

อำนาจไซเบอร์และบทบาทของสหรัฐอเมริกาในฐานะสมองของโลก*

CYBER POWER AND UNITED STATES AS THE GLOBAL BRAIN

อลงกรณ์ ศิลปดอนบม*, สุจิตตรา ฤทธิสกุลชัย

Alongkorn Sillapadonbom*, Suchittra Ritsakulchai

วิทยาลัยการเมืองการปกครอง มหาวิทยาลัยมหาสารคาม มหาสารคาม ประเทศไทย

College of Politics and Governance, Mahasarakham University, Mahasarakham, Thailand

*Corresponding author E-mail: alongkorn.liberty@gmail.com

*Tel: 094-503-4899

บทคัดย่อ

บทความวิจัยนี้ศึกษาบทบาทของสหรัฐอเมริกาในฐานะมหาอำนาจไซเบอร์ และเพื่อวิเคราะห์กลไกที่เอื้อต่อการเป็น “สมองของโลก” ในบริบทศตวรรษที่ 21 โดยใช้แนวคิดสมองของโลกควบคู่กับโครงสร้างโลกไซเบอร์ 4 ลำดับชั้นของ Clark, D. D. ได้แก่ ลำดับชั้นกายภาพ ลำดับชั้นตรรกะ ลำดับชั้นข้อมูล และลำดับชั้นผู้ใช้งาน งานวิจัยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ โดยอาศัยการวิจัยเอกสารจากแหล่งข้อมูลที่เกี่ยวข้องกับนโยบายความมั่นคงไซเบอร์ และพลวัตอำนาจในยุคดิจิทัลอย่างต่อเนื่องในช่วงศตวรรษที่ 21 ผลการศึกษาพบว่า สหรัฐอเมริกามีความได้เปรียบในทุกลำดับชั้นของโลกไซเบอร์ โดยเฉพาะกำหนดนโยบายพัฒนาไซเบอร์เพื่อส่งเสริมการควบคุมโครงสร้างพื้นฐานดิจิทัล นวัตกรรมทางเทคโนโลยีที่มีความเป็นผู้นำจากภาคเอกชน และอิทธิพลของบริษัทเทคโนโลยีขนาดใหญ่ อีกทั้งยังดำเนินยุทธศาสตร์ไซเบอร์อย่างครอบคลุม เช่น การลงทุนโครงสร้างพื้นฐาน ทรัพยากรมนุษย์ การสร้างพันธมิตร ช่วยให้สามารถกำหนดทิศทางข้อมูลและรักษาความเป็นผู้นำในระบบโลกได้อย่างต่อเนื่อง พลวัตของอำนาจการเมืองระหว่างประเทศ ได้เกิดความท้าทายจากการเพิ่มบทบาทของประเทศคู่แข่งอย่างจีน และรัสเซียทำให้การแข่งขันในโลกไซเบอร์รุนแรงขึ้น ก่อให้เกิดการแบ่งแยกทางเทคโนโลยี ดังนั้น อำนาจไซเบอร์จึงเป็นองค์ประกอบสำคัญของโครงสร้างอำนาจโลก โดยแนวคิดสมองของโลกมิได้สะท้อนระบบกระจายศูนย์อย่างสมบูรณ์ แต่แสดงถึงแนวโน้มการรวมศูนย์ข้อมูลในกลุ่มมหาอำนาจและบริษัทเทคโนโลยีขนาดใหญ่ ซึ่งสะท้อนการเปลี่ยนแปลงของอำนาจในยุคดิจิทัล และเน้นย้ำความสำคัญของการสร้างสมดุลระหว่างนวัตกรรม ความมั่นคง และการเข้าถึงข้อมูลอย่างเท่าเทียมในอนาคต พร้อมรับมือความเสี่ยงและความท้าทายด้านการกำกับดูแลอย่างมีประสิทธิภาพในระยะยาวต่อไปในอนาคต

คำสำคัญ: สมองของโลก, อำนาจไซเบอร์, สหรัฐอเมริกา, ความมั่นคงไซเบอร์, ความมั่นคงระหว่างประเทศ

Abstract

This research article examines the role of the United States as a cyber superpower and analyzes the mechanisms that facilitate its position as the “Global Brain” in the context of the 21st century. The study employs the concept of the Global Brain in conjunction with David D. Clark’s four-layer cyberspace framework, consisting of the physical layer, logical layer, information layer, and user layer. This research adopts a qualitative methodology based on documentary research,



drawing upon sources related to cybersecurity policy and the evolving dynamics of power in the digital era throughout the 21st century. The findings reveal that the United States possesses advantages across all layers of cyberspace, particularly through cyber development policies that promote control over digital infrastructure, technological innovation driven by private-sector leadership, and the influence of major technology companies. In addition, the United States has implemented comprehensive cyber strategies, including infrastructure investment, human resource development, and alliance-building, enabling it to shape information flows and sustain leadership within the international system. However, the dynamics of international political power have been challenged by the growing role of rival powers such as China and Russia, intensifying competition in cyberspace and contributing to technological fragmentation. Therefore, cyber power has become a crucial component of the global power structure. The concept of the Global Brain does not fully reflect a decentralized system; rather, it indicates a tendency toward the concentration of information within major powers and large technology corporations. This reflects the transformation of power in the digital age and underscores the importance of balancing innovation, security, and equitable access to information in the future, while effectively addressing governance risks and long-term challenges.

