง ซึ่งแสดงให้เห็นว่า หนึ่งในมุมมองที่สำคัญของผู้เชี่ยวชาญมองว่า ความพึงพอใจของผู้รับปทัสถานมีความสำคัญต่อองค์กรมากกว่าอัตวิสัยส่วนตัวของตน (ผู้เชี่ยวชาญ) ในขั้นตอนนี้มักถูกตัวแสดงที่เรียกว่า “ลูกค้า (client)” ทั้งลูกค้าที่เป็นหน่วยงานภาครัฐและเอกชนปฏิเสธการโน้มน้าวจากผู้เชี่ยวชาญและในท้ายที่สุดผู้เชี่ยวชาญเหล่านั้นจะต้องเปลี่ยนการนำเสนอปทัสถานของพวกเขา อาจกล่าวอีกนัยหนึ่งว่า เกิดความพยายามในการตีความอีกครั้ง (re-interpretation) ในชุดความคิดหรือปทัสถานที่ผู้เชี่ยวชาญได้นำเสนอให้สอดคล้องกับความต้องการของลูกค้าเหล่านั้น เพื่อตอบสนองต่อผลประโยชน์ทางธุรกิจ

ตัวอย่างเช่น เจ้าหน้าที่จากศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (Thai Computer Emergency Response Team: ThaiCERT) ซึ่งเป็นหน่วยงานของรัฐที่รับผิดชอบในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงไซเบอร์ ทั้งนี้ในการทำงานขององค์กรดังกล่าวมีลักษณะเป็นการให้ผู้เชี่ยวชาญด้านเทคนิคจำนวนหนึ่งรับผิดชอบต่อสถานการณ์ด้านความมั่นคงที่เกิดขึ้นในนามขององค์กร ซึ่งสามารถทำหน้าที่เป็นผู้ประกอบการเชิงปทัสถานที่ระดับปัจเจกด้วยการส่งเสริมการยอมรับบรรทัดฐานและมาตรฐานด้านความมั่นคงไซเบอร์ซึ่งสามารถทำงานร่วมกับหน่วยงานภาครัฐ เอกชนและกลุ่มประชาสังคมในการพัฒนาและดำเนินนโยบายด้านยุทธศาสตร์ด้านความมั่นคงไซเบอร์ได้ กล่าวคือ ผู้เชี่ยวชาญในระดับปัจเจกซึ่งรับผิดชอบในเรื่องดังกล่าว สามารถสรุปและเสนอองค์ความรู้ทางเทคนิคซึ่งหมายรวมถึงปทัสถานทางไซเบอร์แบบจีนด้วย ดังที่นักวิชาการด้านรัฐศาสตร์กล่าวถึง พระราชบัญญัติไซเบอร์ของไทยซึ่งมีลักษณะคล้ายคลึงกับจีนอย่างน้อยที่สุดในลักษณะการบังคับใช้กฎหมายการควบคุมทางไซเบอร์แบบกึ่งอำนาจนิยม เช่น จากกฎหมายต่อต้านการก่อการร้ายหรือมาตรา 112 ในประเทศไทย (ธรรมชาติ กรีอักษร, 2562) เป็นต้น อย่างไรก็ดี ตัวแสดงเหล่านี้อาจมีเจตนาเพื่อการแก้ไขปัญหาหรือนำเสนอสาระที่เกิดขึ้นเฉพาะหน้าเท่านั้น ซึ่งอาจไม่คำนึงถึงองค์ประกอบของปัญหาในภาพรวมด้านความมั่นคงหรือแม้แต่ยุทธศาสตร์ของจีนซึ่งช่องว่างของความเข้าใจด้านความมั่นคงไซเบอร์ในภาพใหญ่ดังกล่าวนี้อาจถูกนำไปใช้อย่างผิดเจตนา (misuse) เพื่อตอบสนองความต้องการของตัวแสดงอื่นซึ่งมีความใจเรื่องความมั่นคงไซเบอร์ในภาพใหญ่ได้

อย่างไรก็ตาม จากการศึกษาพบว่า ในกรณีของไทยนั้นผู้มีบทบาททางการเมืองภายในรัฐบาลจะมีผลอย่างมากต่อขีดความสามารถของตัวแสดงที่เป็นผู้เชี่ยวชาญทางเทคนิคในการอำนวยให้เข้าถึงพื้นที่เพื่อแพร่กระจายปทัสถาน ตัวแสดงที่มีบทบาททางการเมืองเหล่านี้สามารถเป็นได้ทั้งในระดับปัจเจกและระดับรัฐ โดยลักษณะสำคัญที่สุดคือ พวกเขาจะต้องสามารถใช้อำนาจและอิทธิพลทางการเมืองเพื่อส่งเสริมวาระการประชุมทางการเมืองได้และดังที่กล่าวไว้ข้างต้นว่า ช่องว่างระหว่างความ

เข้าใจด้านความมั่นคงของผู้เชี่ยวชาญด้านเทคนิคดังกล่าว อาจถูกนำมาใช้โดยตัวกระทำการที่มีบทบาททางการเมืองในระดับนี้ เช่น กรณีการอ้างความชอบธรรมในการเผยแพร่ให้เกิดการยอมรับปทัสถานหนึ่งโดยอ้างอิงข้อมูลซึ่งได้จากผู้เชี่ยวชาญทางด้านเทคนิค ดังกรณีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอีเอส) กล่าวถึงการบังคับใช้กฎหมาย มาตรา 112 ในลักษณะครอบคลุมถึงพื้นที่ไซเบอร์โดยเฉพาะในการใช้โซเชียลมีเดียแสดงความคิดเห็นโจมตีรัฐบาลและสถาบันกษัตริย์ (*The Standard,* 2564) ซึ่งอาจทำให้เกิดการบิดเบือน (misrepresentation) เจตนาและคำแนะนำของผู้เชี่ยวชาญทางเทคนิค จนอาจนำไปสู่การนำไปใช้ในทางที่ผิด (misuse) เนื่องจากในขอบเขตของการตีความที่กว้างของปทัสถาน (กฎหมายภายในประเทศของไทย) (*iLaw,* 2564) เป็นต้น ดังนั้นแล้ว ลักษณะเช่นว่านี้อาจปรากฏขึ้นและถูกใช้เป็นเครื่องมือทางการเมืองในการตีความด้านปทัสถานความมั่นคงไซเบอร์ด้วย

**การโน้มน้าวใจและผลลัพธ์ของผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ของไทย**

ผู้ประกอบการเชิงปทัสถานโดยทั่วไปมักถูกมองว่า มีเป้าหมายเพื่อการโน้มน้าวเป็นหลัก อย่างไรก็ตาม งานศึกษาจำนวนมากชี้ให้เห็นว่า ยังมีผลลัพธ์ในรูปแบบอื่นด้วยเช่นกัน ซึ่งผลลัพธ์ในรูปแบบที่แตกต่างไปนอกจากความพยายามเพื่อโน้มน้าวให้เกิดการยอมรับปทัสถานซึ่งจะนำไปสู่การสร้างความสอดคล้องทางปทัสถาน (norm conformity) ยังปรากฏในรูปของความพยายามสร้างความคล้อยตามทางสังคม (social conformity) รวมถึงผลลัพธ์ซึ่งเกิดจากการใช้เครื่องมือที่แตกต่างกันของตัวกระทำการเพื่อให้บรรลุเป้าหมายสำคัญของตน ส่งผลให้เกิดการแปลปทัสถานนำไปสู่การระบุตัวตนภายในปทัสถานขึ้น (identification) (Rublee, 2008) โดยส่วนนี้จะกล่าวถึงผลลัพธ์ที่ผู้ประกอบการเชิงปทัสถานความมั่นคงไซเบอร์และเครื่องมือที่ใช้เพื่อให้บรรลุผลลัพธ์เหล่านั้น

อนึ่ง ผู้ประกอบการเชิงปทัสถานของไทยสามารถเชื่อมโยงยุทธศาสตร์เส้นทางสายไหมดิจิทัลรวมถึงปทัสถานทางไซเบอร์ของจีนให้เกิดการยอมรับภายในประเทศได้ผ่านการโน้มน้าวใจ (persuasion) ซึ่งเกี่ยวข้องกับการเปลี่ยนแปลงพฤติกรรมและความชอบของตัวแสดงอื่นให้ยอมรับปทัสถานใหม่ จากการศึกษาวรรณกรรมจำนวนมากชี้ให้เห็นว่า การโน้มน้าวใจเป็นหน้าที่หลักของผู้ประกอบการเชิงปทัสถานซึ่งพยายามที่จะเปลี่ยนความคิดของตัวแสดงอื่นให้ยอมรับหรือปฏิบัติตามปทัสถานใหม่ การเปลี่ยนแปลงพฤติกรรมผ่านเครื่องมือที่เรียกว่า การโน้มน้าวใจ แสดงให้เห็นถึงชัยชนะด้วยอำนาจทางความคิดเชิงปทัสถาน (normative idea) ซึ่งหยั่งรากและคงทนมากกว่าจะเป็นเพียงการบีบบังคับด้วยอำนาจเชิงวัตถุ (material leverage) (Payne, 2001)

ทั้งนี้ การโน้มน้าวแบ่งได้เป็น 2 ลักษณะ ได้แก่ การโน้มน้าวเชิงโครงสร้าง (structural persuasion) และการโน้มน้าวเชิงจิตวิทยา (psychological persuasion) ลักษณะที่หนึ่ง การโน้ม

น้าวเชิงโครงสร้าง ซึ่งเกี่ยวข้องกับการเรียกร้องทางกฎหมายใหม่บนกรอบกฎเกณฑ์ที่มีอยู่ กล่าวคือ ผู้ประกอบการเชิงปทัสถานสามารถใช้หรือกล่าวอ้างกฎหมายและข้อบังคับที่มีอยู่เพื่อสนับสนุนข้อโต้แย้งของตัวเองในการผลักดันยุทธศาสตร์เส้นทางสายไหมดิจิทัล เช่น ตัวกระทำการอาจโต้แย้งว่าความคิดริเริ่มนี้จำเป็นต่อการปฏิบัติตามข้อตกลงการค้าระหว่างประเทศ หรือเพื่อส่งเสริมการเติบโตทางเศรษฐกิจอันสอดคล้องเจตนาของรัฐบาล การกล้าวอ้างถึงหลักการที่ระบุไว้ในแผนพัฒนาประเทศในยุทธศาสตร์ชาติ 20 ปีของไทย (สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, 2561) เพื่อให้เกิดการยอมรับและเข้าใจที่ง่ายขึ้นในตัวแสดงอื่น เป็นต้น

ลักษณะที่สอง การโน้มน้าวเชิงจิตวิทยา ซึ่งเกี่ยวข้องกับกระบวนการสื่อสารผ่านการโต้แย้งและการกระทำ กล่าวคือ ผู้ประกอบการเชิงปทัสถานสามารถใช้การดึงดูดทางอารมณ์และเครื่องมือในการโน้มน้าวใจอื่น ๆ เช่น การให้ผลตอบแทน การให้รางวัล เพื่อเปลี่ยนความชอบและความพึงพอใจของตัวแสดงตัวอื่น ๆ ให้ยอมรับปทัสถานใหม่อย่างแยบยล ตัวกระทำการสามารถใช้แคมเปญโซเชียลมีเดียเพื่อสร้างความตระหนักรู้เกี่ยวกับประโยชน์ของยุทธศาสตร์เส้นทางสายไหมดิจิทัล เพื่อสร้างความรู้เกี่ยวกับการดำเนินการ (ภัชภิชา ฤกษ์สิรินุกูล, 2564) รวมถึงการโฆษณาสินค้าของจีนในฐานะสินค้าทางเลือกสำหรับกลุ่มเป้าหมายเพื่อสร้างความน่าเชื่อถือและความคุ้นเคยให้กับสังคม (กรองจันทร์ จันทรพาหา, ม.ป.ป.) เป็นต้น

ผู้ประกอบการเชิงปทัสถานสามารถบรรลุผลลัพธ์ของการโน้มน้าวได้ด้วยกลไก 3 ประการ คือ การเชื่อมโยง การเคลื่อนไหวเชิงประจักษ์และความสม่ำเสมอ ประการที่หนึ่ง การเชื่อมโยง จะถูกใช้เพื่อส่งเสริมอำนาจของการโน้มน้าวเชิงโครงสร้าง กล่าวคือ เมื่อปทัสถานใหม่เชื่อมโยงกับปทัสถานหรือกรอบความคิดเดิมที่ได้รับการยอมรับอย่างดีภายในสังคมแล้วจะส่งผลให้ตัวแสดงอื่นยอมรับปทัสถานใหม่นั้นได้ง่ายขึ้น ซึ่งอาจพิจารณาได้จากกรณีการรับการสนับสนุนกล้องวงจรปิดและระบบสังเกตการณ์สาธารณะจากบริษัทจีนเพื่อการรักษาความสงบเรียบร้อยของกรุงเทพฯ และเพื่ออำนวยผู้ชุมนุมและกลุ่มเคลื่อนไหวทางการเมือง หรือกรณีรักษาความปลอดภัยจากที่ประชุมเอเปค (APEC) ที่จัดขึ้นโดยมีไทยเป็นเจ้าภาพช่วงปี 2022 (*Bangkok Post,* 2022) เช่นเดียวกับการรับสินค้าจากจีนและติดตั้งเครือข่ายการสื่อสารทางไกลเพื่อใช้สำหรับการประชุมในช่วงการแพร่ระบาดของเชื้อ โควิด 19 (เจ้าหน้าที่หน่วยงานความมั่นคงของรัฐ, การสื่อสารส่วนบุคคล, 2566) ซึ่งจะเห็นได้ว่า การเข้ามาของโครงสร้างพื้นฐานดิจิทัลของจีนเหล่านั้นเชื่อมโยงกับการยอมรับของสังคมไทยที่มีอยู่ในช่วงเวลานั้น

อาจกล่าวได้ว่า การโน้มน้าวในลักษณะดังกล่าวเป็นการโน้มน้าวที่สร้างเหตุผลเชิงตรรกะโดยเชื่อมโยงกับปทัสถานหรือกรอบความคิดที่เป็นที่ยอมรับอยู่แล้วในสังคม ซึ่งจะทำให้ปทัสถานใหม่ถูกยอมรับได้ง่าย เนื่องจากเป็นการง่ายสำหรับตัวแสดงในสังคมที่จะทำความเข้าใจ เพราะสามารถ

เปรียบเทียบกับความเข้าใจเดิมที่ตนมีอยู่และมักไม่ตั้งคำถามกับการยอมรับเหล่านั้น เช่น ผู้ใช้บริการอินเทอร์เน็ตที่เป็นลูกค้าของบริษัท TRUE อาจไม่ได้ตระหนักหรือสังเกตถึงความเปลี่ยนแปลงได้อย่างชัดเจนว่า ผลลัพธ์ของการที่ TRUE เข้าถือครองกิจกรรมของ DTAC เป็นเช่นไร เนื่องจากมีความเข้าใจเดิมอยู่แล้วว่าทั้งสองบริษัทเป็นบริษัทผู้ให้บริการทางอินเทอร์เน็ต เช่นเดียวกับการนำสินค้าจีนจำนวนมากเข้าสู่ตลาด อาทิ โทรศัพท์มือถือซึ่งลูกค้าทั่วไปจะพิจารณาเพียงว่า สินค้าเหล่านั้นเป็นเพียงผลิตภัณฑ์ที่มีไว้เพื่อการสื่อสารเท่านั้น (เจ้าหน้าที่ฝ่ายการตลาด หน่วยงานผู้ให้บริการอินเทอร์เน็ต, การสื่อสารส่วนบุคคล, 2565) เช่นเดียวกับผลิตภัณฑ์ของ Apple, Nokiaและ Huawei ลูกค้าโดยทั่วไปจะพิจารณาถึงการใช้งานและความคุ้มค่าเท่านั้น ซึ่งเป็นการยอมรับพื้นฐานที่สุดในชีวิตประจำวัน เป็นต้น กลไกการรับรู้เชิงตรรกะดังกล่าวทำให้ปทัสถานใหม่แทรกซึมเข้ามาภายในประเทศได้อย่างแยบยลและมักไม่ถูกตั้งคำถามหากตรรกะเหล่านั้นไม่ขัดต่อผลประโยชน์ที่ตัวแสดงจะได้รับ

ประการที่สอง การเคลื่อนไหวเชิงประจักษ์ กล่าวคือ ผู้ประกอบการเชิงปทัสถานสามารถใช้ช่องทางการสื่อสารต่าง ๆ เพื่อแสดงให้เห็นความสำคัญของยุทธศาสตร์เส้นทางสายไหมดิจิทัลและชุดความคิดด้านความมั่นคงไซเบอร์ของจีน เช่น การจัดสัมมนา การจัดเวิร์กชอปและการประชุมเพื่อให้ความรู้แก่ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง อย่างไรก็ตาม จากการศึกษาพบว่า ปัจจุบันในประเทศไทยไม่ได้มีวงเสวนาในหัวข้อยุทธศาสตร์เส้นทางสายไหมดิจิทัลเป็นการเฉพาะ แต่หากปรากฏในลักษณะของการถูกพูดถึงในวงเสวนาในลักษณะของการให้ความรู้เรื่องความมั่นคงไซเบอร์มากกว่าจะเป็นประเด็นการเสวนาหลัก ตัวอย่างเช่นงาน Thailand National Cyber Week 2023 (*TechTalkThai*, 2566) เป็นต้นทั้งนี้ เพื่อผลักดันให้ปทัสถานดังกล่าวถูกให้ความสำคัญ การขัดเกลาทางสังคมโดยอ้อมเช่นนี้สามารถนำไปสู่การเปลี่ยนแปลงทางความคิดของผู้มีส่วนได้ส่วนเสียอื่น ๆ ต่อความปทัสถานของจีน ทำให้มีแนวโน้มมากขึ้นที่จะนำมาปฏิบัติใช้ เช่น ผู้กำหนดนโยบายอาจมีแนวโน้มที่จะจัดสรรทรัพยากรและการสนับสนุนทางนโยบายที่สอดคล้องกับยุทธศาสตร์เส้นทางสายไหมดิจิทัล หากเห็นว่า ปทัสถานดังกล่าวถูกให้ความสำคัญโดยตัวแสดงอื่น ๆ ดังที่ปรากฏในการลงนามความเข้าใจร่วมระหว่างไทย-จีน เพื่อส่งเสริมการลงทุนตามนโยบายหนึ่งแถบหนึ่งเส้นทาง เพื่อเชื่อมโยงสู่ยุทธศาสตร์ไทยแลนด์ 4.0 ในปี 2022 (*M Report*, 2565) ซึ่งแสดงให้เห็นถึงความตื่นตัวด้านการลงทุนทางไซเบอร์ระหว่างรัฐบาลไทยและจีนมากขึ้น

ประการที่สาม ความสม่ำเสมอ กล่าวคือ เป็นกลไกซึ่งสนับสนุนการโน้มน้าวใจของตัวแสดงโดยการอ้างการกระทำที่เกิดขึ้นในอดีต หรือการให้คำสัญญาของตัวแสดงเพื่อใช้เป็นเหตุผลสำหรับการกระทำในอนาคต อาจกล่าวได้ว่า ผู้ประกอบการเชิงปทัสถานจะสร้างความสอดคล้องกับพฤติกรรมของตนในอดีตเพื่อแสดงให้เห็นถึงความตั้งใจของตนมาโดยตลอด ตัวกระทำการนี้มักปรากฏ

ในรูปของตัวแสดงที่เป็นผู้มีบทบาททางการเมือง อาทิ การเข้าร่วมของ พล.อ. ประยุทธ์ จันทร์โอชา นายกรัฐมนตรีในขณะนั้นในการประชุมสุดยอดยุทธศาสตร์เส้นทางสายไหม ครั้งที่ 2 เมื่อปี 2019 (นพนนารถ, 2562) และจากการให้สัมภาษณ์ผ่านสื่อมวลชนไทยถึงวิสัยทัศน์และความมุ่งมั่นเพื่อความเชื่อมโยงยุทธศาสตร์เส้นทางสายไหมจีนกับ ยุทธศาสตร์ไทย อาทิ EECและ ACMECS เป็นต้น (*ไทยรัฐออนไลน์,* 2562) ซึ่งมักใช้เครื่องมือในการแพร่กระจายปทัสถานที่เรียกว่า การแสดงความมุ่งมั่น (showing commitment) ซึ่งผู้เขียนจะกล่าวอีกครั้งในส่วนของเครื่องมือของผู้ประกอบการเชิงปทัสถาน

อย่างไรก็ตาม ผู้ประกอบการเชิงปทัสถานสามารถใช้กลไกข้างต้นเพื่อสร้างให้เกิดผลลัพธ์ในรูปแบบอื่นที่ไม่ได้เป็นผลลัพธ์ของการสร้างความคล้อยตามทางปทัสถาน (norm conformity) เพียงอย่างเดียว แต่ยังมีผลลัพธ์ที่สร้างให้เกิดความคล้อยตามทางสังคม (social conformity) และการระบุตัวตนในปทัสถาน (identification) เพื่อส่งเสริมและดำเนินการตามยุทธศาสตร์เส้นทางสายไหมดิจิทัล กล่าวคือ การคล้อยตามทางสังคม หมายถึง การสร้างสภาพแวดล้อมทางสังคมที่มีอิทธิพลต่อพฤติกรรมของตัวแสดงในสังคมโดยไม่เปลี่ยนแปลงความพึงพอใจ หรือความชอบของตัวแสดงเหล่านั้น (Rublee, 2008) หมายความว่า ตัวแสดงเหล่านั้นอาจเปลี่ยนพฤติกรรมของตนหากเห็นว่า การปฏิบัติตามตัวแสดงอื่น ๆ ให้ผลลัพธ์ที่เกิดประโยชน์มากกว่าการไม่ทำปฏิบัติตาม แม้ว่าความสอดคล้องทางสังคมอาจไม่ได้เปลี่ยนแปลงความพึงพอใจ หรือความชอบของตัวแสดงในทันที แต่ในระยะยาวนั้นสามารถเปลี่ยนผ่านได้โดยกระบวนการขัดเกลาทางสังคมซึ่งอาจเกิดจากความคาดหวังชุดใหม่ต่อปทัสถานใหม่ของจีน เช่น นาย A เห็นนาย Bและ C ใช้โทรศัพท์ Xiaomi ซึ่งเป็นผลิตภัณฑ์ของจีน จึงตัดสินใจซื้อโทรศัพท์ประเภทเดียวกันด้วยเหตุผลว่า รุ่นเดียวกัน บริษัทเดียวกัน อาจใช้งานร่วมกันได้สะดวกและอาจขอคำแนะนำจากทั้งสองได้หากเกิดปัญหา ตัวอย่างข้างต้น สะท้อนให้เห็นชุดความคิดโดยทั่วไปทางสังคมว่า นาย A มองเห็นประโยชน์จากการใช้งานผลิตภัณฑ์จากจีนภายใต้เงื่อนไขของการคล้อยตามทางสังคมดังที่ได้กล่าวไป

ในทางกลับกัน การระบุตัวตนในปทัสถานจะเกิดขึ้นเมื่อตัวแสดงแบ่งปันตัวตน (sharing identity) อาจกล่าวอีกนัยหนึ่งว่า ตัวแสดงที่ระบุตัวตนในปทัสถานจะเกิดขึ้นเมื่อตัวแสดงเกิดความพึงพอใจ ยอมรับ หรือความชอบต่อปทัสถานและกล่าวว่าตัวเองนั้นเป็นหนึ่งในผู้สนับสนุนปทัสถานนั้นด้วยตนเอง กล่าวคือ การระบุตัวตนนั้นจะทำให้ตัวแสดงเกิดความพึงพอใจต่อปทัสถานก่อนที่จะเกิดการเปลี่ยนแปลงพฤติกรรม ในขณะที่การเปลี่ยนแปลงพฤติกรรมที่เกิดขึ้นจากความคล้อยตามทางสังคมอาจไม่เปลี่ยนแปลงความพึงพอใจ ความชอบ หรือความสนใจของตัวแสดงได้ (Neville, Novelli, Drury, & Reicher, 2022) ตัวกระทำการในฐานะผู้ประกอบการเชิงปทัสถานของไทยสามารถใช้วิธีการนี้เพื่อส่งเสริมยุทธศาสตร์เส้นทางสายไหมดิจิทัล รวมถึงชุดความคิดทางไซเบอร์ของ

