ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกา ในศตวรรษที่ 21

วิทยานิพนธ์

ของ

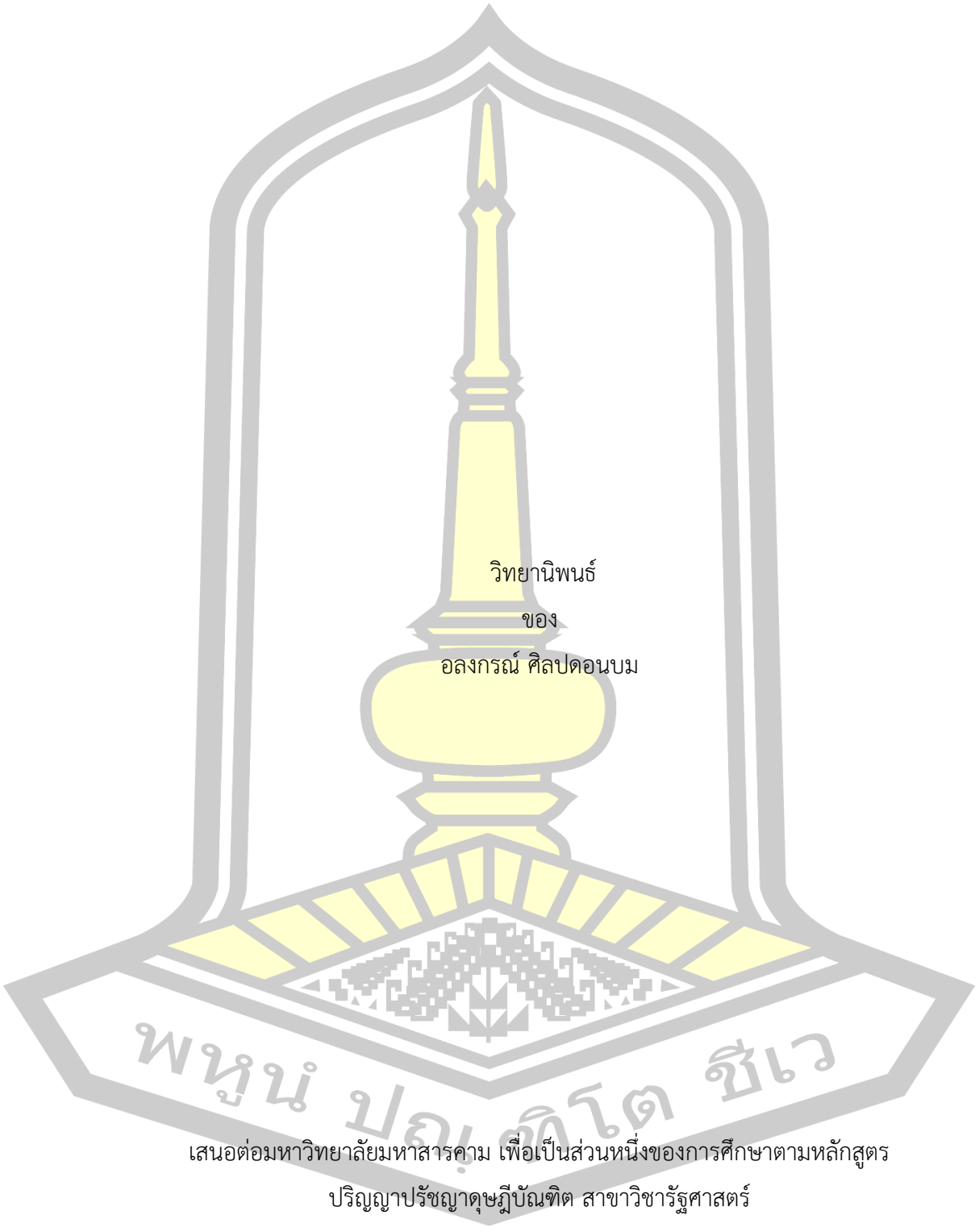
อลงกรณ์ ศิลปดอนบม

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชารัฐศาสตร์

เมษายน 2568

ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกา ในศตวรรษที่ 21



วิทยานิพนธ์

ของ

อลงกรณ์ ศิลปดอนบม

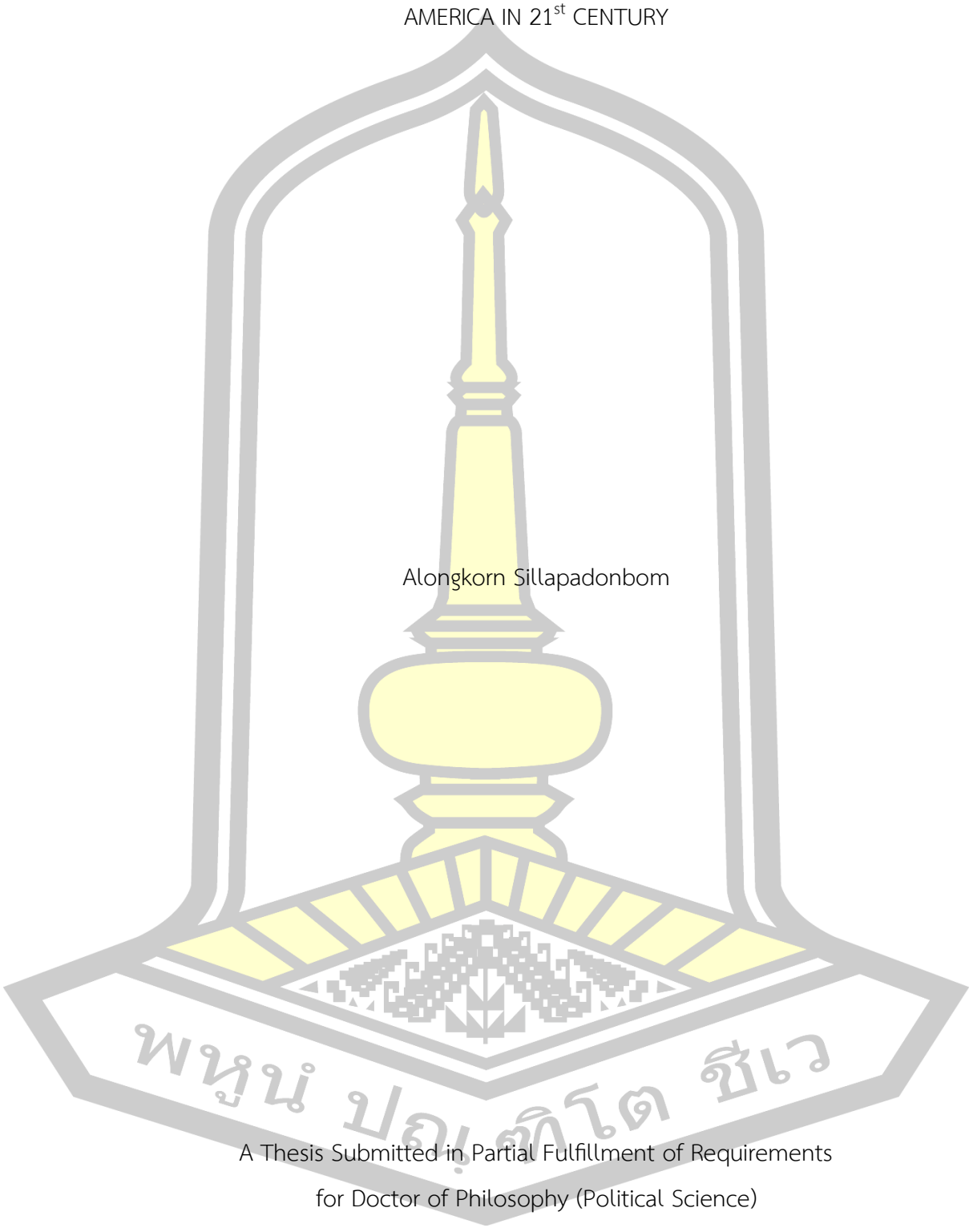
เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชารัฐศาสตร์

เมษายน 2568

CYBERSECURITY AND THE CHALLENGES OF THE GREAT POWER: UNITED STATES OF AMERICA IN 21st CENTURY

Alongkorn Sillapadonbom



A Thesis Submitted in Partial Fulfillment of Requirements

for Doctor of Philosophy (Political Science)

April 2025

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาวิทยานิพนธ์ของนายอลงกรณ์ ศิลปดอนบม แล้วเห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชารัฐศาสตร์ ของมหาวิทยาลัยมหาสารคาม

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(รศ. ดร. อลงกรณ์ อรรคแสง)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รศ. ดร. สุจิตรตรา ฤทธิ์สกุลชัย)

.....กรรมการ
(ผศ. ดร. วนิดา พรมหล้า)

.....กรรมการ
(ผศ. ดร. นิลุบล ไพเราะ)

.....กรรมการผู้ทรงคุณวุฒิภายนอก
(รศ. ดร. ศิวัช ศรีโภคางกุล)

มหาวิทยาลัยอนุมัติให้รับวิทยานิพนธ์ฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญา ปรัชญาดุษฎีบัณฑิต สาขาวิชารัฐศาสตร์ ของมหาวิทยาลัยมหาสารคาม

.....
(ผศ. เชิงชาญ จงสมชัย)
คณบดีวิทยาลัยการเมืองการปกครอง

.....
(ผศ. ดร. พลเดช เชาวรัตน์)
คณบดีบัณฑิตวิทยาลัย

ชื่อเรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกาในศตวรรษที่ 21
ผู้วิจัย อลงกรณ์ ศิลปดอนบม
อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร. สุจิตรตรา ฤทธิ์สกุลชัย
ปริญญา ปรัชญาดุษฎีบัณฑิต **สาขาวิชา** รัฐศาสตร์
มหาวิทยาลัย มหาวิทยาลัยมหาสารคาม **ปีที่พิมพ์** 2568

บทคัดย่อ

งานวิจัยฉบับนี้ มีวัตถุประสงค์ในการวิเคราะห์บทบาทของโลกไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของประเทศมหาอำนาจ โดยเป็นการศึกษาประเทศสหรัฐอเมริกา ซึ่งเป็นประเทศที่มีความเป็นผู้นำทางด้านเทคโนโลยีไซเบอร์ในระดับโลก และเป็นประเทศมหาอำนาจที่มีอิทธิพลต่อประเทศอื่นๆในการเมืองระหว่างประเทศในหลากหลายมิติ ไม่ว่าจะเป็นทางด้านการทหาร เศรษฐกิจ และโครงสร้างพื้นฐานทางไซเบอร์ การศึกษาในงานวิจัย เป็นการวิจัยเชิงคุณภาพ จากการเก็บข้อมูลจากเอกสารชั้นปฐมภูมิและทุติยภูมิ และการวิเคราะห์ประเทศสหรัฐอเมริกาในศตวรรษที่ 21 ด้วยการใช้แนวคิดสัจนิยมใหม่ (Neorealism) และแนวคิดสมองของโลก (Global Brain) เป็นกรอบแนวคิดหลักในการศึกษา

ความสำคัญของการศึกษาในงานวิจัยฉบับนี้ เกิดจากการเล็งเห็นถึงการเปลี่ยนแปลงในโลกไซเบอร์ที่ส่งผลกระทบต่อโครงสร้างอำนาจระหว่างประเทศ การเผชิญหน้าของประเทศมหาอำนาจกับความท้าทายของความเป็นอนาธิปไตยในโลกไซเบอร์ที่ไร้การควบคุม และความพยายามในการรักษาความเป็นอธิปไตยของประเทศตนเอง ประเทศสหรัฐอเมริกาถือว่าเป็นประเทศที่มีความสำคัญในการศึกษา เพราะนอกจากการความท้าทายที่ต้องเผชิญจากโลกไซเบอร์แล้วนั้น การเร่งพัฒนาเทคโนโลยีและการป้องกันภัยคุกคามทางไซเบอร์ เพื่อการรักษาอำนาจความเป็นผู้นำในการเมืองระหว่างประเทศคือสิ่งที่ควรค่าแก่การศึกษาเป็นอย่างยิ่ง งานวิจัยฉบับนี้จึงให้ความสำคัญต่อการวิเคราะห์ประเทศมหาอำนาจในการใช้ไซเบอร์เป็นเครื่องมือในการรักษาอำนาจและความพยายามในการการควบคุมดุลแห่งอำนาจทางภูมิรัฐศาสตร์โลกจากการใช้ไซเบอร์

ผลการศึกษาพบว่า ประเทศสหรัฐอเมริกาใช้กลยุทธ์ทางไซเบอร์ในการสร้างความมั่นคงและขยายอิทธิพลของประเทศตนเอง ไม่ว่าจะเป็นในรูปแบบของการดำเนินนโยบายไซเบอร์ การลงทุนโครงสร้างพื้นฐานทางไซเบอร์ และการพัฒนาองค์ความรู้ของประชากร แต่ถึงอย่างไรก็ตาม การ

กระจายตัวของอำนาจที่เกิดจากโลกไซเบอร์ ได้สร้างการแข่งขันทางไซเบอร์เกิดขึ้น ไม่ว่าจะเป็นจากประเทศจีนและรัสเซีย ที่ได้สร้างความเป็นอธิปไตยทางไซเบอร์ของประเทศตนเอง ทำให้โลกไซเบอร์มีความซับซ้อนมากยิ่งขึ้น อีกทั้งความพยายามในการพัฒนาเทคโนโลยีของประเทศตนเอง ให้มีความทัดเทียมกับประเทศสหรัฐอเมริกา และนอกจากนี้ กลุ่มตัวแสดงที่ไม่ใช่รัฐสามารถสร้างผลกระทบต่อความมั่นคงของประเทศมหาอำนาจได้มากยิ่งขึ้นจากความเป็นอนาธิปไตยทางไซเบอร์

การค้นพบจากงานวิจัยฉบับนี้ระบุถึง การรักษาอำนาจทางไซเบอร์ของประเทศมหาอำนาจ จำเป็นต้องพึ่งพาการดำเนินมาตรการทางกฎหมาย การพัฒนาความก้าวหน้าทางเทคโนโลยี และการสร้างพันธมิตรกับประเทศอื่นๆที่มีแนวคิดทางไซเบอร์แบบเดียวกัน งานวิจัยฉบับนี้เสนอให้มีการส่งเสริมการศึกษา รวมถึงการพัฒนาแรงงานที่มีความเชี่ยวชาญทางด้านไซเบอร์ และการสร้างข้อตกลงระหว่างประเทศเพื่อใช้ในการควบคุมการใช้อำนาจทางไซเบอร์ให้อยู่ในกรอบของกฎหมายระหว่างประเทศและความแตกต่างของโครงสร้างทางการเมือง เพื่อสร้างการวิเคราะห์ผลกระทบที่เกิดจากโลกไซเบอร์ต่อความสัมพันธ์ระหว่างประเทศให้มีความครอบคลุมในหลากหลายมิติ

คำสำคัญ : ความมั่นคงไซเบอร์, มหาอำนาจทางไซเบอร์, สหรัฐอเมริกา, ความมั่นคงแห่งชาติ

TITLE CYBERSECURITY AND THE CHALLENGES OF THE GREAT POWER: UNITED STATES OF AMERICA IN 21st CENTURY

AUTHOR Alongkorn Sillapadonbom

ADVISORS Associate Professor Suchittra Ritsakulchai , Ph.D.

DEGREE Doctor of Philosophy **MAJOR** Political Science

UNIVERSITY Mahasarakham University **YEAR** 2025

ABSTRACT

This research aims to analyze the role of cyberspace in shaping the security dynamics of global superpowers, with a particular focus on the United States. As a leading nation in cyber technology, the U.S. exerts significant influence on international relations across multiple dimensions, including military, economic, and critical cyber infrastructure. This study employs a qualitative research methodology, utilizing primary and secondary sources to conduct a case study of the United States in the 21st century. The research framework is based on the Neorealism theory and the Global Brain concept, which are used to examine the strategic role of cyber capabilities in maintaining national security and global influence.

The significance of this study stems from the evolving cyber landscape, which has fundamentally altered the balance of power among nations. The anarchic nature of cyberspace challenges the ability of superpowers to maintain their dominance. In response, the United States has had to develop advanced cyber technologies and defense mechanisms to uphold its global leadership. This research provides a crucial analysis of how cyber tools are employed by global powers to sustain geopolitical influence and manage the cyber power equilibrium.

The findings indicate that the United States has adopted various cyber strategies to enhance its security and expand its global influence. These strategies

include cyber policies, investments in technological infrastructure, and the promotion of cyber literacy among its population. However, the intensifying cyber competition with rival nations such as China and Russia has created a complex security environment, as these nations are actively developing their own cyber capabilities to counterbalance U.S. dominance. Furthermore, the anarchic nature of cyberspace has enabled non-state actors to engage in cyber operations that pose significant security threats to major powers.

The key findings of this research suggest that maintaining cyber dominance requires a combination of legal frameworks, technological advancements, and strategic cyber alliances with like-minded nations. The study recommends fostering cyber education and workforce development while establishing international agreements to regulate cyber power within the boundaries of international law. Additionally, further research should be conducted on developing nations and politically diverse states to gain a more comprehensive understanding of how cyber dynamics affect international relations across different political and economic contexts.

Keyword : Cybersecurity, Cyber Power, United States, National Security

กิตติกรรมประกาศ

งานวิจัยเรื่อง “ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกาในศตวรรษที่ 21” ฉบับนี้ ข้าพเจ้าขอกราบขอบพระคุณ รองศาสตราจารย์ ดร. สุจิตรตรา ฤทธิ์สกุลชัย อาจารย์ที่ปรึกษา ที่ได้ให้คำแนะนำและข้อเสนอแนะที่เป็นประโยชน์อย่างยิ่งตลอดระยะเวลาการทำวิจัย ความทุ่มเทและความเมตตาของท่านในการให้คำปรึกษา ทำให้ข้าพเจ้าสามารถดำเนินงานวิจัยนี้จนสำเร็จลุล่วง และยังเป็นผู้เบิกทางในการให้ข้าพเจ้าได้รับรู้ถึงความสำคัญของโลกไซเบอร์ต่อบทบาททางการเมืองที่เป็นปัจจัยสำคัญในโลกยุคปัจจุบัน

ข้าพเจ้าขอขอบพระคุณ คณะกรรมการคุมสอบทุกท่าน ที่ได้สละเวลาอันมีค่าให้คำแนะนำและข้อเสนอแนะที่เป็นประโยชน์ต่อการปรับปรุงและพัฒนางานวิจัยให้มีความสมบูรณ์มากยิ่งขึ้น ความกรุณาและความเอาใจใส่ของท่านล้วนเป็นแรงผลักดันที่สำคัญให้ข้าพเจ้าสามารถก้าวผ่านความท้าทายในกระบวนการวิจัยนี้ไปได้ ตลอดจนขอขอบพระคุณรองศาสตราจารย์ ดร.ศิวัช ศรีโภคางกุล ที่กรุณาเป็นผู้ทรงคุณวุฒิภายนอก การให้คำแนะนำ และการให้ความเมตตากรุณาต่อข้าพเจ้าอย่างหาที่สุดไม่ได้

สุดท้ายนี้ ข้าพเจ้าขอพระคุณครอบครัวของข้าพเจ้า ที่สนับสนุนทุกย่างก้าวในชีวิตของข้าพเจ้า รวมถึงภรรยาของข้าพเจ้า ที่คอยเป็นกำลังใจเสมอ ขอบคุณทุกท่านที่มีส่วนร่วมสนับสนุนในทุกขั้นตอนของการศึกษาวิจัยครั้งนี้ หวังว่างานวิจัยชิ้นนี้ จะสามารถเป็นประโยชน์ต่อประเทศชาติ ณ ห้วงเวลาที่โลกแปรผันอย่างรวดเร็ว

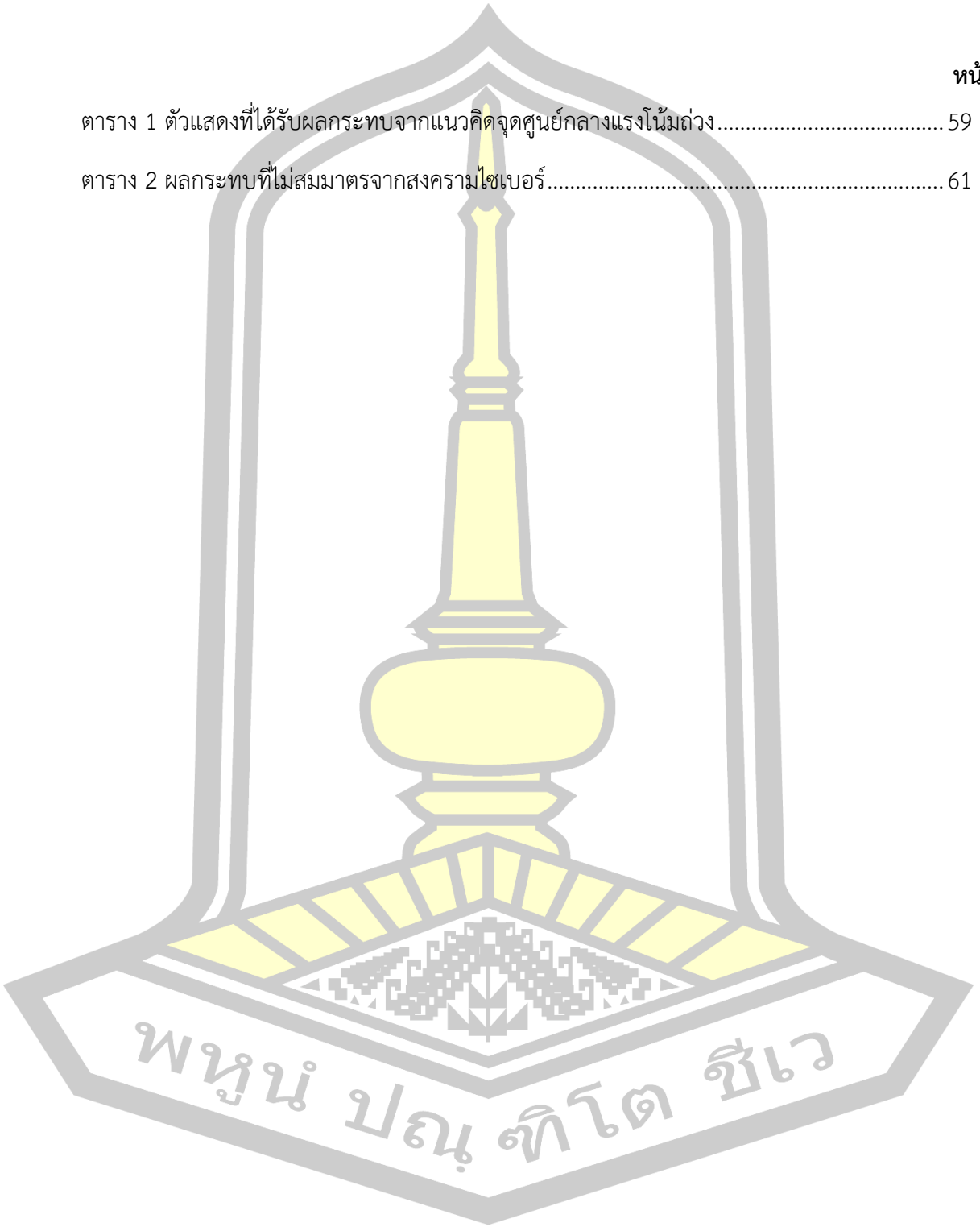
อลงกรณ์ ศิลปดอนบม

สารบัญ

หน้า

สารบัญตาราง

หน้า



สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

ที่มาและความสำคัญ

พัฒนาการทางเทคโนโลยีได้สร้างการเชื่อมต่อการสื่อสารโดยใช้ระบบเครือข่ายอินเทอร์เน็ต และกลายเป็นสิ่งสำคัญในชีวิตประจำวันของมนุษย์จากการนำมาปรับใช้ ไม่ว่าจะเป็นการสื่อสาร การเงิน การเก็บข้อมูล รวมไปถึงเป็นการส่งเสริมภาคเศรษฐกิจ สังคม และ การทำงานของภาครัฐให้มีประสิทธิภาพมากยิ่งขึ้น ระบบเครือข่ายอินเทอร์เน็ต คือส่วนหนึ่งของ “พื้นที่ทางไซเบอร์” หรือ Cyberspace การนำไซเบอร์มาใช้ในชีวิตประจำวันและการใช้งานในที่สาธารณะ สามารถกลายเป็นภัยอันตรายจากการโจมตีทางไซเบอร์ได้ด้วยเช่นกัน ซึ่งเมื่อพูดถึง Cyberspace นั้น คนส่วนมากมักนึกถึงเพียงเฉพาะคำว่า “อินเทอร์เน็ต” แต่แท้จริงแล้ว David Clack (2010) ได้ทำการเสนอแนวคิดโครงสร้างลำดับชั้นของ Cyberspace ซึ่งเป็นแนวคิดที่สำคัญและใช้ในการอธิบายองค์ประกอบของโลกไซเบอร์ได้อย่างชัดเจน ประกอบด้วย 4 ลำดับชั้น คือ ลำดับชั้นทางกายภาพ (Physical layer) ที่อธิบายถึงโครงสร้างพื้นฐานของระบบเครือข่ายอินเทอร์เน็ต ลำดับชั้นทางตรรกะ (Logical layer) ที่อธิบายถึงการสร้างระบบหรือแอพพลิเคชั่นเพื่อใช้งานบนโลกอินเทอร์เน็ต ลำดับชั้นข้อมูล (Information layer) เป็นลำดับชั้นที่เกี่ยวข้องกับข้อมูลต่างๆที่เราได้บรรจุลงบนโลกอินเทอร์เน็ต และลำดับชั้นผู้ใช้งาน (User layer) ซึ่งเป็นลำดับชั้นที่เกี่ยวข้องกับปัจเจกบุคคล องค์กร และรัฐบาลในการใช้งานพื้นที่ทางไซเบอร์เพื่อจุดประสงค์ของตนเอง (Clark, 2010) การเพิ่มขึ้นอย่างรวดเร็วของการใช้งานโลกไซเบอร์ทำให้เกิดความซับซ้อนและการปรับเปลี่ยนรูปแบบของการใช้ชีวิตของมนุษย์อย่างรวดเร็วมากยิ่งขึ้น เพราะการเพิ่มขึ้นของการใช้งานโลกไซเบอร์ของมนุษย์ ไม่ใช่การใช้งานแบบกายภาพที่วัดได้เพียงขนาดของวัตถุนั้นๆเพียงอย่างเดียว แต่เป็นการเพิ่มขึ้นของการใช้งานข้อมูลในโลกไซเบอร์ โดยในช่วงกลาง ค.ศ. 2011 ได้มีการแลกเปลี่ยนข้อมูลเกิดขึ้นในโลกไซเบอร์มากกว่า 2 ล้านล้านรอบ ซึ่งมีขนาดข้อมูลการแลกเปลี่ยนเกิดขึ้นอยู่ที่ 50 ล้านล้านกิกะไบต์ โดยได้มีการคาดการณ์ว่าใน ค.ศ. 2025 จะมีประชากรที่ใช้งานโลกไซเบอร์จำนวน 5.5 พันล้านคน หรือเทียบเป็นอัตราส่วนร้อยละ 60 ของประชากรโลก จะมีการใช้งานแอพพลิเคชั่นมากกว่า 25 ล้านแอพพลิเคชั่นที่จะสร้างการแลกเปลี่ยนข้อมูลเป็น 50 ล้านล้านกิกะไบต์ต่อวัน (Hurley, 2012) การเปลี่ยนแปลงอย่างฉับพลันที่เกิดขึ้นต่อการใช้ชีวิตประจำวันของมนุษย์ที่เกิดจากจำนวนชุดข้อมูลและการแลกเปลี่ยนข้อมูลที่เกิดขึ้นในโลกไซเบอร์ สร้างความซับซ้อนในมิติของชุดข้อมูลต่างๆ ซึ่งทำให้เกิดความเป็นไปได้ต่างๆที่จะส่งผลกระทบต่อรูปแบบการทำงานทางการทหารและสร้างผลกระทบต่อความมั่นคงของรัฐ ทำให้เกิดความต้องการในการสร้างความมั่นคงทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น

การเพิ่มขึ้นของการใช้งานไซเบอร์เพิ่มขึ้นอย่างต่อเนื่อง และความจำเป็นของชีวิตประจำวันได้เป็นจุดที่ทำให้การใช้งานโลกไซเบอร์ คือสิ่งที่จำเป็นในศตวรรษที่ 21 อาทิเช่น กรณีช่วง COVID-19 ที่ผู้คนต่างต้องรักษาระยะห่าง ตรวจสอบข่าวสาร และกักตัวเพื่อความปลอดภัยของสุขภาพ ทั้งของตัวเองและคนรอบข้าง ทำให้การใช้งานไซเบอร์เป็นสิ่งที่ขาดไม่ได้ ณ ช่วงนั้น ส่งผลให้การใช้งานไซเบอร์เพิ่มขึ้นอย่างรวดเร็วกว่าปกติ ในขณะที่การใช้งานเพิ่มขึ้นอย่างรวดเร็วในช่วง COVID-19 ผลกระทบด้านลบของการใช้ไซเบอร์ก็ได้เพิ่มขึ้นด้วยเช่นกัน นั่นคือการโจมตีทางไซเบอร์ ที่เพิ่มขึ้นเป็นอย่างมาก ไม่ว่าจะเป็นการส่งข้อมูลปลอม หรือการส่งลิงค์อินเทอร์เน็ตปลอมเพื่อหลอกล่อเอาข้อมูลของผู้ที่หลงเชื่อลิงค์เหล่านั้น โดยมีรายงานถึงการโจมตีทางไซเบอร์เพิ่มขึ้นร้อยละ 50.1 ระหว่างเดือนธันวาคม ค.ศ. 2019 ถึงเดือนเมษายน ค.ศ.2020 และการเพิ่มขึ้นของการส่งสแปม หรือข้อมูลเท็จเกี่ยวกับ COVID-19 มากถึง 907,000 ข้อความ รวมถึงมัลแวร์ต่างๆที่เกี่ยวกับ COVID-19 มากถึง 48,000 ลิงค์ที่เป็นอันตรายต่อผู้หลงเชื่อ นอกจากผลกระทบจากการโจมตีไซเบอร์ต่อระดับปัจเจกบุคคลแล้วนั้น โครงสร้างพื้นฐานที่สำคัญ ก็ตกเป็นเป้าหมายการโจมตีไซเบอร์ด้วยเช่นกัน ไม่ว่าจะเป็นโรงพยาบาล โดยในประเทศสหรัฐอเมริกา ได้ถูกโจมตีทางไซเบอร์เพื่อขโมยข้อมูลเกี่ยวกับงานวิจัยวัคซีน COVID-19 จากกลุ่มแฮกเกอร์ต่างๆ และกลุ่มอาชญากรรมไซเบอร์ที่ใช้แรนซัมแวร์ในการโจมตีหน่วยงานของระบบสาธารณสุขในสหรัฐอเมริกา ทำให้บางโรงพยาบาลจำเป็นต้องปิดระบบเชื่อมต่ออินเทอร์เน็ตในทันที (Lallie et al., 2021)

นอกจากระบบโครงสร้างพื้นฐานสำคัญที่ได้รับผลกระทบจากการโจมตีไซเบอร์แล้วนั้น ระบบเศรษฐกิจก็เป็นอีกปัจจัยสำคัญที่ได้รับความเสียหายจากไซเบอร์ด้วยเช่นกัน การโจมตีเพื่อสร้างผลกระทบต่อระบบเศรษฐกิจที่ประเทศสหรัฐอเมริกาได้รับผลกระทบ ตัวละครระดับประเทศที่เคยสร้างการโจมตีทางไซเบอร์ เช่น จีน รัสเซีย อิหร่าน และเกาหลีเหนือ ได้สร้างผลกระทบต่อระบบเศรษฐกิจของสหรัฐอเมริกา ส่งผลให้การบริหารงบประมาณทางด้านค่าใช้จ่ายในการสร้างระบบป้องกันภัยคุกคามทางไซเบอร์ต้องเพิ่มมากขึ้น รวมถึงผลกระทบที่ทำให้ระบบสาธารณะต้องปิดใช้งานไปชั่วขณะ อาทิเช่น เหตุการณ์โจมตีสำนักงานบริหารงานบุคคลของรัฐบาลกลางประเทศสหรัฐอเมริกา ที่เกิดขึ้นจำนวน 2 ครั้ง ทั้งใน ค.ศ. 2012 และ ค.ศ. 2015 ซึ่งการโจมตีไซเบอร์ในครั้งนั้น ประเทศสหรัฐอเมริกาได้ถูกขโมยข้อมูลส่วนตัวของพนักงานรัฐบาล ไม่ว่าจะเป็น หมายเลขประกันสังคม ข้อมูลหน้าที่การงาน และประวัติการทำงาน รวมถึงผู้ที่สมัครงาน ได้ถูกขโมยไปจำนวน 19.7 ล้านรายการ และเหตุการณ์โจมตีระบบท่อส่งน้ำมัน ซึ่งถือเป็นการโจมตีทางไวเบอร์ที่ใหญ่ที่สุดต่อระบบโครงสร้างพื้นฐานของประเทศสหรัฐอเมริกา ที่ทำให้ระบบขนส่งเชื้อเพลิงหลักของประเทศสหรัฐอเมริกาต้องหยุดชะงัก ซึ่งกลุ่มโจมตีไซเบอร์ได้ทำการเรียกค่าไถ่จากบริษัท Colonial Pipeline และมีการจ่ายค่าไถ่จำนวน 4.4 ล้านดอลลาร์สหรัฐ ทำให้เกิดผลกระทบทางด้านเศรษฐกิจต่อผู้บริโภคและภาคเอกชนทั่วประเทศ (Asadi, 2022)

การโจมตีทางไซเบอร์สามารถสร้างผลกระทบได้ตั้งแต่ระดับปัจเจกบุคคล ระดับองค์กร ไปจนถึงระดับประเทศ และมีรูปแบบการโจมตีที่มีความคล้ายคลึงกันคือการใช้ระบบอินเทอร์เน็ตในการจู่โจม ผลกระทบและความเสียหายที่เกิดขึ้นจากการโจมตีทางไซเบอร์ สามารถทำให้เกิดการสูญเสียไม่ว่าจะเป็นการสูญเสียทางด้านการเงิน ข้อมูล รวมไปถึงความสัมพันธ์ระหว่างประเทศด้วยเช่นกัน (Mitra, 2010) ซึ่งทำให้บทบาทของไซเบอร์ส่งผลกระทบต่อระบบทางการเมืองโดยตรง และยังเป็นผลกระทบโดยตรงต่อประเทศมหาอำนาจต่างๆ ไม่ว่าจะเป็นประเทศสหรัฐอเมริกา จีน และรัสเซีย อาทิเช่น การโจมตีทางไซเบอร์เพื่อแทรกแซงการเลือกตั้งประธานาธิบดีของประเทศสหรัฐอเมริกา ใน ค.ศ. 2016 ด้วยการใช้แคมเปญข่าวปลอมและการแฮกเข้าระบบเพื่อขโมยข้อมูลของฝ่ายตรงข้าม และเหตุการณ์โจมตีระบบโครงสร้างพื้นฐานทางด้านพลังงาน โดยเป็นการโจมตีจากแฮกเกอร์ที่มีภาครัฐคอยสนับสนุน อาทิเช่น การโจมตีเครือข่ายไฟฟ้าในประเทศยูเครน รวมถึงการเจาะระบบบริษัทพลังงานในประเทศสหรัฐอเมริกา การโจมตีทางไซเบอร์ได้กลายเป็นส่วนสำคัญของสงคราม อาทิเช่น สงครามระหว่างประเทศรัสเซียและประเทศจอร์เจีย ที่ความสำคัญของไซเบอร์ได้ถูกนำมาสร้างเป็นแผนความมั่นคงทางไซเบอร์ระดับชาติของประเทศต่างๆ เพื่อป้องกันการโจมตีจากประเทศรัสเซีย ทำให้เห็นถึงผลกระทบต่อความสัมพันธ์ระหว่างประเทศ และส่งผลต่อการวางนโยบายของประเทศมหาอำนาจต่างๆ เพื่อปรับปรุงกลยุทธ์และนโยบายในการสนับสนุนทางด้านความมั่นคงทางไซเบอร์ ที่จำเป็นต้องพัฒนาอย่างต่อเนื่อง เพื่อรับมือการโจมตีทางไซเบอร์ที่สามารถพัฒนาได้ตลอดเวลา (Azmi & Kautsarina, 2019)

ปัจจุบันความจำเป็นในการใช้อาวุธทางไซเบอร์เป็นสิ่งที่หลีกเลี่ยงไม่ได้ในการเป็นส่วนหนึ่งเพื่อใช้ในการทำสงคราม และได้ส่งผลกระทบต่อกระบวนทัศน์การเมืองระหว่างประเทศ ซึ่งในอดีตโลกไซเบอร์มีส่วนเกี่ยวข้องกับทางการเมืองค่อนข้างน้อย แต่ในปัจจุบัน ความมั่นคงทางไซเบอร์ได้กลายเป็นจุดสำคัญของความขัดแย้งทางด้านผลประโยชน์ทั้งภายในประเทศและระหว่างประเทศ และความมั่นคงทางไซเบอร์ยังส่งผลถึงภาพลักษณ์ในอำนาจของประเทศนั้นๆ (Van Haaster, 2016) นำมาสู่การเปลี่ยนแปลงพฤติกรรมของรัฐต่างๆและได้เกิดการก่อตั้งองค์กรที่รับผิดชอบความมั่นคงทางไซเบอร์ของแต่ละประเทศ เพื่อเป็นการปกป้องผลประโยชน์แห่งชาติของรัฐ การแข่งขันทางด้านเทคโนโลยีไซเบอร์เป็นสิ่งที่ประเทศมหาอำนาจที่มีบทบาทของอำนาจทางการทหารในการกำหนดระเบียบโลกในปัจจุบันให้ความสนใจเป็นอย่างมาก โดยทาง Belfer Center for Science and International Affairs ได้ทำการจัดอันดับประเทศที่มีอำนาจทางไซเบอร์สูงที่สุดในโลกทั้งหมด 10 อันดับ ดังภาพประกอบ 1

ลำดับที่	ค.ศ. 2020	ค.ศ. 2022
1	สหรัฐอเมริกา	สหรัฐอเมริกา
2	จีน	จีน
3	สหราชอาณาจักร	รัสเซีย
4	รัสเซีย	สหราชอาณาจักร
5	เนเธอร์แลนด์	ออสเตรเลีย
6	ฝรั่งเศส	เนเธอร์แลนด์
7	เยอรมัน	เกาหลีเหนือ
8	แคนาดา	เวียดนาม
9	ญี่ปุ่น	ฝรั่งเศส
10	ออสเตรเลีย	อิหร่าน

ภาพประกอบ 1 ข้อมูลเปรียบเทียบประเทศที่มีอำนาจทางไซเบอร์ปี 2022
ที่มา: National Cyber Power Index (2022)

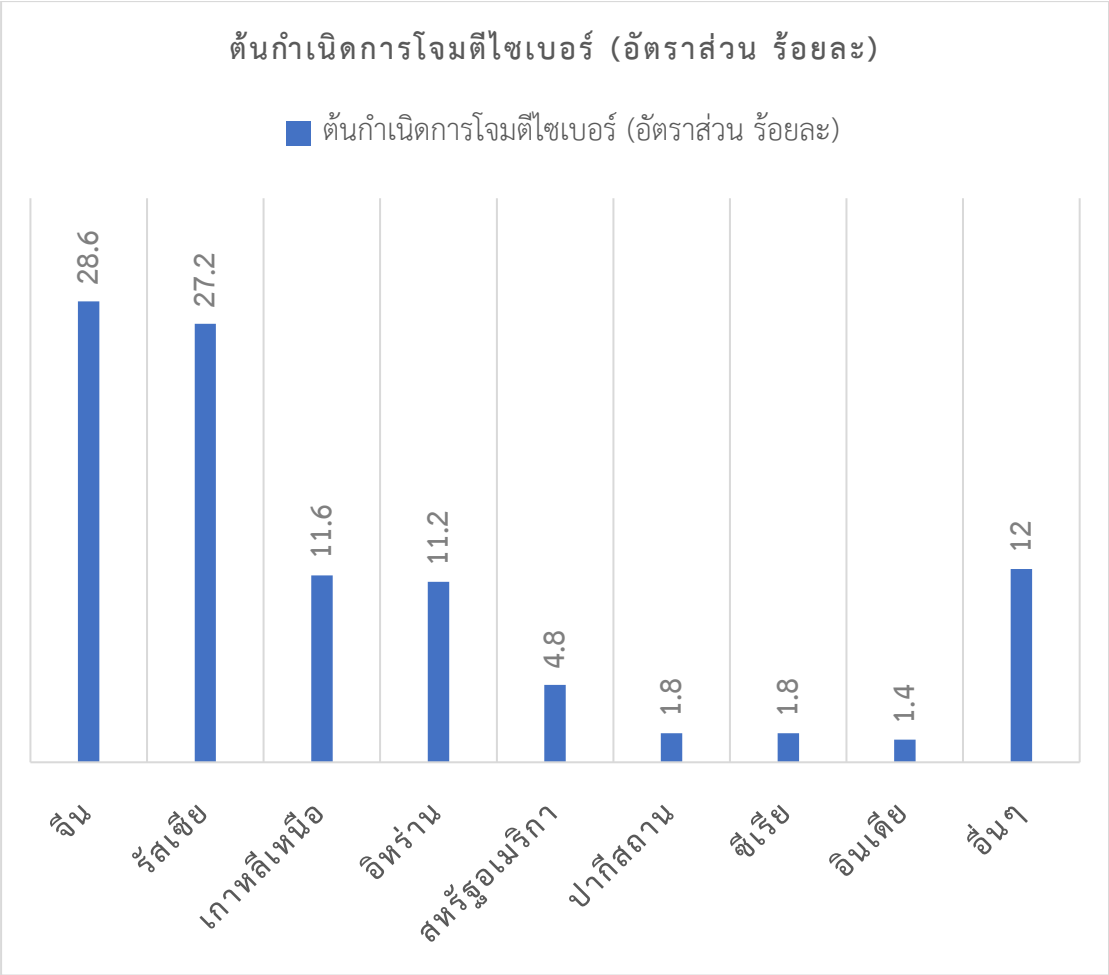
จากรายงาน National Cyber Power Index (2022) ที่ใช้เกณฑ์การเปรียบเทียบด้วยประสิทธิภาพของการป้องกันทางไซเบอร์ การรวบรวมข้อมูล การโจมตีทางไซเบอร์ และอำนาจทางเศรษฐกิจทางไซเบอร์ แสดงให้เห็นว่า ประเทศสหรัฐอเมริกา เป็นผู้นำอันดับหนึ่งทางด้านไซเบอร์ ลำดับถัดมาคือประเทศ จีนและรัสเซีย ความเป็นผู้นำทางด้านเทคโนโลยีของประเทศสหรัฐอเมริกา นอกจากผลประโยชน์ทางด้านเศรษฐกิจ ประเทศสหรัฐอเมริกายังมีบทบาทที่สำคัญ คือ การเป็นประเทศมหาอำนาจทางไซเบอร์ที่มีประสิทธิภาพในการโจมตีและป้องกันทางไซเบอร์อันดับหนึ่งของโลก อีกทั้งมิติการแก้ไขความขัดแย้งระหว่างประเทศนั้น ประเทศสหรัฐอเมริกายังมีบทบาทสำคัญในการกำหนดมาตรฐานต่างๆที่มีความเกี่ยวข้องกับไซเบอร์ด้วยเช่นกัน (Voo et al., 2022)

ประสิทธิภาพของประเทศสหรัฐอเมริกาทางด้านไซเบอร์สามารถเห็นได้อย่างชัดเจน ดังตัวอย่างกรณีการถูกโจมตีโดยกลุ่มก่อการร้าย ISIS ในกรณีการสังหารนักข่าวชาวอเมริกัน ส่งผลให้รัฐบาลในยุคสมัยของประธานาธิบดี Barrack Obama ได้ทำการสั่งโจมตีทางไซเบอร์ไปยังสถาบันการเงินของรัฐอิสลาม โดยมีเป้าหมายในการทำลายค่าเงินเพื่อลดประสิทธิภาพทางด้านการเงินของศัตรู ซึ่งเป็นการทำสงครามแบบผสม (Hybrid war) ที่มีการโจมตีทั้งการทำสงครามแบบดั้งเดิม (Conventional war) และ การโจมตีแบบไซเบอร์ (Cyber Attack) ด้วยเช่นกัน (Crespo, 2018) นอกจากความสามารถในการโจมตีของประเทศสหรัฐอเมริกา อีกด้านหนึ่งของประเทศที่เป็นผู้นำระดับโลกคือ การถูกท้าทายจากการโจมตีทางไซเบอร์จากภายนอกประเทศ ซึ่งเป็นอีกหนึ่งสาเหตุที่ทำ

ให้เพิ่มความขัดแย้งระหว่างประเทศมากยิ่งขึ้น อาทิเช่น การให้ข้อมูลของประเทศสหรัฐอเมริกาใน ค.ศ. 2009 ว่ามีการแฮ็กขโมยข้อมูลเครื่องบินขับไล่โจมตีรุ่น The Joint Strike Fighter ของประเทศสหรัฐอเมริกาโดยมีต้นทางการแฮ็กมาจากประเทศจีน (Hjortdal, 2011) โดยเฉพาะเรื่องการโจมตีทางไซเบอร์ที่เคยถูกแฮ็กเกอร์ชาวรัสเซียพยายามแฮ็กเข้าสู่ระบบโรงงานพลังงานไฟฟ้าของประเทศสหรัฐอเมริกา การเพิ่มขึ้นของพัฒนาการทางไซเบอร์ในแต่ละประเทศ ทำให้ความเป็นผู้นำแบบเสรีนิยมของประเทศสหรัฐอเมริกาถูกท้าทายมากยิ่งขึ้น โลกไซเบอร์ที่ไม่สามารถควบคุมได้เพราะความเป็นอนาธิปไตยของโลกไซเบอร์ และการโจมตีทางไซเบอร์ที่ยากต่อการระบุถึงแหล่งที่มา เหตุจูงใจในการโจมตี และตัวแสดงที่ทำการโจมตีเพื่อจุดประสงค์ใดจุดประสงค์หนึ่ง จึงเป็นเรื่องท้าทายเป็นอย่างมากต่อของประเทศสหรัฐอเมริกาในศตวรรษที่ 21

ในศตวรรษที่ 21 ความเป็นผู้นำแบบเสรีนิยมที่นำโดยประเทศสหรัฐอเมริกายังคงมีบทบาทสำคัญ ความเป็นผู้นำในแบบเสรีนิยมนี้เกิดจากประสิทธิภาพของประเทศสหรัฐอเมริกา อาทิเช่น ความเป็นศูนย์กลางทางด้านตลาดทุนและระบบการเงิน การพัฒนาทางด้านเทคโนโลยีและนวัตกรรม ความแข็งแกร่งทางด้านการทหาร คุณภาพการศึกษาที่อยู่ในระดับสูง การมีสกุลเงินที่ใช้เป็นเงินทุนสำรองของระบบการเงินโลก ผลผลิตทางด้านเศรษฐกิจที่สูง และ ความมั่งคั่งทางด้านทรัพยากรธรรมชาติ ความสามารถทางด้านการทหารของประเทศสหรัฐอเมริกา ถูกจัดลำดับให้อยู่ในลำดับที่ 1 จากดัชนีวัดค่าอำนาจของแต่ละประเทศใน ค.ศ. 2022 โดยมีสัดส่วนค่าใช้จ่ายงบประมาณทางด้านการทหารในสัดส่วนระหว่างประเทศมีอัตราส่วนร้อยละ 40 จากผลรวมทั้งหมด และมีบุคลากรทางการทหารอยู่ในสัดส่วนร้อยละ 7 ของโลก และยังเป็นผู้นำทางด้านเทคโนโลยีและนวัตกรรมด้วยเช่นกัน อย่างไรก็ตาม ในความเป็นผู้นำของโลกของสหรัฐอเมริกากำลังถูกท้าทายจากประเทศจีน ซึ่งเป็นประเทศที่มีการพัฒนาการเติบโตขึ้นอย่างรวดเร็วและมีลำดับดัชนีวัดค่าอำนาจของประเทศอยู่ในลำดับที่สองรองจากประเทศสหรัฐอเมริกา (Dalio, 2022)

อย่างไรก็ตาม การเพิ่มขึ้นของการโจมตีทางไซเบอร์เพิ่มขึ้นอย่างมีนัยสำคัญ รัฐบาลของประเทศต่างๆ ต่างให้ความสำคัญในการใช้เทคโนโลยีไซเบอร์ในการสร้างการโจมตี โดยเฉพาะจากผลการศึกษาเชิงสถิติของ Joe Robinson (2022) ที่ได้ทำการศึกษาเกี่ยวกับความมั่นคงทางไซเบอร์เชิงสถิติ พบว่ามีการเพิ่มขึ้นของเอกสารยืนยันการโจมตีทางไซเบอร์ระหว่างประเทศเป็นการศึกษาในช่วงระหว่าง ค.ศ. 2009 ถึง 2018 ได้มีการเพิ่มขึ้นในอัตราส่วน 440 เปอร์เซ็นต์ โดยจำนวน 28.6 เปอร์เซ็นต์ มีต้นทางการโจมตีมาจากประเทศจีน และ 27.2 เปอร์เซ็นต์ มีต้นทางการโจมตีมาจากประเทศรัสเซีย และอัตราส่วนต้นทางการโจมตีทางไซเบอร์ของประเทศสหรัฐอเมริกาอยู่ที่จำนวน 1.8 เปอร์เซ็นต์ แต่ประเทศสหรัฐอเมริกาเป็นเป้าหมายที่ถูกโจมตีทางไซเบอร์อยู่ในอัตราส่วน 26.3 เปอร์เซ็นต์ และมีอีกหลายประเทศที่ได้ใช้ไซเบอร์ในการโจมตีระหว่างประเทศ ดังภาพประกอบ 2 (Robinson, 2022)



ภาพประกอบ 2 ข้อมูลสถิติการโจมตีทางไซเบอร์ระหว่างประเทศช่วง ค.ศ. 2009 ถึง 2018
ที่มา: Joe Robinson (2022)

ความสำคัญของความท้าทายที่เกิดขึ้นและข้อมูลศึกษาที่กล่าวมาข้างต้น ผู้วิจัยจึงมีความสนใจในการศึกษาถึงการเพิ่มขึ้นของการใช้ไซเบอร์ในการท้าทายขอบเขตของความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา ไม่ว่าจะเป็นการศึกษาการท้าทายความเป็นอนาธิปไตยของโลกไซเบอร์ต่อประเทศสหรัฐอเมริกา วิเคราะห์ปัจจัยที่เสริมสร้างความเป็นมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา และ การศึกษาพฤติกรรมการใช้ไซเบอร์ของประเทศสหรัฐอเมริกา ในฐานะการเป็นผู้นำทางไซเบอร์ระดับโลก เพื่อสร้างความมั่นคงต่อรัฐตนเองและส่งผลต่อความสัมพันธ์ระหว่างประเทศ อย่างไร เพื่อเป็นการวิเคราะห์เหตุการณ์สำคัญที่กำลังเกิดขึ้นโดยมีไซเบอร์เข้ามามีบทบาทและเป็นปัจจัยในการเปลี่ยนแปลงภายใต้ขอบเขตการศึกษาความสัมพันธ์ระหว่างประเทศ

คำถามวิจัย

1. ทำไมความเป็นอนาธิปไตยของโลกไซเบอร์ทำให้ท้าทายอำนาจของประเทศสหรัฐอเมริกาในศตวรรษที่ 21
2. ประเทศสหรัฐอเมริกามีแนวทางและยุทธศาสตร์ในการใช้ไซเบอร์เพื่อเสริมสร้างความมั่นคงแห่งชาติและความเป็นมหาอำนาจทางไซเบอร์ อย่างไร
3. ความเป็นผู้นำทางไซเบอร์ของประเทศสหรัฐอเมริกาส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศและสมดุลแห่งอำนาจในการเมืองระหว่างประเทศ อย่างไร

ความมุ่งหมายของการวิจัย

1. เพื่อวิเคราะห์ความเป็นอนาธิปไตยในโลกไซเบอร์ที่ท้าทายอำนาจของประเทศสหรัฐอเมริกา
2. เพื่อวิเคราะห์บทบาทของไซเบอร์ที่ส่งผลต่อการสร้างความเป็นมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา
3. เพื่อวิเคราะห์ผลกระทบที่เกิดขึ้นของความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่ส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ และสมดุลแหงอำนาจในการเมืองระหว่างประเทศ

สมมติฐานของการวิจัย

1. ความเป็นอนาธิปไตยของโลกไซเบอร์จะมีส่วนท้าทายความเป็นประเทศมหาอำนาจของประเทศสหรัฐอเมริกา และอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกาในศตวรรษที่ 21 จะมีการเปลี่ยนแปลง จากประเทศมหาอำนาจอื่นๆที่เข้ามามีบทบาทในโลกไซเบอร์ด้วยเช่นกัน
2. การให้ความสำคัญทางด้านการพัฒนาทางไซเบอร์ ทั้งทางด้านการทหาร เทคโนโลยี และวิทยาศาสตร์ จะส่งผลให้ประเทศสหรัฐอเมริกามีความมั่นคงแห่งชาติและความมั่นคงทางการทหารมากยิ่งขึ้นในการเมืองระหว่างประเทศมากกว่าประเทศอื่นๆ
3. ประเทศสหรัฐอเมริกามีแนวโน้มที่จะสร้างอิทธิพลทางการเมืองระหว่างประเทศ โดยใช้ความเป็นผู้นำทางไซเบอร์ และการเป็นรากฐานทางเทคโนโลยีไซเบอร์ในระดับโลก รวมถึงอำนาจทางไซเบอร์ในการปฏิบัติการ ทั้งทางด้านนโยบายทางการทูต นโยบายระหว่างประเทศ และการใช้ไซเบอร์ทางการทหารในระดับนานาชาติที่มากยิ่งขึ้น

ระเบียบวิธีวิจัย

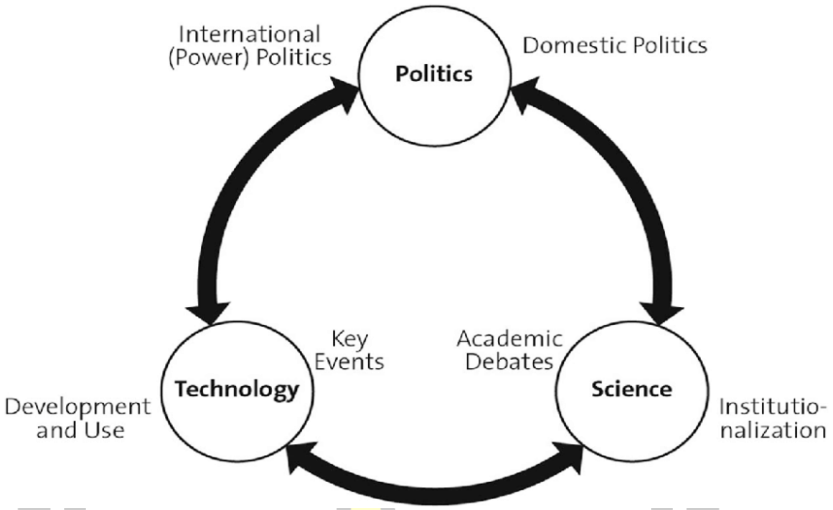
งานวิจัยนี้เป็นงานวิจัยพื้นฐาน (Basic Research) เพื่อหาองค์ความรู้ใหม่ เป็นการศึกษาเชิงคุณภาพ (Qualitative Research) ซึ่งเป็นการเก็บข้อมูลจากเอกสารชั้นปฐมภูมิและทุติยภูมิ เพื่อให้ได้มาซึ่งข้อมูลที่เฉพาะเจาะจงและเจาะลึกในการอธิบายความสัมพันธ์ของตัวแปรต่างๆในช่วงศตวรรษที่ 21 ระหว่างประเทศ ในขอบเขตความมั่นคงทางไซเบอร์ และความท้าทายของประเทศมหาอำนาจ ผู้ศึกษาได้กำหนดทฤษฎี/แนวคิด ที่ใช้ศึกษาออกเป็น 2 ส่วน ดังนี้

1. ทฤษฎีหลัก/แนวคิดหลัก

ความเป็นอนาธิปไตยของไซเบอร์มีความคล้ายกับความเป็นอนาธิปไตยของระบบการเมืองระหว่างประเทศ ซึ่งสอดคล้องกับแนวคิดสัจนิยมใหม่ (Neorealism) ที่มีการวิเคราะห์ที่ครอบคลุมถึงทุกตัวแสดงที่มีบทบาทในการเมืองระหว่างประเทศของตัวแสดงที่เป็นรัฐ ดังนั้น งานวิจัยชิ้นนี้ จึงใช้แนวคิดสัจนิยมคลาสสิคใหม่ในการวิเคราะห์เนื้อหาที่มีความสอดคล้องกับความเป็นอนาธิปไตยของโลกไซเบอร์ในโลกการเมืองระหว่างประเทศ

2. ทฤษฎีรอง/แนวคิดรอง

การศึกษาความเป็นผู้นำทางด้านไซเบอร์ของประเทศสหรัฐอเมริกา สามารถส่งผลต่อโครงสร้างการเมืองระดับโลกและนำมาสู่การวางรากฐานเพื่อเป็นประเทศมหาอำนาจทางไซเบอร์ โดยในทฤษฎีรองของงานวิจัย ผู้วิจัยใช้แนวคิดสมองของโลก (Global Brain) ในการวิเคราะห์ความเป็นประเทศมหาอำนาจที่สามารถวางรากฐานอำนาจผ่านการศึกษาความมั่นคงทางไซเบอร์ ผ่านแนวคิดของ Myriam Dunn Cavelty และ Andreas Wenger (2020) ที่ได้อธิบายถึงความสัมพันธ์ระหว่างเทคโนโลยี, การเมือง และวิทยาศาสตร์ โดยทางด้านเทคโนโลยีสามารถส่งผลต่อปฏิกิริยาทางสังคมและการเมือง ส่งผลต่อการกำหนดนโยบายจากการดำเนินการของรัฐ และการกล่าววาทกรรมต่างๆที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ ที่ส่งผลต่อวิวัฒนาการทางวิทยาศาสตร์ที่เกี่ยวข้องกับโลกไซเบอร์, และ วิทยาศาสตร์



ภาพประกอบ 3 การวิเคราะห์ความมั่นคงทางไซเบอร์

ที่มา: Myriam Dunn Cavelty และ Andreas Wenger (2020)

นอกจากนี้ การวิเคราะห์ไปยังกรอบแนวคิดลำดับสุดท้าย ที่ใช้ในการอธิบายโครงสร้างของโลกไซเบอร์ โดย David Clark (2010) ได้ทำการอธิบายโลกไซเบอร์ผ่าน 4 ลำดับชั้นได้ดังนี้

1. ลำดับชั้นทางกายภาพ (Physical layer) ที่อธิบายถึงโครงสร้างพื้นฐานเชิงกายภาพของระบบเครือข่ายอินเทอร์เน็ต

2. ลำดับชั้นทางตรรกะ (Logical layer) ที่อธิบายถึงการสร้างระบบหรือแอพพลิเคชั่นเพื่อใช้งานและทำให้เกิดการเชื่อมต่อบนโลกอินเทอร์เน็ต

3. ลำดับชั้นข้อมูล (Information layer) เป็นลำดับชั้นที่เกี่ยวข้องกับข้อมูลต่างๆที่เราได้บรรจุลงบนโลกอินเทอร์เน็ต

4. ลำดับชั้นผู้ใช้งาน (User layer) ซึ่งเป็นลำดับชั้นที่เกี่ยวข้องกับปัจเจกบุคคล, องค์กร และรัฐบาลในการใช้งานพื้นที่ทางไซเบอร์เพื่อจุดประสงค์ของประเทศตนเอง

ดังที่กล่าวมาข้างต้น การวิเคราะห์โดยใช้กรอบทฤษฎีจะทำให้ทราบว่าความท้าทายของประเทศมหาอำนาจที่เกิดจากความท้าทายความมั่นคงทางไซเบอร์ที่เกิดขึ้นในศตวรรษที่ 21 ของประเทศสหรัฐอเมริกานั้น ส่งผลกระทบต่อความมั่นคงทางไซเบอร์ระหว่างประเทศอย่างไร และความมั่นคงทางไซเบอร์ สามารถส่งผลต่อการเป็นผู้นำระหว่างประเทศมหาอำนาจในศตวรรษที่ 21 ได้และการศึกษาองค์ประกอบความมั่นคงทางไซเบอร์ และโครงสร้างความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา เพื่อวิเคราะห์ความสามารถในการเป็นสมองของโลกในอนาคต

ขอบเขตของการวิจัย

การศึกษาได้แบ่งขอบเขตการทำวิจัย ดังนี้

1. หน่วยวิเคราะห์

หน่วยวิเคราะห์ที่ใช้ในการวิจัยครั้งนี้คือ องค์กรที่มีส่วนเกี่ยวข้องกับการใช้การโจมตีทางไซเบอร์ อาทิเช่น รัฐบาล ภาคเอกชน กระทรวงกลาโหม กองกำลังทางไซเบอร์ และ แฮ็กเกอร์ที่สนับสนุนโดยรัฐบาล

2. เครื่องมือที่ใช้ในการวิจัย

ผู้วิจัยใช้การค้นคว้าผ่านเว็บไซต์ และการค้นคว้าจากหนังสือต่างประเทศ บทความต่างประเทศ บทความทางการของรัฐบาลที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ และการวิเคราะห์สถิติการโจมตีทางไซเบอร์ระหว่างประเทศสหรัฐอเมริกา ในช่วงทศวรรษที่ 21