Keywords: Global Brain, Cyber Power, United States, Cybersecurity, International Security

บทนำ

ในศตวรรษที่ 21 โลกกำลังเผชิญการเปลี่ยนแปลงทางเทคโนโลยีครั้งใหญ่จากการพัฒนาเทคโนโลยีสารสนเทศ ปัญญาประดิษฐ์ (Artificial Intelligence) และระบบเครือข่ายอินเทอร์เน็ตระดับโลก ซึ่งส่งผลกระทบต่อโครงสร้างอำนาจในระบบระหว่างประเทศอย่างลึกซึ้ง (Floridi, L., 2014) การเข้าสู่ยุค “ข้อมูล คือ อำนาจ” ทำให้การควบคุมข้อมูล การประมวลผล และการไหลเวียนของสารสนเทศ กลายเป็นเครื่องมือสำคัญในการกำหนดความเป็นมหาอำนาจของรัฐในระบบโลก สหรัฐอเมริกาในฐานะผู้นำด้านเทคโนโลยีดิจิทัล มีบทบาทสำคัญในการสร้างโครงสร้างพื้นฐานทางไซเบอร์ระดับโลก ผ่านบริษัทเทคโนโลยีขนาดใหญ่ เช่น Google, Microsoft, Facebook (Meta), Amazon และ OpenAI ซึ่งได้กลายเป็นกลไกหลักของการผลิต ควบคุม และแลกเปลี่ยนข้อมูลในระดับโลก รวมถึงความได้เปรียบเชิงโครงสร้างในระบบไซเบอร์โลกอย่างชัดเจน โดยในปี ค.ศ. 2025 บริษัทสัญชาติสหรัฐอเมริกาครองส่วนแบ่งตลาดคลาวด์คอมพิวเตอร์ทั่วโลกมากกว่าร้อยละ 60 ผ่านผู้ให้บริการหลัก เช่น Amazon Web Services (AWS), Microsoft Azure และ Google Cloud ขณะเดียวกัน การลงทุนด้านความมั่นคงไซเบอร์ของรัฐบาลสหรัฐอเมริกา มีมูลค่าสูงกว่า 20,000 ล้านดอลลาร์สหรัฐต่อปี และมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง (The White House, 2023) การที่สหรัฐอเมริกา สามารถประสานระหว่างอำนาจทางเทคโนโลยี อำนาจทางเศรษฐกิจ และอิทธิพลทางวัฒนธรรม ทำให้ประเทศเข้าใกล้แนวคิด “Global Brain” หรือ “สมองของโลก” ระบบที่ข้อมูลและเทคโนโลยีของมนุษย์เชื่อมโยงกันในระดับโลกเหมือนระบบประสาทหนึ่งเดียว อย่างไรก็ตาม บทบาทดังกล่าวยังเผชิญความท้าทายจากประเทศคู่แข่ง เช่น จีนและรัสเซีย ซึ่งพยายามสร้าง “อธิปไตยทางดิจิทัล” (Digital Sovereignty) และลดการพึ่งพาเทคโนโลยีของสหรัฐอเมริกา การแข่งขันทางไซเบอร์ในปัจจุบันจึงไม่ใช่เพียงสงครามเทคโนโลยี แต่เป็นการแข่งขันเชิงโครงสร้างของอำนาจโลก (Devanny, J., 2024); (Healey, J. , 2018)

อย่างไรก็ตาม งานวิชาการที่มีอยู่ส่วนใหญ่สอดคล้องกับการศึกษาของ Nye, J. S. ที่อธิบายอำนาจไซเบอร์ในฐานะเครื่องมือของรัฐ ความมั่นคง และการแข่งขันเชิงยุทธศาสตร์ในโลกไซเบอร์ ขณะที่ Kello, L. ให้ความสำคัญกับการแข่งขันเชิงยุทธศาสตร์และพลวัตของอำนาจรัฐในโลกไซเบอร์ ส่วน Zuboff มุ่งอธิบายโครงสร้างเศรษฐกิจดิจิทัลและอำนาจของภาคเอกชน แม้งานเหล่านี้ช่วยอธิบายองค์ประกอบของอำนาจไซเบอร์ได้อย่างครอบคลุม แต่ยังขาดการบูรณาการมุมมองที่เชื่อมโยงระหว่างอำนาจรัฐ อำนาจเอกชน และโครงสร้างข้อมูลโลกเข้ากับกรอบแนวคิดเชิงระบบ เช่น แนวคิด “Global Brain” ซึ่งอธิบายโลกไซเบอร์ในฐานะระบบเครือข่ายข้อมูลที่ทำงานเสมือนระบบประสาทของโลก (Nye, J. S., 2017); (Kello, L., 2017)

ช่องว่างทางความรู้ที่น่าไปสู่คำถามสำคัญว่า ในบริบทของ ค.ศ. 2026 ซึ่งการแข่งขันทางไซเบอร์มีความเข้มข้นมากขึ้น และประเทศคู่แข่งอย่างจีนกำลังผลักดันแนวคิด “Digital Sovereignty” เพื่อลดการพึ่งพาเทคโนโลยีของสหรัฐอเมริกา บทบาทของสหรัฐอเมริกาในฐานะ “ศูนย์กลางข้อมูลโลก” มีความมั่นคงเพียงใด และสามารถอธิบายได้ผ่านกรอบแนวคิด “Global Brain” ในระดับใด อีกทั้ง การผสมผสานกันระหว่างอำนาจทางเทคโนโลยี อำนาจทางเศรษฐกิจ และอำนาจทางการเมืองในโลกไซเบอร์ของสหรัฐอเมริกา ส่งผลต่อโครงสร้างอำนาจโลกอย่างไร งานวิจัยนี้ใช้กรอบโครงสร้างโลกไซเบอร์ 4 ลำดับชั้นของ Clark, D. D. ได้แก่ physical, logical, information และ user layer เป็นฐานในการวิเคราะห์อำนาจไซเบอร์ของรัฐ (Clark, D. D., 2010)

ดังนั้น ปัญหาวิจัยของงานชิ้นนี้คือ การอธิบายลักษณะและขอบเขตของอำนาจไซเบอร์ของสหรัฐอเมริกาในฐานะศูนย์กลางของโครงสร้างเครือข่ายข้อมูลโลก ภายใต้บริบทการแข่งขันกับมหาอำนาจอื่นในศตวรรษที่ 21 โดยมุ่งเน้นการวิเคราะห์ว่าสหรัฐอเมริกาสามารถรักษาสถานะดังกล่าวได้มากน้อยเพียงใด

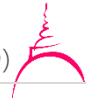
วัตถุประสงค์ของการวิจัย

เพื่อวิเคราะห์บทบาทของสหรัฐอเมริกาในฐานะมหาอำนาจทางไซเบอร์ที่มีความพยายามจะเป็น สมอของโลก (Global Brain)

วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ในรูปแบบการวิจัยเอกสาร (Documentary Research) โดยมุ่งศึกษาความเป็นอนาธิปไตยในโลกไซเบอร์และผลกระทบต่ออำนาจของสหรัฐอเมริกาในศตวรรษที่ 21 ผ่านการวิเคราะห์ข้อมูลจากแหล่งปฐมภูมิและทุติยภูมิอย่างเป็นระบบ แหล่งข้อมูลปฐมภูมิ ประกอบด้วย เอกสารทางการเมืองของรัฐบาลสหรัฐอเมริกา เช่น ยุทธศาสตร์และนโยบายด้านความมั่นคงไซเบอร์ เอกสารจากกระทรวงกลาโหม กองบัญชาการไซเบอร์สหรัฐ และคำสั่งจากทำเนียบขาว โดยกำหนดช่วงเวลาเอกสารระหว่างปี ค.ศ. 2010 - 2026 และคัดเลือกประมาณ 10 ถึง 20 ฉบับที่มีความเกี่ยวข้องโดยตรงกับการใช้อำนาจไซเบอร์ของรัฐ และเอกสารจากหน่วยงานด้านความมั่นคง เช่น กระทรวงกลาโหม และกองบัญชาการไซเบอร์สหรัฐอเมริกา ซึ่งสะท้อนแนวทางการใช้อำนาจไซเบอร์ของรัฐ ขณะที่แหล่งข้อมูลชั้นทุติยภูมิประกอบด้วยหนังสือ บทความวิชาการ และงานวิจัยที่เกี่ยวข้องกับอำนาจไซเบอร์ ความมั่นคงทางไซเบอร์ และความสัมพันธ์ระหว่างประเทศ โดยกำหนดช่วงเวลาเดียวกัน และคัดเลือกประมาณ 10 ถึง 20 ฉบับ

การเก็บรวบรวมข้อมูลดำเนินการผ่านการสืบค้นเอกสารออนไลน์ (Database Search) โดยใช้คำสำคัญ เช่น U.S. Cybersecurity, Cyber Power, Cyber Challenges และ Cyber and International Politics จากฐานข้อมูลวิชาการ เช่น Google Scholar และ ResearchGate รวมถึงเว็บไซต์หน่วยงานภาครัฐของสหรัฐอเมริกา เพื่อให้ได้ข้อมูลที่ถูกต้องและทันสมัย จากนั้นดำเนินการคัดกรองเอกสารอย่างเป็นระบบผ่าน 3 ขั้นตอน ได้แก่ 1) การคัดกรองจากชื่อเรื่องและบทคัดย่อ 2) การพิจารณาเนื้อหาฉบับเต็ม และ 3) การคัดเลือกขั้นสุดท้ายตามความสอดคล้องกับวัตถุประสงค์การวิจัย โดยใช้เกณฑ์การคัดเลือก (inclusion criteria) เช่น ความเกี่ยวข้องโดยตรงกับอำนาจไซเบอร์



การเป็นงานวิชาการที่ผ่านการประเมินโดยผู้ทรงคุณวุฒิหรือเอกสารทางการของรัฐ และการเผยแพร่ในช่วงปีที่กำหนด ขณะที่เกณฑ์การคัดออก (exclusion criteria) ได้แก่ เอกสารที่ขาดความน่าเชื่อถือ ไม่มีแหล่งอ้างอิงชัดเจน เน้นเชิงเทคนิคเฉพาะด้านโดยไม่เชื่อมโยงกับมิติอำนาจ หรือมีความซ้ำซ้อนของเนื้อหา การวิเคราะห์ข้อมูลใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) โดยเริ่มจากการเข้ารหัสข้อมูล (coding) เพื่อระบุประเด็นสำคัญ เช่น อำนาจไซเบอร์ โครงสร้างพื้นฐานดิจิทัล ความเป็นอนาธิปไตยในไซเบอร์ และการแข่งขันระหว่างมหาอำนาจ จากนั้นนำรหัสมาจัดหมวดหมู่ (categorization) ตามกรอบแนวคิดหลัก ได้แก่ มิติอำนาจ มิติโครงสร้างไซเบอร์ และมิติการแข่งขันเชิงภูมิรัฐศาสตร์ ก่อนทำการสังเคราะห์และตีความ (synthesis and interpretation) โดยเชื่อมโยงกับกรอบแนวคิด “Global Brain” และแนวคิดโครงสร้างโลกไซเบอร์ 4 ลำดับชั้น ของ Clark, D. D. ได้แก่ Physical, Logical, Information และ User Layer นอกจากนี้ ยังใช้วิธีการตรวจสอบความน่าเชื่อถือของข้อมูล (triangulation) โดยเปรียบเทียบข้อมูลจากแหล่งปฐมภูมิและทุติยภูมิ เพื่อเพิ่มความถูกต้องและความน่าเชื่อถือของข้อค้นพบในการวิจัย

กรอบแนวคิดทั้งสองถูกนำมาใช้ร่วมกันเป็นเครื่องมือในการวิเคราะห์ โดยแนวคิด “Global Brain” ใช้เพื่ออธิบายลักษณะของโลกไซเบอร์ในฐานะเครือข่ายข้อมูลระดับโลกที่เชื่อมโยงกันอย่างซับซ้อน ขณะที่กรอบโครงสร้างโลกไซเบอร์ 4 ลำดับชั้น (Physical, Logical, Information และ User Layer) ถูกใช้เพื่อจำแนกและวิเคราะห์อำนาจไซเบอร์ของสหรัฐอเมริกาในแต่ละระดับของโครงสร้างดังกล่าว การบูรณาการกรอบแนวคิดทั้งสองช่วยให้สามารถวิเคราะห์ความสัมพันธ์ระหว่างโครงสร้างไซเบอร์กับอำนาจรัฐ รวมถึงประเมินความท้าทายจากตัวแสดงอื่นในระบบระหว่างประเทศได้อย่างเป็นระบบ