จีนด้วยการให้สวัสดิการหรือรางวัลแก่ตัวแสดงที่ระบุตัวเองว่าเป็นส่วนหนึ่งและยอมรับกับปทัสถานของจีน เพื่อแสดงให้เห็นถึงประโยชน์จากการเป็นส่วนหนึ่งของปทัสถานในแบบของจีน เช่น ผู้ให้บริการด้านเครือข่ายอินเทอร์เน็ตให้สิทธิพิเศษสำหรับลูกค้าที่ใช้สินค้าจาก Huaweiและเทคโนโลยี 5G เป็นต้น (*ผู้จัดการออนไลน์*, 2563) การสร้างความรู้สึกเป็นเจ้าของรวมถึงอัตลักษณ์ร่วมระหว่างตัวแสดงในไทยกับตัวกระทำการทั้งจากภายในและภายนอกประเทศจะกระตุ้นให้ตัวแสดงเปลี่ยนความชอบและยึดโยงกับปทัสถานเหล่านั้นของจีน ซึ่งจะทำให้เกิดความเหนียวแน่นในการร่วมมือเพื่อแพร่กระจายปทัสถานทางไซเบอร์ของจีนในไทยมากขึ้น

อย่างไรก็ดี วิธีการดังกล่าวประสบความสำเร็จอย่างมากในกรณีของผลิตภัณฑ์อิเล็กทรอนิกส์ของบริษัท Apple หนึ่งในผู้ผลิตสินค้าเทคโนโลยีและโทรคมนาคมของสหรัฐฯ ซึ่งแม้สินค้าเปิดตัวชิ้นใหม่จะมีราคาสูงอย่างมาก แต่ผู้ที่นิยามตัวเองว่าเป็น “สาวก” ของ Apple ยังคงใช้สินค้าต่อไป (Technophrenia, 2014) หรือแม้แต่กรณีบุคคลทั่วไปที่วิจารณ์ราคาสินค้าสูงจำนวนมากก็ปฏิเสธไม่ได้ว่า ท้ายที่สุดพวกเขาเหล่านั้นก็ยังคงใช้สินค้าของ Apple เช่นเดิม ซึ่งสะท้อนให้เห็นถึงลักษณะของกระบวนการคล้อยตามทางสังคมดังที่ได้กล่าวไปเช่นกัน เป็นต้น

กล่าวโดยสรุป ผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ของไทยสามารถนำแนวคิดของเส้นทางสายไหมดิจิทัลไปใช้ได้โดยการโน้มน้าวใจเพื่อสร้างความคล้อยตามทางสังคมและการระบุตัวตนของตัวแสดงภายในไทย ตัวกระทำการเหล่านั้นสามารถให้รางวัลแก่ตัวแสดงที่ปฏิบัติตามปทัสถานใหม่ของจีน รวมถึงการสร้างความรู้สึกเป็นเจ้าของและอัตลักษณ์ร่วมกันระหว่างตัวแสดงในไทย นอกจากนี้ ตัวกระทำการยังสามารถมีอิทธิพลต่อพฤติกรรมของผู้มีส่วนได้ส่วนเสียผ่านการมีปฏิสัมพันธ์กับรัฐบาลจีนและข้อริเริ่มแทบและทาง เพื่อส่งเสริมความเชื่อมโยงทางดิจิทัลและความร่วมมือระหว่างประเทศ ๆ ในภูมิภาคผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัล รวมถึงลงนามในหนังสือการทำความเข้าใจร่วม (MoU) (*Workpoint Today,* 2565) และเชื่อมโยงกับข้อริเริ่มเดิมของไทยในยุทธศาสตร์ระเบียงเศรษฐกิจภาคตะวันออก (Eastern Economic Corridor: EEC) ซึ่งการพัฒนา EEC จะส่งเสริมการใช้แพลตฟอร์มและเทคโนโลยีดิจิทัลของจีน เช่น อีคอมเมิร์ซ การชำระเงิน ภายใต้บริษัทผู้ให้บริการจากจีน อาทิ Alibaba (*ไทยพับลิก้า,* 2561) เป็นต้น แสดงให้เห็นว่า จีนมีอิทธิพลอย่างมากต่อการส่งเสริมและดำเนินการตามยุทธศาสตร์และมีแนวโน้มที่จะยังคงมีบทบาทสำคัญในการทำเช่นนั้นในไทยต่อไป

**เครื่องมือของผู้ประกอบการเชิงปทัสถานของไทยในกระบวนการนำปทัสถานมาปฏิบัติใช้ภายในประเทศ**

การทำความเข้าใจกระบวนการนำปทัสถานจากภายนอกมาปฏิบัติใช้ภายในประเทศ (norm internalization process) คือ หัวใจสำคัญของการทำความเข้าใจผลลัพธ์ของการนำเอาปทัสถานภายนอกมาแพร่กระจายภายในประเทศเพื่อสร้างความยอมรับอันนำไปสู่การเปลี่ยนพฤติกรรมของตัวแสดงภายในประเทศ ทั้งนี้ ผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ของไทยได้ใช้เครื่องมือและวิธีการแตกต่างกันเพื่อให้บรรลุการเปลี่ยนแปลงพฤติกรรมที่เกี่ยวข้องกับแนวคิดเส้นทางสายไหมดิจิทัล รวมถึงชุดความคิดด้านความมั่นคงไซเบอร์ของจีน ซึ่งแจกแจงไว้ดังนี้

เครื่องมือที่หนึ่ง การตีความใหม่ (reinterpretation) และการดัดแปลง (modification) ซึ่งเป็นเครื่องมือที่สำคัญและถูกใช้ทุกครั้งที่ผู้ประกอบการเชิงปทัสถานในไทยรับปทัสถานมาเผยแพร่ปรากฏชัดในตัวกระทำการที่เป็นหน่วยงานของรัฐโดยตัวกระทำการจะใช้เครื่องมือดังกล่าวในการสร้างความเชื่อมโยงกับปทัสถานที่มีอยู่ภายในประเทศ เพื่อสร้างความชอบธรรมในกิจกรรม อย่างไรก็ตามการตีความใหม่และการดัดแปลงโดยทั่วไปจะเกิดขึ้นโดยเฉพาะอย่างยิ่งเมื่อปทัสถานใหม่นั้นมีช่องว่างในการถกเถียง หรือยังขาดความชัดเจนในการกำหนดปทัสถาน ซึ่งปทัสถานด้านไซเบอร์มีคุณลักษณะดังกล่าว เนื่องจากเป็นปทัสถานที่มีความใหม่และยังคงเป็นที่ถกเถียงกันอยู่ในเวทีระหว่างประเทศ จึงมีช่องว่างให้เกิดการตีความโดยตัวแสดงที่สำคัญใหม่อีกครั้ง รวมถึงสามารถดัดแปลงให้เกิดความคล่องตัวในการนำมาปฏิบัติใช้ภายในประเทศ หรือเพื่อให้บรรลุเป้าหมายในการเปลี่ยนแปลงพฤติกรรมของตัวแสดงภายในประเทศ

ในบริบทของยุทธศาสตร์เส้นทางสายไหมดิจิทัลในประเทศไทย ผู้ประกอบการเชิงปทัสถานสามารถใช้การตีความใหม่หรือดัดแปลงเพื่อเชื่อมโยงปทัสถานทางไซเบอร์ในแบบของจีนเข้ากับปทัสถานที่มีอยู่ในไทยซึ่งอาจไม่เกี่ยวข้องโดยตรงกับประเด็นดังกล่าว เช่น รัฐบาลสามารถตีความด้านความมั่นคงและรักษาความสงบภายในราชอาณาจักรเข้ากับโอกาสในการเชื่อมโยงทางไซเบอร์ของจีนด้วยชุดความคิดเรื่องการเฝ้าระวังโดยรัฐบาล หรือรักษาเสถียรภาพทางการเมืองด้วยการติดตามผู้เกี่ยวข้องทางการเมือง โดยหน่วยงานของรัฐจำนวนมากมักกล่าวถึง ความจำเป็นของระบบเฝ้าระวังและความร่วมมือในการติดตั้งระบบสังเกตการณ์ดังกล่าวหากเกิดขึ้นจริง (*The101.world*, 2563) ทั้งยังสะท้อนให้เห็นถึงความพยายามของบริษัทของจีนในการเข้ามามีบทบาทแพร่กระจายชุดความคิดด้านไซเบอร์บางอย่าง นอกจากนี้ยังแสดงให้เห็นว่า ตัวกระทำการของไทยยังสามารถกล่าวอ้างถึงความร่วมมือทางดิจิทัลกับจีนเป็นสิ่งจำเป็นสำหรับการส่งเสริมความมั่นคงภายในประเทศในยุคดิจิทัล และความร่วมมือในกรอบเส้นทางสายไหมดิจิทัลนี้เป็นองค์ประกอบสำคัญของความพยายามนี้ ซึ่งได้กล่าวไว้ในแถลงการณ์ร่วมต่อสื่อมวลชนระหว่างไทย-จีน ในการเยือนไทยและหารือร่วมระหว่าง

นายกรัฐมนตรีหลี่ เค่อเฉียงและ พล.อ. ประยุทธ จันทร์โอชา นายกรัฐมนตรีเมื่อปี 2019 (กระทรวงการต่างประเทศ, 2562) ทั้งนี้ อาจพิจารณาได้ว่าพฤติการณ์ดังกล่าวของรัฐอาจมีเจตนาทางการเมืองแอบแฝงมากกว่าเจตนาเพื่อสร้างความเชื่อมโยงทางเทคโนโลยี หรือโอกาสทางการพัฒนาด้านไซเบอร์

เครื่องมือที่สอง การบิดเบือนความจริง (misrepresentation) และการนำปทัสถานที่มีอยู่มาใช้อย่างผิดวัตถุประสงค์ (misuse) ทั้งนี้ เครื่องมือดังกล่าวไม่ได้สื่อถือเจตนาในเชิงลบหรือมุ่งเพื่อบรรลุผลลัพธ์ที่เป็นด้านลบของการนำเครื่องมือมาใช้ หากแต่เครื่องมือดังกล่าว ถูกพิจารณาในลักษณะของการโน้มน้าวด้วยเหตุผลและวัตถุประสงค์อันแตกต่างจากปทัสถานดั้งเดิมที่รับมา เพื่อให้เกิดการยอมรับและเข้าใจได้ง่ายต่อผู้รับปทัสถานเหล่านั้น อาจกล่าวได้ว่า เครื่องมือนี้เป็นการกล่าวอ้างถึงความเชื่อมโยงกับหลักการบางอย่างที่สังคมให้การยอมรับอยู่ เช่น ความมั่นคงปลอดภัย สิทธิมนุษยชน ผู้ลี้ภัย สิ่งแวดล้อม ปัญหาโลกร้อน เป็นต้น ผู้เขียนตั้งข้อสังเกตว่า ลักษณะเฉพาะที่น่าสนใจของตัวกระทำการในไทยจำนวนหนึ่งอาจกล่าวอ้างเพื่อความถูกต้องทางศีลธรรม (moral claim) ของตัวแสดงที่พยายามเป็นเล่นบทผู้ประกอบการเชิงศีลธรรม (moral entrepreneur) กล่าวคือ ผู้ประกอบการเชิงปทัสถานจะใช้ปทัสถานที่มีอยู่ในลักษณะที่ไม่สอดคล้องกับเจตนาหรือวัตถุประสงค์เดิม เพื่อบรรลุเป้าหมายให้เกิดการโน้มน้าวตัวแสดงภายในรัฐ ทั้งนี้ วิธีการดังกล่าวโดยทั่วไปมักเกิดกับปทัสถานที่กำลังพัฒนาและมีช่องว่างให้เกิดข้อถกเถียงดังที่ได้กล่าวไว้ข้างต้น ดังเช่นการถูกวิพากษ์วิจารณ์ถึงความเป็นมาตรฐานสากลที่จะนำมาใช้ของพระราชบัญญัติความมั่นคงไซเบอร์ ซึ่งถูกตั้งคำถามถึงการใช้อำนาจทางกฎหมายของหน่วยงานรัฐและโดยเฉพาะเจ้าหน้าที่ของรัฐในขอบเขตของกฎหมายให้ชัดเจน (ชูเกียรติ น้อยฉิมและ วรณัฐ บุญเจริญ, 2563)

ในบริบทของยุทธศาสตร์เส้นทางสายไหมดิจิทัลในประเทศไทย ผู้ประกอบการเชิงปทัสถานสามารถใช้ชั้นเชิงในการบิดเบือนความจริงและใช้ปทัสถานที่มีอยู่ในทางที่ผิดเพื่อส่งเสริมปทัสถานใหม่ด้านไซเบอร์ของจีน ตัวอย่างเช่นตัวกระทำการสามารถโต้แย้งได้ว่า การยอมรับยุทธศาสตร์ของจีนแนวคิดทางไซเบอร์โดยเฉพาะอย่างยิ่งเรื่องอธิปไตยทางไซเบอร์ เป็นส่วนหนึ่งของการธำรงรักษาอธิปไตยแห่งราชอาณาจักรภายใต้กรอบยุทธศาสตร์ชาติ 20 ปี แม้ว่าในความเป็นจริงไม่ได้ระบุไว้อย่างชัดเจนในข้อความดั้งเดิมก็ตาม (ประกาศราชกิจจานุเบกษา เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. 2561-2580), 2561) (เจ้าหน้าที่หน่วยงานความมั่นคงของรัฐ, การสื่อสารส่วนบุคคล, 2565) อย่างไรก็ตาม สิ่งสำคัญ คือ ต้องสังเกตว่า การใช้ปทัสถานในทางที่ผิดนั้นอาจก่อให้เกิดความขัดแย้งและอาจนำไปสู่การปฏิเสธ ไม่ยอมรับจากผู้มีส่วนเกี่ยวข้อง ซึ่งอาจตั้งข้อสังเกตได้ว่า เครื่องมือดังกล่าวจะมีประสิทธิภาพต่อเมื่อผู้ประกอบการเชิงปทัสถานมีความระมัดระวังในการใช้เครื่องมือ โดยเฉพาะอย่างยิ่งเพื่อให้สอดคล้องกับเป้าหมายโดยรวมของยุทธศาสตร์เส้นทางสายไหมดิจิทัลซึ่งต้องไม่บิดเบือนความเป็นจริงหรือนำไปใช้อย่างผิดเจตนาจนทำลายความชอบธรรมของปทัสถานที่ถูกยึดโยงด้วย

จากการศึกษาพบว่า บ่อยครั้งที่ตัวกระทำการของไทยได้พยายามเชื่อมโยงชุดความคิดด้านความมั่นคงด้านไซเบอร์ของจีนในเรื่องการกำกับดูแลไซเบอร์โดยที่เน้นรัฐเป็นผู้มีบทบาทสำคัญในการกำกับดูแล เข้ากับชุดความคิดด้านความมั่นคงของไทยในเรื่องการรักษาความสงบเรียบร้อยของราชอาณาจักร ซึ่งตัวกระทำการในไทยเหล่านั้นมักกล่าวอ้างถึงความชอบธรรมเชิงศีลธรรมและความถูกต้องของการกระทำของตนแม้ว่าการกระทำเหล่านั้นจะขัดกับหลักการสากลว่าด้วยสิทธิมนุษยชน โดยเฉพาะเรื่องการติดตามและสังเกตการณ์พฤติกรรมของประชาชน (*ประชาไท,* 2565) อย่างไรก็ดี ตัวกระทำการจำนวนหนึ่งซึ่งมีส่วนเกี่ยวข้องกับการนำปทัสถานความมั่นคงไปปฏิบัติใช้ภายในประเทศ โดยเฉพาะอย่างยิ่งหน่วยงานภาครัฐที่รับผิดชอบด้านความมั่นคงไซเบอร์ได้โต้แย้งว่า แม้การติดตามและสังเกตการณ์ประชาชน (บางกลุ่ม) อาจดูเหมือนการละเมิดสิทธิส่วนบุคคล แต่บ่อยครั้งเป็นไปเพื่อการรักษาความสงบเรียบร้อยและการติดตามขยายผล โดยเฉพาะเรื่องยาเสพติด (หทัยกาญจน์ ตรีสุวรรณ, 2565) ทั้งนี้ ผู้เขียนต้องการชี้ให้เห็นว่า ช่องว่างของปทัสถานของจีนโดยเฉพาะเรื่องอธิปไตยทางไซเบอร์ซึ่งเป็นเรื่องภายในนั้นเป็นช่องว่างที่กว้าง ซึ่งเปิดให้มีการตีความโดยตัวกระทำการภายในรัฐอีกระดับหนึ่งก่อนจะถูกนำไปปฏิบัติใช้และผลการศึกษาชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสถานของไทยโดยเฉพาะหน่วยงานรัฐที่รับผิดชอบด้านความมั่นคงไซเบอร์ยังคงตีความด้านความมั่นคงไว้ค่อนข้างจำกัด แม้จะสอดคล้องกับชุดความคิดของจีนก็ตาม แต่อาจเป็นการปิดกั้นโอกาสในการพัฒนาด้านความมั่นคงไซเบอร์ให้เกิดข้อถกเถียง ซึ่งอาจนำไปสู่การยอมรับเชิงปทัสถานที่มากขึ้นในไทย

เครื่องมือที่สาม การแสดงความมุ่งมั่น (showing commitment) เป็นเครื่องมือที่สำคัญสำหรับผู้ประกอบการเชิงปทัสถานในไทยที่มีลักษณะเป็นปัจเจก หรือกลุ่มบุคคลและบางครั้งอาจเป็นเครื่องมือของตัวแสดงที่มีความเกี่ยวข้องและสามารถเข้าถึงพื้นที่ทางการเมืองได้ เครื่องมือดังกล่าวมีไว้คู่กับกลไกการโน้มน้าวใจเพื่อสร้างความสม่ำเสมอ เพื่อพัฒนาความน่าเชื่อถือและดึงดูดผู้ติดตามด้วยการแสดงให้เห็นถึงความมุ่งมั่นต่อปทัสถานซึ่งเกี่ยวข้องกับจีนและความมั่นคงไซเบอร์ เช่น การแถลงและการประเมินเชิงนโยบายของรัฐบาลเกี่ยวกับความมุ่งมั่นในการพัฒนาทางเทคโนโลยีจนนำมาสู่แนวทางการออกแผนและนโยบายการรักษาความปลอดภัยไซเบอร์เพื่อเสนอต่อองค์กรที่เกี่ยวข้อง (*รัฐบาลไทย*, 2566) หรือการจัดการอบรม เสวนา ด้านเทคโนโลยีอย่างสม่ำเสมอของหน่วยงานเพื่อแสดงให้เห็นถึงความมุ่งมั่นและความต่อเนื่องในเรื่องเทคโนโลยี เป็นต้น ทั้งนี้เป็นที่ต้องจับตามองเนื่องจากการเมืองไทยอยู่ในช่วงเปลี่ยนผ่านทางการเมือง ซึ่งรัฐบาลชุดต่อไปนั้นจะส่งผลอย่างมีนัยสำคัญต่อการกำหนดแนวนโยบายด้านความมั่นคงไซเบอร์ว่า หากเกิดการเปลี่ยนแปลงรัฐบาลคำถามชุดสำคัญคือ นโยบายและแผนเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยซึ่งเคยประกาศออกไปนั้นจะถูกแก้ไข หรือร่างใหม่มากน้อยเพียงใดซึ่งสิ่งนี้จะส่งผลต่อความต่อเนื่องและภาพลักษณะของความมุ่งมั่นของรัฐบาลด้วย

ในบริบทของไทยที่มีต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัลและปทัสถานความมั่นคงไซเบอร์ของจีน ตัวกระทำการในไทยสามารถใช้นโยบายต่างประเทศในด้านต่าง ๆ เช่น ความกังวลเรื่องภัยคุกคามไซเบอร์ การละเมิดข้อมูลส่วนบุคคลและแทรกแซงการเคลื่อนย้ายของข้อมูล เป็นต้น เพื่อแสดงให้เห็นถึงความมุ่งมั่นที่จะสร้างชื่อเสียง สร้างความเชื่อมั่นให้กับตัวแสดงให้เกิดความน่าเชื่อถือในเรื่องได้สนับสนุนเหล่านั้น เช่น การแสดงให้ตัวกระทำการอื่น ๆ เห็นถึงความมุ่งมั่นเชิงรูปธรรมด้วยการจัดตั้งศูนย์ประสานงานด้านความมั่นคงไซเบอร์ของไทยเพิ่มในปี 2564 (ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฯ, 2564, น. 8-17) และการกำหนดหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ฉบับล่าสุดปี 2023 (ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ฯ, 2566, น. 39-40) ซึ่งตัวกระทำการของไทยสามารถใช้ตัวอย่างเหล่านี้เพื่อดึงความสนใจของตัวแสดงอื่น ๆ ให้เห็นถึงความสำคัญของการแสดงความมุ่งมั่นต่อปทัสถานฐานใหม่เพื่อสนับสนุนปทัสถานที่พวกเขายอมรับ ตัวอย่างเช่น การจัดตั้งศูนย์นวัตกรรมดิจิทัลเพื่อส่งเสริมการประสานงานที่มีประสิทธิภาพระหว่างผู้มีส่วนได้ส่วนเสียในการส่งเสริมปทัสถานทางไซเบอร์ ซึ่งสามารถใช้เป็นกลไกในการประสานความร่วมมือระดับนานาชาติ เป็นต้น

กล่าวโดยสรุป เครื่องมือของผู้ประกอบการเชิงปทัสถานทั้ง 3 ประการข้างต้น เป็นลักษณะเด่นซึ่งปรากฏและถูกใช้อย่างชัดเจนโดยตัวกระทำการของไทยในการแพร่กระจายปทัสถานด้านไซเบอร์ของจีน อย่างไรก็ตาม เพื่อยืนยันว่า การเปลี่ยนแปลงเชิงปทัสถานนั้นไม่ได้เกิดขึ้นมาจากสุญญากาศ แต่เกิดจากการโต้ตอบ (interaction) และตอบสนองของตัวแสดงต่อปทัสถานที่ได้รับการส่งเสริมจากกระบวนการนำเอาปทัสถานภายนอกมาปฏิบัติใช้ภายในประเทศ โดยปกติแล้วจะมีการแข่งขัน ต่อรอง ปรับเปลี่ยนและแก้ไขอยู่เสมอ (Maurer & Hoffman, 2019) ดังนั้น การศึกษากระบวนการแปลปทัสถานภายนอกมาเป็นเรื่องภายในประเทศ (norm localization) จึงเป็นสิ่งจำเป็นที่จะต้องศึกษาเพื่อให้เกิดความเข้าใจการเปลี่ยนแปลงพฤติกรรมของตัวแสดงภายในรัฐ

ทั้งนี้ การแปลปทัสถาน หมายถึง กระบวนการที่ปทัสถานถูกปรับให้เข้ากับบริบทในพื้นที่ (ในที่นี้หมายถึงประเทศไทย) กระบวนการนี้เกี่ยวข้องกับการเจรจาต่อรองและการปรับเปลี่ยนปทัสถานเพื่อให้เหมาะกับบริบทของประเทศ ค่านิยมและความเชื่อของผู้รับปทัสถาน การตีความปทัสถานจะส่งผลต่อการเปลี่ยนแปลงพฤติกรรมให้เกิดการยอมรับเชิงปทัสถานให้ง่ายขึ้น เนื่องจากช่วยให้สามารถปรับปทัสถานให้เข้ากับบริบทในประเทศซึ่งผสมผสานค่านิยมและความเชื่อของแต่ละประเทศไว้