3. การเก็บรวบรวมข้อมูล

ผู้วิจัยได้เลือกวิธีการเก็บรวบรวมข้อมูลผ่านการวิเคราะห์เอกสาร

4. ขอบเขตระยะเวลาที่ทำการศึกษา

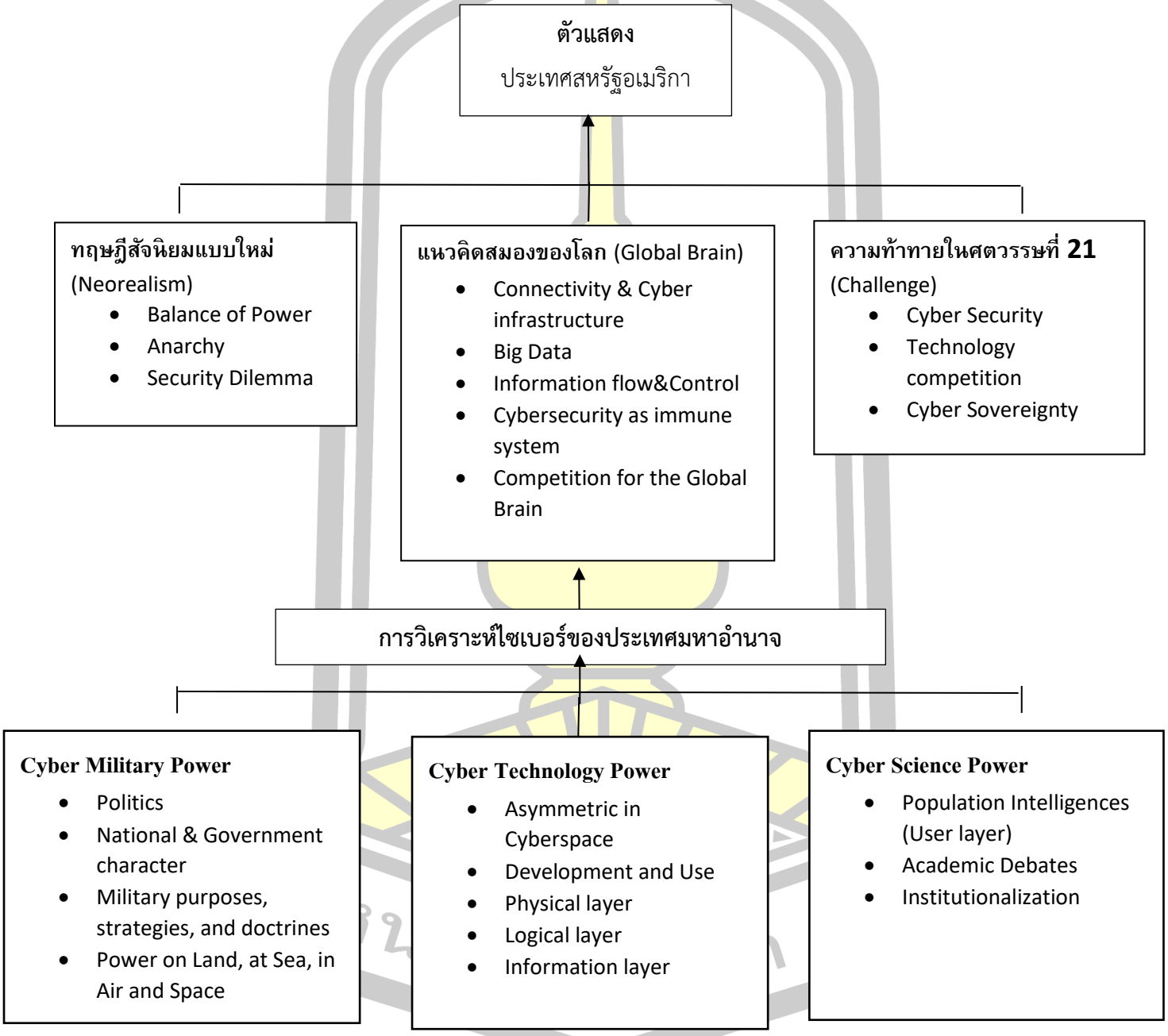
ช่วงเวลาที่ทำการศึกษาและวิเคราะห์ข้อมูล วิทยานิพนธ์ฉบับนี้ศึกษาความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา และการโจมตีทางไซเบอร์ของแต่ละประเทศ ในช่วงระยะเวลาตั้งแต่ ค.ศ. 2000 – 2022 เนื่องจากช่วงเวลาดังกล่าว เป็นช่วงเวลาที่แต่ละประเทศได้นำไซเบอร์เข้ามาเป็นส่วนหนึ่งของความมั่นคงแห่งชาติ การเสริมสร้างความมั่นคงทางไซเบอร์ทั้งทางด้านบุคลากร งบประมาณ และความรู้ทางเทคโนโลยี ที่มีพัฒนาการมาอย่างต่อเนื่อง และการใช้ไซเบอร์ร่วมกับการทำสงครามแบบดั้งเดิม ด้วยเหตุนี้ ผู้วิจัยจึงเลือกช่วงเวลาดังกล่าวเพื่อวิเคราะห์สมมติฐานการวิจัยได้อย่างชัดเจน

5. ขอบเขตหน่วยพื้นที่

วิทยานิพนธ์ฉบับนี้มุ่งวิเคราะห์บทบาทของประเทศสหรัฐอเมริกา เป็นกลุ่มประเทศมหาอำนาจที่มีบทบาทอย่างยิ่งในการใช้ไซเบอร์ในประเด็นทางด้านการเมืองระหว่างประเทศและการโจมตีทางไซเบอร์ในศตวรรษที่ 21 จากการใช้ไซเบอร์ในพฤติกรรมทางด้านความสัมพันธ์ระหว่างประเทศ อาทิเช่น การแฮ็กข้อมูลเพื่อสร้างผลประโยชน์แห่งชาติ การโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงแห่งชาติ และการให้ความสำคัญกับไซเบอร์เพื่อการสร้างความมั่นคงแห่งชาติที่เพิ่มมากขึ้นโดยอาศัยกรอบระยะเวลาข้างต้น เพื่อเป็นกรอบในการศึกษา

กรอบแนวคิดการวิจัย

ผู้วิจัยนำเสนอเป็นกรอบแนวคิดการวิจัยเรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกา ในศตวรรษที่ 21



ภาพประกอบ 4 กรอบแนวคิดการวิจัย

ที่มา: ปรับประยุกต์จาก Myriam Dunn Cavelty และ Andreas Wenger (2020), David Clark (2010)

นิยามศัพท์เฉพาะ

ไซเบอร์ (Cyber) มีต้นกำเนิดมาจากรากศัพท์ภาษากรีกโบราณคำว่า “kybereo” มีความหมายคือ การช่วยเหลือ การควบคุมทิศทาง การแนะนำ การควบคุม และการบริหารจัดการ (Lehto, 2013) และใน ค.ศ. 1984 คำว่าไซเบอร์ได้ปรากฏในรูปแบบของคำว่า “โลกไซเบอร์” (Cyberspace) จากนวนิยายวิทยาศาตร์เรื่อง Neuromancer ของ William Gibson โดยมีการนิยามโลกไซเบอร์ว่า “เป็นการแสดงถึงสิ่งแวดล้อมที่สมมุติขึ้นมา” และ “เป็นการแสดงภาพของข้อมูลจากคอมพิวเตอร์ทุกเครื่องในการใช้งานของมนุษย์” หลังจากนั้น การใช้คำว่า “ไซเบอร์” ได้ถูกนำมาปรับใช้ในการแสดงถึงนามธรรมหรือสิ่งแวดล้อมต่างๆที่มีปฏิกิริยาเกิดขึ้นในโลกอินเทอร์เน็ตและคอมพิวเตอร์ นิยามของคำว่าไซเบอร์ สามารถแบ่งออกได้เป็นทั้งหมด 5 ส่วนหลักสำหรับการใช้งาน ได้แก่ โครงสร้างพื้นฐานทางไซเบอร์ เครือข่ายและการสื่อสาร ระบบสารสนเทศ อุปกรณ์เทคโนโลยี และ สภาพแวดล้อมเสมือนจริง (Azmi & Kautsarina, 2019)

งานวิจัยชิ้นนี้ ผู้วิจัย กำหนดความหมายของคำว่า “ไซเบอร์” ตามบริบทต่างๆที่ได้อธิบายในเนื้อหา ดังนี้

1. ไซเบอร์ ในบริบทเชิงพฤติกรรม เช่น การโจมตี การใช้งานเพื่อสงคราม เรียกว่า การโจมตีทางไซเบอร์ ซึ่งหมายถึงการกระทำการโจมตีโดยไม่ใช่การโจมตีแบบใช้อาวุธแบบดั้งเดิม (Conventional weapons) แต่เป็นการโจมตีทางไซเบอร์ด้วยเทคโนโลยีในพื้นที่โลกเสมือน (Virtual environment)

2. ไซเบอร์ ในบริบทเชิงวัตถุ เช่น สายเคเบิ้ลใต้ทะเล เซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ อุปกรณ์เทคโนโลยี โครงสร้างพื้นฐานสำคัญที่พึ่งพาอินเทอร์เน็ต

3. ไซเบอร์ ในบริบทเชิงนโยบาย เช่น นโยบายทางการทหารของภาครัฐ นโยบายการเมืองระหว่างประเทศ นโยบายความมั่นคงแห่งชาติ กฎหมายในโลกไซเบอร์

4. ไซเบอร์ ในบริบทเชิงผู้ใช้งาน เช่น ภาครัฐ ภาคเอกชน ปัจเจกบุคคล ตัวแสดงที่สนับสนุนโดยภาครัฐ กลุ่มก่อการร้ายทางไซเบอร์

5. ไซเบอร์ ในบริบทเชิงพื้นที่ เช่น การทำสงครามในโลกเสมือน โลกไซเบอร์ อินเทอร์เน็ต

ความมั่นคงทางไซเบอร์ (Cybersecurity) Myriam Dunn Cavelty & Andreas Wenger (2020) ได้อธิบาย ความมั่นคงทางไซเบอร์ ว่า ความมั่นคงทางไซเบอร์ มีนิยามที่เปลี่ยนแปลงตามกาลเวลาและวิวัฒนาการของเทคโนโลยีทางไซเบอร์ แต่สิ่งที่สามารถปูพื้นฐานความเข้าใจของนิยามความมั่นคงทางไซเบอร์มีอยู่ 2 ประการ

ประการแรก คือ การใช้เทคโนโลยีดิจิทัลของมนุษย์ทั้งในทางที่ถูกต้องและไม่ถูกต้องของตัวแสดงที่เป็นมนุษย์ในด้านเศรษฐกิจ สังคม และการเมือง

ประการที่สอง การที่รัฐใช้ไซเบอร์เป็นเครื่องมือที่เป็นทางการและไม่เป็นทางการ ในการเจรจาและแก้ไขความขัดแย้งระหว่างรัฐ รวมถึงความสัมพันธ์ภายในรัฐกับระบบราชการ ภาคเอกชน ภาคประชาสังคม เพื่อกำหนดบทบาท ความรับผิดชอบ ขอบเขตทางกฎหมาย และ กฎต่างๆที่เห็นร่วมกันระหว่างรัฐ ซึ่งบทบาทของรัฐในขอบเขตความมั่นคงไซเบอร์ รัฐมีบทบาทที่หลากหลาย ไม่ว่าจะเป็นการเป็นผู้ออกกฎหมาย ผู้รักษากฎหมาย และผู้บังคับใช้กฎหมายต่อตัวแสดงที่เป็นภัยต่อสังคม และภัยระหว่างรัฐอื่นๆ

นิยามที่แท้จริงของความมั่นคงทางไซเบอร์ มีนิยามที่แตกต่างกันออกไปตามบริบท และวัตถุประสงค์ของแต่ละภาคส่วน ไม่ว่าจะเป็นการนิยามเชิงเทคนิคที่เกี่ยวข้องกับหลักวิทยาศาสตร์ การนิยามเชิงความมั่นคงจากองค์กรต่างๆ การนิยามเชิงสังคมและเศรษฐกิจ ดังนี้

นิยามเชิงเทคนิค

1. ความมั่นคงทางไซเบอร์ หมายถึง วิธีการป้องกันทางไซเบอร์เพื่อใช้ตรวจสอบและขัดขวางการรุกรานทางไซเบอร์ที่สามารถเกิดขึ้นได้ (Kemmerer, 2003)
2. ความมั่นคงทางไซเบอร์ หมายถึง การป้องกันเครือข่ายอุปกรณ์คอมพิวเตอร์และข้อมูลต่างๆที่อยู่ในระบบ จากการโจมตีเพื่อเจาะระบบเข้าไปทำลายหรือขัดขวางการทำงานโดยเจตนา (Lewis, 2006)
3. ความมั่นคงทางไซเบอร์ หมายถึง การลดความเสี่ยงจากการถูกโจมตีไม่ว่าจะเป็นซอฟต์แวร์ คอมพิวเตอร์ และระบบเครือข่ายอินเทอร์เน็ต และความเสี่ยงจากไวรัสคอมพิวเตอร์ การปกป้องโดยใช้โปรแกรมตรวจจับการบุกรุก การบล็อกข้อมูลที่เป็นอันตราย และการปรับใช้การเข้าถึงข้อมูลที่ปลอดภัยมากขึ้น ด้วยการยืนยันตัวตน และการใช้งานรหัสเพื่อเข้าถึงข้อมูล (Amoroso, 2006)

นิยามเชิงความมั่นคงจากองค์กร

1. ความมั่นคงทางไซเบอร์ หมายถึง การรวบรวมเครื่องมือ นโยบาย แนวคิดทางด้านความมั่นคง มาตรการป้องกันและแนวทางการบริหารความเสี่ยง และการใช้เทคโนโลยีเพื่อป้องกันสภาพแวดล้อมทางไซเบอร์ ทรัพยากร และความปลอดภัยของผู้ใช้งาน (ITU, 2009)
2. ความมั่นคงทางไซเบอร์ หมายถึง ประสิทธิภาพในการปกป้องหรือป้องกันสภาพแวดล้อมทางไซเบอร์จากการโจมตีไซเบอร์ (CNSS, 2010)

3. ความมั่นคงทางไซเบอร์ หมายถึง เทคโนโลยี กระบวนการ แนวทางและมาตรการในการโต้ตอบที่ถูกออกแบบมาเพื่อป้องกันเครือข่ายคอมพิวเตอร์จากการถูกโจมตี และความเสียหาย รวมถึงการกีดกันการเข้าถึงข้อมูลลับ โดยเป็นการออกแบบที่สมบูรณ์และพร้อมใช้งานตลอดเวลา (Public Safety Canada, 2014)
4. ความมั่นคงทางไซเบอร์ หมายถึง กระบวนการ ความสามารถ หรือสิ่งที่ทำให้ระบบสารสนเทศและข้อมูลต่างๆอยู่ภายใต้การป้องกันจากความเสียหาย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการแสวงหาผลประโยชน์ในทางไซเบอร์ที่สามารถเกิดขึ้นได้ (DHS, 2014)

นิยามเชิงสังคมและเศรษฐกิจ

1. ความมั่นคงทางไซเบอร์ หมายถึง รูปแบบการสร้างความมั่นคงให้กับระบบสารสนเทศของสังคมภายในประเทศ โดยเป็นการให้ความมั่นใจต่อประสิทธิภาพในการปกป้องข้อมูล ทรัพย์สิน และโครงสร้างพื้นฐานที่สำคัญที่มีส่วนเชื่อมโยงกับโลกไซเบอร์ (Canongia & Mandarino, 2014)
2. ความมั่นคงทางไซเบอร์ หมายถึง สถานะที่ได้รับการปกป้องจากความพยายามเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือ มาตรการที่มีไว้เพื่อป้องกันเหตุการณ์เหล่านี้ (Oxford University Press, 2014)

จากนิยามที่แตกต่างกันออกไปของ ความมั่นคงทางไซเบอร์ ในงานวิจัยชิ้นนี้ เกี่ยวข้องกับความมั่นคงแห่งชาติ ความท้าทาย ความเป็นอนาธิปไตย และความก้าวหน้าทางเทคโนโลยีในศตรวรรษที่ 21 ผู้วิจัยจึงกำหนดนิยามของ ความมั่นคงทางไซเบอร์ สำหรับอธิบายในงานวิจัยชิ้นนี้ หมายถึง ประสิทธิภาพในการป้องกันการโจมตีทางไซเบอร์ ต่อผลประโยชน์แห่งชาติ โครงสร้างพื้นฐาน องค์ความรู้ และประชากร รวมถึงความสามารถในการพัฒนาเทคโนโลยีไซเบอร์ทั้งในด้านเทคโนโลยี วิทยาศาสตร์ และองค์ความรู้ที่เกิดจากประชากรภายในประเทศ และความสามารถในการสร้างความมั่งคั่งทางเศรษฐกิจที่เกิดจากพัฒนาการทางไซเบอร์ ซึ่งการให้นิยามความมั่นคงทางไซเบอร์นี้ จะสามารถทำให้ผู้อ่านได้เข้าใจถึงบริบทความมั่นคงทางไซเบอร์ ไม่ว่าจะเป็นทางด้านการทหาร เทคโนโลยี เศรษฐกิจ และวิทยาศาสตร์ได้อย่างครบถ้วน

สัจนิยมใหม่ (Neo-Realism) เป็นแนวคิดจาก Kenneth Waltz ที่ได้เขียนไว้ในหนังสือ Theory of International Politics ใน ค.ศ. 1979 โดยได้เสนอแนวคิดเกี่ยวกับสิ่งที่กำหนดพฤติกรรมของรัฐ ในการเมืองระหว่างประเทศ ที่ไม่ได้ขึ้นอยู่ที่ลักษณะเฉพาะของรัฐแต่ละรัฐเท่านั้น

แต่ขึ้นอยู่กับโครงสร้างของระบบระหว่างประเทศที่อยู่ภายใต้สภาวะความเป็นอนาธิปไตย โดยองค์ประกอบของแนวคิดสัจนิยมใหม่ ประกอบด้วย

1. ความเป็นอนาธิปไตย (Anarchy) หมายถึง การไม่มีอำนาจศูนย์กลางที่ควบคุมรัฐจากการเมืองระหว่างประเทศ รัฐแต่ละรัฐต่างพึ่งพาตนเอง
2. ความแตกต่างของความสามารถของรัฐ (Distribution of Capabilities) หมายถึง ความแตกต่างของความสามารถของแต่ละรัฐ อาทิเช่น การทหาร เศรษฐกิจ ที่เป็นตัวกำหนดการมีอำนาจในการเมืองระหว่างประเทศ
3. สมดุลแห่งอำนาจ (Balance of Power) หมายถึง ความพยายามในการรักษาสมดุลของอำนาจเพื่อไม่ให้ถูกรุกรานจากรัฐอื่นๆ
4. ระบบการช่วยเหลือตนเอง (Self-Help System) หมายถึง เหตุจากการไม่มีอำนาจควบคุมจากส่วนกลางหรือการเมืองระหว่างประเทศ รัฐแต่ละรัฐจึงต้องพัฒนาความสามารถของตนเพื่อความมั่นคงและการอยู่รอด

แนวคิดสัจนิยมใหม่ของ Kenneth Waltz ได้แยกแนวคิดสัจนิยมใหม่ ออกจากแนวคิดสัจนิยมแบบดั้งเดิม (Classical Realism) โดยมองว่า ปัจจัยเชิงโครงสร้างของระบบการเมืองระหว่างประเทศ มีความสำคัญมากกว่าปัจจัยการวิเคราะห์เชิงอุดมการณ์ของผู้นำในแต่ละรัฐ (Waltz, 1979)

ผู้วิจัยนำแนวคิดสัจนิยมใหม่ อธิบายงานวิจัยชิ้นนี้ ผ่านกรอบแนวคิดสัจนิยมใหม่ ในการให้ความหมาย แนวคิดสัจนิยมใหม่ หมายถึง ความพยายามในการสร้างนโยบายเพื่อรักษาความเป็นมหาอำนาจ การพัฒนากองกำลังทางการทหาร การใช้นโยบายทางเศรษฐกิจเพื่อรักษาอิทธิพลของประเทศ การสร้างพันธมิตรและรักษาสมดุลแห่งอำนาจ จากความท้าทายต่อประเทศมหาอำนาจ ในการเมืองระหว่างประเทศที่มีความเป็นอนาธิปไตย เฉกเช่นกันโลกไซเบอร์

ความเป็นอนาธิปไตย (Anarchy) เป็นองค์ประกอบสำคัญของแนวคิดสัจนิยมใหม่ เป็นการวิเคราะห์แบบโครงสร้าง (Structural Realism) โดย Robert Powell (1994) ได้อธิบายไว้ว่า ความเป็นอนาธิปไตย หมายถึง ระบบการเมืองระหว่างประเทศที่ไม่มีอำนาจสูงสุด (Hierarchy of Power) ซึ่งเป็นสภาวะที่ไม่มีรัฐบาลกลางของโลกในการบัญญัติกฎเกณฑ์ให้ปฏิบัติตาม แตกต่างจากการปกครองภายในประเทศ ที่มีรัฐบาลคอยควบคุมกฎหมายและการสร้างนโยบายความมั่นคงแห่งชาติ ดังนั้น รัฐแต่ละรัฐจึงมีความต้องพึ่งพาตนเอง (Self-Help System) เพื่อการรักษาอำนาจและพัฒนาประเทศของตนเพื่อเพิ่มประสิทธิภาพในการสร้างอำนาจของตนเอง ในสภาวะที่ไม่มีรัฐบาลในความหมายของ Robert Powell นั้น คำว่า ความเป็นอนาธิปไตย ไม่ได้หมายถึง สภาวะที่ทำให้เกิด

ความวุ่นวาย (Chaos) แต่เป็นการไม่มีโครงสร้างที่นำเสนออำนาจสูงสุดในการควบคุมพฤติกรรมของแต่ละรัฐ (Powell, 1994)

ผู้วิจัย กำหนดความหมายของ ความเป็นอนาธิปไตย เพื่อใช้ในการวิเคราะห์วิจัยฉบับนี้ ว่า ความเป็นอนาธิปไตย หมายถึง ระบบการเมืองระหว่างประเทศที่ไม่มีอำนาจสูงสุด และ ความเป็นอนาธิปไตยของโลกไซเบอร์ หมายถึง สภาพแวดล้อมโลกเสมือน ที่ไม่มีผู้กำหนดควบคุมที่ชัดเจน และโดยสมบูรณ์ ทำให้การแข่งขันความมั่นคงทางไซเบอร์ เปรียบเสมือนการแข่งขันทางด้านการพึ่งพาตนเองของรัฐ (Self-Help System) เพื่อป้องกันภัยคุกคามต่างๆที่มีพัฒนาการตลอดเวลา

ประเทศมหาอำนาจ (Great Power country) คำว่า “อำนาจ” ในทางการเมืองสามารถนิยามได้ในหลากหลายมิติและบริบทที่แตกต่างกัน ในความสัมพันธ์ระหว่างประเทศ อำนาจเปรียบเสมือนสิ่งสะท้อนความสัมพันธ์ระหว่างตัวแสดงทางการเมืองต่างๆ โดยเฉพาะการมองอำนาจในรูปแบบของรัฐ การมองอำนาจด้วยตัวแสดงที่เป็นรัฐ มาจากแนวคิดสัจนิยมแบบดั้งเดิม (Classical Realism) ที่มองว่าอำนาจมีความสัมพันธ์โดยตรงกับการควบคุม อำนาจในการกำหนดกฎเกณฑ์ และการสร้างอิทธิพลต่อรัฐอื่นๆ (Kaviani, 2017)

Joseph Nye (2011) ได้อธิบายถึงการมีอำนาจของประเทศใดประเทศหนึ่งไว้ว่า คำว่า “อำนาจ” ไม่ได้หมายถึงอำนาจทางการทหารเพียงอย่างเดียว แต่มีปัจจัยอื่นๆที่ต้องให้ความสำคัญด้วย เช่น Hard Power หมายถึง อำนาจจากความสามารถทางการทหารและเศรษฐกิจ, Soft Power หมายถึง อำนาจทางวัฒนธรรม อุดมการณ์ และนโยบายระหว่างประเทศที่ได้รับความสนใจจากประเทศนานาชาติ และ Smart Power หมายถึง อำนาจที่ใช้ทั้ง Hard Power และ Soft Power เพื่อให้เกิดผลลัพธ์ที่ดีที่สุด รวมถึงการอธิบายการเปลี่ยนผ่านของอำนาจว่า อำนาจของประเทศนั้นๆ สามารถมีการเปลี่ยนแปลงได้เช่นกัน (Nye 2011) ประกอบด้วย

1. การเปลี่ยนผ่านของอำนาจ หมายถึง การเปลี่ยนแปลงขั้วอำนาจจากกลุ่มประเทศหนึ่งไปอีกกลุ่มประเทศหนึ่ง ทั้งอำนาจทางการทหาร และเศรษฐกิจ
2. การกระจายของอำนาจ หมายถึง การให้ความสำคัญของอำนาจที่ไม่ใช่เพียงตัวแสดงที่เป็นรัฐ แต่เป็นการกระจายอำนาจไปยังภาคเอกชนที่มีบทบาทสำคัญต่อโลก กลุ่มก่อการร้าย และองค์กรภายนอกรัฐ

นิยามของการเป็นประเทศมหาอำนาจ Marius Ghincea (2023) ได้อธิบายว่า จะต้องเป็นรัฐที่มีคุณสมบัติทางด้านอำนาจทางการทหาร เศรษฐกิจ และการเมือง ที่สามารถกำหนดกฎระเบียบของโลกและสร้างกลุ่มประเทศพันธมิตรได้ และได้แสดงความเห็นถึงประเทศมหาอำนาจอย่างสหรัฐอเมริกา ในโลกที่กำลังเปลี่ยนแปลงจากการมีอำนาจนำเพียงอำนาจเดียว (Unipolarity) ไปสู่

ความท้าทายที่เกิดขึ้นจากหลากหลายประเทศ อาทิเช่น จีน รัสเซีย อินเดีย รวมถึงสหภาพยุโรป กลายเป็นการกระจายอำนาจแบบหลายขั้วอำนาจ (Multipolarity) (Ghincea, 2023)

ผู้วิจัย กำหนดขอบเขตนิยามของคำว่า ประเทศมหาอำนาจ ในวิจัยฉบับนี้ โดยให้ความหมายประเทศมหาอำนาจ หมายถึง ประเทศที่มีอำนาจทางการทหาร เศรษฐกิจ เทคโนโลยี และเป็นประเทศที่มี Smart Power ด้วยเช่นกัน รวมถึงการเป็นประเทศที่มีพันธมิตรจำนวนมาก

ประโยชน์ที่คาดว่าจะได้รับ

1. งานวิจัยชิ้นนี้จะสามารถช่วยพัฒนาความเข้าใจเกี่ยวกับบทบาทความมั่นคงทางไซเบอร์ของประเทศมหาอำนาจ โดยเฉพาะประเทศสหรัฐอเมริกา ที่มีอิทธิพลสำคัญต่อองค์ความรู้ไซเบอร์ และการเป็นประเทศมหาอำนาจทางไซเบอร์ ซึ่งการศึกษาในวิจัยชิ้นนี้ จะช่วยให้ผู้กำหนดนโยบายและนักวิชาการที่ต้องการศึกษาความรู้ทางไซเบอร์ ได้ศึกษาข้อมูลเชิงลึกเกี่ยวกับการวิเคราะห์ความมั่นคงทางไซเบอร์ ความเป็นอนาธิปไตยในโลกไซเบอร์ และผลกระทบจากการปกครองทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่ส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ

2. งานวิจัยชิ้นนี้สามารถนำไปปรับใช้เป็นต้นแบบในการศึกษาความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศอื่นๆในภูมิภาคได้ เช่น ประเทศจีน และรัสเซีย ซึ่งถือว่าเป็นประเทศมหาอำนาจที่มีบทบาทสำคัญในศตวรรษที่ 21 รวมถึงการเปรียบเทียบความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา และประเทศต่างๆ ส่งผลให้สามารถนำองค์ความรู้ที่เกิดขึ้นไปพัฒนาเป็นนโยบายทางการเมืองเพื่อสร้างความมั่นคง

3. งานวิจัยชิ้นนี้จะเป็นประโยชน์ต่อประเทศไทยจากการนำองค์ความรู้เหล่านี้ มาสร้างและพัฒนาการทำงานทางด้านความมั่นคงไซเบอร์ให้สอดคล้องกับการเปลี่ยนแปลงของโลก โดยเฉพาะการศึกษาเพื่อสร้างมาตรการและนโยบายเพื่อความปลอดภัยจากการคุกคามทางไซเบอร์จากประเทศมหาอำนาจของโลก การพัฒนาความสามารถทางเทคโนโลยีและการกำหนดนโยบายที่เหมาะสมสำหรับการรักษาอิทธิพลของสมดุลแห่งอำนาจในความเป็นอนาธิปไตยของโลกการเมืองระหว่างประเทศและโลกไซเบอร์

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

วิทยานิพนธ์ฉบับนี้ ได้ทำการศึกษาแนวคิด ทฤษฎีที่เกี่ยวข้องกับเรื่องความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ : สหรัฐอเมริกา ในศตวรรษที่ 21 โดยนำแนวคิดสัจนิยมใหม่มาเป็นแนวคิดหลักในการวิเคราะห์พฤติกรรมการใช้ไซเบอร์ของรัฐที่ส่งผลกระทบความสัมพันธ์ระหว่างประเทศและการท้าทายระเบียบโลก และใช้แนวคิดสมองของโลกเป็นแนวคิดรองเพื่อใช้ในการวิเคราะห์รูปแบบความมั่นคงทางไซเบอร์ที่เกิดขึ้นของแต่ละประเทศ

นอกจากนี้ วิทยานิพนธ์ฉบับนี้ได้ทำการศึกษา ค้นคว้า งานวิจัยและเอกสารที่เกี่ยวข้องโดยสรุปเป็นหัวข้อสาระสำคัญดังนี้

1. แนวคิดและทฤษฎีที่เกี่ยวข้อง
   1) แนวคิดสัจนิยมใหม่
   2) แนวคิดสมองของโลก
   3) ความท้าทายในศตวรรษที่ 21
   4) ความมั่นคงทางไซเบอร์
   5) ไซเบอร์และการเมืองระหว่างประเทศ
2. เอกสารและงานวิจัยที่เกี่ยวข้อง

แนวคิดและทฤษฎีที่เกี่ยวข้อง

1) แนวคิดสัจนิยมใหม่ (Neorealism)

การศึกษาเรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจสหรัฐอเมริกา ในศตวรรษที่ 21 เป็นการศึกษาผ่านพฤติกรรมของตัวแสดงที่เป็นรัฐ และตัวแสดงที่ไม่ใช่รัฐที่มีบทบาทในการกำหนดทิศทางความมั่นคงทางไซเบอร์ของแต่ละประเทศ และความเป็นอนาธิปไตยของโลกไซเบอร์ ทำให้พฤติกรรมของรัฐและตัวแสดงที่ไม่ใช่รัฐสามารถสร้างผลกระทบต่อความมั่นคงทางไซเบอร์อย่างไร้พรมแดน ซึ่งก่อนทบทวนวรรณกรรมของแนวคิดสัจนิยมดั้งเดิมแบบใหม่ เราควรทบทวนแนวคิดสัจนิยมแบบดั้งเดิม และ แนวคิดสัจนิยมแบบใหม่ เพื่อให้เห็นถึงวิวัฒนาการขององค์ความรู้และเพื่อเป็นแนวทางในการทำความเข้าใจแนวคิดสัจนิยมดั้งเดิมแบบใหม่ที่ใช้ในการวิเคราะห์วิทยานิพนธ์ฉบับนี้

ทฤษฎีสัจนิยม (Realism) หรือแนวคิดสัจนิยมแบบดั้งเดิม คือ การอธิบายความสัมพันธ์ระหว่างประเทศที่มองว่าการเมืองระหว่างประเทศควรอธิบายจากความเป็นจริงที่เกิดขึ้นมากกว่าการคาดคะเนซึ่ง Morgenthau (1985) ได้ทำการอธิบายแนวคิดทฤษฎีสัจนิยมผ่าน 6 ประการ ดังนี้

1. การเมืองแบบสัจนิยมมีความเชื่อว่า การเมืองและสังคมโดยรวมนั้น ถูกควบคุมและบริหารโดยกฎหมายที่มาจากวัตถุประสงค์ต่างๆที่เกิดจากธรรมชาติของมนุษย์
2. การเมืองแบบสัจนิยมมีแนวคิดในการนิยามผลประโยชน์ (interest) ด้วย อำนาจ (power)
3. การตีความผลประโยชน์ด้วยอำนาจ สามารถแปรเปลี่ยนตามสถานที่และเวลาได้
4. การเมืองแบบสัจนิยมมีแนวคิดว่า ศีลธรรมต่างๆในระดับสากลไม่สามารถถูกปรับใช้กับการกระทำของรัฐที่อยู่ในโลกระหว่างประเทศได้ แต่ต้องเป็นการวิเคราะห์ผ่านสถานการณ์ของเวลาและสถานที่นั้นๆ
5. การเมืองแบบสัจนิยมปฏิเสธในการระบุแรงจูงใจทางศีลธรรมในการกระทำของรัฐควบคู่กับศีลธรรมทางกฎหมายที่ถูกบริหารในระดับสากล
6. ความแตกต่างระหว่างการเมืองแบบสัจนิยมและการเมืองของสำนักคิดอื่นๆคือการมีแนวคิดในการยึดหลักความจริงอย่างลึกซึ้ง

Morgenthau (1948) กล่าวว่า “ไม่ว่าเป้าหมายที่แท้จริงของรัฐในโลกการเมืองระหว่างประเทศคืออะไร อำนาจ คือเป้าหมายที่เป็นที่ต้องการเสมอ” โดยนักคิดสัจนิยมมักเปรียบเทียบอำนาจว่าเปรียบเสมือนทรัพยากรของรัฐ อาทิเช่น ทรัพยากรทางธรรมชาติ ความสามารถทางอุตสาหกรรม ความแข็งแกร่งของกำลังทหาร และ การควบคุมประชากรของรัฐ และในมุมมองของนักสัจนิยมมองว่า ภายในโลกการเมืองระหว่างประเทศนั้น เป็นเรื่องที่ยากในการที่จะสร้างสมดุลทางอำนาจ (balance of power) แต่เป็นการนำโดยประเทศที่มีอำนาจมากที่สุดประเทศหนึ่งเท่านั้น

ภายหลังจากการได้รับอิทธิพลทางความคิดของ Morgenthau นักคิดชาวอเมริกัน Kenneth Waltz ได้เริ่มต้นการพัฒนาทฤษฎีสัจนิยมแบบดั้งเดิมของ Morgenthau ที่ให้ความสำคัญกับการกำหนดนโยบายต่างประเทศ และความสำคัญของธรรมชาติของมนุษย์ในมุมมองการเมืองระหว่างประเทศ เข้าสู่แนวคิดแบบสัจนิยมใหม่ (Neorealism) ที่ให้ความสำคัญไปยังบทบาทของโครงสร้างระหว่างประเทศ ความเป็นอนาธิปไตย (Anarchy) และ การกระจายอำนาจ (Distribution of Power) ในการอธิบายการดำเนินนโยบายและผลลัพธ์ในโลกการเมืองระหว่างประเทศ โดยเริ่มต้นจากการโต้แย้งการอธิบายของ Morgenthau เกี่ยวกับการเป็นธรรมชาติของมนุษย์ที่มักจะนำมาซึ่งสงครามและความขัดแย้งในการเมืองระหว่างประเทศ ซึ่ง Waltz ได้ให้เหตุผลว่า การอธิบายการเมืองระหว่างประเทศโดยวิเคราะห์เพียงการเป็นธรรมชาติของมนุษย์นั้น ไม่สามารถนำมาอธิบายซึ่งการเกิดสงครามหรือสันติภาพได้ ทฤษฎีสัจนิยมใหม่ เป็นการให้ความสำคัญไปยังความเป็นอนาธิปไตยของโลกการเมืองระหว่างประเทศ ในขณะที่ทฤษฎีสัจนิยมแบบดั้งเดิม ให้ความสำคัญกับความเป็น

ธรรมชาติของมนุษย์ โดยเขาได้เสนอการคิดผ่านการวิเคราะห์แบบเป็นลำดับชั้น (level of analysis) และการใช้วิธีที่มีความแม่นยำมากยิ่งขึ้นคือการวิเคราะห์ผ่านการมองให้เป็น ภาพ (image) ถึงแม้ว่าการวิเคราะห์การเมืองระหว่างประเทศจะเหมาะสมกับการใช้แนวคิดเชิงวิเคราะห์ (analytic thinking) แต่การเข้าใจการเมืองระหว่างประเทศให้ครอบคลุมมากยิ่งขึ้น ต้องอาศัยการมองผ่านวิธีการเชิงระบบ (systemic approach) (Waltz, 1959 : 9) โดยถกเถียงถึงการวิเคราะห์ในรูปแบบทั้ง 3 ระดับ คือ

1. ระดับปัจเจกบุคคล (individual) เป็นการศึกษาแบบพฤติกรรมศาสตร์ (Behavioral Sciences) ของตัวแสดงที่เป็นผู้นำในรัฐ โดย Waltz ถกเถียงในการวิเคราะห์ผ่านตัวผู้นำของรัฐว่าการวิเคราะห์ผ่านผู้นำของรัฐ พฤติกรรมของผู้นำของรัฐนั้น จะดำเนินตามนโยบายที่ถูกเสนอ

2. ระดับระบบการเมือง (political system) หรือ รัฐ เป็นการศึกษาผ่านการมองโครงสร้างภายในของรัฐ ว่าปัจจัยภายใน หรือ โครงสร้างของรัฐ คือตัวกำหนดพฤติกรรมของรัฐ

3. ระดับระบบการเมืองระหว่างประเทศ (international system) หรือ โครงสร้างระหว่างประเทศ (international structure) หมายถึง ในโลกอธิปไตย (Anarchy) ของการเมืองระหว่างประเทศ การให้ความสำคัญในการมองไปยังความเป็นไปได้ในการเกิดสงครามของรัฐที่มากกว่าสองรัฐขึ้นไปในการใฝ่หาผลประโยชน์แห่งชาติภายใต้ความเป็นอนาธิปไตยของการเมืองระหว่างประเทศที่ไม่มีรัฐใดๆคอยปกป้องหรือคุ้มครอง รัฐแต่ละรัฐล้วนมุ่งหาผลประโยชน์ของตนเอง ในวิถีทางที่ต้นคิดว่าถูกต้องและดีที่สุด ดังนั้น การมีรัฐบาลโลก (world government) คือหายนะที่จะนำพาไปสู่สงครามโลกในที่สุด (Ibid, 1959 : 238)

งานวิจัยนี้ ใช้ทฤษฎีสัจนิยมใหม่เป็นทฤษฎีหลักในการวิเคราะห์ปัจจัยที่ส่งผลต่อความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา องค์ประกอบของทฤษฎีสัจนิยมใหม่ที่งานวิจัยนำมาใช้ในการวิเคราะห์ เป็นการวิเคราะห์ที่เกี่ยวข้องกับโครงสร้างระหว่างประเทศที่มีความเป็นอนาธิปไตย (Anarchy) การรักษาดุลแห่งอำนาจ (Balance of Power) และสภาวะกลืนไม่เข้าคายไม่ออกทางด้านความมั่นคง (Security Dilemma) เนื่องจากการวิเคราะห์ความมั่นคงทางไซเบอร์ในการเมืองระหว่างประเทศ จะสามารถทำให้เข้าใจถึงความพยายามของรัฐ หรือประเทศมหาอำนาจ ที่ใช้นโยบายไซเบอร์ในการสร้างความได้เปรียบเชิงอำนาจทั้งทางด้านการเมือง เศรษฐกิจ และวิทยาศาสตร์ ภายใต้การแข่งขันในโลกอนาธิปไตยทั้งในการเมืองระหว่างประเทศและโลกไซเบอร์ในศตวรรษที่ 21 ซึ่งได้ทำการค้นคว้าการเชื่อมโยงของแนวคิดที่กล่าวมากับความมั่นคงทางไซเบอร์ ดังนี้

1.1 แนวคิดดุลแห่งอำนาจ (Balance of Power)

ทฤษฎีสัจนิยมใหม่ ให้ความสำคัญกับการรักษาดุลแห่งอำนาจในการเมืองระหว่างประเทศ เป็นการวิเคราะห์ผ่านพฤติกรรมของรัฐที่มีความพยายามสร้างหรือการรักษาอำนาจทางยุทธศาสตร์ โดยจากการศึกษาของ Randall

Schweller (2016) ที่ได้ทำการศึกษาแนวคิดดุลแห่งอำนาจ ในมุมมองทฤษฎีสัจนิยมใหม่ ได้อธิบายถึงพฤติกรรมของความพยายามรักษาอำนาจทั้งในรูปแบบการพัฒนาดุลอำนาจจากภายใน (Internal Balancing) และ การพัฒนาดุลอำนาจจากภายนอก (External Balancing) เช่นความพยายามในการสร้างพันธมิตรเพื่อคานอำนาจรัฐอื่นๆ

1.2 ความเป็นอนาธิปไตย (Anarchy)

การพึ่งพาตนเองของรัฐแต่ละรัฐในการเมืองระหว่างประเทศ เป็นพฤติกรรมเพื่อรักษาความอยู่รอดของรัฐ ซึ่งในการศึกษาของ Kenneth Waltz (1959) ได้กล่าวถึง ภายใต้ความเป็นอนาธิปไตย รัฐแต่ละรัฐต้องสร้างความสามารถของตนเองเพื่อป้องกันภัยคุกคาม ซึ่งในแง่ของความเป็นอนาธิปไตยในโลกไซเบอร์ มีความสอดคล้องในแง่ของการโจมตีทางไซเบอร์ที่ไม่สามารถควบคุมได้ทางกายภาพ อาทิเช่น การโจมตีจากตัวแสดงที่เป็นรัฐและตัวแสดงที่ไม่ใช่รัฐ ที่สามารถสร้างความเสียหายได้โดยไม่จำเป็นต้องพึ่งพาปัจจัยทางด้านภูมิศาสตร์ อีกทั้งยังไม่มีการควบคุมทางกฎหมายอย่างชัดเจน (Kello, 2018) ชี้ให้เห็นถึงความสำคัญของรัฐแต่ละรัฐ ที่ต้องสร้างความสามารถในการป้องกันการโจมตีทางไซเบอร์ ซึ่งเป็นผลกระทบจากความเป็นอนาธิปไตยในโลกไซเบอร์ เพื่อปกป้องความมั่นคงของรัฐตนเอง

1.3 สภาวะกลืนไม่เข้าคายไม่ออกของความมั่นคง (Security Dilemma)

ผลจากความเป็นอนาธิปไตยที่ทำให้รัฐแต่ละรัฐต้องพึ่งพาตนเอง นำไปสู่การสร้างความมั่นคงทางไซเบอร์ของแต่ละรัฐด้วยตนเอง ซึ่งในการสร้างความมั่นคงนี้ ส่งผลให้รัฐอื่นๆรู้สึกไม่ปลอดภัยด้วยเช่นกัน ทำให้เกิดการแข่งขันทางด้านความมั่นคง โดยในการศึกษาของ Gartzke & Lindsay (2022) ได้ทำการศึกษาถึงสภาวะกลืนไม่เข้าคายไม่ออกที่สามารถเกิดขึ้นในโลกไซเบอร์ โดยได้อธิบายว่า เมื่อถึงจุดที่รัฐใดรัฐหนึ่งสามารถพัฒนาความสามารถทางด้านความมั่นคงทางไซเบอร์เพื่อป้องกันตนเองได้สำเร็จ จะถูกมองว่ากลายเป็นภัยคุกคามจากรัฐอื่นๆ อาทิเช่น การที่ประเทศสหรัฐอเมริกาได้สร้าง ยุทธศาสตร์ไซเบอร์แห่งชาติ (National Cyber Strategy) เพื่อป้องกันภัยคุกคามทางไซเบอร์ต่างๆ แต่สำหรับประเทศจีนและรัสเซียแล้วนั้น กลับมองว่าเป็นการสร้างภัยคุกคาม ทำให้เกิดการเร่งพัฒนาความสามารถทางไซเบอร์เพื่อรองรับสงครามไซเบอร์ที่

สามารถเกิดขึ้นได้ตลอดเวลา รวมถึงการศึกษาของ Arslan (2023) ที่ได้ค้นพบถึงความแตกต่างของสภาวะกลืนไม่เข้าคายไม่ออกในความมั่นคงทางไซเบอร์และแบบดั้งเดิม คือ โลกไซเบอร์ไม่มีขอบเขตที่แน่ชัดในการตรวจสอบ ทำให้การโจมตีต่างๆสามารถเกิดขึ้นได้โดยปกปิดตัวตน และสามารถเกิดขึ้นได้อย่างรวดเร็วด้วยเช่นกัน

การวิเคราะห์ทฤษฎีสัจนิยมใหม่ผ่านแนวคิดดุลแห่งอำนาจ ความเป็นอนาธิปไตย และสภาวะกลืนไม่เข้าคายไม่ออกทางด้านความมั่นคง จะสามารถทำให้เห็นถึง ความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกาในศตวรรษที่ 21 ที่สร้างผลลัพธ์ให้เห็นถึงการแข่งขันทางด้านอำนาจในโลกไซเบอร์ ภายใต้โลกอนาธิปไตย อีกทั้งยังใช้ไซเบอร์เป็นเครื่องมือหนึ่งทางด้านเครื่องมือทางยุทธศาสตร์ ที่รัฐได้ใช้เพื่อปกป้องความมั่นคงและสร้างอิทธิพลของตนเอง ดังนั้น การใช้ทฤษฎีสัจนิยมใหม่ในการวิเคราะห์ความมั่นคงทางไซเบอร์ เป็นสิ่งสำคัญที่จะทำให้เข้าใจถึงพฤติกรรมของรัฐและผลกระทบทางไซเบอร์ที่สามารถเกิดขึ้นจากความท้าทายในศตวรรษที่ 21

2) แนวคิดสมองของโลก (Global Brain)

การพัฒนาของโลกที่ผ่านมา ล้วนเกิดจากการเชื่อมต่อของโลกที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ ไม่ว่าจะเป็นทางด้านเทคโนโลยี เศรษฐกิจ และสังคม พัฒนาการทางเครือข่ายได้เติบโตอย่างก้าวกระโดด และสร้างผลกระทบทั้งทางตรงและทางอ้อมต่อผู้ใช้งานและผู้ที่ไม่ได้ใช้งานเครือข่ายคอมพิวเตอร์ เครือข่ายสารสนเทศของโลกได้สร้างความเป็นสากลมากยิ่งขึ้น มีการชี้นำแนวทางของโลกผ่านโครงสร้างทางเทคโนโลยี รวมถึงการชี้นำพฤติกรรมของมนุษย์ในการใช้ชีวิตประจำวัน จนเปรียบเสมือนกับว่า เทคโนโลยีอินเทอร์เน็ตนั้น ได้กลายเป็นระบบประสาทของมนุษยชาติไปแล้ว

แนวคิดสมองของโลก เป็นแนวคิดที่เกิดจากการบรรยายเชิงเปรียบเทียบเกี่ยวกับองค์ความรู้และเครือข่ายความรู้ที่เกิดจากการสรรค์สร้างร่วมกันของมนุษย์ จากการเชื่อมต่อความรู้ทางด้านคอมพิวเตอร์และเทคโนโลยีที่ทำให้องค์ประกอบต่างๆเชื่อมโยงเข้าหากัน การเชื่อมต่อที่เกิดขึ้นทำให้เทคโนโลยีคอมพิวเตอร์ได้มีบทบาทเปรียบเสมือนการสั่งการโดยสมอง ไม่ว่าจะเป็นการตัดสินใจ การแก้ไขปัญหา การหาการเชื่อมต่อใหม่ และการค้นพบองค์ความรู้ใหม่ ไม่มีปัจเจกบุคคล กลุ่มคน องค์กร หรือคอมพิวเตอร์ใดที่ควบคุมระบบนี้ ซึ่งเปรียบเสมือนโลกไซเบอร์ ที่องค์ความรู้ต่างๆที่เกิดขึ้นจากการเชื่อมต่อเครือข่าย ได้ถูกกระจายตัวไปยังทุกตัวแสดงตั้งแต่ภาครัฐ ไปจนถึงปัจเจกบุคคล

รากฐานแนวความคิดสมองของโลกนั้น มีการให้นิยามที่คล้ายคลึง หรือใกล้เคียงมาอย่างยาวนาน โดยในงานของ Francis Heylighen ได้ทำการศึกษาถึงพัฒนาการของแนวคิดสมองของโลก โดยได้แบ่งออกเป็นสามประเภทหลัก คือ

ประเภทแรก เรียกว่า แนวคิดสมองของโลกเหมือนระบบของสิ่งมีชีวิต (Organicism) ซึ่งเป็นประเภทแนวคิดสมัยเก่าที่เปรียบเทียบองค์กรหรือสถาบันเปรียบเสมือนระบบของสิ่งมีชีวิต ที่แต่ละหน่วยในองค์กรหรือสถาบัน จะมีหน้าที่ของตนเองในการดูแลระบบต่างๆเพื่อทำให้ระบบสามารถดำเนินต่อไปได้ โดยได้รับอิทธิพลจากแนวคิดจากนักคิดมากมายในอดีต อาทิเช่น การอธิบายของ Herbert Spencer (1876) ในงาน Principles of Sociology ที่ได้กล่าวถึงการที่สังคมเปรียบเสมือนระบบอวัยวะในร่างกาย มีการชี้ให้เห็นถึงการเปรียบเทียบระหว่างบทบาทของโครงสร้างและหน้าที่ของระบบต่างๆ และนักชีววิทยา Gregory Stock ที่ได้เขียนถึงกระบวนการของการรวมกันของปัจเจกบุคคลเกิดจากการเพิ่มขึ้นของเทคโนโลยีทำให้เกิดสิ่งที่เหนือธรรมชาติระดับโลก (global superorganism) ซึ่งสอดคล้องกับแนวคิดของ Spencer ที่ให้ความสำคัญแนวคิดเกี่ยวกับความเป็นอยู่ของสังคม เศรษฐกิจ พัฒนาการของเทคโนโลยี และพัฒนาการของสิ่งมีชีวิต ที่มีความสอดคล้องและพึ่งพากันและกัน ยกตัวอย่าง การเพิ่มขึ้นของรถไฟ หรือการเพิ่มขึ้นของเทคโนโลยีการเชื่อมต่อสื่อสาร ที่เปรียบเสมือนการเพิ่มขึ้นของหลอดเลือดหัวใจ หรือ ระบบประสาท

ประเภทที่สอง เรียกว่า แนวคิดสมองของโลกเหมือนเครือข่ายสารานุกรมสากล (Encyclopedism) เป็นแนวคิดเกี่ยวกับการบันทึกข้อมูลสาธารณะต่างๆที่เกี่ยวกับองค์ความรู้ของมนุษย์ ซึ่งแนวคิดนี้ได้ถูกค้นพบใน ค.ศ. 1737 ในคำปราศัยของ Chevalier de Ramsay ที่อธิบายหนึ่งในจุดประสงค์ขององค์กรฟรีเมสัน โดยได้กล่าวว่า “เพื่อการเตรียมการวัตถุดิบสำหรับพจนานุกรมสากล ใน ณ ที่นี้คือการรวบรวมแสงสว่างจากรัฐต่างๆที่จะถูกรวมกันในผลงานชิ้นเดียว ที่จะกลายเป็นห้องสมุดสากลที่สวยงาม ยอดเยี่ยม ส่องสว่าง แข็งแกร่ง และเป็นประโยชน์ทั้งทางด้านวิทยาศาสตร์และศิลปะอันสูงส่ง ผลงานชิ้นนี้จะเพิ่มพูนในทุกศตวรรษ ตามการเพิ่มขึ้นของความรู้” สิ่งที่เป็นผลกระทบสำคัญต่อแนวคิดนี้คือ สารานุกรมของประเทศฝรั่งเศสที่ถูกตีพิมพ์ในช่วง ค.ศ. 1751 ถึง 1772 ที่เป็นการเผยแพร่องค์ความรู้ของแนวคิดการใช้เหตุและผล วิทยาศาสตร์ และเทคโนโลยี และเป็นรากฐานของการก่อให้เกิดอุตสาหกรรมและการปฏิวัติฝรั่งเศส ในเวลาต่อมาในช่วงท้ายศตวรรษที่ 19 องค์ความรู้ต่างๆได้เกิดขึ้นอย่างรวดเร็วและมากจนเกินไปที่จะถูกตีพิมพ์และจัดเก็บไว้ในการรวบรวมแบบใดแบบหนึ่ง นักเขียนชาวเบลเยี่ยมนาม Paul Otlet ผู้เป็นบิดาแห่งบรรณานุกรม ซึ่งต่อมาถูกเรียกว่าสารสนเทศศาสตร์ ที่ได้จัดการแก้ไขปัญหาการรวบรวมและจัดการองค์ความรู้ของโลกใบนี้ เขาได้ออกแบบระบบโครงสร้างของเอกสารที่ได้บรรจุตัวอักษรหรือรูปภาพที่เชื่อมโยงกันและก่อตั้ง Union of International Organizations เพื่อช่วยในการรวบรวมองค์ความรู้เหล่านี้ และใน ค.ศ. 1935 Otlet ยังได้พัฒนาแนวคิดสมองของโลกที่คล้ายกับการสร้าง world-wide web ด้วยเช่นกัน โดยได้ให้ทัศนะถึงการที่มนุษย์ไม่จำเป็นที่จะต้องใช้เอกสารในการเก็บข้อมูลอีกต่อไป แต่ต้องมาจากการใช้เครื่องจักรในการสร้างทุกสิ่งให้เป็นสากล ผู้คนสามารถเข้าถึงข้อมูลเหล่านั้นได้จากระยะทางที่แตกต่างกัน และในขณะเดียวกัน นักเขียนชาวอังกฤษ H.G.Wells ก็ได้มีจินตนาการ

เกี่ยวกับสมองของโลกด้วยเช่นกัน ถึงกระนั้น Otlet และ Wells ก็ยังไม่สามารถแสดงให้เห็นถึงแนวคิดที่ชัดเจนเกี่ยวกับการนำเทคโนโลยีเข้ามาใช้ในการสร้างระบบขององค์ความรู้ จนกระทั่งใน ค.ศ. 1991 นักวิทยาศาสตร์ชาวอังกฤษ Tim Berners-Lee ได้ทำการคิดค้น World-Wide Web ซึ่งเป็นการนำ เอกสาร hypertext (HTML) และแบบแผนในการสร้างตำแหน่งที่ตั้งของเอกสารบนอินเทอร์เน็ต (URL) ซึ่งเอกสารเหล่านี้สามารถเชื่อมต่อกันได้โดยตรง ขึ้นอยู่กับจุดประสงค์ของการใช้งานมากกว่าตำแหน่งของภูมิประเทศที่อยู่อาศัย ส่งผลให้เว็บได้เป็นส่วนแพร่กระจายองค์ความรู้ไปทั่วโลกและมีความเปิดเผย และเป็นประชาธิปไตยทางด้านข้อมูลมากกว่าระบบรวมศูนย์

ประเภทที่สาม เป็นประเภทแนวคิดสมองของโลกเกี่ยวกับอุบัตินิยม (Emergentism) ที่เกี่ยวข้องกับมุมมองของวิญญาณ และความเชื่อทางศาสนา ที่ว่าด้วยการบรรลุนิพพานด้วยการเข้าสู่การทำสมาธิและทิ้งความเป็นปัจเจกเพื่อหลอมรวมความเป็นมนุษย์เข้ากับโลกใบนี้ เป็นมุมมองที่เกี่ยวข้องกับความเชื่อทางศาสนา โดยนักเขียนที่ได้พัฒนาแนวคิดนี้ขึ้นมาคือ นักบรรพชีวิตวิทยาชาวฝรั่งเศสและเป็นนักบวชนิกายเยซูอิต Pierre Teilhard de Chardin ที่ได้รวบรวมความรู้ของการวิวัฒนาการและศาสนศาสตร์ เข้าสู่ความเชื่อทางศาสนาและมุมมองของการเขียนบทกวีเกี่ยวกับการวิวัฒนาการในอนาคต ซึ่งในงานเขียนของ Teilhard ได้นิยามวิวัฒนาการว่า เป็นการเพิ่มขึ้นของความซับซ้อนและการมีสมาธิที่มีลักษณะเพิ่มขึ้นจากการเชื่อมต่อระหว่างองค์ประกอบต่างๆ ดังนั้น สมองของมนุษย์ที่มีเซลล์ประสาทมากกว่าพันล้านเซลล์และการตั้งสมาธิ คือการทำงานร่วมกันของระบบประสาทที่มีความซับซ้อนมากที่สุดในทางชีววิทยา แต่วิวัฒนาการของระบบนิเวศของโลกที่ทำให้เกิดการเกิดขึ้นนูสเฟียร์ (Noosphere) ซึ่งเป็นวิวัฒนาการของระบบนิเวศ รวมถึงระบบการเชื่อมต่อทางความคิดของโลก ระบบสารสนเทศและการสื่อสาร ล้วนเป็นเป้าหมายของกลุ่มองค์กรทางศาสนาที่ต้องการจะทำให้บรรลุ จนกระทั่งภายหลังการตายของ Teilhard ใน ค.ศ. 1955 งานเขียนหลักของเขาได้ถูกตีพิมพ์ และนักเทววิทยาชาวเบลเยี่ยม Max Wildiers ได้นำแนวคิดวิวัฒนาการของจิตใจของ Teilhard มาพัฒนาต่อโดยให้ความสำคัญไปยังบทบาทของเทคโนโลยีในนูสเฟียร์ และในเวลาต่อมา ได้มีการนำเทคโนโลยีเข้ามาปรับใช้ในการสนับสนุนการขยายตัวของการทำสมาธิในการพัฒนาสภาพจิตใจของมนุษย์ ซึ่งเมื่อถึงยุคอินเทอร์เน็ต การเชื่อมต่อของการสื่อสารทำให้มนุษย์สามารถเชื่อมต่อกันได้ทั่วโลก เปรียบเสมือนการเชื่อมต่อของเซลล์ประสาทของมนุษย์ทั่วโลกที่เชื่อมเข้าหากัน ทำให้เปรียบเสมือนการทำสมาธิของมนุษย์มีประสิทธิภาพมากยิ่งขึ้น (Heylighen, 2011)

จากมุมมองทั้งสามประเภทที่กล่าวมา แสดงให้เห็นถึงวิวัฒนาการที่พยายามเชื่อมโยงองค์ความรู้ของโลกภายใต้แนวคิดสมองของโลก โดยเป็นการวิวัฒนาการตั้งแต่ยุคของนักคิดที่รวบรวมตัวหนังสือลงสู่กระดาษ มาจนถึงการใช้เทคโนโลยีอินเทอร์เน็ตเข้ามามีบทบาทในการพัฒนากระบวนการเรียนรู้ของมนุษย์ให้มีประสิทธิภาพสูงสุด เป็นการอธิบายเชิงเปรียบเทียบในการสร้างองค์

ความรู้ผ่านการร่วมมือกันระหว่างมนุษย์ผ่านการใช้งานเทคโนโลยีเครือข่ายคอมพิวเตอร์ หรือ โลกไซเบอร์ ที่ทำหน้าที่คล้ายกับสมอง ในการตัดสินใจ แก้ปัญหา และสร้างองค์ความรู้ใหม่ ในสภาวะอนาธิปไตยที่ไม่มีผู้ควบคุม แต่เป็นเครือข่ายระบบที่กระจายตัวอยู่ทั่วโลก

การศึกษาของ Marios Kyriazis (2015) ได้ศึกษาเกี่ยวกับแนวคิดสมองของโลกและได้ผลสรุปการศึกษา แนวคิดสมองของโลก คือแนวคิดที่อธิบายถึงการที่มนุษยชาติได้ก้าวข้ามวิวัฒนาการของการใช้สมองเพื่อการเรียนรู้จากในอดีตที่เป็นการสื่อสารเพียงบุคคลต่อบุคคล สู่การใช้เทคโนโลยีไซเบอร์ที่เปลี่ยนแปลงวิธีการทำงานร่วมกันของมนุษย์ ที่กลายเป็นเครือข่ายเปรียบเสมือนสมองของโลก และนอกจากนี้ยังให้นิยามถึงการควบรวมระหว่างมนุษย์และเทคโนโลยีเข้าหากัน ไม่ว่าจะเป็นทางด้านการพัฒนาเมืองอัจฉริยะ (Smart city) การสร้างสิ่งแวดล้อมที่เอื้อต่อการแบ่งปันข้อมูล รวมถึงการฝังอุปกรณ์ทางชีวภาพเข้าสู่มนุษย์ และในภาคสังคม ยังได้กล่าวถึงการเพิ่มความเข้มแข็งของภาคสังคมด้วยการส่งเสริมให้เกิดการสร้างเครือข่ายโซเชียลมีเดียที่มีศีลธรรม แชร์ข้อมูลที่ส่งผลประโยชน์ต่อส่วนรวม และสร้างการรับรู้ในสังคมออนไลน์ ทำให้การเมืองมีความมั่นคงได้มากยิ่งขึ้น

งานวิจัยชิ้นนี้ ใช้ปัจจัยสำคัญที่เป็นส่วนประกอบของแนวคิดสมองของโลก ในการวิเคราะห์ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกา ในศตวรรษที่ 21 ดังต่อไปนี้

- การเชื่อมต่อและโครงสร้างพื้นฐานไซเบอร์ (Connectivity & Cyber Infrastructure) หมายถึง การวิเคราะห์ปัจจัยสำคัญของการสร้างความเป็นสมองของโลกผ่านพัฒนาการเทคโนโลยีสารสนเทศและการพัฒนาระบบเครือข่ายเพื่อสร้างการเชื่อมโยงระหว่างมนุษย์และเทคโนโลยีสารสนเทศที่มีประสิทธิภาพมากยิ่งขึ้น ไม่ว่าจะเป็นทางด้านการเพิ่มความรวดเร็วในการถ่ายโอนข้อมูล การส่งเสริมการสร้างองค์ความรู้ในการแข่งขันระดับโลก ระบบโครงสร้างพื้นฐานไซเบอร์ และความมั่นคงทางไซเบอร์ที่มีอิทธิพลต่อการเมืองระหว่างประเทศ
- ศูนย์รวมข้อมูลขนาดใหญ่ (Big Data) หมายถึง ส่วนสำคัญของแนวคิดสมองของโลกที่ทำหน้าที่รวบรวมข้อมูล วิเคราะห์ข้อมูล และความสามารถในการประมวลข้อมูลจำนวนมหาศาลเพื่อใช้ประกอบการตัดสินใจที่ส่งผลต่อความมั่นคงทางไซเบอร์ ความสามารถในการเข้าถึงข้อมูลจำนวนมากเพื่อใช้ในการพัฒนาองค์ความรู้ และการนำข้อมูลจำนวนมากมาสร้างนวัตกรรมเพื่อป้องกันภัยคุกคามทางไซเบอร์ได้อย่างแม่นยำมากยิ่งขึ้น ส่งเสริมให้ประเทศมหาอำนาจสามารถมีระบบป้องกันที่มีประสิทธิภาพมากกว่าประเทศอื่นๆ

- การไหลเวียนและการควบคุมข้อมูล (Information Flow & Control) หมายถึง ความสามารถในการควบคุมการไหลเวียนของข้อมูลต่างๆในการใช้งานระหว่างประเทศ ส่งผลให้ประเทศมหาอำนาจมีความสามารถในการเป็นผู้กำหนดทิศทางแนวทางของการสื่อสารในการใช้งานระหว่างประเทศ รวมถึงข้อมูลข่าวสารต่างๆด้วยเช่นกัน
- ระบบภูมิคุ้มกันทางไซเบอร์ (Cybersecurity as Immune System) หมายถึง การเปรียบเทียบความมั่นคงทางไซเบอร์เสมือนระบบภูมิคุ้มกัน ที่มีหน้าที่ป้องกันภัยคุกคามทางไซเบอร์ซึ่งเป็นส่วนสำคัญของการสร้างความมั่นคงทางไซเบอร์ในรัฐนั้นๆ โดยเฉพาะประเทศมหาอำนาจที่มีผลกระทบต่อประเทศต่างๆในการสร้างระบบภูมิคุ้มกันทางไซเบอร์ที่ทำให้รัฐอื่นมองว่าเป็นภัยคุกคาม
- การแข่งขันเพื่อการเป็นสมองของโลก (Competition for the Global Brain) หมายถึง การแข่งขันระหว่างประเทศมหาอำนาจที่ต้องการเป็นผู้ควบคุมสมองของโลก โดยเฉพาะประเทศสหรัฐอเมริกา จีน และรัสเซีย ที่มีความพยายามสร้างอิทธิพลทางไซเบอร์ในการเมืองระหว่างประเทศ ทั้งในแง่นโยบาย และการลงทุนเพื่อพัฒนาเทคโนโลยีไซเบอร์ให้มีความสามารถมากกว่าประเทศอื่นๆ รวมถึงความพยายามในการแทรกแซงและเข้าถึงข้อมูลต่างๆเพื่อนำมาปรับใช้ในเชิงกลยุทธ์ส่งผลกระทบต่อสมดุลแห่งอำนาจทั้งในด้านการเมือง เศรษฐกิจ และวิทยาศาสตร์ในระดับนานาชาติ