ผลการวิจัย

ผลการวิจัยพบว่า บทบาทของสหรัฐอเมริกาในฐานะมหาอำนาจไซเบอร์สามารถอธิบายได้ผ่านการสะสม “ความได้เปรียบเชิงโครงสร้าง” (structural asymmetry) ที่พัฒนาต่อเนื่องมาตั้งแต่หลังสงครามโลก และขยายตัวอย่างชัดเจนในยุคดิจิทัล ความได้เปรียบดังกล่าวไม่ได้จำกัดอยู่เพียงด้านเทคโนโลยี แต่ครอบคลุมถึงการควบคุมโครงสร้างพื้นฐานข้อมูล การพัฒนาแพลตฟอร์มดิจิทัล และการบูรณาการระหว่างรัฐกับภาคเอกชน ซึ่งสอดคล้องกับแนวคิด “Global Brain” กล่าวคือ สหรัฐอเมริกามีบทบาทเป็นศูนย์กลางของเครือข่ายข้อมูลโลกทั้งในมิติของการประมวลผล การจัดเก็บ และการไหลเวียนของข้อมูล อย่างไรก็ตาม โครงสร้างดังกล่าวก่อให้เกิดความเปราะบาง (vulnerability) ควบคู่กัน เนื่องจากการพึ่งพาเทคโนโลยีไซเบอร์ในระดับสูงทำให้โครงสร้างพื้นฐานสำคัญ เช่น ระบบพลังงาน ระบบการเงิน และเครือข่ายการสื่อสาร กลายเป็นเป้าหมายของการโจมตีทางไซเบอร์ และการแทรกแซงข้อมูล

ในเชิงโครงสร้างอำนาจไซเบอร์ ผลการวิจัยชี้ให้เห็นว่า สหรัฐอเมริกาส่งเสริมความได้เปรียบผ่านการพัฒนา “ระบบนิเวศไซเบอร์” (cyber ecosystem) ที่เชื่อมโยงภาครัฐ ภาคเอกชน และสถาบันวิจัยเข้าด้วยกันอย่างเป็นระบบ โดยภาคเอกชนมีบทบาทสำคัญในการพัฒนาเทคโนโลยีและโครงสร้างพื้นฐาน เช่น Amazon Web Services (AWS), Microsoft Azure และ Google Cloud ซึ่งครองสัดส่วนหลักของตลาดคลาวด์โลก ขณะที่ภาครัฐทำหน้าที่กำหนดยุทธศาสตร์และสร้างกลไกด้านความมั่นคง เช่น การจัดตั้งกองบัญชาการไซเบอร์สหรัฐอเมริกา (USCYBERCOM) และการดำเนินนโยบาย “defend forward” เพื่อตอบโต้ภัยคุกคามตั้งแต่ต้นทาง การบูรณาการดังกล่าวทำให้สหรัฐอเมริกาสามารถควบคุมทั้งมิติของโครงสร้างพื้นฐาน (infrastructure) และมิติของข้อมูล (information layer) ได้อย่างมีประสิทธิภาพ ซึ่งเป็นองค์ประกอบสำคัญของการทำหน้าที่เป็น “Global Brain” อย่างไรก็ตาม การพัฒนาในมิตินี้ยังนำไปสู่การแข่งขันที่เข้มข้นจากประเทศคู่แข่ง และเพิ่มความเสี่ยงจากการโจมตีแบบ state-sponsored cyber attacks

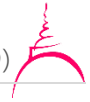
ในระดับโครงสร้างพื้นฐานเชิงกายภาพเชิงกายภาพ ผลการวิจัยพบว่า สหรัฐอเมริกามีความได้เปรียบอย่างมีนัยสำคัญในด้านโครงข่ายสื่อสารและการจัดเก็บข้อมูลระดับโลก การสร้างและจ่ายพลังงานไปยังระบบต่าง ๆ สร้างความท้าทายต่อการสร้างความมั่นคงในการปกป้องระบบไฟฟ้า ซึ่งเป็นหนึ่งในโครงสร้างพื้นฐานที่สำคัญของประเทศสหรัฐอเมริกา และการปกป้องการพัฒนาเทคโนโลยีเพื่อสร้างความก้าวหน้าในลำดับถัดไป อาทิเช่น การพัฒนาปัญญาประดิษฐ์อัจฉริยะ ที่จะมีบทบาทสำคัญต่อโลกไซเบอร์ ด้วยการทำงานที่ซับซ้อนมากยิ่งขึ้น อาทิเช่น การใช้ปัญญาประดิษฐ์ในการสร้างความมั่นคงทางไซเบอร์ เป็นต้น

การได้เปรียบเชิงกายภาพอีกหนึ่งมิติสำคัญของสหรัฐอเมริกา คือบทบาทของบริษัทเอกชนในการพัฒนาและควบคุมโครงสร้างพื้นฐานสายเคเบิลใต้น้ำ (submarine cables) ซึ่งเป็นแกนหลักของการสื่อสารข้อมูลระดับโลก โดยในปัจจุบัน บริษัทเทคโนโลยีสหรัฐอเมริกา เช่น Google Meta และ Microsoft มีบทบาทโดยตรงในการลงทุนและเป็นเจ้าของร่วมในโครงการสายเคเบิลใต้น้ำจำนวนมาก เช่น Dunant (เชื่อมสหรัฐ - ยุโรป) และ Curie (เชื่อมสหรัฐ - อเมริกาใต้) ซึ่งช่วยเพิ่มความเร็วและเสถียรภาพของการส่งข้อมูลข้ามทวีปอย่างมีนัยสำคัญ ทั้งนี้ มีการประเมินว่ามากกว่าร้อยละ 95 ของข้อมูลอินเทอร์เน็ตระหว่างประเทศถูกส่งผ่านสายเคเบิลใต้น้ำ ทำให้โครงสร้างดังกล่าวเปรียบเสมือน “ระบบประสาทหลักของโลกไซเบอร์” และนอกจากบทบาทของสายเคเบิลใต้น้ำในฐานะโครงสร้างพื้นฐานด้านการสื่อสารแล้ว ผลการวิจัยยังสะท้อนว่าการควบคุมโครงข่ายดังกล่าวมีนัยเชิงภูมิรัฐศาสตร์ เนื่องจากโครงสร้างพื้นฐานเหล่านี้ไม่เพียงรองรับการไหลของข้อมูล แต่เป็นฐานของอำนาจในการกำหนดความมั่นคง การเข้าถึงข้อมูล และความได้เปรียบเชิงยุทธศาสตร์ในระบบโลก การที่บริษัทเทคโนโลยีสหรัฐอเมริกามีบทบาทในการลงทุนและเป็นเจ้าของร่วมในโครงสร้างดังกล่าว จึงสะท้อนการผกผันกันระหว่างอำนาจเอกชนกับอำนาจรัฐในมิติ physical layer อย่างชัดเจน