ดังนั้น ผลลัพธ์ซึ่งจะสะท้อนปทัสถานด้านความมั่นคงไซเบอร์ของไทยที่รับอิทธิพลจากผู้ประกอบการเชิงปทัสถานของจีนในกรอบยุทธศาสตร์เส้นทางสายไหมดิจิทัล สามารถพิจารณาได้จากมุมมองด้านความมั่นคงไซเบอร์และความรู้ความเข้าใจของไทยที่มีต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัล โดยเฉพาะอย่างยิ่งเมื่อมุมมองด้านความมั่นคงไซเบอร์และการรับรู้ของผู้ประกอบการเชิง

ปทัสถานของไทยที่มีต่อยุทธศาสตร์และชุดความคิดดังกล่าวของจีนถูกพิจารณาร่วมกับเครื่องมือที่ตัวกระทำการไทยใช้ในกระบวนการนำเอาปทัสถานภายนอกมาปฏิบัติใช้ภายในประเทศ (norm internalization process) เพื่อให้บรรลุเป้าหมายในแพร่กระจายปทัสถานทางใดทางหนึ่ง ผลลัพธ์ดังกล่าวจะชี้ให้เห็นได้ว่า ผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ของไทยเลือกรับและไม่เลือกรับสิ่งใดจากยุทธศาสตร์เส้นทางสายไหมดิจิทัล โดยเฉพาะอย่างยิ่งด้านความมั่นคงไซเบอร์

**มุมมองด้านความมั่นคงไซเบอร์และความเข้าใจของตัวกระทำการในไทยที่มีต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัลและอธิปไตยทางไซเบอร์**

มุมมองด้านความมั่นคงของพื้นที่ไซเบอร์โดยทั่วไปกล่าวถึง อำนาจในการกำกับดูแลพื้นที่ไซเบอร์ (cyberspace) นักวิชาการจำนวนมากได้เปรียบเปรย (metaphor) กลไกการเกิดและการทำงานของตัวแสดงจำนวนมากที่ทำงานอยู่ในพื้นที่ไซเบอร์ซึ่งมีส่วนเกี่ยวข้องและเชื่อมโยงกันในการกำกับดูแลพื้นที่นั้นว่าเป็น “ระบบนิเวศ (ecosystem)” ทางไซเบอร์ (DeNardis & Raymond, 2013) ในขณะเดียวกัน Nye (2014) อธิบายว่า พื้นที่ไซเบอร์ คือ พื้นที่ซึ่งประกอบด้วยหน่วยจำนวนมากคอยกำกับดูแลอยู่ภายใต้ระบอบการปกครองที่ซับซ้อน (regime complex) เป็นพื้นที่ซึ่งมีความสัมพันธ์ เชื่อมโยงและโต้ตอบระหว่างกัน โดยรวมเอาตัวแสดงของรัฐและตัวแสดงที่ไม่ใช่รัฐเข้าด้วยกัน ตัวแสดงในฐานะผู้ประกอบการเชิงปทัสถานที่สำคัญซึ่งมีบทบาทในการกำหนดปทัสถาน กำหนดกฎเกณฑ์และแนวปฏิบัติในพื้นที่นี้ด้วยเครื่องมือต่าง ๆ ได้แก่ รัฐบาลและหน่วยงานภาครัฐ หน่วยงานภาคเอกชนและตัวกระทำการในระดับปัจเจกในฐานะผู้เชี่ยวชาญ

**ตัวกระทำการที่เป็นรัฐบาลและหน่วยงานภาครัฐ**



ผู้ประกอบการเชิงปทัสถานด้านไซเบอร์ของไทยที่เป็นภาครัฐได้ให้คำอธิบายเรื่องอธิปไตยทางไซเบอร์ว่า อธิปไตยของชาติเป็นสิ่งสำคัญ การควบคุมและสามารถกำหนดชะตากรรม ‘ทางไซเบอร์’ ของชาติเป็นสิ่งสำคัญ คำถามที่เกิดขึ้น คือ ขอบเขตในการใช้อธิปไตยทางไซเบอร์ดังที่ตัวแสดงของไทยเข้าใจนั้นนิยามไปกว้างและลึกเพียงใด กล่าวอีกนัยหนึ่ง “พื้นที่ไซเบอร์” (cyberspace) ในมุมมองของไทยนั้นมีขอบเขตเพียงใดและมีความเข้าใจปทัสถานทางไซเบอร์ของจีนซึ่งแพร่กระจายผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัลเพียงใด

จากการศึกษาพบว่า ผู้ประกอบการเชิงปทัสถานด้านไซเบอร์ของไทยซึ่งเป็นตัวกระทำการที่เป็นภาครัฐและหน่วยงานของรัฐ มีทรรศนะในเชิงบวกต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัล (Digital Silk Road) เนื่องจากพิจารณาแล้วว่า ความร่วมมือในกรอบดังกล่าวเป็นองค์ประกอบหนึ่งภายใต้ข้อริเริ่มแถบและทางของจีน (Belt and Road Initiative) โดยตัวกระทำการไทยมีมุมมองว่า กรอบความร่วมมือดังกล่าวถือเป็นหนึ่งในกรอบความร่วมมือที่สำคัญสำหรับการพัฒนาโครงสร้างพื้นฐาน

และการเชื่อมโยงตลาดไทยเข้าสู่ตลาดโลก ซึ่งมุมมองดังกล่าวปรากฏชัดจากการที่ พล.อ. ประยุทธ จันทร์โอชา นายกรัฐมนตรีของไทยเข้าร่วมเป็นประธานในพิธีเริ่มการก่อสร้างระบบรถไฟฟ้าความเร็วสูงสายกรุงเทพฯ หนองคายเมื่อปี 2017 ซึ่งการเปิดโครงการนี้ค้านสายตาคนไทยซึ่งมองว่าโครงการนี้ในภาพลักษณ์เชิงลบ (ธีรนัย จารุวัสตร์, 2562) ในขณะเดียวกันคณะทูตจีนประจำประเทศไทยเข้าพบหน่วยงานด้านการศึกษาและธุรกิจในพื้นที่โดยได้รับการต้อนรับจากหน่วยงานบริหารส่วนท้องถิ่นจังหวัดหนองคายในปีเดียวกันนั้น สะท้อนให้เห็นถึงความมุ่งมั่นและความพยายามในการปรับภาพลักษณ์ต่อสังคมให้ยอมรับและมองโครงการของจีนในเชิงบวกมากขึ้น (Jian, 2018) ทรรศนะดังกล่าวสะท้อนให้เห็นว่า ตัวกระทำการของไทยคำนึงถึงผลประโยชน์ด้านเศรษฐกิจและโอกาสในการสร้างความสัมพันธ์ทางการค้าระหว่างจีนเป็นสำคัญหรืออย่างน้อยที่สุดหน่วยงานที่มีบทบาทในการกำหนดนโยบายการด้านการพาณิชย์ การคมนาคมและการสื่อสารมีทรรศนะเช่นนั้น

ผู้เขียนตั้งข้อสังเกตว่า หน่วยงานซึ่งรับผิดชอบด้านความมั่นคงอาจตระหนักถึงภัยคุกคามอย่างเปิดเผยกว่าเมื่อเทียบกับหน่วยงานรัฐอื่น ๆ ด้านหนึ่งเป็นที่ชัดเจนถึงหน้าที่ของหน่วยงานรัฐซึ่งรับผิดชอบด้านความมั่นคงจะคำนึงถึงประเด็นด้านความมั่นคงเป็นพันธกิจ ซึ่งระบุไว้อย่างชัดเจนถึงหน้าที่และลักษณะภัยคุกคามดังปรากฏในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยเรื่อง การกำหนดหลักเกณฑ์และลักษณะหน่วยงานที่รับผิดชอบในการควบคุมและกำกับดูแลด้านความมั่นคงไซเบอร์ (ประกาศคณะกรรมการการรักษาความมั่งคงปลอดภัยไซเบอร์ฯ, 2564, น. 14) และประกาศเดียวกันเรื่อง แนวทางการปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ (ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์, 2564, น. 9-15) เป็นต้น ดังนั้น โจทย์ที่ตามมา คือ หน่วยงานด้านความมั่นคงของไทยในฐานะตัวกระทำการที่สำคัญที่รับปทัสถานด้านความมั่นคง มีความตระหนักและเข้าใจประเด็นด้านความมั่นคงไซเบอร์ของจีนเพียงใด

อย่างไรก็ตาม ผู้ประกอบการเชิงปทัสถานด้านไซเบอร์ของไทยจำนวนมาก ไม่เพียงเฉพาะหน่วยงานด้านความมั่นคง โดยเฉพาะภาควิชาการและภาคธุรกิจโดยเฉพาะผู้ประกอบการด้านเทคโนโลยีเชื่อว่า อธิปไตยทางไซเบอร์ของไทยถูกละเมิดอยู่แล้วในปัจจุบัน (ปริญญา หอมอเนก, 2563) ชุดความคิดดังกล่าว แสดงให้เห็นว่า ตัวกระทำการที่สำคัญของไทยด้านไซเบอร์มีความคิดที่ว่ารัฐไทยควรมีอำนาจในการกำกับ กำหนดและควบคุมการเคลื่อนไหว หรือกิจกรรมที่เกิดขึ้นในพื้นที่ ไซเบอร์ (*The States Times*, 2565) อย่างไรก็ตาม ตัวกระทำการเหล่านั้นในไทยมีความพยายามในการตีความชุดความคิดเรื่องอธิปไตยทางไซเบอร์ในการยึดโยงกับชุดความคิดที่มีอยู่แล้วในเรื่องอธิปไตยของชาติโดยเฉพาะอย่างยิ่งอธิปไตยซึ่งเป็นเขตแดนทางกายภาพ (territory) ซึ่งมองเห็น ระบุ

และจับต้องได้อย่างเป็นรูปธรรม ข้อโต้แย้งดังกล่าวตั้งอยู่บนข้อพิจารณาว่า ตัวกระทำการของไทยแม้จะเชื่อว่าอธิปไตยทางไซเบอร์ของไทยถูกละเมิด แต่ในความเป็นจริงกลับดูเหมือนไทยจะยินยอมให้มีการยินยอมและเต็มใจให้ถูกละเมิด เนื่องจากเอกสารเปิดจำนวนมากของรัฐบาลและเอกสารเชิงยุทธศาสตร์ซึ่งเกี่ยวข้องกับการกำหนดนโยบายและแผน (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562, น. 20-50) รวมถึงแผนพัฒนาเศรษฐกิจและความมั่นคงของชาติ หรือแม้แต่แผนยุทธศาสตร์ชาติ 20 ปีของไทยได้ระบุถึงการเชื่อมโยงด้านสารสนเทศ เทคโนโลยีและดิจิทัล (ประกาศราชกิจจานุเบกษา เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. 2561-2580), 2561) ไม่ได้มีการกล่าวถึงข้อจำกัดในการเข้ามามีส่วนเกี่ยวข้องในพื้นที่ไซเบอร์ของไทยอยู่ในเอกสารเหล่านั้น แต่ปรากฏเพียงการนิยามเรื่องภัยคุกคามทางไซเบอร์โดยไม่ได้ระบุถึงขอบเขตของภัยคุกคามว่ามีขอบเขตในพื้นที่ไซเบอร์เพียงใด มีเพียงการระบุถึงภัยในลักษณะที่ส่งผลต่อระบบและเครือข่าย ซึ่งถือเป็นนิยามอย่างแคบและไม่ชัดเจนอย่างมากในนิยามของพื้นที่ไซเบอร์สากล ซึ่งมีขอบเขตครอบคลุมไปถึงตัวตนบนโลกอินเทอร์เน็ต ทั้งนี้ อาจตั้งข้อสังเกตได้ 2 ประการว่า ผู้กำหนดนโยบายของไทยไม่มีความเข้าใจเรื่องพื้นที่ไซเบอร์อย่างแท้จริง ซึ่งเป็นพื้นฐานสำคัญของชุดความคิดเรื่องอธิปไตยไซเบอร์และอีกประการคือ หลักการดังกล่าวของไทยตั้งอาจอยู่บนพื้นฐานของผลประโยชน์ทางเศรษฐกิจและการพัฒนาเป็นสำคัญ (ที่ปรึกษาด้านธุรกิจบริษัทเอกชน, การสื่อสารส่วนบุคคล, 2565)

เมื่อพิจารณาจากข้อเท็จจริงดังกล่าว ตีความได้ว่า ตัวกระทำการของไทยโดยเฉพาะอย่างยิ่งตัวแสดงที่เป็นภาครัฐซึ่งมีบทบาทในการกำหนดนโยบายใช้เครื่องมือในการเชื่อมโยงปทัสถานทางไซเบอร์ด้วยการโน้มน้าวเชิงโครงสร้าง (structural persuasion) กล่าวคือ ผู้ประกอบการเชิงปทัสถานไทยที่เป็นตัวแสดงภาครัฐ ได้สร้างความเชื่อมโยงปทัสถานใหม่ ในบริบทนี้หมายถึง อธิปไตยทางไซเบอร์ เข้ากับปทัสถานเดิมเรื่องเขตแดนและอำนาจอธิปไตยของรัฐ ซึ่งเป็นสิ่งที่ถูกอธิบายและถกเถียงจนเกิดผลึกเชิงตรรกะ ส่งผลให้กลไกการรับรู้เชิงตรรกะดังกล่าวทำให้ปทัสถานใหม่นั้นทำความเข้าใจได้ง่ายขึ้นและมักไม่ถูกตั้งคำถามหากตรรกะเหล่านั้นไม่ขัดต่อผลประโยชน์ที่ตัวแสดงจะได้รับ

นอกจากนี้มิติด้านความมั่นคงภายในประเทศเป็นอีกหนึ่งประเด็นที่ถูกกล่าวถึงอย่างมีนัยสำคัญ “ภัยคุกคามทางความคิด” เป็นสิ่งผู้ประกอบการเชิงปทัสถานไทยโดยเฉพาะภาครัฐกล่าวถึงหนึ่งในเหตุการณ์สำคัญที่เกิดขึ้นถูกยกตัวอย่างบ่อยครั้งในเหตุการณ์ “Arab Spring” เหตุการณ์ซึ่งมีผลต่อการเลือกตั้งและการเมืองภายในได้ถูกบ่งชี้ว่าเป็นภัยทางไซเบอร์ซึ่งเปลี่ยนความคิด จิตใจ ความเชื่อ ความศรัทธาของผู้คน ทำให้เกิดความชอบหรือไม่ชอบในบุคคล สินค้า บริการและบริษัทต่าง ๆ ตลอดจนผู้นำ (เจ้าหน้าที่หน่วยงานความมั่นคงของรัฐ, การสื่อสารส่วนบุคคล, 2566) ทรรศนะเช่นนี้ของผู้ประกอบการเชิงปทัสถานของไทยโดยเฉพาะหน่วยที่รับผิดชอบด้านความมั่นคงกำลังกล่าวเป็น

นัยสำคัญว่า อธิปไตยทางไซเบอร์ของไทยอาจกำลังถูกนำมาตีกรอบเพื่อรับมือกับสิ่งตัวแสดงเหล่านี้ เรียกว่า “ภัยคุกคามทางความคิด”

อย่างไรก็ตาม เมื่อพิจารณาตามบริบท “ภัยคุกคามทางความคิด” ข้างต้นแล้วจะพบว่า เงื่อนไขของการเกิดปรากฏการณ์เช่นนั้น คือ เมื่อประชาชนรับรู้ข้อมูล ข่าวสาร ข้อเท็จจริง หรือแม้แต่ความเท็จจากข้อมูลที่เคลื่อนไหวอยู่ในพื้นที่ไซเบอร์ นั่นหมายความว่า การป้องกันภัยคุกคามในลักษณะดังกล่าว ย่อมหมายรวมถึง การกำกับดูแลข้อมูลในพื้นที่ไซเบอร์ หรือการคัดกรองข้อด้านข้อมูล (data filter) ทั้งนี้ ปฏิเสธไม่ได้ว่า การกระทำดังกล่าวเป็นการจำกัดเสรีภาพในการเสพข้อมูลอย่างมีนัยสำคัญ โจทย์สำคัญของประเด็นดังกล่าว คือ ผู้ใดมีส่วนในการกำกับดูแล หรือคัดกรองด้านข้อมูล เป็นคำถามสำคัญที่ผู้ประกอบการเชิงปทัสถานไทยโดยเฉพาะภาครัฐในฐานะผู้กำหนดนโยบายต้องถกเถียงอย่างรอบคอบ

อย่างไรก็ตาม จากการศึกษาโดยงานวิจัยชิ้นนี้ซึ่งได้เข้าถึงการสัมภาษณ์ผู้มีส่วนในการกำหนดนโยบายด้านความมั่นคงของหน่วยงานด้านความมั่นคงของรัฐ พบว่า ตัวกระทำการที่สำคัญเหล่านั้นไม่ได้มีการกล่าวถึงผู้เกี่ยวข้องในกระบวนการเหล่านี้ หรืออย่างน้อยที่สุดข้อมูลดังกล่าวก็ไม่ได้ถูกเปิดเผยอย่างชัดเจนต่อการศึกษา

จากทรรศนะข้างต้นสามารถวิเคราะห์ได้ว่า ความเข้าใจของตัวกระทำการที่สำคัญของไทยโดยเฉพาะภาครัฐนั้นมองว่าอำนาจอธิปไตยของไทยไม่ได้จำกัดอยู่ภายใต้เขตแดนทางกายภาพเท่านั้น หากแต่ได้พยายามเข้าไปใช้อำนาจอธิปไตยของตนในพื้นที่ไซเบอร์อย่างชัดเจน ดังข้อเท็จจริงที่ว่า เกิดการจับกุมและดำเนินคดีทางไซเบอร์จำนวนมากภายใต้ข้อกล่าวหาว่า การกระทำทางไซเบอร์นั้นมีผลกระทบต่อความมั่นคงต่อราชอาณาจักรไทย (*VoiceTV, 2566*) คำอธิบายเหล่านี้ชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสถานไทย มีความเข้าใจปทัสถานด้านไซเบอร์ของจีนไม่ว่าจะด้วยความเข้าใจอย่างตรงไปตรงมาแท้จริง หรือความเข้าใจที่เกิดจาก “ความไม่รู้” จนนำไปสู่ความพยายามในการตีความใหม่ (re-interpretation) เพื่อให้ตัวกระทำการที่สำคัญเหล่านั้นสามารถทำความเข้าใจได้ง่ายขึ้น ในเรื่อง อธิปไตยทางไซเบอร์ (cyber sovereignty) และการกำกับดูแลทางไซเบอร์ (cyber governance) ซึ่งดูเหมือนว่า ประเด็นหลังเรื่องการกำกับดูแลทางไซเบอร์ ผู้ประกอบการเชิงปทัสถานไทยที่เป็นตัวแสดงรัฐจะไม่ได้ตระหนักถึงคำสำคัญนี้ไม่ว่าจะด้วยเจตนาปกปิด หรือเลี่ยงที่จะไม่กล่าวถึง (avoiding) เช่นที่ปรากฏจากการลงนามความเข้าใจร่วมกันของรัฐบาลกับหน่วยงานด้านเทคโนโลยีจากจีนอย่าง Huawei เมื่อปี 2022 ซึ่งมีการกล่าวถึงการกำกับดูแลทางไซเบอร์อย่างชัดเจน แต่ก็ไม่ได้กล่าวถึงหรือเปิดเผยถึงขอบเขตของการควบคุมเหล่านั้น (*Bangkok Post*, 2022) ในขณะที่ข้อเท็จจริงบ่งชี้ว่า ตัวแสดงเหล่านี้มีความเข้าใจกระบวนการทำงานของชุดความคิดข้างต้นจากข้อเท็จจริงเบื้องต้นเรื่อง การกำกับดูแลด้านข้อมูลและการคัดกรองข้อมูล จึงอาจตั้งข้อสังเกตได้ว่า ตัว

กระทำการเหล่านี้ มีเจตนาไม่อ้างถึงคำสำคัญดังกล่าว เพื่อเลี่ยงข้อท้าทายในประเด็นเรื่องสิทธิมนุษยชนและการปิดกั้นเสรีภาพในการเสพข้อมูลในพื้นที่ไซเบอร์ ซึ่งเป็นคำตอบว่า ผู้ประกอบการเชิงปทัสถานที่เป็นภาครัฐเลือกรับและไม่เลือกรับ หรือในบริบทเช่นนี้อาจตีความได้ว่า ประเด็นที่ตัวกระทำการเหล่านั้นไม่เลือกรับได้ถูกเบี่ยงเบน (distract) มากกว่าจะเป็นการบิดเบือนความเป็นจริงจากการตีความ (misrepresentation)

**ตัวกระทำการที่เป็นหน่วยงานภาคเอกชน**

ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชน[1] มีจุดร่วมทางความคิดประการสำคัญในเรื่องอธิปไตยทางไซเบอร์ในลักษณะใกล้เคียงกับผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงองค์กรรัฐ โดยเฉพาะอย่างยิ่งเมื่อกล่าวถึง การถูกละเมิดข้อมูลทางไซเบอร์ ตัวกระทำการทั้งสองกลุ่มมีความเห็นที่สอดคล้องกันว่า ปัจจุบันอธิปไตยทางไซเบอร์ของไทยถูกละเมิดอยู่ตลอดเวลา (ที่ปรึกษาด้านเทคโนโลยี องค์กรเอกชน, การสื่อสารส่วนบุคคล, 2565) ดังนั้น ในส่วนนี้จะอภิปรายในประเด็นอื่นซึ่งมีความน่าสนใจแตกต่างออกไป ดังนี้

จากการศึกษาพบว่า นอกเหนือจากความคล้ายคลึงกันทางความคิดเรื่องอธิปไตยทางไซเบอร์ระหว่างภาครัฐและภาคเอกชนแล้วนั้น สิ่งสำคัญอย่างมากสำหรับผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชน คือ ความเชื่อมั่นที่ได้รับจากผู้รับบริการ อีกนัยหนึ่ง ภาพลักษณ์และชื่อเสียงขององค์กรเป็นปัจจัยสำคัญในการแพร่กระจายปทัสถาน กล่าวคือ ตัวกระทำการที่เป็นภาคเอกชนจะเลี่ยงไม่ให้เกิดสิ่งกระทบต่อภาพลักษณ์ขององค์กรเป็นสำคัญ โดยทั่วไปแล้วการยกระดับศักยภาพขององค์กรเพื่อลดปัญหาเรื่องการละเมิดความเป็นส่วนตัวด้านข้อมูลเป็นสิ่งที่ชัดเจนและตรวจสอบได้ ในขณะที่การรักษาภาพลักษณ์ หรือการป้องกันไม่ให้ข้อเท็จจริงที่ว่าองค์กรมีความเปราะบางด้านการรักษาความปลอดภัยด้านข้อมูลอยู่ ตัวกระทำการจึงมักทำการปกปิดหรือบิดเบือนความเป็นจริง (บทสัมภาษณ์วิศวกรฝ่ายจัดการระบบ หน่วยงานผู้ให้บริการอินเทอร์เน็ต) ดังเช่นกรณีที่เกิดจากความคลุมเครือของการแถลงจุดยืนของบริษัท เช่น กรณีข้อมูลรั่วไหลจากบริษัทผู้ให้บริการด้านอินเทอร์เน็ตอย่าง AIS ซึ่งอ้างถึงการถูกบุกรุกข้อมูลโดยระบบภายนอก Ransomware มากกว่าเป็นความผิดพลาดจากบุคคลของบริษัท (*คมชัดลึกออนไลน์,* 2565) สอดคล้องกับ Deitelhoffและ Wolf (2013) ซึ่งได้อธิบายในลักษณะเดียวกันว่า ผู้ประกอบการเชิงปทัสถานในลักษณะองค์กรมักถูกผลักดันให้ตัดสินใจโดยชุดความคิดพื้นฐานเพื่อผลประโยชน์ทางธุรกิจ โดยใช้เครื่องมือต่าง ๆ เพื่อตีความใหม่ให้สอดคล้องกับเป้าหมายทางธุรกิจและสร้างความชอบธรรมให้กับกิจกรรมทางธุรกิจเหล่านั้น