ในทัศนะของผู้วิจัย เล็งเห็นว่า หากแนวคิดสมองของโลก คือ การรวบรวมองค์ความรู้ของโลกเพื่อใช้ร่วมกันของมนุษยชาติ แล้วถ้าหากว่าองค์ความรู้หลักนั้น เกิดจากประเทศเพียงประเทศเดียวจะส่งผลกระทบอย่างไรต่อมนุษยชาติ ? นำมาสู่การประยุกต์แนวคิดสมองของโลกเข้าสู่องค์ความรู้ของการเมืองระหว่างประเทศของวิจัยฉบับนี้ ที่ผู้วิจัยต้องการนำมาปรับใช้กับความมั่นคงทางไซเบอร์ที่หากมีประเทศใดประเทศหนึ่ง สามารถวางโครงสร้างความมั่นคงทางไซเบอร์ในระดับโลก และทั้งโลกจำเป็นต้องใช้ทรัพยากรนั้นตามประเทศมหาอำนาจที่วางโครงสร้างไว้ ผลกระทบที่สามารถเกิดขึ้นจะส่งผลอย่างไรต่อการเมืองระหว่างประเทศในอนาคตอันใกล้

3) ความท้าทายในศตวรรษที่ 21

ความท้าทาย (Challenge) ในแง่ของการเมืองระหว่างประเทศ Finszter & Sabjanics (2018) ได้ให้นิยามถึงบริบทต่างๆที่เราสามารถใช้คำว่า ความท้าทาย ในการศึกษาการเมืองระหว่างประเทศ เช่น

1. ความท้าทายเชิงโครงสร้างด้านอำนาจระหว่างประเทศ ที่เกี่ยวข้องกับการสลับขั้วอำนาจของการเมือง รวมถึงการท้าทายจากกลุ่มตัวแสดงที่ไม่ใช่รัฐที่สร้างผลกระทบต่อความมั่นคงแห่งชาติ

2. ความท้าทายจากโลกาภิวัตน์ ที่ทำให้การเชื่อมโยงของระบบเศรษฐกิจของโลกและการเคลื่อนไหวของเงินทุน มีการพึ่งพาซึ่งกันและกันมากยิ่งขึ้น รวมถึงการเปลี่ยนแปลงของสภาพภูมิอากาศ และการเคลื่อนไหวของอาชญากรรมข้ามชาติ และกลุ่มก่อการร้ายต่างๆ ที่เกิดจากการเปิดกว้างของโลกใบนี้

3. ความท้าทายทางด้านความมั่นคงและการเมือง หมายถึง การเพิ่มขึ้นของอำนาจในประเทศอื่นๆ ที่สร้างความท้าทายให้กับประเทศมหาอำนาจ ส่งผลต่อความมั่นคงในเสถียรภาพของประเทศนั้นๆ

4. ความท้าทายของการเกิดขั้วอำนาจใหม่ ที่เกิดจากประเทศมหาอำนาจหลายฝ่ายที่ไม่มีอำนาจสูงสุด เริ่มรวมตัวกันให้การเมืองและความขัดแย้งระหว่างประเทศซับซ้อนมากยิ่งขึ้น

5. ความท้าทายจากตัวแสดงที่ไม่ใช่รัฐ อาทิเช่น องค์กรก่อการร้าย บริษัทข้ามชาติ ได้ทำให้การเมืองระหว่างประเทศมีความซับซ้อนมากยิ่งขึ้น

การศึกษาเพิ่มเติมของ Hamourtziadou (2019) ในการนิยามคำว่า ความท้าทาย ที่เกี่ยวข้องกับความมั่นคงกับความสัมพันธ์ระหว่างประเทศในศตวรรษที่ 21 ให้นิยามดังนี้

1. ความท้าทายทางด้านสิทธิและความมั่นคงขั้นพื้นฐาน เช่น ความมั่นคงทางด้านการมีชีวิตอยู่ในประเทศนั้นให้ปลอดภัยทางด้านการทหาร และได้รับสิทธิขั้นพื้นฐานของมนุษย์ที่ปลอดภัยจากความยากจน ความไม่เท่าเทียม รวมถึงสิทธิเสรีภาพในการแสดงออก
2. ความท้าทายทางด้านภัยคุกคามที่ไม่เกี่ยวข้องกับทางการทหาร เช่น การคุกคามที่ส่งผลต่อสุขภาพ ประชากร และวัฒนธรรม รวมถึงการคุกคามที่มาในรูปแบบ นโยบายทางการเมือง การเปลี่ยนแปลงพรมแดน การสนับสนุนกลุ่มบางกลุ่ม หรือการลดทอนคุณค่าของคนกลุ่มใดกลุ่มหนึ่ง
3. ความท้าทายความมั่นคงของมนุษย์ เช่น เศรษฐกิจ อาหาร สุขภาพ สิทธิส่วนบุคคล ค่านิยมของการเป็นพลเมือง สิทธิเสรีภาพทางการเมือง และสิ่งแวดล้อม

4. ความท้าทายทางด้านสิทธิเสรีภาพ เช่น การให้ความสำคัญกับความมั่นคงของมนุษย์แบบศูนย์กลาง ที่เน้นให้ความมั่นคงกับมนุษย์ก่อนสิ่งอื่นใด

การศึกษาเกี่ยวกับนิยามของ ความท้าทาย ของ Katz (2018) ในบริบทความท้าทายของประเทศมหาอำนาจในศตวรรษที่ 21 ได้ให้นิยามดังนี้

1. ความท้าทายด้านการเปลี่ยนแปลงขั้วอำนาจของโลก หมายถึง การเพิ่มขึ้นของอำนาจในประเทศมหาอำนาจอื่นๆ เช่น จีน และ รัสเซีย
2. ความท้าทายของระบบหลายขั้วอำนาจ หมายถึง ความพยายามของประเทศมหาอำนาจอื่นๆในการแย่งชิงอำนาจทางการเมืองระหว่างประเทศ ทำให้เกิดความไม่แน่นอนในสมดุลแห่งอำนาจระหว่างประเทศ (Balance of Power) รวมถึงการรวมตัวของประเทศมหาอำนาจต่างๆ เพื่อแย่งชิงอำนาจ เช่น การรวมตัวของประเทศจีนและรัสเซีย เพื่อคานอำนาจประเทศสหรัฐอเมริกา
3. ความท้าทายในศักยภาพของประเทศมหาอำนาจ หมายถึง นิยามของประเทศมหาอำนาจ คือ ประเทศที่ต้องมีศักยภาพด้านต่างๆและความสามารถในการป้องกันผลประโยชน์แห่งชาติของตนเอง ซึ่งประเทศมหาอำนาจบางประเทศอาจขาดความสามารถในด้านใดด้านหนึ่ง เช่น การมีประสิทธิภาพทางด้านการทหาร แต่ขาดความมั่นคงทางเศรษฐกิจ
4. ความท้าทายด้านความขัดแย้งจากภายในและภายนอกประเทศ หมายถึง การที่ประเทศมหาอำนาจต้องเผชิญความท้าทายจากภายในประเทศตนเอง เช่น ความขัดแย้งทางการเมือง ศาสนา เชื้อชาติ วัฒนธรรม ส่งผลให้การสนับสนุนนโยบายทางการเมืองระหว่างประเทศลดลง หรือ การแข่งขันของการเมืองระหว่างประเทศ ที่เป็นอุปสรรคต่อการสร้างสมดุลแห่งอำนาจระหว่างประเทศ เช่น การแข่งขันทางด้านอิทธิพลและการค้าระหว่างประเทศสหรัฐอเมริกาและจีน
5. ความท้าทายในการสร้างพันธมิตรและการสร้างระเบียบโลกใหม่ หมายถึง การปกครองโลกในการเมืองระหว่างประเทศ คือสิ่งที่เกิดขึ้นได้ยากในการปกครองโดยลำพัง ดังนั้นหลากหลายประเทศจึงเริ่มต้นในการสร้างพันธมิตรกับประเทศต่างๆ เพื่อสร้างอิทธิพลในการต่อรองต่างๆ แต่ในการสร้างพันธมิตรนั้น ก็มาพร้อมความซับซ้อนในกระบวนการด้วยเช่นกัน เช่น การสร้างพันธมิตรระหว่างประเทศจีนและรัสเซีย ที่มีความร่วมมือกันในบางเรื่อง แต่ก็มีความขัดแย้งทางด้านผลประโยชน์ในบางเรื่อง

จากการศึกษานิยามคำว่า ความท้าทาย ผู้วิจัยศึกษา ความท้าทาย ที่ใช้ในงานวิจัยชิ้นนี้ ในขอบเขตของสิ่งที่สร้างผลกระทบต่อความเป็นประเทศมหาอำนาจและอิทธิพลในสมดุลแห่งอำนาจระหว่างประเทศ รวมถึงผลกระทบที่เกิดจากภัยคุกคามรูปแบบใหม่ เช่น ความมั่นคงทางไซเบอร์ และความท้าทายที่เกิดจากการแข่งขันทางด้านเทคโนโลยีและเศรษฐกิจ เช่น การพัฒนาขีดความสามารถทางด้านไซเบอร์ ส่งผลไปยังความพยายามที่จะสร้างความมั่นคงทางไซเบอร์ของประเทศของตนเอง ทำให้ประเทศอื่นๆรู้สึกไม่ปลอดภัย ดังนั้น งานวิจัยชิ้นนี้ มุ่งเน้นในการศึกษาความท้าทายไปยัง 3 ปัจจัยหลัก ได้แก่

- ความมั่นคงทางไซเบอร์ (Cybersecurity)
- การแข่งขันทางเทคโนโลยี (Technology Competition)
- ความเป็นอธิปไตยทางไซเบอร์ (Cyber Sovereignty)

การวิเคราะห์ความท้าทายดังกล่าว จะทำให้เห็นถึงการวิเคราะห์ความท้าทายที่ได้รับผลกระทบจากโลกไซเบอร์ ที่ทำให้ประเทศมหาอำนาจได้มีการเปลี่ยนแปลงนโยบายและการแข่งขันทางเทคโนโลยีเพื่อการเป็นมหาอำนาจทางไซเบอร์ และความพยายามในการสร้างอำนาจอธิปไตยทางไซเบอร์ของตนเอง เพื่อป้องกันภัยคุกคามทางไซเบอร์ที่สามารถเกิดขึ้นได้ทุกเมื่อ

4) แนวคิดความมั่นคงทางไซเบอร์

นับตั้งแต่การให้ความสำคัญในเรื่องของ แนวความมั่นคงทางการทหารภายหลังยุคสงครามเย็น ที่เน้นการกำหนดนโยบายและมาตราการต่างๆในการตอบสนองต่อภัยคุกคามที่มาจากรัฐที่เป็นศัตรู โดยนักทฤษฎีด้านความมั่นคงได้ให้นิยามว่าเป็น “ความมั่นคงแบบดั้งเดิม” หรือ Traditional Security เมื่อเวลาผ่านไป กระบวนทัศน์ (paradigm) ที่เกี่ยวกับความมั่นคงได้แปรเปลี่ยนไปจากการเผชิญหน้ากันทางทหารและการเมือง กลายเป็นการแข่งขันกันทางด้านต่างๆไม่ว่าจะเป็นทางด้านเศรษฐกิจ ทรัพยากรทางธรรมชาติ และเทคโนโลยี ได้กลายมาเป็นปัจจัยที่ส่งผลต่อกระบวนทัศน์ในการวิเคราะห์ความมั่นคง และปัญหาความมั่นคงระหว่างประเทศที่เกิดขึ้น อาทิเช่น ปัญหาความมั่นคงทางด้านสิ่งแวดล้อม ปัญหาการอพยพของประชากรและผู้ลี้ภัย ปัญหาความมั่นคงของมนุษย์ ปัญหาความมั่นคงทางเศรษฐกิจ ปัญหาความขัดแย้งทางศาสนา ชาตินิยม และความขัดแย้งระหว่างประเทศ รวมถึงการก่อการร้ายข้ามชาติด้วยเช่นกัน ประเด็นปัญหาต่างๆที่กล่าวมาข้างต้น เป็นประเด็นที่ดำรงอยู่ในสังคมตลอดมา เพียงแต่ยังมิใช่ประเด็นหลัก ทำให้นักทฤษฎีความมั่นคงได้นิยามแนวคิดในการมองปัญหาความมั่นคงต่างๆที่มีมากกว่าการมองเพียงปัญหาทางด้านการทหารคือ “ความมั่นคงรูปแบบใหม่” หรือ Non-Traditional Security (สุรชาติ บำรุงสุข, 2545)

สุรชาติ บำรุงสุข (2545: 240 - 251) ได้ทำการจำแนกประเด็นปัญหาความมั่นคงที่รัฐต้องเผชิญในอนาคต ดังนี้

1. ความมั่นคงทางด้านสิ่งแวดล้อม (Environmental Security) หมายถึง ความมั่นคงที่เกิดจากปัญหาการพังทลายของระบบนิเวศ ที่เกิดจากการทำลายป่าทำให้เกิดการสูญเสียทางด้านการเกษตร การสร้างความเสียหายต่อพื้นที่การทำประมง การใช้น้ำมากเกินกว่าความจำเป็นและปัญหามลภาวะในน้ำ เป็นต้น
2. ความมั่นคงของมนุษย์ (Human Security) หมายถึง การศึกษาผลกระทบต่างๆที่กระทบต่อมนุษย์โดยตรงและหากผลกระทบต่างๆเกิดขึ้นเป็นวงกว้าง จะสามารถก่อให้เกิดผลกระทบต่อความมั่นคงของรัฐได้ด้วยเช่นกัน อาทิเช่น ปัญหาทางด้านอัตราการว่างงานที่อาจส่งผลต่อการเพิ่มขึ้นของประชากรที่มีความยากจนส่งผลให้อัตราการก่ออาชญากรรมเพิ่มขึ้น หรือปัญหาทางด้านสาธารณสุข อาทิเช่น การแพร่เชื้อของเชื้อ HIV ที่อาจมีส่วนในการทำให้ประชากรของบางประเทศลดลง เป็นต้น
3. ชาตินิยม วัฒนธรรม และสงครามเล็ก หมายถึง ความขัดแย้งของชนกลุ่มในประเทศเดียวกันที่มีความขัดแย้งทางความคิด ชาตินิยม และวัฒนธรรม ก่อให้เกิดสงครามขนาดเล็ก (small war)
4. อาชญากรรมข้ามชาติ หมายถึง ปัญหาจากการปฏิบัติการผิดกฎหมายข้ามประเทศ โดยมีส่วนเกิดจากการเพิ่มขึ้นของเศรษฐกิจแบบทุนนิยม ที่ทำให้องค์กรอาชญากรรมข้ามชาติสามารถหาช่องทางในการประกอบธุรกิจผิดกฎหมายมากยิ่งขึ้น รวมถึงมีการรวมกลุ่มขององค์กรอาชญากรรมข้ามชาติ ทำให้รัฐต้องเผชิญหน้ากับปัญหาเหล่านี้อย่างหลีกเลี่ยงไม่ได้

จากการจำแนกความมั่นคงรูปแบบใหม่ดังกล่าว สุรชาติ บำรุงสุข (2545) ยังได้อธิบายถึงปัญหาความมั่นคงในอนาคตที่อาจเกิดขึ้น เพราะปัญหาและความซับซ้อนที่เกิดจากการเปลี่ยนแปลงทางสังคม เราไม่สามารถที่จะอาศัยกระบวนการคิดและทัศนะแบบเก่าในการวิเคราะห์ปัญหาเพื่อกำหนดนโยบายความมั่นคงใหม่ได้อีกต่อไป และยังวิเคราะห์ไปยังมิติของการทำสงครามในอนาคต หากเปรียบเทียบกับสงครามเย็นที่เป็นการต่อสู้ทางอุดมการณ์ทางการเมืองแล้วนั้น สงครามในอนาคตจะเป็นสงครามที่เกิดจากการแย่งชิงทรัพยากร หรือความขัดแย้งทางเศรษฐกิจ ซึ่งสามารถส่งผลกระทบโดยตรงต่อการดำรงอยู่ของรัฐในสภาวะสงคราม รวมถึงความเหนือกว่าทางด้านเศรษฐกิจ จะทำให้รูปแบบของการมีนวัตกรรมทางเทคโนโลยีปูทางไปสู่สงครามรูปแบบใหม่ คือ “สงครามเทคโนโลยี” ที่มีระบบอาวุธสมัยใหม่ รวมถึง เทคโนโลยีสารสนเทศ ที่สามารถก่อให้เกิดสงครามเทคโนโลยีสารสนเทศ (Information Warfare) และการครอบครองเทคโนโลยีที่มีสมรรถนะทางทหารสูง เป็นภาพสะท้อนของรัฐที่มีอำนาจทางเศรษฐกิจ และปัญหาเหล่านี้ จะมีผลกระทบต่อความมั่นคงของรัฐในอนาคตด้วยเช่นกัน

ความมั่นคงทางไซเบอร์

จากมุมมองความมั่นคงที่กล่าวมา ทำให้เห็นถึงความสำคัญของการก่อสงครามเทคโนโลยีสารสนเทศ และความสำคัญทางเทคโนโลยีต่อความสามารถทางการทหาร ซึ่งปรากฏการณ์การโจมตีทางไซเบอร์ อาทิเช่น Stuxnet WannaCry และ NotPetya หรือ การแทรกซึมการเลือกตั้งของประเทศสหรัฐอเมริกาในสมัยของ Donald Trump ได้ทำให้การโจมตีทางไซเบอร์เป็นสิ่งที่รัฐต่างๆให้ความสำคัญมากยิ่งขึ้นและมีการพัฒนาทางด้านความมั่นคงทางไซเบอร์ให้มีการปฏิรูปให้ทันสมัย และใช้งานเพื่อกลยุทธ์ทางการเมืองและการทหารมากยิ่งขึ้น แสดงให้เห็นถึงการเพิ่มขึ้นของการใช้เทคโนโลยีดิจิทัลในการปรับใช้ในทางการเมืองในระดับประเทศและระดับระหว่างประเทศ รวมถึงนโยบายระหว่างประเทศที่มีส่วนเกี่ยวข้องกับความมั่นคงเพื่อตอบสนองความพยายามในการรุกรานของภัยร้ายรูปแบบใหม่ที่ได้เกิดขึ้น

ความมั่นคงทางไซเบอร์ ไม่ควรถูกวางกรอบแนวคิดให้อยู่ภายในทฤษฎีใดทฤษฎีหนึ่ง ความมั่นคงทางไซเบอร์เป็นสิ่งที่อยู่เหนือกว่าการวิเคราะห์ด้วยทฤษฎีที่ตายตัว การพิจารณาว่าความมั่นคงทางไซเบอร์คือความรู้แบบสหวิทยาการ หรือการนำหลากหลายศาสตร์มาพัฒนาองค์ความรู้นี้ การจะช่วยสร้างกรอบแนวคิด ข้อมูล และวิธีการใหม่ที่เหมาะสมกับพัฒนาการทางเทคโนโลยีที่จะพัฒนาอย่างรวดเร็วในอนาคต ไปพร้อมกับความซับซ้อนที่เพิ่มมากขึ้นของโลกไซเบอร์ต้องใช้องค์ความรู้ทางวิทยาศาสตร์ในการแก้ไขปัญหาและมองสะท้อนถึงปัญหา ซึ่งเป็นสิ่งที่สำคัญในการเข้าใจถึงการเมืองกับเทคโนโลยี และการเชื่อมต่อของขอบเขตเศรษฐกิจและสังคม สามารถกระทบกับภาคประชาสังคม เศรษฐกิจและรัฐได้ภายในอนาคต

Myriam Dunn Cavelty & Andreas Wenger (2020) ได้ทำการวิเคราะห์ถึง 5 ปัจจัยที่ใช้ในการอธิบายความมั่นคงทางไซเบอร์ในทางการเมือง และเสนอกรอบแนวคิดในการอธิบายความมั่นคงทางไซเบอร์ผ่านกรอบแนวคิดความมั่นคงระหว่างประเทศของ Buzan และ Hansen ที่ได้พัฒนากรอบแนวคิดความมั่นคงระหว่างประเทศขึ้นมาด้วยความสัมพันธ์ระหว่าง 5 ปัจจัย ได้แก่ การเมืองเชิงอำนาจ (great power politics) เทคโนโลยี (technology) เหตุการณ์สำคัญต่างๆ (key events) การถกเถียงทางวิชาการ (academic debates) และ สถาบัน (institutionalization) ซึ่งปัจจัยทั้งหมดที่กล่าวมามีความเชื่อมโยงกัน ดังนี้

เทคโนโลยี (Technology) คือ ปัจจัยทางด้านเทคโนโลยีถูกออกแบบโดยความคิดทางการเมือง และโครงสร้างอำนาจทางการเมือง รวมถึงความเป็นไปได้ของทิศทางการเมืองในอนาคตที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ รวมถึง เหตุการณ์สำคัญต่างๆ (key events) หมายถึงปรากฏการณ์ภายนอกที่ส่งผลกระทบต่อความมั่นคงไซเบอร์ในทางการเมือง

การเมือง (Politics) ในขอบเขตระหว่างประเทศ คือการเชื่อว่าอำนาจทางการเมืองรูปแบบใหม่ คือ อำนาจทางไซเบอร์ (Cyber power) และรูปแบบความร่วมมือและความขัดแย้งระหว่าง

ประเทศมหาอำนาจรูปแบบใหม่ และ การเมืองภายใน หมายถึง การแก้ไขปัญหาความขัดแย้งในบทบาทความรับผิดชอบของสถาบันทางการเมืองภายในประเทศ เศรษฐกิจ และสังคม ที่ส่งผลถึงความขัดแย้งทางการเมืองทั้งในประเทศและระหว่างประเทศ

วิทยาศาสตร์ (Science) มีสองปัจจัยเช่นกัน คือ การถกเถียงทางวิชาการ (Academic debates) หรือการแข่งขันทางด้านวิชาการ ขอบเขตการศึกษาทางด้านภววิทยาและญาณวิทยาที่ทำหน้าที่ศึกษาค้นคว้ารูปแบบความสัมพันธ์ระหว่างประเทศและการศึกษาความมั่นคงเพิ่มเติมเพื่อเติมเต็มองค์ความรู้ความมั่นคงทางไซเบอร์ และ ความเป็นสถาบัน (Institutionalization) คือ โอกาสและข้อจำกัดสำหรับนักวิจัยในการค้นคว้าหาความรู้เพิ่มเติม การหาแหล่งเงินทุนในการศึกษา และงานวิจัยต่างๆที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

Myriam Dunn Cavelty & Andreas Wenger (2019) ได้ศึกษาบทบาทของรัฐในความมั่นคงทางไซเบอร์ โดยวิเคราะห์ไปยัง 3 มิติ คือ 1. มิติเชิงทฤษฎี ศึกษาถึงบทบาทของรัฐและไซเบอร์ในเชิงทฤษฎี 2. มิติเชิงประจักษ์ ศึกษาถึงบทบาทของรัฐในการสร้างความมั่นคงทางไซเบอร์เพื่อความมั่นคงแห่งชาติ และรัฐมีบทบาทแบบอื่นด้วยหรือไม่ อย่างไร 3. มิติเชิงปทัสถาน ศึกษาถึงบทบาทแบบใดที่รัฐควรเป็นผู้ดำเนินการ นโยบายความมั่นคงทางไซเบอร์สามารถดำเนินการได้อย่างสำเร็จจะต้องมีความร่วมมือจากทั้ง 3 ภาคส่วนคือรัฐบาล เอกชน และ สังคมเข้าด้วยกัน ซึ่งภาครัฐ ภาคเศรษฐกิจ และภาคสังคม ล้วนเป็นตัวกำหนดทิศทางของนโยบายความมั่นคงทางไซเบอร์ และต้องปรับตัวให้รวดเร็วตามพัฒนาการของเทคโนโลยี เพราะว่าการเมืองของรัฐ มีการเลือกตั้งและแต่งตั้งรัฐบาลใหม่เสมอและการเปลี่ยนแปลงทางสังคม ทำให้ส่งผลกระทบต่อนโยบาย

ความมั่นคงทางไซเบอร์ในประเทศสหรัฐอเมริกา

ความท้าทายของประเทศมหาอำนาจและบทบาทการเป็นผู้นำระเบียบโลกของประเทศสหรัฐอเมริกากลายเป็นเรื่องที่มีความสำคัญมากยิ่งขึ้นในทศวรรษที่ 21 โดยเฉพาะเมื่อเกิดเหตุการณ์การโจมตีของกลุ่มก่อการร้าย Al Qaeda ในเหตุการณ์ 911 ทำให้ภายหลังการถูกก่อการร้าย โลกไซเบอร์ ได้กลายเป็นหนึ่งในเรื่องความสำคัญของความมั่นคงแห่งชาติของประเทศสหรัฐอเมริกา โดยมีการระบุความสำคัญต่อการปกป้องโลกไซเบอร์เป็นครั้งแรกในเอกสารยุทธศาสตร์แผนความมั่นคงระดับชาติ (National Security Strategy (NSS)) ในสมัยรัฐบาลของประธานาธิบดี Barrack Obama ใน ค.ศ. 2010

Peritz & Sechrist (2010) ได้ศึกษาความมั่นคงทางไซเบอร์ของสหรัฐอเมริกา โดยได้มีการวางโครงสร้างพื้นฐานเกี่ยวกับการจัดการข้อมูลที่เกี่ยวกับความมั่นคงและการสร้างความเข้าใจที่ตรงกันของหน่วยงานที่เกี่ยวข้องในการดำเนินการปกป้องความมั่นคงทางไซเบอร์ โดยชี้ให้เห็นถึง

ผลกระทบที่สามารถเกิดขึ้นได้กับการทำงานของระบบราชการและกระทรวงกลาโหมที่สามารถเกิดความเสี่ยงได้ในอนาคต

รูปแบบการโต้ตอบต่อภัยคุกคามของประเทศสหรัฐอเมริกา จะเกิดขึ้นก็ต่อเมื่อได้รับผลกระทบโดยมีผู้ใช้ความสามารถทางไซเบอร์ในการสร้างความเสียหายที่รุนแรงและส่งผลกระทบต่อประชากรของประเทศหรือระดับระหว่างประเทศ ซึ่งการโจมตีทางไซเบอร์ที่สร้างความเสียหายอย่างรุนแรงต่อประเทศสหรัฐอเมริกา เป็นการกระทำที่สามารถก่อให้เกิดสงครามทั้งในการทหารและทางการทูต การโต้ตอบในการทำสงครามของประเทศสหรัฐอเมริกาจึงสามารถกระทำได้โดยทันที มีความชอบธรรม และสามารถตอบโต้ได้ในทุกรูปแบบทางการทหาร ความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกาเป็นสิ่งที่ครอบคลุมไปยังความมั่นคงทางด้านเศรษฐกิจ การเมือง และสังคมของประเทศด้วยเช่นกัน เพราะปัจจัยแต่ละอย่างสามารถสร้างความเสียหายต่อประเทศได้เป็นจำนวนมากด้วยเช่นกัน

5) ไซเบอร์และการเมืองระหว่างประเทศ

ความมั่นคงทางไซเบอร์ได้มีความสำคัญเพิ่มมากขึ้นในโลกทางการเมือง โดยภัยความมั่นคงทางไซเบอร์ได้กลายเป็นส่วนหลักของภัยความมั่นคงทั้งในแง่ของความมั่นคงแห่งชาติ ความปลอดภัยของสาธารณะ และความท้าทายเชิงเศรษฐกิจที่หลากหลายรัฐต้องเผชิญในศตวรรษที่ 21 ในขณะที่โลกไซเบอร์ได้ถูกนิยามสำหรับการมีชีวิตที่ทันสมัย การเชื่อมต่ออย่างแพร่หลายและทั่วโลกระหว่างปัจเจกบุคคลและสังคมทั่วไปจากการใช้ประโยชน์จากโลกไซเบอร์ รวมถึงระดับประเทศด้วยเช่นกัน โดยรัฐแต่ละรัฐ ล้วนต้องการหาผลประโยชน์จากไซเบอร์ในการสร้างผลประโยชน์แห่งชาติ ความต้องการในการเพิ่มความสามารถทางไซเบอร์ ได้กลายเป็นประเด็นที่แต่ละรัฐให้ความสนใจ เพื่อผลประโยชน์แห่งชาติและการสร้างความได้เปรียบทางการทหารจากอำนาจการโจมตีทางไซเบอร์ด้วยเช่นกัน (Tsakanyan, 2017)

4.1 โครงสร้างลักษณะของโลกไซเบอร์

David Clark (2010) ได้ทำการแบ่งแยกโครงสร้างลักษณะของโลกไซเบอร์ออกเป็น 4 ลำดับชั้น ดังนี้

4.1.1 ลำดับชั้นทางกายภาพ (The Physical Layer) หมายถึง โครงสร้างพื้นฐานทางกายภาพของโลกไซเบอร์ ที่มีลักษณะเป็นวัตถุทางกายภาพ โลกไซเบอร์เกิดจากการเชื่อมต่อกันของอุปกรณ์คอมพิวเตอร์ ดังนั้นโครงสร้างพื้นฐานของโลกไซเบอร์จะประกอบด้วย คอมพิวเตอร์ และเซิร์ฟเวอร์ ซุปเปอร์คอมพิวเตอร์ และ โครงข่ายไฟฟ้า ระบบเซนเซอร์ และ ทรานส์ดิวเซอร์ ระบบอินเทอร์เน็ตและเครือข่ายเชื่อมต่ออื่นๆและช่องทางการสื่อสารต่างๆ ซึ่งช่องทางการสื่อสารอาจ

เกิดขึ้นผ่านสายไฟ หรือ สายไฟเบอร์ เครื่องส่งสัญญาณวิทยุ หรือ ผ่านทางการขนส่งทางกายภาพของระบบคอมพิวเตอร์ หรือ อุปกรณ์เก็บข้อมูลจากที่หนึ่งไปสู่อีกที่หนึ่ง ลำดับชั้นทางกายภาพนี้ เป็นสิ่งที่ง่ายที่สุดในการจับต้องได้ เนื่องจากเป็นสิ่งที่สามารถมองเห็นด้วยตาเปล่า และจากความเป็นสิ่งที่จับต้องได้ ทำให้สามารถระบุถึงตำแหน่งของวัตถุทางกายภาพเหล่านี้ได้ด้วยเช่นกัน

4.1.2 ลำดับชั้นทางตรรกะ (The Logical Layer) จากการที่โลกไซเบอร์เกิดจากลำดับชั้นทางกายภาพ ทำให้โลกไซเบอร์สามารถถูกนิยามได้ว่าเป็นสิ่งประดิษฐ์ที่ถูกสร้างขึ้นจากส่วนประกอบที่มีอยู่จริง จับต้องได้ทางกายภาพ มิใช่สิ่งที่สมมุติขึ้นมาโดยปราศจากแหล่งที่มาหรือพื้นฐานต่างๆ แต่ทว่า ประสิทธิภาพความแข็งแกร่งและขีดความสามารถของธรรมชาติของโลกไซเบอร์นั้น มาจากกระบวนการพื้นฐานตรรกะทางความคิด หรือความเป็นเหตุและผล มากกว่าพื้นฐานทางกายภาพ กล่าวคือ ระบบอินเทอร์เน็ต ถูกออกแบบมาเพื่อเป็นการขยายขีดความสามารถในการรับส่งข้อมูลต่างๆ แต่สิ่งที่ทำให้ระบบอินเทอร์เน็ตสามารถเพิ่มขีดความสามารถของตนเองเพิ่มขึ้นได้นั้น เกิดจากการมีลำดับชั้นทางตรรกะความคิด ในการวิเคราะห์โลกไซเบอร์ให้มีความซับซ้อนมากยิ่งขึ้นเพื่อรองรับการใช้งานและบริการต่างๆที่จะเกิดขึ้นในอนาคต

การออกแบบอินเทอร์เน็ตที่นำมาสู่โลกไซเบอร์นั้น ถูกสร้างขึ้นจากองค์ประกอบที่มีลำดับชั้นในการประกอบสร้างขึ้นเพื่อตอบสนองการใช้งานที่ซับซ้อนในอนาคต การออกแบบระบบอินเทอร์เน็ตขั้นพื้นฐาน ประกอบด้วย การสร้างสิ่งแวดล้อมของโปรแกรมขึ้นมา การสร้างระบบกลไกในการเคลื่อนย้ายข้อมูล และการกำหนดพื้นฐานของรูปแบบของลักษณะข้อมูลต่างๆ ลำดับถัดมาคือการสร้างแอพพลิเคชั่นและแพลตฟอร์มต่างๆ อาทิเช่น แอพพลิเคชั่นประมวลคำต่างๆ ระบบฐานข้อมูล และเว็บไซต์ ซึ่งจากการรวบรวมขั้นตอนที่กล่าวมาข้างต้น ทำให้เกิดความซับซ้อนของระบบอินเทอร์เน็ตเกิดขึ้น ยกตัวอย่างเช่น การรวบรวมฐานข้อมูลของเว็บ ทำให้เห็นถึงเนื้อหาและข้อมูลต่างๆของแต่ละเว็บ ยกตัวอย่างเช่น เฟสบุ๊ค คือตัวอย่างของแพลตฟอร์มที่เกิดขึ้นจากการพัฒนาแอพพลิเคชั่นบนเว็บของระบบอินเทอร์เน็ต ดังนั้น ธรรมชาติของโลกไซเบอร์ คือสิ่งที่มีนวัตกรรมพัฒนาอย่างก้าวกระโดดในด้านความสามารถและบริการ ที่มาจากกระบวนการประกอบสร้างของตรรกะความคิดสร้างสรรค์ของผู้ใช้งานที่ทำงานบนโครงสร้างพื้นฐานทางกายภาพของโลกไซเบอร์

ดังนั้น ลำดับชั้นทางตรรกะของโลกไซเบอร์ คือลำดับชั้นที่เกี่ยวกับแพลตฟอร์มที่เกิดจากการประกอบสร้างของตรรกะความคิด และแพลตฟอร์มนั้นๆสามารถถูกพัฒนาเพื่อสร้างนวัตกรรมใหม่ได้ในอนาคต ทำให้โลกไซเบอร์มีโครงข่ายในการเชื่อมต่อจากการสร้างแพลตฟอร์มต่างๆทับซ้อนกันเรื่อยๆผ่านนวัตกรรมที่ถูกสร้างทับซ้อนกันตามการประกอบสร้างของตรรกะแนวคิดใหม่อย่างต่อเนื่อง และถึงแม้ว่าแพลตฟอร์มใหม่ที่ถูกสร้างขึ้นจะมีความแตกต่างทางด้านข้อมูลหรือรูปแบบการทำงานบางอย่าง แต่แพลตฟอร์มนั้นล้วนมีส่วนเกี่ยวข้องในการแบ่งปันและเชื่อมต่อข้อมูลต่อแพลตฟอร์มที่เป็นโครงสร้างพื้นฐานของแพลตฟอร์มใหม่ ทำให้เกิดการเชื่อมต่อซึ่งกันและกันอยู่เสมอ

4.1.3 ลำดับชั้นข้อมูล (The Information Layer) แนวคิดโลกไซเบอร์ที่มีนิยามเกี่ยวกับการเชื่อมต่อของผู้คนผ่านการใช้เทคโนโลยีเป็นสื่อกลางนั้น สิ่งที่เป็นใจความสำคัญคือข้อมูลที่ถูกสร้างขึ้น ได้รับ จัดเก็บ และกระบวนการต่างๆที่ดำเนินการกับข้อมูล ซึ่งข้อมูลนั้นมีหลากหลายรูปแบบ ไม่ว่าจะเป็นเพลงหรือคลิปวิดีโอที่ถูกแชร์ การเก็บข้อมูลทางธุรกิจหรือทางภาครัฐต่างๆ และข้อมูลต่างๆที่เกิดขึ้นบนเว็บไซต์

ลักษณะทางข้อมูลของโลกไซเบอร์ได้เปลี่ยนแปลงไปอย่างรวดเร็ว โดยมีจุดเริ่มต้นจากการที่คอมพิวเตอร์ที่ไร้การเชื่อมต่อได้เกิดการทำงานกับชุดข้อมูล จนในเวลาต่อมา คอมพิวเตอร์ได้เกิดการเชื่อมต่อซึ่งกันและกันผ่านเครือข่ายอินเทอร์เน็ต การจัดเก็บข้อมูลมีจุดเริ่มต้นจากการเก็บข้อมูลผ่านการจดบันทึก จัดเก็บ และนำมาใช้เมื่อต้องการ ไม่ว่าจะเป็นในรูปแบบสมุดหนังสือ การจัดเก็บรูปภาพต่างๆผ่านรูปภาพกระดาษ รวมถึงบันทึกข้อมูลจำนวนมากของบริษัทต่างๆในคลังจัดเก็บข้อมูล จนกระทั่งเมื่อมีการนำเทคโนโลยีมาใช้ ข้อมูลต่างๆได้ถูกนำมาจัดเก็บในรูปแบบของฐานข้อมูลในโลกไซเบอร์

4.1.4 ลำดับชั้นผู้ใช้งาน (The User Layer) ผู้ใช้งานในโลกไซเบอร์คือผู้ที่รับข้อมูลและผลกระทบจากกระบวนการทำงานของไซเบอร์ และ เป็นผู้กระทำและออกแบบการใช้งานไซเบอร์ พฤติกรรมผู้ใช้งานในโลกไซเบอร์อาจมีความแตกต่างกันในแต่ละพื้นที่ ดังนั้นการให้ความสำคัญกับการวิเคราะห์ผู้ใช้งานในโลกไซเบอร์จึงเป็นเรื่องที่สำคัญ

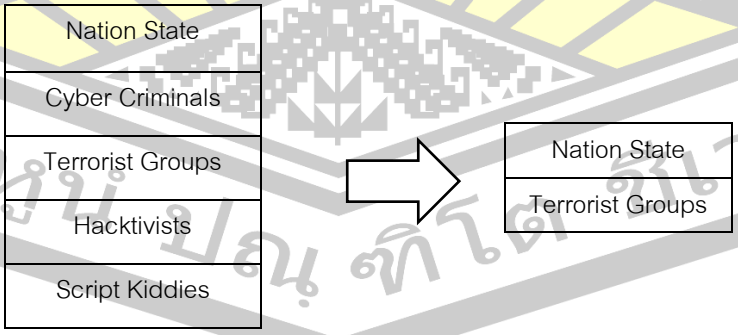
การพิจารณาลำดับชั้นผู้ใช้งานทางไซเบอร์จากธรรมชาติของโลกไซเบอร์นั้น ตำแหน่งที่อยู่อาศัยที่แตกต่างกันถือเป็นปัจจัยที่สำคัญในการวิเคราะห์ เพราะเป็นการชี้ให้เห็นถึงประสิทธิภาพและอำนาจทางไซเบอร์ของประเทศนั้นๆ ยกตัวอย่าง การเป็นผู้นำทางด้านการปฏิวัติทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่มีการพัฒนานวัตกรรมและการทดลองอย่างต่อเนื่อง ความเป็นผู้นำทางด้านเทคโนโลยีสามารถทำให้ประเทศที่มีความสามารถทางเทคโนโลยีสร้างผลประโยชน์จากการพัฒนานวัตกรรมเหนือประเทศอื่นๆได้ โดยเฉพาะการใช้นวัตกรรมทางด้านการทหาร ที่มีความต้องการในการพัฒนาแนวคิดนวัตกรรมอย่างรวดเร็วและการแต่งตั้งหน่วยงานรับผิดชอบอย่างเป็นทางการเพื่อตอบสนองความต้องการได้อย่างรวดเร็ว

ตัวอย่างความสามารถจากการเป็นผู้นำทางด้านไซเบอร์ของประเทศสหรัฐอเมริกา คือ โครงการ 100$ laptop (OLPC) ที่เป็นการบริจาคแล็บท็อปให้กับเด็กและเยาวชนในประเทศที่กำลังพัฒนาทั่วโลก ซึ่งหากโครงการนี้สำเร็จ จะทำให้เกิดกำลังพลทางการทหารที่มีอายุในช่วงวัยผู้ใหญ่ที่มีความคุ้นเคยในการใช้งานจากเครื่องมือต่างๆของโลกไซเบอร์ซึ่งอาจเป็นสิ่งที่ดีต่อการพัฒนานวัตกรรมให้กับคนทั้งโลก แต่ก็อาจเป็นผลร้ายจากการที่ประชาชนใช้อาวุธทางไซเบอร์ในการเผชิญหน้ากับรัฐด้วยเช่นกัน

การทำความเข้าใจถึงความมั่นคงทางไซเบอร์ของรัฐ จำเป็นที่จะต้องศึกษาลำดับชั้นของโลกไซเบอร์ให้ครบทุกลำดับ การโจมตีและผลกระทบที่เกิดขึ้น สามารถมาจากลำดับชั้นใดก็ได้ไม่ว่าจะเป็นจากการทำลายลำดับชั้นทางกายภาพ หรือ การปรับแต่งแนวคิดและตรรกะการคิดของเหตุและผลในการกระทำของลำดับชั้นตรรกะ หรือ การบิดเบือนข้อมูล ไปตลอดจนการใช้ไซเบอร์ในทางที่ผิดจากผู้ใช้งาน ดังนั้นความมั่นคงทางไซเบอร์จึงต้องเกิดจากการวิเคราะห์ลำดับชั้นของโลกไซเบอร์ทุกลำดับชั้น

4.2 ตัวแสดงในโลกไซเบอร์

ความก้าวหน้าของเทคโนโลยีโลกไซเบอร์ได้กลายเป็นปัญหาความขัดแย้งที่สำคัญ จากผู้ใช้งาน หรือ หน่วยงานที่ใช้งานเพื่อผลประโยชน์ส่วนตัว และเพื่อผลประโยชน์แห่งชาติ การให้ความสำคัญต่อการศึกษาบทบาทของตัวแสดงทางไซเบอร์ คือสิ่งที่จะทำให้เราเข้าใจถึงเป้าหมาย และแรงจูงใจในการใช้งานของแต่ละตัวแสดงเพื่อจุดประสงค์ใดจุดประสงค์หนึ่ง ซึ่งในบทบาทของภาครัฐเป็นตัวแสดงที่สามารถควบคุมข้อมูลต่างๆ การกำหนดขอบเขตการใช้งานไซเบอร์ในรัฐที่ตนเอง การกำหนดอิสรภาพทางข้อมูลที่เผยแพร่ทางอินเทอร์เน็ต การสร้างสมดุลระหว่างความเป็นส่วนตัวและความมั่งคงปลอดภัยในโลกออนไลน์ การใช้อินเทอร์เน็ตเพื่อการบริหารระดับภาครัฐและความเป็นกลางในการใช้อินเทอร์เน็ต รวมถึงการปกป้องความมั่นคงทรัพยากรทางด้านการเงิน ทำให้รัฐกลายเป็นตัวแสดงหลักที่สำคัญของโลกไซเบอร์ ในการดำเนินการต่างๆ ไม่ว่าจะเป็นการโจมตีทางไซเบอร์ หรือการเสริมสร้างความมั่นคงทางไซเบอร์ของประเทศ อีกทั้งรัฐยังสามารถเป็นผู้สนับสนุนกลุ่มแฮ็กเกอร์ ในการทำการโจมตีได้ด้วยเช่นกัน โดยลำดับความสำคัญของตัวแสดงในโลกไซเบอร์สามารถเห็นได้ดังภาพประกอบ 5 ซึ่งเรียงลำดับความสำคัญตัวแสดงในโลกไซเบอร์และประสิทธิภาพในโลกไซเบอร์จากตัวแสดงที่มีประสิทธิภาพมากที่สุดในระดับบน สู่ตัวแสดงที่มีประสิทธิภาพน้อยที่สุดในระดับล่าง



ภาพประกอบ 5 ลำดับชั้นอำนาจทางไซเบอร์ของตัวแสดงในโลกไซเบอร์

ที่มา: Johan Sigholm (2016)

บทบาทของตัวแสดงทางไซเบอร์ ส่งผลต่อภัยคุกคามที่สามารถเกิดขึ้นได้จากการเชื่อมต่อบนโลกไซเบอร์ ซึ่งระดับภัยคุกคามที่สามารถเกิดขึ้นได้จากตัวแสดงในโลกไซเบอร์ เรียงลำดับตามตารางข้างต้น กลุ่มตัวแสดงที่สร้างความเสียหายได้มากที่สุดไปหาน้อยที่สุด คือ กลุ่มตัวแสดงจากรัฐ (Nation State) องค์กรอาชญากรรมทางไซเบอร์ (Cyber Criminals) กลุ่มก่อการร้าย (Terrorist Groups) กลุ่มแฮ็กทิวิสต์ (Hactivists) และกลุ่มแฮ็กเกอร์มือสมัครเล่น (Script Kiddies) จากการศึกษาของ Sailio et al., (2020) เกี่ยวกับการวิเคราะห์ตัวแสดงที่สามารถสร้างผลกระทบทางไซเบอร์ที่เสียหายมากที่สุด ซึ่งได้ให้ความสำคัญไปยังตัวแสดงเหล่านี้ คือ กลุ่มตัวแสดงจากรัฐ (Nation State) องค์กรอาชญากรรมทางไซเบอร์ (Cyber Criminals) กลุ่มก่อการร้าย (Terrorist Groups) และ คู่แข่งจากภาคเอกชน (Competitors) เนื่องจากการโจมตีทางไซเบอร์ที่สามารถสร้างความเสียหายและเป็นภัยความมั่นคงทางไซเบอร์แห่งชาติ เกิดจากผลกระทบ 3 รูปแบบ (Sailio et al., 2020) คือ

- การจารกรรมทางอุตสาหกรรม เช่น การขโมยเทคโนโลยีเพื่อสร้างข้อได้เปรียบต่างๆ
- การโจมตีโครงสร้างพื้นฐาน เช่น การโจมตีท่อส่งน้ำมัน ระบบพลังงาน
- การใช้ไซเบอร์เพื่อสร้างความไม่มั่นคง เช่น ปฏิบัติการข้อมูลข่าวสาร (Information Operations หรือ IO) ในการแทรกแซงกระบวนการทางการเมืองของประเทศเป้าหมาย

ดังนั้น งานวิจัยฉบับนี้ จึงมุ่งเน้นไปยังการวิเคราะห์กลุ่มตัวแสดงจากรัฐ (Nation State) และกลุ่มก่อการร้าย (Terrorist Groups) เพราะสามารถสร้างความเสียหายต่อความมั่นคงไซเบอร์แห่งชาติได้โดยตรง อีกทั้งการมีทรัพยากรที่เพียงพอในการสร้างความเสียหายในระดับชาติ โดยในงานวิจัยฉบับนี้ วิเคราะห์ไปยังประเทศสหรัฐอเมริกา เป็นกลุ่มตัวแสดงจากรัฐ (Nation State) รวมถึงการโจมตีที่เกิดขึ้นที่สร้างผลกระทบต่อประเทศสหรัฐอเมริกาที่เกิดจากประเทศอื่นๆด้วยเช่นกัน ส่วนกลุ่มก่อการร้าย (Terrorist Groups) จะเป็นการวิเคราะห์ไปยังการโจมตีที่เกิดจากตัวแสดงที่ไม่ใช่รัฐที่สามารถสร้างผลกระทบโดยตรงต่อความมั่นคงไซเบอร์ของประเทศสหรัฐอเมริกา

ความเป็นอนาธิปไตยของไซเบอร์และการเมืองระหว่างประเทศ

Kuusisto and Kuusisto (2015) ได้ทำการอธิบายปฏิสัมพันธ์ระหว่างโลกไซเบอร์ (Cyber world) และ โลกทางกายภาพ (Physical world) คือ ปฏิสัมพันธ์แบบที่หนึ่ง หมายถึง โลกไซเบอร์มีการพึ่งพาอาศัยกับโลกทางกายภาพในรูปแบบของโครงสร้างพื้นฐานทางกายภาพ และ ปฏิสัมพันธ์แบบที่สอง หมายถึง โลกไซเบอร์เป็นการสร้างปฏิกิริยาระหว่างจุดเชื่อมต่อเครือข่ายอินเทอร์เน็ตเพื่อ

เข้าสู่โลกอินเทอร์เน็ต ดังนั้น ผลกระทบในโลกไซเบอร์จะส่งผลต่อโลกทางกายภาพเสมอ เพราะมีการพึ่งพาซึ่งกันและกัน

โลกไซเบอร์ (Cyberspace) มีความแตกต่างจากโลก (earth) ที่เราอยู่อาศัยคือ การอยู่อาศัยของประชากรบนโลกใบนี้ ล้วนอาศัยอยู่ในเขตแดนของรัฐใดรัฐหนึ่ง ซึ่งมีการแบ่งเขตแดนระหว่างประเทศอย่างชัดเจน โดย Johan Sigholm (2016) ได้กล่าวว่า ในโลกไซเบอร์นั้น เป็นโลกที่ผู้คนสามารถเข้าถึงได้ทั่วโลกอย่างไร้พรมแดนด้วยระบบการเชื่อมต่อเครือข่ายอินเทอร์เน็ตของคอมพิวเตอร์ โทรศัพท์มือถือสมาร์ทโฟน หรือ อุปกรณ์ต่างๆที่สามารถเชื่อมต่อเครือข่ายได้ เมื่อการใช้อินเทอร์เน็ตกลายเป็นเรื่องปกติในช่วงท้าย ค.ศ. 1990 แล้วนั้น การใช้การกระทำบนโลกไซเบอร์ (Cyberactions) เพื่อสร้างผลประโยชน์บนโลก (earth) และสร้างความขัดแย้งได้เริ่มต้นขึ้นด้วยตัวแสดงที่ไม่ใช่รัฐ

การศึกษาของ Michiel Foulon & Gustav Meibauer (2024) เกี่ยวกับความสัมพันธ์ระหว่างโลกไซเบอร์และความสัมพันธ์ระหว่างประเทศ ได้อธิบายถึงมุมมองในการวิเคราะห์โลกไซเบอร์ ซึ่งได้เปรียบเทียบมุมมองการวิเคราะห์โลกไซเบอร์ในแง่ของ มุมมองแบบเก่า คือ โลกไซเบอร์เปรียบเสมือนพื้นที่ หรือ โดเมน ใหม่ที่รัฐใช้ในการปฏิบัติการ ไม่ว่าจะเป็นการโจมตี หรือการจารกรรมทางข้อมูล และได้เสนอมุมมองแบบใหม่ คือ โลกไซเบอร์เปรียบเสมือน “ตัวแสดงที่ปรับเปลี่ยนโครงสร้างที่ไม่ได้ปรับเปลี่ยนโดยตรง” หรือ Structural Modifier หมายถึง ตัวแสดงที่ส่งผลต่อพฤติกรรมของรัฐทุกรัฐภายใต้ระบบความสัมพันธ์ระหว่างประเทศ ซึ่งไซเบอร์ได้ถูกเปรียบเทียบในแง่ของการพัฒนาประสิทธิภาพของไซเบอร์ ที่ไม่ได้เปลี่ยนแปลงความสัมพันธ์ระหว่างประเทศโดยตรง แต่เป็นการปรับเปลี่ยนพฤติกรรมของรัฐอื่นๆจากการพัฒนาที่เกิดขึ้น หากเปรียบเทียบแนวคิดนี้กับเหตุการณ์ที่เคยเกิดขึ้น ยกตัวอย่างเช่น การสะสมอาวุธนิวเคลียร์ ที่ไม่ได้เปลี่ยนแปลงโครงสร้างของความเป็นอนาธิปไตยในความสัมพันธ์ระหว่างประเทศ แต่ได้เปลี่ยนแปลงพฤติกรรมของรัฐต่างๆ จนนำไปสู่สงครามและความขัดแย้งทางการเมือง โดย Michiel Foulon & Gustav Meibauer ได้เสนอปัจจัยทั้งหมด 4 ปัจจัย ที่ส่งผลกระทบต่อโลกไซเบอร์ในฐานะการเป็นตัวแสดงที่ปรับเปลี่ยนโครงสร้าง ดังนี้

1. การส่งผลกระทบต่อขอบเขตการปกป้อง (Deterrence) หมายถึง การที่โลกไซเบอร์ได้สร้างความซับซ้อนในการปกป้องทางการทหารมากขึ้น
2. การส่งผลกระทบต่อการเลือกเครื่องมือทางนโยบายต่างประเทศ (Foreign Policy Tool Choice) หมายถึง การเข้ามามีบทบาทของไซเบอร์ในแง่การดำเนินนโยบายระหว่างประเทศไม่ว่าจะเป็นทางการทูต ทางการทหาร และเศรษฐกิจ และเพิ่มความซับซ้อนในการดำเนินนโยบายต่างๆด้วยเช่นกัน

3. การส่งผลกระทบต่อความไม่แน่นอนในการตัดสินใจ (Uncertainty) หมายถึง การสะสมข้อมูลที่ได้จากหน่วยข่าวกรองมากเกินไป จนทำให้การตัดสินใจเป็นไปได้ยาก และการตัดสินใจดังกล่าว อาจเกิดข้อผิดพลาดได้เช่นกัน
4. การส่งผลกระทบต่อความสัมพันธ์ระหว่างภาครัฐและตัวแสดงที่ไม่ใช่รัฐ (State and Non-State Actor Interaction) หมายถึง การที่โลกไซเบอร์ได้เพิ่มบทบาทของตัวแสดงที่ไม่ใช่รัฐ เช่น บริษัทเอกชน กลุ่มก่อการร้าย และแฮ็กเกอร์ ได้มีบทบาทมากยิ่งขึ้นในเหตุการณ์ที่เกี่ยวข้องกับความสัมพันธ์ระหว่างประเทศ

การนำแนวคิดตัวแสดงที่ปรับเปลี่ยนโครงสร้างที่ไม่ได้ปรับเปลี่ยนโดยตรง หรือ Structural Modifier มาวิเคราะห์ไซเบอร์ จะทำให้การวิเคราะห์มีความแม่นยำและอธิบายบริบทของไซเบอร์ในการเมืองระหว่างประเทศได้ดีมากยิ่งขึ้น เนื่องจากไซเบอร์ไม่ได้เป็นตัวแปรในการเปลี่ยนแปลงโครงสร้างการเมืองระหว่างประเทศ ที่มีความเป็นอนาธิปไตยเฉกเช่นเดียวกันกับโลกไซเบอร์ แต่เป็นการวิเคราะห์ให้เห็นถึงบริบทของโลกไซเบอร์ที่สร้างผลกระทบต่อความมั่นคงของรัฐอื่นๆ ดังนั้น งานวิจัยชิ้นนี้จึงหยิบยกแนวคิดของ Michiel Foulon & Gustav Meibauer มาอธิบายในการตอบความมุ่งหมายข้อแรก ในการวิเคราะห์ความเป็นอนาธิปไตยในโลกไซเบอร์ที่ท้าทายอำนาจของประเทศสหรัฐอเมริกา (Foulon & Meibauer, 2024)

5. สงครามไซเบอร์ (Cyberwarfare)

5.1 Cyber warfare คืออะไร

นิยามของ Cyber warfare ยังเป็นข้อถกเถียงกันอยู่ ณ ปัจจุบัน โดยการทำความเข้าใจนิยามคำว่า Cyber Warfare นั้น เป็นการต้องทำความเข้าใจถึงคำประกอบทั้งสองคำ คือ คำว่า Cyber และ Warfare โดยผู้วิจัยได้ทำการอธิบายนิยามคำว่า Cyber ในหัวข้อข้างต้น โดยในส่วนนี้จะอธิบายเฉพาะคำว่า Warfare และให้นิยามเพื่อใช้ในการทำความเข้าใจและวิเคราะห์เนื้อหาในวิทยานิพนธ์

Jason Andress & Steve Winterfield (2013) ได้ให้นิยามคำว่า Warfare โดยอ้างถึงองค์ความรู้ทางประวัติศาสตร์ที่เกี่ยวข้องกับทฤษฎีทางการทหาร โดยแบ่งออกเป็นสองทฤษฎีทางการทหาร โดยเริ่มต้นจากเอกสารการวางแผนการรบในช่วงสงครามนโปเลียนใน ค.ศ. 1837 ชื่อว่า “On War” และ เอกสารเกี่ยวกับการสร้างสงครามในช่วงทศวรรษที่ 16 ชื่อว่า “The Art of War” ซึ่งจากนิยามของทฤษฎีทางการทหารทั้งสองทฤษฎีที่กล่าวมา สามารถปรับใช้กับสงครามไซเบอร์ได้ด้วยเหตุผลสองประการ ประการแรก การที่ไม่มีนิยามที่แท้จริงในการอธิบายการสงคราม ทำให้การใช้นิยามหรือความหมายของสงครามนั้น สามารถใช้ได้ตามจุดประสงค์และมุมมองของผู้ใช้งาน ไม่ว่าจะเป็นรัฐบาล สถาบันทางการเงิน ผู้ใช้งานอินเทอร์เน็ต องค์กรระหว่างประเทศ องค์กรภาคเอกชนที่มีจุดประสงค์เฉพาะ และ นักกฎหมายที่ให้ความหมายที่แตกต่างออกไป จากแนวคิดทางประวัติศาสตร์

ที่เป็นการอิงถึงหลักภูมิศาสตร์ในการทำสงคราม ซึ่งไม่สามารถนำมาปรับใช้กับสงครามไซเบอร์ได้และประการสุดท้าย หากต้องการที่จะศึกษาประเด็นที่เกี่ยวกับสงคราม ควรใช้การศึกษาในมุมมองทางการทหารในการวิเคราะห์สงครามไซเบอร์ เนื่องจากเป็นสมภูมิรบที่มีความเกี่ยวเนื่องกันกับรูปแบบการรบในสมภูมิต่างๆด้วยเช่นกัน

5.2 กลยุทธ์และวิธีการโจมตีทางไซเบอร์เชิงรุกและเชิงรับ

5.2.1 กลยุทธ์และวิธีการโจมตีทางไซเบอร์เชิงรุก (Offensive tactics and procedures)

การแสวงหาผลประโยชน์จากการใช้เครือข่ายคอมพิวเตอร์ (Computer Network Exploitation : CNE) คือจุดเริ่มต้นของการใช้สงครามไซเบอร์ในรูปแบบของการทหาร โดยมีนิยาม คือ การจัดตั้งปฏิบัติการและการรวบรวมความสามารถทางไซเบอร์เพื่อใช้เครือข่ายคอมพิวเตอร์ในการรวบรวมข้อมูลสำคัญจากเป้าหมาย อาทิเช่น การรวบรวมข้อมูลสาธารณะ (Open Source Intelligence : OSINT) การแสวงหาผลประโยชน์ (Reconnaissance) การสอดแนมแบบเจาะจง (Surveillance) การดักฟัง (Voice Surveillance) การสอดแนมข้อมูล (Data Surveillance) และการสอดแนมแบบวงกว้าง (Large Scale Surveillance Programs) ซึ่งการสอดแนมต่างๆสามารถนำไปใช้เป็นข้อมูลในการวิเคราะห์พฤติกรรมที่อาจก่อให้เกิดสงครามได้

นอกจากนั้น การโจมตีทางเครือข่ายคอมพิวเตอร์ (Computer Network Attack: CNA) ยังเป็นอีกหนึ่งรูปแบบที่สามารถใช้ในการสร้างความเสียหายจากการใช้ไซเบอร์ด้วยเช่นกัน โดยมีนิยามว่า เป็นการกระทำที่ใช้เครือข่ายคอมพิวเตอร์ในการสร้างผลกระทบ ความเสียหาย หรือ ทำลายข้อมูลของคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์อื่นๆ หรือเครือข่ายของคอมพิวเตอร์นั้นๆ ซึ่งการโจมตีต่างๆนั้นมีความแตกต่างทางด้านความเสียหายจากตัวแสดงที่ทำการโจมตี ซึ่งรัฐเป็นตัวแสดงหลักที่สามารถสร้างความเสียหายได้มากกว่าตัวแสดงที่ไม่ใช่รัฐเนื่องจากมีทรัพยากรที่มากกว่า ซึ่งสงครามไซเบอร์สามารถส่งผลกระทบต่อปัจจัยต่างๆที่มีความสำคัญในการทำสงคราม อาทิเช่น การทำสงครามด้านกายภาพ (Physical warfare) คือ การที่การทำสงครามทางกายภาพได้รับผลกระทบจากการโจมตีทางไซเบอร์ ทำให้กระบวนการดำเนินงานต่างเกิดขัดข้องและนำไปสู่ความล้มเหลวในการเตรียมการทำสงคราม การทำสงครามด้านอิเล็กทรอนิกส์ (Electronic warfare) คือ การโจมตีเข้าสู่อุปกรณ์อิเล็กทรอนิกส์ต่างๆที่ใช้เป็นส่วนประกอบในการทำสงคราม และการทำสงครามด้านตรรกะ (Logical warfare) คือ การโจมตีโดยใช้อาวุธทางไซเบอร์ต่างๆต่อระบบเครือข่ายและระบบโครงสร้างพื้นฐานของศัตรู

5.2.2 กลยุทธ์และวิธีการโจมตีทางไซเบอร์เชิงรับ Defensive tactics and procedures

สงครามไซเบอร์สามารถโจมตีได้ทุกเวลา การป้องกันทางเครือข่ายคอมพิวเตอร์ (Computer Network Defense: CND) จึงเป็นเรื่องที่จำเป็นในการนำมาวิเคราะห์ด้วยเช่นกัน โดยกระทรวงกลาโหมสหรัฐ ได้ให้นิยามการป้องกันทางเครือข่ายคอมพิวเตอร์ ว่า “เป็นการกระทำที่ใช้เครือข่ายคอมพิวเตอร์ในการปกป้อง ตรวจสอบ วิเคราะห์ ตรวจจับ และโต้ตอบกิจกรรมทางคอมพิวเตอร์ที่ไม่ได้รับอนุญาตให้เข้าถึงระบบข้อมูลและเครือข่ายคอมพิวเตอร์ของกระทรวงกลาโหมสหรัฐ”

การป้องกันทางเครือข่ายคอมพิวเตอร์ เป็นการป้องกันข้อมูลที่มีความละเอียดอ่อน อาทิเช่น รายชื่อ ที่อยู่ หมายเลขประกันสังคม ประวัติการรักษาพยาบาล ประวัติทางการเงิน และข้อมูลที่เกี่ยวข้องต่างๆ และในแง่ทางการทหารและการเมือง การป้องกันเครือข่ายคอมพิวเตอร์ ยังครอบคลุมไปถึงการป้องกันข้อมูลลับต่างๆ อาทิเช่น แผนปฏิบัติการทางการทหาร ยุทธศาสตร์การทำสงคราม แผนการเคลื่อนไหวของพลทหาร ข้อมูลเฉพาะของอุปกรณ์และอาวุธต่างๆ ข้อมูลของหน่วยข่าวกรอง และข้อมูลอื่นๆที่ส่งผลกระทบโดยตรงต่อทางการทหารและรัฐบาล ซึ่งหากข้อมูลต่างๆถูกเข้าควบคุมหรือรั่วไหล สามารถส่งผลต่อดุลอำนาจทางการเมืองได้ด้วยเช่นกัน ทำให้การสร้างความมั่นคงทางไซเบอร์จึงเป็นเรื่องที่สำคัญต่อการเมืองระหว่างประเทศ (Andress & Winterfeld, 2013)