ความพยายามปิดกั้นการเข้าแทรกแซงจากประเทศอื่น ๆ ถือเป็นการสร้างความมั่นคงไซเบอร์ของประเทศสหรัฐอเมริกาด้วยเช่นกัน ดังนั้น ประเทศสหรัฐอเมริกาจึงมีการก่อตั้งกองบัญชาการไซเบอร์สหรัฐ เพื่อรองรับการปฏิบัติการการสร้างความมั่นคงทางไซเบอร์ทั้งเชิงรุกและเชิงรับ เพื่อป้องกันความเสียหายต่อโครงสร้างพื้นฐานของประเทศ ที่อาจนำมาสู่การทำลายเศรษฐกิจได้อย่างมหาศาล อาทิเช่น กรณีศึกษาเหตุการณ์การโจมตี SolarWinds cyberattack สะท้อนให้เห็นถึงข้อจำกัดเชิงโครงสร้างของอำนาจไซเบอร์ของสหรัฐอเมริกาอย่างชัดเจน กล่าวคือ แม้สหรัฐอเมริกาจะมีความได้เปรียบในฐานะศูนย์กลางของโครงสร้างข้อมูลโลกตามแนวคิด “Global Brain” แต่ยิ่งโครงสร้างดิจิทัลมีความเชื่อมโยงสูงและมีประสิทธิภาพมากเท่าใด ระดับความเปราะบางเชิงระบบก็ยิ่งเพิ่มขึ้นตามไปด้วย ความเชื่อมโยงดังกล่าวทำให้การโจมตีได้จำกัดอยู่ที่การเจาะระบบโดยตรง แต่สามารถอาศัยห่วงโซ่อุปทานซอฟต์แวร์เป็นช่องทางแทรกซึมเข้าสู่โครงสร้างพื้นฐานสำคัญของรัฐได้ ข้อค้นพบนี้สะท้อนว่าอำนาจไซเบอร์มิได้หมายถึงการมีความเหนือกว่าด้านขีดความสามารถเท่านั้น แต่รวมถึงความสามารถในการบริหารจัดการความเปราะบางของระบบที่ตนเองสร้างขึ้นด้วย ความเชื่อมโยงของระบบซอฟต์แวร์และเครือข่ายในระดับสูงกลับสร้างช่องโหว่ที่เปิดโอกาสให้ผู้ไม่หวังดีสามารถแทรกซึมผ่านห่วงโซ่อุปทาน (supply chain) ได้ เหตุการณ์ดังกล่าวจึงชี้ให้เห็นว่า การมีอำนาจเหนือโครงสร้างไซเบอร์ไม่ได้หมายถึงความปลอดภัยโดยสมบูรณ์ หากแต่ต้องเผชิญกับความเสี่ยงเชิงระบบ (systemic risk) ที่เพิ่มขึ้นตามระดับของการพึ่งพาและการเชื่อมโยงของโครงสร้างดิจิทัล

อภิปรายผล

ผลการศึกษานี้สะท้อนให้เห็นว่าสหรัฐอเมริกายังคงดำรงบทบาทเป็นมหาอำนาจทางไซเบอร์ที่มีอิทธิพลต่อโครงสร้างอำนาจของระบบระหว่างประเทศในศตวรรษที่ 21 อย่างมีนัยสำคัญ โดยข้อค้นพบดังกล่าวมีความสอดคล้องกับงานศึกษาหลายชิ้นในวรรณกรรมที่เกี่ยวข้อง



ประการแรก สหรัฐอเมริกาสามารถควบคุมทั้ง “information layer” และ “physical layer” ตามกรอบการวิเคราะห์ของ Clark, D. D. ผ่านบทบาทของบริษัทเทคโนโลยีขนาดใหญ่ เช่น Amazon Web Services, Microsoft Azure และ Google Cloud เมื่อพิจารณาในมิติของ information layer ข้อค้นพบยังสะท้อนว่าอำนาจของสหรัฐอเมริกาไม่ได้จำกัดอยู่เพียงการครอบครองข้อมูลในเชิงปริมาณ แต่รวมถึงความสามารถในการกำหนดโครงสร้างการไหลเวียนของข้อมูล การประมวลผล และการเข้าถึงข้อมูลในระดับโลกผ่านแพลตฟอร์มและระบบคลาวด์ขนาดใหญ่ ความได้เปรียบดังกล่าวทำให้ information layer มีได้เป็นเพียงมิติของข้อมูล แต่เป็นพื้นที่เชิงอำนาจที่เอื้อต่อการกำหนดพฤติกรรม มาตรฐาน และทิศทางของระบบดิจิทัลโลก ควบคู่กับการจัดตั้ง United States Cyber Command และการดำเนินยุทธศาสตร์เชิงรุก เช่น defend forward ซึ่งสะท้อนถึงการแปลงศักยภาพเชิงโครงสร้างให้เป็นอำนาจเชิงยุทธศาสตร์ได้อย่างมีประสิทธิภาพ สอดคล้องกับการศึกษาของ Singer, P. W. & Friedman, A. ที่มองว่าอำนาจไซเบอร์เกี่ยวข้องกับการควบคุมทั้งโครงสร้างและการปฏิบัติการ ขณะเดียวกันในระดับ physical layer ข้อค้นพบแสดงให้เห็นว่าอำนาจไซเบอร์ของสหรัฐอเมริกาไม่ได้ตั้งอยู่บนโครงสร้างพื้นฐานทางกายภาพในฐานะทรัพยากรประกอบเท่านั้น แต่โครงสร้างดังกล่าวเป็นฐานรองรับอำนาจเชิงยุทธศาสตร์ของรัฐทั้งในมิติของศูนย์ข้อมูล เครือข่ายคลาวด์ โครงข่ายการสื่อสาร และสายเคเบิลใต้น้ำที่รองรับการไหลของข้อมูลระดับโลก ความได้เปรียบในระดับนี้จึงมีนัยเกินกว่าความเหนือกว่าทางเทคนิค แต่สะท้อนการครอบครองตำแหน่งเชิงโครงสร้าง (structural position) ภายในโลกไซเบอร์ ซึ่งสอดคล้องกับกรอบวิเคราะห์ของ Clark, D. D. และข้อค้นพบเกี่ยวกับบทบาทโครงสร้างพื้นฐานข้อมูลโลกของสหรัฐอเมริกา เมื่อ information layer และ physical layer ทำงานเชื่อมโยงกัน ข้อค้นพบจึงชี้ว่า ความได้เปรียบของสหรัฐอเมริกาไม่ได้อยู่ในแต่ละลำดับชั้นแบบแยกส่วน หากแต่เกิดจากการบูรณาการข้ามลำดับชั้น (cross-layer integration) ซึ่งเป็นกลไกสำคัญที่ทำให้สหรัฐอเมริกาสามารถแปลงความได้เปรียบเชิงโครงสร้างให้กลายเป็นอำนาจไซเบอร์เชิงยุทธศาสตร์ และเข้าใกล้คุณลักษณะของ “Global Brain” ตามกรอบการวิเคราะห์ของการศึกษานี้ (Clark, D. D., 2010); (Singer, P. W. & Friedman, A., 2013); (TeleGeography, 2023)