[1] ผู้ประกอบการเชิงปทัสถานทางไซเบอร์ที่เป็นตัวแสดงภาคเอกชนในงานชิ้นนี้ หมายถึง ผู้ให้บริการด้านอินเทอร์และผู้ให้บริการด้านคำปรึกษาทางธุรกิจโดยเฉพาะด้านเทคโนโลยี

อย่างไรก็ดี ความพยายามในการตีความใหม่ (re-interpretation) เพื่อให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจเป็นสิ่งที่เกิดขึ้นอยู่เสมอในตัวกระทำการภาคเอกชน ความแตกต่างสำคัญระหว่างการใช้เครื่องมือดังกล่าวของผู้ประกอบการที่เป็นภาครัฐและเอกชน คือ ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชนจะนำเสนอชุดความคิดในลักษณะที่เป็นการปฏิบัติร่วม (co-regulation) รูปแบบซึ่งรัฐและองค์กรเอกชนที่มีส่วนเกี่ยวข้องในเครือข่ายทางไซเบอร์มีปฏิสัมพันธ์กันเพื่อสร้างระบบในการกำกับดูแลพื้นที่ไซเบอร์ (Bossong & Wagner, 2017) เพื่อสร้างความสมดุลทางอำนาจในการกำหนดระเบียบข้อตกลงในการจัดสรรอำนาจหน้าที่ในพื้นที่ไซเบอร์ ในทางปฏิบัติอาจหมายถึง การกำหนดองค์กรที่เป็นเอกชนในการเป็นกลไกกำกับดูแลพื้นที่ไซเบอร์ เช่นเดียวกับที่ปรากฏในเอกสารนโยบายและแผนของหน่วยงาน (ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฯ, 2564, น. 8) ควบคู่ไปกับการกำกับดูแลโดยหน่วยงานภาครัฐ (ประกาศคณะกรรมการการรักษาความมั่งคงปลอดภัยไซเบอร์ฯ, 2564, น. 14) ซึ่งแน่นอนว่าหลายสิ่งนั้นรัฐไม่อาจทำได้ แม้ว่าตัวกระทำการที่เป็นองค์กรรัฐจะมีความชอบธรรมตามกฎหมาย แต่ความสามารถความเชี่ยวชาญและการควบคุมมักอยู่ในระบบการทำงานของภาคเอกชน (Etzioni, 2011) ซึ่งเป็นข้อได้เปรียบเชิงโครงสร้างในพื้นที่ไซเบอร์ กล่าวอีกนัยหนึ่ง ตัวแสดงที่เป็นภาครัฐมีเครื่องมือในการอ้างความชอบธรรมในการแพร่กระจายปทัสถานในเชิงกฎหมาย ส่วนตัวแสดงที่เป็นภาคเอกชนมีเครื่องมือในลักษณะของการเป็นผู้ให้เชี่ยวชาญ หรือผู้ให้บริการโดยตรง เช่น ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชนสามารถกล่าวอ้างความชอบธรรมในฐานะผู้เชี่ยวชาญทางอินเทอร์เน็ต หรือผู้เชี่ยวชาญเฉพาะทางที่เกี่ยวข้องในฐานะผู้สร้างสถาปัตยกรรมทางอินเทอร์เน็ตเพื่อบิดเบือนข้อเท็จจริงด้านความมั่นคง ดังอาจสังเกตได้จากเหตุการณ์ต่อต้านแอปพลิเคชัน TikTok ในแคนาดา แม้กรณีนี้อาจไม่ปรากฏขึ้นในไทย แต่ลักษณะของการอ้างความมั่นคงในการไม่ยอมรับการใช้งานแอปพลิเคชันดังกล่าวในแคนาดาอาจเป็นกรณีเทียบเคียงที่สำคัญว่า อาจเกิดการกล่าวอ้างในลักษณะเดียวกันนี้กับตัวแสดงของไทยได้เช่นเดียวกัน (*ไทยรัฐออนไลน์*, 2566) กล่าวคือ ปัญหาทางเทคนิคที่เกี่ยวข้องกับความมั่นคง โดยเฉพาะอย่างยิ่งความเสี่ยงที่อาจเกิดขึ้นกับโครงสร้างในพื้นที่ ไซเบอร์ซึ่งไม่สามารถพิสูจน์ได้ความรู้เพียงเล็กน้อย ทำให้อำนาจในการกำหนดความถูกต้องตกอยู่ในมือของตัวกระทำการเหล่านั้นและตัวกระทำการที่เป็นผู้เชี่ยวชาญเหล่านั้นท้ายที่สุดมักกระทำไปเพื่อบรรลุผลลัพธ์ทางธุรกิจ

ดังนั้น จึงเป็นเรื่องไม่น่าแปลกใจที่ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชน จะนำเสนอแนวคิดซึ่งรักษาอำนาจของตนในพื้นที่ไซเบอร์ไว้ ทั้งนี้ อาจตั้งข้อสังเกตได้ว่า ความเข้าใจเชิงปทัสถานเรื่องอธิปไตยทางไซเบอร์ที่ตัวกระทำการที่เป็นภาคเอกชนที่ถูกกล่าวไว้ในตอนต้นว่า มีความเข้าใจสอดคล้องกับผู้ประกอบการเชิงปทัสถานที่เป็นหน่วยงานรัฐ ซึ่งปทัสถานด้านอธิปไตยในลักษณะเช่นว่านั้น ผลลัพธ์ในทางปฏิบัติ คือ การเพิ่มอำนาจของตัวแสดงซึ่งมีอำนาจอธิปไตย ซึ่งหมายถึง รัฐ

ชาติ ดังนั้นแล้ว จึงดูเหมือนจะเป็นสิ่งย้อนแย้งกับชุดความคิดของตัวกระทำการที่เป็นภาคเอกชนว่าการกำกับร่วมกันเป็นกลไกที่สำคัญ ทั้งนี้ ผู้เขียนได้ข้อสรุปว่า ตัวกระทำการภาคเอกชนมักตัดสินใจบนพื้นฐานทางธุรกิจดังที่กล่าวไว้ในตอนต้น เพื่อไม่ให้เกิดความขัดแย้งระหว่างภาครัฐและเอกชน จึงปรากฏบ่อยครั้งว่า ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชน โดยเฉพาะอย่างยิ่งผู้ให้คำปรึกษาด้านเทคโนโลยีจะมีกระบวนการดัดแปลง (modify) เพื่อบิดเบือนความเป็นจริงทางปทัสถานที่กำลังเสนอสู่ตัวแสดงที่ทางธุรกิจเรียกว่า “ลูกค้า” เพื่อให้บรรลุผลลัพธ์ทางธุรกิจ จึงเป็นเรื่องปกติที่ผู้ให้บริการจะดัดแปลง “สินค้า” เพื่อให้สอดคล้องกับความต้องการของลูกค้าเหล่านั้น ซึ่งเป็นข้อบ่งชี้ว่า ผู้ประกอบการเชิงปทัสถานจะรับหรือเลือกรับปทัสถานทางไซเบอร์ของจีนในลักษณะใดนั้นขึ้นอยู่กับผลลัพธ์ทางธุรกิจและความต้องการของลูกค้าเป็นหลัก

ตัวอย่างเพื่อให้สอดคล้องกับคำอธิบายเรื่อง อธิปไตยทางไซเบอร์ เช่น หน่วยงานด้านความมั่นคงของรัฐมีฐานะเป็น ‘ลูกค้า’ ซึ่งมารับบริการด้านคำปรึกษาด้านเทคโนโลยี ผู้ให้บริการด้านคำปรึกษาในฐานะผู้ขายเพื่อให้บรรลุผลลัพธ์ทางธุรกิจ ซึ่งอาจกล่าวได้ว่า เพื่อให้สามารถขายสินค้าได้ ผู้ขายจึงมักใช้กระบวนการโน้มน้าวด้วยการดัดแปลงอัตลักษณ์ของสินค้า ในสถานการณ์ที่สามารถเข้าใจได้ง่ายอื่น ๆ เช่น เมื่อผู้ซื้อต้องการซื้อสินค้าในราคาถูกจึงต่อรองราคาสินค้าส่งผลให้กระบวนการคิดของผู้ขายจำเป็นต้องคิดใหม่เพื่อกำหนดราคาที่เหมาะสมเพื่อให้สินค้าสามารถสร้างความพึงพอใจแก่ลูกค้าได้ เป็นต้น (ที่ปรึกษาด้านเทคโนโลยี องค์กรเอกชน, การสื่อสารส่วนบุคคล, 2565)

อย่างไรก็ตาม จากการศึกษาชี้ให้เห็นว่าไม่สามารถสร้างข้อสรุปแบบเหมารวมได้ว่า ตัวกระทำการในระดับปัจเจกหรือผู้เชี่ยวชาญเหล่านั้นมีกระบวนการคิดในลักษณะที่สอดคล้องกับองค์กรเพียงอย่างเดียว ผู้เชี่ยวชาญเหล่านั้นบ่อยครั้งมีชุดความคิดซึ่งแตกต่างไปจากผลลัพธ์ในตอนท้ายของธุรกิจ ดังนั้น การศึกษาความพยายามในการแพร่กระจายปทัสถานทางไซเบอร์ของผู้ประกอบการเชิงปทัสถานในลักษณะปัจเจก จึงมีความจำเป็นต่อการทำความเข้าใจทรรศนะด้านความมั่นคงไซเบอร์ของไทย ซึ่งจะอธิบายในส่วนต่อไป



**ตัวกระทำการที่เป็นปัจเจกในฐานะผู้เชี่ยวชาญ**

ผู้ประกอบการเชิงปทัสถานในบทบาทผู้เชี่ยวชาญโดยทั่วไปแล้วอาจถูกพิจารณาว่า เป็นส่วนหนึ่งของตัวแสดงในระดับเดียวกับองค์กรภาคเอกชน หรือรัฐบาล ดังนั้น ผู้เขียนจึงใคร่ย้ำอีกครั้งว่า ตัวกระทำการในฐานะผู้เชี่ยวชาญในส่วนนี้จะพิจารณาตัวกระทำการเหล่านั้นในระดับ “ปัจเจก” เป็นการเฉพาะ ซึ่งหมายถึง ทรรศนะของผู้เชี่ยวชาญในนามบุคคล ไม่ใช่ในนามขององค์กรหรือหน่วยงานแต่อย่างใด แม้ว่าในความเป็นจริงบ่อยครั้งที่ผลลัพธ์จะนำไปสู่ข้อสรุปที่ว่า ผู้เชี่ยวชาญเหล่านั้นแพร่กระจายปทัสถานเพื่อให้สอดคล้องกับผลลัพธ์ขององค์กร อย่างไรก็ตาม ผู้เขียนต้องการเสนอว่า

ทรรศนะเหล่านั้นของตัวกระทำการในระดับนี้มีผลสำคัญต่อกระบวนการนำเอาปทัสถานจากภายนอกเข้ามาปฏิบัติภายในประเทศและเพื่อชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสถานที่เป็นผู้เชี่ยวชาญแต่ละรายมีเป้าหมายและการใช้เครื่องมือที่แตกต่างกันเพื่อสร้างการสนับสนุนวิสัยทัศน์ด้านความมั่นคงไซเบอร์ให้เกิดจุดเปลี่ยน (tipping point) หลังจากที่ปทัสถานบางอย่างเริ่มแพร่กระจาย (Finnemore & Sikkink, 1998)

หนึ่งในผู้ศึกษาด้านความมั่นคงได้เสนอแนวคิดที่ว่า ตัวกระทำการทางไซเบอร์ที่สำคัญและมีอำนาจที่สุดหาใช่รัฐแต่คือ ผู้เชี่ยวชาญ (expert) (Boyle, 1997) นักวิชาการด้านกฎหมายความมั่นคงไซเบอร์ของไทย อธิบายว่า ชุดความคิดในลักษณะนี้เกิดจากมุมมองในรูปแบบที่มีเทคโนโลยีเป็นตัวกำหนด (technology determinism) ซึ่งมองว่า ผู้ที่มีอำนาจในพื้นที่ไซเบอร์แท้จริงแล้วเป็นผู้สร้างและผู้เขียนโปรแกรม อาจกล่าวอีกนัยหนึ่งว่า เป็นวิศวกร หรือช่างเทคนิคที่มีความชำนาญในการออกแบบสถาปัตยกรรมทางอินเทอร์เน็ต (internet architecture) (ทศพล ทรรศนกุลพันธ์, 2558) เนื่องจากโครงสร้างและสิ่งแวดล้อมที่เป็นองค์ประกอบภายในของพื้นที่ไซเบอร์เกิดจากการเขียนรหัสดิจิทัลเป็นการหมุนเวียนของข้อมูลและระบบปฏิบัติการ หากเปรียบรหัสดิจิทัลเหล่านี้เป็นดังภาษาในพื้นที่ไซเบอร์ ในโลกความเป็นจริงคงไม่ต่างกับภาษาที่เป็นเครื่องมือสำคัญในการกำหนดกฎเกณฑ์ ดังเช่นเหตุการณ์ที่เกิดขึ้นในเรื่องการติดตามอาชญากรรมทางไซเบอร์ในไทยโดยเฉพาะอย่างยิ่งกรณีของเว็บพนัน ซึ่ง “ตำรวจไซเบอร์” หน่วยงานตำรวจของไทยที่ถูกเรียกเช่นนั้นเพื่อแสดงให้เห็นถึงบทบาทในการกำกับดูแลความมั่นคงไซเบอร์ไม่มีศักยภาพเพียงพอที่จะดำเนินการใด ๆ กับกรณีดังกล่าวในปัจจุบัน เนื่องจากอาชญากรรมในพื้นที่ไซเบอร์นั้นมักเกิดขึ้นในพื้นที่นอกราชอาณาจักรหรือเขตแดนของไทย (*เดลินิวส์ ออนไลน์*, 2565) ดังนั้น จึงเป็นเรื่องยากที่จะติดตามอาชญากรรมทางไซเบอร์เมื่อเหตุเกิดขึ้นข้ามพรมแดน โดยเฉพาะอย่างยิ่งต่างเขตอำนาจศาล ซึ่งในปัจจุบันอำนาจทางกฎหมายในพื้นที่ไซเบอร์ยังคงเป็นที่ถกเถียงอยู่ ส่งผลให้ ผู้ใดก็ตามที่สามารถควบคุม สอดส่องการเคลื่อนไหวของข้อมูล คือ ผู้มีอำนาจและผู้ที่สามารถวางระบบเพื่อกรองและติดตามการเคลื่อนไหวข้อมูลเหล่านั้น คือ ผู้มีอำนาจแท้จริง (Lessig, 1998)

จากการศึกษาพบว่า ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงในลักษณะผู้เชี่ยวชาญได้โน้มน้าวตัวแสดงอื่นในบทบาทแบบปัจเจกบ่อยครั้งล้มเหลว ซึ่งในท้ายที่สุดผลลัพธ์ของการโน้มน้าวเหล่านั้นจะแตกต่างไปจากจุดเริ่มต้นที่ผู้เชี่ยวชาญเหล่านั้นเสนอ เช่น หนึ่งในผู้เชี่ยวชาญด้านเทคโนโลยีให้ข้อมูลว่า “...โดยทั่วไปแล้ววิศวกร หรือทีมวิจัยที่ศึกษาทางเทคโนโลยีและความมั่นคงมักรู้ถึงความเสี่ยงของเครือข่ายและช่องโหว่อยู่แต่แรกแล้ว... แต่สุดท้ายก็ต้องยอมทำตามเงื่อนไขที่เป็นความเสี่ยงพวกนั้นของลูกค้าหรือบริษัท เพราะไม่อย่างนั้น งานจะไม่สามารถดำเนินต่อไปได้...” (วิศวกรฝ่ายจัดการระบบ หน่วยงานผู้ให้บริการอินเทอร์เน็ต, การสื่อสารส่วนบุคคล, 2565)

กล่าวเพิ่มเติมในสถานการณ์ของการให้คำปรึกษาด้านกฎหมายหน่วยงานความมั่นคงของรัฐ ซึ่งมีบทบาทสำคัญในการกำหนดนโยบายด้านความมั่นคงไซเบอร์ของไทยว่า ช่องโหว่ของกฎหมายซึ่งอิงแอบหลักอธิปไตยที่ระบุเขตแดนได้นั้นในพื้นที่ไซเบอร์แทบเป็นไปไม่ได้เลยที่จะระบุสถานที่ตั้งของผู้กระทำผิด กล่าวคือ เมื่อกฎหมายไทยห้ามกระทำการบางอย่างซึ่งละเมิดต่อความมั่นคงของประเทศ โจทย์สำคัญที่ตามมา คือ จะทำอย่างไรเมื่อผู้ละเมิดนั้นดำเนินกิจกรรมภายในประเทศไทยแต่ใช้สิ่งที่เรียกว่า ตัวตนสมมติ หรือเครือข่ายเสมือน (Virtual Private Network: VPN) ส่งผลให้เสมือนว่าเขาดำเนินกิจกรรมเหล่านั้นเกิดขึ้นในพื้นที่ทางไซเบอร์จากต่างประเทศ หรือที่ใดก็ได้บนโลกกายภาพ (Teendifferent, 2023) ตัวอย่างเช่นว่านี้ ถูกตัวแสดงที่มีสถานะเป็นดัง “ลูกค้า” ตามคำอธิบายเช่นเดียวกับตัวกระทำการในลักษณะธุรกิจภาคเอกชน ส่งผลให้ผู้เชี่ยวชาญเหล่านี้มักเกิดกระบวนการลดทอน ปรับปรุง (modify) และโดยเฉพาะอย่างยิ่งเมื่อลูกค้าเหล่านั้นเป็นตัวกระทำการที่สำคัญในลักษณะองค์กรรัฐ

ในขณะที่องค์กรภาครัฐมักใช้เครื่องมือในการทำความเข้าใจปทัสถานในลักษณะที่การทำความเข้าใจเชิงโครงสร้าง ซึ่งเป็นการทำความเข้าใจเชิงตรรกะที่ยึดโยงกับคำอธิบายปทัสถานที่มีอยู่เดิมในสังคม ส่งผลให้ในท้ายที่สุด ผู้เชี่ยวชาญอาจไม่สามารถโน้มน้าวปทัสถานความมั่นคงไซเบอร์ต่อตัวกระทำการที่เป็นลูกค้าเหล่านั้นยอมรับปทัสถานใด ๆ ได้อย่างตรงไปตรงมา หรืออาจถูกใช้ในทางที่ผิด (misuse) เพื่อสนับสนุนความชอบธรรมทางความคิดเชิงปทัสถานในลักษณะที่กล่าวอ้างถึงศีลธรรม (moral claim) และความถูกต้องเพื่อบิดเบือนความเป็นจริง เช่น การกล่าวอ้างความถูกต้องอันสมควรในการป้องกันประเทศประเทศด้วยวิธีการซึ่งขัดต่อหลักการหรือปทัสถานอื่น ๆ โดยเฉพาะอย่างยิ่งสิทธิมนุษยชน การปิดกั้น การคัดกรองและการควบคุมเสรีภาพในการรับข้อมูลของประชาชน ดังเช่นที่เกิดขึ้นเมื่อไม่กี่ปีมานี้นับตั้งแต่กระแสเสรีประชาธิปไตยตื่นตัวในไทยโดยเฉพาะในเรื่องการเมือง ปี 2019 คือหนึ่งในตัวอย่างสำคัญซึ่งมีการตีความพระราชบัญญัติความมั่นคงไซเบอร์ฯ เพื่อผลประโยชน์ทางการเมือง (สฤณี ทอาชวานันกุล, 2562) ซึ่งเป็นตัวอย่างที่ชัดเจนสำหรับประเด็นนี้

นอกจากนี้ ผู้ประกอบการเชิงปทัสถานที่เป็นผู้เชี่ยวชาญเทคนิค คือ ตัวกระทำการทางไซเบอร์ที่มีบทบาทในการแพร่กระจายปทัสถานทางไซเบอร์ของจีนที่แยบยลที่สุด ดังที่ได้กล่าวไว้ข้างต้น ผู้เชี่ยวชาญจะแพร่กระจายปทัสถานโดยการโน้มน้าวทางเทคนิคให้เกิดการยอมรับปทัสถาน เช่น การเตือนถึงความเสี่ยงของผลิตภัณฑ์เพื่อให้ผู้ใช้บริการตระหนักถึงความเสี่ยง คำแนะนำถึงความเสี่ยงของการติดตั้งระบบขององค์กร (วิศวกรฝ่ายจัดการระบบ หน่วยงานผู้ให้บริการอินเทอร์เน็ต, การสื่อสารส่วนบุคคล, 2565) เป็นต้น การโน้มน้าวเหล่านี้หากพิจารณาความสำเร็จของการแพร่กระจายปทัสถานโดยทั่วไป การศึกษาอาจจบลงที่การยอมทำตามข้อแนะนำของผู้เชี่ยวชาญ อย่างไรก็ตามมุมมองเช่นนี้อาจเป็นเพียงมุมมองที่ตื้นเขิน ดังที่ได้ Lessig (1998) กล่าวไว้ว่า ผู้ที่สามารถวางระบบ

ในพื้นที่ไซเบอร์ได้นั้น คือ ตัวกระทำการที่มีอำนาจมากที่สุดในพื้นที่ไซเบอร์ ซึ่งข้อถกเถียงเช่นนี้สะท้อนนัยสำคัญบางประการที่เป็นลักษณะสำคัญของยุทธศาสตร์ของจีน โดยเฉพาะเรื่อง การที่โครงการจะต้องใช้ทรัพยากรบุคคลที่มีความชำนาญจากจีนเป็นหลัก (Chandran, 2018)

ผู้เชี่ยวชาญสามารถถูกพิจารณาได้ว่า แพร่กระจายปทัสถานสำเร็จในลักษณะของการยัดเยียดปทัสถานสู่เป้าหมายได้และมีนัยสำคัญอย่างยิ่งต่อการแพร่กระจายปทัสถานทางไซเบอร์ของจีน เนื่องจากภาษาในพื้นที่ไซเบอร์ หรือชุดรหัสเป็นภาษาเฉพาะที่ตรวจสอบได้ยากหากขาดความชำนาญในลักษณะเดียวกัน วิศวกรระบบสามารถใส่ชุดรหัสป้องกัน หรือแม้แต่คำสั่งการล้วงข้อมูลในระบบประตูหลัง (backdoor) เพื่อเข้าถึงข้อมูลเฉพาะ ดังกรณีที่เกิดขึ้นในที่เกิดขึ้นในสหรัฐฯ ซึ่งถูกเปิดเผยโดย Edward Snowden ถึงการสอดส่องข้อมูลส่วนบุคคลโดยรัฐบาลสหรัฐฯ เมื่อปี 2013 (Macaskill & Dance, 2013) ซึ่งถือเป็นการล่วงล้ำข้อมูลทางเทคนิคที่แยบยลและตรวจสอบได้ยากหากปราศจากความรู้ความชำนาญ แม้ว่าในกรณีของประเทศไทยนั้นอาจจะยังไม่ปรากฏกรณีในลักษณะดังกล่าวขึ้น ทั้งนี้ อาจเนื่องจากตัวกระทำการของไทยในหลายระดับยังไม่มีขีดความสามารถเพียงพอในการตรวจสอบ หรือตรวจจับประเด็นเปราะบางดังกล่าวเช่นที่เกิดขึ้นในสหรัฐฯ แต่ก็ปรากฏบ่อยครั้งถึงการถูกบุกรุกเข้าสู่แหล่งข้อมูลของรัฐบาลหรือหน่วยงานอยู่เสมอ (พระจันทร์ เอียมซืน, 2565) สิ่งนี้เองดูเหมือนจะสอดคล้องกับข้อเท็จจริงของโครงการและยุทธศาสตร์ของจีนที่ในเรื่องการนำบุคลากรทางเทคนิคของตนมาใช้ในการดำเนินการซึ่งอาจนำไปสู่ประเด็นอ่อนไหวเมื่อข้อมูลที่อาจถูกละเมิดเหล่านั้นเป็นข้อมูลทางยุทธศาสตร์และภูมิศาสตร์ของประเทศ เช่นในกรณีของการขุดคลองคอคอดกระ (*Post Today,* 2563; Mathews, 2003) ด้วยเหตุนี้ ผู้เชี่ยวชาญทางเทคนิคของไทยจึงจำเป็นต้องพัฒนาทักษะเพื่อเตรียมรับมือกับเรื่องนี้