5.3 โครงสร้างพื้นฐานของสงครามไซเบอร์ (Infrastructures of Cyber Warfare)

Robert S. Owen (2007) ได้อธิบายถึงโครงสร้างพื้นฐานในการทำสงครามไซเบอร์ว่า เป้าหมายหลักของการทำสงครามไซเบอร์ คือการโจมตีไปยัง โครงสร้างพื้นฐานสำคัญของประเทศ (Critical infrastructure) ไม่ว่าจะเป็นความมั่นคงทางกายภาพของประเทศ ความมั่นคงทางเศรษฐกิจ และความมั่นคงทางสาธารณะสุข หรือ ความปลอดภัย ซึ่งประกอบไปด้วยอุตสาหกรรมที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญของประเทศ อาทิเช่น พลังงาน อาหาร การขนส่ง การธนาคาร การเชื่อมต่อ รัฐบาล และ โลกไซเบอร์

ผลกระทบที่เกิดขึ้นกับความมั่นคงของโครงสร้างพื้นฐานสำคัญของประเทศ ที่เกิดจากสงครามไซเบอร์ ไม่จำเป็นต้องเป็นการโจมตีโครงสร้างพื้นฐานสำคัญของประเทศโดยตรง แต่เป็นการได้รับผลกระทบจากการถูกโจมตี โครงสร้างที่ไม่ใช่โครงสร้างพื้นฐานสำคัญของประเทศ (Non-critical infrastructure) โดยการโจมตีสามารถเกิดจากตัวแสดงที่ไม่ใช่รัฐที่ทำการโจมตีเพื่อสร้างผลกระทบต่อเศรษฐกิจ หรือ สิ่งจำเป็นที่ใช้ในการดำรงชีวิตของประชากร เช่น การทำให้การเชื่อมต่ออินเทอร์เน็ตเกิดการติดขัดโดยการอัดแน่นของจำนวนการเชื่อมต่ออินเทอร์เน็ต หรือ การโจมตีที่กำหนดเป้าหมายไปยังโครงสร้างพื้นฐานที่สามารถกระทบไปยังโครงสร้างพื้นฐานสำคัญของประเทศ หรือ การโจมตี

โครงสร้างพื้นฐานทางกายภาพที่สร้างผลกระทบไปยังระบบเศรษฐกิจ หรือ การโจมตีเพื่อลดคุณภาพของชีวิตประชากร ซึ่งถึงแม้การโจมตีเหล่านี้จะไม่สามารถส่งผลกระทบอย่างรุนแรงและเป็นโดยกว้างได้ แต่การโจมตีเหล่านี้สามารถปิดกั้นการเข้าถึงเทคโนโลยีของประชากรที่สามารถส่งผลกระทบต่อการขาดการเชื่อมต่อต่างๆ

ผลกระทบทางกายภาพจากการถูกโจมตีโครงสร้างอินเทอร์เน็ตจากสงครามไซเบอร์อาจดูราวกับว่าไม่สามารถสร้างผลกระทบอย่างรุนแรงได้ แต่การโจมตีเหล่านี้สามารถเป็น “อาวุธในการสร้างความเสียหายชั่วคราว” โดยที่ “ความเสียหายชั่วคราว” นี้ สามารถกลายเป็นผลลัพธ์ที่ได้รับผลกระทบทที่สร้างผลกระทบต่อระบบเศรษฐกิจโดยตีมูลค่าประมาณระดับพันล้านดอลลาร์ได้ด้วยเช่นกัน ซึ่งการสร้างความเสียหายชั่วคราว ประกอบด้วย (Owen, 2007)

1. ความพยายามในการเข้าถึงระบบ (Probe) หมายถึง ความพยายามในการเข้าถึงระบบต่างๆ
2. การสแกน (Scan) หมายถึง การพยายาม probe หลายๆครั้งโดยการใช้เครื่องมืออัตโนมัติ
3. การเจาะเข้าบัญชีผู้ใช้ (Account compromise) หมายถึง การใช้บัญชีคอมพิวเตอร์โดยไม่ได้รับอนุญาต
4. การเจาะเข้าบัญชีผู้ดูแลระบบ (Root compromise) หมายถึง การเข้าถึงบัญชีผู้ดูแลระบบ
5. การรวบรวมข้อมูล (Packet sniffing) หมายถึง การรวบรวมข้อมูลต่างๆที่มีการเคลื่อนย้ายข้อมูลผ่านเครือข่าย
6. การโจมตีแบบ Denial of service หมายถึง การทำให้ระบบไม่สามารถเข้าถึงได้โดยตัดขาดการเข้าถึงระบบ
7. การใช้ไวรัสในการโจมตี (Malicious programs and malware) หมายถึง โปรแกรมที่ถูกซ่อน หรือ โปรแกรมที่ทำงานมากเกินหน้าที่ที่ควรจะเป็นและส่งผลทำให้เกิดผลที่คาดคิดต่อระบบ

จากการสำรวจใน ค.ศ. 2005 จาก 700 บริษัทที่ทำการสำรวจโดยสถาบันความมั่นคงทางคอมพิวเตอร์สหรัฐอเมริกา สำนักงานสืบสวนของสหรัฐอเมริกา (FBI) ได้ค้นพบว่า การโจมตีโดยใช้ไวรัสสามารถทำให้เกิดการสูญเสียทางการเงินโดยมีมูลค่าประมาณ 42.8 ล้านดอลลาร์สหรัฐ (Gordon et al., 2005) และใน ค.ศ. 2003 มีรายงานมูลค่าการเสียหายจากการถูกโจมตีโดย Malicious programs ประมาณ 13,000 ล้านดอลลาร์สหรัฐ ซึ่งหากเปรียบเทียบจากการก่อการร้าย 9/11 ที่มีมูลค่า 50,000 ล้านดอลลาร์สหรัฐ อาจจะเปรียบเทียบมูลค่าความเสียหายระหว่างกันไม่ได้

แต่ถึงกระนั้น การโจมตีแบบ Malicious programs คือการโจมตีเพียงปีเดียว ซึ่งสามารถเกิดการโจมตีแบบนี้ได้ทุกปีและอาจสามารถสร้างมูลค่าความเสียหายทางเศรษฐกิจได้อย่างมหาศาลและต่อเนื่องทุกปี เมื่อเปรียบเทียบกับการก่อการร้าย 9/11 ที่เกิดขึ้นเพียงครั้งเดียว ทำให้การโจมตีเพื่อสร้างความเสียหายชั่วคราวนี้ อาจเกิดขึ้นได้อย่างสม่ำเสมอจนกระทบภาคเศรษฐกิจอย่างหลีกเลี่ยงไม่ได้

5.4 เครื่องมือและเทคนิคทางไซเบอร์ (Cyber tools and techniques)

5.4.1 อาวุธเชิงตรรกะ (Logical Weapons)

อาวุธเชิงตรรกะ (Logical weapons) หมายถึง เครื่องมือหรือโปรแกรมซอร์ฟเวร์ที่ใช้ในการสอดแนมเครือข่ายและระบบการทำงานของศัตรู และรวมถึงการโจมตีหรือการสร้างผลประโยชน์จากการโจมตีโดยใช้โปรแกรมซอร์ฟแวร์ โดยสามารถแบ่งประเภทได้ดังนี้

1) เครื่องมือแสวงหาผลประโยชน์ (Reconnaissance Tools) หมายถึง เครื่องมือที่ใช้ในการรวบรวมข้อมูลของฝ่ายศัตรูจากเครือข่ายและระบบการทำงาน อาทิเช่น การเก็บรวบรวมข้อมูลจากเว็บไซต์สาธารณะ การค้นหาเซิร์ฟเวอร์ของระบบโดเมน การรวบรวมข้อมูล Metadata จากเอกสารที่เข้าถึงได้ การค้นหาข้อมูลเฉพาะทางผ่านการใช้ระบบการค้นหาบนเว็บไซต์ต่างๆ เช่น เว็บไซต์ต่างๆ เว็บไซต์ค้นหาข้อมูลต่างๆ การแฮ็กเว็บ google เว็บไซต์ค้นหาเฉพาะทางเช่น WHOIS Maltego และ Metadata

2) เครื่องมือสแกน (Scanning Tools) หมายถึง เครื่องมือที่ใช้หาข้อมูลที่เจาะลึกลงไปในรายละเอียดที่อยู่ในข้อมูลที่ค้นหาได้ทั่วไป โดยเป็นการค้นหาที่ละเอียดและเฉพาะเจาะจงต่อข้อมูลเป้าหมายที่เราต้องการค้นหา ประกอบไปด้วยเครื่องมือ อาทิเช่น Nmap Nessus และ OpenVAS

3) เครื่องมือการเข้าถึง (Access and Escalation Tools) หมายถึง เครื่องมือการแฮ็กต่างๆที่ใช้ในการเข้าถึงและเจาะระบบการทำงาน โดยมีจุดประสงค์ในการเข้าถึงระบบต่างๆและการเข้าควบคุมการใช้งานเมื่อสามารถแฮ็กเข้าระบบนั้นๆได้ ประกอบไปด้วยเครื่องมือ อาทิเช่น เครื่องมือการเดารหัสผ่านต่างๆ Metaspolit และ CANVAS

4) เครื่องมือสร้างการรั่วไหลของข้อมูล (Exfiltration Tools) หมายถึง เครื่องมือที่สร้างการรั่วไหลของข้อมูลต่างๆโดยใช้เครือข่ายอินเทอร์เน็ต หรือ การใช้การขนย้ายข้อมูลทางกายภาพ อาทิเช่น การเข้าถึงข้อมูลและสร้างการรั่วไหลข้อมูลโดยทางกายภาพ การนำข้อมูลเข้ารหัสลับ หรือ การอำพรางข้อมูล การสร้างช่องทางในการรั่วไหลของข้อมูล และ Out-of-band (OOB) methods

5) เครื่องมือสร้างความมั่นคงในการเข้าถึงข้อมูล (Sustainment Tools) หมายถึง เมื่อเราสามารถเข้าถึงข้อมูลต่างๆของเป้าหมายตามที่เราต้องการได้แล้วนั้น การใช้เครื่องมือเพื่อสร้างความมั่นคงในการสามารถเข้าถึงระบบต่างๆที่ถูกเราแฮ็กได้ในอนาคตถือเป็นเรื่องที่สำคัญ เพราะถึงแม้ว่า

เราจะสามารถเข้าถึงข้อมูลได้ ณ ช่วงเวลาหนึ่ง แต่ไม่หมายความว่าเราจะสามารถเข้าถึงข้อมูลนั้นๆได้ตลอดเวลา โดยมีเครื่องมืออาทิเช่น การสร้างบัญชีที่มีอำนาจเข้าถึงระบบไว้ในระบบนั้นๆ การเข้าข้อมูลหลังบ้าน และการสร้างระบบดักฟัง

6) เครื่องมือการโจมตี (Assault Tools) หมายถึง เครื่องมือที่ใช้ในการโจมตีอุปกรณ์ต่างๆ เป็นเครื่องมือที่โจมตีเพื่อสร้างการเปลี่ยนแปลงในการทำงานของระบบและปรับแต่งการใช้งานของระบบต่างๆ ดังการสร้าง botnets เพื่อใช้ในการสร้างการโจมตีแบบ Denial of Service จากการแฮ็กเข้าสู่ระบบของอุปกรณ์นั้นๆ ยกตัวอย่างเครื่องมือการโจมตี อาทิเช่น ซอร์ฟแวร์หรือฮาร์ดแวร์ต่างๆที่ถูกออกแบบมาเพื่อโจมตี และ การเปลี่ยนแปลงการทำงานของเป้าหมายที่ถูกโจมตี

7. เครื่องมือสร้างความสับสน (Obfuscation Tools) หมายถึง เครื่องมือที่ใช้ในการสร้างความสับสนของเป้าหมาย โดยเป็นการสร้างความสับสนในความต้องการของเป้าหมายที่ต้องการค้นหาร่องรอย หรือ ตำแหน่งที่ตั้งของสิ่งต่างๆ ไม่ว่าจะเป็น สถานที่ แหล่งจัดเก็บข้อมูล และไฟล์ต่างๆ

5.4.2 อาวุธเชิงกายภาพ (Physical Weapons)

อาวุธเชิงกายภาพ (Physical Weapons) ในสงครามไซเบอร์นั้น เป็นปัจจัยสำคัญที่ต้องทำความเข้าใจด้วยเช่นกันเพราะนอกจากเราจะทำความเข้าใจอาวุธเชิงตรรกะที่มีความเกี่ยวโยงในโลกไซเบอร์แล้วนั้น การโจมตีในโลกเชิงกายภาพก็ยังสามารถส่งผลกระทบต่อโลกไซเบอร์ได้ด้วยเช่นกัน

หากเรามองภาพของการทำงานที่ทับซ้อนกันของโลกไซเบอร์ระหว่างลำดับชั้นทางกายภาพ (Physical layer) และลำดับชั้นทางตรรกะ (Logical layer) จะทำให้เห็นถึงการเชื่อมต่อที่ทับซ้อนกันอย่างเห็นได้ชัด โดยระบบทางตรรกะ อาทิเช่น ซอร์ฟแวร์ และ แอพพลิเคชั่นต่างๆ ล้วนทำงานบนพื้นฐานทางระบบทางกายภาพและระบบโครงสร้างพื้นฐานในการทำงาน หากเกิดการเปลี่ยนแปลงไม่ว่าจะเป็นในลำดับชั้นทางกายภาพ หรือลำดับชั้นทางตรรกะ ย่อมส่งผลกระทบต่อกันและกันไม่มากก็น้อย

ในสงครามแบบดั้งเดิม (Conventional warfare) ต่างๆที่เกิดขึ้น โครงสร้างพื้นฐานและระบบขนส่งรูปแบบต่างๆคือสิ่งที่สำคัญ เพราะหากมีการแทรกซึมเข้าถึงของกองทัพศัตรูในการโจมตีโครงสร้างพื้นฐานหรือระบบขนส่ง จะทำให้เกิดผลกระทบต่างๆเกิดขึ้นต่อความสามารถในการทำสงครามทางกายภาพของกองทัพทันที และผลกระทบเหล่านั้น สามารถเกิดจากการสร้างผลกระทบทางกายภาพต่อโลกไซเบอร์ลำดับชั้นทางกายภาพอีกด้วย เช่นการสร้างการระเบิดต่างๆ การตัดสายเคเบิล การทำให้ระบบขนส่งติดขัด

ทฤษฎีอำนาจทางการทหาร (Theories of Military Power)

เมื่อพูดถึงอำนาจทางการทหาร ความแตกต่างของพื้นที่ที่ใช้ในการทำสงคราม เช่น พื้นดิน (land), ทะเล (Sea), อากาศ (Air) และ อวกาศ (Space) นำมาสู่ความแตกต่างทางด้านกลยุทธ์ในการทำสงคราม ทำให้เกิดนักคิดที่มีความเชี่ยวชาญเฉพาะด้านในแต่ละพื้นที่ อาทิเช่น หากพูดถึงการทำสงครามบนพื้นดิน นักคิดที่มักจะเอ่ยถึงคือ Sun Tzu, Antoine-Henri Jomini และ Carl von Clausewitz, ส่วนการทำสงครามทางทะเล ก็จะมีการเอ่ยถึง Alfred Thayer Mahan และ Julian S. Corbett, และเมื่อนึกถึงการทำสงครามทางอากาศ นักคิดผู้เชี่ยวชาญที่มักถูกเอ่ยถึงคือ Giulio Douhet, Billy Mitchell, John Boyd และ John Warden และมีความพยายามในการเขียนทฤษฎีอำนาจในอวกาศด้วยเช่นกัน อาทิเช่น David E. Lupton ในชิ้นงาน On Space Warfare ใน ค.ศ. 1998 แต่ภายหลังได้มีการจำกัดพื้นที่ทางอวกาศให้กลายเป็นพื้นที่ที่ใช้อำนวยความสะดวกให้มนุษย์มากกว่าเป็นพื้นที่สงคราม (Elbaum, 2008) ในขณะเดียวกัน อำนาจทางไซเบอร์ (Cyber Power) ที่ใช้ในทางการทหาร ไม่ควรถูกละเลยหรือแบ่งแยกจากการทำสงครามแบบดั้งเดิม Elbaum, J.M. ได้ให้เหตุผลว่าพื้นที่ทางไซเบอร์นั้น เปรียบเสมือนพื้นที่ที่การป้องกันที่ดีที่สุด อาจหมายถึงการโจมตีศัตรูก่อน, การทำสงครามไซเบอร์ อาจเป็นการทำสงครามเพื่อปกป้องเขตแดนของประเทศ หรือแม้กระทั่งแรงจูงใจทางการเมือง (Political motives) ที่ใช้ในพื้นที่ทางไซเบอร์ อาจสร้างความไม่เป็นมิตรต่อประเทศต่างๆ อำนาจทางการทหารของแต่ละพื้นที่มีความแตกต่างกัน ดังนี้

อำนาจบนพื้นดิน (Power on Land)

การทำสงครามบนพื้นดินเป็นการทำสงครามที่เก่าแก่ที่สุด และเป็นการทำสงครามที่คนส่วนมากเข้าใจมากที่สุด อย่างไรก็ตาม การทำสงครามบนพื้นดินนั้น มีความสัมพันธ์กับอำนาจไซเบอร์น้อยที่สุดเพราะลักษณะภูมิประเทศและสภาพอากาศไม่มีส่วนสำคัญในการโจมตีทางไซเบอร์ ดังนั้นการโจมตีแบบดั้งเดิม (kinetic war) ที่เป็นการโจมตีโดยใช้กำลังพลทหาร, อาวุธยุทโธปกรณ์, รถถัง และอาวุธภาคพื้นดิน จะมีประสิทธิภาพมากกว่าการโจมตีด้วยไซเบอร์ อย่างไรก็ตาม สิ่งที่เกี่ยวข้องกับอำนาจทางไซเบอร์ที่มีความสัมพันธ์กับอำนาจบนพื้นดิน คือ การใช้ผลกระทบจากการโจมตีจุดศูนย์กลางของประเทศนั้นๆ เช่น การโจมตีระบบการเงิน, เศรษฐกิจ และ ข้อมูล ที่เป็นสถานที่หรือมีลักษณะเป็นกายภาพ เช่น ธนาคาร หรือ โรงงานไฟฟ้า เป็นต้น แนวคิดการโจมตีเข้าสู่จุดศูนย์กลางนี้ มาจากนักคิดชาวตะวันตก ผู้เป็นนักปรัชญาทางการทหารชื่อว่า Carl von Clausewitz ผู้ซึ่งเคยเป็นทหารชาวปรัสเซียและนักคิดเชิงยุทธวิธีที่ใช้ชีวิตในช่วงทศวรรษที่ 18 และ 19 และเป็นผู้ที่นำแนวคิดของขงจื้อมาประยุกต์และปรับใช้ให้เข้ากับประสบการณ์ของตนเอง มุมมองของเขาสะท้อนให้เห็นถึงแนวคิดของชาวตะวันตกเกี่ยวกับการทำสงคราม และการความก้าวหนเทางเทคโนโลยี ทำให้งานของเขากลายเป็นงานที่ปรับใช้ได้จริง Clausewitz ได้กล่าวถึงการได้มาซึ่งอำนาจทางบกจากการใช้ยุทธศาสตร์ โดยการนิยามสงครามทาง

บกว่า “เป็นการใช้กำลังเพื่อทำให้ศัตรูทำตามสิ่งที่เราต้องการ” และ “การทำตามคำสั่งที่เราเป็นผู้กำหนด” โดยเป็นการทำให้ศัตรูปราศจากการขัดขืน ต่อสู้ หรือปลอดอาวุธ “เพื่อทำให้ศัตรูไม่สามารถกลับมาโจมตีเราได้อีก”

แนวคิดในการโจมตีแบบเต็มกำลังและความสามารถที่มีเพื่อทำลายเป้าหมาย เป็นแนวคิดที่นำมาปรับใช้ในแนวคิดการโจมตีเข้าสู่จุดศูนย์กลาง (Center of Gravity) ซึ่ง Clausewitz ได้เขียนถึง 5 ส่วนประกอบของยุทธศาสตร์ทางบกที่นำแนวคิดของจื้อมาปรับใช้ด้วยเช่นกัน ประกอบด้วย ศีลธรรม, กายภาพ, หลักคณิตศาสตร์, ลักษณะภูมิศาสตร์ และ หลักสถิติ โดยคำอธิบายในแต่ละส่วนประกอบ มีรายละเอียดดังนี้

1. หลักศีลธรรม (Moral) คือ ส่วนประกอบที่นำแนวคิดของของจื้อมาปรับใช้ เนื่องจากการมีหลักศีลธรรมในการทำสงคราม คือสิ่งที่หลีกเลี่ยงไม่ได้เพื่อสร้างความชอบธรรมในการทำสงครามนั้นๆ
2. กายภาพ (Physical) คือ ส่วนประกอบที่เกี่ยวข้องกับขนาดของกองกำลังทหาร, คลังอาวุธที่มีและอื่นๆ ซึ่งส่วนประกอบนี้เป็นสิ่งที่แตกต่างจากแนวคิดของของจื้อ ในรายละเอียดการให้นิยามคำว่า กายภาพ คือ แนวคิดของของจื้อมองว่า กองทัพในรูปแบบกายภาพ คือ กองทัพที่ประกอบด้วยกำลังพลจำนวน 1,000 นาย หรือการนับจำนวนทหารในปริมาณที่มาก แต่แนวคิดของ Clausewitz มองว่า จำนวนทหารไม่จำเป็นต้องมีขนาดใหญ่ในการปฏิบัติการทางการทหารต่างๆ แต่เป็นการแบ่งจำนวนทหารแยกออกเป็นหลากหลายหน่วย เพื่อปฏิบัติการในเป้าหมายที่แตกต่างกัน ในสนามรบที่แตกต่างกันด้วยเช่นกัน
3. หลักคณิตศาตร์ (Mathematical) คือ ส่วนประกอบที่เกี่ยวข้องกับการคำนวณเส้นทางที่ใช้ในการปฏิบัติการ, จุดบรรจบกันหรือจุดแยกทางกันของการเคลื่อนกำลังพลทางการทหารโดยใช้หลักการคำนวณ
4. ลักษณะภูมิศาสตร์ (Geographical) คือ ส่วนประกอบที่เกี่ยวข้องกับผลกระทบที่เกิดจากสภาพแวดล้อม, ภูมิประเทศ และภูมิอากาศ ถึงแม้ว่าปัจจุบัน เทคโนโลยีจะทำให้อุปสรรคทางด้านภูมิประเทศและภูมิอากาศไม่กลายเป็นปัญหาต่อไปในการทำสงครามทางบก แต่ภูมิศาสตร์ก็ยังคงเป็นหนึ่งในส่วนประกอบที่ Clausewitz ให้ความสำคัญ ณ ช่วงเวลานั้น
5. หลักสถิติ (Statistical) คือ ส่วนประกอบที่ใช้ในการคำนวณเพื่อการสนับสนุนกำลังพลทางการทหาร และการรักษาความมั่นคงของกองกำลังทางการทหาร

เมื่อนำส่วนประกอบที่กล่าวมาข้างต้น มาเปรียบเทียบกับอำนาจทางไซเบอร์ ส่วนประกอบแรกคือหลักศีลธรรม ที่ต้องใช้ในการโจมตีทางไซเบอร์ด้วยเช่นกัน เพราะการโจมตีเข้าสู่สถาบันทางการเงินของศัตรู ที่ศัตรูใช้ในการดำเนินการต่างๆภายในประเทศ อาจเป็นการโจมตีที่ไม่ทำให้เกิดผู้คนล้มตายจากการโจมตี แต่นั่นก็อาจเป็นสิ่งที่เราไม่ควรทำ ส่วนประกอบต่อมา คือ หลักกายภาพ กองกำลังไซ

เบอร์ คือกองกำลังที่มีจำนวนที่น้อยกว่ากองกำลังทางการทหารปกติอยู่มาก เนื่องจากต้องใช้ความสามารถขั้นสูงในการโจมตีและความสามารถในการใช้อุปกรณ์ต่างๆที่ใช้ในการโจมตี ส่วนประกอบถัดมาคือ หลักคณิตศาสตร์ ซึ่งส่วนประกอบนี้เป็นส่วนที่สำคัญในการปฏิบัติการทางไซเบอร์ เพราะการรู้ว่าเราสามารถสร้างผลกระทบอะไรต่อศัตรูได้บ้าง คือสิ่งที่สำคัญในการโจมตีทางไซเบอร์ และยังเป็นกุญแจสำคัญในการทำการโจมตีแบบเข้าสู่จุดศูนย์กลางแรงโน้มถ่วงด้วยเช่นกัน ส่วนประกอบที่สี่ คือ หลักภูมิศาสตร์ ที่มีความสำคัญน้อยที่สุดของโลกไซเบอร์ เพราะโลกไซเบอร์เชื่อมต่อกันโดยใช้เครือข่ายอินเทอร์เน็ต และส่วนประกอบสุดท้าย คือ หลักสถิติ ซึ่งมีผลกระทบน้อยกับโลกไซเบอร์ เพราะการโจมตีทางไซเบอร์ไม่จำเป็นต้องการการสนับสนุนกำลังพลที่มากมาย หากเพียงต้องการแค่พื้นที่ปลอดภัยขนาดเล็ก และคอมพิวเตอร์ที่มีประสิทธิภาพในการโจมตีเพื่อการใช้งานของกองกำลังไซเบอร์ที่มีประสิทธิภาพ

อำนาจทางทะเล (Power at Sea)

Alfred Thayer Mahan นักคิดผู้ยิ่งใหญ่ในการวางแผนการรบทางทะเล ซึ่งบางคนเปรียบเทียบ Mahan ว่าเป็นนักคิดที่ทรงพลังในการรบทางทะเล เปรียบเสมือน Clausewitz ที่เป็นนักคิดที่ยิ่งใหญ่ในการรบบนพื้นดิน ได้กล่าวไว้ว่า “การพาณิชย์ในทะเล ที่เกี่ยวข้องกับความมั่งคั่งและความแข็งแกร่งของประเทศต่างๆ คือการแสดงให้เห็นอย่างชัดเจนถึงประสิทธิภาพ และอำนาจของประเทศนั้นๆ ดังนั้น หากสงครามเกิดขึ้น การวิเคราะห์ว่าประเทศใดคือประเทศที่มีความแข็งแกร่ง สามารถวิเคราะห์ได้จากประเทศที่มีอำนาจการควบคุมทางทะเล” (Elbaum , 2008)

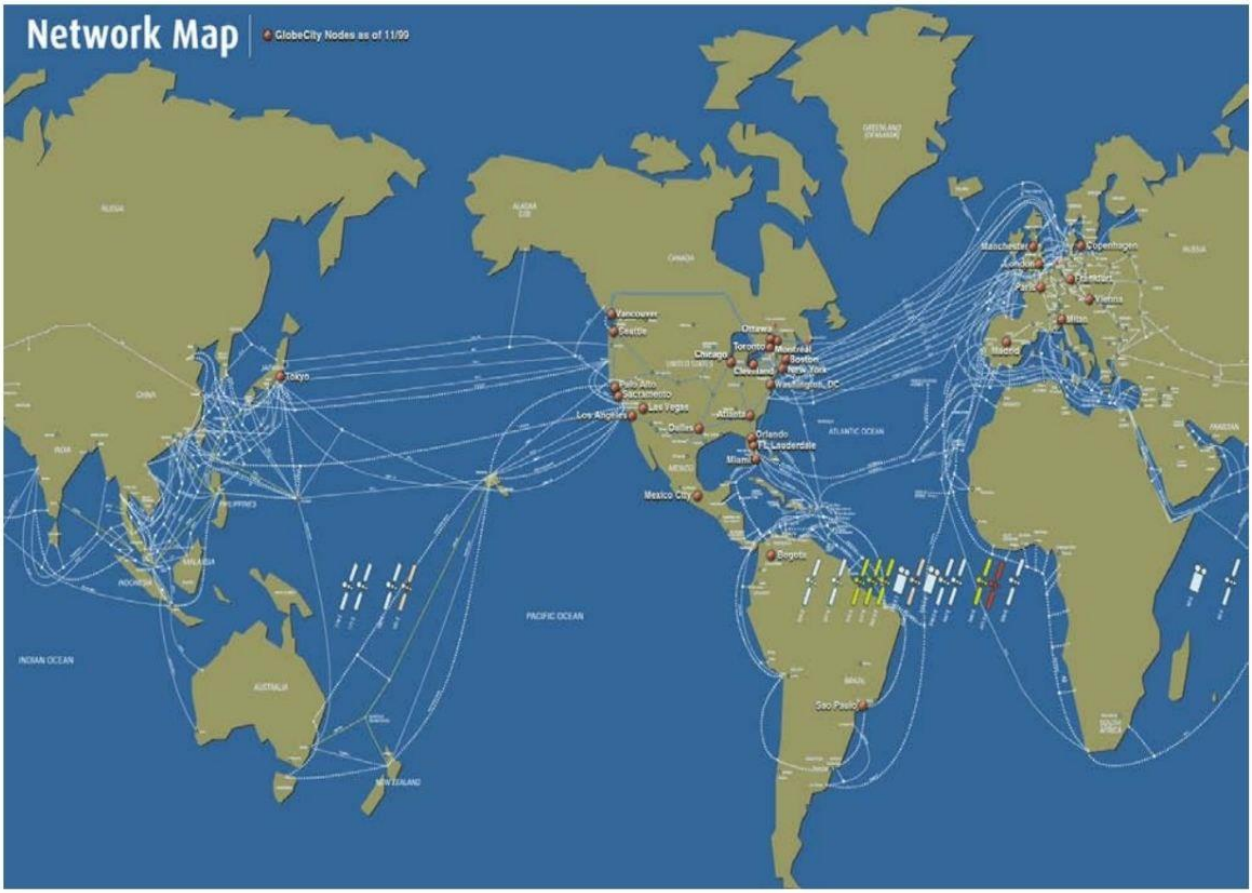
คำนิยามอำนาจทางทะเลของ Mahan มีความคล้ายคลึงกับโลกไซเบอร์เป็นอย่างมาก ในความเป็นจริงแล้ว หากสงครามไซเบอร์มีความคล้ายคลึงน้อยมากหากเทียบกับสงครามบนพื้นดิน แต่มีความคล้ายคลึงมากที่สุดกับการทำสงครามในทะเล กล่าวคือ หากเราเปลี่ยนคำว่า “การพาณิชย์ในท้องทะเล” เป็น “การพาณิชย์อิเล็กทรอนิกส์” และเปลี่ยนคำว่า “ทะเล” ให้กลายเป็น “โลกไซเบอร์” จะทำให้เห็นถึงนิยามที่เปรียบเสมือนสิ่งคู่ขนานกันระหว่างพื้นที่ในทะเล และโลกไซเบอร์

อิทธิพลทางแนวคิดของ Mahan สามารถเห็นได้ชัดเจนจากแผนการพัฒนาและรูปแบบการวางแผนการรบทางทะเลของอำนาจทางทะเลของประเทศสหรัฐอเมริกา และแนวคิดการวางแผนการรบทางทะเลของประเทศสหรัฐอเมริกาไม่ได้มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ หรือแทบจะเหมือนเดิมตั้งแต่ ค.ศ. 1992 จากหนังสือ From the sea ที่ทำให้เกิดการเปลี่ยนแปลงทางทะเลครั้งสำคัญจากปฏิบัติการทะเลสีน้ำเงิน (Blue water operations) สู่การเป็นมหาอำนาจทางทะเลและการเข้าควบคุมขอบเขตทางทะเล

ท้องทะเลคืออาณาเขตที่กว้างใหญ่ไพศาล และครอบคลุมพื้นที่ทั่วโลก ซึ่งมีความคล้ายคลึงกับโลกไซเบอร์เป็นอย่างมาก เนื่องจากความสำคัญของโลกไซเบอร์คือการเชื่อมต่อระหว่างกัน อินเทอร์เน็ตคือการเชื่อมต่อเครือข่ายทั่วโลกของเครือข่ายที่เล็กกว่า ที่เกิดจากการเชื่อมต่อของผู้ใช้งาน

อินเทอร์เน็ตหลากหลายระดับ, เครือข่ายธุรกิจ, เครือข่ายมหาวิทยาลัย และ รัฐบาลของแต่ละประเทศ เครือข่ายเหล่านี้คือการเชื่อมโยงของการเชื่อมต่อในรูปแบบกายภาพ (Physical layer) และ รูปแบบเชิงตรรกะ (Logical layer) โดยผู้ใช้งานอินเทอร์เน็ตเชื่อมต่อโลกไซเบอร์ด้วยการเข้าถึงผ่านสายอินเทอร์เน็ตหรือเน็ตไฟเบอร์ออฟติก (Fiber Optic) หรือผ่านการใช้โทรศัพท์เชื่อมต่อเข้าอินเทอร์เน็ตโดยระบบ wireless และ ใช้งานอินเทอร์เน็ตเพื่อเข้าสู่โลกไซเบอร์ผ่านระบบปฏิบัติการ World Wide Web และระบบอื่นๆ โลกไซเบอร์ถูกวางโครงสร้างเพื่อใช้ทางเทคนิค, ระหว่างประเทศ และบนพื้นฐานทางกฎหมายที่ถูกต้อง แต่โลกไซเบอร์ก็มีส่วนที่ไม่ได้ถูกออกแบบวางโครงสร้างเพื่อให้คนทั่วไปเข้าไปใช้ด้วยเช่นกัน โดยพื้นที่ที่ไม่ได้ถูกออกแบบวางโครงสร้างไว้ เปรียบเสมือนน่านน้ำของทะเลที่อยู่นอกอาณาเขตการปกครองอย่างถูกกฎหมายของประเทศต่างๆ ซึ่งทำให้บุคคลทั่วไปสามารถเข้าใช้พื้นที่ส่วนนี้เพื่อทำสิ่งที่ผิดกฎหมาย โดยปราศจากความกลัวในการที่จะถูกจับกุมและบทลงโทษต่างๆ ไม่ต่างจาก “โจรสลัด” (pirate) ในท้องทะเลที่ทำสิ่งผิดกฎหมายต่างๆ และสามารถใช้นิยามคำว่าโจรสลัดกับบุคคลเหล่านี้ที่ใช้อินเทอร์เน็ตในทางที่ผิดกฎหมายได้ด้วยเช่นกัน

สิ่งที่น่าสนใจอีกอย่างหนึ่งของการเปรียบเทียบอำนาจในทะเลกับอำนาจไซเบอร์ คือ การมีอำนาจในพื้นที่ทั้งสองนี้ อาศัยเส้นทางในการติดต่อ (Lines of Communications)เหมือนกัน ทหารเรือถูกสร้างมาเพื่อปกป้องการเดินเรือและการพาณิชย์ทางทะเล Mahan เชื่อว่าเรือรบมีความต้องการเพื่อสร้างการควบคุมทางทะเล โดยการกำจัดเรือของศัตรูและเพื่อสร้างเขตปกครองดินแดนของตนเอง การสร้างเขตปกครองของตนเองสามารถกระทำได้โดยการปิดเส้นทางการเดินเรือของศัตรูและการสร้างคำสั่งห้ามเดินเรือพาณิชย์ในเขตปกครองของตน และการควบคุมอำนาจในทะเลนั้น ขึ้นอยู่กับพื้นที่ทางกายภาพของประเทศนั้นๆ ว่าอาศัยอยู่ในแถบทะเลส่วนใด ทำให้ง่ายต่อการบริหารจัดการเส้นทางในการติดต่อ (LOCs) ซึ่งโลกไซเบอร์มีความคล้ายคลึงกับอำนาจในทะเล เพราะมีความสัมพันธ์กับ LOCs ด้วยเช่นกัน ดังภาพประกอบที่ 6

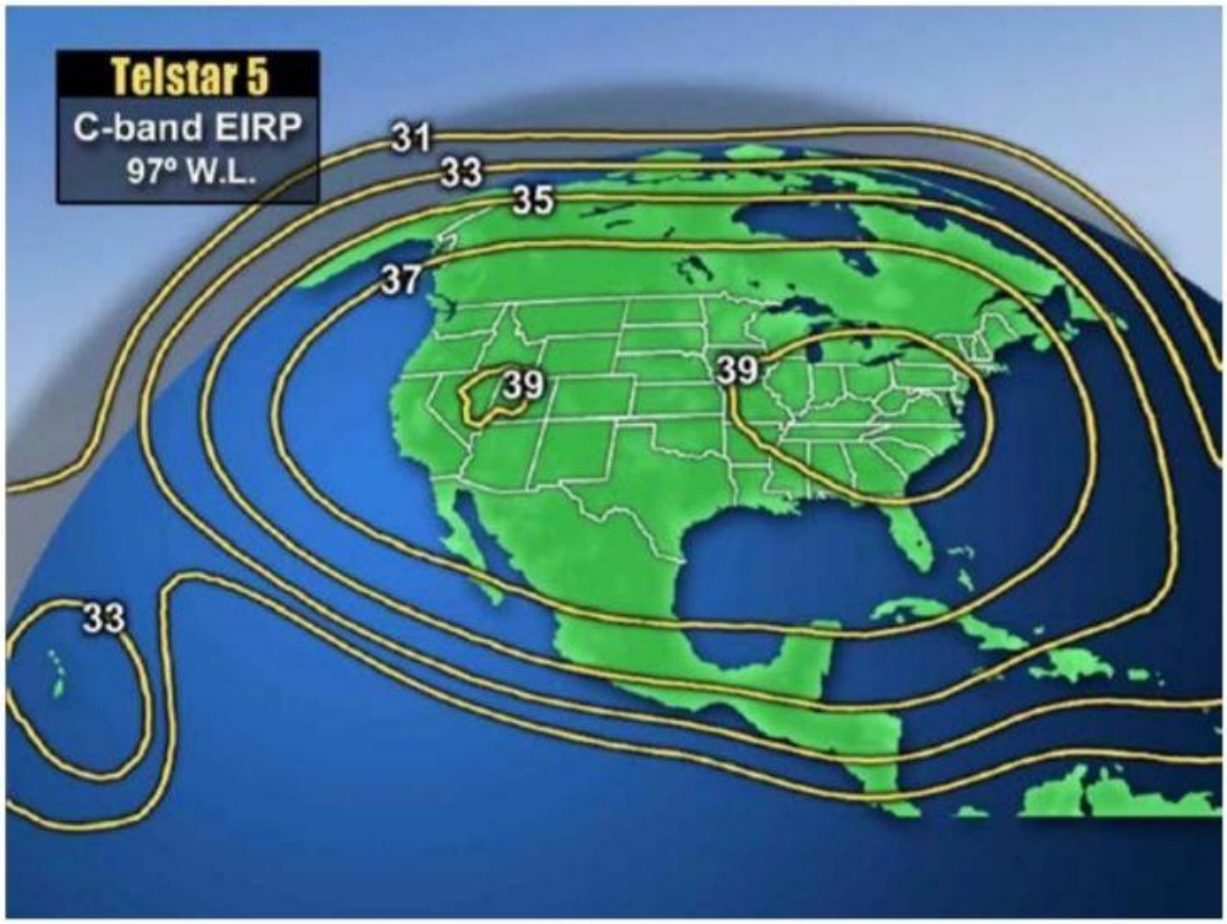


ภาพประกอบ 6 แผนที่เส้นทางการเชื่อมต่อของโลกไซเบอร์ – สายเคเบิ้ลใต้ทะเล

ที่มา: Elbaum (2008)

จากภาพประกอบที่ 6 ทำให้เราเห็นแผนที่การเชื่อมต่อของโลกไซเบอร์ที่มีความคล้ายกับเส้นทางเดินเรืออย่างเห็นได้ชัด การสร้างความเสียหายของการเคลื่อนย้ายข้อมูลของโลกไซเบอร์สามารถทำได้ผ่านเส้นทางของ โนด(nodes) ที่ทำหน้าที่คล้ายกับท่าเรือ (ports) หรือ การโจมตีเส้นทางการเชื่อมต่อ (LOCs) โดยการใช้การโจมตีแบบดั้งเดิม (kinetic strikes), การโจมตีผ่านเครือข่ายคอมพิวเตอร์, และสงครามอิเล็กทรอนิกส์ หรือการโจมตีทั้งสามรูปแบบพร้อมกัน กองทัพเรือสหรัฐให้ความสำคัญกับเส้นทางและท่าเรือรวมถึงอันตรายที่สามารถเกิดขึ้นได้จากการอนุญาตเส้นทางเรือที่เข้ามาใกล้เขตของประเทศตนเอง ซึ่งสามารถเห็นได้จากแผนการปฏิบัติงานของกองทัพเรือสหรัฐ กล่าวว่า “เนื่องจากประเทศสหรัฐอเมริกา เป็นประเทศที่มีการเดินเรือสมุทร, แผนความมั่นคงของเราคือการให้ความสำคัญกับเส้นทางการเดินเรือข้ามมหาสมุทร สิ่งสำคัญที่เราต้องให้ความสนใจเป็นพิเศษ คือการปกป้องเขตแดนทะเลของเรา จุดถึงจุดสิ้นสุดของเขตปกครองของประเทศสหรัฐอเมริกา” จากข้อความดังกล่าวทำให้เราได้เห็นถึงความเป็นจริงที่มีความคล้ายคลึงกับโลกไซเบอร์ คือ หากจุดสิ้นสุดของเส้นทางขนส่งและท่าเรือถูกโจมตีหรือทำลาย นั่นไม่ได้หมายความว่าพื้นที่ทางทะเลจะถูกทำลายไปด้วย มันเป็นเพียงการทำลาย

ปัจจัยที่ใช้ทะเลในการขนส่งเท่านั้น ซึ่งในโลกไซเบอร์ เครื่องมือที่เปรียบเสมือนท่าเรือ หรือ พอร์ท ยังเป็นสิ่งที่สร้างโลกไซเบอร์ด้วยเช่นกัน การปิดเครือข่ายอินเทอร์เน็ตหรือเซิร์ฟเวอร์ของเว็บไซต์ต่างๆ เป็นเพียงการทำให้สัดส่วนของโลกไซเบอร์ลดลงเพียงเท่านั้น จุดศูนย์กลางของแรงโน้มถ่วงของโลกไซเบอร์อาจเป็นจุดเชื่อมต่อโดยตรงต่อการเชื่อมต่อต่างๆ และการที่จุดศูนย์กลางเหล่านี้ถูกทำลายอาจสร้างผลลัพธ์ที่ทำให้การเชื่อมต่อโลกไซเบอร์ในบริเวณเหล่านั้นถูกทำลายลง และทำให้เกิดผลกระทบที่สำคัญต่อประเทศ และอาจกล่าวได้ว่า การทำลายท่าเรือของประเทศนั้นๆ หรือ การทำลายจุดเชื่อมต่อของโลกไซเบอร์ของประเทศนั้นๆ คือการนำมาซึ่งความเสียหายที่อาจทำให้เกิดการยอมจำนน หรือ การไม่สามารถใช้เส้นทางการเดินเรือ หรือ การเชื่อมต่อโลกไซเบอร์ได้นั่นเอง ความแตกต่างของทะเลและโลกไซเบอร์ คือ การกระทำในโลกไซเบอร์อาจเปลี่ยนพื้นที่ขอบเขตของโลกไซเบอร์ในบริเวณนั้นๆ ซึ่งขอบเขตการโจมตีไซเบอร์ที่โจมตีเข้าสู่จุดศูนย์กลางแรงโน้มถ่วงนั้น สามารถทำได้เพียงในขอบเขตของการโจมตีระบบการเงิน, เศรษฐกิจ และ ระบบข้อมูลต่างๆ การโจมตีทางไซเบอร์ไม่สามารถสร้างความเสียหายโดยตรงต่อคลังอาวุธทางการทหารได้ และสามารถใช้ได้เพียงการโจมตีสนับสนุนหรือการโจมตีทางอ้อมที่ช่วยทำให้ภารกิจการโจมตีต่างๆลุล่วง หรือ เป็นการใช้ไซเบอร์เพื่อขอบเขตในการปกป้องความมั่นคงของประเทศ เป็นต้น



ภาพประกอบ 7 ขอบเขตเส้นทางดาวเทียมที่สำคัญที่ใช้สำหรับการเชื่อมต่อโลกไซเบอร์ของประเทศสหรัฐอเมริกา

ที่มา: Elbaum (2008)

นับตั้งแต่ทศวรรษที่ 1920 มหาสมุทรอันกว้างใหญ่ได้แบ่งแยกประเทศสหรัฐอเมริกาออกจากประเทศอื่นๆ การโจมตีจำเป็นที่จะต้องข้ามมหาสมุทร ทำให้การโจมตีเป็นไปได้ยาก เมื่อมีการพัฒนาวิทยาศาสตร์ทางด้านอากาศยาน การวางแผนยุทธศาสตร์ป้องกันความมั่นคงจากการถูกโจมตีทางอากาศได้กลายมาเป็นปัจจัยที่สำคัญ และในปัจจุบัน การโจมตีทั้งทางอากาศและทางทะเลได้ถูกมองผ่านได้มากยิ่งขึ้น เมื่อการโจมตีไซเบอร์ได้กลายมาเป็นสิ่งที่มีประสิทธิภาพมากกว่าในแง่ของการเดินทางและการสร้างความเสียหายได้อย่างทันทีจากระยะไกล โดย Dr. Lani Kass ผู้ควบคุมฐานทัพอากาศสหรัฐที่ดูแลในสัดส่วนของโลกไซเบอร์และผู้ช่วยพิเศษกองทัพอากาศสหรัฐ ได้กล่าวว่า “สนามรบแรกของสงครามในอนาคตคือการทำสงครามเพื่อเข้าควบคุมโลกไซเบอร์”

Mahan ได้กล่าวไว้ว่า “การควบคุมทางทะเลได้ ไม่ได้หมายความว่าศัตรูที่มีจำนวนน้อยกว่าหรือจำนวนกองเรือเพียงน้อยนิดจะไม่สามารถสร้างความเสียหายต่อท่าเรือได้ ประวัติศาสตร์ที่ผ่านมาได้พิสูจน์ถึงความเป็นไปได้ถึงการสร้างความเสียหายจากกองกำลังที่น้อยกว่า รวมถึงกองทหารที่มีความอ่อนแอกว่า ก็สามารถสร้างความเสียหายต่อท่าเรือต่างๆได้เช่นกัน” จากคำกล่าวที่ผ่านมา สามารถเปรียบเทียบกับโลกไซเบอร์ได้อย่างดี เพราะความแตกต่างระหว่างการสร้างความเสียหายจากกองกำลังที่น้อยกว่า สามารถสร้างความเสียหายได้ เปรียบเสมือนการอัพโหลดไฟล์ผ่านโลกไซเบอร์ที่สามารถอัพโหลดไวรัสเพื่อสร้างความเสียหายอย่างกว้างต่อเซิร์ฟเวอร์คอมพิวเตอร์และคอมพิวเตอร์ต่างๆ

จากข้อมูลที่กล่าวมาข้างต้น Mahan ได้ทำการสรุป 8 เงื่อนไขที่สามารถสร้างผลกระทบทางทะเลต่อประเทศได้ ประกอบด้วย ตำแหน่งทางภูมิศาสตร์, โครงสร้างทางกายภาพของประเทศ, ขอบเขตของประเทศ, จำนวนประชากร, ลักษณะประชากร และ ลักษณะของรัฐบาล แต่หากนำมาใช้เปรียบเทียบกับอำนาจไซเบอร์แล้วนั้น ทำให้มีบางเงื่อนไขที่ไม่สามารถนำมาใช้เปรียบเทียบได้ อาทิเช่น

ตำแหน่งทางภูมิศาสตร์คือสิ่งที่ Mahan ให้ความสำคัญ แต่ในโลกไซเบอร์นั้น ตำแหน่งทางภูมิศาสตร์ของประเทศต่างๆเป็นเรื่องที่ไม่สำคัญ เว้นแต่การใช้การโจมตีแบบดั้งเดิม การโจมตีทางไซเบอร์สามารถเกิดขึ้นได้ตลอดเวลา และทุกคนสามารถกระทำได้ เพียงแค่เชื่อมต่ออินเทอร์เน็ตเพียงเท่านั้น ถึงแม้ว่าเซิร์ฟเวอร์อินเทอร์เน็ตอาจอยู่ภายนอกประเทศและโครงสร้างพื้นฐานของเครือข่ายอินเทอร์เน็ตอาจเป็นของประเทศใดประเทศหนึ่ง แต่ตำแหน่งของโลกไซเบอร์คือโลกเสมือน

เงื่อนไขถัดมาที่ไม่สามารถนำมาเปรียบเทียบกับอำนาจไซเบอร์ได้ คือ โครงสร้างทางกายภาพของประเทศ ที่ Mahan ให้ความสำคัญในการเปรียบเทียบอำนาจทางทะเล ที่มาจากการที่ประเทศนั้นๆมีความยาวของพื้นที่ท่าเรือที่กว้างขวาง ส่งผลให้ประเทศนั้นๆมีอำนาจทางทะเลมากกว่าประเทศที่มีพื้นที่

ทางทะเลที่น้อยกว่า ซึ่งหากเปรียบเทียบกับอำนาจทางไซเบอร์ สามารถเปรียบเทียบได้กับประเทศที่อยู่เชื่อมต่อกับท่อสายเคเบิ้ลอินเทอร์เน็ตขนาดใหญ่ ทำให้สามารถใช้งานอินเทอร์เน็ตได้มีประสิทธิภาพมากกว่าประเทศที่มีการเชื่อมต่อท่อสายเคเบิ้ลอินเทอร์เน็ตที่อยู่ปลายสาย การได้เปรียบนี้สามารถทำให้ประเทศที่ได้เปรียบ สามารถสร้างการโจมตีทางไซเบอร์ได้มีประสิทธิภาพมากกว่า แต่ถึงอย่างไรก็ตาม พื้นที่ทางไซเบอร์นั้นคือสิ่งแวดล้อมที่ถูกมนุษย์สร้างขึ้น ดังนั้นมนุษย์สามารถปรับเปลี่ยนพื้นที่ทางไซเบอร์ได้ตามที่ต้องการ อีกทั้งการสร้างไฟล์วอล์ (firewall), เราท์เตอร์อินเทอร์เน็ต และอื่นๆอีกมากมาย ที่มนุษย์สามารถสร้างเพื่อสร้างความมั่นคงและอำนาจทางไซเบอร์ได้เช่นกัน

เงื่อนไขในเรื่องขอบเขตประเทศ เมื่อเปรียบเทียบกับอำนาจไซเบอร์แล้ว สิ่งที่แตกต่างกันคือเหตุผลของ Mahan นิยามขอบเขตประเทศว่า หากประเทศมีเขตแดนที่ติดชายทะเลมาก ก็ยิ่งมีอำนาจทางทะเลมาก ซึ่งไม่สามารถเปรียบเทียบกับอำนาจทางไซเบอร์แล้ว การที่โลกไซเบอร์มีพื้นที่ที่กว้างขวางอาจส่งผลให้เกิดผลร้ายมากกว่า เพราะยิ่งพื้นที่ของโลกไซเบอร์กว้างมากเท่าไหร่ เรายิ่งจำเป็นต้องสร้างแนวป้องกันมากขึ้นด้วยเช่นกัน การสร้างแนวป้องกันของโลกไซเบอร์ จำเป็นต้องใช้ทรัพยากรจำนวนมาก ซึ่งการสร้างแนวป้องกันทางไซเบอร์ที่มากขึ้น ไม่ได้หมายความว่า ประสิทธิภาพการโจมตีทางไซเบอร์ของเราจะมากขึ้นตามไปด้วย เพราะการโจมตีทางไซเบอร์เกิดจากการใช้ประสิทธิภาพการโจมตีที่พัฒนาจากความเชี่ยวชาญทางด้านไซเบอร์เท่านั้น

การเปรียบเทียบจำนวนประชากร เป็นเงื่อนไขที่สำคัญเช่นกัน แต่เป็นความสำคัญที่แตกต่างจากนิยามอำนาจทางทะเล โดย Mahan ได้กล่าวว่า จำนวนประชากรคือสิ่งที่สำคัญ เพราะเป็นส่วนสำคัญในการใช้แรงงานเพื่อสร้างท่าเรือและการสร้างเรือ และเป็นเงื่อนไขที่ง่ายในการนำประชากรจากต่างแดนมาเพื่อใช้แรงงาน และเป็นสิ่งที่สามารถสอนได้โดยง่าย หากนำมาเปรียบเทียบกับอำนาจทางไซเบอร์แล้วนั้น ประชากรที่มีความสามารถทางไซเบอร์มีจำนวนน้อยมาก และจำนวนประชากรนั้นมีส่วนสำคัญเพียงเพื่อเพิ่มโอกาสในการที่ประเทศนั้นๆ จะสามารถสร้างประชากรจำนวนหนึ่งที่มีความสามารถทางไซเบอร์ เพื่อเพิ่มประสิทธิภาพไซเบอร์ของประเทศ และการป้องกันความมั่นคงทางไซเบอร์ของประเทศด้วยเช่นกัน

บทบาทหรือลักษณะของประเทศนั้นๆ คือสิ่งที่ Mahan ให้ความสำคัญเป็นอย่างมาก Mahan เชื่อว่า ลักษณะของประเทศนั้นๆ และความพร้อมที่จะเรียนรู้และพัฒนาประเทศ คือสิ่งที่สำคัญอย่างมากต่อการสร้างอำนาจทางทะเล โดย Mahan ได้กล่าวว่า หากหลากหลายประเทศมองเห็นตรงกันว่า อำนาจทางทะเลขึ้นอยู่ที่ความสันติสุขของท้องทะเล และ การขนส่งพาณิชย์ที่กว้างขวางคือจุดประสงค์หลักของหลากหลายประเทศ การปรึกษาหารือและการตัดสินใจร่วมกันของประเทศต่างๆ คือโอกาสที่ดีในการสร้างความร่วมมือกันเพื่อพัฒนาเส้นทางเดินเรือต่างๆในทะเล ซึ่งเปรียบเสมือนโลกไซเบอร์ ที่อินเทอร์เน็ตคือเครื่องมือหลักในการพาณิชย์และการเคลื่อนไหวของข้อมูลและความรู้ผลประโยชน์ทางการค้าขายหรือพาณิชย์ จะทำหน้าที่ในการค้นคว้าและพัฒนาเทคโนโลยีโลกไซเบอร์มาก

ยิ่งขึ้น เพราะสามารถสร้างประโยชน์ได้มากขึ้น และผู้ใช้งานจะพยายามสร้างนวัตกรรมใหม่เสมอ เพื่อความสะดวกสบายในการใช้งานและการสร้างองค์ความรู้ใหม่เพื่อตอบสนองการใช้งานของพื้นที่ในโลกไซเบอร์ ดังนั้น ประเทศใดก็ตามที่ให้ความสำคัญในการพัฒนาโลกไซเบอร์ จะกลายเป็นประเทศที่ได้ประโยชน์จากการพาณิชย์และองค์ความรู้ในโลกไซเบอร์มากที่สุด

เงื่อนไขสุดท้ายของการเปรียบเทียบระหว่างอำนาจทางทะเลและอำนาจไซเบอร์ คือ ลักษณะของรัฐบาล โดย Mahan ได้กล่าวว่า “รัฐบาลคือสถาบันทางการเมืองที่มีการทำงานสอดคล้องกับความต้องการของประชาชน จะกลายเป็นรัฐบาลที่ประสบความสำเร็จและก้าวหน้าในทุกด้านของการทำงาน” ซึ่งสามารถเห็นได้ชัดเจนหากนำมาเปรียบเทียบกับโลกไซเบอร์ ประเทศสหรัฐอเมริกา หรือ ประเทศที่ใช้ระบอบทุนนิยมในการบริหารประเทศ คือประเทศที่ชื่นชอบในการค้าขาย สอดคล้องกับบริบทของประชากรในประเทศ และท้ายที่สุด ส่งผลให้เกิดนักพัฒนานวัตกรรมมากมายในโลกไซเบอร์ของโลกใบนี้ ระบบอินเทอร์เน็ตมีจุดกำเนิดจากประเทศสหรัฐอเมริกา และเป็นโฮส (host) ของระบบอินเทอร์เน็ตทั่วโลกอยู่ที่ 6 ใน 13 เซิร์ฟเวอร์หลักของโลก และเราท์เตอร์, สวิตช์ต่างๆ ,ระบบไฟล์วอร์ และระบบตรวจจับสิ่งผิดปกติในระบบอินเทอร์เน็ต ที่ถูกออกแบบโดยชาวอเมริกา ถูกผลิตและจัดจำหน่ายไปยังทั่วโลกด้วยเช่นกัน ความรักและชื่นชอบในการมีอิสระในการเรียนรู้ของประชากรของประเทศสหรัฐอเมริกาได้นำมาซึ่งคำถามที่ชวนคิดถึงความก้าวหน้าของโลกไซเบอร์ คือ รัฐบาลควรที่จะยังคงสนับสนุนประชากรและอำนาจทางไซเบอร์อยู่หรือไม่ หากอำนาจทางไซเบอร์สามารถกลายเป็นความเสี่ยงของประเทศ

ในปัจจุบัน อำนาจทางทะเลยังคงมีบทบาทสำคัญอย่างมากในการพาณิชย์ของโลกใบนี้ โดยความมั่นคงของระบบเศรษฐกิจของโลกใบนี้ ยังคงขึ้นอยู่กับการค้าขายระหว่างประเทศ และ 90% ของการค้าขายของโลก รวมถึง 00% ของการขนส่งระหว่างประเทศ ยังคงใช้การขนส่งทางเรือ ทำให้ความสำคัญของเส้นทางการเดินเรือยังคงมีบทบาทสำคัญอย่างมากต่อการอยู่รอดของระบบเศรษฐกิจต่างๆในโลกใบนี้ ในขณะเดียวกัน การค้าขายในโลกออนไลน์ได้เติบโตขึ้นอย่างมาก โดยในปี 2022 ได้มีการค้าขายในโลกออนไลน์เป็นจำนวนเงินทั้งหมด 1 พันล้านเหรียญดอลลาร์สหรัฐ (Retail Dive, 2022) จึงเห็นได้ชัดว่า ความสำคัญของอำนาจทางทะเลและอำนาจทางไซเบอร์ คือสิ่งที่สำคัญเป็นอย่างมากต่อระบบเศรษฐกิจของโลกใบนี้

การให้ความสำคัญของกองทัพเรือในการควบคุมอำนาจทางทะเล คือเป้าหมายหลักในช่วงการทำสงคราม และความสามารถในการควบคุม ไม่ว่าจะเป็นทางทะเล ทางอากาศ หรือในโลกไซเบอร์ล้วนแต่วัดจากความสามารถของกองกำลังทางการทหารที่ครอบครองอยู่ แผนยุทธศาสตร์การรบทางทะเลของกองทัพเรือสหรัฐ การบรรลุเป้าหมายในการควบคุมทางทะเล จะสามารถบรรลุเป้าหมายได้จากการปฏิบัติตามแผนยุทธศาสตร์การรบทางทะเล ที่มีขั้นตอนปฏิบัติการ คือ “การทำลายหรือการสร้างความสียหายเรือ เรือดำน้ำ อากาศยาน และระเบิดของศัตรู, การสร้างความเสียหายต่อระบบสื่อสารและควบคุมของศัตรู, การทำลายหรือการสร้างความเสียหายต่อโครงสร้างพื้นฐานของฐานที่มั่นที่ใช้ในการ

สนับสนุนหรือ การควบคุมการติดต่อการรบของศัตรู, การเข้ายึดเกาะ จุดสำลัก(จุดยุทธศาสตร์ทางทะเล เช่นช่องแคบสมุทร) คาบสมุทร และชายฝั่งของศัตรู, และ การสร้างเกราะกำบังเพื่อป้องกันจุดสำลักทั้งในรูปแบบใต้น้ำ บนผิวน้ำ และทางอากาศ”

ซึ่งหากนำมาเปรียบเทียบกับโลกไซเบอร์แบบเรียงลำดับตามนิยามข้างต้นแล้วนั้น การทำลายหรือการสร้างความเสียหายต่อเครื่องจักรที่ใช้ในการทำสงคราม เป็นเรื่องยากในโลกไซเบอร์ ไม่เหมือนกับการทำลายอาคารต่างๆที่ต้องใช้การลงทุนทางด้านทรัพยากรจำนวนมาก แต่การโจมตีโลกไซเบอร์นั้นสามารถทำได้โดยไม่จำเป็นต้องใช้ทรัพยากรจำนวนมาก คอมพิวเตอร์เพียงเครื่องเดียวก็สามารถสร้างผลกระทบได้อยากง่ายดาย ทรัพยากรที่สำคัญที่แท้จริงในการโจมตีคือ องค์ความรู้และความสามารถของแฮ็กเกอร์ที่ทำการโจมตี ดังนั้น หากเปรียบเทียบการทำลายหรือการสร้างความเสียหายต่อเครื่องจักรที่ใช้ในการทำสงครามแล้วนั้น ควรจะเป็นคำสั่งปฏิบัติการที่เน้นการทำลายกองกำลังไซเบอร์ของฝ่ายศัตรู

การเปรียบเทียบลำดับถัดมา คือการสร้างความเสียหายต่อระบบสื่อสารและควบคุมของศัตรู ซึ่งเป็นขั้นตอนที่สำคัญเป็นอย่างมาก เนื่องจากการทำสงครามในแต่รูปแบบนั้น จำเป็นที่จะต้องพึ่งพาการสื่อสารและควบคุมต่างๆ ลำดับถัดมาคือการเปรียบเทียบการทำลายโครงสร้างพื้นฐานของฐานที่มั่นที่ใช้ในการสนับสนุนหรือคควบคุม ต่อต่อการรบของศัตรู หากนำมาเปรียบเทียบกับโลกไซเบอร์แล้วนั้น จะเห็นได้ถึงความต่างในขั้นตอนการสื่อสารระหว่างศูนย์ควบคุมกับเรือรบ หรือระหว่างเรือรบด้วยกันเอง โดยการทำลายฐานที่มั่นที่ใช้ในการสนับสนุนหรือติดต่อระหว่างศูนย์ควบคุมกับเรือรบนั้น จะสร้างความเสียหายเป็นอย่างมากต่อปฏิบัติการต่างๆ แต่กองกำลังทางไซเบอร์สามารถสื่อสารกันได้ เพียงการตะโกนหากัน เนื่องจากการปฏิบัติการของกองกำลังไซเบอร์นั้น คือการทำงานที่อยู่ใกล้ชิดกัน หรืออยู่ในห้องเดียวกัน อย่างไรก็ตาม การทำลายฐานที่มั่นที่ใช้ในการสนับสนุนการปฏิบัติการของกองกำลังทางไซเบอร์หรือการโจมตีทางกายภาพต่อกองกำลังทางไซเบอร์ ยังคงเป็นการโจมตีที่มีประสิทธิภาพอย่างมากเช่นเดียวกัน เพราะสามารถสร้างความเสียหายต่อการกองกำลังทางไซเบอร์โดยตรง