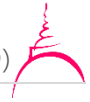
ประการที่สอง ผลการวิจัยยังชี้ให้เห็น “ความอ่อนแอเชิงโครงสร้าง” ของอำนาจไซเบอร์ คือ ความได้เปรียบที่เกิดจากการเชื่อมโยงของระบบในระดับสูงกลับก่อให้เกิดความเปราะบางเชิงระบบ (systemic vulnerability) โดยเฉพาะในลักษณะของการโจมตีแบบห่วงโซ่อุปทาน กรณี SolarWinds cyberattack แสดงให้เห็นอย่างชัดเจนว่าผู้โจมตีสามารถแทรกซึมผ่านซอฟต์แวร์ที่เชื่อถือได้และเข้าถึงโครงสร้างสำคัญของรัฐได้โดยไม่ถูกตรวจจับในระยะเริ่มต้น ซึ่งสอดคล้องกับรายงานของ Cybersecurity and Infrastructure Security Agency และสะท้อนว่าการเป็นศูนย์กลางของโครงสร้างข้อมูลโลกมิได้แปลว่ามีความมั่นคงโดยสมบูรณ์ หากแต่ต้องเผชิญความเสี่ยงที่ขยายตัวตามระดับของการเชื่อมโยง อีกประเด็นหนึ่งที่ผลการศึกษาส่งสะท้อน คือ อำนาจไซเบอร์มิได้เป็นเพียงอำนาจเชิงโครงสร้าง (structural power) แต่ยังมีลักษณะเป็นอำนาจเชิงความสัมพันธ์ (relational power) กล่าวคือ ความได้เปรียบของสหรัฐอเมริกาไม่ได้เกิดจากการควบคุมโครงสร้างพื้นฐานดิจิทัลเพียงอย่างเดียว แต่รวมถึงความสามารถในการกำหนดมาตรฐาน พฤติกรรม และบรรทัดฐานของตัวแสดงอื่นในระบบไซเบอร์ระหว่างประเทศด้วย ในมิตินี้ อำนาจไซเบอร์จึงมีลักษณะใกล้เคียงกับการสร้างอำนาจในการกำหนดบรรทัดฐานและกติกา ซึ่งช่วยให้สหรัฐอเมริกาดำรงสถานะผู้นำในระบบโลกไซเบอร์ได้อย่างต่อเนื่อง ข้อค้นพบดังกล่าวสอดคล้องกับ Nye ที่มองว่าอำนาจในไซเบอร์มิได้จำกัดอยู่เพียงการบังคับเชิงอำนาจ แต่รวมถึงความสามารถในการกำหนดเงื่อนไขและพฤติกรรมของผู้อื่นผ่านโครงสร้างเครือข่ายด้วยเช่นกัน ดังนั้น อำนาจไซเบอร์มิได้เป็นเพียงส่วนขยายของอำนาจรัฐแบบดั้งเดิม แต่มีลักษณะเปลี่ยนแปลงธรรมชาติของอำนาจเอง กล่าวคือ เดิมอำนาจมักถูกอธิบายผ่านทรัพยากรทางทหาร เศรษฐกิจ หรือดินแดน แต่ในโลกไซเบอร์ อำนาจปรากฏผ่านความสามารถในการควบคุมโครงสร้างเครือข่ายการกำหนดการไหลของข้อมูล และการจัดระเบียบพื้นที่ดิจิทัล ข้อค้นพบนี้สะท้อนว่า อำนาจไซเบอร์ ไม่ได้เป็นเพียงองค์ประกอบ

ใหม่ของอำนาจรัฐ แต่กำลังปรับเปลี่ยนวิธีทำความเข้าใจอำนาจในระบบระหว่างประเทศเอง (Cybersecurity and Infrastructure Security Agency, 2021); (Nye, J. S., 2017)

ประการที่สาม ในมิติของเศรษฐกิจดิจิทัลและอำนาจของภาคเอกชน ผลการศึกษาชี้ให้เห็นถึงบทบาทของบริษัทเทคโนโลยีขนาดใหญ่ของสหรัฐอเมริกาในการควบคุมข้อมูลและแพลตฟอร์มดิจิทัลระดับโลก ซึ่งสอดคล้องกับแนวคิดที่อธิบายถึง “surveillance capitalism” ว่าเป็นรูปแบบใหม่ของอำนาจที่เกิดจากการครอบครองและใช้ประโยชน์จากข้อมูลผู้ใช้งานในระดับมหาสถาบัน ส่งผลให้บริษัทเทคโนโลยีไม่ได้เป็นเพียงตัวแสดงทางเศรษฐกิจ แต่กลายเป็นตัวแสดงเชิงอำนาจในระบบระหว่างประเทศ (Zuboff, 2019) และในมิติของโครงสร้างพื้นฐานเชิงกายภาพ ผลการวิจัยชี้ให้เห็นว่าการควบคุม “โครงข่ายการไหลของข้อมูล” เป็นปัจจัยกำหนดอำนาจไซเบอร์ที่สำคัญ โดยเฉพาะโครงสร้างสายเคเบิลใต้น้ำที่บริษัทสหรัฐ เช่น Google, Meta และ Microsoft มีบทบาทลงทุนและเป็นเจ้าของร่วม ซึ่งรองรับข้อมูลระหว่างประเทศมากกว่าร้อยละ 95 ข้อค้นพบนี้แสดงให้เห็นว่า “Global Brain” ในทางปฏิบัติไม่ได้กระจายศูนย์อย่างสมบูรณ์ แต่มีลักษณะของการรวมศูนย์เชิงโครงสร้างอยู่ในกลุ่มประเทศและบริษัทเทคโนโลยีขนาดใหญ่ โดยเฉพาะสหรัฐอเมริกา (TeleGeography, 2023); (International Telecommunication Union, 2022)