อย่างไรก็ตาม การแพร่กระจายเชิงปทัสถานทางเทคนิคในลักษณะข้างต้นในความเป็นจริงนั้นอาจเป็นเรื่องยากที่จะควบคุม เนื่องจากตัวแสดงจำนวนมากในไทยขาดความรู้และความเข้าใจอย่างแท้จริงต่อปทัสถานทางไซเบอร์ จึงอาจตกเป็นเหยื่อของการโน้มน้าวด้วยเครื่องมือของการบิดเบือนความเป็นจริง (misrepresenting) โดยผู้ประกอบการเชิงปทัสถานได้ เช่นในสถานการณ์ที่หน่วยงานความมั่นคงของรัฐแห่งหนึ่งต้องการติดตั้งระบบควบคุมความปลอดภัยของบริษัทเอกชน A โดยผู้เชี่ยวชาญทางเทคนิคของบริษัทนี้ได้เตือนถึงความเสี่ยงของการอาจถูกคุกคามทางไซเบอร์ได้ ดังนั้นจึงมีความจำเป็นต้องติดตั้งระบบเพื่อติดตามและป้องกันการเดินทางของข้อมูลเพื่อคัดกรองข้อมูล ซึ่งในความเป็นจริงนั้นหน่วยงานความมั่นคงของรัฐแห่งนั้นไม่อาจพิสูจน์ความโปร่งใสและความปลอดภัยของชุดระบบควบคุมความปลอดภัยและระบบคัดกรองเพื่อป้องกันตามคำเตือนของผู้เชี่ยวชาญได้เลยหากปราศจากความเชี่ยวชาญในลักษณะเดียวกัน เหตุการณ์ที่อาจเทียบเคียงในเชิงรูปธรรมและเคยเกิดขึ้นมาแล้ว คือ เหตุการณ์ซื้อเทคโนโลยีตรวจจับรถเบิดอัจฉริยะ GT 200 แต่ความเป็นจริงนั้นไม่

สามารถใช้งานได้จริง (*The Standard,* 2565) ซึ่งกรณีเทียบเคียงนี้นำคำถามสำคัญมาสู่สังคมไทยว่า งบประมาณจำนวนมากที่จะถูกใช้เป็นไปเพื่อการพัฒนาจริงหรือไม่ หน่วยงานที่ใช้รัฐบาลมีความรู้แท้จริงต่อการนำเข้าอุปกรณ์ทางเทคโนโลยี หรือในที่นี้อาจกล่าวในบริบทของการนำเข้าปทัสถานของจีนในการใช้อุปกรณ์ทางเทคโนโลยี ดังนั้น การติดตั้งกลไกป้องกันความเสี่ยงในลักษณะแพ็กเกจเป็นสิ่งที่จีนทำอยู่ จึงนำมาสู่คำถามสำคัญว่า ผู้ไม่รู้เหล่านั้นจะตรวจสอบภาษาทางไซเบอร์ได้อย่างไร

นอกจากนี้ จากบริบทดังกล่าวเมื่อพิจารณาร่วมกับเครื่องมือปกปิดตัวตนทางไซเบอร์ (VPN) คำถามเบื้องต้นที่สำคัญ คือ เจ้าหน้าที่ไทยจะบังคับใช้กฎหมายไทยได้หรือไม่และปัญหาจะทวีความซับซ้อนมากขึ้นเมื่อเป็นกรณีที่เกิดขึ้นในบางประเทศที่มีกฎหมายความมั่นคงไซเบอร์เข้มแข็ง จะสามารถบังคับใช้กฎหมายที่มีศักยภาพสูงเหล่านั้นภายในประเทศไทยได้หรือไม่ รัฐบาลไทย ผู้เชี่ยวชาญและตัวแสดงภาคเอกชนที่มีบทบาทในการกำกับดูแลพื้นที่ไซเบอร์ของไทยจะอนุญาตหรือไม่ เป็นอีกหนึ่งประเด็นสำคัญซึ่งยังไม่มีข้อสรุปในเวลานี้

**สรุปผลลัพธ์ของผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ของไทย**

ผู้ประกอบการเชิงปทัสถานในไทยใช้เครื่องมือที่แตกต่างในการโน้มน้าวตัวแสดงให้เกิดการคล้อยตามทางปทัสถานในสังคม ทั้งนี้ การศึกษานี้ชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสถานด้านไซเบอร์ของไทยต้องตระหนักถึงความสำคัญและใช้เครื่องมือในการนำปทัสถานมาปฏิบัติใช้ภายในประเทศอย่างรอบคอบเพื่อไม่ให้เกิดความขัดแย้งทางปทัสถาน กล่าวคือ เครื่องมือที่ตัวกระทำการเชิงปทัสถานเหล่านั้นใช้ในการสร้างความยอมรับปทัสถานทางไซเบอร์แบบจีนในสังคมไทยนั้น เกิดจากการตีความใหม่ (re-interpretation) จนบางครั้งอาจนำไปสู่การบิดเบือนความเป็นจริงจากการตีความ (misrepresentation) โดยการเชื่อมโยงกับปทัสถานเดิมที่มีอยู่แล้วในสังคมไทย เพื่อให้เกิดความเข้าใจที่ง่ายขึ้น ซึ่งในความเป็นจริงนั้นอาจเป็นการเพิ่มเงื่อนไขในการทำความเข้าใจและส่งผลต่อความเป็นจริงที่รัฐบาลจีนต้องการสื่อสารกับผู้รับปทัสถาน ดังนั้น จึงเป็นเรื่องสำคัญที่จะต้องมีการทำความเข้าใจเกี่ยวกับเป้าหมายและแรงจูงใจของผู้ประกอบการเชิงปทัสถาน เพื่อให้แน่ใจว่าการแพร่กระจายปทัสถานความมั่นคงไซเบอร์นั้นถูกต้อง หรือสอดคล้องกับปทัสถานใหม่ภายนอกประเทศหรือไม่

**ตารางที่ 1: ตารางสรุปเพื่อเปรียบเทียบผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ของไทย**

| ผู้ประกอบการเชิงปทัสถานของไทย | จุดสนใจ (focus) | เครื่องมือ (tools and tactics) | ผลลัพธ์ (outcome) |
|---|---|---|---|
| รัฐบาลและหน่วยงานภาครัฐ | อธิปไตย (Sovereignty) | การตีความใหม่ (reinterpretation) | 1) พื้นที่ไซเบอร์ถือเป็นเขตแดนของรัฐ รัฐจึงจำเป็นต้องกำกับดูแลเขตแดนของตนจะให้ใครละเมิดมิได้<br>2) อธิปไตยของรัฐชาติและอธิปทางไซเบอร์เป็นเรื่องเดียวกัน |
| | | การดัดแปลง (modification) | การใช้ปทัสถานที่มีอยู่ในลักษณะที่ไม่สอดคล้องกับเจตนาหรือวัตถุประสงค์ดั้งเดิมเพื่อโน้มน้าวตัวแสดงในรัฐ เช่น อ้างความชอบธรรมในการรักษาความสงบเรียบร้อยภายในรัฐ |
| | | การแสดงความมุ่งมั่น (showing commitment) | แสดงให้เห็นถึงความมุ่งมั่นต่อยุทธศาสตร์ที่เกี่ยวข้องกับจีน เช่น BRI, DSR เพื่อสร้างความน่าเชื่อถือในการสร้างความมั่นคงของรัฐ |
| องค์กรภาคเอกชน | เป้าหมายเชิงธุรกิจ (Business Alignment) | การตีความใหม่ (reinterpretation) | เชื่อมโยงปทัสถานไซเบอร์ของจีนกับปทัสถานที่มีอยู่ในประเทศไทย โดยเฉพาะความมั่นคง เช่น ระบบการเฝ้าระวังเพื่อรักษาความสงบเรียบร้อยและเสถียรภาพทางการเมือง |
| | | การดัดแปลง (modification) | 1) ปทัสถานถูกตัดทอนสาระบางอย่างเพื่อให้ตัวแสดงอื่นยอมรับ<br>2) ใช้ปทัสถานที่มีอยู่ในทางที่ผิดเพื่อสนับสนุนปทัสถานทางไซเบอร์ของจีน เช่น การอ้างแนวคิดอำนาจอธิปไตยทางไซเบอร์ในการรักษาความมั่นคงของราชอาณาจักร เพื่อเสนอต่อหน่วยงานของรัฐ |

| | | | |
|---|---|---|---|
| | | การแสดงความมุ่งมั่น (showing commitment) | แสดงนโยบายและตัวอย่างที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์และการละเมิดข้อมูลส่วนบุคคลเพื่อเน้นย้ำถึงความมุ่งมั่นและความสำคัญของปทัสถาน |
| ผู้เชี่ยวชาญ | หลากหลายประเด็นขึ้นอยู่กับความชำนาญเฉพาะบุคคล (technical expertise) | การบิดเบือนความจริง (misrepresentation) | บิดเบือนข้อเท็จจริงทางปทัสถานเพื่อผลประโยชน์อื่นใดอย่างแยบยล เช่น การติดต่อเครื่องมือสอดแนมข้อมูลแฝงไปกับระบบการควบคุมความปลอดภัยขององค์กร |
| | | การดัดแปลง (modification) | ตัดทอนสาระบางอย่างที่ตนสนับสนุนเพื่อให้เกิดการยอมรับ |

**ที่มา:** เรียบเรียงโดยผู้เขียน

กล่าวโดยสรุป ผู้ประกอบการเชิงปทัสถานทางไซเบอร์ที่เป็นรัฐบาลและหน่วยงานภาครัฐของไทยมีความเข้าใจเกี่ยวกับอำนาจอธิปไตยทางไซเบอร์ว่า อำนาจอธิปไตยทางไซเบอร์เป็นเรื่องของการกำหนดชะตากรรมของรัฐแบบเดียวกับอำนาจอธิปไตยของรัฐชาติ ด้วยเหตุนี้แนวทางในการกำกับดูแลความมั่นคงไซเบอร์นั้นสามารถทำได้โดยการตีความอธิปไตยไซเบอร์ให้สอดคล้องกับแนวคิดที่มีอยู่ของอำนาจอธิปไตยของชาติ แม้ว่าหน่วยงานความมั่นคงของรัฐจะมีข้อกังวลเกี่ยวกับความมั่นคงและภัยคุกคามทางไซเบอร์อยู่บ้าง แต่มุมมองเชิงบอกต่อปทัสถานด้านไซเบอร์ของจีนที่เผยแพร่ผ่านยุทธศาสตร์เส้นทางสายไหมดิจิทัล โดยพิจารณาว่าเป็นองค์ประกอบของการพัฒนาโครงสร้างพื้นฐานและความสัมพันธ์ทางการค้า

ในขณะเดียวกัน ผู้ประกอบการเชิงปทัสถานทางไซเบอร์ที่เป็นองค์กรเอกชน มีมุมมองด้านความมั่นคงไซเบอร์ที่สอดคล้องกับภาครัฐว่า ยุทธศาสตร์เส้นทางสายไหมดิจิทัลเป็นองค์ประกอบของการพัฒนาโครงสร้างพื้นฐานและความสัมพันธ์ทางการค้า แม้ว่าภาคเอกชนจะยอมรับและตระหนักว่าอธิปไตยทางไซเบอร์ของไทยกำลังถูกละเมิด แต่เพื่อหลีกเลี่ยงความขัดแย้งกับภาครัฐ องค์กรเอกชนอาจยอมรับปทัสถานทางไซเบอร์ของจีนตามผลลัพธ์ทางธุรกิจและความต้องการของลูกค้า โดยให้ความสำคัญกับภาพลักษณ์ขององค์กรโดยเฉพาะเรื่องการปกป้องความเป็นส่วนตัวของข้อมูล

อย่างไรก็ตาม ผู้ประกอบการเชิงปทัสถานทางไซเบอร์ที่เป็นผู้เชี่ยวชาญ อาจมีมุมมองด้านความมั่นคงไซเบอร์แตกต่างจากตัวแสดงอื่น ๆ เนื่องจาก ผู้เชี่ยวชาญมีความหลากหลายจึงเป็นเหตุให้มีมุมมองที่แตกต่างกันเกี่ยวกับยุทธศาสตร์เส้นทางสายไหมดิจิทัล แต่การโน้มน้าวใจของผู้เชี่ยวชาญ

อาจสอดคล้องกับผลลัพธ์และเป้าหมายขององค์กร ทั้งนี้จากการศึกษาชี้ว่า ผู้เชี่ยวชาญทางเทคนิคดูเหมือนจะมีความเข้าใจถึงเป้าหมายและวิสัยทัศน์ด้านอธิปไตยไซเบอร์มากที่สุด

# บทที่ 5

## สรุปและข้อเสนอแนะ

ข้อริเริ่มแถบและทางของจีนได้ขยายไปสู่ขอบเขตทางไซเบอร์ผ่านภายใต้ยุทธศาสตร์เส้นทางสายไหมดิจิทัล เพื่อขยายขีดความสามารถในการพึ่งพาตนเองของจีนในด้านวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม ยุทธศาสตร์ดังกล่าว ผลักดันให้ธุรกิจทางเทคโนโลยีสารสนเทศภายในของจีนเพื่อเน้นความสำคัญในการส่งออกควบคู่ไปกับยุทธศาสตร์เชิงโครงสร้างพื้นฐานระหว่างประเทศโดยมีรัฐบาลจีนเป็นผู้เกี่ยวข้องหลัก

จากการศึกษาชี้ให้เห็นว่า เทคโนโลยีของจีนมีบทบาทสำคัญทางเศรษฐกิจในหลายภูมิภาค โดยเฉพาะอย่างยิ่งในเอเชียใต้ เอเชียตะวันออกเฉียงใต้และแอฟริกา รัฐบาลจีนและบริษัทต่าง ๆ ลงทุนจำนวนมหาศาลกับธุรกิจด้านอีคอมเมิร์ซและธุรกรรมออนไลน์เพื่อสร้างรูปแบบพฤติกรรมที่ใช้ในชีวิตประจำวันอย่างแยบยล โดยเฉพาะเมื่อยุทธศาสตร์เส้นทางสายไหมดิจิทัลได้ยกระดับประสิทธิภาพของอุตสาหกรรมระดับภูมิภาคและระดับรากฐานในสังคมซึ่งเป็นพื้นที่ซึ่งคนทั่วไปในสังคมใช้งานอยู่ในพื้นที่ทางไซเบอร์ระดับนั้น ส่งผลให้เกิดการปลูกฝังชุดความคิดในการพึ่งพาทางเทคโนโลยีจีนสู่ระดับโครงสร้างอย่างมีนัยสำคัญ นอกจากนี้ บริษัทเอกชนโดยเฉพาะอย่างยิ่งผู้ให้บริการด้านแพลตฟอร์มทางอินเทอร์เน็ตจะเป็นหนึ่งในกุญแจสำคัญซึ่งทำให้ผู้คนในสังคมเชื่อมโยงกับเทคโนโลยีของจีน เนื่องจากรัฐบาลจีนสนับสนุนให้เกิดการใช้ปัญญาประดิษฐ์ในการเข้าถึงข้อมูลของผู้ใช้จำนวนมาก ประกอบกับบริบทของกลุ่มประเทศซึ่งเป็นเป้าหมายของยุทธศาสตร์จีนเป็นกลุ่มประเทศซึ่งตระหนักถึงภัยการเข้าถึงความเป็นส่วนตัวด้านของมูลของปัญญาประดิษฐ์เท่าไหร่นัก เมื่อเทียบกับ สังคมตะวันตกในเรื่องความกังวลเรื่องความเป็นส่วนตัวด้านข้อมูล ส่งผลให้ ในสังคมตะวันตกการนำปัญญาประดิษฐ์มาใช้ในพื้นที่ไซเบอร์ โดยเฉพาะ ในระดับผู้ใช้บริการ (application layer) เป็นเรื่องยาก ซึ่งสิ่งนี้จะทำให้จีนได้เปรียบในการใช้เทคโนโลยี

บริบทข้างต้นจะสนับสนุนให้จีนขยายขีดความสามารถในการวางตัวเป็นผู้กำหนดมาตรฐานทางเทคโนโลยีและดิจิทัลในลักษณะของจีนสู่ระดับสากล โดยเฉพาะอย่างยิ่งในแง่ของความเป็นส่วนตัวของข้อมูลและความมั่นคงไซเบอร์ จีนได้สร้างและพยายามแพร่กระจายปทัสถานเรื่องการบังคับใช้อำนาจในการกำกับดูแลข้อมูลโดยรัฐบาล ซึ่งรวมถึงมาตรฐานในการกำกับดูแลพื้นที่ไซเบอร์และการเข้าถึงข้อมูลส่วนตัวบุคคล ในขณะที่มาตรฐานระเบียบดังกล่าวของจีนถูกวิพากษ์วิจารณ์ถึงความเข้มงวดในการตรวจสอบข้อมูลข้ามชาติและการตีความกฎหมายความมั่นคงไซเบอร์ของจีนที่

คลุมเครือ จึงเกิดเป็นข้อท้าทายประการสำคัญสำหรับการแพร่กระจายปทัสถานทางไซเบอร์ของจีน ความทะเยอทะยานของรัฐบาลจีนในการวางตัวเป็นผู้กำหนดปทัสถานทางเทคโนโลยีและไซเบอร์ใหม่ปรากฏชัดเจนขึ้นเมื่อรัฐบาลจีนผลักดันข้อยุทธศาสตร์ทางไซเบอร์ของตนเข้าสู่ระดับองค์การระหว่างประเทศ เช่น สหภาพโทรคมนาคมระหว่างประเทศ (ITU) และการประชุมอินเทอร์เน็ตโลก (WIC) เป็นต้น

จากการศึกษาชี้ให้เห็นว่า บริษัทจีนที่ดำเนินงานอยู่ทั่วโลก คือ เครื่องมือสำคัญซึ่งทำให้จีนสามารถสร้างมาตรฐานในระดับสากลและควบคุมโครงสร้างพื้นฐานดิจิทัล กลไกการสร้างความร่วมมือกับบริษัทท้องถิ่นในตลาดเกิดใหม่จะทำให้จีนกลายเป็นผู้นำตลาดและได้ประโยชน์จากการผูกขาดและเกิดข้อได้เปรียบในการเข้าถึงสังคม ดังที่ผู้เขียนได้เน้นย้ำว่า โครงสร้างพื้นฐานดิจิทัลมีความสำคัญต่อการกำหนดตำแหน่งแห่งที่ของตัวเองในพื้นที่ไซเบอร์

อย่างไรก็ตาม ยุทธศาสตร์เส้นทางสายไหมของจีนได้นำมาซึ่งข้อกังวลเกี่ยวกับอำนาจอธิปไตยและความท้าทายทางเศรษฐกิจ จริยธรรมและความมั่นคง กล่าวคือ ปทัสถานทางดิจิทัลและไซเบอร์ของจีนนั้นสร้างความท้าทายต่อประชาคมระหว่างประเทศ เนื่องจาก ผลกระทบที่อาจเกิดขึ้นต่อประเด็นเรื่องอำนาจอธิปไตยของรัฐ หนึ่งในประเด็นสำคัญของปทัสถานด้านความมั่นคงไซเบอร์ของจีน คือ การกำกับดูแลพื้นที่ไซเบอร์ซึ่งให้ความสำคัญกับการเฝ้าระวังและการควบคุมด้านข้อมูลโดยรัฐบาลกลาง เช่นเดียวกับรัฐบาลจีนที่ใช้กฎระเบียบและกลไกในการตรวจสอบที่เข้มงวดเพื่อควบคุมข้อมูล โดยเฉพาะเพื่อกำจัดความขัดแย้งและเป้าหมายในการติดตามเพื่อผลประโยชน์ทางการเมือง ประเด็นเหล่านี้ถูกวิพากษ์จากผู้สังเกตการณ์ระหว่างประเทศจำนวนมาก ซึ่งการกำกับดูแลพื้นที่ไซเบอร์ในระดับเช่นนี้มีลักษณะที่สวนทางกับอุดมคติของการแสดงออกอย่างเสรีและการเข้าถึงข้อมูลที่เปิดกว้างซึ่งถือเป็นปทัสถานทางไซเบอร์ที่ประเทศต่าง ๆ ในปัจจุบันให้การยอมรับ

นอกจากนี้ การศึกษายังชี้ให้เห็นถึงมิติด้านความมั่นคงทางภูมิศาสตร์ภายในประเทศและการคุกคามต่อเสรีภาพทางความคิดและวัฒนธรรมอย่างมีนัยสำคัญ กล่าวคือ เมื่อเทคโนโลยีของจีนผสานเข้ากับโครงสร้างพื้นฐานทางกายภาพของประเทศอื่น ๆ มากขึ้น ประเทศเหล่านั้นจึงมีความจำเป็นที่จะต้องพึ่งพาบริษัทจีนมากขึ้นโดยเฉพาะอย่างยิ่งในการบำรุงรักษาเทคโนโลยีและโครงสร้างพื้นที่ฐานที่เกี่ยวข้องเหล่านั้น สิ่งนี้อาจสร้างความอ่อนไหวด้านความมั่นคงทางภูมิศาสตร์ได้ เนื่องจากบริษัทจีนจะสามารถเข้าถึงข้อมูลทางภูมิศาสตร์ที่ละเอียดอ่อน ซึ่งอาจนำไปใช้เพื่อวัตถุประสงค์ของตนเองได้ ในขณะเดียวกัน ความกังวลต่อการครอบงำทางวัฒนธรรมและอัตวิสัยส่วนบุคคลเป็นอีกหนึ่งประเด็นที่จำเป็นต้องให้ความสำคัญ การกล่อมเกลาพฤติกรรมของผู้ใช้งานผ่านการเข้าถึงอินเทอร์เน็ตและความ

เคยชินกับเทคโนโลยีที่หยั่งรากฐานอยู่ในสังคม จึงอาจสามารถครอบงำทางความคิดของผู้คนในประเทศอื่น ๆ โดยเฉพาะอย่างยิ่งในประเทศซึ่งจีนเป็นผู้บุกเบิกทางเทคโนโลยี ดังเช่นในแอฟริกา หรือประเทศกำลังพัฒนาโดยเฉพาะประเทศที่มีศักยภาพในการรับมือภัยคุกคามทางไซเบอร์ในระดับ การควบคุมในลักษณะนี้จึงพิจารณาได้ว่าเป็นภัยคุกคามต่อเสรีภาพส่วนบุคคลและความหลากหลายทางวัฒนธรรม

ปทัสถานทางเทคโนโลยีและความมั่นคงไซเบอร์ของจีนนั้น มีเป้าหมายหลักในประเทศโลกใต้และประเทศกำลังพัฒนา โดยเฉพาะอย่างยิ่ง เมื่อพิจารณาจากเส้นทางของข้อริเริ่มแถบและทาง รวมถึงเส้นทางสายไหมดิจิทัล จะพบว่า กลุ่มเป้าหมายหลักของยุทธศาสตร์ซึ่งดำเนินการได้อย่างรวดเร็ว คือ กลุ่มประเทศแอฟริกา เอเชียใต้และเอเชียตะวันออกเฉียงใต้ ซึ่งแสดงให้เห็นว่า ประเทศโลกใต้และประเทศกำลังพัฒนา ซึ่งเป็นกลุ่มประเทศที่มีความต้องการทางเทคโนโลยีและการพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ มีกำลังซื้อและโดยเฉพาะอย่างยิ่งในบางประเทศยังมีลักษณะการเมืองแบบอำนาจนิยมซึ่งสอดคล้องกับปทัสถานทางไซเบอร์ของจีนอย่างมีนัยสำคัญ ทั้งนี้ อัตราการเพิ่มขึ้นของการเข้าถึงอินเทอร์เน็ตและผู้ใช้งานอย่างรวดเร็วในประเทศที่ขาดความพร้อมในการรับภัยคุกคามทางไซเบอร์และมีความเข้าใจปทัสถานทางเทคโนโลยีและไซเบอร์ของจีนในระดับต่ำ อาจก่อให้เกิดปัญหา เช่น การฉ้อโกง การโจมตีทางไซเบอร์และการเผยแพร่ข้อมูล ดังนั้น การลดช่องว่างทางเทคโนโลยีและองค์ความรู้จึงเป็นสิ่งสำคัญอย่างยิ่งสำหรับประเทศเหล่านั้น