การเข้ายึดเกาะ จุดสำลัก คาบสมุทร และชายฝั่งของศัตรู สามารถเปรียบเทียบกับโลกไซเบอร์ได้ โดยเป็นการเปรียบเสมือนการเข้ายึดและควบคุมเราท์เตอร์อินเทอร์เน็ต และจุดเชื่อมต่ออินเทอร์เน็ตของศัตรู ที่ฝ่ายศัตรูใช้ในการเข้าถึงอินเทอร์เน็ตเพื่อปฏิบัติการกับโลกไซเบอร์ และการเปรียบเทียบลำดับสุดท้ายคือ การสร้างเกราะกำบังเพื่อป้องกันจุดสำลักทั้งในรูปแบบใต้น้ำ บนผิวน้ำ และทางอากาศ สามารถนำมาเปรียบเทียบกับโลกไซเบอร์ได้เช่นกัน โดยเป็นการเปรียบเทียบเมื่อเรามีกุญแจหรือรหัสที่ใช้ในการเข้าเราท์เตอร์อินเทอร์เน็ตที่สำคัญ ซึ่งจำเป็นต้องทำให้หลีกเลี่ยงจากการเข้าถึงหรือการรับรู้จากโลกภายนอก เพื่อความมั่นคงทางไซเบอร์ (Cyberpower 21st, p.64)

จากการเปรียบเทียบอำนาจทางทะเล และอำนาจทางไซเบอร์ ทำให้เราได้เห็นถึงความเหมือนและความแตกต่างของการเปรียบเทียบ การมีอำนาจทางทะเล สามารถเปรียบเทียบได้ใน “การมีอำนาจในการปกป้องเส้นทางเดินเรือที่ใช้ในการติดต่อสื่อสาร การกำจัดศัตรูใช้เส้นทางเดินเรือในการ

พาณิชย์และการใช้เพื่อการทหารบนท้องทะเลในเขตปกครอง การสร้างเขตแดนในการปฏิบัติการเพื่อสร้างอำนาจในเขตท่าเรือต่างๆ การสนับสนุนปฏิบัติการที่ใช้ทั้งทางบกและทางทะเลร่วมกัน และการปกป้องการขนส่งทางทะเลเพื่อการเสริมสร้างอาวุธที่ใช้ในการทำสงครามทางทะเล” โดยในโลกไซเบอร์นั้น การสื่อสาและการแลกเปลี่ยนข้อมูล ถือเป็นเรื่องที่สำคัญเป็นอย่างมาก และเป็นเป้าหมายหลักของการมีโลกไซเบอร์ และการปกป้องโครงสร้างพื้นฐานที่ใช้สำหรับการปฏิบัติการทางไซเบอร์ ถือว่าเป็นเรื่องที่สำคัญเป็นอย่างมากถึงมากที่สุด การทำลายหรือการสร้างความเสียหายการสื่อสารของฝ่ายศัตรูเป็นเรื่องที่ต้องให้ความสำคัญเช่นเดียวกัน ความไม่สมมาตรของโลกไซเบอร์ คือเรื่องที่ต้องใช้ในการวิเคราะห์โลกไซเบอร์ด้วยเช่นกัน เพราะสามารถชี้ให้เห็นถึงประเทศที่มีเทคโนโลยีที่ล้ำสมัย จะสามารถสร้างผลประโยชน์ในโลกไซเบอร์ได้มาก แต่ขณะเดียวกันก็สามารถเกิดความเสียหายจากโลกไซเบอร์ได้อย่างมากด้วยเช่นกัน การสร้างอำนาจในเขตแดนทางทะเล คือสิ่งที่สามารถใช้ในการเปรียบเทียบกับการสร้างอำนาจทางไซเบอร์ และท้ายที่สุด การเสริมสร้างเส้นทางในการขนส่งกองกำลังทางทหารเหมือนอำนาจทางทะเล ไม่มีบทบาทที่สำคัญในอำนาจทางไซเบอร์ เว้นเสียแต่ว่า เป็นการทำงานร่วมกันระหว่างหน่วยปฏิบัติการพิเศษที่มีการใช้ความสามารถทางไซเบอร์เข้าไปช่วยเหลือในปฏิบัติการนั้นๆ

อำนาจในอากาศและอวกาศ (Power in Air and Space)

อำนาจในอากาศและอวกาศ มีความเหมือนอำนาจในทะเล อาทิเช่น การทำงานของโลกไซเบอร์สามารถผลกระทบต่อการทำงานในพื้นที่อื่น เช่น พื้นที่บนบก, โลกไซเบอร์คือโลกที่อยู่ระหว่างเวลาและอากาศ, โลกไซเบอร์สร้างการโจมตีข้ามเขตแดนที่สามารถสร้างความเสียหายต่อโครงสร้างภายในของศัตรูได้ และ ความสำคัญในการควบคุมโลกไซเบอร์จะสามารถสร้างการควบคุมพื้นที่อื่นได้ด้วยเช่นกัน

การเปรียบเทียบทฤษฎีอำนาจทางอากาศนั้น สามารถนำทฤษฎีของ Giulio Douhet และ Billy Mitchell มาอธิบายความเหมือนระหว่างอำนาจทางอากาศและอำนาจทางไซเบอร์ได้ดังนี้

Douhet คือ ผู้สนับสนุนทางด้านยุทธศาสตร์การรบทางอากาศแบบจู่โจม และ Mitchell คือผู้สนับสนุนทางด้านยุทธศาสตร์ที่มีการใช้ทั้งในรูปแบบจู่โจมและการตั้งรับ เพื่อรักษาความสมดุลของกองกำลัง Douhet ได้เขียนไว้ว่า “กองกำลังทางอากาศคือกองกำลังจู่โจมที่สามารถสร้างการโจมตีด้วยความเร็วบนอาณาเขตของศัตรูทั้งบนบกและในน้ำได้จากทุกทิศทาง และสามารถสร้างแรงกดดันจากทางอากาศให้กับศัตรูได้ด้วยเช่นกัน” อำนาจทางอากาศนี้สามารถใช้เปรียบเทียบความเหมือนกับอำนาจไซเบอร์ ได้โดยการโจมตีทางไซเบอร์สามารถสร้างการโจมตีด้วยความเร็วสูงได้ถึงระดับโลก และสามารถสร้างแรงกดดันให้กับฝ่ายศัตรูได้ (เมื่อศัตรูยังคงไม่สามารถปิดการเชื่อมต่อทางอินเทอร์เน็ต) แต่ไม่อาจสร้างความเสียหายหรือการสอดแนมได้เท่ากับการอธิบายอำนาจทางอากาศของ Douhet องค์ความรู้และความก้าวหน้าทางแนวคิดเชิงตรรกะที่ใช้ในการสร้างอำนาจทางไซเบอร์ คือ อาวุธที่จะสามารถนำมาใช้ในการทำลายการป้องกันทางไซเบอร์ Douhet คือผู้ติดตามสำนักคิด Clausewitzian และมี

ความเชื่อว่า เป้าหมายการโจมตีทางอากาศ คือการโจมตีเพื่อสร้างความเสียหายอย่างใหญ่หลวงในระยะเวลาอันสั้น ซึ่งสามารถนำความเชื่อของ Douhet มาเปรียบเทียบการโจมตีทางไซเบอร์ที่สามารถทำการโจมตีได้ในชั่วพริบตาได้ด้วยเช่นกัน Douhet ยังได้เปรียบเทียบการโจมตีทางอากาศไว้ว่าเปรียบเสมือนการโจมตีของเหล่าทหารม้า ที่มีแนวคิดว่า การป้องกันที่ดีที่สุด คือการโจมตี, ดังนั้น อำนาจทางอากาศ จะสามารถมีการปกป้องที่ดีได้ ต้องมาจากการโจมตีศัตรูก่อน และต้องเป็นการโจมตีแบบเต็มกำลังเท่านั้น ซึ่งได้รับอิทธิพลมาจากแนวคิดของ Clausewitz แต่ถึงกระนั้น แนวคิดของ Douhet ก็มีความแตกต่างที่ไม่สามารถนำมาเปรียบเทียบกับโลกไซเบอร์ด้วยเช่นกัน คือ แนวคิดที่กล่าวถึงการหลบหนีเมื่อมีการโจมตีจากศัตรู โดยที่เราไม่สามารถโต้ตอบกับศัตรูได้ แต่ในโลกไซเบอร์นั้น ผู้ที่มีหน้าที่ปกป้องโลกไซเบอร์ มีหลากหลายวิธีในการป้องกันความเสียหายที่สามารถเกิดขึ้นจากการโจมตี ทำให้ไม่จำเป็นต้องหลบหนีหรือสละเครื่องเหมือนกับแนวคิดอำนาจทางอากาศของ Douhet ดังนั้น การป้องกันทางไซเบอร์จึงเป็นเรื่องที่ไม่ควรถูกมองข้าม

แนวคิดของ Mitchell ให้ความสำคัญกับแนวคิดการป้องกันมากกว่าแนวคิดของ Douhet และมองว่า สงครามไซเบอร์เป็นเพียงการทำสงครามเพื่อสนับสนุนปฏิบัติการของการทำสงครามรูปแบบอื่นๆ ถึงแม้ว่า Mitchell จะมีแนวคิดที่คล้ายกับ Douhet ในเรื่องของอำนาจทางอากาศ แต่ Mitchell ได้ให้แง่มุมของอำนาจทางอากาศไว้ว่า “การทำสงครามการรบ ทุกสิ่งทุกอย่างเริ่มต้นและจบลงที่พื้นดิน, เราไม่สามารถอาศัยอยู่บนอากาศตลอดไป เฉกเช่นการอาศัยอยู่บนทะเล ท้ายที่สุดแล้ว การตัดสินใจในสงครามต่างมาจากการตัดสินใจจากภาคพื้นดิน” และเขายังได้ให้มุมมองต่อว่า “เราไม่สามารถโจมตีกองทัพที่อยู่บนบกทั้งหมดได้จากการโจมตีทางอากาศ แต่เราสามารถได้รับการโจมตีอย่างหนักหน่วงจากการโจมตีบนบกสู่อากาศ” แนวคิดของ Mitchell ในการอธิบายอำนาจทางอากาศ มีความเป็นยุทธวิธีมากกว่า Douhet โดยเขาได้อธิบายว่า “ ภารกิจการโจมตีทางอากาศคือ การโจมตีกองกำลังบก, รถไฟขนส่งยุทโธปกรณ์, รถไฟลำเลียงอาหารและเสบียง, เส้นทางเดินรถไฟ, รถถัง, การเดินทางของรถไฟ, เรือหรือ กองทัพเรือ, หรืออุปกรณ์ทางการทหารต่างๆ ที่อยู่บนพื้นดินหรือในทะเล ที่สามารถมองเห็นได้อย่างชัดเจนจากอากาศ และสามารถถูกโจมตีจากปืนใหญ่, ปืนกล หรือ ระเบิดจากเครื่องบิน” แนวคิดของ Mitchell สามารถนำมาเปรียบเทียบกับการโจมตีทางไซเบอร์ได้ คือ การโจมตีทางไซเบอร์สามารถสร้างผลกระทบให้กับเครื่องบินรบได้โดยการทำให้เรดาห์ทำงานผิดปกติ หรือ การทำให้เครื่องบินรบขาดการติดต่อจากศูนย์ควบคุม ซึ่งแสดงให้เห็นว่า อำนาจทางไซเบอร์สามารถใช้ในการทำยุทธวิธีได้ด้วยเช่นกัน อาทิเช่น การรุกรานของประเทศรัสเซียที่ทำการโจมตีประเทศ South Ossetia

แนวคิดการควบคุมอำนาจแบบเบ็ดเสร็จทางอากาศ คือสิ่งที่นักคิดทั้งสองคนได้ให้ความคิดเห็นที่ตรงกัน โดย Douhet ได้ให้มุมมองว่า “การเข้ายึดอำนาจทางอากาศ คือการทำให้ศัตรูไม่สามารถนำเครื่องบินรบขึ้นบินได้ จำเป็นที่จะต้องทำให้การโจมตีทางอากาศ ทำได้เพียงฝ่ายเดียวเท่านั้น”

ในขณะที่ Mitchell ได้เขียนไว้ว่า “รัฐควรที่จะเข้าควบคุมอำนาจทางอากาศอย่างเบ็ดเสร็จ เพื่อการควบคุมโลกที่ง่ายดายมากขึ้นกว่าในอดีต” แนวคิดเหล่านี้สามารถนำมาเปรียบเทียบกับโลกไซเบอร์ได้อย่างชัดเจน เพียงแต่ปรับใช้ได้เฉพาะประเทศที่พึ่งพาโลกไซเบอร์เท่านั้น เพราะประเทศที่ไม่ได้ใช้โลกไซเบอร์เป็นวงกว้าง จะได้รับผลกระทบเพียงเล็กน้อยจากการเข้ายึดโลกไซเบอร์หรือการโจมตีโลกไซเบอร์ อย่างไรก็ตาม หากประเทศที่พึ่งพาไซเบอร์ได้ถูกโจมตีทางไซเบอร์ ความเสียหายที่เกิดขึ้นจะส่งผลต่ออำนาจทางการทหารของประเทศนั้นๆโดยทันที โดยเฉพาะเมื่อกองกำลังทางการทหารเหล่านั้นถูกโจมตีทางไซเบอร์ แล้วไม่รู้ว่าจะปฏิบัติการทางการทหารต่อได้อย่างไรในสงคราม

ทฤษฎีอำนาจทางอากาศแบบใหม่ของกองทัพอากาศสหรัฐ อิงแนวคิดอำนาจทางอากาศของ Mitchell มากกว่าแนวคิดของ Douhet เนื่องจากประชากรประเทศสหรัฐอเมริกาได้ให้คุณค่าทางด้านอุดมคติ และศีลธรรมมากยิ่งขึ้นในทศวรรษที่ 21 ทำให้การใช้ความรุนแรงในการทำสงครามต่อประเทศต่างๆถูกกีดกันจากสังคม อย่างไรก็ตาม ยุทธวิธีในการเลือกใช้หัวรบนิวเคลียร์ ก็ยังคงเป็นทางเลือกหนึ่งที่ไม่ได้ถูกกีดกันจากสังคม เพื่อรับมือในสถานการณ์ที่จำเป็นมากที่สุด กองทัพอากาศมีประสิทธิภาพมากยิ่งขึ้น โดยเฉพาะหากเปรียบเทียบประสิทธิภาพในช่วงทำสงครามโลกครั้งที่ 2, สงครามเกาหลี, สงครามเวียดนาม และยุคสงครามเย็น เพราะพัฒนาการและนวัตกรรมทางเทคโนโลยีที่ทำให้อาวุธต่างๆมีความล้ำสมัยและมีประสิทธิภาพมากยิ่งขึ้น การโจมตีทางอากาศได้กลายเป็นงานวิจัยที่ถูกให้ความสำคัญอย่างมาก การทิ้งระเบิดใส่เมืองต่างๆ กลายเป็นเรื่องที่ไม่จำเป็นต่อการทำสงคราม เพราะเป็นการทำลายวงกว้างที่ไม่เฉพาะเจาะจงต่อเป้าหมายในการทำสงคราม อีกทั้งยังสร้างความเสียหายโดยกว้าง มากกว่าการทำให้เป้าหมายหลักเสียหาย อีกทั้งยังส่งผลต่อคุณค่าทางด้านศีลธรรมด้วยเช่นกัน พัฒนาการทางเทคโนโลยีทำให้ความหมายของคำว่า “มวล” หรือ Mass เปลี่ยนไปจากอดีต หากเราใช้คำว่า Mass กับการโจมตีทางอากาศ ในอดีตอาจหมายถึงเครื่องบินรบจำนวนร้อยกว่าลำเผชิญหน้ากับกองทัพศัตรู แต่ ณ ปัจจุบันกลับหมายถึงระเบิดลูกเดียวที่ถูกบรรจุไว้ในเครื่องบินรบที่สามารถสร้างความเสียหายเป็นวงกว้าง ซึ่งเปรียบเสมือนอำนาจทางไซเบอร์ ที่การโจมตีทางไซเบอร์ที่สามารถส่งผลกระทบเป็นวงกว้าง สามารถเกิดจากการใช้คอมพิวเตอร์เพียงเครื่องเดียวเท่านั้นในการโจมตี

แนวคิดการโจมตีเข้าสู่จุดศูนย์กลางและความไม่สมมาตรของโลกไซเบอร์

จากอดีตถึงปัจจุบัน ประเทศต่างๆต้องการที่จะเสริมสร้างกำลังทางการทหารและอาวุธเพื่อให้ประเทศตนเองมีอำนาจมากยิ่งขึ้นกว่าประเทศอื่นๆ กระทรวงกลาโหมของประเทศสหรัฐอเมริกาได้มีการกำหนดแผนยุทธศาสตร์เพื่อรับมือกับสิ่งที่จะเกิดขึ้นดังนี้ 1. เพื่อปกป้องประเทศจากภัยอันตรายภายนอกประเทศ 2. เพื่อป้องกันความขัดแย้งและการโจมตีอย่างเฉียบพลัน 3. เพื่อตอบโต้ภัยคุกคามต่างๆ จากการวางแผนยุทธศาสตร์ทางการทหารต่างๆ นำมาสู่กระบวนการบริหารงาน, ฝึกฝนกองกำลังทางการทหาร และการ

รวบรวมเครื่องมือ อาวุธ และยุทโธปกรณ์ต่างๆเพื่อสร้างกองกำลังทางการทหารเพื่อต่อสู้สงคราม (Warfighter)

เป้าหมายของแผนยุทธศาสตร์ทางการทหารล้วนแต่ต้องการเพิ่มและรักษาขีดความสามารถทางการทหารให้สามารถตอบโต้ต่อภัยต่างๆที่จะเกิดขึ้นทั้งรูปแบบกายภาพ และรูปแบบที่ไม่ใช่กายภาพ (non-physical methods) แต่การที่จะได้มาซึ่งความสามารถในการกระทำต่างๆทางการทหาร ล้วนเกิดจากปัจจัยต่างๆของประเทศนั้นๆ เช่น ความสามารถทางการทูต (Diplomatic), ความสามารถทางข้อมูล (Informational), อำนาจทางการทหาร (Military) และเศรษฐศาสตร์ (Economic) (DIME) ซึ่งภายหลังได้มีการเพิ่มปัจจัยอื่นๆเข้าร่วมด้วย เช่น ระบบการเงิน (Financial system), ความสามารถทางด้านความรู้ (Intelligence), และการบังคับใช้กฎหมาย (Law enforcement) (DIMEFIL) (Elbaum, 2008)

หากประเทศนั้นๆได้อำนาจมา อำนาจที่เกิดขึ้น ควรที่จะถูกปรับใช้ในทิศทางไหน นิยามทางด้านอำนาจเหล่านี้ได้ถูกศึกษาโดยนักทฤษฎีทางการทหารหลากหลายคน แต่แนวคิดอำนาจที่ผู้เขียนต้องการนำมาต่อยอดในการค้นคว้า คือ แนวคิดจุดศูนย์กลางของแรงโน้มถ่วง (Center of gravity) ของ Carl von Clausewitz นายพลชาวเยอรมันปรัสเซีย และนักทฤษฎีทางการทหารที่สนใจในกฎของฟิสิกส์ ที่ได้นำแนวคิดแรงโน้มถ่วงมาเชื่อมโยงกับแนวคิดทางการทหาร ซึ่งแนวคิดจุดศูนย์กลางของแรงโน้มถ่วงของ Clausewitz ได้อธิบายว่า การเป็นจุดศูนย์กลางของอำนาจทางการทหารของโลกนี้ ไม่ได้เกี่ยวข้องกับความแข็งแกร่งของอำนาจ หรือเกี่ยวกับแหล่งที่มาของความแข็งแกร่งทางอำนาจ แต่เกี่ยวข้องกับความสามารถในการเป็นจุดศูนย์กลางของโครงสร้างหรือระบบ ที่มีความจำเป็นอย่างยิ่งต่อทั้งทุกด้านของโครงสร้าง และเป็นจุดยึดเหนี่ยวให้โครงสร้างเหล่านั้นยังสามารถดำรงอยู่ได้ด้วยกัน ซึ่งแนวคิดจุดศูนย์กลางของแรงโน้มถ่วงของ Clausewitz เน้นไปทางการศึกษาผลกระทบที่เกิดขึ้น และผลจากการล่มสลายของศัตรู มากกว่าการศึกษาความสามารถต่างๆในการทำสงคราม ซึ่งสอดคล้องกับแนวคิด Effects-Based Operations (EBO) (Elbaum, 2008)

Clausewitz สนับสนุนรูปแบบการทำสงครามโดยการโจมตีจุดศูนย์กลางของแรงโน้มถ่วง ซึ่งสามารถสรุปแนวคิดของเขาได้ดังนี้ “สงครามคือการแสดงออกของการใช้กำลัง และไม่มีขีดจำกัดใดในการใช้กำลังเหล่านั้น”, “จุดมุ่งหมายสูงสุดของการกระทำการทางการทหารทั้งหมดคือเพื่อเอาชนะศัตรู” และ “การทำลายล้างศัตรูคือสิ่งที่สำคัญที่สุดเสมอ” แนวคิดจุดศูนย์กลางแรงโน้มถ่วงและการทำสงครามแบบเบ็ดเสร็จ (Absolute war) คือสิ่งที่สำคัญเป็นอย่างมากต่ออำนาจไซเบอร์ แม้การโจมตีเป้าหมายในโลกไซเบอร์จะไม่สามารถฆ่าศัตรูได้โดยตรง แต่สามารถกระทำการปลิดชีพฝ่ายตรงข้ามได้โดยอ้อม หรือการยึดดินแดนต่างๆ

การใช้แนวคิดของ Clausewitz ในการเปรียบเทียบอำนาจทางไซเบอร์ที่สามารถสร้างผลกระทบต่อปัจจัยต่างๆที่เป็นจุดศูนย์กลางของระบบโครงสร้างที่สามารถเข้าถึงได้โดยใช้ไซเบอร์ เช่น ระบบการเงิน, ระบบเศรษฐกิจ, และฐานข้อมูลต่างๆ และผู้ที่กระทำการโจมตี ต้องเตรียมพร้อมสำหรับผลกระทบที่เป็น

อันตรายต่อประชากรในประเทศที่เป็นเป้าหมายการโจมตีด้วยเช่นกัน อำนาจไซเบอร์สามารถเป็นเครื่องมือที่ใช้ในการชนะสงคราม แต่หากใช้ในการโจมตีที่เฉพาะเจาะจง หรือโจมตีเป้าหมายที่เป็นวงแคบมากยิ่งขึ้น การใช้ไซเบอร์ในการโจมตีจะมีประสิทธิภาพมากยิ่งขึ้น

การโจมตีทางไซเบอร์โดยใช้แนวคิดจุดศูนย์กลางแรงโน้มถ่วงของ Clausewitz สามารถแบ่งตัวแสดง และประเภทออกได้เป็น 3 ประเภท ดังตาราง 1 (Elbaum, 2008)

Actor Center of Gravity Dependence

Actor Category \ Cyber COG	Financial	Economic	Informational
Capitalistic Superpower	●	●	○
Communist Superpower	◎	◎	◎
Average Dictatorship	◎	○	◎
Average Democracy	●	◎	○
Terrorist Organization	◎	○	●
Drug Cartel	●	○	○
Third World	○	○	○

○ = Little to no dependance ◎ = Moderate dependance ● = Heavy dependance

ตาราง 1 ตัวแสดงที่ได้รับผลกระทบจากแนวคิดจุดศูนย์กลางแรงโน้มถ่วง
ที่มา: Elbaum (2008)

การเปรียบเทียบการใช้แนวคิดจุดศูนย์กลางแรงโน้มถ่วงในโลกไซเบอร์ การโจมตีฐานข้อมูลจะมีประโยชน์เป็นอย่างมากในการโจมตีประเทศที่มีโอกาสเกิดการรัฐประหาร, การปฏิวัติ, หรือประเทศล้มละลาย ในการสร้างมายาคติหรือการสร้างโฆษณาชวนเชื่อเพื่อสร้างความวุ่นวายในสังคม เช่นเดียวกัน การโจมตีเศรษฐกิจหรือระบบการเงิน คือสิ่งที่สามารถสร้างผลกระทบได้อย่างมากต่อประเทศที่พึ่งพาโลกไซเบอร์ในการเคลื่อนย้ายผ่านระบบทางการเงิน เช่นระบบบัญชีธนาคาร

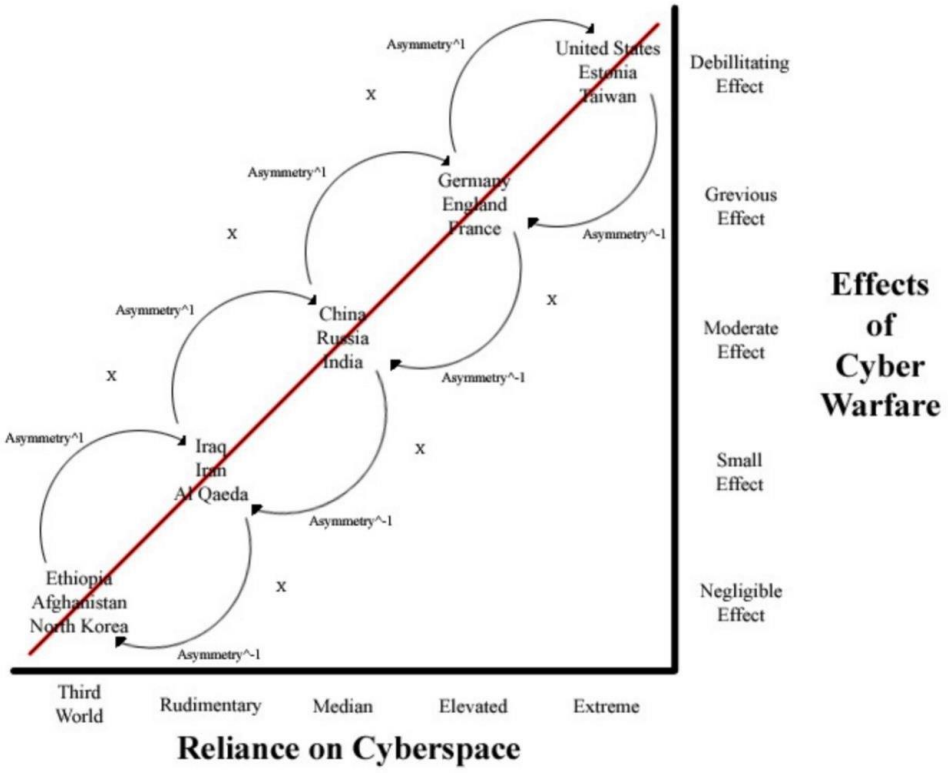
ข้อมูลจากตารางที่ 1 ข้อมูลตารางทางด้านซ้าย แสดงให้เห็นถึงประเภทตัวแสดงที่ได้มีส่วนเชื่อมโยงกับแนวคิดจุดศูนย์กลางแรงโน้มถ่วงที่เกี่ยวข้องกับไซเบอร์ เรียงลำดับจากมากไปถึงน้อย ยกตัวอย่าง เช่น ประเทศมหาอำนาจที่ปกครองแบบทุนนิยม เช่น ประเทศสหรัฐอเมริกา การโจมตีจุด

ศูนย์กลางของระบบการเงินและเศรษฐกิจ จะสร้างผลกระทบอย่างมากต่อประเทศ แต่การโจมตีเพื่อบิดเบือนข้อมูล, การโจมตีโดยใช้การสร้างมายาคติ, หรือการสร้างความไม่เชื่อใจต่อรัฐบาลหรือประเทศนั้นส่งผลกระทบน้อยกว่ามาก โดยเฉพาะประเทศที่มีรัฐบาลที่มีประวัติศาสตร์อย่างยาวนานในการก่อตั้งจากประชากรของประเทศนั้นๆ

การโจมตีจุดศูนย์กลางผ่าน 3 ปัจจัยที่กล่าวมาในประเทศสาธารณรัฐประชาชนจีนที่มีโปรแกรมตรวจจับข้อมูลการใช้งานอินเทอร์เน็ตของประชาชนที่เข้มงวดและรัดกุมที่ถูกยินยอมให้เผยแพร่ข้อมูลเฉพาะข้อมูลที่ได้รับการอนุญาตเท่านั้นจากผู้นำประเทศ การโจมตีข้อมูลที่สร้างความวุ่นวายในประเทศอาจจะไม่สามารถสร้างผลกระทบใดๆได้เลย และ ในขณะเดียวกัน การโจมตีจุดศูนย์กลางของระบบเศรษฐกิจของประเทศจีน อาจสร้างความเสียหายได้เพียงบางส่วน เพราะประเทศจีนเป็นประเทศที่มีอัตราส่วนการผลิตอุตสาหกรรมและการเกษตรเป็นส่วนใหญ่ และการโจมตีจุดศูนย์กลางทางการเงินก็อาจสร้างความเสียหายได้บางส่วนเช่นกัน เนื่องจากการปกครองในรูปแบบสังคมนิยมคอมมิวนิสต์นั้น การทำงานของประชากรคือการทำงานเพื่อส่วนรวมโดยไม่ได้ค่าตอบแทนที่แตกต่างกัน

องค์กรก่อการร้าย เป็นตัวแสดงที่ได้รับผลกระทบจากการถูกโจมตีจุดศูนย์กลางระบบการเงินในระดับกลาง เนื่องจากบัญชีทางการเงินได้ถูกกระจายไปยังหลากหลายประเทศ และหลากหลายบัญชี จึงยากที่จะทำการโจมตีได้ แต่อย่างไรก็ตาม องค์กรก่อการร้าย Al Qaeda ยังคงสามารถสร้างการโจมตีได้โดยไม่จำเป็นต้องใช้เงินทุนในการโจมตี เพราะ Al Qaeda ได้ใช้ความเชื่อทางศาสนาในการสร้างการโจมตีขึ้นมา และในส่วนของการโจมตีระบบเศรษฐกิจขององค์กรก่อการร้าย ไม่ถือว่าได้รับผลกระทบใดๆ เนื่องจากองค์กรก่อการร้ายไม่ได้ทำการค้าขายหรือผลิตใดๆระหว่างกัน แต่การโจมตีเข้าสู่จุดศูนย์กลางข้อมูล สามารถสร้างความรุนแรงได้อย่างมาก เนื่องจากองค์กรก่อการร้ายเกิดจากแนวคิดอุดมคติและมายาคติที่สร้างอำนาจให้พวกเขาเหล่านั้น

นอกจากแนวคิดการโจมตีจุดศูนย์กลางแรงโน้มถ่วง ที่เป็นการโจมตีเพื่อสร้างผลกระทบเชิงโครงสร้างแล้วนั้น ยังมีข้อมูลที่สำคัญต่อการศึกษาความมั่นคงทางไซเบอร์ด้วยเช่นกัน ดังตาราง 2



ตาราง 2 ผลกระทบที่ไม่สมมาตรจากสงครามไซเบอร์

ที่มา: Elbaum (2008)

ตาราง 2 แสดงให้เห็นถึงความสัมพันธ์ของความเสียหายที่เกิดจากการโจมตีเป้าหมายในโลกไซเบอร์ โดยใช้ตัวแสดงเป็นระดับประเทศ ซึ่งชี้ให้เห็นว่า ประเทศโลกที่สามที่พึ่งพาโลกไซเบอร์เพียงน้อยนิด หรือโลกไซเบอร์แทบจะไม่มีบทบาทในการจัดการในประเทศนั้นๆ การโจมตีทางไซเบอร์จะส่งผลกระทบเพียงน้อยนิดต่อประเทศเหล่านั้น ส่วนประเทศที่มีอัตราส่วนประชากรที่อาศัยอยู่ในชนบทจำนวนมากที่เข้าถึงโลกไซเบอร์ได้อย่างจำกัด อาทิเช่น จีน, รัสเซีย และ อินเดีย การโจมตีไซเบอร์เข้าสู่ประเทศเหล่านี้ จะส่งผลกระทบเพียงบางส่วน แต่จะไม่สามารถส่งผลกระทบระดับประเทศที่ส่งผลต่อการล้มละลายหรือสร้างความเสียหายอย่างมากได้ ส่วนประเทศที่มีความพัฒนาทางด้านเทคโนโลยีขั้นสูง และเป็นประเทศที่ใช้การเชื่อมโยงโครงสร้างพื้นฐานโดยใช้สายเคเบิลหรือสายต่างๆ อาทิเช่น ประเทศสหรัฐอเมริกา, เอสโทเนีย และ ไต้หวัน คือประเทศที่มีส่วนเกี่ยวข้องแทบทั้งหมดของประเทศในโลกไซเบอร์ ดังนั้น การโจมตีจุดศูนย์กลางทางไซเบอร์ จะสามารถสร้างความเสียหายได้อย่างมากต่อประเทศเหล่านี้

หากเรานำตารางทั้งสองมาวิเคราะห์ จะทำให้เห็นถึงความสำคัญของการใช้ไซเบอร์ในการโจมตีเข้าสู่จุดศูนย์กลางของแรงโน้มถ่วง หรือเป็นการโจมตีจุดศูนย์กลางของโครงสร้าง ที่สามารถส่งผลกระทบร้ายแรงต่อโครงสร้างทางการเมือง การเงิน และเศรษฐกิจได้ โดยเฉพาะประเทศที่มีความสัมพันธ์กับโลกไซเบอร์ ก็จะสามารถได้รับผลกระทบจากการโจมตีได้มากกว่าประเทศที่มีความสัมพันธ์กับโลกไซเบอร์น้อย

กว่า และจากตารางที่สอง ที่เป็นตารางเกี่ยวกับผลกระทบที่ไม่สมมาตรจากการโจมตีของโลกไซเบอร์ ทำให้เราวิเคราะห์ได้ว่า ประเทศที่เป็นโลกที่สาม หรือประเทศที่กำลังพัฒนา สามารถสร้างความเสียหายอย่างมากให้กับประเทศที่พึ่งพาโลกไซเบอร์ หรือประเทศที่ใช้โลกไซเบอร์ในขั้นตอนที่สำคัญของประเทศต่างๆ ไม่ว่าจะเป็นโครงสร้างพื้นฐาน การบริหารจัดการ หรือ การทหาร ทำให้ต้นทุนในการดูแลรักษา การพัฒนาวิจัย และองค์ความรู้ทางวิทยาศาสตร์ของประเทศเหล่านี้ จะมีต้นทุนที่สูงมากในการป้องกันโลกไซเบอร์ และบางครั้งอาจมาจากการโจมตีโดยใช้คอมพิวเตอร์โน๊ตบุคมือสอง และโค้ดที่สามารถดาวน์โหลดได้ในโลกไซเบอร์เพื่อทำการโจมตีแบบง่ายๆ

เอกสารและงานวิจัยที่เกี่ยวข้อง

ไซเบอร์ในศตวรรษที่ 21

เทคโนโลยีได้กลายเป็นปัจจัยที่มีความสำคัญมากยิ่งขึ้นในศตวรรษที่ 21 โดยเฉพาะในด้านขอบเขตความมั่นคงแห่งชาติ โดยในงานของ Andrea Monti & Raymond Wacks (2021) ได้แสดงให้เห็นถึงบทบาทความสำคัญ และผลกระทบของเทคโนโลยีที่ส่งผลกระทบต่อทางด้านการเมือง อำนาจ และสิทธิส่วนบุคคล รวมถึงการวิเคราะห์ไปยังความสัมพันธ์ของเทคโนโลยีที่มีส่วนเกี่ยวข้องกับการปรับเปลี่ยนรูปแบบนโยบายสาธารณะให้มีความแตกต่างไปจากอดีต ซึ่งแสดงให้เห็นถึงข้อจำกัดของความเข้าใจแบบดั้งเดิมของนโยบายสาธารณะ ความมั่นคงแห่งชาติ และ หลักกฎหมาย ที่เทคโนโลยีดิจิทัลได้เข้ามามีบทบาททำให้เห็นช่องว่างที่สามารถสร้างผลกระทบต่อการบริหารจัดการสาธารณะและผลกระทบที่สามารถสร้างความโกลาหลให้กับสังคม อย่างไรก็ตาม เทคโนโลยีก็ถือว่าเป็นปัจจัยที่สามารถทำให้ประเทศที่กำลังพัฒนา สามารถก้าวข้ามกลายเป็นประเทศที่มีการพัฒนาตามหลังประเทศที่พัฒนาแล้วได้อย่างรวดเร็ว ดังในงานของ Cecilia Rikap & Bengt-Åke Lundvall (2021) ได้กล่าวถึงการที่การปฏิวัติเทคโนโลยีคือสิ่งที่สัมพันธ์กันกับความเป็นผู้นำระดับโลก โดยได้มีการยกตัวอย่างจากงานของ Christopher Freeman (2007) ที่ได้กล่าวถึงพัฒนาการของเทคโนโลยีและระบบนวัตกรรมของประเทศ (The National Innovation System (NIS)) โดยในศตวรรษที่ 18 ระบบนวัตกรรมของประเทศอังกฤษ ได้พัฒนาคุณลักษณะของนวัตกรรมของประเทศที่มีนวัตกรรมพลังไอน้ำและการถักทอผ้าทำให้ได้กลายเป็นประเทศที่มีอำนาจ ณ ขณะนั้น ในเวลาต่อมา เมื่อนวัตกรรมเทคโนโลยีได้แปรเปลี่ยนกลายเป็นการใช้ไฟฟ้าและความรู้ทางด้านเคมี ประเทศเยอรมนีและสหรัฐอเมริกาได้กลายเป็นประเทศมหาอำนาจแทนที่ประเทศอังกฤษ

การพัฒนานวัตกรรมทางเทคโนโลยี คือ ปัจจัยที่สามารถทำให้ประเทศที่ล้าหลัง สามารถก้าวกระโดดกลายเป็นประเทศมหาอำนาจได้อย่างชัดเจน งานของ Yan Xuetong (2020) ได้ทำการศึกษาการแข่งขันของระบบสองขั้วอำนาจในยุคเริ่มต้นทางเทคโนโลยี โดยเป็นการให้ความสำคัญกับประเทศสหรัฐอเมริกาและจีน ในการแข่งขันของสองขั้วอำนาจที่มีความแตกต่างจากระบบสองขั้วอำนาจสมัย

สงครามเย็น ซึ่งในสมัยสงครามเย็นเป็นการแข่งขันทางด้านอุดมการณ์แต่ ณ ปัจจุบัน การแข่งขันพัฒนาการดิจิทัลก่อให้เกิดการแข่งขันทางกลยุทธ์ระหว่างสหรัฐอเมริกาและจีน การพัฒนาทางเทคโนโลยีดิจิทัลนำมาสู่การสร้างการป้องกันความมั่นคงรูปแบบใหม่ การสะสมความมั่งคั่งแห่งชาติจากพัฒนาการทางเทคโนโลยี และการกระจายเทคโนโลยีที่แพร่หลายสู่ระบบนานาประเทศ ความมั่นคงทางไซเบอร์ได้กลายมาเป็นส่วนหลักของความมั่นคงแห่งชาติและส่วนแบ่งทางเศรษฐกิจดิจิทัลได้กลายมาเป็นอำนาจทางเศรษฐกิจจากสินค้าดิจิทัลที่เพิ่มมากขึ้นอย่างมีในนัยสำคัญ การแข่งขันเชิงกลยุทธ์ทางไซเบอร์ได้กลายมาเป็นกลยุทธ์ที่ล้ำหน้ามากกว่าการแข่งขันทางด้านขอบเขตทางกายภาพ

การเสริมสร้างองค์ความรู้เพื่อผลิตบุคลากรเกี่ยวกับเทคโนโลยีไซเบอร์ คือสิ่งที่พัฒนาอย่างรวดเร็วในศตวรรษที่ 21 Oktavianto & Sibarani (2024) ได้ทำการศึกษาเกี่ยวกับการสร้างความตระหนักรู้ที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา ในช่วง ค.ศ. 2009 ถึง ค.ศ. 2024 ชี้ให้เห็นถึงพัฒนาการทางด้านการศึกษาไซเบอร์ใน 3 เนื้อหาสำคัญที่ได้รับความสนใจ คือ 1. นโยบายทางด้านการศึกษาและนวัตกรรมเกี่ยวกับความมั่นคงทางไซเบอร์ 2. การศึกษาการตระหนักรู้ความมั่นคงไซเบอร์ในบริบทต่างๆ เช่น ภายในโรงเรียน โรงพยาบาล และภาคประชาสังคม 3. การศึกษาเกี่ยวกับแนวคิดและกระบวนการสอนทางด้านความมั่นคงทางไซเบอร์ แสดงให้เห็นถึงการสนับสนุนทางด้านการศึกษาเกี่ยวกับไซเบอร์อย่างต่อเนื่อง และเพิ่มขึ้นอย่างมีนัยสำคัญในช่วง ค.ศ. 2020 ถึง ค.ศ. 2024 และหากมองในแง่ของการแข่งขันในบทบาทของการสร้างความมั่นคงทางไซเบอร์ การแข่งขันทางด้านการศึกษาก็เป็นปัจจัยที่เห็นได้อย่างชัดเจนเช่นกัน

ปัจจัยที่สัมพันธ์กับการเพิ่มขึ้นของการศึกษาเกี่ยวกับไซเบอร์ ในอีกนัยหนึ่ง เป็นผลมาจากวิกฤตการแพร่ระบาดของ COVID-19 Mahmood et al. (2024) ได้ทำการศึกษาความท้าทายความมั่นคงทางไซเบอร์ในช่วงการแพร่ระบาดของ COVID-19 ผลการศึกษาพบว่า มีการเพิ่มขึ้นของภัยคุกคามไซเบอร์อย่างมีนัยสำคัญ เนื่องจากการกักตัว การเปลี่ยนแปลงของสภาพแวดล้อมในการทำงาน และการหลีกเลี่ยงการพบปะของผู้คน ทำให้การพึ่งพาเทคโนโลยี และ อินเทอร์เน็ตมีมากขึ้น โดยความเสียหายที่เกิดขึ้น เกิดจาก 5 ปัจจัยด้วยกัน ดังนี้ 1. ปัจจัยทางด้านสังคม หมายถึง การขาดความตระหนักรู้ของสังคม 2. ปัจจัยทางด้านระบบและเทคนิค หมายถึง การถูกโจมตีไซเบอร์ผ่านช่องโหว่ทางเทคโนโลยีต่างๆ 3. ปัจจัยทางด้านการเมืองและกฎหมาย หมายถึง ความล้าสมัยของระบบกฎหมายไซเบอร์ และการขาดมาตรการในการรับมือผลกระทบที่เกิดจากความมั่นคงทางไซเบอร์ 4. ปัจจัยทางด้านเศรษฐกิจ หมายถึง การขาดงบประมาณและทรัพยากรมนุษย์ในการรองรับการสร้างความมั่นคงทางไซเบอร์ 5. ปัจจัยทางด้านสิ่งแวดล้อม หมายถึง อุปกรณ์ที่ใช้ในสาธารณะถูกโจมตี เช่น เครือข่าย Wi-Fi หรือการโจมตีจากตัวแสดงที่ไม่ใช่รัฐ เช่นกลุ่มแฮกเกอร์

การเติบโตและพัฒนาอย่างรวดเร็วของไซเบอร์ ทั้งทางด้านการใช้งานและการโจมตี ในแง่ของความสัมพันธ์ระหว่างประเทศในศตวรรษที่ 21 ได้รับผลกระทบเช่นกัน ในการศึกษาของ Rehman &

Rassias (2024) ได้ทำการศึกษาเกี่ยวกับภัยคุกคามทางไซเบอร์ที่ส่งผลต่อความมั่นคงระหว่างประเทศในแง่ทางการทูต ทั้งในรูปแบบของการโจมตีทางไซเบอร์ การจารกรรมข้อมูล และการบิดเบือนข้อมูลต่างๆ สร้างผลกระทบต่อการไว้วางใจในแง่ของความสัมพันธ์ระหว่างประเทศ อีกทั้งยังสร้างอุปสรรคต่อการเจรจาต่อรองข้องตกลงต่างๆด้วยเช่นกัน อีกทั้งการพัฒนาทางไซเบอร์ ได้สร้างการแข่งขันทางไซเบอร์ ก่อให้เกิดความขัดแย้งทางด้านความสัมพันธ์ระหว่างประเทศ อาทิเช่น การที่ประเทศสหรัฐได้มีข้อขัดแย้งต่างๆกับประเทศอื่นๆ ไม่ว่าจะเป็นประเทศจีน ในกรณีการจารกรรมข้อมูล และประเทศรัสเซีย ในกรณีการแทรกแซงผลการเลือกตั้งในปี ค.ศ. 2016 และประเทศเกาหลีเหนือ ในกรณีการโจมตีบริษัท Sony Pictures ส่งผลให้เกิดการตอบโต้ด้วยนโยบายทางการทูต อาทิเช่น นโยบายการคว่ำบาตรทางเศรษฐกิจ หรือ การตอบโต้ด้วยปฏิบัติการไซเบอร์ ในสถานการณ์ดังกล่าวที่เกิดขึ้น ชี้ให้เห็นถึงการไม่มีกฎหมายสากลที่สามารถบังคับใช้ในข้อขัดแย้งที่ชัดเจน ก่อให้เกิดความท้าทายในความขัดแย้งที่เกิดขึ้นในโลกไซเบอร์ สำหรับการแก้ไขปัญหาต่างๆที่เกิดขึ้น ผลกระทบต่างๆนำไปสู่ความขัดแย้งทางการเมืองระหว่างประเทศ การทำลายความเชื่อมั่นระหว่างประเทศ นำไปสู่การไม่ร่วมมือทางการทูตต่างๆ

ไซเบอร์ได้ถูกใช้เป็นเครื่องมือในการแสวงหาผลประโยชน์ ตอบสนองความต้องการ และ ถูกใช้เป็นเครื่องมือเพื่อสร้างความเสียหายมากยิ่งขึ้น โดยเฉพาะในช่วงศตวรรษที่ 21 โดย John Shier (2020) ได้ศึกษาถึงปรากฏการณ์ภัยทางไซเบอร์ในระยะเวลาระหว่าง ค.ศ. 2000 ถึง ค.ศ. 2020 โดยแบ่งแยกภัยทางไซเบอร์ตามยุคสมัย แบ่งช่วงเวลาโดยเริ่มต้นจาก ค.ศ. 2000-2004 ใช้การนิยามว่าเป็นช่วงเวลาของยุคไวรัสหนอน หมายถึง ช่วงเวลาที่ไวรัสหนอนระบาด สร้างความเสียหายต่อเศรษฐกิจเป็นมูลค่ากว่าหลายพันล้านดอลลาร์ และสร้างผลกระทบต่อระบบการทำงานของเครือข่ายอย่างกว้างขวาง และเป็นสาเหตุหนึ่งที่ทำให้บริษัท Microsoft ได้เริ่มต้นอัปเดตระบบแบบรายเดือน ลำดับถัดมาคือช่วงเวลาระหว่าง ค.ศ. 2005-2012 คือยุคแห่งอาชญากรรมทางไซเบอร์ หมายถึง ยุคเริ่มต้นของอาชญากรรมทางไซเบอร์ที่มีแรงจูงใจในการสร้างความเสียหายทางการเงิน อาทิเช่น การระบาดของสแปม บอทเน็ต และมัลแวร์ที่ขโมยข้อมูลธนาคารต่างๆ และช่วงเวลาระหว่าง ค.ศ. 2013 จนถึงปัจจุบัน เป็นยุคแห่งแรนซัมแวร์ หมายถึง การระบาดของแรนซัมแวร์ที่กลายเป็นภัยคุกคามทางไซเบอร์ที่สร้างผลกระทบร้ายแรงมากที่สุดในปัจจุบัน รวมถึงการใช้สกุลเงินดิจิทัล หรือ คริปโตเคอเรนซี่ ในการชำระเงิน เพื่อให้หลีกเลี่ยงการจับตัวจากทางภาครัฐ และภัยคุกคามระดับสูง (APT) รวมถึงเครื่องมือที่ถูกใช้งานจากทางภาครัฐ เริ่มถูกกลุ่มอาชญากรนำไปใช้งาน โดยผู้วิจัยได้เรียงลำดับเหตุการณ์ รวมถึงการอธิบายแบบสรุปในแต่ละเหตุการณ์ดังนี้

1. เหตุการณ์สำคัญในยุคไวรัสหนอน (The Worm Era ค.ศ. 2000 ถึง ค.ศ. 2004)

   ILOVEYOU ค.ศ. 2000 เป็นเหตุการณ์แพร่กระจายไวรัสผ่านอีเมล์ด้วยการส่งไฟล์แนบเพื่อให้เหยื่อเปิดใช้งาน

   CodeRed ค.ศ. 2001 เป็นเหตุการณ์กระจายไวรัสผ่านช่องโหว่ IIS ของ Microsoft ซึ่งเป็นการทำให้เว็บไซต์ดังกล่าวถูกเปลี่ยนหน้า (Defacement)

SQL Slammer ค.ศ. 2003 เป็นเหตุการณ์ที่ไวรัสหนอนได้เข้าถึงช่องโหว่ของ Microsoft SQL Server และทำให้เครือข่ายดังกล่าวล่มภายใน 10 นาที

Blaster ค.ศ. 2003 เป็นเหตุการณ์โจมตีทางไซเบอร์ต่อระบบปฏิบัติการ Windows XP/2000 ผ่านระบบ RPC Service

MyDoom ค.ศ. 2004 เป็นเหตุการณ์ที่ไวรัสหนอนแพร่กระจายรวดเร็วมากที่สุดในประวัติศาสตร์ ซึ่งมีการแพร่กระจายของไวรัสถึงอัตราส่วนร้อยละ 25 ของอีเมล์ทั้งหมดใน ค.ศ. 2004

2. เหตุการณ์สำคัญในยุคแห่งอาชญากรรมทางไซเบอร์ (The Monetization Era ค.ศ. 2005 ถึง ค.ศ. 2012)

Storm Botnet ค.ศ. 2007 เป็นหนึ่งในบอทเน็ตที่ใหญ่ที่สุด และมีประสิทธิภาพเทียบเท่ากับซุปเปอร์คอมพิวเตอร์ในช่วงเวลานั้น

Zeus ค.ศ. 2007 เป็นมัลแวร์ขโมยข้อมูลระบบธนาคารและเป็นจุดเริ่มต้นของการบริการอาชญากรรม หรือ Crimeware as a service

Conficker ค.ศ. 2008 เป็นไวรัสหนอนคอมพิวเตอร์ที่เกิดการแพร่ระบาดสู่คอมพิวเตอร์จำนวน 15 ล้านเครื่องทั่วโลก

Stuxnet ค.ศ. 2010 เป็นมัลแวร์ที่ใช้งานในการโจมตีโรงงานนิวเคลียร์ของประเทศอิหร่าน และถือเป็นจุดเริ่มต้นของ สงครามไซเบอร์ หรือ Cyber Warfare

Blackhole Exploit Kit ค.ศ. 2010 เป็นชุดเครื่องมือที่มีไว้สำหรับการโจมตีช่องโหว่ของเบราว์เซอร์เว็บไซต์และซอฟต์แวร์ยอดนิยมต่างๆ

3. เหตุการณ์สำคัญในยุคแห่งแรนซัมแวร์ (The Ransomware Era ค.ศ. 2013 ถึงปัจจุบัน)

Snowden Leaks ค.ศ. 2013 เป็นการเปิดโปงโครงการสอดแนมของหน่วยงานความมั่นคงสหรัฐอเมริกา หรือ NSA และเป็นช่วงที่ทำให้เกิดการตั้งรหัสเพื่อเข้าข้อมูลมากยิ่งขึ้น

CryptoLocker ค.ศ. 2013 เป็นแรนซัมแวร์ยุคใหม่ที่ใช้การเข้ารหัสไฟล์ต่างๆและเรียกค่าไถ่โดยใช้ Bitcoin

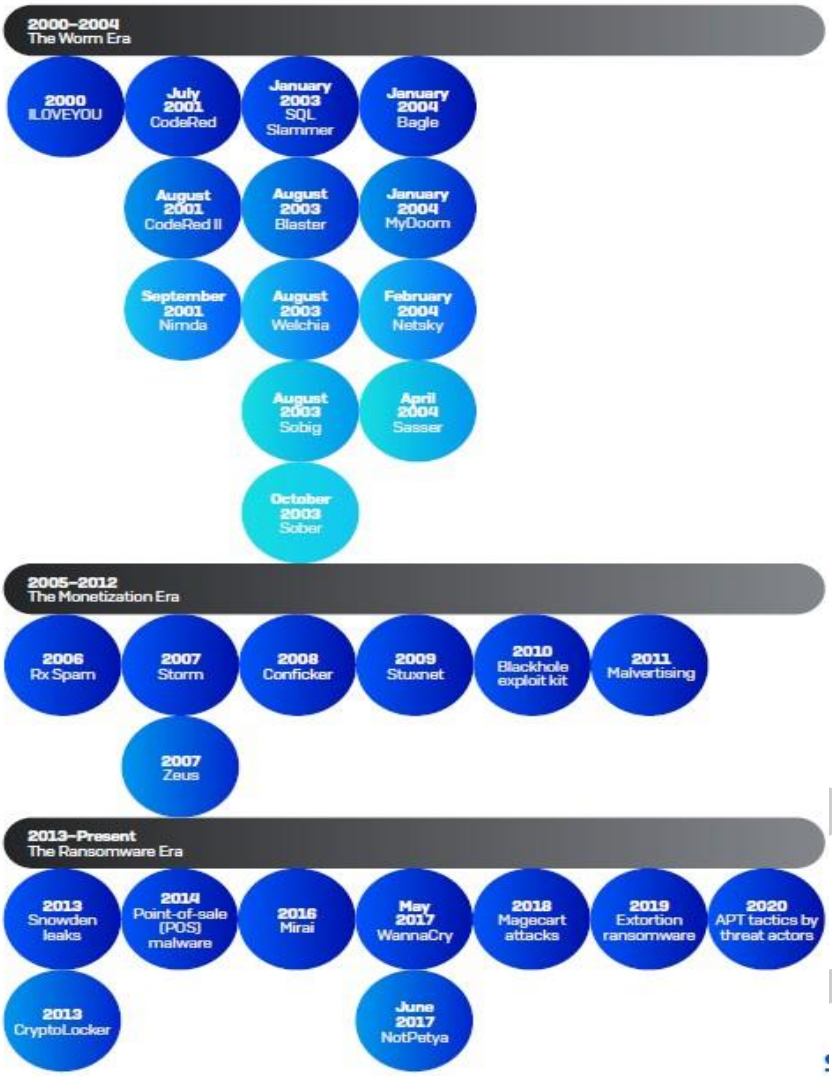
Mirai Botnet ค.ศ. 2016 เป็นการใช้ IoT Devices ในการโจมตี DDoS ที่รุนแรงที่สุดในช่วงนั้น

Wannacry ค.ศ. 2017 เป็นแรนซัมแวร์แบบไวรัสหนอนที่ใช้ช่องโหว่ของ EternalBlue ของหน่วยงานความมั่นคงสหรัฐ หรือ NSA ในการแพร่กระจาย

NotPetya ค.ศ. 2018 เป็นมัลแวร์ที่มีเป้าหมายคือการทำลายข้อมูล

Magecart ค.ศ. 2018 เป็นการโจมตีโดยการใช้ Web Skimming เพื่อขโมยข้อมูลบัตรเครดิตจากเว็บไซต์ต่างๆ

Double Extortion Ransomware ค.ศ. 2019 เป็นเทคนิคเรียกค่าไถ่ด้วยการขู่ว่าจะปล่อยข้อมูลเหยื่อ ดังภาพประกอบ 2.3 (Shier, 2020)



ภาพประกอบ 8 ลำดับเหตุการณ์ภัยร้ายทางไซเบอร์ในศตวรรษที่ 21 (ค.ศ. 2000 ถึง 2020)
ที่มา: John Shier (2020)

การโจมตีทางไซเบอร์ในขอบเขตระหว่างประเทศ และเป็นการโจมตีที่เข้าสู่องค์กรภาครัฐ บริษัทเทคโนโลยีขนาดใหญ่ และการก่ออาชญากรรมทางเศรษฐกิจ ที่ส่งผลกระทบหลายล้านดอลลาร์

เกิดขึ้นอย่างต่อเนื่องในช่วงศตวรรษที่ 21 โดยการรวบรวมข้อมูลจากรายงานของ Center for Strategic and International Studies (CSIS) (n.d.) ที่ได้รวบรวมการโจมตีทางไซเบอร์ตั้งแต่ ค.ศ. 2003 จนถึงปัจจุบัน ซึ่งมีการโจมตีเกิดขึ้นเป็นจำนวนมาก รวมถึงการโจมตีระหว่างประเทศที่สร้างผลกระทบต่อภาคอุตสาหกรรมด้วยจุดประสงค์ต่างๆ ที่มีการรวบรวมข้อมูลจากงานของ Andrew Ginter (2018) แสดงให้เห็นถึงความเสียหายที่เกิดจากการโจมตีทางไซเบอร์ต่อภาคอุตสาหกรรมและเป็นงานที่ชี้ให้เห็นถึงข้อผิดพลาดของการประมาณค่าการโจมตีทางไซเบอร์ที่ต่ำเกินไปของภาคอุตสาหกรรม สามารถส่งผลกระทบอย่างมากต่อความเสียหายที่เกิดขึ้นจากเหตุการณ์ต่างๆ

เหตุการณ์การโจมตีทางไซเบอร์ต่อสถาบันการเงิน คือส่วนหนึ่งที่สามารถสร้างความเสียหายต่อเศรษฐกิจโดยตรง โดยจากการค้นคว้าในรายงานของ Carnegie endowment. (n.d.) ที่มีการรวบรวมเหตุการณ์การโจมตีทางไซเบอร์ต่อสถาบันทางการเงินมากกว่า 200 เหตุการณ์ และในช่วงที่ผ่านมา การโจมตีทางไซเบอร์ต่อสถาบันการเงินมีแนวโน้มที่จะอันตรายและยากที่จะควบคุมมากยิ่งขึ้น โดยเฉพาะการโจมตีทางไซเบอร์ที่มีการสนับสนุนจากภาครัฐบาลในการโจมตีเพื่อจุดประสงค์ทางการเมือง ที่มีการพัฒนาความสามารถในการโจมตีอย่างต่อเนื่องในทุกๆปี

การโจมตีทางไซเบอร์สามารถกระทำได้อย่างง่ายดาย และพัฒนาการทางเทคโนโลยีที่พัฒนาอย่างรวดเร็ว ส่งผลให้การโจมตีทางไซเบอร์เพิ่มความรุนแรงมากยิ่งขึ้น และการควบคุมที่เป็นไปได้ยาก เนื่องจากสภาวะความเป็นอนาธิปไตยของโลกไซเบอร์ที่ไร้ผู้ควบคุมและยากที่จะกำหนดกฎเกณฑ์ต่างๆ การศึกษาการใช้เทคโนโลยีไซเบอร์และภัยคุกคามที่เกิดจากกลุ่มก่อการร้ายโดย คณะกรรมการต่อต้านการก่อการร้ายแห่งสหประชาชาติ หรือ United Nations Security Council Counter-Terrorism Committee (2025) ที่ชี้ให้เห็นถึงการเปลี่ยนแปลงของรูปแบบการก่อการร้ายผ่านความเป็นอนาธิปไตยของโลกไซเบอร์ ความก้าวหน้าทางเทคโนโลยีส่งเสริมให้กลุ่มก่อการร้ายสามารถใช้ประโยชน์จากโลกไซเบอร์ จากสมัยก่อนที่การก่อการร้ายจำเป็นต้องพึ่งพาอาวุธที่สงวนไว้ใช้สำหรับกองทัพเท่านั้น แต่ปัจจุบันการก่อการร้ายสามารถกระทำได้ เพียงแค่มีอินเทอร์เน็ต โซเชียลมีเดีย และอุปกรณ์อิเล็กทรอนิกส์ รวมถึงการใช้สื่อโซเชียลมีเดียในการเผยแพร่แนวคิดและสร้างความขัดแย้งให้กับสังคมซึ่งส่งผลต่อความสัมพันธ์ระหว่างประเทศ

ความไร้พรมแดนของความเป็นอนาธิปไตยในโลกไซเบอร์ ส่งผลกระทบต่อความเป็นอธิปไตยของรัฐ จากการศึกษาของ Paul Timmers (2024) เรื่องความท้าทายที่เกิดขึ้นกับอำนาจอธิปไตยของรัฐจากภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นในปัจจุบัน จากความเป็นอนาธิปไตยของโลกไซเบอร์ที่ไม่สามารถควบคุมได้ และได้เสนอแนวคิดเกี่ยวกับการรักษาอำนาจอธิปไตยของรัฐ อาทิเช่น แนวคิดกลยุทธ์ในการปกครองตนเอง ประกอบด้วยยุทธศาสตร์ทั้งหมด 4 วิธี คือ 1. การพึ่งพารัฐของตนเองโดยไม่พึ่งพาปัจจัยภายนอก (Autarky) 2. การบริหารจัดการความเสี่ยง (Risk Management) 3. การสร้างพันธมิตรเชิงกลยุทธ์ที่มีแนวคิดไปทางเดียวกัน (Strategic Partnerships) 4. การสร้างความร่วมมือระดับโลกในการ

บริหารจัดการเชิงนโยบาย เช่น การสร้างนโยบายการป้องกันภัยคุกคามทางไซเบอร์ และ การเปลี่ยนแปลงของสภาพภูมิอากาศในระดับโลก หรือ ภาวะโลกร้อน Paul Timmers ได้ศึกษาถึงการเปลี่ยนแปลงของอำนาจอธิปไตยที่ได้รับผลกระทบจากเทคโนโลยีไซเบอร์ โดยได้ทำการแยกอำนาจอธิปไตยออกเป็น 3 รูปแบบ คือ 1. อำนาจอธิปไตยเชิงพื้นที่ หมายถึง การเพิ่มขึ้นของทรัพย์สินทางดิจิทัล เช่น การเพิ่มขึ้นของข้อมูลประชากร และ โครงสร้างพื้นฐานทางไซเบอร์ 2. อำนาจอธิปไตยเชิงสถาบัน หมายถึง พัฒนาการทางด้านเทคโนโลยี เช่น เทคโนโลยีปัญญาประดิษฐ์ (A.I.) และเทคโนโลยี Blockchain 3. อำนาจอธิปไตยเชิงโครงสร้างพื้นฐาน หมายถึง การมีบริษัทเทคโนโลยีขนาดใหญ่ เช่น บริษัท Google และ Facebook ที่มีอำนาจทางด้านข้อมูลมากยิ่งขึ้น ดังนั้น Paul Timmers จึงได้เสนอนโยบายสำหรับการควบคุมอำนาจอธิปไตยในยุคไซเบอร์ไว้ว่า 1. การออกกฎหมายเพื่อควบคุมเทคโนโลยี 2. การกำหนดมาตรฐานความปลอดภัยทางไซเบอร์ที่ใช้งานในกระบวนการต่างๆ ทั้งด้านเศรษฐกิจ สังคม และการทหาร 3. การสนับสนุนการพัฒนาอุตสาหกรรมเทคโนโลยีไซเบอร์แห่งชาติ เพื่อลดการพึ่งพาบริษัทต่างชาติ

จากการทบทวนวรรณกรรม ข้อมูลเอกสาร เกี่ยวกับไซเบอร์ในศตวรรษที่ 21 สามารถแยกประเภทของงานวิจัยได้ ดังนี้

ลำดับ	หัวข้อการศึกษา	ปีการศึกษา	แหล่งที่มา	ประเภทการศึกษา
1	ผลกระทบของเทคโนโลยีต่อการเมือง อำนาจ และสิทธิส่วนบุคคล	2021	Andrea Monti & Raymond Wacks	ผลกระทบจากไซเบอร์
2	การปฏิวัติเทคโนโลยีกับความเป็นผู้นำระดับโลก	2021	Cecilia Rikap & Bengt-Åke Lundvall	บทบาทความเป็นผู้นำของเทคโนโลยีระดับโลก
3	การแข่งขันของระบบสองขั้วอำนาจทางเทคโนโลยี	2020	Yan Xuetong	การเปรียบเทียบการแข่งขันทางเทคโนโลยี