อย่างไรก็ตาม ผลการศึกษา ยังพบว่า บทบาทของสหรัฐอเมริกากำลังเผชิญความท้าทายจากการเพิ่มขึ้นของมหาอำนาจอื่น โดยเฉพาะจีนและรัสเซีย ซึ่งสอดคล้องกับการศึกษาของ Segal, A. ที่ชี้ให้เห็นแนวโน้มของ “digital sovereignty” และความพยายามของรัฐในการควบคุมโครงสร้างไซเบอร์ภายใต้อธิปไตยของตน ขณะเดียวกัน Devanny, J. อธิบายว่า การแข่งขันทางไซเบอร์กำลังพัฒนาไปสู่การแข่งขันเชิงโครงสร้างของอำนาจโลก แนวโน้มดังกล่าวนำไปสู่ภาวะการแบ่งขั้วทางเทคโนโลยี (technological fragmentation) ซึ่งลดทอนลักษณะความเป็นสากลของอินเทอร์เน็ต อีกทั้งผลการวิจัยยังสะท้อนว่า การรักษาสถานะอำนาจไซเบอร์ในอนาคตมิได้ขึ้นอยู่กับการพัฒนาเทคโนโลยีเพียงลำพัง แต่ขึ้นอยู่กับความสามารถในการรักษาสสมดุลระหว่างนวัตกรรม ความมั่นคง และการกำกับดูแลโครงสร้างดิจิทัลด้วย ความท้าทายจากการแข่งขันของจีนและรัสเซียได้หมายความว่าบทบาทของสหรัฐอเมริกาในฐานะ “Global Brain” ลดลงโดยตรง หากแต่สะท้อนการเปลี่ยนผ่านของโครงสร้างดังกล่าวไปสู่รูปแบบที่มีการแข่งขันและการต่อรองสูงขึ้น กล่าวคือ “Global Brain” มิได้หายไป แต่กำลังเผชิญการจัดระเบียบใหม่ภายใต้การแข่งขันเชิงอำนาจในโลกไซเบอร์ ข้อเสนอเชิงนโยบายจากงานวิจัยนี้จึงเน้นให้รัฐให้ความสำคัญกับการสร้างความร่วมมือด้านบรรทัดฐานระหว่างประเทศเพื่อลดความขัดแย้งเชิงโครงสร้างในโลกไซเบอร์ การลดความเสี่ยงของห่วงโซ่อุปทานดิจิทัล และ ความสามารถในการรับมือและฟื้นตัวของโครงสร้างพื้นฐานไซเบอร์เมื่อมีความเสียหายเกิดขึ้น อินเทอร์เน็ต (Segal, A., 2016); (Devanny, J., 2024)

สุดท้าย เมื่อพิจารณาผลการศึกษาในกรอบแนวคิด “Global Brain” พบว่า แม้แนวคิดมองว่าโลกไซเบอร์เป็นระบบเครือข่ายแบบกระจายศูนย์ (decentralized system) แต่ในทางปฏิบัติ ผลการศึกษากลับสะท้อนแนวโน้มของการรวมศูนย์อำนาจข้อมูล (data centralization) อยู่ในกลุ่มประเทศมหาอำนาจและบริษัทเทคโนโลยีขนาดใหญ่ โดยเฉพาะสหรัฐอเมริกา ซึ่งชี้ให้เห็นว่าโครงสร้างของ infosphere ในยุคดิจิทัลไม่ได้กระจายอำนาจอย่างสมบูรณ์ แต่มีลักษณะของการกระจุกตัวของอำนาจเชิงข้อมูล อีกด้าน ข้อค้นพบยังสะท้อน “ความย้อนแย้งของการกระจุกตัวของอำนาจข้อมูล” กล่าวคือ การรวมศูนย์ข้อมูลและแพลตฟอร์มไว้ในกลุ่มตัวแสดงหลักช่วยสร้างประสิทธิภาพ นวัตกรรม และความสามารถในการกำหนดทิศทางของระบบไซเบอร์โลก แต่ในอีกด้านกลับเพิ่มความเสี่ยงเชิงระบบ การพึ่งพิง และความไม่สมดุลของอำนาจในระดับโลก ความย้อนแย้งดังกล่าวชี้ว่า “Global Brain” มิได้เป็นเพียงระบบปัญญาร่วมของโลก แต่เป็นพื้นที่แข่งขันของการรวมศูนย์อำนาจเชิงข้อมูลด้วยเช่นกัน (Heylighen, F. & Lenartowicz, M., 2017); (Kyriazis, M., 2015); (Floridi, L., 2014)



ดังนั้น อภิปรายผลของการศึกษานี้ชี้ให้เห็นว่า อำนาจไซเบอร์ของสหรัฐอเมริกาไม่ได้เป็นเพียงผลจากความก้าวหน้าทางเทคโนโลยีเท่านั้น แต่เป็นผลจากการบูรณาการระหว่างโครงสร้างพื้นฐาน เทคโนโลยี นโยบายรัฐ และอำนาจของภาคเอกชน ซึ่งทำให้สหรัฐอเมริกาสามารถเข้าใกล้การเป็น “ศูนย์กลางของสมองโลก” ได้ และมีความกระฉุกตัวทางข้อมูล อย่างไรก็ตาม แนวโน้มการแข่งขันและการแบ่งขั้วทางเทคโนโลยีกำลังท้าทายบทบาทดังกล่าว และอาจนำไปสู่การปรับเปลี่ยนโครงสร้างอำนาจของโลกไซเบอร์ในอนาคต