รัฐบาลจีนเชื่อว่า ปทัสถานทางไซเบอร์และการกำกับดูแลพื้นที่ไซเบอร์มีศักยภาพเพียงพอที่จะแพร่กระจายอิทธิพลของตนในเวทีโลก โดยเฉพาะอย่างยิ่งเพื่อเปลี่ยนผ่านสถานะจากการเป็นผู้ปฏิบัติตามกฎ (rule-taker) เป็นผู้กำหนดกฎเกณฑ์ (rule-maker) ทั้งนี้ ความท้าทายการแพร่กระจายปทัสถานทางไซเบอร์และความพยายามในการเป็นผู้กำหนดกฎเกณฑ์ของจีน คือ ปทัสถานทางไซเบอร์ที่ดำรงอยู่เดิมและประเด็นเรื่องอธิปไตยของรัฐ กล่าวคือ ปทัสถานทางไซเบอร์ของจีนซึ่งให้ความสำคัญกับอำนาจรัฐในการกำกับควบคุมพื้นที่ไซเบอร์นั้นขัดแย้งกับความเป็นจริงที่ว่า ปทัสถานการกำกับดูแลแบบผู้มีส่วนได้ส่วนเสียหลายฝ่าย (multistakeholder) เป็นปทัสถานซึ่งประชาคมระหว่างประเทศให้การยอมรับอยู่ในปัจจุบัน หรืออาจกล่าวอีกนัยหนึ่งว่า พื้นที่ไซเบอร์ในปัจจุบันได้ถูกกำกับดูแลโดยตัวกระทำการมากกว่า 1และตัวกระทำการเหล่านั้นไม่ได้กล่าวถึงอำนาจของรัฐเพียงอย่างเดียว

อย่างไรก็ตาม ปฏิเสธไม่ได้ว่ารัฐบาลจีนอย่างน้อยที่สุดประสบความสำเร็จในการสร้างการยอมรับทางเทคโนโลยีและการเสนอปทัสถานทางเลือก แม้ในความเป็นจริงนั้น ปทัสถานทางไซเบอร์

ของจีนอาจไม่ได้รับการยอมรับ หรือนำมาปฏิบัติใช้ภายในประเทศต้นทางอย่างชัดเจน แต่หลายประเทศไม่เพียงแต่ประเทศที่เป็นส่วนหนึ่งของข้อริเริ่มแทบและทาง หรือยุทธศาสตร์เส้นทางสายไหมดิจิทัลเท่านั้น แต่ยังหมายรวมถึงประเทศโลกเสรีและชาติตะวันตก เช่น สหราชอาณาจักร ญี่ปุ่น สิงคโปร์ ได้ยอมรับเทคโนโลยีของจีนมาใช้ภายในประเทศ

ในขณะเดียวกัน การแพร่กระจายปทัสถานทางไซเบอร์ของจีนนั้นนำมาซึ่งประเด็นท้าทายด้านความมั่นคงไซเบอร์ดังได้กล่าวไว้ในตอนต้นและเมื่อนำบริบทดังกล่าวมาพิจารณากับประเด็นด้านอธิปไตยของรัฐ ก่อให้เกิดโจทย์สำคัญว่า อธิปไตยของรัฐในพื้นที่ทางไซเบอร์นั้นมีขอบเขตเพียงใด ส่งผลให้จำเป็นอย่างยิ่งที่จะต้องประเมินตัวกระทำการที่สำคัญในภายในรัฐ โดยเฉพาะอย่างยิ่ง เมื่อคำถามเหล่านี้ตั้งอยู่บนสมมติฐานที่ว่า ตัวกระทำการภายในประเทศโดยเฉพาะอย่างยิ่งประเทศโลกใต้หรือประเทศกำลังพัฒนามักขาดความสามารถในการรับมือและความเข้าใจกับปทัสถานความมั่นคงไซเบอร์ ซึ่งทวีความซับซ้อนเมื่อปทัสถานทางไซเบอร์ของจีนนั้นเป็นปทัสถานใหม่ ดังนั้น ในฐานะที่ประเทศไทยเป็นหนึ่งในประเทศผู้มีส่วนได้ส่วนเสียในยุทธศาสตร์เส้นทางสายไหมดิจิทัลและมีลักษณะสอดคล้องกับกลุ่มเป้าหมายของการแพร่กระจายปทัสถานทางเทคโนโลยีและทางไซเบอร์ของจีน การทำความเข้าใจกระบวนการนำปทัสถานภายนอกเข้ามาปฏิบัติใช้ภายในประเทศ (norm internalization) ของตัวกระทำการในไทยในฐานะผู้ประกอบการเชิงปทัสถาน จึงเป็นสิ่งสำคัญสำหรับการพัฒนาความมั่นคงไซเบอร์ในกลุ่มประเทศเป้าหมายของจีน

ทั้งนี้ การยอมรับบรรทัดฐานความปลอดภัยทางไซเบอร์ในประเทศไทย เป็นส่วนหนึ่งของยุทธศาสตร์เส้นทางสายไหมดิจิทัลโดยมีผู้ประกอบการเชิงปทัสถานในไทยเป็นตัวกระทำการที่สำคัญในการสนับสนุนปทัสถานดังกล่าว ตัวแสดงภาครัฐ ภาคเอกชนและผู้เชี่ยวชาญทางเทคนิค ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและด้านความมั่นคง คือ ตัวกระทำการที่สำคัญที่สามารถมีอิทธิพลต่อการยอมรับและการเผยแพร่ปทัสถานด้านความมั่นคงไซเบอร์ ผู้เขียนต้องการชี้ให้เห็นว่า การวิเคราะห์ในระดับภายในด้วยสภาพแวดล้อมทางการเมือง วัฒนธรรม ความเชื่อ รวมถึงปทัสถานอื่นใดที่ดำรงอยู่ภายในประเทศมีส่วนสำคัญอย่างยิ่งต่อการรับนำปทัสถานภายนอกมาแพร่กระจายภายในประเทศ

ในขณะเดียวกัน ตัวกระทำการด้านไซเบอร์ที่สำคัญภายในไทยในฐานะผู้ประกอบการเชิงปทัสถานจะเลือกยอมรับและเบี่ยงเบนข้อโต้แย้งของปทัสถานภายนอกก่อนจะนำมาปรับใช้ ตัวกระทำการที่สำคัญ ได้แก่ 1) หน่วยงานภาครัฐ เช่น สำนักงานรักษาความมั่นคงไซเบอร์แห่งชาติ (สมช.) และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ซึ่งมีบทบาทสำคัญตามกฎหมายในการออกแบบนโยบายและแผนสำหรับการกำกับดูแลด้านความมั่นคงไซเบอร์ของประเทศ 2) ตัวกระทำการในระดับ

เอกชน ซึ่งหมายรวมถึงตัวแทนผู้บริหารและผู้นำในระดับองค์กรที่เกี่ยวข้องกับอุตสาหกรรมดิจิทัลในประเทศไทย สามารถมีบทบาทสำคัญในการกำหนดพฤติกรรมของตัวแสดงอื่น ๆ ในอุตสาหกรรมที่เกี่ยวกับดิจิทัลได้ ตัวแสดงเหล่านี้สามารถใช้อิทธิพลและเครือข่ายเพื่อส่งเสริมการยอมรับปทัสถานใหม่ของจีนที่เกี่ยวข้องกับการเชื่อมต่อทางดิจิทัลภายในประเทศ 3) ผู้เชี่ยวชาญด้านเทคนิค วิศวกร โดยเฉพาะอย่างยิ่งผู้ที่อยู่ในสาขาเทคโนโลยีสารสนเทศและอินเทอร์เน็ต ซึ่งมีส่วนสำคัญอย่างมากในฐานะผู้ซ่อมบำรุงและพัฒนาสถาปัตยกรรมทางอินเทอร์เน็ต

อย่างไรก็ตาม ปทัสถานทางไซเบอร์ในปัจจุบันยังคงเป็นเรื่องใหม่และยากต่อการจะจำกัดความให้ชัดเจนถึงขอบเขตของสิ่งที่เรียกว่า “ความมั่นคงในพื้นที่ไซเบอร์” ซึ่งช่องว่างทางปทัสถานเช่นนี้จะส่งผลต่อกระบวนการนำปทัสถานภายนอกมาปรับใช้ อาจกล่าวอีกนัยหนึ่งว่า เกิดช่องว่างของการตีความเชิงปทัสถานขึ้นระหว่างตัวแสดง สิ่งนี้จะนำมาซึ่งการไม่ลงรอยกันของการตีความและการนำไปใช้ เพื่อบรรลุผลลัพธ์ที่แตกต่างกัน ทั้งนี้ ผู้ประกอบการเชิงปทัสถานทางไซเบอร์ของไทยสามารถใช้เครื่องมือที่หลากหลายในการนำเอาปทัสถานภายนอกมาใช้ภายในประเทศ โดยทั่วไปแล้วผลลัพธ์ที่ชัดเจนที่สุดของผู้ประกอบการเชิงปทัสถาน คือ การโน้มน้าวให้ตัวแสดงอื่นในประเทศยอมรับปทัสถานซึ่งตนกำลังสนับสนุน (norm conformity) ในขณะเดียวกัน ผลลัพธ์ในอีกระดับซึ่งอาจจะง่ายและเกิดขึ้นก่อน คือ การคล้อยตามทางสังคมของตัวแสดง (social conformity) ดังเช่นที่การศึกษาชี้ให้เห็น ถึงการยอมรับเทคโนโลยีของจีนในชีวิตประจำวัน สิ่งนี้สนับสนุนข้อเสนอที่ว่ารัฐบาลจีนอย่างน้อยที่สุดประสบความสำเร็จในการสร้างความยอมรับทางเทคโนโลยีภายในสังคมแล้ว

อย่างไรก็ดี การศึกษาชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสถานไซเบอร์ของไทยขาดความเข้าใจโดยรวมเกี่ยวกับปัญหาด้านความมั่นคงในพื้นที่ไซเบอร์ โดยเฉพาะอย่างยิ่งปัญหาจากการครอบงำตัวกระทำการอื่น ๆ โดยเฉพาะ ตัวแสดงในฐานะผู้เชี่ยวชาญทางเทคนิค ซึ่งนำความคิดเห็นของผู้เชี่ยวชาญไปใช้ประโยชน์โดยเจตนาอื่นแอบแฝง ทั้งผลประโยชน์ทางการเมืองและการเพื่อสนับสนุนการแพร่กระจายปทัสถานของตัวเองในระดับอื่น ๆ ปรากฏการณ์เหล่านี้แสดงให้เห็นถึง การนำไปใช้ในทางที่ผิด (misuse) เพื่อบิดเบือนหรือเบี่ยงเบน (distract) ข้อเท็จจริงบางอย่างของผู้กระทำการ

กระบวนการนำปทัสถานภายนอกมาปฏิบัติใช้ภายในประเทศไทยเกี่ยวข้องกับการปรับปทัสถานให้เหมาะกับบริบทภายในประเทศ เช่น วัฒนธรรม สังคมและค่านิยมทางการเมือง เป็นต้น เพื่อให้ง่ายต่อการยอมรับการเปลี่ยนแปลง การศึกษาชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสถานที่เป็นตัวแสดงภาคเอกชนจะแบ่งปันชุดความคิดที่มีอยู่สอดคล้องกับตัวกระทำการในระดับหน่วยงานของรัฐเรื่องอธิปไตย เนื่องจาก ตัวกระทำการที่เป็นเอกชนมักมีกระบวนการตัดสินใจพื้นฐานเชิงธุรกิจ ซึ่งมี

วัตถุประสงค์ทางธุรกิจและเพื่อหลีกเลี่ยงความขัดแย้งที่อาจส่งผลต่อผลประโยชน์ขององค์กร ตัวกระทำการในระดับนี้จึงมักดัดแปลง (modify) ปทัสถานเพื่อให้สอดคล้องกับความพึงพอใจของตัวแสดงอื่นในฐานะลูกค้า

ด้วยเหตุนี้ ตัวแสดงเหล่านี้จึงเข้าใจถึงความสำคัญของการปรับปทัสถานให้เหมาะสมกับค่านิยมและความเชื่อตามบริบทของตนในแต่ละประเทศเพื่อให้ได้รับการยอมรับในวงกว้าง นอกจากนี้ กระบวนการนำปทัสถานมาปฏิบัติใช้ภายในประเทศยังเกี่ยวข้องกับการตีความร่วม (collective interpretation) และการดำเนินการตามปทัสถานที่ถูกแนะนำโดยตัวแสดงภายในรัฐ ดังนั้นการตีความที่แตกต่างกันอาจส่งผลให้เกิดความไม่สอดคล้องกันของการตีความผู้แพร่กระจายปทัสถานหนึ่งไปยังผู้แพร่ปทัสถานหนึ่ง โดยเฉพาะอย่างยิ่งเมื่อมีบริบททางคุณค่าและความเชื่อที่แตกต่างกัน ทั้งนี้ การศึกษาสรุปว่า ผู้ประกอบการเชิงปทัสถานภาคเอกชนในสังคมแบ่งปันแนวคิดและความเข้าใจที่สอดคล้องกับหน่วยงานของรัฐเกี่ยวกับอำนาจอธิปไตย

ในบริบทของยุทธศาสตร์เส้นทางสายไหมดิจิทัลในประเทศไทย ผู้ประกอบการเชิงปทัสถานสามารถใช้กระบวนการแปลปทัสถานใหม่ (reinterpretation) ปทัสถานเพื่อเชื่อมโยงปทัสถานทางไซเบอร์ของจีนกับปทัสถานที่มีอยู่ในประเทศไทยที่อาจไม่มีความเกี่ยวข้องโดยตรงกับประเด็นดังกล่าว ดังเช่น การเชื่อมโยงโอกาสทางไซเบอร์ของจีนเข้ากับแนวคิดในการสอดแนมของรัฐบาล หรือรักษาเสถียรภาพทางการเมือง หน่วยงานของรัฐหลายแห่งในประเทศไทยมักกล่าวถึงความจำเป็นของระบบเฝ้าระวังและความร่วมมือในการติดตั้งระบบสังเกตการณ์ดังกล่าวหากเกิดขึ้นจริง อย่างไรก็ตาม สิ่งสำคัญคือต้องเข้าใจว่ากระบวนการนำปทัสถานมาปรับใช้ภายในประเทศยังสามารถใช้ในทางที่แตกต่างได้ด้วยการบิดเบือนความจริง (misrepresentation) และการใช้ปทัสถานที่มีอยู่ในทางที่ผิด (misuse) เพื่อส่งเสริมปทัสถานทางไซเบอร์ใหม่ของจีน ซึ่งอาจส่งผลให้เกิดความขัดแย้งและการปฏิเสธการยอมรับจากผู้มีส่วนได้ส่วนเสีย หากผู้ประกอบการเชิงปทัสถานไม่ระมัดระวังในการใช้เครื่องมือดังกล่าว

ดังนั้น การกำกับดูแลร่วมกันจึงเป็นสิ่งสำคัญในการกำกับดูแลพื้นที่ไซเบอร์ เพื่อทำให้เกิดการถ่วงดุลอำนาจในการกำหนดกฎเกณฑ์และข้อบังคับในการจัดสรรทางอำนาจ โดยผู้ประกอบการเชิงปทัสถานสามารถมีบทบาทสำคัญในการกำหนดระเบียบ กฎเกณฑ์และแนวปฏิบัติในพื้นที่ไซเบอร์ ผลการศึกษาชี้ให้เห็นว่า ผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์ของไทยมีมุมมองเชิงบวกต่อยุทธศาสตร์เส้นทางสายไหมดิจิทัล หรืออย่างน้อยที่สุดเมื่อพิจารณาว่ายุทธศาสตร์ดังกล่าวเป็นองค์ประกอบของข้อริเริ่มแถบและทางของจีนซึ่งไทยมองว่ากรอบแนวคิดนี้มีความสำคัญอย่างยิ่งต่อการพัฒนาโครงสร้างพื้นฐานและการเชื่อมโยงตลาดไทยสู่ตลาดโลก

**ข้อเสนอแนะ**

ผู้เขียนมีข้อเสนอแนะบางประการเพื่อพัฒนาความเข้าใจและแก้ปัญหาความหมิ่นเหม่ทางความคิดระหว่างผู้ประกอบการเชิงปทัสถานด้วยกันเอง เพื่อสร้างความเป็นหนึ่ง (unity) ในการกำหนดกฎเกณฑ์เพื่อให้สอดคล้องกับปทัสถานความมั่นคงที่ไทยเลือกรับ ผ่านตัวแบบเพื่อสร้างความเข้าใจถึงผลลัพธ์ที่อาจนำมาซึ่งความเสี่ยงโดยเฉพาะอย่างยิ่ง ผลลัพธ์ที่เกิดจากการพัฒนาทางความคิดของรัฐซึ่งตื่นตัวต่อการพัฒนาด้านความมั่นคงไซเบอร์ในโลกตะวันตก ดังนี้

ประการแรก ปัญหาการตีความทางกฎหมายที่แตกต่างกันจากความร่วมมือในการสร้างความมั่นคงด้านข้อมูลส่วนบุคคล ซึ่งเป็นข้อบ่งชี้ว่า การตีความด้านอธิปไตยทางไซเบอร์ไม่อาจทำได้เพียงลำพัง อาจกล่าวอีกนัยได้ว่า เขตแดนทางไซเบอร์ไม่อาจเกิดขึ้นได้จริง

จากรายงานของ World Economic Forum (WEF) ระบุว่า กว่าร้อยละ 75 ของข้อมูลในโลกตะวันตกถูกเก็บไว้ควบคุมโดยองค์กรเอกชนโดยเฉพาะอย่างยิ่งสหรัฐฯ เป็นผู้ถือครอง (World Economic Forum, 2022) จากกรณีดังกล่าว ก่อให้เกิดความกังวลที่จะถูกชาติอื่นรุกล้ำข้อมูลภายในส่งผลให้เกิดกระแสการตื่นตัวเกี่ยวกับเรื่องอธิปไตยไซเบอร์อย่างมีนัยสำคัญ หนึ่งในเหตุการณ์สำคัญในเรื่องการรุกล้ำข้อมูลส่วนบุคคลที่เกิดขึ้น คือ Schrems II[2] กรณีซึ่งบุคคลหนึ่งถูกตัดสินโดยมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) ว่าข้อมูลส่วนบุคคลไม่ผ่านมาตรฐานการป้องกันข้อมูลส่วนบุคคล คดีดังกล่าวชี้ว่า ข้อมูลส่วนบุคคลของผู้เกี่ยวข้องถูกเข้าถึงโดยหน่วยงานของสหรัฐฯ จากคดีดังกล่าวส่งผลให้กรอบความร่วมมือร่วมด้านความมั่นคงด้านข้อมูลระหว่างสหรัฐฯ และยุโรป อาทิ หลักการ Safe Harborและ Privacy Shield ถูกยกเลิก (Morrow, 2020) ส่งผลให้ปัจจุบันบริษัทหลายแห่งของสหรัฐฯ รวมทั้งบริษัทขนาดใหญ่อย่าง Googleและ Facebook สูญเสียความน่าเชื่อถือในการปกป้องข้อมูลส่วนบุคคลของผู้ใช้บริการ (Privacy Shield Framework, 2023)

ซึ่งชี้ให้เห็นว่า อธิปไตยทางไซเบอร์มีความซับซ้อนและสามารถตีความได้หลากหลายกว่าอธิปไตยทางกายภาพเนื่องจากพื้นที่ไซเบอร์ยังคงเป็นที่ถกเถียงอยู่ว่ามีขอบเขตเพียงใด โดยเฉพาะอย่างยิ่ง เมื่อเครือข่ายข้อมูลในปัจจุบันถูกดำเนินการในระบบคลาวด์ (cloud) ซึ่งได้ขยายขอบเขตของ

[2] Schrems II คือ ชื่อคดีซึ่งถูกพิจารณาโดยศาลยุติธรรมยุโรป ตั้งตาม Maximillian Schrems เจ้าของคดีซึ่งยื่นฟ้องต่อศาลยุติธรรมยุโรปถึงการละเมิดข้อมูลส่วนตัวของเขาโดยหน่วยงานของสหรัฐฯ ส่งผลให้ในทางปฏิบัติส่งผลให้ไม่สามารถถ่ายโอนข้อมูลของพลเมืองยุโรปไปยังสหรัฐฯ ได้อีกต่อไปเนื่องจากมีการตัดสินว่าข้อมูลส่วนตัวเหล่านั้นไม่สามารถรับรองมาตรฐานความเป็นส่วนตัวตามกฎหมาย GDPR ของยุโรปกำหนดได้ อ่านเพิ่มเติมใน *Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*

พื้นที่ไซเบอร์ให้ซับซ้อนมากขึ้น ประเทศซึ่งมีความตื่นตัวด้านความมั่นคงไซเบอร์โดยเฉพาะอย่างยิ่งสหรัฐฯ ได้ออกกฎหมายว่าด้วยการกำหนดมาตรฐานและควบคุมข้อมูลในระบบ CLOUD (Clarifying Lawful Overseas Use of Data Act: CLOUD Act) อย่างไรก็ตาม ไม่มีทางใดที่จะรับประกันความปลอดภัยของข้อมูลส่วนบุคคลได้เนื่องจากอาจเกิดกรณีซึ่งหน่วยงานของรัฐบาลกลางสหรัฐฯ ออกหมายจับซึ่งโดยกฎหมายภายในของสหรัฐฯ สามารถบังคับให้ผู้เก็บข้อมูลส่วนบุคคลเหล่านั้น เช่น Google หรือ Facebook เปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับผู้ใช้ได้ตลอดเวลาโดยที่ไม่จำเป็นต้องขอการยินยอมจากผู้นั้น อนึ่ง เครือข่ายข้อมูลที่อยู่ในเครือข่ายคลาวด์ (cloud) โดยทั่วไปแล้วเพื่อความปลอดภัยของข้อมูล บริษัทผู้ให้บริการจัดการด้านข้อมูลเหล่านั้นจะมีลักษณะเป็นบริษัทบุคคลที่สาม (third party) ส่งผลให้บริษัทซึ่งเป็นที่ตั้งของผู้ให้บริการด้านการจัดการข้อมูลในระบบคลาวด์ (cloud) สามารถถูกบังคับให้เปิดเผยข้อมูลส่วนบุคคลได้ตลอดเวลาหากประเทศที่ตั้งบริษัทเหล่านั้นมีการบังคับให้เปิดเผยข้อมูลตามกฎหมายภายในประเทศที่ตั้งบริษัท