4	การสร้างความตระหนักรู้เกี่ยวกับความมั่นคงทางไซเบอร์ของสหรัฐฯ	2024	Oktavianto & Sibarani	การศึกษาการตระหนักรู้ความมั่นคงทางไซเบอร์
ลำดับ	หัวข้อการศึกษา	ปีการศึกษา	แหล่งที่มา	ประเภทการศึกษา
5	ความท้าทายความมั่นคงทางไซเบอร์ในช่วง COVID-19	2024	Mahmood et al.	ผลกระทบทางไซเบอร์ในช่วง Covid-19
6	ภัยคุกคามทางไซเบอร์ต่อความยคุกคามทางไซเบอร์ที่ส่งผลต่อความมั่นคงระหว่างประเทศในแง่ทางการทูตระหว่างประเทศ	2024	Rehman & Rassias	วิเคราะห์ภัยความมั่นคงไซเบอร์ทางการทูต
7	ภัยทางไซเบอร์ในช่วง ค.ศ. 2000-2020	2020	John Shier	วิเคราะห์ภัยคุกคามทางไซเบอร์
8	การรวบรวมการโจมตีทางไซเบอร์ตั้งแต่ ค.ศ. 2003 จนถึงปัจจุบัน	n.d.	Center for Strategic and International Studies (CSIS)	รวบรวมข้อมูลการโจมตีทางไซเบอร์
9	การรวบรวมเหตุการณ์การโจมตีทางไซเบอร์ต่อสถาบันทางการเงินมากกว่า 200 เหตุการณ์	n.d.	Carnegie endowment	ศึกษาการโจมตีไซเบอร์ต่อสถาบันการเงิน
10	การเปลี่ยนแปลงของรูปแบบการก่อการร้ายผ่านความเป็นอนาธิปไตยของโลกไซเบอร์	2025	United Nations Security Council Counter-	การวิเคราะห์วิวัฒนาการของกลุ่มก่อการร้ายในโลกไซเบอร์

			Terrorism Committee	
11	ความท้าทายที่เกิดขึ้นกับอำนาจอธิปไตยของรัฐ จากภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นในปัจจุบัน	2024	Paul Timmers	ศึกษาผลกระทบของภัยคุกคามไซเบอร์ต่ออำนาจอธิปไตยของรัฐ

ตาราง 3 ตารางประเภทงานวิจัยที่เกี่ยวข้อง
ที่มา: ผู้วิจัย

ตาราง 3 แสดงให้เห็นถึงประเภทของงานวิจัยที่เกี่ยวข้องจากการทบทวนวรรณกรรม ข้อมูลเอกสาร ซึ่งเอกสารงานวิจัยส่วนมาก จะมุ่งเน้นไปที่เนื้อหาการศึกษาไซเบอร์ ไม่ว่าจะเป็นนิยามไซเบอร์ รูปแบบการวิเคราะห์ไซเบอร์ การวิเคราะห์ไซเบอร์ทางด้านภัยคุกคาม การวิเคราะห์ไซเบอร์ในเชิงนโยบายของผู้นำประเทศ และเชิงนโยบายความสัมพันธ์ระหว่างประเทศ ผลกระทบที่เกิดจากไซเบอร์ทั้งภายในประเทศและความสัมพันธ์ระหว่างประเทศ สงครามไซเบอร์ การโจมตีทางไซเบอร์ ความมั่นคงทางไซเบอร์ การศึกษาปรากฏการณ์ทางไซเบอร์ในช่วงทศวรรษที่ 21 และจากการทบทวนวรรณกรรมและเอกสารงานวิจัยที่เกี่ยวข้อง ผู้วิจัยได้เล็งเห็นช่องว่างการวิจัย หรือ Research Gap ดังนี้

1. การศึกษาความเป็นอนาธิปไตยของโลกไซเบอร์ มีความท้าทายอย่างไรต่อความสัมพันธ์ระหว่างประเทศ
2. การศึกษาทางด้านความเป็นมหาอำนาจไซเบอร์ที่วิเคราะห์จากอำนาจทางการทหาร เทคโนโลยี และวิทยาศาสตร์
3. การศึกษาความเป็นผู้นำทางไซเบอร์ของประเทศสหรัฐอเมริกาผ่านแนวคิดสมองของโลก (Global Brain) ที่การเชื่อมโยงเครือข่ายและการสื่อสารส่งผลประทบอย่างไรต่อความสัมพันธ์ระหว่างประเทศ

งานวิจัยชิ้นนี้ จึงต้องการศึกษาเพื่อทำให้ทราบถึงความท้าทายที่เกิดขึ้นจากความเป็นอนาธิปไตยทางไซเบอร์ต่อความสัมพันธ์ระหว่างประเทศ แนวทางในการวิเคราะห์ความเป็นมหาอำนาจทางไซเบอร์ผ่านการใช้รูปแบบการวิเคราะห์ไซเบอร์ และการศึกษาความเป็นผู้นำทางไซเบอร์ที่มีรากฐานทางไซเบอร์ผ่านแนวคิดสมองของโลก กรณีศึกษา ประเทศสหรัฐอเมริกา ในศตวรรษที่ 21 เพื่อเป็นแนวทางในการศึกษาผลกระทบที่สามารถเกิดขึ้นโลกไซเบอร์ในทศวรรษที่ 21 ผ่านตัวแสดงที่มีความเป็นผู้นำและมีวิวัฒนาการทางไซเบอร์มาอย่างยาวนาน

บทที่ 3
วิธีดำเนินการวิจัย

งานวิจัยเรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ : สหรัฐอเมริกา ในศตวรรษที่ 21 เป็นงานวิจัยเชิงคุณภาพ (Qualitative Research) ผู้วิจัยทำการศึกษาและค้นคว้าผ่านวิธีการดำเนินการวิจัย ดังต่อไปนี้

1. หน่วยวิเคราะห์
2. เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล
3. การเก็บรวบรวมข้อมูล
4. การจัดกระทำกับข้อมูลและวิเคราะห์ข้อมูล

หน่วยวิเคราะห์

องค์กรที่มีส่วนเกี่ยวข้องกับความมั่นคงทางไซเบอร์ ดังนี้

1. หน่วยงานภาครัฐที่มีบทบาทต่อความมั่นคงทางไซเบอร์
    - กระทรวงกลาโหมสหรัฐ (Department of Defense (DOD)) เพราะ มีหน้าที่โดยตรงต่อความมั่นคงแห่งชาติ
    - กองบัญชาการไซเบอร์แห่งประเทศสหรัฐอเมริกา (U.S. Cyber Command (USCYBERCOM)) เพราะ มีหน้าที่โดยตรงต่อความมั่นคงไซเบอร์แห่งชาติ
    - สำนักงานความมั่นคงแห่งชาติ (National Security Agency (NSA)) เพราะมีหน้าที่ในการดูแลและปกป้องโครงสร้างพื้นฐานสำคัญของประเทศ
2. ฝ่ายบริหารของรัฐบาลและผู้กำหนดนโยบาย
    - ประธานาธิบดีแห่งประเทศสหรัฐอเมริกา เพราะ เป็นตัวแสดงที่มีบทบาทสำคัญในการกำหนดนโยบายและจัดตั้งหน่วยงานที่เกี่ยวกับความมั่นคงทางไซเบอร์
3. ภาคเอกชนและหน่วยงานเกี่ยวข้องกับเทคโนโลยี
    - บริษัทเทคโนโลยีที่เกี่ยวข้องกับไซเบอร์ เช่น Google, Microsoft, Amazon, Sony และ Facebook เพราะ มีส่วนเกี่ยวข้องโดยตรงต่อกิจกรรมต่างๆที่เกิดขึ้นในโลกไซเบอร์ รวมถึงความเสียหายจากการโจมตีไซเบอร์ด้วยเช่นกัน
    - บริษัทที่เกี่ยวข้องกับโครงสร้างพื้นฐาน เช่น บริษัททางด้านพลังงาน และสถาบันการเงิน โรงพยาบาล เพราะได้รับผลกระทบทางไซเบอร์โดยตรง

4. องค์กรระหว่างประเทศ

- NATO Cooperative Cyber Defence Centere of Excellence (CCDCOE) เพราะ เป็นหน่วยงานที่ให้ความรู้และสร้างการป้องกันภัยคุกคามทางไซเบอร์ให้กับประเทศพันธมิตรต่างๆ
- United Nations (UN) และ European Union (EU) เพราะ มีการกำหนดนโยบายไซเบอร์ระหว่างประเทศ

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

งานวิจัยฉบับนี้เป็นการวิจัยข้อมูลแบบการวิจัยเชิงเอกสาร (Documentary Research) โดยเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งใช้ข้อมูลจากการศึกษาเอกสารชั้นปฐมภูมิและทุติยภูมิ มีการใช้เครื่องมือในการเก็บรวบรวมข้อมูลวิจัยดังต่อไปนี้

1. แหล่งข้อมูลชั้นปฐมภูมิ (Primary Sources)
   - เอกสารทางการและนโยบายของรัฐบาลสหรัฐอเมริกา ที่มีความเกี่ยวข้องกับความมั่นคงทางไซเบอร์ เช่น นโยบายความมั่นคงทางไซเบอร์, นโยบายหรือคำสั่งโดยตรงจากทำเนียบขาวและประธานาธิบดี, กลยุทธ์ทางไซเบอร์ของกระทรวงกลาโหม
   - เอกสารทางการขององค์กรระหว่างประเทศ เช่น International Telecommunication Union (ITU) และ North Atlantic Treaty Organization (NATO)
   - ข้อมูลการรวบรวมการโจมตีทางไซเบอร์และภัยความมั่นคงทางไซเบอร์ที่เผยแพร่จากหน่วยงานรัฐ
   - ข้อมูลที่ได้รับการเผยแพร่จากเว็บไซต์ทางการของหน่วยงานที่เกี่ยวข้องกับความมั่นคงไซเบอร์ เช่น US Cyber Command (USCYBERCOM) และ National Security Agency (NSA)
2. แหล่งข้อมูลชั้นทุติยภูมิ (Secondary Sources)
   - วิเคราะห์เอกสารวิชาการและบทความที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์
   - หนังสือที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

- ข้อมูลที่มีความเกี่ยวข้องกับเหตุการ์หรือปรากฏการ์ความมั่นคงทางไซเบอร์ เช่น การโจมตีทางไซเบอร์ หรือ ผลกระทบทางไซเบอร์ที่ส่งผลต่อความสัมพันธ์ระหว่างประเทศ

การเก็บรวบรวมข้อมูล

ผู้วิจัยใช้การเก็บรวบรวมข้อมูลแบบงานวิจัยเชิงคุณภาพ (Qualitative Research) ทั้งจากเอกสารชั้นปฐมภูมิและชั้นทุติยภูมิ โดยมีวิธีการดังนี้

1. การสืบค้นเอกสารออนไลน์ (Database Search)
   - ใช้การค้นหาด้วย คำค้นหา (Keywords) ที่มีความเกี่ยวข้องกับความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา ความท้าทายทางไซเบอร์ในศตวรรษที่ 21 ผลกระทบจากความมั่นคงทางไซเบอร์ต่อความสัมพันธ์ระหว่างประเทศ เช่น U.S. Cybersecurity, Cybersecurity, Cybersecurity in 21st century, Cyber Challenges และ Cyber and International Politics
   - ใช้เครื่องมือการค้นหาข้อมูล เช่น Google Scholar, Research Gate และ E-IR เพื่อการเข้าถึงเอกสารวิชาการที่น่าเชื่อถือ
   - ค้นหาแหล่งข้อมูลจากเว็บไซต์ทางการ เช่น ทำเนียบขาว (White House), กระทรวงกลาโหมสหรัฐ (DoD) และหน่วยงานด้านความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา เช่น NSA และ USCYBERCOM
2. การวิเคราะห์เอกสาร (Data Analysis)
   - วิเคราะห์ข้อมูลสำคัญที่เกี่ยวข้องกับงานวิจัย เช่น ความมั่นคงทางไซเบอร์ ความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา ความท้าทายทางไซเบอร์ ความท้าทายของประเทศมหาอำนาจ ความมั่นคงทางไซเบอร์ในศตวรรษที่ 21 และการวิเคราะห์ความมั่นคงไซเบอร์
   - วิเคราะห์โดยการอ้างอิงจากงานวิชาการ และแหล่งข้อมูลที่เป็นทางการ
3. การเปรียบเทียบและสังเคราะห์เอกสาร (Comparative and Synthesis Approach)
   - เปรียบเทียบและวิเคราะห์แหล่งข้อมูลชั้นปฐมภูมิและทุติยภูมิเพื่อการเห็นข้อมูลที่มีความครอบคลุม

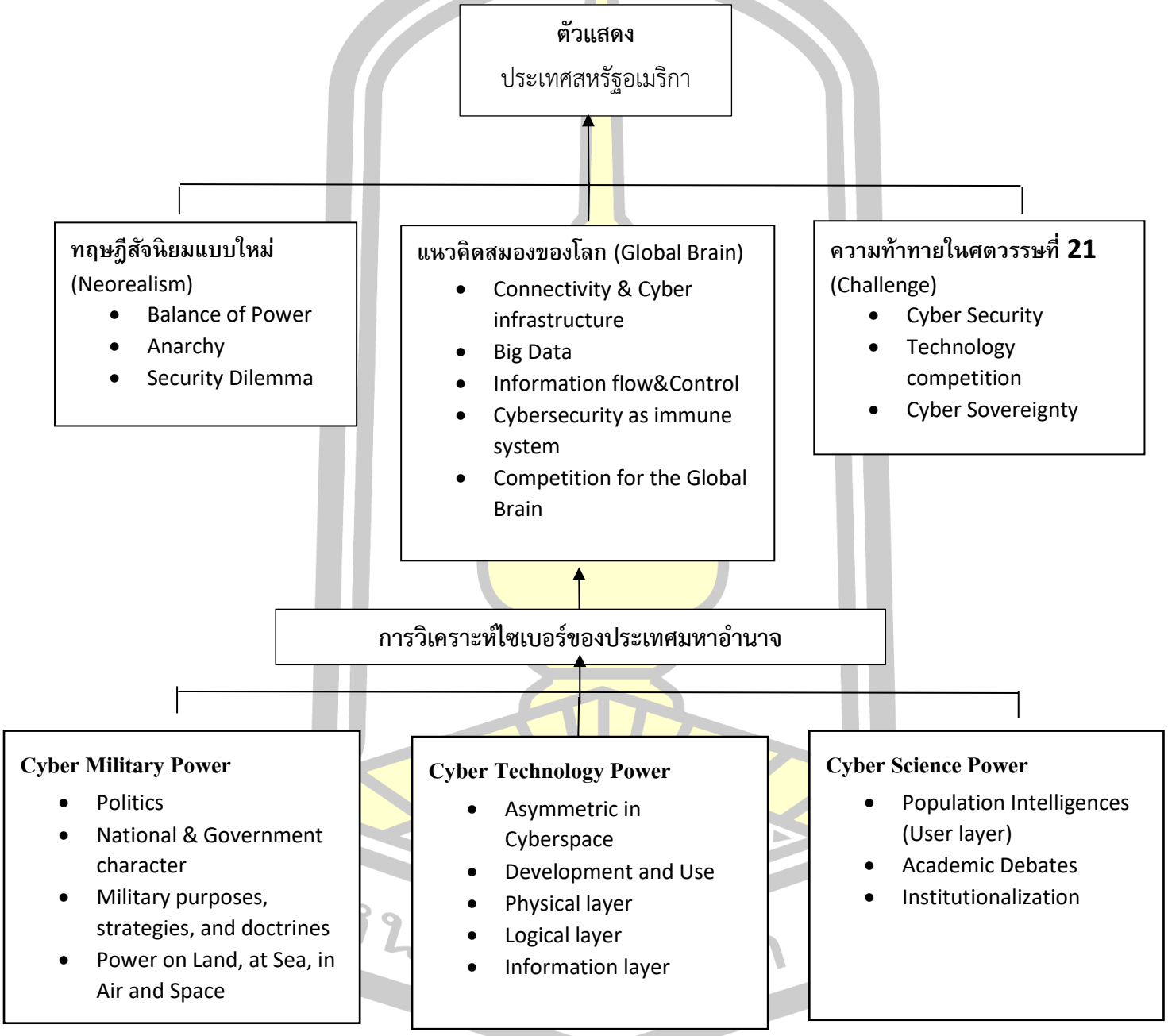
- วิเคราะห์ความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกาในระดับนานาชาติและความท้าทายของบทบาทประเทศสหรัฐอเมริกาในศตวรรษที่ 21

การจัดกระทำกับข้อมูลและการวิเคราะห์ข้อมูล

งานวิจัยเรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศสหรัฐอเมริกา ในศตวรรษที่ 21 ผู้วิจัยวิเคราะห์โดยใช้ทฤษฎีสัจนิยมใหม่ (Neorealism) เป็นทฤษฎี/แนวคิดหลักในการวิเคราะห์ถึงความท้าทายทางไซเบอร์ที่เกิดขึ้นต่อประเทศสหรัฐอเมริกา ในศตวรรษที่ 21 และแนวคิดสมองของโลก (Global Brain) เป็นทฤษฎี/แนวคิดรองในการวิเคราะห์ลักษณะการใช้งานไซเบอร์ของประเทศสหรัฐอเมริกา โครงสร้างความมั่นคงทางไซเบอร์ และผลกระทบที่เกิดจากการใช้งานไซเบอร์เพื่อวิเคราะห์ความพยายามในการเป็นสมองของโลกของประเทศสหรัฐอเมริกา จากนั้นวิเคราะห์ความท้าทายที่เกิดจากความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่ส่งผลต่อความสัมพันธ์ระหว่างประเทศ แล้วจึงนำข้อมูลมาวิเคราะห์เพื่อหาข้อสรุปถึงความมั่นคงทางไซเบอร์ระหว่างประเทศสหรัฐอเมริกา ในศตวรรษที่ 21

กรอบแนวคิดการวิจัย

ผู้วิจัยนำเสนอเป็นกรอบแนวคิดการวิจัยเรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกา ในศตวรรษที่ 21



ภาพประกอบ 9 กรอบแนวคิดการวิจัย

ที่มา: ปรับประยุกต์จาก Myriam Dunn Cavelty และ Andreas Wenger (2020), David Clark (2010)

จากกรอบแนวคิดภาพประกอบ 4 ผู้วิจัยขออธิบายตัวแปรที่เลือกใช้เพื่อใช้วิเคราะห์รายละเอียด ดังนี้

การวิเคราะห์ตัวแสดงหลัก คือ ประเทศสหรัฐอเมริกา ซึ่งเป็นประเทศที่มีบทบาทสำคัญในโลกไซเบอร์ และเป็นประเทศที่มีเทคโนโลยีไซเบอร์ที่ก้าวหน้าอันดับ 1 ของโลก ที่ต้องเผชิญต่อความท้าทายในศตวรรษที่ 21

กรอบแนวคิดทฤษฎีสัจนิยมใหม่ ที่นำมาวิเคราะห์การแข่งขันระหว่างประเทศมหาอำนาจในมิติของไซเบอร์ มุ่งเน้นวิเคราะห์ไปยัง สมดุลแห่งอำนาจ (Balance of Power) เพื่อวิเคราะห์ความพยายามรักษาดุลแห่งอำนาจของประเทศสหรัฐอเมริกา ด้วยการกำหนดนโยบายและกฎหมายเพื่อรักษาสถานะความเป็นประเทศมหาอำนาจ การวิเคราะห์ความเป็นอนาธิปไตย (Anachy) เพราะในโลกไซเบอร์นั้น ไม่มีการควบคุมจากศูนย์กลางหรือหน่วยงานใด ทำให้การแข่งขันระหว่างรัฐมีความรุนแรงมากยิ่งขึ้น และสภาวะกลืนไม่เข้าคายไม่ออกทางด้านความมั่นคง (Security Dilemma) คือผลลัพธ์ที่เกิดจากความกังวลในการเมืองระหว่างประเทศ ที่ต่างรัฐต่างระแวงกัน ทำให้เกิดความไม่เชื่อใจกันและกันในการพัฒนาไซเบอร์

การวิเคราะห์โดยใช้แนวคิดสมองของโลก ช่วยอธิบายถึงพฤติกรรมของประเทศสหรัฐอเมริกา ในความพยายามเป็นสมองของโลก ผ่านปัจจัยในกรอบแนวคิด ไม่ว่าจะเป็นการวิเคราะห์ การเชื่อมต่อและโครงสร้างพื้นฐานทางไซเบอร์ (Connectivity & Cyber Infrastructure) ที่ศึกษาถึงโครงสร้างพื้นฐานทางไซเบอร์และการเชื่อมต่อของประเทศ ข้อมูลจำนวนมาก (Big Data) คือความได้เปรียบทางไซเบอร์ การนำปัจจัยนี้มาวิเคราะห์ จะช่วยให้เราเข้าใจถึงการรวบรวมข้อมูล และการนำข้อมูลเหล่านั้นมาวิเคราะห์เพื่อสร้างความได้เปรียบทางไซเบอร์ได้เป็นอย่างดี การศึกษาการไหลเวียนของข้อมูลและการควบคุม (Information Flow & Control) คือการนำข้อมูลที่วิเคราะห์ได้มาใช้เพื่อผลประโยชน์ทางการเมือง อาทิเช่น การออกนโยบายทางไซเบอร์ การสร้างการป้องกันเพื่อความมั่นคงทางไซเบอร์เปรียบเสมือนระบบภูมิคุ้มกันของร่างกาย (Cybersecurity as Immune System) ที่จะทำหน้าที่ป้องกันโครงสร้างพื้นฐานทางไซเบอร์ เฉกเช่นระบบภูมิคุ้มกันที่ป้องกันร่างกายจากเชื้อโรคต่างๆ และการศึกษาการแข่งขันเพื่อการเป็นสมองของโลก (Competition for the Global Brain) คือการศึกษาแนวทางของประเทศมหาอำนาจที่แข่งขันกันเพื่อการเป็นสมองของโลก

ความท้าทายในศตวรรษที่ 21 คือการวิเคราะห์เพื่อให้เห็นถึงสิ่งที่เป็นปัจจัยสำคัญที่สร้างผลกระทบให้กับความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ไม่ว่าจะเป็นการศึกษาความมั่นคงทางไซเบอร์ การแข่งขันทางด้านเทคโนโลยี และความเป็นอธิปไตยทางไซเบอร์ที่สร้างการแบ่งขั้วอำนาจในศตวรรษที่ 21

การวิเคราะห์ความมั่นคงทางไซเบอร์ผ่านกลยุทธ์การโจมตีหรือการทำสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ เป็นการศึกษาอำนาจไซเบอร์ทางการทหารของประเทศ (Cyber Military Power) การวิเคราะห์การโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ รวมถึงการวิเคราะห์นโยบายความมั่นคงทางไซเบอร์ โครงสร้างทางการทหาร และการใช้เทคโนโลยีทางไซเบอร์ในการทำสงคราม

ประสิทธิภาคของเทคโนโลยี คือปัจจัยสำคัญในการวิเคราะห์อำนาจไซเบอร์ทางเทคโนโลยีที่ศึกษาการครอบครองเทคโนโลยีต่างๆ ที่ถูกใช้ในทางยุทธศาสตร์ การสร้างความได้เปรียบในโลกไซเบอร์ในหลากหลายลำดับชั้น ไม่ว่าจะเป็น Physical layer Logical layer และ Information layer และการใช้ไซเบอร์เพื่อสร้างนโยบายที่ได้เปรียบต่อประเทศคู่แข่งที่มีประสิทธิภาพที่น้อยกว่าประเทศตนเอง

องค์ความรู้ทางวิทยาศาสตร์ คือสิ่งที่สร้างอำนาจทางไซเบอร์ให้มีความมั่นคงและยั่งยืน การศึกษาอำนาจทางไซเบอร์ทางด้านวิทยาศาสตร์ คือสิ่งสำคัญในการวิเคราะห์ความสามารถของประชากรที่มีความเชี่ยวชาญเกี่ยวกับไซเบอร์ การสนับสนุนของรัฐบาลในการสร้างสถาบันวิจัย และการสร้างหน่วยงานเพื่อพัฒนาและถ่ายทอดองค์ความรู้ให้กับประชาชน และนำองค์ความรู้ที่เกิดขึ้นมาพัฒนาเป็นนโยบายเพื่อใช้ในการสร้างความได้เปรียบในโลกไซเบอร์ในความสัมพันธ์ระหว่างประเทศ

กรอบแนวคิดของงานวิจัยฉบับนี้ เป็นกรอบแนวคิดที่ใช้วิเคราะห์ความมั่นคงทางไซเบอร์ของประเทศมหาอำนาจ กรณีศึกษาในงานวิจัยนี้ คือประเทศสหรัฐอเมริกา ในศตวรรษที่ 21 ได้อย่างครอบคลุม โดยเป็นการเชื่อมโยงในแง่มุมของทางการเมือง เทคโนโลยี และวิทยาศาสตร์ การใช้ทฤษฎีสัจนิยมใหม่ เพื่ออธิบายการแข่งขันทางไซเบอร์ระหว่างประเทศ แนวคิดสมองของโลก จะช่วยอธิบายกลยุทธ์ของประเทศสหรัฐอเมริกาในความพยายามควบคุมโครงสร้างพื้นฐานทางไซเบอรในระดับนานาชาติ ความท้าทายในศตวรรษที่ 21 คือการวิเคราะห์อุปสรรคที่ประเทศสหรัฐอเมริกต้องเผชิญไม่ว่าจะเป็น ความมั่นคงทางไซเบอร์ การแข่งขันทางเทคโนโลยี และความพยายามในการรักษาอธิปไตยทางไซเบอร์ และการวิเคราะห์อำนาจทางไซเบอร์ทั้ง 3 ด้าน ไม่ว่าจะเป็นทางการทหาร เทคโนโลยี และวิทยาศาสตร์ ทำให้การใช้กรอบแนวคิดนี้ สามารถมองเห็นภาพรวมของการแข่งขันไซเบอร์ในการเมืองระหว่างประเทศ และบทบาทของประเทศสหรัฐอเมริกาในการรักษาดุลแห่งอำนาจทางไซเบอร์ในศตวรรษที่ 21

บทที่ 4

ความเป็นอนาธิปไตยในโลกไซเบอร์ที่ท้าทายอำนาจของประเทศสหรัฐอเมริกา

ความเป็นอนาธิปไตยของโลกไซเบอร์ ได้เข้ามามีบทบาทมากยิ่งขึ้นจากการเพิ่มขึ้นของการใช้งานในศตวรรษที่ 21 เป็นพื้นที่ใช้งานที่มีความซับซ้อนและไร้ขอบเขต ส่งผลให้รัฐต่างๆไม่สามารถควบคุมโลกไซเบอร์ได้โดยสมบูรณ์ ทำให้โลกไซเบอร์ถูกให้นิยามให้เป็นพื้นที่ ที่มีความเป็นอนาธิปไตย และเป็นสิ่งที่สร้างความท้าทายให้ประเทศสหรัฐอเมริกา ผู้เป็นประเทศมหาอำนาจทางไซเบอร์ ความเป็นอนาธิปไตยของโลกไซเบอร์ เมื่อนำกรอบแนวคิดสัจนิยมใหม่มาอธิบาย จะทำให้เห็นถึงความท้าทายต่างๆที่เกิดขึ้นได้อย่างชัดเจนต่อประเทศสหรัฐอเมริกา โดยแนวคิดสัจนิยมใหม่ ได้อธิบายว่าโครงสร้างการเมืองระหว่างประเทศมีความเป็นอนาธิปไตย ไม่มีอำนาจจากส่วนกลางในการควบคุมด้วยกฎหมายของรัฐใดรัฐหนึ่ง ซึ่งหากเปรียบเทียบความเป็นอนาธิปไตยของโลกไซเบอร์ ผ่านแนวคิดสัจนิยมใหม่ที่สร้างความท้าทายต่อประเทศสหรัฐอเมริกา ทำให้โลกไซเบอร์ถูกวิเคราะห์ถึงการมีลักษณะ ดังนี้

1. โลกไซเบอร์เป็นสิ่งที่ไร้ผู้ควบคุมโลกอินเทอร์เน็ต หมายถึง การที่อินเทอร์เน็ตเป็นรูปแบบเครือข่ายที่ไร้พรมแดนทางกฎหมาย รัฐบาลของประเทศสหรัฐอเมริกาไม่สามารถเข้าควบคุมการใช้งานและปิดกั้นข้อมูลต่างๆจากทั่วโลกได้ทั้งหมด ถึงแม้ว่าประเทศสหรัฐอเมริกาจะเป็นประเทศที่มีบทบาทสำคัญในโลกไซเบอร์ก็ตาม แต่การปิดกั้นการโจมตีจากทั่วโลกเป็นสิ่งที่ไม่สามารถหลีกเลี่ยงได้ เพราะในปัจจุบัน รัฐบาลต่างๆทั่วโลกต่างมีการใช้งานโลกไซเบอร์ในหลากหลายด้าน ไม่ว่าจะเป็นการติดตามประชาชน เช่น การสอดแนมระบบโทรคมนาคม การดักฟังข้อมูล รวมถึงการเก็บข้อมูลออนไลน์ที่เกี่ยวข้องกับพฤติกรรมของประชาชน อีกทั้งการฝึกใช้งานไซเบอร์เพื่อโจมตีและแฮ็กข้อมูล ซึ่งเป็นปัญหาใหญ่ในการเมืองระหว่างประเทศ และการที่กลุ่มก่อการร้ายมีการใช้มัลแวร์ และการเจาะระบบเพื่อเข้าโจมตีหรือขโมยข้อมูลความลับต่างๆของรัฐบาล หรือการโจมตีเข้าสู่โครงสร้างพื้นฐานสำคัญที่ต้องพึ่งพาโลกไซเบอร์ ภาคเอกชนที่เข้ามามีบทบาทสำคัญของประเทศสหรัฐอเมริกา เช่น Google, Facebook และ บริษัทอื่นๆที่มีความเกี่ยวข้องกับการเป็นส่วนสำคัญของโลกไซเบอร์ ได้ถูกคุมคามจากการโจมตีด้วยเช่นกัน แต่ภาคเอกชนเหล่านี้ ก็ได้รับผลกระทบจากรัฐบาลประเทศสหรัฐอเมริกา จากนโยบายทางภาครัฐ ที่บังคับให้บริษัทจำเป็นต้องเปิดเผยข้อมูลของประชาชนให้มีความโปร่งใส เพื่อหลีกเลี่ยงการคุกคามข้อมูลส่วนตัว การไร้ผู้ควบคุมในโลกไซเบอร์ ได้สร้างการเคลื่อนไหวทางการเมืองผ่านกลุ่มนักเคลื่อนไหวดิจิทัล หรือกลุ่ม แฮ็กทิวิสต์ ไม่ว่าจะเป็นกลุ่ม Anonymous หรือ Citizen Lab ที่มีการเคลื่อนไหวเพื่อปกป้องสิทธิเสรีภาพทางด้านความเป็นส่วนตัวและเสรีภาพในการใช้งานโลกไซเบอร์ แต่ในทางกลับกัน ทางภาครัฐก็ได้มีนโยบายในการเฝ้าระวังการใช้งานโลกไซเบอร์ต่อประชาชน ทำให้การเฝ้าระวังต่างๆ ไม่สามารถกำหนดขอบเขตได้ และเสี่ยงต่อการละเมิดสิทธิเสรีภาพในการแสดงออกด้วยเช่นกัน อาทิเช่น การที่รัฐบาลเฝ้าระวังข้อมูล

เกี่ยวกับการเลือกตั้งและการจำกัดการเข้าถึงข้อมูลของประชาชน ดังนั้น ความเป็นอนาธิปไตยของโลกไซเบอร์ที่ไร้คนกลางในการควบคุม สามารถมองได้ทั้งการเป็นเครื่องมือที่ส่งเสริมความเป็นประชาธิปไตย และการเป็นเครื่องมือกดขี่ประชาชน ขึ้นอยู่ที่สถานการณ์ของรัฐบาล ณ ขณะนั้น (Deibert, 2013)

2. โลกไซเบอร์เป็นสิ่งที่ทำให้ความมั่นคงอยู่ในสภาวะกลืนไม่เข้าคายไม่ออก (Security Dilemma) หมายถึง การที่ประเทศสหรัฐอเมริกาเป็นประเทศมหาอำนาจทางไซเบอร์ และมีการพัฒนาองค์ความรู้เทคโนโลยีไซเบอร์อย่างต่อเนื่อง ทำให้ประเทศสหรัฐอเมริกามีระบบการป้องกันประเทศทางไซเบอร์ที่แข็งแกร่ง แต่กลับทำให้ประเทศอื่นๆไม่ว่าจะเป็นประเทศพันธมิตรกับประเทศสหรัฐอเมริกาหรือไม่ก็ตาม ได้มีการพัฒนาเทคโนโลยีไซเบอร์เพื่อป้องกันการโจมตีจากประเทศสหรัฐอเมริกาด้วยเช่นกัน การเพิ่มขีดความสามารถทางไซเบอร์เป็นสิ่งที่ถูกมองว่าเป็นภัยคุกคาม เนื่องจากการตรวจสอบความโปร่งใสในการพัฒนาที่เป็นไปได้ยาก ว่าการพัฒนาเหล่านั้นถูกพัฒนาไปเพื่อสิ่งใด ซึ่งมีความแตกต่างจากการพัฒนาขีปนาวุธ หรือเรือรบต่างๆ ทำให้เกิดความกังวลจากฝ่ายตรงข้ามของศักยภาพทางไซเบอร์ของประเทศสหรัฐอเมริกา อีกทั้งการโจมตีทางไซเบอร์ในโลกไซเบอร์ที่เป็นอนาธิปไตย สามารถกระทำได้ทุกเวลา ทำให้รัฐอื่นๆไม่สามารถคาดการณ์ได้ว่าจะถูกโจมตีทางไซเบอร์เมื่อไหร่ ส่งผลให้เกิดความพยายามในการพัฒนาศักยภาพในการป้องกันทางไซเบอร์ของประเทศตนเอง อาทิเช่น การที่ประเทศสหรัฐอเมริกามีการลงทุนทางด้านการสร้างหน่วยงานไซเบอร์ (USCYBERCOM) เพื่อพัฒนาการโจมตีทางไซเบอร์และศักยภาพการป้องกันทางไซเบอร์ ส่งผลให้ประเทศจีน และประเทศรัสเซีย เร่งสร้างหน่วยสงครามไซเบอร์ของประเทศตนเอง และได้ส่งผลกลับให้ประเทศสหรัฐอเมริกามีการเพิ่มงบประมาณทางด้านความมั่นคงทางไซเบอร์มากยิ่งขึ้น ความครุกรุ่นทางการแข่งขันการพัฒนาศักยภาพทางไซเบอร์ดังกล่าว อาจนำไปสู่สภาวะการสร้างความมั่นคงที่ทำให้เกิดความไม่มั่นคง หรือ Security Paradox ที่กลายเป็นการแข่งขันการสะสมอาวุธทางไซเบอร์ของแต่ละประเทศ เสี่ยงทำให้เกิดสงครามไซเบอร์อย่างไม่ตั้งใจเกิดขึ้นได้ อีกทั้งความเสี่ยงทางด้านการยกระดับความขัดแย้งทางไซเบอร์ หรือ Cyber Escalation ที่สามารถทำให้การโจมตีทางไซเบอร์มีความรุนแรงมากขึ้นจากความขัดแย้งต่างๆ เช่น การโจมตีที่ส่งผลต่อพลเรือนโดยตรง อาจยกระดับการตอบโต้ทางไซเบอร์ทำให้เกิดสงครามที่รุนแรง และเป็นผลมาจากการที่โลกไซเบอร์ขาดการควบคุมในระดับนานาชาติ และกฎหมายระหว่างประเทศ ที่เป็นตัวกำหนดถึงความรุนแรงทางไซเบอร์แบบใดที่อาจนำมาสู่ความขัดแย้งระดับการก่อให้เกิดสงคราม (Libicki, 2009)

3. โลกไซเบอร์เป็นสิ่งที่ส่งผลต่อดุลอำนาจระหว่างรัฐ (Balance of Power) หมายถึง การที่ประเทศสหรัฐอเมริกาเป็นผู้นำทางด้านเทคโนโลยีไซเบอร์ ในขณะเดียวกัน ประเทศจีน รัสเซีย และประเทศอิหร่าน ได้พัฒนาศักยภาพของเทคโนโลยีไซเบอร์เพื่อถ่วงดุลอำนาจของประเทสสหรัฐอเมริกาด้วยเช่นกัน ส่งผลให้เกิดการแข่งขันทางไซเบอร์ที่รุนแรงระหว่างรัฐในการเมืองระหว่างประเทศ อีกทั้ง

การเพิ่มขึ้นของตัวแสดงที่ไม่ใช่รัฐ (Non-state actor) ที่เข้ามามีบทบาทต่อการโจมตีทางไซเบอร์ รวมถึงการเผยแพร่แนวคิดทางออนไลน์ต่างๆ ส่งผลกระทบโดยตรงต่อการดุลอำนาจระหว่างรัฐ ความท้าทายของประเทศสหรัฐอเมริกาทางด้านดุลอำนาจระหว่างรัฐ จำเป็นต้องพึ่งพาสิ่งที่เรื่องว่า Smart Power หรือ การผสมผสานกันระหว่างการควบคุมอำนาจโดยใช้ Hard Power (ประสิทธิภาพของกองทัพ และ เศรษฐกิจ) และ Soft Power (การสร้างวัฒนธรรม และ ค่านิยม) เพื่อการรักษาดุลอำนาจในศตวรรษที่ 21 ที่การแข่งขันระหว่างรัฐนั้น ไม่ใช่เพียงการแข่งขันทางด้านการทหารเพียงอย่างเดียว แต่รวมถึงการแข่งขันทางด้านเศรษฐกิจ เทคโนโลยี และอิทธิพลทางวัฒนธรรม ที่จะสามารถทำให้ประเทศมีความเป็นมหาอำนาจได้ในศตวรรษที่ 21 (Nye, 2017)

ความเป็นมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา จำเป็นต้องพึ่งพาความได้เปรียบทางข้อมูลและเทคโนโลยีไซเบอร์ แต่การสร้างความได้เปรียบเหล่านั้น ก่อให้เกิดความท้าทายที่ประเทศมหาอำนาจที่ต้องการสร้างข้อได้เปรียบทางไซเบอร์จำเป็นต้องเผชิญในศตวรรษที่ 21 เราสามารถใช้แนวคิดสมองของโลกในการวิเคราะห์ถึงองค์ประกอบที่สำคัญและความท้าทายที่สามารถเกิดขึ้นได้ ดังต่อไปนี้

1. การเชื่อมต่อและโครงสร้างพื้นฐานทางไซเบอร์ (Connectivity and Cyber Infrastructure) หมายถึง ความเป็นอนาธิปไตยทางไซเบอร์ที่ไร้การควบคุมจากศูนย์กลาง ทำให้ความซับซ้อนของเครือข่ายอินเทอร์เน็ตและการควบคุมข้อมูลในระดับนานาชาติเป็นไปได้ยาก หรือ ไม่สามารถควบคุมได้ แม้กระทั่งความเป็นบริษัทเอกชนที่เป็นผู้สร้างช่องทางการสื่อสาร หรือการใช้โลกอินเทอร์เน็ตเพื่อแสวงหาผลประโยชน์ต่างๆ อาทิเช่น Google Microsoft Facebook ที่มีส่วนสำคัญในการสร้างโลกอินเทอร์เน็ตและการสร้างการเชื่อมต่อของผู้คนผ่านข้อมูลออนไลน์ ก่อให้เกิดการสร้างเครือข่ายสาธารณะจากโลกอินเทอร์เน็ต (Networked Publics) ส่งผลให้การไหลเวียนของข้อมูลมีความอิสระและเสรี และได้ส่งผลต่อภาคเศรษฐกิจ ก่อให้เกิด ระบบเศรษฐกิจแบบเปิด (Open Economy) ในการสร้างความร่วมมือระหว่างภาครัฐ ภาคเอกชน การศึกษา และการสร้างนโยบายสาธารณะต่างๆด้วยเช่นกัน

การเกิดขึ้นของการเชื่อมต่อทางไซเบอร์ได้สร้างความท้าทายให้กับสื่อกระแสหลัก เนื่องจากโลกไซเบอร์ได้สร้างทางเลือกทางด้านข้อมูลให้กับผู้ใช้งานในการเข้าถึงข่าวสารที่มีข้อมูลที่แตกต่างจากสื่อกระแสหลักได้ด้วยเช่นกัน ความท้าทายทางด้านข้อมูลแบบรวมศูนย์ (Centralized Media) กำลังถูกท้าทายด้วยโครงสร้างการกระจายศูนย์ทางข้อมูล (Decentralized Media) และการแลกเปลี่ยนข้อมูลอย่างเสรี ได้กลายเป็นความท้าทายต่อภาครัฐและภาคเอกชนถึงการควบคุมและป้องกันความปลอดภัยของข้อมูลที่มีความละเอียดอ่อน หรือ ข้อมูลที่ส่งผลต่อความมั่นคงแห่งชาติ จากการสอดแนม การจารกรรมข้อมูลไซเบอร์ และการแฮ็กข้อมูลต่างๆ แต่การเข้ามาควบคุมเหล่านี้ ต้องคำนึงถึงสิทธิเสรีภาพของประชาชนด้วยเช่นกัน (Benkler, 2016)

2. การควบคุมข้อมูลจำนวนมากและการควบคุมการไหลเวียนของข้อมูล (Big Data and Information Flow & Control) หมายถึง การเพิ่มขึ้นของการใช้งานไซเบอร์ ก่อให้เกิดข้อมูลจำนวนมากที่มีการกระจายตัวในรูปแบบของเครือข่ายอินเทอร์เน็ต (Decentralized Networks) ข้อมูลจำนวนมากเหล่านี้เป็นสิ่งที่ยากในการควบคุมและเป็นความท้าทายต่อประเทศมหาอำนาจทางไซเบอร์อย่างประเทศสหรัฐอเมริกาในศตวรรษที่ 21

Luciano Floridi (2014) ได้วิเคราะห์ถึงการปฏิวัติทางดิจิทัลในศตวรรษที่ 21 ว่าเป็นการสร้างการเปลี่ยนแปลงครั้งใหญ่ เปรียบดั่งการเป็น การปฏิวัติทางปัญญาครั้งที่ 4 (The Fourth Revolution) ซึ่งหมายถึงการเปลี่ยนแปลงความเข้าใจของความเป็นมนุษย์เกี่ยวกับการเข้าใจตัวเองและความเป็นจริงต่างๆรอบตัว โดยการปฏิวัติทางปัญญาที่เกิดขึ้นก่อนหน้าทั้งหมด 3 ครั้ง ประกอบด้วย

การปฏิวัติโคเปอร์นิคัส (Copernican Revolution) เป็นการปฏิวัติที่เกิดจากนิโคลัส โคเปอร์นิคัสที่อธิบายถึงการที่โลกไม่ใช่ศูนย์กลางของจักรวาล โลกเป็นเพียงดาวเคราะห์ที่โคจรรอบดวงอาทิตย์ ทำให้มนุษย์ยอมรับว่าตนเองไม่ใช่ศูนย์กลางของทุกสิ่ง

การปฏิวัติที่มาจากทฤษฎีของชาร์ลส์ ดาวิน (Darwinian Revolution) ว่าด้วยการที่มองว่ามนุษย์เป็นช่วงหนึ่ง หรือกระบวนการหนึ่งของวิวัฒนาการทางด้านชีววิทยา ซึ่งไม่ใช่สิ่งที่ถูกสร้างขึ้นมาเฉพาะ หรือสร้างขึ้นมาเป็นมนุษย์โดยสมบูรณ์

การปฏิวัติของฟรอยด์ (Freudian Revolution) ซึ่งซิกมันด์ ฟรอยด์ได้มองว่า จิตใจของมนุษย์นั้น ไม่ใช่สิ่งที่มนุษย์สามารถควบคุมเองได้ทั้งหมด แต่เป็นการถูกขับเคลื่อนจิตใจด้วยจิตไร้สำนึก (Unconscious mind) ด้วยเช่นกัน ทำให้มนุษย์เรานั้นมีความซับซ้อนมากกว่าที่เราเข้าใจ และสำหรับการปฏิวัติครั้งที่ 4 Luciano Floridi ได้ให้นิยามว่าเป็น การปฏิวัติสารสนเทศ ซึ่งเป็นจุดเปลี่ยนแปลงของมนุษย์ที่เทคโนโลยีและปัญญาประดิษฐ์ (AI) เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์ ทำให้การตัดสินใจต่างๆของมนุษย์ไม่ได้มาจากจิตหรือหลักเหตุผลของมนุษย์เพียงอย่างเดียว แต่เป็นการประกอบร่วมกับข้อมูลที่ถูกสร้างขึ้นมาด้วยเทคโนโลยี อัลกอริธึม คอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ต ซึ่งบทบาทของเทคโนโลยีกลายเป็นสิ่งที่กำหนดทิศทางและมุมมองของมนุษย์ในการมองโลก

จากการปฏิวัติครั้งที่ 4 Luciano Floridi ได้เสนอแนวคิด Infosphere หมายถึง แนวคิดที่ระบบข้อมูลเกิดจากการมีปฏิสัมพันธ์กันระหว่างมนุษย์และเทคโนโลยี ซึ่งประเทศสหรัฐอเมริกา เป็นประเทศที่มีบทบาทสำคัญในการเป็นศูนย์กลางของโลกไซเบอร์ เนื่องจากเป็นต้นกำเนิดของบริษัทชั้นนำที่เกี่ยวข้องกับโลกไซเบอร์ เช่น Google ที่เป็นทั้งบริษัทรวบรวมข้อมูลและปัญญาประดิษฐ์ Apple ที่เป็นบริษัทเกี่ยวกับอุปกรณ์และการสื่อสาร Facebook (Meta) ที่เป็นบริษัทเกี่ยวกับโซเชียลมีเดียและเมต้าเวิร์ส และเป็นบริษัทที่สามารถสร้างผลกระทบต่อการตัดสินใจทางการเมือง และเศรษฐกิจ

ได้ Amazon เป็นบริษัทเกี่ยวกับ E-Commerce และ Cloud Computing และ Microsoft ที่เป็นบริษัทสร้างระบบปฏิบัติการ และ ChatGPT ที่เป็นปัญญาประดิษฐ์ที่ล้ำหน้ามากที่สุด ณ ปัจจุบัน ซึ่งบทบาทของบริษัทที่กล่าวมาข้างต้น เป็นปัจจัยที่กำหนดกระบวนการเข้าถึงข้อมูลต่างๆของมนุษย์ การใช้งานปัญญาประดิษฐ์และระบบนิเวศทางดิจิทัล ที่ประเทศสหรัฐอเมริกากำลังสร้าง ทำให้ประเทศสหรัฐอเมริกาเข้าใกล้การเป็น สมองของโลก หรือ Global Brain ที่มีระบบประสาทในการเชื่อมต่อข้อมูลทั่วโลกได้ในอนาคตอันใกล้ และในศตวรรษที่ 21 นี้ มนุษย์ไม่ได้เป็นเพียงบุคคลธรรมดา แต่กำลังกลายเป็นสิ่งมีชีวิตเชิงข้อมูลที่อยู่ร่วมกับอัลกอริธึม หรือ (Information Organisms) อาทิ เช่น มนุษย์เป็นส่วนประกอบของการตลาดแบบกำหนดเป้าหมาย (Targeted Advertising) ไม่ว่าจะเป็น Facebook Youtube หรือ Google ต่างใช้อัลกอริธึมในการวิเคราะห์ข้อมูลผู้ใช้งานเพื่อเสนอสิ่งที่ผู้ใช้งานเหล่านั้นมีความสนใจ และมีพฤติกรรมที่เหมาะกับการเสนอสิ่งเหล่านั้น รวมถึงในแง่ของการเมืองด้วยเช่นกัน เช่น การใช้ข้อมูล Facebook เพื่อกำหนดการโฆษณาในช่วงเลือกตั้งของประเทศสหรัฐอเมริกา ทำให้ Donald Trump ได้รับชนะการเลือกตั้ง และนอกจากการถูกกำหนดเป้าหมายทางการตลาดแล้วนั้น ผลกระทบทางด้านเศรษฐกิจที่มาจากการเป็นส่วนหนึ่งกับข้อมูลทางเทคโนโลยี คือ การใช้แพลตฟอร์มเพื่อสร้างรายได้ เช่น Uber ที่ทำให้เกิดแรงงานจำนวนมากในการใช้แอพพลิเคชั่นในการสร้างรายได้ (Floridi, 2014)

3. การเปรียบเทียบความมั่นคงทางไซเบอร์เหมือนกับระบบภูมิคุ้มกัน (Cybersecurity as Immune System) หมายถึง ความท้าทายที่เกิดขึ้นต่อความมั่นคงแห่งชาติ ที่มีความจำเป็นต้องปรับเปลี่ยนตลอดเวลาเพื่อให้สอดคล้องกับพัฒนาการทางเทคโนโลยีไซเบอร์ เปรียบเสมือนการปรับเปลี่ยนของภูมิคุ้มกันของร่างกาย ที่ต้องปรับตัวเพื่อป้องกันโรคภัยต่างๆที่เกิดขึ้นใหม่และมีความแตกต่างกัน

Dunn Cavelty (2018) ได้เสนอแนวคิดการป้องกันภัยจากโลกไซเบอร์ว่า นอกจากการเป็นการป้องกันเชิงรับ (Passive Defense) แล้วนั้น การป้องกันภัยจำเป็นต้องสามารถตอบสนองอย่างทันท่วงที และมีการปรับตัวอย่างต่อเนื่อง โดยได้แบ่งขั้นตอนการป้องกันโดยใช้แนวคิดระบบภูมิคุ้มกันออกเป็น 4 ขั้นตอน คือ 1. การเฝ้าระวัง (Detection and Monitoring) หมายถึง การตรวจจับภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว เหมือนกับร่างกายตรวจจับเชื้อโรค 2. การตอบสนองต่อภัยคุกคาม (Threat Response and Containment) หมายถึง การจัดการและตอบสนองต่อการโจมตีที่เกิดขึ้นอย่างรวดเร็ว เพื่อป้องกันความเสียหายที่อาจเพิ่มขึ้นได้ เปรียบเสมือนเซลล์เม็ดเลือดขาวที่กำจัดเชื้อโรคในร่างกาย 3. การฟื้นตัวและการเสริมสร้างภูมิคุ้มกัน (Recovery and Resilience) หมายถึง การฟื้นฟูระบบให้กลับมาใช้งานได้อย่างรวดเร็วหลังจากการถูกโจมตี เปรียบเสมือนร่างกายฟื้นฟูหลังจากการติดเชื้อ และ 4. การปรับตัวและแลกเปลี่ยนองค์ความรู้ (Adaptive Security and Intelligence Sharing) หมายถึง การสร้างองค์ความรู้จากภัยคุกคามที่เกิดขึ้น และพัฒนาเทคโนโลยีให้ดียิ่งขึ้น

รวมถึงการแลกเปลี่ยนข้อมูลกับประเทศพันธมิตร เพื่อเสริมสร้างประสิทธิภาพให้กันและกัน อาทิเช่น กรณีประเทศสหรัฐอเมริกาถูกโจมตีท่อส่งน้ำมันที่ใหญ่ที่สุดในประเทศ (Colonial Pipeline) ใน ค.ศ. 2021 โดยกลุ่มแฮ็กเกอร์นามว่า Darkside ที่ใช้การโจมตีทางไซเบอร์ด้วย Ransomware (การเรียกค่าไถ่ผ่านมัลแวร์) ซึ่งทำให้การขนส่งน้ำมันถูกปิดระบบ โดยท่อขนส่งน้ำมันดังกล่าวมีระยะทางขนส่งอยู่ที่ 8,850 กิโลเมตร สร้างความเสียหายทำให้เกิดน้ำมันขาดแคลนในหลายรัฐ และส่งผลให้ราคาน้ำมันพุ่งสูงขึ้นทันที และในขณะนั้น บริษัท Colonial Pipeline ได้ทำการจ่ายค่าไถ่ให้กับกลุ่มแฮ็กเกอร์ดังกล่าวด้วย Bitcoin เป็นจำนวนเงิน 4.4 ล้านดอลลาร์สหรัฐเพื่อกู้คืนระบบ ภายหลัง รัฐบาลสหรัฐอเมริกาและภาคเอกชนได้ให้ความสำคัญกับความมั่นคงไซเบอร์มากยิ่งขึ้น และได้เริ่มปราบปรามกลุ่มแฮ็กเกอร์ในการตอบโต้ด้วยเช่นกัน (Dunn Cavelty, 2018)

4. การแข่งขันเพื่อเป็นสมองของโลก (Competition for the Global Brain) หมายถึง การที่ประเทศสหรัฐอเมริกาได้พัฒนาเทคโนโลยีไซเบอร์อย่างต่อเนื่อง และความร่วมมือจากภาคเอกชนในการพัฒนาเทคโนโลยีระดับสูง ไม่ว่าจะเป็นปัญญาประดิษฐ์ (Aritficial Intelligence) และคอมพิวเตอร์ควอนตัม (Quantum Computing) ทำให้มองได้ว่า ประเทศสหรัฐอเมริกามีความพยายามในการรักษาอำนาจในการเป็นประเทศมหาอำนาจทางไซเบอร์ แต่ในขณะเดียวกัน ประเทศจีนและรัสเซีย ได้มีความพยายามลดการพึ่งพาเทคโนโลยีจากประเทศสหรัฐอเมริกา และพัฒนาองค์ความรู้ทางเทคโนโลยีของประเทศตนเอง ทำให้เกิดความท้าทายทางด้านการกระจายตัวของอำนาจทางไซเบอร์ โดย Sharma (2020) ได้เสนอแนวคิดอธิปไตยทางดิจิทัล (Digital Sovereignty) ซึ่งเกี่ยวกับการที่ประเทศต่างๆมีความพยายามในการควบคุมโครงสร้างพื้นฐานทางดิจิทัลของตนเองด้วยประเทศตนเอง ไม่ว่าจะเป็นเครือข่ายอินเทอร์เน็ต แหล่งเก็บข้อมูล และแพลตฟอร์มแอพพลิเคชั่นต่างๆ เพื่อเป็นการป้องกันภัยคุกคามทางไซเบอร์ และสร้างอำนาจทางไซเบอร์ของประเทศตนเองเพื่อความมั่นคงทางด้านการทหาร เศรษฐกิจ และอำนาจทางการเมือง อาทิเช่น การที่ประเทศจีน มีความพยายามในการสร้าง Great Firewall เพื่อควบคุมการใช้งานโลกไซเบอร์ภายในประเทศ และสนับสนุนแพลตฟอร์มแอพพลิเคชั่นของประเทศตนเอง เช่น Wechat และ Alibaba หรือการที่ประเทศสหรัฐอเมริกามีการใช้นโยบายในการควบคุมภาคเอกชนที่เกี่ยวข้องกับเทคโนโลยี เช่น การแบนบริษัท Huawei และ Tiktok โดยให้เหตุผลว่าเพื่อรักษาความมั่นคงทางไซเบอร์ของประเทศ (Sharma, 2020)

ภายใต้ความเป็นอนาธิปไตยในโลกไซเบอร์ บทบาทของประเทศสหรัฐอเมริกาและองค์กรระหว่างประเทศต่างๆที่เกี่ยวข้องกับโลกไซเบอร์ ได้ถูกท้าทายจากความเป็นอนาธิปไตยของโลกไซเบอร์ ซึ่ง ณ ปัจจุบัน การใช้อินเทอร์เน็ตของโลกใบนี้ ไม่ได้ถูกควบคุมโดยรัฐใดรัฐหนึ่ง แต่มีการถูกวางรากฐานและมาตรฐานของอินเทอร์เน็ต ภายใต้การบริหารขององค์กรที่มีบทบาทสำคัญในการจัดการโครงสร้างพื้นฐานทางอินเทอร์เน็ต อาทิเช่น Internet Corporation for Assigned Names

and Numbers (ICANN) และ International Telecommunication Union (ITU) ซึ่งประเทศสหรัฐอเมริกา เป็นประเทศที่มีอิทธิพลต่อทั้งสององค์กรดังกล่าว ทำให้เกิดความกังวลต่อประเทศอื่นๆ ชี้ให้เห็นถึงสภาวะการกังวลในเรื่องสมดุลแห่งอำนาจของรัฐ แต่การขยายตัวและการเติบโตอย่างรวดเร็วของการใช้งานเทคโนโลยีดิจิทัล ทำให้การใช้งานโลกไซเบอร์ได้สร้างการกระจายอำนาจทางไซเบอร์ไปยังนานาประเทศ ซึ่งไม่ได้ขึ้นตรงกับประเทศสหรัฐอเมริกาเพียงอย่างเดียว

ความเป็นอนาธิปไตยทางไซเบอร์สร้างความท้าทายต่อการควบคุมอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกาจากการกระจายตัวและการเพิ่มขึ้นของจำนวนผู้ใช้งาน อีกทั้งตัวแสดงที่เป็นรัฐอื่นๆ เริ่มสร้างกฎทางไซเบอร์ของประเทศตนเอง เพื่อสร้างความเป็นอธิปไตยทางไซเบอร์ แทนที่การปฏิบัติตามมาตรฐานที่กำหนดโดยประเทศสหรัฐอเมริกา อีกทั้งการเพิ่มขึ้นของผู้ใช้งานโลกไซเบอร์ ทำให้เกิดสภาวะ โลกที่ไม่มีปุ่มปิด (A World with No Off Switch) ที่หมายถึงการใช้งานโลกไซเบอร์ที่ไม่มีวันหยุด และการทำงานของข้อมูลและระบบที่เชื่อมต่อกันทั่วโลกตลอดเวลา รวมถึงอุปกรณ์ IoT (Internet of Things) ต่างๆ อาทิเช่น กล้องวงจรปิด เครื่องใช้ไฟฟ้าในชีวิตประจำวัน รถยนต์อิจฉริยะที่ไม่ได้ถูกควบคุมโดยภาครัฐอีกต่อไป ทำให้ความท้าทายจากสิ่งเหล่านี้ ที่มีช่องโหว่ในอุปกรณ์จากการสามารถถูกโจมตีโดยอาวุธไซเบอร์ จากตัวแสดงต่างๆไม่ว่าจะเป็นแฮ็กเกอร์ และการโจมตีจากรัฐบาลประเทศอื่นๆ กลายเป็นความท้าทายที่หลีกเลี่ยงไม่ได้จากความเป็นอนาธิปไตยในโลกไซเบอร์ต่อประเทศสหรัฐอเมริกาในศตวรรษที่ 21 (DeNardis, 2020)

การไร้ผู้ควบคุมที่ชัดเจนเกี่ยวกับโลกไซเบอร์ หรือความเป็นอนาธิปไตยในโลกไซเบอร์ เป็นความท้าทายที่สำคัญต่ออำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ไม่ว่าจะเป็นทางด้านความสัมพันธ์ระหว่างประเทศ ที่ไม่สามารถควบคุมกฎเกณฑ์ทางไซเบอร์ การทำให้เกิดภาวะกลืนไม่เข้าคายไม่ออกทางด้านความมั่นคงที่ต้องเผชิญจากความพยายามสร้างความมั่นคงทางไซเบอร์ของประเทศตนเอง ส่งผลให้เกิดปัญหาทางด้านดุลแห่งอำนาจที่นานาประเทศมีความพยายามในการพัฒนาเทคโนโลยีของตนเอง อาทิเช่นประเทศจีน และรัสเซีย การใช้แนวคิดสมองของโลกวิเคราะห์ความเป็นอนาธิปไตยของโลกไซเบอร์ที่ส่งผลต่อประเทศสหรัฐอเมริกา ทำให้เห็นถึงความสามารถประสิทธิภาพ และปัจจัยที่ส่งผลให้ประเทศสหรัฐอเมริกาสามารถใช้พื้นที่อนาธิปไตยในโลกไซเบอร์เพื่อสร้างข้อได้เปรียบ แต่ในขณะเดียวกัน ความเป็นอนาธิปไตยของโลกไซเบอร์สามารถสร้างภัยคุกคามต่อประเทศสหรัฐอเมริกาได้ด้วยเช่นกัน เนื่องจากไม่มีประเทศใดสามารถควบคุมภัยคุกคามทางไซเบอร์ได้โดยสมบูรณ์ แม้กระทั่งประเทศที่มีความเป็นอำนาจทางไซเบอร์อย่างประเทศสหรัฐอเมริกา อีกทั้งความท้าทายจากการแข่งขันทางไซเบอร์ที่เกิดขึ้นจากประเทศต่างๆด้วยเช่นกัน

บทที่ 5

ความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา

ภายหลังสงครามโลกครั้งที่ 2 ประเทศสหรัฐอเมริกาได้ขึ้นมาเป็นมหาอำนาจทั้งทางด้านเศรษฐกิจ การเงิน และทางการทหาร ไซเบอร์ คือ องค์ประกอบใหม่ที่เสริมอำนาจให้กับประเทศสหรัฐอเมริกา ซึ่งเมื่อพูดถึงพื้นที่ที่ใช้ในการทำสงคราม โดยทั่วไปแล้วสามารถแบ่งออกเป็นทั้งหมด 4 ประเภท คือ บนพื้นดิน (land) ทะเล (sea) อากาศ (air) และ อวกาศ (space) แต่สำหรับพื้นที่ทางไซเบอร์ (cyberspace) นั้นแตกต่างออกไป เพราะพื้นที่ทางไซเบอร์เกี่ยวข้องกับการทำงานร่วมกันของเครื่องมือทางกายภาพ และ เทคโนโลยีไซเบอร์ซึ่งเป็นภาพเสมือน และการที่เราจะโต้ตอบกับพื้นที่ไซเบอร์ได้ มีเพียงการใช้เครื่องมือในการส่งคำสั่งผ่านระบบเครือข่ายที่สร้างโดยฝีมือมนุษย์และพื้นที่ไซเบอร์ไม่ใช่พื้นที่ที่มนุษย์สามารถเข้าถึงได้โดยกายภาพ ดังนั้น พื้นที่ทางไซเบอร์จึงมีความแตกต่างจากพื้นที่ที่ใช้ในการทำสงครามทั้ง 4 ประเภทที่กล่าวไว้ข้างต้น ซึ่งถึงแม้ว่ากระบวนการสเปกตรัมแม่เหล็กไฟฟ้า (electromagnetic spectrum) ซึ่งเป็นหนึ่งในขั้นตอนในการเคลื่อนย้ายข้อมูลจะไม่ได้เกิดจากฝีมือมนุษย์ แต่องค์ประกอบที่สร้างให้เกิดกระบวนการเคลื่อนย้ายข้อมูลต่างๆในพื้นที่ไซเบอร์นั้นเกิดจากฝีมือมนุษย์ทั้งสิ้น (AFCEA Cyber Committee, n.d.)