สรุปและข้อเสนอแนะ

งานวิจัยนี้ต่อบัตถุประสงค์ได้อย่างชัดเจนว่า สหรัฐอเมริกามีบทบาทเป็น “Global Brain” ในเชิงโครงสร้าง โดยทำหน้าที่เป็นศูนย์กลางของการประมวลผล ควบคุม กำหนดการไหลเวียนของข้อมูลระดับโลก ผ่านการบูรณาการโครงสร้างพื้นฐานดิจิทัล แพลตฟอร์มข้อมูล และกลไกรัฐเข้าด้วยกันในระบบเดียว อย่างไรก็ตาม บทบาทดังกล่าวมีลักษณะเป็น “อำนาจควบคุมความเปราะบาง” เนื่องจากความเชื่อมโยงของระบบไซเบอร์ในระดับสูงเพิ่มความเสี่ยงเชิงระบบ ดังที่ปรากฏในกรณี SolarWinds ผลการวิจัยยังเสนอว่าแนวคิด “Global Brain” สามารถใช้เป็นกรอบวิเคราะห์อำนาจไซเบอร์ที่เชื่อมโยงระดับโครงสร้าง ข้อมูล และการกำกับดูแลเข้าด้วยกัน ซึ่งช่วยขยายการศึกษาความสัมพันธ์ระหว่างประเทศในยุคดิจิทัลให้ก้าวพ้นการมองอำนาจผ่านรัฐและกำลังทางทหารแบบดั้งเดิม ไปสู่การทำความเข้าใจอำนาจในฐานะการครอบครองและจัดระเบียบเครือข่ายข้อมูลระดับโลก และเพื่อให้แนวคิด “Global Brain” มีความชัดเจนเชิงแบบจำลอง งานวิจัยเสนกรอบแนวคิด 3 ระดับในการวิเคราะห์คุณสมบัติการเป็นสมองของโลกในแต่ละประเทศมหาอำนาจ ได้แก่ 1) Infrastructure Layer หรือ โครงสร้างพื้นฐานที่รองรับการไหลของข้อมูล 2) Data & Platform Layer หรือ ระบบแพลตฟอร์มที่ควบคุมและประมวลผลข้อมูล และ 3) Governance & Security Layer หรือ ความสามารถของกลไกรัฐที่กำกับและป้องกันภัยคุกคาม การบูรณาการของทั้งสามระดับนี้ทำให้สหรัฐอเมริกาสามารถรักษาสถานะศูนย์กลางของระบบไซเบอร์โลกได้ ซึ่งเป็นการต่อยอดจากกรอบ 4 ลำดับชั้นของ Clark, D. D. ข้อเสนอเชิงทฤษฎี สามารถนำไปใช้เป็นกรอบวิเคราะห์อำนาจไซเบอร์ การแข่งขันเชิงโครงสร้าง และการกำหนดนโยบายความมั่นคงไซเบอร์ของรัฐได้ ข้อเสนอแนะจากการวิจัย คือ รัฐควรให้ความสำคัญกับการพัฒนาโครงสร้างพื้นฐานดิจิทัล การเสริมความมั่นคงของห่วงโซ่อุปทานไซเบอร์ และการกำกับบทบาทของบริษัทเทคโนโลยีข้ามชาติในฐานะตัวแสดงร่วมทางอำนาจ ขณะที่การนำผลการวิจัยไปใช้สามารถประยุกต์ต่อยอดในด้านการวิเคราะห์ยุทธศาสตร์ไซเบอร์ การออกแบบนโยบายสาธารณะ และการศึกษาพลวัตอำนาจในความสัมพันธ์ระหว่างประเทศ สำหรับการวิจัยครั้งต่อไปควรศึกษาวิเคราะห์เชิงเปรียบเทียบกับมหาอำนาจอื่น เช่น จีนและรัสเซีย เพื่อประเมินแนวโน้มการกระจายหรือการแตกตัวของ “Global Brain” รวมทั้งศึกษาบทบาทของเทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ Web 3.0 และพลวัตของ digital sovereignty ที่อาจเปลี่ยนโครงสร้างอำนาจโลกดิจิทัลในอนาคต

กิตติกรรมประกาศ

บทความวิจัยนี้เป็นส่วนหนึ่งของปริญญาโท สาขาวิชารัฐศาสตร์ วิทยาลัยการเมืองการปกครอง มหาวิทยาลัยมหาสารคาม เรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกา ในศตวรรษที่ 21

เอกสารอ้างอิง

- Clark, D. D. (2010). Characterizing Cyberspace: Past, Present and Future. Retrieved August 19, 2025, from <https://dspace.mit.edu/handle/1721.1/141692>
- Cybersecurity and Infrastructure Security Agency. (2021). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations. Retrieved April 23, 2026, from <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a>
- Devanny, J. (2024). Artificial intelligence and cyber power: Foreign policy implications. Retrieved August 4, 2025, from <https://shorturl.asia/LM698>
- Floridi, L. (2014). The fourth revolution: How the infosphere is reshaping human reality. Retrieved August 4, 2025, from <https://www.oii.ox.ac.uk/research/publications/the-fourth-revolution>
- Healey, J. (2018). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 4(1), 1-15.
- Heylighen, F. & Lenartowicz, M. (2017). The Global Brain as a model of the future information society: An introduction to the special issue. *Technological Forecasting and Social Change*, 114, 44-50. <https://doi.org/10.1016/j.techfore.2016.10.063>
- International Telecommunication Union. (2022). Measuring digital development: Facts and figures 2022. Retrieved April 23, 2026, from <https://shorturl.asia/Fh2Ou>
- Kello, L. (2017). The virtual weapon and international order. Retrieved August 20, 2025, from <https://shorturl.asia/2eXV4>
- Kyriazis, M. (2015). Systems neuroscience in focus: From the human brain to the global brain? *Frontiers in Systems Neuroscience*, 9, 1-4. <https://doi.org/10.3389/fnsys.2015.00007>
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44-71.
- Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. Retrieved August 25, 2025, from <https://shorturl.asia/V6EnO>
- Singer, P. W. & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press.
- TeleGeography. (2023). Do submarine cables account for over 99% of intercontinental data traffic? Retrieved April 23, 2026, from <https://shorturl.asia/oqpU0>
- The White House. (2023). National Cyber Workforce and Education Strategy. Retrieved August 2, 2025, from <https://shorturl.asia/Xo39H>