<u>ประการที่สอง</u> ความท้าทายด้านอธิปไตยไซเบอร์ไม่ใช่แค่เรื่องสถานที่ในการจัดเก็บข้อมูลเพียงอย่างเดียว แต่หมายรวมถึงคำถามว่า ใครมีสิทธิ์เข้าถึงข้อมูลเหล่านั้นได้และจะเข้าถึงข้อมูลอย่างถูกกฎหมายอย่างไร ด้วยเหตุนี้ กฎหมายหรือข้อกำหนดที่จะป้องกันข้อมูล จำเป็นต้องระบุมาตรการที่จำเป็นเพื่อป้องกันข้อมูลตามอำนาจอธิปไตยในระดับเดียวกับ “ประเทศต้นทาง” อาจเปรียบได้เหมือนกรณีกฎหมายระหว่างประเทศในหลักว่าด้วยเขตอำนาจศาล (jurisdiction) ตัวอย่าง เช่น กรณีในประมวลกฎหมายอาญาลักษณะที่ 1 หมวด 2 มาตรา 4 ว่าด้วยเรื่องการใช้กฎหมายอาญา “ผู้ใดกระทำผิดในราชอาณาจักร ต้องรับโทษตามกฎหมาย การกระทำความผิดในเรือไทยหรืออากาศยานไทย ไม่ว่าจะอยู่ ณ ที่ใด ให้ถือว่ากระทำผิดในราชอาณาจักร” (พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ. 2499, 2564) ซึ่งล้อกับกฎหมายระหว่างประเทศว่าด้วยหลักดินแดน (Territorial principle) (Perkins, 1971) เช่น เรือหรือยานบินพลเรือน ถือเป็นเขตแดนตามสัญชาติที่ยานบินหรือเรือถือ ส่งผลให้เมื่อความผิดที่เกิดขึ้นในเรือหรือยานบินนั้นถือเป็นความผิดในเขตแดนทำให้ขอบเขตอำนาจศาลต้องพิจารณาตามเขตแดนนั้นไม่ว่าจะอยู่ในพื้นที่อื่นใดก็ตาม

ช่องว่างทางกฎหมายเช่นนี้ทำให้คำถามข้างต้นว่า ใครมีสิทธิ์เข้าถึงข้อมูลเหล่านั้นได้อย่างถูกกฎหมาย เมื่อพิจารณาบริบทเช่นนี้ ทำให้เกิดข้อกังวลว่า ประเทศที่ตั้งบริษัทจะบังคับเพื่อละเมิดข้อมูลส่วนบุคคลโดยไม่พิจารณาถึงข้อบังคับทางกฎหมายตามสัญชาติของบริษัทนั้น เนื่องจากไม่ถือว่าเป็นเขตแดนของรัฐ ผู้เขียนมีข้อเสนอแนะว่า การนิยามเรื่องเขตแดนของรัฐทางกายภาพมีความจำเป็นต้องถูกทบทวนใหม่เพื่อป้องกัน หรือลดช่องว่างความเหลื่อมล้ำทางกฎหมายของรัฐต้นทางกับรัฐที่ตั้ง ซึ่งอาจถูกพิจารณาในลักษณะเช่นเดียวกับสถานทูตทางใดทางหนึ่ง อย่างไรก็ตาม ประเด็นดังกล่าวมีความอ่อนไหว เนื่องจากบริษัทถือเป็นสิ่งปลูกสร้างซึ่งแตกต่างจากกรณีสัญชาติที่ครอบคลุม

เรือหรือยานบิน จึงอาจถือเป็นการละเมิดอธิปไตยทางเขตแดนโดยชัดเจน บริษัทที่มีจำนวนที่ตั้งมากในประเทศปลายทางย่อมหมายถึงการถูกละเมิดอธิปไตยขนาดใหญ่ ซึ่งประเด็นเหล่านี้ควรได้รับการถกเถียงต่อไป

อย่างไรก็ตาม ข้อเสนอเสนอแนะข้างต้นจะสร้างความย้อนแย้งทางปทัสถานในการทำความเข้าใจเขตอำนาจอธิปไตยของรัฐในโลกไซเบอร์กับพื้นที่กายภาพในลักษณะที่เรียกว่า “Hyper Sovereignty” เนื่องจากพื้นที่ไซเบอร์ไม่มีเส้นเขตแดนของรัฐที่ชัดเจนเหมือนเส้นเขตแดนทางภูมิศาสตร์ แม้ว่าในความเป็นจริงหลายพื้นที่จะไม่ยังคงอยู่ในขั้นตอนการปักปันเขตแดน หรือยังคงขัดแย้งในการขีดเส้นพรมแดนอันเป็นที่ยอมรับ แต่ปฏิเสธไม่ได้ว่า พื้นที่ทางกายภาพเป็นสิ่งสามารถสัมผัสและรับรู้ได้ด้วยตาจึงง่ายต่อการทำความเข้าใจ เมื่อเทียบกับพื้นที่ไซเบอร์นั้น การกำหนดข้อระเบียบ กฎเกณฑ์ทางปทัสถาน หรือแม้แต่การบังคับใช้กฎหมายของแต่ละประเทศ “ที่มีอยู่แล้ว” ในพื้นที่ไซเบอร์ จะถือเป็นการใช้อำนาจอธิปไตยภายในประเทศนอกเขตอธิปไตยตามหลักกฎหมายระหว่างประเทศสากลหรือไม่ (universal jurisdiction) และสิ่งเหล่านี้จะถือเป็นการละเมิดอำนาจอธิปไตยของประเทศหรือไม่

ผู้เขียนใคร่เสนอว่า ประเทศไทศจำเป็นต้องถกเถียงและแสดงให้เห็นอย่างชัดเจนถึงความจำเป็นที่จะต้องมีการวางโครงสร้างเชิงกฎหมายสำหรับพื้นที่ทางไซเบอร์เป็นการเฉพาะ โดยประเด็นสำคัญ ต้องแยกสิ่งที่เรียกว่า “เขตแดน” ออกมาศึกษาเพื่อวางขอบเขต การบังคับใช้และการวินิจฉัยข้อกฎหมายเป็นพิเศษจากระบบกฎหมายทั่วไปที่ใช้กับเรื่องอื่น ๆ โดยเฉพาะเรื่อง เขตแดนอธิปไตยทางกายภาพ อย่างไรก็ตาม นักวิชาการผู้ศึกษากฎหมายไซเบอร์ของสหรัฐฯ เสนอความคิดที่แตกต่างว่า การศึกษาอินเทอร์เน็ตและพื้นที่ทางไซเบอร์เพื่อแยกข้อกฎหมายออกเป็นลักษณะพิเศษไม่มีความจำเป็น เนื่องจากไม่ต่างอะไรกับ “Law of the Horse” หรือ “กฎหมายว่าด้วยลักษณะม้า” ในสหรัฐฯ (Easterbrook, 1996) กรณีข้างต้น เป็นกรณีที่สำคัญอย่างมากต่อนักวิชาการกลุ่มไม่สนับสนุนให้เกิดการแยกตัวของพื้นที่ทางไซเบอร์กับกายภาพที่มากเกิน ซึ่งเสนอว่า ครั้งหนึ่งศาลอุทธรณ์สหรัฐฯ ได้มีการตัดสินคดีซึ่งเกี่ยวกับม้าว่า การขโมยม้า การลักม้า การทำร้าย หรือแม้แต่การฆ่าม้า สามารถใช้หลักกฎหมายทั่วไป (general rules) มาปรับใช้ได้เพื่อให้สะดวกต่อการพิจารณาโดยไม่จำเป็นต้องสร้างสิ่งใหม่หรือ “กฎหมายลักษณะเฉพาะม้า” ขึ้นมาเพื่อพิจารณาคดี ข้อเสนอดังกล่าวนั้นสนับสนุนข้อถกเถียงที่ว่า ในทางกฎหมายแล้วสามารถใช้กฎหมายทั่วไปมาปรับใช้ได้โดยไม่มีความจำเป็นต้องสร้าง “Cyberlaw” หรือ กฎหมายลักษณะเฉพาะว่าด้วยเรื่องไซเบอร์แต่อย่างใด อย่างไรก็ตาม เนื่องจากพลวัตทางเทคโนโลยีและความชัดเจนของความแตกต่างระหว่างพื้นที่ทางไซเบอร์กับพื้นที่ทางกายภาพเริ่มซับซ้อนมากขึ้นในปัจจุบัน ส่งผลให้ชุดความคิดดังกล่าว ดูเหมือนจะล้าสมัยไปเสียแล้ว

จะเห็นได้ว่าจำเป็นต้องมีการทบทวนปทัสถานด้านไซเบอร์ใหม่ โดยเฉพาะอย่างยิ่งเมื่อพื้นที่ไซเบอร์มีขอบเขตที่ทับซ้อนกับพื้นที่ทางกายภาพมากขึ้น อย่างไรก็ดี โจทย์ซึ่งเป็นข้อท้าทายอย่างมากต่อการพัฒนาข้อถกเถียงด้านไซเบอร์ในปัจจุบัน กับพลวัตทางไซเบอร์ดูเหมือนจะขัดแย้งกัน เนื่องจากหากลองพิจารณาถึงกระบวนการกำหนดกฎเกณฑ์ การนำเสนอและแพร่กระจายปทัสถาน ไปจนถึงการนำไปปฏิบัติใช้ จะพบว่า กระบวนการเหล่านี้ไม่สามารถไล่ตามความเร็วของการพัฒนาทางเทคโนโลยีและชุมชนของข้อมูลได้ทัน

นอกจากนี้พื้นที่ไซเบอร์ยังเป็นสิ่งที่ถูกสร้างขึ้นโดยมนุษย์โดยอาศัยรหัสดิจิทัลในการออกแบบสถาปัตยกรรมทางอินเทอร์เน็ต ดังนั้น ผู้ออกแบบระบบหรือวิศวกร สถาปนิกในพื้นที่ไซเบอร์ย่อมมีความได้เปรียบในการใช้อำนาจควบคุมทิศทางและกิจกรรมต่าง ๆ ให้ขับเคลื่อนไปในแนวทางที่ตนต้องการได้อย่างแท้จริง อำนาจซึ่งไม่ได้อยู่ในมือของตัวกระทำการในลักษณะองค์กรของรัฐบาลโดยสมบูรณ์นั้นได้นำมาซึ่งความท้าทายในการกำกับดูแลและการใช้อำนาจทางกฎหมายเพื่อกำหนดระเบียบในพื้นที่ไซเบอร์ อย่างไรก็ตาม ตัวแบบในปัจจุบันซึ่งเป็นที่ยอมรับโดยทั่วกัน คือ การกำกับดูแลโดยผู้มีส่วนได้ส่วนเสียหลายฝ่าย (multistakeholder) เนื่องจากรัฐต้องร่วมมือกับผู้ประกอบการอื่น หรือเจ้าของเทคโนโลยีในการติดตามค้นหา เพราะฉะนั้น คำถามสำคัญที่เกิดขึ้น คือ รัฐมีอำนาจใดในการการบังให้ตัวแสดงภาคเอกชนทั้งหลายทำตามคำสั่ง หรือให้ความร่วมมือภายใต้ขอบเขตทางอำนาจที่กฎหมายกำหนดและยิ่งทวีความซับซ้อนเมื่อขอบเขตอำนาจศาลในเขตแดนกายภาพที่มีอยู่จะสอดคล้องหรือนำมาปรับใช้ได้เพียงใดกับพื้นที่ไซเบอร์ รัฐจะสามารถใช้ลักษณะกฎหมายสากลว่าด้วยอำนาจศาลนอกพื้นที่อธิปไตยได้หรือไม่ (extraterritorial jurisdiction) ข้อโต้แย้งเหล่านี้จำเป็นต้องได้รับการถกเถียงต่อไป

# บรรณานุกรม

## English


AAE-1. (2022). ABOUT AAE-1. Retrieved from http://www.aaeone.com/aaeportal/

Acharya, A. (2004). How ideas spread: Whose norms matter? Norm localization and institutional change in Asian regionalism. *International Organization, 58*(2), 239-275.

Association of Southeast Asian Nations. (2019, November 3). ASEAN-China Leaders' Statement on Smart City Cooperation Initiative. Retrieved from http://asean.org/storage/2019/11/Final-ASEAN-China-Leaders-Statement-on-Smart-City-Cooperation-Initiative-2.pdf.

Bangkok Post. (2022a). National Cyber Security Agency signs MoU with Huawei. *Bangkok Post*. Retrieved from https://www.bangkokpost.com/thailand/pr/2360342/national-cyber-security-agency-signs-mou-with-huawei

*Bangkok Post*. (2022b, 9 August). NCSA signs MoU with Huawei for cyber security development. Retrieved from https://www.bangkokpost.com/tech/2364706/ncsa-signs-mou-with-huawei-for-cyber-security-development

*Bangkok Post.* (2022c, November 18). 23,000 CCTVs added for Apec meet. Bangkok Post. Retrieved from https://www.bangkokpost.com/thailand/general/2440395/23-000-cctvs-added-for-apec-meet

Becker, H. S. (1963). *Outsiders: Studies in the Sociology of Deviance*. New York: The Free Press.

Bossong, R., Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime Law Soc Change 67*, 265–288. https://doi.org/10.1007/s10611-016-9653-3

Boyle, J. (1997). Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors. *University of Cincinnati Law Review, 66,* 177-205.

Cai, S., Jun, M., & Yang, Z. (2009). Implementing supply chain information integration in

China: The role of institutional forces and trust. *Journal of Operations Management, 28*, 257-268.

Chandran, N. (2018, 14 September). China can make its Belt and Road project more successful if it taps locals, experts say. *CNBC.* Retrieved from https://www.cnbc.com/2018/09/14/china-must-do-more-to-tap-locals-in-belt-and-road-initiative-panel.html

Chang, Y. Y. (2023). China beyond China, establishing a digital order with Chinese characteristics: China's growing discursive power and the Digital Silk Road. *Politics & Policy, 00,* 1–39. doi:10.1111/polp.12524.

Charter of the United Nations. (n.d.). Chapter I - Purposes and Principles: Article 2(1)-(5). Codification Division, Office of Legal Affairs. Retrieved from https://legal.un.org/repertory/art2.shtml

Chinese Ministry of Foreign Affairs. (2015, December 16). Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference. Retrieved from http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

Chinese Ministry of Foreign Affairs. (2020, September 8). Global Initiative on Data Security. Retrieved from https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html.

Chinese Ministry of Foreign Affairs. (2022, August 4). Wang Yi Holds Talks with Cambodian Deputy Prime Minister and Foreign Minister Prak Sokhonn. Retrieved from https://www.fmprc.gov.cn/eng/zxxx_662805/202208/t20220806_10736425.html.

Congressional Research Service. (2021). *International Financial Messaging Systems*. Retrieved from https://crsreports.congress.gov/product/pdf/R/R46843

Conley, H. A., Hillman, J. E., McCalpin, M., & Ruy, D. (2020). The Second Wave: Digital Infrastructure. In *Becoming a Chinese Client State: The Case of Serbia* (Report Part Title). Center for Strategic and International Studies (CSIS). Retrieved from

https://www.jstor.org/stable/resrep26534.6

Consulate General of The People's Republic of China in Chicago. (2015, October 8). Xinhua Insight: New cross-border interbank payment system a milestone in RMB internationalization. Retrieved from http://chicago.china-consulate.gov.cn/eng/xw/201510/t20151008_4653714.htm

Cui, B. G., & Liu, J. (2020). On the Platform Governance in Cyberspace. *Journal Global Media Journal, 7*, 86-101.

Cyberspace Administration of China. (2020, April 16). Translate from “The Second Anniversary of the Implementation of the "Network Security Law": Let the Internet in the Rule of Law Track Healthy Operation.” Retrieved from http://www.cac.gov.cn/2020-04/16/c_1588583174020809.htm.

Daniel, C. (2023). *Huawei Revenue and Growth Statistics (2023).* SignHouse. Retrieved from https://www.usesignhouse.com/blog/huawei-stats

Dekker, B., & Okano-Heijmans, M. (2020). Business: e-commerce, the platform economy and digital payments. In *Europe's Digital Decade?: Navigating the global battle for digital supremacy* (Report Part Title). Clingendael Institute. Retrieved from https://www.jstor.org/stable/resrep26543.6

Dekker, B., Okano-Heijmans, M., & Zhang, E. S. (2020, July 27). Unpacking China's Digital Silk Road. Clingendael. Retrieved from https://www.clingendael.org/publication/unpacking-chinas-digital-silk-road

DeNardis, L., & Raymond, M. (2013). Thinking clearly about multistakeholder Internet governance. GigaNet: Global Internet Governance Academic Network, Annual Symposium. November 14. Retrieved March 30, 2021, from https://doi.org/10.2139/ssrn.2354377

Ding, M. (2020). Digital Economy and Cyberspace Governance Strategy of Japan. *Journal Contemporary Economy of Japan, 1*, 01-12.

Easterbrook, F. H. (1996). *Cyberspace and the Law of the Horse. University of Chicago*

*Legal Forum*, 1996(1), Article 7.

Eastern Economic Corridor (EEC). (2022). *Business Opportunities*. Retrieved from https://www.eeco.or.th/en/business-opportunities

Etzioni, A. (2011). Cybersecurity in the Private Sector. *Issues in Science and Technology, 28*(1). Retrieved from https://issues.org/etzioni-2-cybersecurity-private-sector-businesses/

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization, 52*(4), 887-917. Retrieved from https://www.jstor.org/stable/2601361

Florini, A. (1996) The evolution of international norms. *International Studies Quarterly 40*(3): 363- 389.

Global Connectivity Index (GIC). (2020). *Shaping the New Normal with Intelligent Connectivity*. Retrieved from https://www.huawei.com/minisite/gci/en/

Guo, H. (2017). Big Earth data: A new frontier in Earth and information sciences. *Big Earth Data, 1,* 4-20. https://doi.org/10.1080/20964471.2017.1403062

Horgan, D., Hackett, J., Westphalen, C. B., Kalra, D., Richer, E., Romao, M., Andreu, A. L., Lal, J. A., Bernini, C., Tumiene, B., Boccia, S., & Montserrat, A. (2020). Digitalisation and COVID-19: The Perfect Storm. *Biomed Hub, 5*(3), 1–23. https://doi.org/10.1159/000511232

Huawei Technologies. (2022). Thai Prime Minister Attends Thailand 5G Alliance Announcement. *Huawei News*. Retrieved from https://www.huawei.com/en/news/2022/6/thailand-5g-summit

*Huawei.* (2020, December 20). Huawei Supported to Build Laos's First Smart Highway. Retrieved from http://e.huawei.com/cn/news/ebg/2020/first-expressway-laos.

Hurley, J., Morris, S., & Portelance, G. (2019). Examining the debt implications of the Belt and Road Initiative from a policy perspective. *Journal of Infrastructure Policy and*

*Development, 3,* 139-175.

Iwamoto, K. (2020, September 4). China's Ant Eyes Southeast Asia e-Payment Dominance With IPO. *Nikkei Asia.* Retrieved from http://asia.nikkei.com/Business/Business-Spotlight/China-s-Ant-eyes-Southeast-Asia-e-payment-dominance-with-IPO.

Japan Cybersecurity Innovation Committee (JCIC). (August 2020). *JAPAN CYBERSECURITY INNOVATION COMMITTEE Policy Proposals for Realizing a True Digital Society in the Post-Coronavirus Era.* Retrieved from https://www.j-cic.com/column/JCIC-Policy-Proposal-2020-EN.html

Japanese Ministry of Foreign Affairs. (2019, January 23). Speech by Prime Minister Abe at the World Economic Forum Annual Meeting. Retrieved from http://www.mofa.go.jp/ecm/ec/page4e_000973.html.

Jian, L. (2018). Belt and Road Initiative Enables China and Thailand to Increase Affinity. Embassy of The People's Republic of China in The Kingdom of Thailand. Retrieved from http://th.china-embassy.gov.cn/eng/ztgx/201809/t20180928_10161817.htm

Job.banks.am. (2022, July 13). Russia considers China's CIPS an alternative to SWIFT. Retrieved from https://banks.am/en/news/fintech/24168

Keck, M. E., & Sikkink, K. (1998). *Activists beyond Borders: Advocacy Networks in International Politics*. Ithaca and London: Cornell University Press.

Khalil, L. (2020). Digital Authoritarianism, China and COVID. *Lowy Institute Analyses*. Retrieved from https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid

Le Corre, P. (2018). Conclusion. In *China's Rise as a Geoeconomic Influencer: Four European Case Studies* (Report Part Title). Carnegie Endowment for International Peace. Retrieved from http://www.jstor.com/stable/resrep20979.9

Lee, K., Rasser, M., Fitt, J., & Goldberg, C. (2020). *Digital Entanglement: Lessons Learned from China's Growing Digital Footprint in South Korea*. Center for a New American

Security. Retrieved from https://www.jstor.org/stable/resrep27454

Lessig, L. (1998). What Things Regulate Speech: CDA 2.0 vs. Filtering. *Jurimetrics Journal, 38*, 640.

Leswing, K. (2017, December 4). The CEOs of Apple and Google spoke at a conference that critics say makes them 'complicit actors in the Chinese censorship regime'. *Insider.* Retrieved from https://www.businessinsider.com/apple-ceo-tim-cook-google-sundar-pichai-spoke-china-controversial-world-internet-conference-2017-12

Lew, J. J., Roughead, G., Hillman, J., & Sacks, D. (2021). China's Belt and Road Report: Implications for the United States. Council on Foreign Relations. Retrieved from https://www.jstor.org/stable/resrep29893.5

Li, H. M. (2019). The Digital Silk Road and the Reconstruction of Global Cyberspace Governance. *Journal of International Forum*, 21, 15-29.

Lin, N. H., & MinMin. (2020, December 15). Hundreds of Huawei CCTV Cameras With Facial Recognition Go Live in Naypyitaw. Myanmar Now. Retrieved from http://www.myanmar-now.org/en/news/hundreds-of-huawei-cctv-cameras-with-facial-recognition-go-live-in-naypyitaw

Macaskill, E., & Dance, G. (2013). NSA FILES: DECODED What the revelations mean for you. *The Guardian*. Retrieved from https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

Mathews, B. (2003). Bangkok's Fine Balance: Thailand's China Debate. Asia-Pacific Center for Security Studies. Retrieved from https://dkiapcss.edu/Publications/SAS/ChinaDebate/ChinaDebate_Mathews.pdf

Maurer, T., & Hoffman, W. (2019). The privatization of security and the market for cyber tools and services. *Geneva Centre for Security Sector Governance No. 23*/2019. Retrieved from https://carnegieendowment.org/2019/08/23/privatization-of-security-and-market-for-cyber-tools-and-services-pub-80356

Microwave Journal. (2019, August 26). “Canalys Reports Chinese Smartphone Brands Take 62% of Southeast Asia’s 30.7M Shipments.” *Microwave Journal*. Retrieved from https://www.microwavejournal.com/articles/32721-canalys-reports-chinese-smartphone-brands-take-62-of-southeast-asias-307m-shipments

Ministry of Communications & IT, India. (2019, June 20). "To Contribute in Activating Afghansat 2." Retrieved from https://mcit.gov.af/en/india-contribute-activating-afghansat-2

Ministry of Foreign Affairs, the People's Republic of China. (2022, June 24). Chair’s Statement of the High-level Dialogue on Global Development. Retrieved from https://www.fmprc.gov.cn/eng/wjdt_665385/2649_665393/202206/t20220624_10709812.html

Mochinaga, D. (2021). The Digital Silk Road and China’s Technology Influence in Southeast Asia. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/digital-silk-road-and-chinas-technology-influence-southeast-asia

Moritz, W., & Vytautas, J. (2019). Securing cyberspace: How states design governance arrangements. *Journal Governance, 2*, 259-275.

Morrow, S. (2020). *First Safe Harbor, then Privacy Shield: What EU-US data-sharing agreement is next?.* Infosec. Retrieved from https://resources.infosecinstitute.com/topic/first-safe-harbor-then-privacy-shield-what-eu-us-data-sharing-agreement-is-next/

National People’s Congress of the People’s Republic of China. (2016, November 7). Cybersecurity Law of the People's Republic of China. Retrieved from http://www.npc.gov.cn/npc/c30834/201611/270b43e8b35e4f7ea98502b6f0e26f8a.shtml

Naughton, B., Chen, L., & Barry, C. (2016). An Institutionalized Policy-Making Mechanism: China's Return to Techno-Industrial Policy. *Research Policy, 45*(10), 2138-2152.

Neville, F. G., Novelli, D., Drury, J., & Reicher, S. D. (2022). Shared social identity transforms social relations in imaginary crowds. *Group Processes & Intergroup Relations,*

*25*(1), 158–173. https://doi.org/10.1177/1368430220936759

NPC Observer. (2017). *National Intelligence Law*. Retrieved from https://npcobserver.com/legislation/national-intelligence-law/

Nye, J. S. (2014). The regime complex for managing global cyber activities. Global Commission on Internet Governance. Retrieved March 30, 2021, from https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

Payne, R.A. (2001). Persuasion, frames and norm construction. *European Journal of International Relations, 7(*1). 37-61.