มนุษย์ได้สร้างพื้นที่เพื่อใช้ในการสนับสนุนการทำงานการเคลื่อนย้ายข้อมูลในการปฏิบัติการจากพื้นที่หนึ่ง ไปอีกพื้นที่หนึ่ง จนนำมาสู่การใช้ไซเบอร์ทั้งในรูปแบบอาชญากรรมไซเบอร์และสงครามไซเบอร์ เมื่อกล่าวถึงอำนาจในการทำสงคราม อำนาจทางไซเบอร์จึงได้กลายมาเป็นส่วนหนึ่งของสงคราม ดังนั้น ก่อนที่เราจะศึกษาข้อมูลและองค์ประกอบของไซเบอร์ ที่ช่วยเสริมสร้างความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกาในด้านต่างๆ ไม่ว่าจะเป็นทางด้านการทหาร เทคโนโลยีและวิทยาศาสตร์ เราควรที่จะเรียนรู้ถึงประวัติศาสตร์ของอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ว่าอำนาจที่กำลังสร้างความได้เปรียบนี้ มีจุดเริ่มต้นจากอะไร มีที่มาอย่างไร มีองค์ประกอบอย่างไร และเพราะเหตุใด ประเทศสหรัฐอเมริกาจึงมีอำนาจทางไซเบอร์เป็นอันดับหนึ่งของโลก ณ ปัจจุบัน (Voo, Hemani, & Cassidy, 2022)

จุดเริ่มต้นของอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา เริ่มต้นขึ้นในทศวรรษ ค.ศ. 1920 โดยเริ่มต้นจากการนำนวัตกรรมเครื่องเอนิกมา (enigma) ของกองทัพเรือเยอรมัน ที่เป็นเครื่องเข้ารหัสที่ใช้ในการป้องกันความลับในทางการทูต ทางการทหาร ที่ประกอบไปด้วยฮาร์ดแวร์และซอฟต์แวร์ โดยในทศวรรษ ค.ศ. 1930 กองทัพเรือของประเทศสหรัฐอเมริกาได้ทำการดัดแปลงอุปกรณ์ที่มีความสามารถคล้ายกับเครื่องเอนิกมา ชื่อเครื่อง SIGABA โดยเจ้าหน้าที่หน่วยข่าวกรองได้ใช้ในการส่งข้อความลับระหว่างกันและกัน และถูกใช้อย่างแพร่หลายในช่วงสงครามโลกครั้งที่ 2 และ

ในขณะเดียวกันในช่วงปลายทศวรรษ ค.ศ. 1930 นักพัฒนาชาวเยอรมันชื่อ Konrad Zuse ได้ทำการพัฒนาคอมพิวเตอร์เชิงกลที่ขับเคลื่อนด้วยมอเตอร์ ชื่อว่า Z1

คอมพิวเตอร์ดิจิทัลไฟฟ้าเครื่องแรกได้กำเนิดขึ้นในช่วงทศวรรษ ค.ศ. 1940 ในประเทศสหรัฐอเมริกา ชื่อ Atanasoff-Berry Computer (ABC) เป็นเครื่องคำนวณแก้สมการเชิงเส้น 29 ตัวแปร และยังเป็นเครื่องบุกเบิกในการเป็นส่วนประกอบที่สำคัญของคอมพิวเตอร์สมัยใหม่ประกอบด้วย ระบบสวิตช์อิเล็กทรอนิกและความสามารถในการคำนวณสมการฐานสอง และในขณะเดียวกัน ได้มีการพัฒนาทรานซิสเตอร์ (transistor) อุปกรณ์ขยายสัญญาณไฟฟ้าหรือพลังงานไฟฟ้า ที่ถูกพัฒนาในห้องแล็บส์ AT&T Bell โดย John Bardeen และ Walter Brattain

นวัตกรรมการประดิษฐ์เครื่องคอมพิวเตอร์ของประเทศสหรัฐอเมริกาได้ดำเนินมาอย่างต่อเนื่องจนถึงทศวรรษ ค.ศ. 1950 บริษัท IBM ได้ทำการร่างภาษาคอมพิวเตอร์แรกของโลก คือ ภาษาฟอร์แทรน (FORTRAN) และในขณะเดียวกันก็ได้มีการพัฒนา ไอซี (IC หรือ Integrated Circuit) เป็นวงจรรวมที่นำอุปกรณ์อิเล็กทรอนิกส์ชนิดต่างๆมารวมกัน อาทิเช่น ตัวต้านทาน (Resistor) ตัวเก็บประจุไดโอด (Diode) ทรานซิสเตอร์ (Transistor) และอุปกรณ์ต่างๆของวงจรมาต่อรวมกัน ซึ่งในเวลาต่อมาก็ได้พัฒนากลายเป็นแผงวงจรแบบ silicon chip หรือ ชิป (Chip) โดย Robert Noyce

จุดเริ่มต้นครั้งสำคัญของการเชื่อมต่อโลกอินเทอร์เน็ต เกิดขึ้นในทศวรรษ ค.ศ. 1960 โดยหน่วยงานพัฒนาโครงการ(Advanced Research Projects Agency) ที่กำกับดูแลโดยกระทรวงกลาโหมสหรัฐอเมริกา (Department of Defense หรือ DOD) ได้พัฒนาเครือข่ายคอมพิวเตอร์แรกของโลกชื่อว่า ARPAnet (Advanced Research Projects Agency Network) โดยการใช้เทคนิคที่เรียกว่า packet switching ซึ่งเป็นเทคนิคในการแลกเปลี่ยนข้อมูลมากกว่าหนึ่งชุดข้อมูลในสายโทรศัพท์เดียวกันในเวลาเดียวกัน และเป็นจุดกำเนิดของอินเทอร์เน็ตในเวลาต่อมา และเมื่อเวลาผ่านไป ในทศวรรษ ค.ศ. 1970 ระบบโทรคมนาคมระบบแรกที่เรียกว่า ระบบเครือข่าย packet switching ได้ออกสู่สาธารณะและให้บริการในชื่อ Telenet ในขณะเดียวกัน ระบบเครือข่าย ARPAnet ได้เริ่มเชื่อมต่อกับระบบเครือข่ายอื่นๆ และการเริ่มต้นเชื่อมต่อกับระบบเครือข่ายอื่นๆนี้ได้ถูกเรียกว่า Internetwork ซึ่งถูกทำให้เรียกสั้นๆว่า Internet ในเวลาต่อมา (AFCEA Cyber Committee, n.d.)

การประกาศใช้ระบบเครือข่ายอินเทอร์เน็ตสำหรับทางการทหารเริ่มต้นใน ค.ศ. 1982 โดยกระทรวงกลาโหมได้ประกาศใช้ระบบปฏิบัติการแบบ TCP/IP เป็นมาตรฐานการใช้งาน และในค.ศ.1983 กระทรวงกลาโหมสหรัฐอเมริกายังได้ทำการแบ่งระบบเครือข่าย ARPAnet ออกเป็นสองเครือข่ายคือ ARPAnet และ MILnet ระบบโดเมนแรกของโลกได้กำเนิดขึ้นใน ค.ศ. 1985 ชื่อว่าระบบ .com โดยบริษัท Symbolics Inc. และ Symbolics.com คือโดเมนโทรคมนาคมจดทะเบียน

แรกของโลกและเก่าแก่ที่สุดในโลกอินเทอร์เน็ต และระยะเวลาต่อมาไม่นานใน ค.ศ. 1988 ได้กำเนิดไวรัสอินเทอร์เน็ตแรกของโลก ชื่อว่า Morris Worm สร้างโดย Robert Tappan Morris ชาวอเมริกัน มีเป้าหมายทำลายระบบคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ต โดยไวรัสนี้ทำงานโดยเริ่มต้นในการส่งตัวเองไปยังเครื่องคอมพิวเตอร์อื่นๆ และการเจาะเข้าระบบความปลอดภัย สร้างความเสียหายเป็นอย่างมาก จนกระทั่งใน ค.ศ. 1990 เครือข่าย ARPAnet ได้ถูกปลดการใช้งานและได้มีการพัฒนาระบบปฏิบัติการ World Wide Web ที่พัฒนาโดย Tim Bernes-Lee ใน ค.ศ. 1991 รวมถึงการจดทะเบียน Google.com ใน ค.ศ. 1997 ที่ได้กลายเป็นเครื่องมือค้นหาของโลกอินเทอร์เน็ตจนถึงปัจจุบัน (AFCEA Cyber Committee, n.d.)

หลังสงครามโลกครั้งที่ 2 ความเป็นมหาอำนาจในด้านต่างๆ ทำให้ประเทศเกิดการพัฒนาอย่างต่อเนื่อง รวมถึงการนำเทคโนโลยีมาปรับใช้กับรูปแบบของสงคราม จากในอดีต พื้นที่ที่ใช้ในการทำสงครามแบ่งได้เป็น 4 ประเภท คือ บนพื้นดิน, ทะเล, อากาศ, และอวกาศ และในภายหลัง ได้กำเนิดพื้นที่ใหม่ล่าสุดคือ พื้นที่ทางไซเบอร์ ซึ่งมีความแตกต่าง เนื่องจากพื้นที่ทางไซเบอร์เกี่ยวข้องกับเครื่องมือทางกายภาพและเทคโนโลยี เป็นสิ่งที่ถูกสร้างเพื่อสนับสนุนการทำงานและการเคลื่อนย้ายข้อมูล การโต้ตอบในพื้นที่ไซเบอร์จะใช้เครื่องมือในการส่งคำสั่งผ่านเครือข่าย และกลายเป็นส่วนหนึ่งของการทำสงคราม โดยมีจุดเริ่มต้นการพัฒนาเทคโนโลยีใน ค.ศ. 1920 ด้วยการพัฒนาเครื่องเอนิกมาและคอมพิวเตอร์ ภายหลังมีการพัฒนาการเชื่อมต่อเครือข่ายอินเทอร์เน็ต และใน ค.ศ. 1982 การใช้ระบบเครือข่ายอินเทอร์เน็ตสำหรับทางการทหารได้เริ่มต้นขึ้น

เนื้อหาในบทที่ 4 ผู้วิจัยจะกล่าวถึง องค์ประกอบทางไซเบอร์ที่เสริมอำนาจให้กับประเทศสหรัฐอเมริกา ด้วยการอธิบายตามกรอบแนวคิดการวิจัย ประกอบด้วย ความเป็นมหาอำนาจทางไซเบอร์ทางการทหาร อำนาจทางไซเบอร์ทางด้านเทคโนโลยี และอำนาจทางไซเบอร์ทางด้านวิทยาศาสตร์ การปฏิบัติการทางไซเบอร์กลายเป็นส่วนสำคัญของการทำสงครามและการเสริมสร้างความมั่นคงของประเทศสหรัฐอเมริกาในปัจจุบัน โดยผู้วิจัยแบ่งเนื้อหา ดังนี้

1. ความเป็นมหาอำนาจไซเบอร์ทางการทหาร
    1.1 บทบาททางการเมือง
    1.2 ลักษณะความเป็นรัฐบาล
    1.3 วัตถุประสงค์ทางการทหาร
    1.4 อำนาจทางการทหาร

2. ความเป็นมหาอำนาจไซเบอร์ทางด้านเทคโนโลยี
    2.1 ความไม่สมมาตรของโลกไซเบอร์
    2.2 การพัฒนาและการปรับใช้โลกไซเบอร์

2.3 ลำดับชั้นทางกายภาพ

2.4 ลำดับชั้นทางตรรกะ

2.5 ลำดับชั้นทางข้อมูล

3. ความเป็นมหาอำนาจไซเบอร์ทางวิทยาศาสตร์

3.1 ลำดับชั้นทางด้านผู้ใช้งาน

3.2 การอภิปรายทางวิชาการ

3.3 ความเป็นสถาบันนิยม

1. ความเป็นมหาอำนาจทางไซเบอร์ทางการทหาร (Cyber Military Power)

1.1 บทบาททางการเมือง (Politics)

ภายหลังสงครามโลกครั้งที่ 2 ประเทศสหรัฐอเมริกามีบทบาทในการเมืองระหว่างประเทศในส่วนของการกำหนดกฎเกณฑ์ การให้นิยามในหลายๆสิ่ง การกำหนดจุดประสงค์หรือการกำหนดทิศทางของโลกในหลากหลายด้าน และการสร้างความสัมพันธ์กับหลากหลายประเทศทั่วโลก บทบาททางการเมืองของประเทศสหรัฐอเมริกาสามารถถูกเปรียบเทียบได้ว่า เป็นประเทศที่วางบรรทัดฐานทางการเมืองระหว่างประเทศ หรือ การเป็นผู้สร้างนโยบายทางการเมืองระหว่างประเทศเพื่อการพัฒนา การดำเนินการ และการวัดประสิทธิภาพเพื่อการแก้ไขปัญหาการเมืองระหว่างประเทศด้วยประเทศตนเอง และประเทศอื่นๆ มีหน้าที่ในการทำความเข้าใจถึงนโยบายต่างๆที่ประเทศสหรัฐอเมริกาได้เป็นผู้กำหนดและเข้าใจถึงบทบาทของประเทศสหรัฐอเมริกาที่มีต่อโลกใบนี้

บทบาทของประเทศสหรัฐอเมริกาในการเมืองระหว่างประเทศ สามารถอธิบายเป็น 4 องค์ประกอบ ดังนี้

1. ความเป็นผู้นำระดับโลก (Global Leadership)

ความเป็นผู้นำระดับโลกของประเทศสหรัฐอเมริกา ได้เริ่มต้นขึ้นหลังสงครามโลกครั้งที่ 2 สิ้นสุดลง โดยประเทศสหรัฐอเมริกาได้กลายเป็นผู้ชี้ให้เห็นถึงปัญหาต่างๆในการเมืองระหว่างประเทศ, เป็นผู้เข้าแก้ไขปัญหา, เป็นแบบอย่างให้กับประเทศอื่นๆได้ปฏิบัติตาม และเป็นผู้กำหนดกฎเกณฑ์ต่างๆในการเมืองระหว่างประเทศ มุมมองของผู้สังเกตการณ์ในหลายปีที่ผ่านมาได้ให้ความเห็นว่า บทบาทความเป็นผู้นำของประเทศสหรัฐอเมริกาในการเมืองระหว่างประเทศ สามารถให้นิยามได้ในหลากหลายความหมาย ซึ่งมีทั้งผู้เห็นด้วยและผู้ไม่เห็นด้วยในการให้นิยามเหล่านี้ อาทิเช่น การเป็นผู้นำของโลกเสรี การเป็นประเทศมหาอำนาจ การเป็นประเทศที่ทรงคุณค่าต่อโลกใบนี้ การเป็นประเทศที่คอยควบคุมดูแล ประเทศที่ไม่มีประเทศไหนสามารถแข่งขันได้ (Hyperpower) การเป็นตำรวจโลก หรือ การเป็นประเทศอำนาจนำของโลกใบนี้

บทบาทความเป็นผู้นำระดับโลกของประเทศสหรัฐอเมริกาสามารถสังเกตได้จากการมีส่วนร่วมในด้านต่างๆของการเมืองระหว่างประเทศ อาทิเช่น การมีส่วนร่วมหลักในการกำหนดนโยบายระหว่างประเทศ นโยบายสาธารณะระหว่างประเทศ อาทิเช่น การสร้างนโยบายในการขนส่งสินค้าระหว่างประเทศ การมีส่วนร่วมเชิงลึกในการเมืองระหว่างประเทศ การกำหนดนโยบายระหว่างประเทศด้วยแนวคิดเสรีนิยมเป็นพื้นฐาน การสร้างแนวคิดเสรีนิยามประชาธิปไตยในการเมืองระหว่างประเทศ หรือ อำนาจนำแบบเสรีนิยม (Liberal hegemony) และความเป็นผู้สร้างนวัตกรรมทางด้านนโยบายต่างประเทศเพื่อการเป็นอำนาจนำของโลก

2. การสร้างความมั่นคงและการสนับสนุนการสร้างกฎระเบียบระหว่างประเทศแบบเสรีนิยม (Defense and Promotion of Liberal International Order)

องค์ประกอบที่สองที่ประเทศสหรัฐอเมริกาและประเทศที่พันธมิตรให้ความสำคัญ คือ การสร้างความมั่นคงและการสนับสนุนการสร้างกฎระเบียบระหว่างประเทศแบบเสรีนิยมที่สร้างภายหลังการสิ้นสุดของสงครามโลกครั้งที่ 2 โดยกฎระเบียบระหว่างประเทศแบบเสรีนิยม มีนิยามโดยทั่วไปดังนี้

- การเคารพขอบเขตของประเทศต่างๆ และไม่รุกล้ำขอบเขตของประเทศอื่นๆ โดยการใช้ความรุนแรง
- การสนับสนุนการแก้ไขข้อพิพาทระหว่างประเทศด้วยสันติ ปราศจากการสร้างภัยคุกคามด้วยการใช้กำลัง และการเคารพธรรมเนียมและข้อบังคับระหว่างประเทศ
- การเคารพกฎหมายระหว่างประเทศ, กฎหมายและธรรมเนียมระดับโลก และการให้คุณค่าโดยทั่วไป ประกอบด้วย สิทธิมนุษยชน เป็นต้น
- การสร้างสถาบันทางการเมืองระหว่างประเทศที่แข็งแกร่งเพื่อสนับสนุนการทำงานระหว่างประเทศในการสร้างความพัฒนาต่อนานาประเทศ รวมถึงการสร้างผลประโยชน์ทางเศรษฐกิจและการเติบโตร่วมกัน
- การปฏิบัติตนในเขตน่านน้ำสากล น่านฟ้าสากล อวกาศ และ โลกไซเบอร์ เพื่อการใช้งานร่วมกันมากกว่าการใช้งานเพื่อสร้างอธิปไตยของประเทศ

อย่างไรก็ตาม ความตั้งใจในการขยายการสร้างกฎระเบียบระหว่างประเทศแบบเสรีนิยมของประเทศสหรัฐอเมริกาสามารถถูกอธิบายได้ในอีกรูปแบบหนึ่งเช่นกัน คือ ความพยายามในการสร้างความมั่นคงทางการเมืองระหว่างประเทศโดยใช้แนวคิดแบบเสรีนิยมเพื่อสร้างความมั่นคงในการเป็นผู้นำทางการเมืองของโลกใบนี้ และเป็นการสนับสนุน

ผลประโยชน์แห่งชาติของสหรัฐอเมริกาในระยะยาว ไม่ว่าจะเป็นทางด้านความมั่นคง การเมือง และ เศรษฐกิจ เป็นต้น

3. การสร้างความมั่นคงและการสนับสนุนสิทธิเสรีภาพ ประชาธิปไตย และ สิทธิมนุษยชน (Defense and Promotion of Freedom Democracy and Human Rights)

ประเทศสหรัฐอเมริกา มีบทบาทในการสนับสนุนสิทธิเสรีภาพ ประชาธิปไตย และสิทธิมนุษยชน มากขึ้นภายหลังสงครามโลกครั้งที่ 2 รวมถึงการต่อต้านระบอบการปกครองแบบเผด็จการ และรัฐบาลที่กีดกันสิทธิเสรีภาพของประชาชน สิ่งเหล่านี้เป็นองค์ประกอบหลักอันทรงคุณค่าของการปกครองโดยประเทศสหรัฐอเมริกา ที่มีความเป็นประเทศประชาธิปไตย มีความรับผิดชอบต่อประชาชน และหลีกเลี่ยงการทำสงคราม การปกป้องและสนับสนุนสิทธิเสรีภาพ ประชาธิปไตย และ สิทธิมนุษยชนเหล่านี้ คือการสร้างซอฟท์พาวเวอร์ (Soft Power) ให้กับภาพลักษณ์ของประเทศสหรัฐอเมริกา เพราะเป็นการรณรงค์ทางความคิดให้องค์กรต่างๆ และภาคประชาชนที่มีการทำงานร่วมกับประเทศสหรัฐอเมริกา รับรู้และเข้าใจถึงการปฏิบัติงานของประเทศสหรัฐอเมริกา

4. การกีดกันการกำเนิดของประเทศมหาอำนาจใหม่ในแถบทวีปยูเรเซีย (Prevention of Emergence of Regional Hegemons in Eurasia)

องค์ประกอบสุดท้ายของบทบาทของประเทศสหรัฐอเมริกาในการเมืองระหว่างประเทศ เป็นองค์ประกอบที่ไม่ถูกระบุไว้ในนโยบายสาธารณะ คือการกีดกันการกำเนิดของประเทศมหาอำนาจใหม่ในแถบทวีปยูเรเซีย จุดประสงค์ของนโยบายนี้ สะท้อนให้เห็นถึงมุมมองของประเทศสหรัฐอเมริกาในภูมิรัฐศาสตร์และแผนการพัฒนาประเทศจากนักเขียนยุทธศาสตร์และนโยบายของประเทศสหรัฐอเมริกาในช่วงหลังสงครามโลกครั้งที่ 2 และพฤติกรรมของประเทศสหรัฐอเมริกาสามารถแสดงให้เห็นถึงเป้าหมายในการพยายามกีดกันการกำเนิดของประเทศมหาอำนาจใหม่ในแถบทวีปยูเรเซียได้ดังต่อไปนี้

- การเข้าร่วมสงครามโลกครั้งที่ 1 สงครามโลกครั้งที่ 2 สงครามเกาหลี และสงครามเวียดนาม ของประเทศสหรัฐอเมริกา
- การสร้างพันธมิตรและองค์กรความมั่นคงของประเทศสหรัฐอเมริกา ประกอบด้วย องค์กรนาโต้ (NATO alliance) ที่ถูกสร้างขึ้นมาเพื่อการตอบโต้สหภาพโซเวียต (ปัจจุบันคือประเทศรัสเซีย) เพื่อการสร้างความเป็นอำนาจนำในแถบทวีปยุโรป
- การสร้างพันธมิตรกับประเทศแถบเอเชียตะวันออกและแปซิฟิก ที่ถูกสร้างขึ้นเพื่อตอบโต้สหภาพโซเวียต และ ประเทศจีน เพื่อการสร้างความเป็นอำนาจนำในแถบทวีปเอเชีย

- การสร้างองค์กรความมั่นคงกับประเทศต่างๆในแถบทวีปเปอร์เซีย ที่ถูกสร้างขึ้นเพื่อตอบโต้สหภาพโซเวียต และประเทศอิหร่าน เพื่อการสร้างความเป็นอำนาจนำในทวีปนั้นๆ
- และการสร้างนโยบายทางการเมืองระหว่างประเทศ นโยบายทางการทูต และนโยบายทางเศรษฐกิจต่างๆที่ตอบโต้สหภาพโซเวียตในช่วงสงครามเย็น อาทิเช่น แผนมาร์แชล (Marshall Plan)

ความพยายามในการบรรลุเป้าหมายเพื่อกีดกันการกำเนิดประเทศมหาอำนาจใหม่ในแถบทวีปยูเรเซียของประเทศสหรัฐอเมริกานั้น ในบางครั้ง นักนโยบายสาธารณะของประเทศสหรัฐอเมริกาได้ตัดสินใจในการสนับสนุนประเทศที่ไม่ได้มีการปกครองแบบระบอบประชาธิปไตย เพื่อจุดประสงค์ทางการเมือง จากมุมมองที่มองว่าประเทศรัสเซีย จีน และอิหร่าน เป็นคู่แข่งหรือภัยคุกคามของประเทศของตน ซึ่งในท้ายที่สุด เป้าหมายในการกีดกันการกำเนิดประเทศมหาอำนาจใหม่ ในการปกป้องสิทธิเสรีภาพ ประชาธิปไตย และ สิทธิมนุษยชน นำมาซึ่งแรงกดดันทางการเมืองระหว่างประเทศในแถบทวีปเอเชีย (O'Rourke, 2022)

การเป็นประเทศมหอำนาจของประเทศสหรัฐอเมริกา มีปัจจัยส่งเสริมดังที่กล่าวมา ไม่ว่าจะเป็นความเป็นผู้นำระดับโลกหลังสงครามโลกครั้งที่ 2 เป็นผู้วางกฎเกณฑ์และธรรมเนียมของการเมืองระหว่างประเทศ การสร้างกฎระเบียบระหว่างประเทศแบบเสรีนิยมที่เป็นระบอบการปกครองของประเทศของตนเอง การส่งเสริมสิทธิเสรีภาพ สร้างความรับผิดชอบต่อประชากรของประเทศ และมีส่วนในการรับผิดชอบต่อนานาประเทศพันธมิตรด้วยเช่นกัน รวมถึงความพยายามในการสร้างอำนาจในทวีปต่างๆเพื่อวางรากฐานและรักษาความมั่นคงทางอำนาจการเมืองระหว่างประเทศ ซึ่งส่งเสริมการสร้างอำนาจทางไซเบอร์ทางการทหาร ที่จำเป็นต้องพึ่งพาบทบาทและอำนาจทางการเมืองในการสร้างความมั่นคงไซเบอร์ด้วยเช่นกัน

1.2 ลักษณะความเป็นรัฐบาล (Government Characteristic)

รัฐบาลของประเทศสหรัฐอเมริกาให้ความสำคัญกับการปกป้องโลกไซเบอร์เป็นอย่างมาก โดยเฉพาะเรื่องความมั่นคงของประเทศ และความท้าทายต่อโครงสร้างพื้นฐานของประเทศที่ใช้ระบบดิจิทัลเป็นส่วนใหญ่ทั้งด้านการโทรคมนาคม เศรษฐกิจ และสังคม ประธานาธิบดีของประเทศสหรัฐอเมริกา Joe Biden ได้ให้วิสัยทัศน์ต่อแผนยุทธศาสตร์ความมั่นคงทางไซเบอร์แห่งชาติ ไว้ว่า “เทคโนโลยีดิจิทัลคือส่วนหนึ่งของชีวิตประจำวันของประชากรของประเทศสหรัฐอเมริกา การเปิดกว้างและการเชื่อมต่อของโลกอินเตอร์เน็ตคือจุดเปลี่ยนสำคัญที่ทำให้เกิดการการรวมกลุ่มของหลากหลาย รวมถึงความสำคัญของเทคโนโลยีดิจิทัลที่ได้เพิ่มมากขึ้นจากช่วงการระบาดของโรค COVID-19 โดยได้จัดสรรการบริหารงบประมาณจำนวนหกหมื่นห้าพันล้านดอลลาร์สหรัฐ เพื่อให้

มั่นใจได้ว่า ประชากรชาวสหรัฐอเมริกา ได้รับการเชื่อมต่ออินเทอร์เน็ตอย่างทั่วถึง และเป็นอินเทอร์เน็ตความเร็วสูง เพื่อตอบสนองความต้องการในการใช้งานอินเทอร์เน็ตในชีวิตประจำวันไม่ว่าจะเป็นการติดต่อสื่อสารระหว่างผู้ใช้งาน หรือการทำธุรกิจต่างๆผ่านอินเทอร์เน็ต อีกทั้งการสร้างความปลอดภัยต่อการใช้งานอินเทอร์เน็ตที่มีความน่าเชื่อถือ และมีความปลอดภัยขั้นสูง” (United States Government, 2023)

แผนยุทธศาสตร์ความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา ได้ให้ความสำคัญกับการใช้งานของเทคโนโลยีอินเทอร์เน็ตหรือโลกไซเบอร์ ในการใช้งานเพื่อสนับสนุนแนวคิดประชาธิปไตย การมีอิสระในการแสดงความคิดเห็น การพัฒนานวัตกรรม และความเท่าเทียม แต่ในการใช้งานโลกไซเบอร์นั้น ก็มีการใช้งานในทางที่ผิดด้วยเช่นกัน เช่น การใช้งานเพื่อสร้างความขัดแย้งข้ามประเทศ และความเป็นเผด็จการในโลกไซเบอร์ การโจรกรรมข้อมูลและสิทธิบัตรต่างๆ การกระจายข้อมูลเพื่อบิดเบือน การสร้างความเสียหายต่อโครงสร้างพื้นฐาน การใช้งานเพื่อการล่วงละเมิดต่างๆ การก่ออาชญากรรม หรือการสนับสนุนการใช้ความรุนแรงแบบสุดขั้ว ซึ่งล้วนแต่ส่งผลกระทบต่อความสงบและความมั่นคงทั้งสิ้น การเพิ่มขึ้นของการเชื่อมต่อระหว่างประชากรด้วยเทคโนโลยีโลกไซเบอร์สามารถสร้างผลที่ดีต่อการใช้ชีวิต รวมถึงผลร้ายด้วยเช่นกัน

ประเทศสหรัฐอเมริกาให้ความสำคัญกับโลกไซเบอร์เชิงนโยบายในรูปแบบการวิเคราะห์เชิงกลยุทธ์ในการวางแผนยุทธศาสตร์ความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา การวิเคราะห์ไปยังหลากหลายปัจจัยเพื่อให้ครอบคลุมกับวิสัยทัศน์ของประธานาธิบดี Joe Biden การเกิดขึ้นของกระแสโลกไซเบอร์ที่สามารถสร้างโอกาสการพัฒนา ความท้าทายต่างๆที่ต้องเผชิญ รวมถึงวิเคราะห์ตัวแสดงที่มุ่งร้ายต่อกระบวนการการทำงานโลกไซเบอร์ของประเทศสหรัฐอเมริกาเพื่อการพัฒนาแผนยุทธศาสตร์ให้มีความครอบคลุม เที่ยงตรง เป็นไปได้ และดำเนินการไปพร้อมกับแนวคิดระบอบประชาธิปไตย ปัจจัยที่ใช้ในการประเมินรูปแบบการวิเคราะห์เชิงกลยุทธ์ในการวางแผนยุทธศาสตร์ความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา ประกอบไปด้วย 2 ปัจจัย ดังนี้

1. ปัจจัยทางด้านแนวโน้มที่สามารถเกิดขึ้นได้ในอนาคต (Emerging trends)

ปัจจัยที่เกี่ยวข้องกับการที่โลกกำลังก้าวเข้าสู่ช่วงที่มีความซับซ้อนทางเทคโนโลยีมากยิ่งขึ้น ซอฟต์แวร์และระบบต่างๆได้มีการพัฒนาให้มีการทำงานที่ซับซ้อนเพื่อตอบสนองความต้องการของผู้บริโภคและสร้างผลประกอบการให้กับบริษัทต่างๆ แต่การพัฒนาต่างๆนั้นมาพร้อมกับความไม่ปลอดภัยที่เพิ่มมากขึ้นด้วยเช่นกัน เทคโนโลยีที่เริ่มเป็นกระแส ณ ปัจจุบัน และเป็นสิ่งที่ควรให้ความสำคัญคือเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) ที่สามารถทำงานได้อย่างรวดเร็ว และไม่สามารถคาดการณ์ผลลัพธ์ที่สามารถเกิดขึ้นได้แม้กระทั่งต่อผู้พัฒนาเองก็ตาม

การขับเคลื่อนด้วยระบบเทคโนโลยีที่มีความซับซ้อนและเป็นมีระบบที่พึ่งพาซึ่งกันและกัน อินเทอร์เน็ตได้เชื่อมต่อผู้ใช้งาน ธุรกิจต่างๆ สังคม และประเทศต่างๆเข้าหากันบนแพลตฟอร์มเดียวกัน เพื่อทำการปฏิสัมพันธ์หรือแลกเปลี่ยนข้อมูลซึ่งกันและกันในระหว่างประเทศ แต่ในการเชื่อมต่อเหล่านี้ก็สามารถส่งผลร้ายได้ด้วยเช่นกัน การโจมตีองค์กร บริษัท หรือ ประเทศ ที่สามารถเกิดขึ้นได้อย่างรวดเร็วผ่านการโจมตีทางไซเบอร์ อาทิเช่น การโจมตีจากประเทศรัสเซียใน ค.ศ. 2017 ในการโจมตีไซเบอร์ NotPetya ที่ได้ทำการโจมตีประเทศยูเครน ซึ่งการโจมตีนั้นได้ทำการแพร่กระจายความเสียหายไปยังทวีปยุโรป เอเชีย และสหรัฐอเมริกาด้วยเช่นกัน สร้างความเสียหายมากกว่าหลายร้อยล้านดอลลาร์สหรัฐ การกำเนิดขึ้นของความซับซ้อนทางเทคโนโลยีดิจิทัล จะสามารถสร้างความเป็นไปได้ และโอกาสรูปแบบใหม่ให้กับมนุษยชาติ และสามารถสร้างความเสี่ยงในการเกิดผลกระทบทางด้านลบได้มากยิ่งขึ้นด้วยเช่นกัน

2. ปัจจัยทางด้านตัวแสดงที่มุ่งร้ายต่อประเทศ (Malicious actors)

พฤติกรรมที่สร้างความเสียหายจากการโมตีทางไซเบอร์ได้มีการพัฒนามาอย่างต่อเนื่อง ไม่ว่าจะเป็นการแฮ็กเว็บไซต์เพื่อสร้างความเสียหายทางภาพลักษณ์ (nuisance defacement) การจารกรรมข้อมูล (espionage) และการโจรกรรมสินทรัพย์ปัญญหา (intellectual property theft) การโจมตีเพื่อสร้างความเสียหายต่อโครงสร้างพื้นฐาน (damaging attack against critical infrastructure) การโจมตีด้วยแรนซัมแวร์ (ransom attacking) และ การใช้โลกไซเบอร์ในการสร้างผลกระทบต่อภาพลักษณ์ของระบอบประชาธิปไตยของประเทศสหรัฐอเมริกา ในปัจจุบัน มีเพียงบางประเทศในโลกเท่านั้นที่มีทรัพยากรทางเทคโนโลยีที่เพียงพอต่อการโจมตีทางไซเบอร์ อาวุธทางไซเบอร์ได้เสริมสร้างประสิทธิภาพในการโจมตีให้กับประเทศเหล่านี้ในการสร้างความเสียหายต่อผลประโยชน์แห่งชาติของประเทศสหรัฐอเมริกาในโลกไซเบอร์ และทำให้องค์กรก่อการร้ายระหว่างประเทศมีการพัฒนาอาวุธเพื่อสร้างภัยคุกคามรูปแบบใหม่ได้มากยิ่งขึ้น โดยประเทศที่เป็นภัยคุกคามในมุมมองของรัฐบาลสหรัฐอเมริกา ประกอบด้วย ประเทศจีน, รัสเซีย, อิหร่าน, เกาหลีเหนือ และประเทศอื่นๆที่ปกครองด้วยระบอบอำนาจนิยมที่ได้รับอิทธิพลจากแนวคิดของ Karl Marx ในการสร้างการโจมตีทางไซเบอร์อย่างรุนแรงเพื่อบรรลุจุดประสงค์ต่างๆของประเทศตนเองโดยขัดหลักประเพณีระหว่างประเทศที่ประเทศสหรัฐอเมริกาได้ยึดถือเป็นธรรมเนียมเสมอมา (The White House, 2023)

การบริหารประเทศโดยรัฐบาลแบบประเทศสหรัฐอเมริกา ส่งเสริมอำนาจทางไซเบอร์ด้วยการให้ความสำคัญกับความมั่นคงทางไซเบอร์ ผ่านนโยบายการบริหารงบประมาณที่ถูกจัดสรรมาเพื่อพัฒนาไซเบอร์เพื่อความมั่นคงของโครงสร้างพื้นฐานที่สำคัญ การใช้ชีวิตประจำวันของประชากรเพื่อ

ส่งเสริมการสร้างองค์ความรู้และความคุ้นชินกับการใช้ไซเบอร์ในด้านต่างๆของประชากร การสนับสนุนสิทธิเสรีภาพในการใช้งานไซเบอร์เพื่อการแสดงความคิดเห็นต่างๆ และการสร้างเสถียรภาพของการดำเนินระบบเศรษฐกิจของประเทศสหรัฐอเมริกา

1.3 วัตถุประสงค์ทางการทหาร (Military purposes)

กองทัพบกสหรัฐได้นำหลักการในงานเขียนของ Clausewitz ที่มีชื่อว่า “On War” และนักคิดทางการทหารหลากหลายคน มาทำการดัดแปลงและนำไปใช้ในการวางแผนยุทธศาสตร์การทำสงครามเพื่อให้การโจมตีที่อิงจากแนวคิดจุดแรงโน้มถ่วงของ Clausewitz มีประสิทธิภาพมากยิ่งขึ้น และตีพิมพ์ในคู่มือแผนปฏิบัติการ FM 3-0 ซึ่งหลักการการทำสงครามของกองทัพบกสหรัฐประกอบด้วย

1. จุดประสงค์ (Objective) คือ “ทิศทางการปฏิบัติการทางการทหารที่มีเป้าหมายชัดเจน, เด็ดขาด, และ มีความเป็นไปได้”
2. การรุกราน (Offensive) คือ การเข้ายึด, รักษาให้คงอยู่, และ การแสวงหาผลประโยชน์
3. การจัดสรรพละกำลัง (Economy of Force) คือ การจัดสรรพละกำลังของการโจมตีให้น้อยที่สุดเพื่อการโจมตีในครั้งถัดไป
4. มวล (Mass) คือ “การประเมินผลกระทบที่เกิดขึ้นจากการปฏิบัติการอย่างรอบคอบทั้งในแง่ของสถานที่และเวลา”
5. การซ้อมรบ (Maneuver) คือ “การวางตำแหน่งสถานที่ในตำแหน่งที่ศัตรูเสียเปรียบผ่านการรูปแบบการรบที่ยืดหยุ่น”
6. ความเป็นเอกภาพของการสั่งการ (Unity of command) คือ “การยึดมั่นในจุดประสงค์ หรือ เป้าหมายของคำสั่งภายใต้ผู้บังคับบัญชาเพียงคนเดียว”
7. ความเรียบง่าย (Simplicity) คือ “การเตรียมการที่ชัดเจน, การวางแผนที่ไม่ซับซ้อนและชัดเจน, สร้างความรัดกุมเพื่อความเข้าใจที่ง่ายต่อการปฏิบัติการ”
8. การสร้างความเสียหายโดยไม่ทันตั้งตัว (Surprise) คือ “การโจมตีศัตรูในช่วงเวลา หรือ สถานที่ หรือ สถานการณ์ที่ศัตรูไม่ทันตั้งตัว”
9. ความปลอดภัย (Security) คือ “การไม่ยินยอมให้ศัตรูสร้างความได้เปรียบอย่างไม่คาดคิด”

การศึกษาความสัมพันธ์และผลกระทบจากการโจมตีทางไซเบอร์ ตัวแสดงที่หลากหลายที่ได้รับผลกระทบทางไซเบอร์ จะได้รับผลกระทบที่แตกต่างกัน ทำให้เราได้เห็นถึงปัจจัยที่เป็นจุดสำคัญ

หรือเรียกว่า จุดศูนย์กลางแรงโน้มถ่วง (Center of gravity) ที่สามารถส่งผลกระทบต่อโครงสร้างสำคัญของประเทศได้จากการถูกโจมตี รวมถึงการศึกษาแนวทางการวางยุทธศาสตร์การทำสงครามของแผนยุทธศาสตร์ของกองทัพบกสหรัฐ ที่มีการวางแผนไว้อย่างครอบคลุมในการปฏิบัติการ แต่ยุทธศาสตร์ที่วางแผนมานั้น เมื่อนำมาปฏิบัติจริง อาจมีความแตกต่างทางด้านข้อได้เปรียบในแต่ละสถานที่ที่ใช้ในการทำสงครามที่แตกต่างกันออกไป (Elbaum, 2008)

นอกจากแผนยุทธศาสตร์ในการทำสงครามของประเทศสหรัฐอเมริกาแล้วนั้น ในแผนความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา เป็นสิ่งที่ควรทำการศึกษาด้วยเช่นกัน โดยกระบวนการสร้างความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา มีจุดประสงค์หลัก คือ การสร้างความร่วมมือระหว่างประเทศเพื่อสร้างระบบนิเวศทางดิจิทัล (digital ecosystem) ให้กลายเป็นรากฐานสำคัญในการสร้างความมั่นคงให้กับประเทศสหรัฐอเมริกาและประเทศพันธมิตร โดยหลักการที่นำมาปรับใช้ในการสร้างความมั่นคงทางไซเบอร์นี้ ประกอบไปด้วย 5 เสาหลักด้วยกัน คือ 1. การปกป้องโครงสร้างพื้นฐานสำคัญ 2. การจำกัดการเข้าถึงโลกไซเบอร์ของตัวแสดงที่เป็นภัยต่อประเทศสหรัฐอเมริกา 3. กำหนดกลไกตลาดให้ขับเคลื่อนในการพัฒนาความมั่นคง 4. การลงทุนเพื่อการสร้างความมั่นคงในอนาคต และ 5. การสร้างความสัมพันธ์ที่ดีระหว่างประเทศเพื่อร่วมกันบรรลุเป้าหมาย หลักการต่างๆ จำเป็นต้องพึ่งพาการร่วมมือกันของหลากหลายองค์กรในการสร้างความมั่นคงทางไซเบอร์ ไม่ว่าจะเป็น ภาคเอกชน ภาคอุตสาหกรรม ภาคประชาสังคม และประเทศพันธมิตรต่างๆ ซึ่งในแต่ละเสาหลักมีวัตถุประสงค์เชิงกลยุทธ์ที่แตกต่างกันออกไป (The White House, 2023) ดังนี้

1. การปกป้องโครงสร้างพื้นฐานสำคัญ (Defend critical infrastructure) คือ การปกป้องระบบและทรัพย์สินที่มีความสำคัญต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ และเศรษฐกิจ ประชากรชาวอเมริกันต้องมีความมั่นใจในระบบความปลอดภัยและการทำงานที่สามารถปรับเปลี่ยนตามสถานการณ์ได้ตลอดเวลาของระบบโครงสร้างพื้นฐาน โดยรัฐบาลสหรัฐอเมริกา มุ่งเป้าไปยังการสร้างความร่วมมือในการสร้างการปกป้องโครงสร้างพื้นฐานที่มีการปฏิบัติการที่มีประสิทธิภาพและมั่นคงเพื่อลดความเสี่ยง และการขับเคลื่อนระดับของความปลอดภัยของโลกดิจิทัลให้ดียิ่งขึ้น

การป้องกันภัยคุกคามร้ายแรงทางไซเบอร์ สามารถกระทำได้จากการมีเทคโนโลยีที่ทันสมัย มีการป้องกันความมั่นคงทางไซเบอร์อย่างเพียงพอ เพื่อที่จะทำให้ผู้โจมตีไม่สามารถสร้างความเสียหายต่อประเทศได้ ฝ่ายบริหารของประเทศสหรัฐอเมริกาเห็นถึงความสำคัญของความมั่นคงทางไซเบอร์ และได้ทำการสร้างความมั่นคงทางไซเบอร์ในหลากหลายภาคส่วน โดยเฉพาะภาคส่วนที่มีความสำคัญต่อความมั่นคงของประเทศ

รวมถึงการร่วมมือจากภาคเอกชน ที่ได้ให้ความสำคัญในการร่วมมือกับภาครัฐในการสร้างความร่วมมือในการปกป้องความมั่นคงทางไซเบอร์ของประเทศ อาทิเช่น การรณรงค์ Shields Up ที่ได้ถูกนำมาใช้ในช่วง ค.ศ. 2022 ในเหตุการณ์สงครามระหว่างประเทศรัสเซียและยูเครน เพื่อเป็นการสร้างการเตรียมพร้อมและสนับสนุนการตั้งรับการโจมตีทางไซเบอร์ที่สามารถเกิดขึ้นได้ในช่วงเวลาดังกล่าว ซึ่งเป็นตัวอย่างการทำงานร่วมกันระหว่างภาครัฐบาลและภาคเอกชนที่มีประสิทธิภาพเป็นอย่างมาก

รัฐบาลสหรัฐอเมริกามีความต้องการในการสร้างขีดความสามารถและนวัตกรรมรูปแบบใหม่ที่สามารถทำให้เกิดความร่วมมือกันระหว่างหลากหลายภาคส่วนไม่ว่าจะเป็นรัฐบาลหรือผู้มีส่วนเกี่ยวข้องกับโครงสร้างพื้นฐาน องค์กรภาครัฐ ภาคเอกชน และผู้มีส่วนเกี่ยวข้องในการร่วมมือกันเพื่อทำให้เกิดเทคโนโลยีใหม่ที่มีความเร็วและขีดความสามารถที่ล้ำหน้ามากยิ่งขึ้น องค์กรภาครัฐที่มีส่วนเกี่ยวข้องกับการทำงานในโครงสร้างพื้นฐาน ควรมีการเพิ่มการพัฒนาและขีดความสามารถในการทำงานร่วมกันกับหลากหลายองค์กร เมื่อมีสถานการณ์ฉุกเฉินเกิดขึ้น องค์กรภาครัฐต้องสามารถตอบโต้และรับมือต่อเหตุการณ์ต่างๆที่เกิดขึ้นได้อย่างทันท่วงทีด้วยการทำงานร่วมกันระหว่างองค์กร รวมถึงการร่วมมือกับภาคเอกชนด้วยเช่นกัน

2. การจำกัดการเข้าถึงโลกไซเบอร์ของบทบาทตัวแสดงที่เป็นภัยต่อประเทศสหรัฐอเมริกา (Disrupt and Dismantle threat actors) คือ การใช้ทรัพยากรทุกอย่างด้วยอำนาจของรัฐในการจำกัดภัยคุกคามจากตัวแสดงที่มุ่งร้ายต่อผลประโยชน์แห่งชาติของประเทศสหรัฐอเมริกา ไม่ว่าจะเป็นทางด้านการเมือง ด้านข้อมูล ด้านการทหาร (ทั้งการทหารแบบดั้งเดิมและไซเบอร์) ด้านการเงิน ด้านองค์ความรู้ และ ด้านการบังคับใช้กฎหมาย ด้วยเป้าหมายในการทำให้ตัวแสดงที่เป็นภัยคุกคามไม่สามารถเข้าถึงโลกไซเบอร์ในการปฏิบัติการต่างๆได้ และเป็นการสร้างความมั่นคงให้กับประเทศและสาธารณะจากภัยคุกคามต่างๆที่สามารถเกิดขึ้น

ความพยายามในการร่วมมือกันระหว่างภาครัฐและภาคเอกชน ได้พิสูจน์ให้เห็นถึงประสิทธิภาพในการทำลายปฏิบัติการการโจมตีทางไซเบอร์ต่างๆ ไม่ว่าการโจมตีนั้นจะพมาจากภาครัฐของต่างประเทศ อาชญากร และตัวแสดงที่เป็นภัยอื่นๆ องค์กรภาครัฐได้เพิ่มขีดความสามารถในการตอบโต้เหตุการณ์ทางไซเบอร์ต่างๆที่สามารถเกิดขึ้น ไม่ว่าจะเป็น การจับกุมองค์กรอาชญากรไซเบอร์ข้ามชาติด้วย (Transnational cybercriminals) และ แฮ็กเกอร์ที่ได้รับการสนับสนุนจากรัฐ (state-sponsored

actors) การกำหนดบทลงโทษให้กับตัวแสดงทางไซเบอร์ที่เป็นภัยคุกคาม (malicious cyber actors) ไม่ว่าจะเป็นการสั่งห้ามในการเดินทางและการปิดกั้นการเข้าถึงการใช้บริการทางการเงิน และการกีดกันตัวแสดงที่เป็นภัยในการเข้าถึงโครงสร้างพื้นฐานทางดิจิทัลและเครือข่ายอาชญากรรมต่างๆ ทางภาครัฐได้ทำการมุ่งเป้าไปยังการโจมตีโครงสร้างพื้นฐานทางการเงินที่ใช้ในการปฏิบัติการโจมตีทางไซเบอร์จากตัวแสดงที่เป็นภัยต่อภาครัฐ การสร้างการเมืองระหว่างประเทศแบบใหม่ในการร่วมมือกันเพื่อทำลายกิจกรรมทางไซเบอร์ต่างๆที่เป็นภัย เพื่อทำให้ตัวแสดงนั้นๆไม่สามารถดำเนินปฏิบัติการต่อได้ และช่วยทำให้กู้คืนสินทรัพย์ต่างๆที่ถูกได้มาโดยมิชอบ โดยมีมูลค่ามากกว่าร้อยล้านดอลลาร์

3. กำหนดกลไกตลาดให้ขับเคลื่อนในการพัฒนาความมั่นคงและความยืดหยุ่น (Shape market forces to drive security and resilience) คือ การสร้างความมั่นคงและความยืดหยุ่นสำหรับอนาคตที่รัฐบาลสหรัฐอเมริกาต้องการ เป็นการกำหนดทิศทางตลาดในการสร้างความรับผิดชอบต่อกลุ่มผู้ใช้งานระบบนิเวศทางดิจิทัลเพื่อให้ผู้ใช้งานมีความปลอดภัยมากที่สุดเพื่อการลดความเสี่ยงต่างๆที่สามารถเกิดขึ้นได้ รัฐบาลสหรัฐอเมริกาต้องการลดความเสี่ยงจากการมีความมั่นคงทางไซเบอร์ที่ต่ำให้ได้มากที่สุดเพื่อหลีกเลี่ยงภัยอันตรายต่างๆ และทำให้ระบบนิเวศทางดิจิทัลหรือโลกไซเบอร์ของประเทศสหรัฐอเมริกา เป็นระบบนิเวศทางดิจิทัลที่มีความน่าเชื่อถือให้ได้มากที่สุด เป้าหมายของรัฐบาลสหรัฐอเมริกาในการกำหนดกลไกตลาดนี้ คือความตั้งใจในการส่งเสริมตลาดที่เกี่ยวข้องกับโลกไซเบอร์เพื่อสร้างความปลอดภัยและเพื่อการพัฒนานวัตกรรมและการแข่งขันต่างๆ โดยไม่ใช่การชี้นำตลาดหรือการแทรกแซงทางการตลาดแต่อย่างใด

การถูกแทรกแซงโครงสร้างพื้นฐานและการจารกรรมข้อมูลผู้ใช้งานในภาคเอกชนคือสิ่งที่ทำให้เห็นได้ชัดเจนว่า ภาคเอกชนไม่สามารถที่จะขับเคลื่อนตลาดได้ จำเป็นที่จะต้องพึ่งพาการนำความมั่นคงทางไซเบอร์และความยืดหยุ่นทางการบริหารบริษัทเข้ามาทำหน้าที่ในการรักษาความมั่นคงและปลอดภัยของบริษัทต่างๆ ในหลากหลายกรณีที่เกิดขึ้นนั้น องค์กร หรือ บริษัทต่างๆเลือกที่จะไม่ลงทุนทางด้านความปลอดภัยทางไซเบอร์ ส่งผลให้เกิดการกระทบต่อความมั่นคงของบริษัทนั้นๆอยู่บ่อยครั้ง และผลกระทบที่เกิดขึ้น ส่งผลต่อเครือข่ายบริษัทต่างๆที่ได้ทำธุรกิจต่างๆด้วยเช่นกัน ดังนั้นการส่งเสริมการขับเคลื่อนตลาดเพื่อสร้างความมั่นคงทางไซเบอร์ของรัฐบาลสหรัฐอเมริกา คือการสนับสนุนในการสร้างความมั่นคงทางไซเบอร์เพื่อให้การขับเคลื่อนทางเศรษฐกิจมีความ

มั่นคง ปลอดภัย และยืดหยุ่นต่อทุกสถานการณ์ที่สามารถเกิดขึ้นได้จากผลกระทบทางไซเบอร์

4. การลงทุนเพื่อการสร้างความมั่นคงในอนาคต (Invest in a resilient future) คือ การสร้างอนาคตทางดิจิทัลที่มีความมั่นคง และสามารถปรับเปลี่ยนได้อย่างมีประสิทธิภาพตามสถานการณ์ คือการลงทุนที่ต้องเริ่มจากปัจจุบัน การสร้างความปลอดภัย ความมั่นคง และความเป็นส่วนตัว รวมทั้งการสร้างระบบนิเวศทางดิจิทัล คือ การดำเนินการผ่านแผนการลงทุนและการทำงานร่วมกันของทุกภาคส่วน ในการที่จะบรรลุเป้าหมายนี้ ประเทศสหรัฐอเมริกาจำเป็นต้องรักษาการเป็นผู้นำทางด้านนวัตกรรมทั้งทางด้านความปลอดภัยและความมั่นคงของเทคโนโลยีและโครงสร้างพื้นฐานทั้งในปัจจุบันและอนาคต

ส่วนประกอบพื้นฐานที่สำคัญของระบบนิเวศทางดิจิทัล อาทิเช่น อินเทอร์เน็ต คือสิ่งที่สร้างความมั่นคงและสนับสนุนระบบเศรษฐกิจไม่ว่าจะเป็นทั้งภาครัฐและภาคเอกชน อย่างไรก็ตาม การลงทุนทางด้านความมั่นคงทางไซเบอร์ของทางภาครัฐและภาคเอกชนล้วนเผชิญภัยคุกคามและความท้าทายต่างๆมากมาย นับตั้งแต่การเริ่มต้นสร้างโครงสร้างพื้นฐานทางดิจิทัลในยุคใหม่ จากการสื่อสารแบบโทรคมนามคม สู่การปฏิวัติทางด้านเทคโนโลยีและทรัพยากรพลังงานต่างๆ รวมถึงนวัตกรรมปัญญาประดิษฐ์และการคำนวณเชิงควอนตัม ความต้องการในการลงทุนทางด้านเทคโนโลยีและดิจิทัลได้กลายเป็นส่วนสำคัญในการลงทุนเพื่อสร้างการพัฒนาสำหรับภาครัฐและภาคเอกชนมากขึ้นอย่างมีนัยสำคัญ

องค์กรภาครัฐต้องจัดสรรงบประมาณเพื่อลงทุนในการสร้างนวัตกรรมทางดิจิทัลและเทคโนโลยี การค้นคว้าและพัฒนา และการพัฒนาทางด้านศึกษาเพื่อขับเคลื่อนผลลัพธ์ที่สามารถทำให้ระบบเศรษฐกิจขับเคลื่อนอย่างมั่นคงและสร้างผลประโยชน์แห่งชาติให้กับประเทศได้ ภาครัฐจำเป็นต้องยกระดับมูลนิธิวิทยาศาสตร์แห่งชาติ (National Science Foundation) ที่ใช้ในการพัฒนานวัตกรรมทางด้านเครื่องจักร การพัฒนาความปลอดภัยระยะยาว และการสร้างความน่าเชื่อถือในโลกไซเบอร์ รวมถึงการส่งเสริมทางด้านเงินทุนในการสร้างกฎหมายโครงสร้างพื้นฐานฉบับใหม่ (Bipartisan Infrastructure law), กฎหมายลดอัตราเงินเฟ้อ (Inflation Reduction Act), กฎหมายชิปส์และวิทยาศาสตร์ (CHIPS and Science Act) การพัฒนาสถาบันศึกษาทางด้านต่างๆ และองค์ประกอบอื่นๆที่มีส่วนในการศึกษาและพัฒนาดดิจิทัลของภาครัฐด้วยเช่นกัน

5. การสร้างความสัมพันธ์ที่ดีระหว่างประเทศเพื่อร่วมกันบรรลุเป้าหมาย (Forge International Partnerships To Pursue Shared Goals) คือ ประเทศสหรัฐอเมริกามี

วิสัยทัศน์ที่เกี่ยวข้องกับโลกไซเบอร์ของโลกใบนี้คือ การให้คุณค่าประเทศที่มีความรับผิดชอบต่อโลกไซเบอร์ ควรได้รับการสนับสนุนและได้รับคุณค่าในการทำงานร่วมกัน และประเทศที่ใช้ไซเบอร์ในทางที่ผิดหรือไม่มีความรับผิดชอบต่อโลกไซเบอร์ คือประเทศที่จะไม่ได้รับการสนับสนุนจากประเทศสหรัฐอเมริกา การทำให้หลักการข้อนี้บรรลุผลลัพธ์จำเป็นที่จะต้องสร้างความร่วมมือระหว่างประเทศเพื่อร่วมกันกำหนดจุดประสงค์ร่วมกันอย่างชัดเจนในการกำหนดปัญหาที่สามารถเกิดขึ้นได้ และร่วมกันวางแผนในการเปิดโลกเสรีในการทำงานร่วมกันทางด้านไซเบอร์ และร่วมกันสร้างความมั่นคงทางไซเบอร์ให้สำเร็จ

ในหลากหลายทศวรรษที่องค์กรความร่วมมือระหว่างประเทศได้ทำงานร่วมกันเพื่อนิยามและการร่วมกันดูแลความรับผิดชอบต่อพฤติกรรมต่างๆที่เกิดขึ้นในโลกไซเบอร์ กระบวนการความร่วมมือระหว่างประเทศที่เกิดขึ้นในองค์กรต่างๆไม่ว่าจะเป็น the United Nations (UN), Group of Governmental Experts and Open-Ended Working Group ในการพัฒนากรอบแนวคิดที่ประกอบไปด้วยการกำหนดบรรทัดฐานการประพฤติปฏิบัติในช่วงที่ปราศจากสงครามในโลกไซเบอร์ และการสร้างมาตรการสร้างความมั่นใจและความปลอดภัยระหว่างประเทศที่สมาชิก UN ได้เข้าร่วมลงนามเห็นชอบในงานประชุมประจำปีของ UN ประเทศสหรัฐอเมริกาสนับสนุนการขยายงานประชุมที่ประเทศ Budapest เกี่ยวกับอาชญากรรมทางไซเบอร์ (Cybercrime) และกิจกรรมต่างๆทั่วโลกที่มีส่วนเกี่ยวข้องกับการพัฒนาทำให้เกิดความมั่นคงทางไซเบอร์ต่อโลกใบนี้ เพื่อตอบโต้ภัยต่างๆที่เกิดขึ้นในโลกไซเบอร์ด้วยการประสานความร่วมมือระหว่างประเทศ และทำให้โลกอินเทอร์เน็ตของโลกใบนี้เป็นโลกเสรีที่ปลอดภัยและมั่นคง ปราศจากการคุกคามทางไซเบอร์ระหว่างประเทศ และการสร้างระบบนิเวศดิจิทัลร่วมกัน จะสามารถทำให้เกิดความมั่นคงให้กับโลกไซเบอร์ได้มากยิ่งขึ้นในทุกภาคส่วน ประเทศสหรัฐอเมริกามีวัตถุประสงค์ในการทำงานร่วมกันเพื่อต่อต้านองค์กรอาชญากรรมข้ามชาติและตัวแสดงไซเบอร์ต่างๆที่เป็นภัยคุกคาม รวมถึงการสร้างการทำงาร่วมกันกับประเทศพันธมิตรเพื่อร่วมกันสร้างกฎหมายระหว่างประเทศในการควบคุมพฤติกรรมที่ไม่เหมาะสมต่างๆในโลกไซเบอร์ร่วมกัน (The White House, 2023)

1.4 อำนาจทางการทหาร (Military Power)

อำนาจทางการทหารของประเทศต่างๆ ประกอบด้วย อำนาจทางบก (Power on Land) อำนาจในทะเล (Power at Sea) อำนาจในอากาศ (Power in Air) และ อำนาจในอวกาศ (Power in Space) ผู้เขียนได้ทำการศึกษาอำนาจทางการทหารประเภทต่างๆของประเทศสหรัฐอเมริกา มีเนื้อหาดังต่อไปนี้

1. อำนาจทางบกของประเทศสหรัฐอเมริกา (Power on Land)

กองทัพบกสหรัฐ คือ หน่วยงานหลักของประเทศสหรัฐอเมริกาในการทำสงครามทางบก ถึงแม้ว่าทหารบกจะมีความสามารถที่หลากหลายในการปฏิบัติหน้าที่ได้หลายรูปแบบ แต่หน้าที่หลักของทหารบกคือการปกป้องผลประโยชน์แห่งชาติและทำลายศัตรูในสนามรบทางบก กองกำลังทหารบกสหรัฐได้ทำการเข้าร่วมในการปกป้องและผลักดันผลประโยชน์แห่งชาติของประเทศสหรัฐอเมริกาอย่างต่อเนื่องตั้งแต่อดีตจนถึงปัจจุบัน โดยในเดือนพฤษภาคม ค.ศ. 2021 จนถึงเดือน เมษายน ค.ศ. 2022 กองทัพบกสหรัฐได้ทำการส่งกำลังเสริมจำนวน 120,000 นายเข้าร่วมมากกว่า 140 ประเทศ โดยเฉพาะประเทศในเขตกลุ่มประเทศ NATO ที่ได้เป็นป้อมปราการในการต่อต้านการรุกรานของประเทศรัสเซียในสงครามรัสเซียยูเครน

กองทัพบกสหรัฐกำลังเผชิญหน้ากับแรงกดดันทางด้านปฏิบัติการทางการทหารที่เหนือความคาดหมาย ไม่ว่าจะเป็นการเปลี่ยนแปลงของรูปแบบสงครามที่ใช้เทคโนโลยีมากยิ่งขึ้น รวมถึงการเผชิญหน้ากับแรงกดดันทางด้านการเงิน นวัตกรรมทางเทคโนโลยีที่ใช้ในการทำสงคราม ไม่ว่าจะเป็นขีปนาวุธทางไกล สงครามอิเล็กทรอนิกส์ และอาวุธยุทโธปกรณ์ต่างๆ ล้วนแต่ใช้ทรัพยากรทางด้านการเงินเป็นอย่างมาก และได้รับผลกระทบทางการเงินจากอัตราเงินเฟ้อที่เพิ่มสูงขึ้นด้วยเช่นกัน การเผชิญความท้าทายทางด้านการพัฒนาทางเทคโนโลยี อาทิเช่น ประเทศคู่แข่งที่มีความสามารถในการพัฒนาการใช้โดรนในการโจมตีอย่างประเทศจีน สงครามข้อมูล หรือสงครามไซเบอร์ที่จำเป็นต้องพึ่งพาความรวดเร็วและการตัดสินใจที่เด็ดขาดในการทำการโจมตี พัฒนาการต่างๆที่เกิดขึ้นนำพามาสู่การเปลี่ยนแปลงของรูปแบบสงครามอย่างหลีกเลี่ยงไม่ได้ และกองทัพบกสหรัฐได้พัฒนารูปแบบปฏิบัติการทางทหารมาอย่างต่อเนื่องจากการปรับใช้เทคโนโลยีต่างๆ

อัตราเงินเฟ้อกลายเป็นปัจจัยหนึ่งในการสร้างผลกระทบต่อกองทัพบกสหรัฐ โดยกองทัพบกสหรัฐได้สูญเสียงบประมาณในการจัดซื้ออาวุธจำนวนสี่หมื่นหกพันล้านดอลลาร์

สหรัฐจากงบประมาณ ค.ศ. 2019 และหากเปรียบเทียบอัตราเงินเฟ้อที่เพิ่มสูงขึ้น 5 เปอร์เซ็นต์จาก ค.ศ. 2022 ถึง ค.ศ. 2023 งบประมาณที่กองทัพบกสหรัฐได้ถูกจำกัดลดลงจำนวนมากกว่าหกพันล้านดอลลาร์สหรัฐ สัญญาณจากการถูกลดงบประมาณทางการทหารทำให้เห็นถึงการถูกลดทอนอำนาจทางการทหารของกองทัพบกสหรัฐ และเป็นการลดทอนงบประมาณในอัตราส่วนที่ต่ำมากกว่าประวัติศาสตร์ที่เคยผ่านมา

การถูกลดทอนความสำคัญทางด้านอำนาจทางบกของประเทศสหรัฐอเมริกา คือสิ่งที่น่ากังวลโดยมีข้อถกเถียงว่า ประเทศสหรัฐอเมริกานั้น ไม่จำเป็นต้องมีกองทัพกำลังทางการทหารที่มีประสิทธิภาพมาก ด้วยเหตุผลในการยกตัวอย่างประเทศจีน ที่เป็นประเทศมหาอำนาจแต่ยังไม่เคยเกิดการโจมตีทางกายภาพเกิดขึ้นนับตั้งแต่ประวัติศาสตร์ แต่ความเป็นจริงที่เกิดขึ้น ณ ปัจจุบัน สงครามรัสเซียยูเครนในยุโรปคือสิ่งที่ทำให้เห็นถึงความสำคัญของอำนาจทางบกที่ต้องใส่ใจกับการเสริมสร้างประสิทธิภาพให้กับประเทศสหรัฐอเมริกา รวมถึงความสำคัญในการสร้างอำนาจในทุกสนามรบที่สามารถเกิดขึ้นได้ทั้งในระยะสั้นและระยะยาว