Perkins, R. M. (1971). The Territorial Principle in Criminal Law. *Hastings Law Journal, 22*, 1155. Retrieved from https://repository.uchastings.edu/hastings_law_journal/vol22/iss5/2

Privacy Shield Framework. (2023). *Privacy Shield lists*. Retrieved from https://www.privacyshield.gov/list

Rublee, M. R. (2008). Taking stock of the nuclear nonproliferation regime: Using social psychology to understand regime effectiveness. *International Studies Review, 10*. 420-450.

Sadasivam, K., Samudrala, B., & Yang, A. (2005). Design of Network Security Projects Using Honey-pots. *Journal of Computing Sciences in Colleges, 20*(4), 282–293.

Sharon, A. (2022). Thailand Proposes Additional Regulations to Boost Cybersecurity. *OpenGov Asia.* Retrieved from https://opengovasia.com/thailand-proposes-additional-regulations-to-boost-cybersecurity/

Sheehan, M., Blumenthal, M., & Nelson, M. R. (2021). Three Takeaways From China's New Standards Strategy. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2021/10/28/three-takeaways-from-china-s-new-standards-strategy-pub-85678

Technophrenia. (2014). The psychology behind Apple's fans. Blind loyalty or just wanting to belong?. *The Conversation.* Retrieved from https://theconversation.com/the-

psychology-behind-apples-fans-blind-loyalty-or-just-wanting-to-belong-31671

Teendifferent. (2023). The Dark Side of Cyberspace: A Thrilling Journey into the World of Malware and Cyber Threats. *Medium*. https://medium.com/@teendifferent7/the-dark-side-of-cyberspace-a-thrilling-journey-into-the-world-of-malware-and-cyber-threats-ea3616980b9f

The State Council Information Office, The People's Republic of China. (2023). Full text: China's Law-Based Cyberspace Governance in the New Era. *Xinhua*. Retrieved from http://english.scio.gov.cn/whitepapers/2023-03/16/content_85172148.htm

The State Council Information Office, The People's Republic of China. (2022). *White Paper on Jointly Build a Community with a Shared Future in Cyberspace.* Retrieved from http://english.scio.gov.cn/node_8033411.html

The State Council Information Office, The People's Republic of China. (2023). Full text: China's Law-Based Cyberspace Governance in the New Era. *Xinhua*. Retrieved from http://english.scio.gov.cn/whitepapers/2023-03/16/content_85172148.htm

Triolo, P. (2020). China’s 5G Strategy: Be First Out of the Gate and Ready to Innovate. In S. Kennedy (Ed.), *China’s Uneven High-Tech Drive: Implications for the United States* (pp. 21–28). Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep22605.10

Tugendhat, H., & Voo, J. (2021). China's Digital Silk Road in *Africa and the Future of Internet Governance* (Policy Brief No. 60/2021). China Africa Research Initiative (CARI), School of Advanced International Studies (SAIS), Johns Hopkins University. Retrieved from http://www.sais-cari.org/publications-policy-briefs

United Nations Conference on Trade and Development. (2022). *Digitalization of Services: What does it imply to trade and development?* Retrieved from https://unctad.org/publication/digitalization-services-what-does-it-imply-trade-and-development

Wang, W. (2018). Singapore’s Cyberspace Governance and Its Enlightenment to China.

*Journal of Pacific Journal, 26*, 35-45.

World Economic Forum. (2022). *Do data regulations properly protect consumers?* Retrieved from https://www.weforum.org/agenda/2022/08/do-data-regulation-properly-protect-consumers/

*Xinhuanet.* (2016, April 19). Translate from “Xi Jinping's Full Speech at the Symposium on Internet Information.” Xinhuanet. Retrieved from http://www.xinhuanet.com/politics/2016-04/25/c_1118731175.htm

*Xinhuanet*. (2018, January 10). Standard Administration Committee Discussing China Standard 2035. Xinhuanet. Retrieved from http://www.xinhuanet.com/fortune/2018-01/10/c_129787658.htm.

*Xinhuanet*. (2020a, November 3). Translate from “The Proposal of the Central Committee of the Communist Party of China on the Formulation of the Fourteenth Five-Year Plan for National Economic and Social Development and the Visionary Goals for 2035.” Xinhuanet. Retrieved from http://www.xinhuanet.com/politics/2020-11/03/c_1126693293.htm

*Xinhuanet.* (2020b, September 15). Pakistan welcomes China-proposed Global Initiative on Data Security. Xinhuanet. Retrieved from http://www.news.cn/english/2020-09/15/c_139368094.htm.



Zhao, F., Shi, Y., & Yao, K. (2021). Challenges and Countermeasures of China’s Cyberspace Governance in the New Era. SHS Web of Conferences, 96, 01005. Retrieved from https://doi.org/10.1051/shsconf/20219601005

Zhao, F., Shi, Y., & Yao, K. (2021). Challenges and Countermeasures of China’s Cyberspace Governance in the New Era. SHS Web of Conferences, 96, 01005. Retrieved from https://doi.org/10.1051/shsconf/20219601005

Zhao, F., Shi, Y., & Yao, K. (2021). Challenges and Countermeasures of China’s Cyberspace Governance in the New Era. SHS Web of Conferences, 96, 01005. Retrieved from https://doi.org/10.1051/shsconf/20219601005

Zittrain, J., & Edelman, B. (2003). Internet Filtering in China. *IEEE Internet Computing, 7*(2), 70-77. doi: 10.1109/MIC.2003.1189191.

**ภาษาไทย**

กรองจันทร์ จันทรพาหา. (ม.ป.ป.). วิเคราะห์เศรษฐกิจ-สังคมจีน “เทคโนโลยีในยุค 5.0 กับวิถีชีวิตของคนจีนในปัจจุบัน. สถาบันเอเชียศึกษาจุฬาลงกรณ์มหาวิทยาลัย. https://shorturl.asia/XI2qL

กระทรวงการต่างประเทศ. (2562, 5 พฤศจิกายน). แถลงการณ์ร่วมต่อสื่อมวลชน ระหว่างรัฐบาลราชอาณาจักรไทยกับรัฐบาลสาธารณรัฐประชาชนจีน (คำแปลอย่างไม่เป็นทางการ) เผยแพร่วันที่ ๕ พฤศจิกายน ๒๕๖๒ ณ กรุงเทพมหานคร. https://shorturl.asia/V604G

*คมชัดลึกออนไลน์.* (2565, 18 กุมภาพันธ์). ด่วน “AIS” โร่แจ้งถูกแฮก ข้อมูลลูกค้ารั่วไหลกว่าแสนราย. https://www.komchadluek.net/hot-social/505879

เจ้าหน้าที่ฝ่ายการตลาด หน่วยงานผู้ให้บริการอินเทอร์เน็ต. (2565, 22 ตุลาคม). การสื่อสารส่วนบุคคล.

เจ้าหน้าที่ฝ่ายการตลาด หน่วยงานผู้ให้บริการอินเทอร์เน็ต. (2566, 14 กุมภาพันธ์). การสื่อสารส่วนบุคคล.

เจ้าหน้าที่หน่วยงานความมั่นคงของรัฐ. (2565). การสื่อสารส่วนบุคคล.

เจ้าหน้าที่หน่วยงานความมั่นคงของรัฐ. (2566). การสื่อสารส่วนบุคคล.

ชูเกียรติ น้อยฉิมและ วรณัฐ บุญเจริญ. (2563). นิติปรัชญากับการศึกษาวิเคราะห์ร่างพระราชบัญญัติความมั่นคงไซเบอร์. *MFU CONNEXION, 3*(2). 249-280.

*เดลินิวส์ ออนไลน์*. (2565, 4 มีนาคม). เพราะไม่กลัวถูกจับ ‘เว็บพนัน’ ถึงผุดโผล่ไม่หยุด. https://www.dailynews.co.th/articles/814498/

*เดอะสเต็ทส์ไทม์* [The States Times]. (2565, 13 กรกฎาคม). 'ดร.นิว' ชวน 'บิ๊กตู่' ทำบุญประเทศครั้งใหญ่ เร่งสร้าง 'อธิปไตยไซเบอร์' สกัดก๊วนกบฏ 3 นิ้ว. https://thestatestimes.com/post/2022071317

*เดอะสแตนดาร์ด* [The Standard]. (2564, 29 มีนาคม). ชัยวุฒิ รมว. ดีอีเอส เดินหน้าสานต่อจับตากลุ่มทำผิด ม. 112 ย้ำมีกฎหมายบังคับใช้อยู่แล้ว. https://thestandard.co/chaiwut-move-forward-on-m112-watching/.

*เดอะสแตนดาร์ด* [The Standard]. (2565, 6 มิถุนายน). ย้อนรอย GT200 ในตำนาน กับ ‘คำตอบ’

ของ ‘คำถาม’ ที่ว่า กลาโหมจ่าย 7.5 ล้านบาท เพื่อตรวจพลาสติกเปล่าทำไม?. https://thestandard.co/gt200-history/

*ทรู* [True.th.] (2563, 19 สิงหาคม). เปิดตัว ทรู 5G พร้อมพลิกโฉมไทยสู่ประเทศอัจฉริยะที่ยั่งยืน. https://www.true.th/truemoveh/site/news/detail/1718.

ทศพล ทรรศนกุลพันธ์. (2558). ไม่มีแดนเถื่อนในโลกไซเบอร์?: การศึกษาตัวแบบในการกำกับดูแลโลกไซเบอร์. *วารสารนิติสังคมศาสตร์, 8*(2).

ที่ปรึกษาด้านเทคโนโลยี องค์กรเอกชน. (2565, 18 มีนาคม). การสื่อสารส่วนบุคคล.

ที่ปรึกษาด้านเทคโนโลยี องค์กรเอกชน. (2566, 4 กุมภาพันธ์). การสื่อสารส่วนบุคคล.

ที่ปรึกษาด้านธุรกิจบริษัทเอกชน. (2565, 16 สิงหาคม). การสื่อสารส่วนบุคคล.

ที่ปรึกษาด้านธุรกิจบริษัทเอกชน. (2566, 8 กุมภาพันธ์). การสื่อสารส่วนบุคคล.

*เทคทอล์กไทย* [TechTalkThai]. (2566, 3 กุมภาพันธ์). ร่วมเสวนาด้าน CYBERSECURITY สำหรับหน่วยงาน CII ทั้ง 8 กลุ่ม ในงาน NCSA THAILAND NATIONAL CYBER WEEK 2023 วันที่ 17–18 กุมภาพันธ์ ณ สามย่านมิตรทาวน์. https://www.techtalkthai.com/ncsa-thailand-national-cyber-week-2023-panel-discussion/.

*ไทยพับลิก้า*. (2561, 19 เมษายน). “อาลีบาบา” จับมือรัฐบาลไทยลงทุนดิจิทัลฮับ-ชี้มีวิสัยทัศน์ “ยกระดับ-สร้างโอกาส” ธุรกิจเอกเอ็มอีร่วมกัน. https://thaipublica.org/2018/04/jack-ma-mou-thai-government/

*ไทยรัฐออนไลน์*. (2562, 27 เมษายน). "นายกฯ"ยก 5 ปีไทย-จีน สัมพันธ์ดี เชื่อมความร่วมมือประเทศ เส้นทางสายไหม. https://www.thairath.co.th/news/politic/1554810.

*ไทยรัฐออนไลน์*. (2565). USA ชวนไทยลงนาม MOU ไซเบอร์ ป้องอาชญากรรมออนไลน์เด็ก. https://www.thairath.co.th/news/politic/2531241

*ไทยรัฐออนไลน์*. (2566, 28 กุมภาพันธ์). แคนาดาสั่งห้ามติดตั้งแอปฯ “TikTok” ในอุปกรณ์ของรัฐ อ้างปัญหาความมั่นคง. https://www.thairath.co.th/news/foreign/2641173

ธรรมชาติ กรีอักษร. (2562, 18 มิถุนายน). เมื่อ พ.ร.บ. ไซเบอร์ไทย ตามรอยพี่ใหญ่จีน: คุยกับจันจิรา สมบัติพูนศิริ. *ประชาไท*. https://prachatai.com/journal/2019/06/83025

ธีรนัย จารุวัสตร์. (2562, 16 มีนาคม). ไทยถาม จีนตอบ: โครงการ “หนึ่งแถบหนึ่งเส้นทาง” ไทยได้หรือ

เสีย?. *ข่าวสดออนไลน์.* https://www.khaosod.co.th/chinawatch/news_2315070

นพ นนารถ. (2562, 21 เมษายน). การประชุมสุดยอดครั้งที่ 2 ยุทธศาสตร์หนึ่งแถบหนึ่งเส้นทาง. *ผู้จัดการออนไลน์.* https://mgronline.com/daily/detail/9620000038673.

*บีบีซี* [BBC]. (22 มกราคม 2564). ม. 112: เปิดสำนวนตำรวจ ทำอะไรถึงเข้าข่าย "หมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาทฯ. https://www.bbc.com/thai/thailand-55768153.

*แบรนด์อินไซด์* [Brandinside]. (2565). สกมช. แถลงผลสำเร็จโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ยกระดับบุคลากรไซเบอร์ไทยทัดเทียมสากล ทะลุเป้ากว่า 4,000 คน. https://brandinside.asia/intensive-cybersecurity-capacity-building-program/.

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570). (2565, 9 ธันวาคม). *ราชกิจจานุเบกษา.* เล่ม 139, ตอน 288 ง, ฉบับพิเศษ. หน้า 7.

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564. (2564, 23 สิงหาคม). *ราชกิจจานุเบกษา.* เล่ม 138, ตอน 194 ง, ฉบับพิเศษ. หน้า 8-17. https://drive.ncsa.or.th/s/DXs7pjtjFS5R2Zc

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล (2564, 23 สิงหาคม). *ราชกิจจานุเบกษา.* เล่ม 138, ตอน 194 ง, ฉบับพิเศษ. หน้า 14. https://drive.ncsa.or.th/s/weLZNyzwApDdiR5

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 (2564, 6 กันยายน). *ราชกิจจานุเบกษา.* เล่ม 138, ตอน 208 ง, ฉบับพิเศษ. หน้า 9-15. https://drive.ncsa.or.th/s/6rFJ66fNstfK6ni

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566. (2566, 9 พฤษภาคม). *ราชกิจจานุเบกษา.* เล่ม 140, ตอน 107 ง, ฉบับพิเศษ. หน้า 39-40. https://drive.ncsa.or.th/s/NGSL3XZLbdJaZdg

ประกาศราชกิจจานุเบกษา เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. 2561-2580). (2561, 13 ตุลาคม). *ราชกิจจานุเบกษา.* เล่ม 135 ตอนที่ 82 ก. หน้า 1.

*ประชาไท.* (2565, 17 ธันวาคม). อาร์ติเคิล 19 ออกรายงานจี้รัฐไทย ยุติสลายชุมนุม-ใช้คดีปิดกั้นเสรีภาพ วงเสวนาสะท้อนรัฐกดปราบรุนแรง. https://prachatai.com/journal/2022/12/101900

ประลองยุทธ ผงงอย. (2566, 16 กุมภาพันธ์). TRUE-DTAC เดินหน้าลุยควบรวมกิจการ ดันมาร์เก็ตแคปบริษัทใหม่แตะ 3 แสนล้านบาท จับตาปัจจัยเสี่ยงฉุดรายได้ ทำต้นทุนพุ่ง. *The Standard*. https://thestandard.co/true-dtac-merger/.

ปริญญา หอมอเนก. (2563, 15 เมษายน). ความจริงเรื่องเอกราชและอธิปไตยไซเบอร์ของประเทศไทย (จบ). *กรุงเทพธุรกิจ.* https://www.bangkokbiznews.com/blogs/columnist/124875

ปวีร์ เจนวีระนนท์. (2566, 22 พฤษภาคม). นักวิชาการ แนะรัฐบาลใหม่ปลุกความเชื่อมั่นด้วยนโนบายป้องกัน ‘ภัยไซเบอร์’. *กรุงเทพธุรกิจ.* https://www.bangkokbiznews.com/tech/gadget/1069590.

*ผู้จัดการออนไลน์*. (2563, 19 ตุลาคม). AIS - Huawei จับมือเป็นพันธมิตรทางกลยุทธ์ 5G เสริมสิทธิพิเศษให้ลูกค้าเซเรเนด. https://mgronline.com/cyberbiz/detail/9630000106561

*ผู้จัดการออนไลน์.* (2563, 22 เมษายน). ทรูมูฟ เอช เปิดจอง HUAWEI P40 Series I 5G เต็มอิ่มกับสิทธิประโยชน์สุดคุ้มถึง 11 ต่อ. https://mgronline.com/entertainment/detail/9630000042339.

*ผู้จัดการออนไลน์.* (2566, 29 มีนาคม). ทรู ดิจิทัล ไซเบอร์ ซิเคียวริตี้ ผนึกกำลัง 3 พันธมิตรยกระดับบริการด้านบริหารจัดการระบบความปลอดภัยไซเบอร์. https://mgronline.com/cyberbiz/detail/9660000029356

พระจันทร์ เอียมชืน. (2565, 20 มกราคม). ส่องเว็บไซต์หน่วยงานไทยถูกแฮก 5 ครั้ง ใน 5 เดือน. *BrandThink*. https://www.brandthink.me/content/hacker-in-thai

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม 136, ตอน 69 ก. หน้า 20-50.

พระราชบัญญัติสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2562. (2562, 14 เมษายน). *ราชกิจจานุเบกษา.* เล่ม 136, ตอนที่ 49 ก. หน้า 45-57.

พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ. 2499. (2499, 15 พฤศจิกายน). *ราชกิจจานุเบกษา.* เล่ม 73, ตอน 95 ก, ฉบับพิเศษ. หน้า 1–4.

*โพสต์ทูเดย์* [Post Today]. (2563, 23 กันยายน), คอคอดกระชักศึกเข้าบ้าน? จีน สหรัฐ อินเดีย ออสเตรเลีย จะรุมทึ้งไทย. https://www.posttoday.com/international-news/633780

*โพสต์ทูเดย์* [Post Today]. (2564, 7 ธันวาคม). ‘ค่ายรถยนต์จีน’ เล็กขึ้นแท่นผู้นำตลาด ‘ยานยนต์ไฟฟ้า’ ของไทย. https://www.posttoday.com/international-news/670063

ภัชภิชา ฤกษ์สิรินุกูล. (2564, 12 ธันวาคม). Digital Silk Road เส้นทางสายไหมเดิม เพิ่มเติมคือเทคโนโลยี & ประชากรดิจิทัล. *Springnews.* https://www.springnews.co.th/spring-life/818998.

*มติชนออนไลน์.* (2566, 5 กรกฎาคม). ไซเบอร์ อีลีท ผนึกภาครัฐ เอกชน ร่วมมือป้องกันภัยคุกคามไซเบอร์. https://www.matichon.co.th/publicize/news_3702639.

*รัฐบาลไทย.* (2566, 21 มีนาคม). สรุปข่าวการประชุม ครม. https://www.thaigov.go.th/news/contents/details/66428

*วอยซ์ทีวี* [VoiceTV]. (2566, 15 เมษายน). สองปีเศษ สถิติ 112 พุ่ง 258 คดี เกินครึ่งมาจากความเห็นบนโลกออนไลน์. https://voicetv.co.th/read/HTTkg-24L

*วันโอวัน* [The101.world]. (2563). ถอดบทเรียนเศรษฐกิจดิจิทัลผ่านโมเดลไซเบอร์ประเทศจีน: ไทยอยู่ตรงไหนในสงครามแพลตฟอร์ม?. https://www.the101.world/china-cyber-security-law/

วิศวกรฝ่ายจัดการระบบ หน่วยงานผู้ให้บริการอินเทอร์เน็ต. (2565, 24 พฤษภาคม). การสื่อสารส่วนบุคคล.

วิศวกรฝ่ายจัดการระบบ หน่วยงานผู้ให้บริการอินเทอร์เน็ต. (2566, 12 มกราคม). การสื่อสารส่วนบุคคล.

*เวิร์คพอยท์ทูเดย์* [Workpoint Today]. (2565, 25 กุมภาพันธ์). หัวเว่ยเข้าเซ็น MOU กับกระทรวงดิจิทัล กระชับความร่วมมือด้านคลาวด์พัฒนาทักษาของบุคลากรภาครัฐ. https://today.line.me/th/v2/article/j7YNxYz

สกมช. (2566). *แผนปฏิบัติการ ประจำปีงบประมาณ พ.ศ. 2566 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.* https://drive.ncsa.or.th/s/JwPmxYwRnJJwmTc

สฤณี ทอาชวานันกุล. (2562, 4 มีนาคม). พ.ร.บ. ไซเบอร์: เมื่อหลักความมั่นคงไซเบอร์แพ้ทัศนคติ

“ความมั่นคง 0.4”. *ThaiPublica*. https://thaipublica.org/2019/03/cybersecurity-principles-lost-national-security/

*สำนักข่าวอินโฟเควสท์*. (2565, 29 สิงหาคม). กลุ่ม TRUE เปิดตัว ทรูดิจิทัล ไซเบอร์ ซิเคียวริตี้ บริการครบวงจรเจาะองค์กร. https://www.infoquest.co.th/2022/229408.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [สกมช.]. (ม.ป.). หน้าที่และอำนาจของสำนักงาน NCSA. https://www.ncsa.or.th/functions-and-powers-of-the-office.html

สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ. (2561). *ยุทธศาสตร์ชาติ พ.ศ. 2561-2580 (ฉบับย่อ).* สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. http://nscr.nesdc.go.th/wp-content/uploads/2023/06/NS_SumPlanOct2018.pdf.

หทัยกาญจน์ ตรีสุวรรณ. (2565, 18 กรกฎาคม). เพกาซัส สปายแวร์: ไอลอว์เปิดรายงานพบ 30 นักวิชาการ-นักกิจกรรมการเมืองไทยถูกสปายแวร์สอดแนม. *BBC News ไทย.* https://www.bbc.com/thai/thailand-62163614

*เอ็ม รีพอร์ต* [M Report]. (2565, 22 พฤศจิกายน). ไทย-จีน เซ็น MOU ปั้นนิคมฯ ส่งเสริมการลงทุนตามนโยบาย “หนึ่งแถบ หนึ่งเส้นทาง” ของจีนเชื่อมโยงสู่ “ไทยแลนด์ 4.0”. https://www.mreport.co.th/news/government-news/348-MOI-and-MOFCOM-signed-mou-to-drive-Belt-and-Road-Initiatives-and-Thailand-4.

*ไอลอว์* [iLaw]. (2564, 13 กรกฎาคม). มาตรา 112 ใช้แตกต่างกันไปตามสถานการณ์การเมือง. https://freedom.ilaw.or.th/node/934.

# ประวัติผู้เขียน

| | |
|---|---|
| **ชื่อ-สกุล** | ธนาวิทย์ หวังภุชเคนทร์ |
| **วัน เดือน ปี เกิด** | 27 มิถุนายน 2538 |
| **วุฒิการศึกษา** | คณะรัฐศาสตร์ความสัมพันธ์ระหว่างประเทศ จุฬาลงกรณ์มหาวิทยาลัย |
| **ผลงานตีพิมพ์** | Jittiang, Bhanubhatra, Worrawit Sirijintana, Tanawit Wangpuchakane. 2022. Ad Hoc and As Usual: The Thai Government's Responses to the Myanmar Crisis Since the 2021 Coup. Brisbane: Asia-Pacific Centre for the Responsibility to Protect<br>ธนาวิทย์ หวังภุชเคนทร์. 2567. การระบุตัวแสดง และบทบาทของผู้ประกอบการเชิงปทัสถานด้านความมั่นคงไซเบอร์สหรัฐฯ. วารสารรัฐศาสตร์และรัฐประศาสนศาสตร์, 15(1). |