นอกจากอัตราเงินเฟ้อที่ส่งผลต่ออำนาจทางบกของกองทัพสหรัฐแล้ว ผลกระทบจากโรค COVID-19 ก็เป็นอีกหนึ่งปัจจัยที่ลดทอนความสามารถของกองกำลังทหารสหรัฐจากการยกเลิกการฝึกทหารและการรับสมัครทหารในปีงบประมาณ ค.ศ. 2021 รวมถึงผลกระทบทางด้านเศรษฐกิจที่ทำให้การรับสมัครทหารเป็นไปอย่างยากลำบาก ในปัจจุบัน ค.ศ. 2023 การลดทอนงบประมาณทางการทหารส่งผลให้เกิดการลดจำนวนการรับสมัครทหารทั้งหมดจำนวน 12,000 นาย นับตั้งแต่ค.ศ. 2018 กองทัพสหรัฐต้องเผชิญกับการรับสมัครทหารที่ไม่สามารถทำให้บรรลุเป้าหมายที่วางไว้ และจำเป็นต้องรับสมัครทหารที่เคยรับราชการให้กลับมาปฏิบัติหน้าที่ต่อ ผลลัพธ์ของปัญหาการรับสมัครทหารใหม่ประกอบด้วยการลดลงของจำนวนผู้ชายที่ต้องการสมัครทหาร การเผชิญกับปัญหาการว่างงาน และความพร้อมในหลากหลายด้าน รวมถึงปัญหาทางด้านเศรษฐกิจที่ส่งผลกระทบต่องบประมาณในการสร้างกองกำลังที่สามารถส่งเสริมในการสร้างอำนาจทางบกของประเทศสหรัฐอเมริกาเป็นปัญหาที่ต้องแก้ไขในระยะยาว (Spoehr, 2023)

2. อำนาจในทะเลของประเทศสหรัฐอเมริกา (Power at Sea)

กองทัพเรือสหรัฐได้สร้างความได้เปรียบในอำนาจทางการทหารให้กับประเทศสหรัฐอเมริกาโดยการสร้างอำนาจทางการทหารในทะเลข้ามมหาสมุทรโดยการควบคุมกิจกรรมต่างๆในทะเลในทุกครั้งที่ต้องการ ขีดความสามารถในการแข่งขันทางด้านการกองทัพเรือสหรัฐมีประสิทธิภาพมากยิ่งขึ้น กิจกรรมต่างๆที่เกิดขึ้นในทะเลได้ทำให้กองทัพเรือสหรัฐสามารถพัฒนา “กลยุทธ์กองทัพเรือแบบใหม่” ให้เกิดขึ้น เรียกว่า ความได้เปรียบใน

ทะเล หรือ Advantage at Sea ซึ่งหากกลยุทธ์กองทัพเรือแบบใหม่นี้ถูกปรับใช้ จะทำให้กองทัพเรือสหรัฐสามารถเข้ารุกล้ำเขตน่านน้ำต่างๆเพื่อท้าทายอำนาจทางการทหารของประเทศจีนและรัสเซีย ด้วยเหตุนี้เอง กองทัพเรือสหรัฐจึงได้จัดสรรกำลังพลไปยังพื้นที่ต่างๆ ตามความต้องการทางการทหาร ณ ปัจจุบันที่เกิดจากสงครามในประเทศยูเครนและความตึงเครียดที่เพิ่มมากขึ้นในทวีปเอเชีย

เป้าหมายหลักทางการทหารของกองทัพเรือสหรัฐ คือ การเสริมสร้างความสามารถทางการทหารระดับโลก เพื่อความต้องการในการสร้างความได้เปรียบเมื่อเกิดการทำสงคราม กองทัพเรือสหรัฐได้ให้ความสำคัญไปยังการลงทุนในหลากหลายปัจจัยเพื่อบรรลุเป้าหมายที่ตั้งไว้ อาทิเช่น การลงทุนทางด้านการขยายอำนาจทางทะเล การควบคุมทางทะเล ความมั่นคงของกองทัพเรือ กลยุทธ์ทางด้านเขตน่านน้ำและการเข้าถึงน่านน้ำทะเลต่างๆ กลยุทธ์ของกองทัพเรือสหรัฐมีความต้องการในการสร้างอำนาจทางทะเลที่เหนือการรบแบบดั้งเดิม ประเทศจีนและรัสเซียได้ใช้กองทัพเรือในการสร้างอำนาจทางทะเลในแต่ละทวีป และการสร้างอำนาจทางทะเลเหล่านั้นกลายเป็นปัจจัยสำคัญต่อผลประโยชน์ทางด้านเศรษฐกิจและความมั่นคงและเพื่อกำหนดกฎเกณฑ์ต่างๆที่สามารถผลกระทบต่อประเทศอื่นๆด้วยเช่นกัน การโต้ตอบต่อสถานการณ์นี้ กองทัพเรือสหรัฐได้นำเรือรบเข้าสู่น่านน้ำของประเทศพันธมิตรต่างๆเพื่อสร้างความมั่นใจต่อประเทศพันธมิตร รวมถึงการส่งสัญญาณต่อประเทศที่เป็นศัตรูให้ทราบถึงอำนาจทางทะเลของประเทศสหรัฐและประเทศที่เป็นศัตรูต่างๆไม่สามารถใช้น่านน้ำตามเป้าหมายที่ประเทศของตนเองต้องการได้อย่างอิสระ ดังนั้นกองทัพเรือสหรัฐจึงต้องให้ความสำคัญในสองภารกิจหลัก คือ การเตรียมความพร้อมของกองเรือรบหากเกิดสงคราม และในขณะเดียวกัน ต้องเตรียมความพร้อมในการแสดงอำนาจทางทะเลในน่านน้ำต่างๆระหว่างช่วงไร้สงคราม การบรรลุสองภารกิจหลักเหล่านี้มีความต้องการทหารเรือและเรือรบจำนวนมากเพื่อความพร้อมในการปฏิบัติการและกองเรือที่ใหญ่พอที่จะรักษาความมั่นคงทางอำนาจและการทำสงครามได้ทุกเมื่อด้วยเช่นกัน (Sadler, 2023)

3. อำนาจในอากาศของประเทศสหรัฐอเมริกา (Power in Air)

ภารกิจของกองทัพอากาศสหรัฐได้มีบทบาทมากยิ่งขึ้นนับตั้งแต่ ค.ศ. 1947 เมื่อกองทัพอากาศได้ถูกแบ่งการปฏิบัติหน้าที่ในการทำสงคราม จุดเริ่มต้นของปฏิบัติการแบ่งออกเป็นสี่องค์ประกอบหลัก คือ การปฏิบัติการตามคำสั่งยุทธศาสตร์ทางอากาศ การปฏิบัติการตามคำสั่งยุทธวิธีทางอากาศ การปฏิบัติการตามคำสั่งการป้องกันทางอากาศ และการปฏิบัติการเคลื่อนย้ายทางการทหารในอากาศ โดยมีเป้าหมายหลักคือการ “บิน, จู่โจม เพื่อชัยชนะ” การเริ่มต้นของความสำคัญในการรบในอากาศ ได้เริ่มในช่วงทศวรรษ ค.ศ. 1950 ที่ได้นำความสามารถทางด้านองค์ความรู้ (Intelligence) การเฝ้าระวัง

(Surveillance) และ การลาดตระเวน (Reconnaissance) หรือ ISR และระบบบัญชาการและการควบคุม (Command and Control) หรือ C2 เข้ามาปรับใช้ในการทำสงคราม การกำเนิดของกองทัพอวกาศ (Space Force) ในเดือนธันวาคม ค.ศ. 2019 ทำให้กองทัพอากาศได้เริ่มต้นที่จะเพิ่มขีดความสามารถทางอากาศ ขึ้นไปอีกระดับหนึ่งคือการทำงานที่เกี่ยวข้องกับวัตถุที่อยู่ในอากาศและอวกาศ ผลกระทบที่เกิดขึ้นจากเหตุการณ์ดังกล่าวได้สร้างผลกระทบต่อพื้นที่ปฏิบัติภารกิจและรูปแบบการทำงานของกองทัพอากาศด้วยกันทั้งหมดสามประการ คือ ความมีอำนาจใจพื้นที่อากาศ อวกาศ ISR และ C2 เพราะพื้นที่ปฏิบัติภารกิจและรูปแบบการทำงานของกองทัพอากาศนั้น มาจากการนำแนวคิดการใช้อุปกรณ์หรืออาวุธทางอากาศในการปฏิบัติภารกิจ การกำหนดพื้นที่อวกาศทำให้ขีดความสามารถในการปฏิบัติหน้าที่ในพื้นที่ทางอากาศของกองทัพอากาศลดลง แต่ ณ ปัจจุบันได้มีการแยกหน่วยงานการทำงานอย่างชัดเจนและเป็นสัดส่วน โดยกองทัพอากาศรับผิดชอบเพียงพื้นที่ในอากาศ และโลกไซเบอร์ และกองทัพอวกาศได้แยกการปฏิบัติหน้าที่ออกไปด้วยเช่นกัน

ภายหลังจากวิกฤต COVID-19 ในช่วงฤดูร้อน ค.ศ. 2022 กองทัพอากาศสหรัฐได้ฟื้นฟูกองกำลังและความพร้อมอย่างเต็มที่ แต่สิ่งที่น่าสนใจคือ ระดับความพร้อมในการปฏิบัติหน้าที่ที่ควรจะมีอัตราสัดส่วนที่เพิ่มขึ้นมากกว่าในอดีต จากการวัดระดับความสามารถกลับพบว่ามีการเพิ่มขึ้นเพียงบางส่วนเท่านั้น (Venable, 2023) ความสามารถในการปฏิบัติการนำมาสู่การเปรียบเทียบจำนวนชั่วโมงบินในการฝึกทำให้เห็นได้ถึงความพร้อมในการปฏิบัติการที่ลดลง ประสิทธิภาพจากการฝึกฝนทางการทหาร, กองกำลังทหารสำรองและการฝึกนักบิน อยู่ในระดับเดียวกันกับก่อนหน้าที่จะเกิดวิกฤต COVID-19 มากไปกว่านั้นตลอดระยะเวลามากกว่า 30 ปีในการพยายามลดขนาดกองทัพ ทำให้กองทัพอากาศมีอัตราส่วนกำลังพลเหลือเพียง 25 เปอร์เซ็นต์ ซึ่งเป็นอัตราส่วนที่ต่ำมากกว่าระดับที่ต้องการหากเปรียบเทียบกับการทำสงครามกับประเทศที่เป็นคู่แข่ง และจะมีการลดอัตราส่วนกำลังพลกองทัพอากาศให้เหลือเพียง 20 เปอร์เซ็นต์ในอีก 5 ปีข้างหน้าด้วยเช่นกัน ทำให้ความน่ากังวลในการแข่งขันกับประเทศคู่แข่งอย่างประเทศจีนและรัสเซีย กองทัพอากาศสหรัฐจำเป็นที่จะต้องพึ่งพางบประมาณมากกว่าที่เป็นอยู่ในปัจจุบันเพื่อที่จะเพิ่มขีดความสามารถหรือการพัฒนาประสิทธิภาพของกองทัพ

จากแบบประเมินของ Index of US Military Strength 2023 คะแนนของกองทัพอากาศสหรัฐอยู่ในระดับที่ “อ่อนแออย่างมาก” เนื่องจากการขาดแคลนนักบินและอัตราการบินของนักบินที่ต่ำกว่าเกณฑ์ ทำให้ประสิทธิภาพของกองทัพอากาศอยู่ในเกณฑ์ระดับต่ำ กองทัพอากาศสหรัฐมีความจำเป็นอย่างยิ่งในการปรับคุณภาพในการเตรียมพร้อมสำหรับการทำสงครามในอากาศ การสร้างอำนาจในอากาศ ต้องการความสามารถและ

ประสิทธิภาพที่ระดับที่พร้อมจะทำสงครามได้ทุกเมื่อ นักบินจู่โจมควรที่จะได้รับการฝึกฝนการบินเพื่อพัฒนาทักษะที่จำเป็นในการทำสงคราม และการเตรียมความพร้อมหากเกิดวิกฤตรูปแบบเดียวกันกับ COVID-19 การเสริมสร้างขีดความสามารถของกองทัพอากาศสหรัฐไม่ใช่เพียงการเพิ่มจำนวนอากาศยานหรืองบประมาณ แต่จำเป็นที่จะต้องเพิ่มจำนวนการซ้อมรบและจำนวนทหารอากาศด้วยเช่นกัน (Venable, 2023)

4. อำนาจในอวกาศของประเทศสหรัฐอเมริกา (Power in Space)

กองทัพอวกาศสหรัฐถูกก่อตั้งขึ้นใน ค.ศ. 2019 โดยอำนาจของกระทรวงความมั่นคงแห่งชาติสหรัฐ การก่อตั้งกองทัพอวกาศสหรัฐ เป็นการก่อตั้งกองทัพเพื่อใช้ในยุทธภูมิที่ 5 ในการทำสงครามภายใต้การควบคุมของกระทรวงกลาโหมและกองทัพอากาศ การปฏิบัติหน้าที่ของกองทัพอวกาศสหรัฐอยู่ภายใต้การนำของเลขานุการกองทัพอากาศสหรัฐ

หน้าที่ของกองทัพอวกาศสหรัฐคือการบริหารจัดการ การฝึก และเตรียมความพร้อมกำลังรบเพื่อปกป้องผลประโยชน์ของประเทศสหรัฐและพันธมิตรในพื้นที่อวกาศ และเพื่อเพิ่มขีดความสามารถความร่วมมือของกองกำลังทหาร ความรับผิดชอบหลักของกองทัพอวกาศสหรัฐ คือ “การพัฒนาการ์เดี้ยน (กองกำลังทางทหารที่มีความเชี่ยวชาญทางด้านอวกาศ), การสร้างระบบทางการทหารในอวกาศ, การสร้างหลักยุทธศาสตร์ทางการทหารสำหรับอำนาจในอวกาศ และการบริหารกองทัพอวกาศในการพร้อมรับคำสั่งทุกเวลา”

ผลการศึกษาจากศูนย์วิจัยนโยบายต่างประเทศของสหรัฐอเมริกาและแคนาดา (RAND) ใน ค.ศ. 2001 ค้นพบว่าอัตราส่วน 95 เปอร์เซ็นต์ของเทคโนโลยีทั่วโลกที่เกี่ยวข้องกับการใช้งานพื้นที่ในอากาศและอวกาศของผู้ใช้งานทั้งรูปแบบของภาคประชาชน หรือภาคเอกชน ล้วนถูกนำมาปรับใช้โดยตรงกับระบบทางการทหารหรือการใช้งานทั้งสองรูปแบบ ความเป็นจริงที่เกิดขึ้นและการเข้ามามีบทบาทของทั้งสองภาคส่วนที่ส่งผลต่อการทำงานของกองทัพอวกาศ สร้างผลกระทบต่อการประเมินรูปแบบใหม่ในความเป็นมหาอำนาจในอวกาศ การแข่งขันในอวกาศระหว่างประเทศมหาอำนาจจึงจำเป็นต้องพึ่งพาจากทั้งสามภาคส่วนดังกล่าว คือ ความสามารถในอวกาศทางการทหาร, ภาคประชาชน และภาคเอกชน

ประเทศสหรัฐอเมริกามีความเชี่ยวชาญทางด้านเทคโนโลยีอวกาศมาอย่างยาวนาน และชีวิตประจำวันของมนุษย์ในโลกใบนี้ทุกคนล้วนพึ่งพาเทคโนโลยีอวกาศที่เกิดจากประเทศสหรัฐอเมริกาไม่ว่าจะเป็นการธนาคาร การพาณิชย์ การท่องเที่ยว ความบันเทิง ระบบการทำงานของรัฐบาล รวมถึงการทหาร ล้วนจำเป็นต้องพึ่งพาทรัพยากรที่อยู่ในอวกาศ การพัฒนาเทคโนโลยีทางอวกาศของประเทศสหรัฐถูกส่งต่อผ่านนโยบายของประธานาธิบดีมา

มากกว่าหกทศวรรษ นั่นจึงเป็นเหตุผลที่ทำให้ประสิทธิภาพทางเทคโนโลยีอวกาศของประเทศสหรัฐอเมริกามีความก้าวหน้ามากกว่าประเทศอื่นๆ

ประสิทธิภาพของภารกิจในการสนับสนุนทางด้านอวกาศของกระทรวงกลาโหมสหรัฐได้ถูกให้ความสำคัญในช่วงปฏิบัติการพายุทะเลทรายในการปลดปล่อยอิรัก (Operation Desert Storm) ที่ประเทศที่เป็นศัตรูได้ทำการโต้ตอบอย่างหนักหน่วง ทำให้ประเทศสหรัฐให้ความสำคัญมากขึ้นในพื้นที่อวกาศและตั้งมั่นในการที่จะทำให้ประเทศตนเองมีอำนาจในพื้นที่เหล่านี้

อย่างไรก็ตาม ประเทศสหรัฐอเมริกาไม่ใช่ประเทศเดียวที่มีการพัฒนาเทคโนโลยีอวกาศ ประเทศคู่แข่งอย่างประเทศจีนและรัสเซีย ได้พัฒนายุทธศาสตร์ องค์กร และประสิทธิภาพทางเทคโนโลยีอวกาศเพื่อท้าทายประเทศสหรัฐอเมริกาและการปฏิบัติการต่างๆในพื้นที่อวกาศ รวมถึงความพยายามในการขยายพื้นที่การทำงานในพื้นที่อวกาศด้วยเช่นกัน ประเทศเหล่านี้แสดงให้เห็นถึงความสามารถในการสร้างความเสียหายหรือความเสี่ยงให้กับทรัพย์สินทางอวกาศของประเทศสหรัฐอเมริกา

งบประมาณใน ค.ศ. 2023 ได้มีการเพิ่มงบประมาณให้กับกองทัพอวกาศสหรัฐเพื่อบรรลุเป้าหมายในหลากหลายภารกิจที่ถูกตั้งไว้ โดยงบประมาณในส่วนของ การปฏิบัติการและซ่อมแซม (Operations and Maintenance) คือ 4 พันล้านดอลลาร์สหรัฐ งบทางด้านวิจัยและพัฒนา 15.8 พันล้านดอลลาร์สหรัฐ และเพิ่มการจัดซื้อจัดจ้างเป็น 3.6 พันล้านดอลลาร์สหรัฐด้วยเช่นกัน ซึ่งมีอัตราส่วนเพิ่มขึ้นจากงบประมาณ ค.ศ. 2022 เป็นอัตราส่วน 41 เปอร์เซ็นต์ ทำให้ประเทศสหรัฐสามารถใช้งบประมาณของกองทัพอวกาศสหรัฐในการเสริมความแข็งแกร่งของกองทัพด้วยการสร้างทหารอัตราจ้างจำนวน 13,527 นายซึ่งเพิ่มจากงบประมาณ ค.ศ. 2022 จำนวน 763 นาย ทำให้กำลังพลของกองทัพอวกาศสหรัฐมีประสิทธิภาพมากยิ่งขึ้น เทคโนโลยีดาวเทียมต่างๆที่ใช้ในพื้นที่อวกาศของกองทัพอวกาศสหรัฐ ไม่ว่าจะเป็นการระบุตำแหน่ง, ระบบนำทาง และระบบเวลา (Position, Navigation and Timing) ระบบบัญชาการและการควบคุม (Command and Control) ระบบการสื่อสาร (Communications) ระบบตรวจวัดสภาพอากาศ (Weather) ความสามารถทางด้านองค์ความรู้ (Intelligence) การเฝ้าระวัง (Surveillance) การลาดตระเวน (Reconnaissance) และ การตรวจจับความเคลื่อนไหวในพื้นที่อวกาศ (Space Situational Awareness) จนยากที่จะมีคู่แข่งจากประเทศต่างๆในการพัฒนาเทคโนโลยีอวกาศเพื่อเข้ามาแข่งขัน

กองทัพอวกาศสหรัฐได้ทำการบริหาร โครงการระบบการส่งจรวดอวกาศเพื่อความมั่นคงแห่งชาติ (the National Security Space Launch (NSSL)) โดยเป็นการร่วมมือ

ระหว่างบริษัทเอกชนและภาครัฐในการส่งดาวเทียมต่างๆเข้าสู่วงโคจรโลก ใน ค.ศ. 2018 กองทัพอากาศได้ทำการเซ็นสัญญากับ 3 บริษัทที่เกี่ยวกับการขนส่งจรวดในการพัฒนาเครื่องจักรต่างๆในการใช้งาน และใน ค.ศ. 2020 กองทัพอวกาศได้ทำการจัดสัญญากับบริษัท ULA และ SpaceX ในการให้บริการขนส่งทางอวกาศให้กับกองทัพอวกาศสหรัฐจนถึง ค.ศ. 2027

ในทศวรรษที่ 21 ประเทศที่มีความสามารถที่สามารถแข่งขันทางด้านเทคโนโลยีอวกาศกับประเทศสหรัฐอเมริกาได้ คือประเทศจีน รัสเซีย ซึ่งใน ค.ศ. 2022 ประเทศสหรัฐอเมริกาได้ทำการวางแผนในการปล่อยจรวดเข้าสู่อวกาศจำนวน 101 ภารกิจ ประเทศจีนและรัสเซียได้ทำการวางแผนในการปล่อยจรวดเข้าสู่อวกาศจำนวน 26 และ 21 ด้วยเช่นกัน จำนวนการปล่อยจรวดเข้าสู่อวกาศของประเทศจีนและรัสเซียที่ได้รับการเผยแพร่สู่สาธารณะนั้น มักจะเป็นข้อมูลที่ผิดด้วยเช่นกัน เนื่องจากใน ค.ศ. 2021 ประเทศจีน ได้ทำการวางแผนปล่อยจรวดเข้าสู่อวกาศจำนวน 22 ภารกิจ แต่กลับพบว่า ความเป็นจริงคือประเทศจีนได้ทำการปล่อยจรวดจำนวน 51 ภารกิจ ถึงแม้ประเทศสหรัฐอเมริกาจะเป็นผู้นำทางด้านเทคโนโลยีอวกาศมานานหลายปี แต่ดูเหมือนว่าพัฒนาการทางเทคโนโลยีอวกาศของประเทศคู่แข่งต่างๆ เริ่มมีความใกล้เคียงเข้ามาในทุกปีที่ผ่านมา ดังภาพประกอบนี้

Space Launches by Country Since 2010

	U.S.	China	Russia	India
2010	17	16	16	3
2011	19	19	20	3
2012	12	19	12	2
2013	19	15	18	3
2014	21	15	22	4
2015	19	19	14	3
2016	24	22	13	7
2017	29	18	13	4
2018	29	39	13	7
2019	20	34	14	6
2020	53	19	21	14
2021	57	51	23	1
2022	101	26	21	5
Total	**420**	**312**	**220**	**62**

ภาพประกอบ 10 สถิติการปล่อยจรวดเข้าสู่ห้วงอวกาศของประเทศสหรัฐอเมริกา จีน รัสเซีย และอินเดีย

ที่มา: John Venable (2023)

สรุป

จากการวิเคราะห์โดยใช้กรอบแนวคิดการวิจัย (ภาพประกอบ 4) ซึ่งเป็นกรอบแนวคิดประยุกต์โดยผู้วิจัย ที่นำการวิเคราะห์ความมั่นคงทางไซเบอร์ ของ Myriam Dunn Cavelty และ Andreas Wenger (2020) ในการวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยการเมือง, เทคโนโลยี และวิทยาศาสตร์ โดยในแต่ละปัจจัย มีการวิเคราะห์แบบเจาะจงไปยังสิ่งที่สามารถสร้างผลกระทบต่อความมั่นคงทางไซเบอร์ได้ โดยในแง่ของปัจจัยทางการเมือง เป็นการวิเคราะห์ไปยัง อำนาจทางการเมือง ลักษณะของผู้นำรัฐบาลและความเป็นรัฐบาล วัตถุประสงค์และทฤษฎีทางการทหารของประเทศนั้นๆ และอำนาจทางการทหารในทุกสมรภูมิ และเป็นการนำการวิเคราะห์ความมั่นคงทางไซเบอร์ มาปรับใช้ร่วมกับแนวคิดการแบ่งลำดับชั้นของโลกไซเบอร์ของ David Clark (2010) ทำให้เราสามารถวิเคราะห์อำนาจทางการทหารของประเทศนั้นๆได้โดยละเอียด และครบทุกมิติ ในการวิเคราะห์ความเป็นประเทศมหาอำนาจทางไซเบอร์ในทุกมิติ

องค์ประกอบของทางไซเบอร์ที่ช่วยเสริมสร้างอำนาจให้กับประเทศสหรัฐอเมริกาทางด้านการทหารประกอบด้วย อำนาจทางการเมือง ลักษณะความเป็นรัฐบาล วัตถุประสงค์ทางการทหาร

อำนาจทางยุทธภูมิต่างๆไม่ว่าจะเป็นบนบก ในน้ำ ในอากาศและอวกาศ ล้วนแต่เป็นการวิเคราะห์ถึงองค์ประกอบที่เป็นส่วนสำคัญในการวิเคราะห์อำนาจไซเบอร์ ที่ถูกนำมาปรับใช้จากปัจจัยต่างๆที่กล่าวมาข้างต้นของประเทศสหรัฐอเมริกา คือ ความเป็นประเทศที่มีการปกครองแบบระบอบประชาธิปไตย มีความเป็นประเทศมหาอำนาจที่เป็นผู้นำทางด้านแนวคิดเสรีนิยม การบรรจุนโยบายที่เกี่ยวข้องกับการพัฒนาโลกไซเบอร์ไว้ในนโยบายประเทศ ประสิทธิภาพของยุทธศาสตร์ในการทำการรบและอำนาจทางการทหาร รวมถึงการวิเคราะห์ไปยังความเป็นมหาอำนาจทางด้านการรบทางบก ในน้ำ ในอากาศและอวกาศ ชี้ให้เห็นถึงจุดแข็งและจุดอ่อนทางการทหารของประเทศสหรัฐอเมริกาสามารถสะท้อนไปยังประสิทธิภาพของอำนาจไซเบอร์ทางการทหาร

ลำดับถัดไป จะเป็นการวิเคราะห์ความเป็นมหาอำนาจไซเบอร์ทางด้านเทคโนโลยี ที่เป็นการนำกรอบแนวคิดการวิจัย มาวิเคราะห์อำนาจไซเบอร์ทางด้านเทคโนโลยีของประเทศสหรัฐอเมริกา ที่ช่วยสร้างความได้เปรียบมากกว่าประเทศอื่นๆ และการวิเคราะห์ถึงปัจจัยทางด้านชำดับชั้นของโลกไซเบอร์ที่อ้างอิงจากกรอบแนวคิดการวิจัย เพื่อการวิเคราะห์ที่ครอบคลุมในทุกมิติ

2. ความเป็นมหาอำนาจไซเบอร์ทางด้านเทคโนโลยี (Cyber Technology Power)

โลกไซเบอร์ เกิดจากพัฒนาการของเทคโนโลยี โดยเฉพาะต้นกำเนิดที่มาจากการพัฒนาเทคโนโลยีเพื่อใช้สื่อสารในการทำสงครามโลกครั้งที่ 2 ของประเทศสหรัฐอเมริกาทำให้เกิดนวัตกรรมทางเทคโนโลยีทางด้านโลกไซเบอร์เป็นไปอย่างก้าวกระโดด และได้ถูกนำมาปรับใช้ในด้านต่างๆ รวมถึงระบบโครงสร้างพื้นฐานของประเทศ อีกทั้งการขยายการใช้งานเทคโนโลยีที่เกี่ยวข้องกับโลกไซเบอร์ของประเทศสหรัฐอเมริกาในระดับโลก ทำให้อำนาจทางด้านเทคโนโลยีของประเทศสหรัฐอเมริกามีความสำคัญต่อการวิเคราะห์อำนาจไซเบอร์ทางด้านเทคโนโลยีอย่างเห็นได้ชัด โดยผู้เขียนทำการวิเคราะห์ไปยัง 5 ปัจจัยที่สำคัญ ดังนี้

2.1 ความไม่สมมาตรของโลกไซเบอร์ (Asymmetric National Power in Cyberspace)

ประสิทธิภาพในการใช้ประโยชน์จากโลกไซเบอร์ สามารถใช้เป็นตัววัดทางด้านความก้าวหน้าทางเทคโนโลยี โดยเฉพาะการใช้ไซเบอร์ในการทำสงคราม “สงครามไซเบอร์คือการใช้ศิลปะและวิทยาศาสตร์ในการทำสงครามที่ไม่จำเป็นต้องต่อสู้แบบเผชิญหน้า เป็นการเอาชนะศัตรูโดยปราศจากการสูญเสียเลือดเนื้อของศัตรู” (Carr, 2012) จากผลการศึกษาของ Aslanoglu และ Tekir ใน ค.ศ. 2012 เหตุการณ์สงครามไซเบอร์ครั้งใหญ่ มีทั้งหมด 4 เหตุการณ์ใน 4 ประเทศ คือ ประเทศเอสโทเนียใน ค.ศ. 2007 จอร์เจียใน ค.ศ. 2008, ปฏิบัติการ Aurora ใน ค.ศ. 2009 และ ไวรัส Stuxnet worm ในประเทศอิหร่านใน

ค.ศ.2010 (Aslanoglu & Tekir, 2012) ผลลัพธ์ของเหตุการณ์ที่เกิดขึ้นทั้งหมด ทำให้เกิดผลกระทบต่อมิติทางการเมือง ที่ส่งผลกระทบโดยอ้อมต่อตัวแสดงที่เป็นรัฐ และตัวแสดงที่ไม่ใช่รัฐด้วยเช่นกัน เหตุการณ์ต่างๆที่เกิดขึ้นนำมาสู่การอธิบายถึงความเกี่ยวโยงที่สำคัญของโลกไซเบอร์ต่อพื้นที่สงครามในความไม่สมมาตรทางเทคโนโลยี ความเป็นผู้นำทางด้านอินเทอร์เน็ตของประเทศสหรัฐอเมริกา แสดงให้เห็นจากศักยภาพในการโจมตีโครงสร้างพื้นฐานของประเทศอิหร่านด้วยไวรัส Stuxnet worm แต่อย่างไรก็ตาม ความเป็นผู้นำทางด้านอินเทอร์เน็ตนั้นก็ยังไม่สามารถปิดกั้นการโจมตีทางไซเบอร์ได้เช่นกัน อาทิเช่น ปฏิบัติการ Aurora ที่เกิดจากการโจมตีต้นทางจากประเทศจีน การใช้ไซเบอร์ในการโจมตีได้สร้างความไม่สมมาตรทางโลกไซเบอร์ที่สามารถส่งผลต่อความขัดแย้งระหว่างประเทศอย่างหลีกเลี่ยงไม่ได้ในปัจจุบัน (Sumari, Gunawan, & Munthaha, 2014)

ความไม่สมมาตรในโลกไซเบอร์ที่ประเทศสหรัฐอเมริกาสามารถได้รับผลกระทบอย่างรุนแรง เกี่ยวข้องกับการไหลเวียนของข้อมูลและการปกป้องความเป็นระบอบประชาธิปไตย การไหลเวียนของข้อมูลและระบอบประชาธิปไตยมีความสำคัญต่อกันและกันเป็นอย่างมาก การคงไว้ซึ่งระบอบประชาธิปไตย ประชาชนต้องสามารถสื่อสารและแลกเปลี่ยนข้อมูลกันอย่างอิสระเสรี บันทึกของ Hamilton เมื่อ 200 ปีที่แล้วได้กล่าวไว้ว่า “ประชาชนของระบอบประชาธิปไตยจำเป็นที่จะต้องมีการศึกษา การเรียนรู้และการสร้างองค์ความรู้ต่างๆ คือ การสนับสนุนความเป็นธรรมให้กับระบบการเลือกตั้งและรัฐบาล เพื่อสร้างความมั่นคงให้กับเศรษฐกิจของประเทศ เมื่อประเทศมีพื้นฐานตามที่กล่าวมาแล้วนั้น ระบอบประชาธิปไตยจะสามารถใช้สร้างการถกเถียงทางการเมืองเพื่อสร้างองค์ความรู้ในการค้นหา, การเข้าใจ, การถกเถียง และแก้ไขปัญหาร่วมกัน ในทางตรงกันข้าม ประเทศที่ถูกปกครองด้วยระบอบเผด็จการต้องการยึดครองข้อมูลทางการเมืองแบบผูกขาด เพื่อให้คงอยู่ซึ่งระบบการปกครองที่ไม่โปร่งใส และควบคุมประชากรให้อยู่ในการปกครอง”

การไหลเวียนของข้อมูลและการติดต่อสื่อสารเป็นพื้นฐานของการรักษาระบอบประชาธิปไตยให้คงอยู่อย่างมั่นคง หากประชากรส่วนใหญ่ หรือประชากรบางกลุ่มของประเทศเลือกที่จะไม่ร่วมแสดงความคิดเห็นหรือการยอมรับในระบบการเลือกตั้ง ความถูกต้องตามกฎหมาย ความเป็นธรรมทางด้านเศรษฐกิจ และรัฐบาล เมื่อนั้นระบอบประชาธิปไตยจะไม่มีความมั่นคง นอกจากนั้น หากสังคมไม่มีการยอมรับหลักเกณฑ์กฎหมาย ที่ใช้ในการอาศัยอยู่ร่วมกัน และการแสดงความร่วมมือต่อกันและกัน ส่งผลให้สังคมจะไม่สามารถสร้างความสำเร็จในการดำเนินนโยบายต่างๆ ทำให้เกิดความโกลาหลและความวุ่นวายตามมา ในทางกลับกัน หากสังคมที่เป็นอยู่ถูกปิดกั้นทางด้านความคิด รัฐบาลอนุญาตให้แบ่งปันเพียงข้อมูลที่ถูกอนุมัติเท่านั้น สังคมเหล่านั้นจะกลายเป็นสังคมที่ประชากร

ถูกปิดกั้นทางด้านความคิด การถกเถียง และนวัตกรรมทางเศรษฐกิจ ซึ่งนำมาสู่การปกครองแบบระบอบเผด็จการ (Klipstein & Breuer, 2021)

ประเทศในโลกนี้ที่มีการปกครองแบบระบอบประชาธิปไตย ประเทศสหรัฐอเมริกาคือประเทศที่มีความอันตรายจากการได้รับการโจมตีทางด้านการแลกเปลี่ยนข้อมูลโดยใช้เทคโนโลยีเป็นอย่างมาก เนื่องจากมีเพียงไม่กี่ประเทศในโลกนี้ที่ โลกไซเบอร์คืออัตราส่วนที่สำคัญในการขับเคลื่อนข้อมูลต่างๆภายในประเทศ และระบบโครงสร้างพื้นฐานของประเทศสหรัฐอเมริกา ล้วนใช้การเชื่อมต่อกับอินเทอร์เน็ต การโจมตีเข้าสู่โลกไซเบอร์ต่อประเทศสหรัฐอเมริกาจะสามารถสร้างความไม่สมมาตรในการโจมตีต่อประเทศได้อย่างมีนัยสำคัญ นั่นจึงทำให้การให้ความสำคัญกับความสามารถในการป้องกันโลกไซเบอร์ของประเทศสหรัฐอเมริกาคือเรื่องที่สำคัญต่อความมั่นคงของประเทศมากกว่าประเทศอื่นๆ

ในปัจจุบัน การบิดเบือนข้อมูลรูปแบบใหม่ได้กลายเป็นภัยระดับชาติที่สำคัญต่อการรักษาระบอบประชาธิปไตยให้มั่นคงในประเด็นเรื่องการให้ข้อมูลต่อสาธารณะ ประเทศสหรัฐอเมริกาอยู่ในจุดที่เสียเปรียบทางด้านการแก้ไขปัญหาอย่างเห็นได้ชัด หากใช้วิธีแก้ปัญหาด้วยวิธีการใช้ไซเบอร์ทางการทหารโดยไม่ใช้ปัจจัย DIME ดังที่กล่าวข้างต้น ยกตัวอย่างเช่น การแข่งขันที่จำกัดเพียงแค่ในขอบเขตโลกไซเบอร์ ประเทศสหรัฐอเมริกาเป็นประเทศที่เสียเปรียบมากกว่าประเทศอื่นๆ เพราะว่า ประสิทธิภาพในการแข่งขันทางด้านโลกไซเบอร์นั้น ไม่ได้จำกัดเพียงการแข่งขันโดยการเปรียบเทียบการสร้างโครงสร้างพื้นฐานเชิงกายภาพ (Physical Layer) ที่ใช้ในโลกไซเบอร์ แต่ยังเป็นการแข่งขันทางด้านโครงสร้างพื้นฐานทางสังคมด้วยเช่นกัน โดยเฉพาะข้อเสียเปรียบของประเทศที่ปกครองด้วยระบอบประชาธิปไตยอย่างประเทศสหรัฐอเมริกา หากเปรียบเทียบกับประเทศที่ปกครองด้วยระบอบเผด็จการแล้วนั้น ประเทศเผด็จการได้ควบคุมโครงสร้างการสื่อสารภายในประเทศไว้ทั้งหมด ทำให้สามารถควบคุมการเข้าถึงข้อมูลในอินเทอร์เน็ตและเป็นการปกป้องโครงสร้างพื้นฐานของประเทศนั้นๆด้วยเช่นกัน (Klipstein & Breuer, 2021)

2.2 การพัฒนาและการปรับใช้โลกไซเบอร์ (Development and Use)

พัฒนาการและความพัฒนาทางด้านเศรษฐกิจเปรียบเสมือนฉากหน้าในการแสดงออกถึงการมีทรัพยากรที่เพียงพอและการสร้างความได้เปรียบต่อคู่แข่ง การแข่งขันทางด้านวิทยาศาสตร์และเทคโนโลยีได้ถูกนำมาเปรียบเทียบทางด้านการแข่งขันในความเจริญก้าวหน้าและความมั่นคงของประเทศในระดับประเทศและทวีป อย่างไรก็ตาม ปัจจัยหลักในประสิทธิภาพของความก้าวหน้าทางเทคโนโลยีคือคุณภาพและปริมาณของความสามารถของประชากรในการเป็นผู้ประกอบการที่มีส่วนช่วยในเรื่องการพัฒนา

นวัตกรรมทางด้านเทคโนโลยีที่ก่อให้เกิดการพัฒนาทางด้านวิทยาศาสตร์ในรูปแบบของการปรับใช้ในรูปแบบธุรกิจ, ระบบสาธารณะ หรือ การนำมาปรับใช้ควบคู่กัน

พัฒนาการทางด้านไซเบอร์ (Cyber-Development) คือ รูปแบบของเครื่องมือ กระบวนการ และ แนวทางปฏิบัติที่ยกระดับเทคโนโลยีอินเทอร์เน็ตและการสื่อสารในการทำหน้าที่ขับเคลื่อนการพัฒนาทางด้านสังคม, การเมือง และเศรษฐกิจ หรือในอีกความหมายหนึ่ง พัฒนาการทางด้านไซเบอร์ คือ ความสามารถในการใช้เทคโนโลยีอินเทอร์เน็ตและการสื่อสาร และพัฒนาการทางด้านความรู้ทางด้านเศรษฐกิจ ที่สามารถทำให้เกิดการพัฒนาทางด้านเศรษฐกิจของประเทศ และทำให้องค์ความรู้ทางด้านเทคโนโลยีที่เกิดขึ้นกลายเป็นปัจจัยสำคัญในการขับเคลื่อนเศรษฐกิจของประเทศ (Carayannis, Campbell, & Efthymiopoulos, 2014) ในทศวรรษที่ 18 Adam Smith ได้ให้นิยาม ที่ดิน แรงงาน และทุน คือปัจจัยหลักในระบบเศรษฐกิจ ต่อมาในช่วงต้นทศวรรษที่ 20 Joseph Schumpeter ได้เพิ่มปัจจัยทางด้าน เทคโนโลยี และ ผู้ประกอบการ เพิ่มเติมในปัจจัยหลักของระบบเศรษฐกิจ ซึ่งเขาได้ทำความเข้าใจเกี่ยวกับบทบาทและแรงขับเคลื่อนที่เกิดจากการเปลี่ยนแปลงทางด้านเทคโนลีและนวัตกรรมที่เปรียบเสมือนจุดชี้วัดถึงคุณภาพของระบบเศรษฐกิจ เทคโนโลยีได้สร้างสิ่งที่ไม่เคยมีมาก่อนในอดีต คือการสร้างปฏิสัมพันธ์ในการทำงานร่วมกันระหว่างภาครัฐและภาคเอกชนให้ประสิทธิภาพมากขึ้น และเห็นได้ชัดมากยิ่งขึ้นจากในอดีต ความสามารถทางด้านเทคโนโลยีในการลดต้นทุนทางด้านการแลกเปลี่ยนได้กระตุ้นให้เกิดการเปลี่ยนแปลงทางด้านเทคโนโลยีอินเทอร์เน็ตและการสื่อสารในพัฒนาการในหลากหลายด้านด้วยเช่นกัน

ดังนั้น ความก้าวหน้าทางวิทยาศาสตร์และเทคโนโลยีต้องการการพัฒนาทางด้านนโยบายและสิ่งแวดล้อมทางด้านการดำเนินการนโยบายต่างๆ เพื่อใช้ในการพัฒนาทางด้านเศรษฐกิจ และการระบุถึงความเสี่ยงที่สามารถเกิดขึ้นได้รวมถึง ประโยชน์ที่ได้จากการสร้างเทคโนโลยีรูปแบบใหม่ การเติบโตทางด้านพัฒนาการทางด้านเทคโนโลยีไซเบอร์ จำเป็นต้องพึ่งพาการสร้างสิ่งแวดล้อมที่ก่อให้เกิดความคิดสร้างสรรค์เพื่อการสร้างนวัตกรรมใหม่ๆให้เกิดขึ้น รวมถึงความสำเร็จหรือล้มเหลวในการบริหารของรัฐบาล ได้ถูกกำหนดด้วยความสามารถของรัฐบาลในการสร้างประโยชน์สูงสุดจาก 4 องค์ประกอบ คือ 1. ความร่วมมือและการทำงานร่วมกันในความสัมพันธ์ระหว่างรัฐบาล ผู้ประกอบการ สถาบันวิจัยและองค์ประกอบอื่นๆที่เฉพาะทาง มาหวิทยาลัย และองค์กรสนับสนุนต่างๆ เพื่อการพัฒนาของภาคธุรกิจขนาดกลางและขนาดเล็ก (SMEs) 2. อำนาจทางด้านข้อมูลและการติดต่อสื่อสารทางเทคโนโลยี 3. ประสิทธิภาพในการจัดการและบริหารระบบที่สามารถสร้างผลผลิตและระบบพาณิชย์ต่างๆ และ 4. การทำข้อตกลง ระเบียบ กฎเกณฑ์ ความร่วมมือ

ระดับนานาชาติ ซึ่ง 4 องค์ประกอบที่กล่าวมาจะสามารถสร้างส่งผลที่ดีทางด้านการสร้างความสร้างสรรค์และนวัตกรรมในระดับเล็ก (micro level) และส่งเสริมการพัฒนานวัติกรรมและการแข่งขันในระดับใหญ่ (macro level) อาทิเช่นการแข่งขันระดับอุตสาหกรรม, ระดับชาติ และระดับโลก (Carayannis, Campbell, & Efthymiopoulos, 2014)

การเพิ่มขึ้นของการเชื่อมต่อในโลกอินเทอร์เน็ต ทำให้ความปลอดภัยทางด้านข้อมูลและการใช้ชีวิตประจำวันของประชากรประเทศสหรัฐอเมริกาขึ้นอยู่กับความมั่นคงทางไซเบอร์ ประธานาธิบดี Joe Biden ได้ให้ความสำคัญในการเสริมสร้างความแข็งแกร่งให้กับการป้องกันการโจมตีทางไซเบอร์ ให้เป็นนโยบายสำคัญในแผนการบริหารของเขา และสิ่งที่ทำให้ความมั่นคงทางไซเบอร์มีความสำคัญมากยิ่งขึ้นคือความสำคัญของโครงสร้างพื้นฐานและประสิทธิภาพทางด้านการผลิตของประเทศที่มีการพึ่งพาโลกไซเบอร์อย่างมีนัยสำคัญ (U.S. Department of Energy, 2022) ภาคพลังงานของประเทศสหรัฐอเมริกาต้องเผชิญหน้ากับภัยความมั่นคงทางไซเบอร์อย่างต่อเนื่อง ใน ค.ศ. 2022 รายงานภัยความมั่นคงประจำ ค.ศ. 2022 ของสำนักงานหน่วยสืบราชการลับสหรัฐ ได้รายงานถึงความสำคัญในการรักษาความมั่นคงทางด้านประสิทธิภาพทางไซเบอร์เพื่อป้องกันการโจมตีทางไซเบอร์ต่อระบบโครงสร้างพื้นฐานที่สำคัญของประเทศ อาทิเช่น ระบบควบคุมอุตสาหกรรมพลังงานของประเทศสหรัฐอเมริกา การโจมตีความมั่นคงทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญของประเทศคือสิ่งที่สำคัญต่อประเทศและสามารถส่งผลกระทบต่อหลากหลายภาคส่วน และเป็นเป้าหมายสำคัญในการดำเนินการนโยบายเพื่อพัฒนาความสามารถของกระทรวงพลังงานของประเทศสหรัฐอเมริกา (U.S. Department of Energy’s (DOE)) สำนักงานความมั่นคงทางไซเบอร์, ความมั่นคงทางพลังงาน และ การตอบโต้ฉุกเฉิน (Office of Cybersecurity, Energy Security, and Emergency (CESER)) รวมถึงความร่วมมือระหว่างภาครัฐและภาคเอกชนด้วยเช่นกัน ปัญหาที่เกิดขึ้นทำให้เกิดความพยายามในความร่วมมือระหว่างภาครัฐและภาคเอกชนในการสร้างความมั่นคงให้กับระบบพลังงานของประเทศในอนาคต การสร้างระบบพลังงานที่ปลอดภัยด้วยการออกแบบรูปแบบการไหลเวียนของการทำงานในแต่ละกระบวนการให้เป็นระบบ จากนั้นจึงนำไปพัฒนา ติดตั้ง และนำมาปรับใช้ เพื่อให้มีความมั่นคงและสามารถฟื้นฟูระบบได้อย่างรวดเร็วจากการโจมตีทางไซเบอร์ต่างๆที่สามารถเกิดขึ้นได้

ประเทศสหรัฐได้นำรูปแบบการทำงานทางด้านวิศวกรรมข้อมูลไซเบอร์ (Cyber-informed Engineering (CIE)) มาปรับใช้ในการสนับสนุน 5 นโยบายหลักของกระทรวงพลังงานสหรัฐทั้งหมด 5 ด้าน คือ 1. การสร้างความแข็งแกร่งที่เป็นรูปธรรมต่อภัยคุกคามทางไซเบอร์ในระบบพลังงาน 2. การระบุความเสี่ยงทางด้านห่วงโซ่อาหาร (supply chains)

ของประเทศ 3. การสนับสนุนความมั่นคงและความยืดหยุ่นในการออกแบบกระบวนการที่ปรับใช้ในการทำงาน 4. การสร้างประสิทธิภาพทางไซเบอร์และความยืดหยุ่นในภาคเอกชน ภาครัฐ ท้องถิ่น และชุมชนต่างๆ 5. การเตรียมความพร้อมในการตอบสนองความร่วมมือกับภาครัฐและภาคอุตสาหกรรมเมื่อเกิดเหตุทางไซเบอร์ในภาคพลังงาน โดยรูปแบบการทำงานทางด้านวิศวกรรมข้อมูลไซเบอร์ หรือ CIE คือ กรอบการทำงานที่มีจุดเริ่มต้นจากห้องปฏิบัติการขั้นสูงแห่งชาติของกระทรวงพลังงานในการสร้างความมั่นคงทางไซเบอร์ให้กับระบบพลังงานของประเทศให้มีการปกป้องตั้งแต่ระดับชั้นพื้นฐานเพื่อสร้างความมั่นคงที่สำคัญ สำนักงาน CESER ได้นำ CIE มาปรับใช้ในการปกป้องโครงสร้างพื้นฐานทางพลังงานที่สำคัญของประเทศและยกระดับทักษะให้กับหน่วยงานความร่วมมือทั้งหลาย ยกตัวอย่างเช่น CESER ได้ทำงานร่วมกับสำนักงานระหว่างหน่วยงาน อาทิเช่น สำนักงานประสิทธิภาพทางด้านพลังงานหมุนเวียน สำนักงานทางด้านไฟฟ้า สำนักงานหน่วยข่าวกรองและต่อต้านข่าวกรอง และหน่วยงานอื่นๆเพื่อให้มั่นใจในความมั่นคงไซเบอร์ที่ถูกออกแบบมาเพื่อการปกป้องระบบพลังงานทั้งในปัจจุบันและอนาคต (U.S. Department of Energy, 2022)

รูปแบบการทำงานทางด้านวิศวกรรมข้อมูลไซเบอร์ หรือ CIE คือกระบวนการที่มีเป้าหมายในการนำกระบวนการและขั้นตอนการตัดสินใจต่างๆที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ เข้าสู่การออกแบบกระบวนการ การสร้างกระบวนการ และการปฏิบัติการของระบบโครงสร้างทางกายภาพต่างๆที่เกี่ยวข้องกับการเชื่อมต่อทางดิจิทัล การสอดส่อง หรือ ควบคุมทางดิจิทัล หรือในอีกความหมายหนึ่ง คือ การผสานกระบวนการและขั้นตอนการตันสินใจต่างๆที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ให้กลายเป็นส่วนประกอบขั้นพื้นฐานที่สำคัญในการจัดการความเสี่ยงทางด้านวิศวกรรมที่มีหน้าที่การทำงานที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล ซึ่งได้แบ่งการนำ CIE เข้ามาปรับใช้ในระบบโครงสร้างพื้นฐานทางด้านพลังงานออกเป็น 5 กลยุทธ์หลัก ประกอบด้วย

1. การสร้างความตระหนักรู้ (Awareness) หมายถึง การสร้างความตระหนักรู้ในรูปแบบการทำงานทางด้านวิศวกรรมข้อมูลไซเบอร์ หรือ CIE ในภาคอุตสาหกรรมพลังงาน ไม่ว่าจะเป็นผู้ประกอบการ ผู้ปฏิบัติงาน วิศวกรรมทางด้านระบบ ผู้ผลิต นักวิจัย และ ผู้นำประเทศ ซึ่งการสร้างความตระหนักรู้ต้องพึ่งพาการสร้างวัฒนธรรมที่ให้ความสำคัญกับความปลอดภัยในภาควิศวกรรมที่มีการเปลี่ยนตลอดเวลา การสร้างความเข้าใจเกี่ยวกับการทำงานที่มีกระบวนการแบบระบบนิเวศ (ecosystem) ของระบบโครงสร้างพื้นฐานทางด้านพลังงานที่จำเป็นต้องพึ่งพา CIE และการนำ CIE ไปปรับใช้ในด้านต่างๆ

เพื่อจำกัดความสามารถการโจมตีทางไซเบอร์ที่สามารถเกิดขึ้นได้ตลอดเวลาต่อความมั่นคงของประเทศและระบบเศรษฐกิจ

2. การศึกษา (Education) หมายถึง การพัฒนาบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับ CIE ผ่านการให้ความรู้ การฝึกฝน และประกาศนียบัตรสำหรับผู้ผ่านการอบรมความรู้และทักษะทางด้าน CIE การสร้างแรงงานคือสิ่งสำคัญในความต้องการนำ CIE มาปรับใช้ในระบบนิเวศของโครงสร้างพื้นฐานทางด้านพลังงานที่สำคัญ การสร้างบุคลากรที่มีความรู้ทางด้านความมั่นคงทางไซเบอร์ต้องพึ่งพาการสนับสนุนที่มั่นคงทั้งจากทางภาครัฐและภาคเอกชนในการผลิตบุคลากรที่เชี่ยวชาญ การสร้างบุคลากรเหล่านี้จะส่งผลให้เกิดการขยายทางด้านความหลากหลายทางแรงงาน พัฒนาประสิทธิภาพของแรงงาน และพัฒนาประสิทธิภาพของแรงงานภาคพลังงานอย่างยั่งยืน
3. การพัฒนา (Development) หมายถึง การทำให้รูปแบบการทำงานทางด้านวิศวกรรมข้อมูลไซเบอร์ หรือ CIE มีข้อมูลที่ครบถ้วนและรูปแบบการทำงานที่พร้อมในการปฏิบัติการด้วยการสร้างพื้นที่ในการเก็บเครื่องมือ รูปแบบการทำงาน วิธีการ และองค์ประกอบต่างๆที่ถูกตกตะกอนจากการทำงานมาแล้วเพื่อให้ผู้ฝึกฝนหรือผู้ที่จะนำไปใช้ สามารถนำ CIE ไปปรับใช้ให้เข้ากับโครงสร้างพื้นฐานปัจจุบัน และในอนาคต รวมถึงการรวบรวมบทเรียนต่างๆที่ได้จากการทำงานด้วย CIE ในทุกหน่วยหรือระดับการทำงานของโครงสร้างพื้นฐาน เพื่อใช้ในการพัฒนาองค์ความรู้อย่างต่อเนื่องและเติมเต็มองค์ความรู้เพื่อนำไปใช้ในการสร้างคำแนะนำ กรณีศึกษา และปฏิบัติการต่างๆในภาคอุตสาหกรรมพลังงาน
4. โครงสร้างพื้นฐานปัจจุบัน (Current Infrastructure) หมายถึง การนำ CIE มาปรับใช้CIE ในระบบการจัดการโครงสร้างพื้นฐานที่สำคัญของประเทศ ณ ปัจจุบัน กลยุทธ์นี้สามารถสร้างความปลอดภัยที่ดียิ่งขึ้นให้กับโครงสร้างพื้นฐานที่สำคัญ ณ ปัจจุบันด้วยการเสริมสร้างความยากในการโจมตีของศัตรูและการทำให้ทุกการโจมตีสามารถเกิดขึ้นได้อย่างยากลำบากในการสร้างผลกระทบต่อกระบวนการทำงานของโครงสร้างพื้นฐานของประเทศ
5. โครงสร้างพื้นฐานในอนาคต (Future Infrastructure) หมายถึง การสร้างหน่วยงานค้นคว้าและพัฒนา (Research and Development) และพัฒนารากฐานอุตสาหกรรมในการสร้าง CIE เพื่อปรับใช้ในระบบโครงสร้างพื้นฐานและเทคโนโลยีในอนาคตและความมั่นคงทางไซเบอร์กลายเป็นส่วนหนึ่งของ

ระบบวิศวกรรมต่างๆในโครงสร้างพื้นฐาน การที่จะทำให้กลยุทธ์นี้เกิดความสำเร็จได้ จำเป็นที่จะต้องให้ความสำคัญกับการสร้างหน่วยงานค้นคว้าและออกแบบระบบพลังงานในอนาคตที่ใช้ CIE เป็นแนวทางในการปฏิบัติ รวมถึงการสนับสนุนการนำ CIE เข้าไปเป็นส่วนหนึ่งในระบบนิเวศทางเทคโนโลยีและภาคธุรกิจให้มีการใช้งานอย่างสม่ำเสมอ การนำ CIE เข้ามาปรับใช้ในทุกกระบวนการที่กล่าวมา จำสร้างโอกาสในภาคอุตสาหกรรมการผลิตภายในประเทศให้มีการเติบโตมากยิ่งขึ้น และสร้างโอกาสในการรักษาความเป็นผู้นำทางด้านระบบพลังงานหมุนเวียนที่ล้ำหน้าที่สามารถเพิ่มความปลอดภัยทางด้านพลังงานและลดการปล่อยมลพิษด้วยเช่นกัน

ในหลายปีที่ผ่านมาได้มีการนำ CIE เข้ามาปรับใช้ในกระทรวงพลังงานของประเทศสหรัฐอเมริกา องค์กรต่างๆ ภาคอุตสาหกรรม และหน่วยงานที่ให้ความร่วมมือทางด้านการศึกษาให้การสนับสนุนในการพัฒนากระบวนการโครงสร้างและวิธีการต่างๆในการนำ CIE มาปรับใช้ในโครงสร้างพื้นฐานที่สำคัญของประเทศสหรัฐอเมริกา กระบวนการต่างๆที่ถูกนำมาปรับใช้ได้ทำให้เกิดการลดความเสี่ยงในโครงสร้างพื้นฐานปัจจุบันและนำความเสี่ยงที่สามารถเกิดขึ้น ไปต่อยอดและพัฒนาให้เกิดกระบวนการเรียนรู้จากความเสี่ยงต่างๆที่เกิดขึ้นเพื่อพัฒนาในการออกแบบระบบใหม่ในอนาคต (U.S. Department of Energy, 2022)

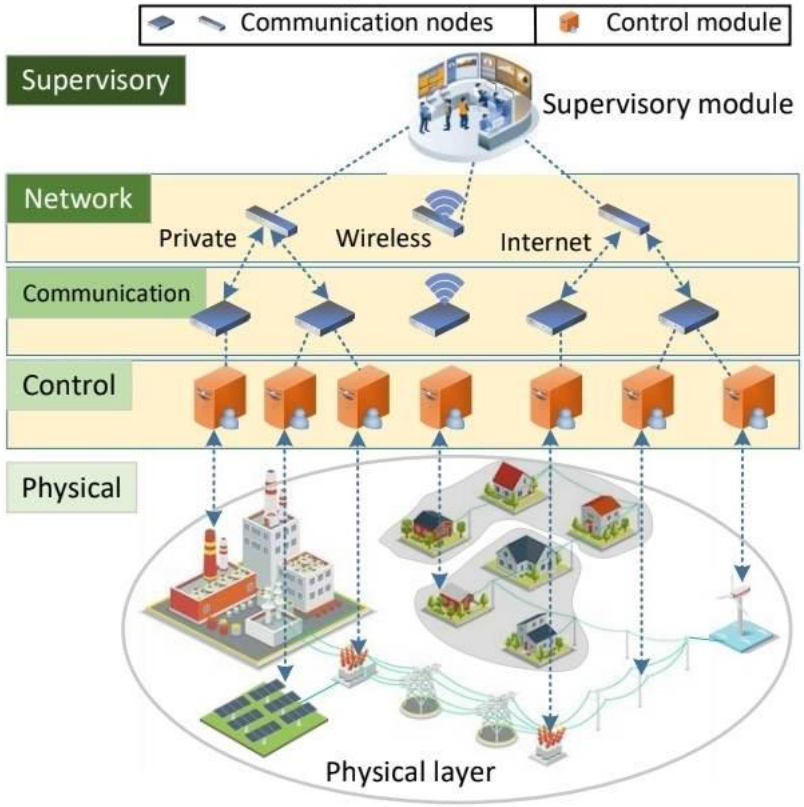
2.3 ลำดับชั้นทางกายภาพ (Physical Layer)

ความก้าวหน้าของเทคโนโลยีการสื่อสารได้เพิ่มขึ้นอย่างมีนัยสำคัญในทศวรรษที่ผ่านมา ส่งผลให้เกิดการกระจายตัวของข้อมูลและการปรับใช้ระบบไฟฟ้ากำลัง (Electric power system) ที่เพิ่มมากยิ่งขึ้น โลกไซเบอร์จำเป็นต้องพึ่งพาระบบไฟฟ้าที่มีความมั่นคงและมีศักยภาพในการขนส่งข้อมูลผ่านระบบที่เป็นโครงข่ายและกระจายระบบได้อย่างทั่วถึงต่อทุกภาคส่วนและความต้องการในการใช้งาน ความทันสมัยของกริด (Grid Modernization) หรือ ความทันสมัยของระบบไฟฟ้าที่ทำหน้าที่จ่ายไฟฟ้าไปยังส่วนต่างๆของระบบ ได้กลายเป็นสิ่งที่เรียกว่า ระบบพลังงานทางกายภาพของโลกไซเบอร์ (Cyber-physical power systems หรือ CPPSs) โดยระบบนี้ประกอบไปด้วย ลำดับชั้นทางไซเบอร์ (cyber layer) อาทิเช่น ระบบสื่อสาร และระบบควบคุม และลำดับชั้นทางกายภาพ (physical layer) หมายถึง ระบบที่ทำหน้าที่สร้างและจ่ายพลังงาน (power systems) ดังนั้น การเพิ่มขึ้นของภัยร้ายที่สามารถทำการโจมตีการทำงานของระบบพลังงาน รวมถึงภัยร้ายทางไซเบอร์ ทำให้การสร้างความปลอดภัยในลำดับชั้นทางไซเบอร์ของระบบพลังงานกลายเป็นเรื่องที่ต้องให้ความสำคัญเป็นอย่างมาก เนื่องจากแพลตฟอร์มต่างๆที่มนุษย์ใช้ในชีวิตประจำวัน

ระบบปฏิบัติการคลาวด์ และเครื่องมือปัญญาประดิษฐ์อัจฉริยะ ทำให้การวิเคราะห์ในการทำงานของระบบ CPPSs มีความซับซ้อนมากยิ่งขึ้น (Abdelmalak et al., 2023)

ลำดับชั้นไซเบอร์ (Cyber layer) สามารถอธิบายได้ว่า เป็นลำดับชั้นที่เกี่ยวข้องกับการคำนวณ วิเคราะห์ และประเมินระบบพลังงานของระดับทวีปและระดับโลก การให้นิยามในขอบเขตการทำงานของลำดับชั้นไซเบอร์ในระบบพลังงานทางกายภาพของโลกไซเบอร์สามารถให้นิยามได้ดังนี้ ลำดับชั้นทางไซเบอร์ คือ ส่วนที่เกี่ยวข้องกับความก้าวหน้าในเทคโนโลยีข้อมูลและการสื่อสาร ส่งผลให้เกิดการสร้างเครื่องประมวลผลที่มีกระบวนการคำนวณอัจฉริยะที่ทำงานในทุกอุปกรณ์ของระบบพลังงานไฟฟ้าต่างๆ ในขณะที่พลังงานไฟฟ้า (Power Grid) คือสิ่งที่แสดงถึงกระบวนการทำงานในลำดับชั้นกายภาพ

ระบบพลังงานทางกายภาพของโลกไซเบอร์ ประกอบด้วยการทำงานที่หลากหลาย อาทิเช่น การตรวจจับ (sensor) การป้องกัน (protection) การสื่อสาร (communication) การประมวลผล (computation) และการควบคุม (control) และการนำลำดับชั้นต่างๆที่อยู่ในลำดับชั้นไซเบอร์มาทำงานร่วมกัน จะทำให้เกิดความซับซ้อนมากยิ่งขึ้นในกระบวนการทำงาน เนื่องจากลำดับชั้นต่างๆในลำดับชั้นไซเบอร์นั้น มีความเสียหายที่เกิดขึ้นในรูปแบบที่แตกต่างกัน ดังตัวอย่างในภาพประกอบ



ภาพประกอบ 11 ลำดับชั้นของระบบพลังงานทางกายภาพของโลกไซเบอร์

ที่มา: Abdelmalak et al. (2023)

ความแตกต่างในลำดับชั้นของระบบพลังงานทางกายภาพของโลกไซเบอร์ที่ประกอบด้วยระบบควบคุม ทำให้เห็นถึงการทำงานที่แบ่งแยกลำดับชั้นได้อย่างชัดเจน โดยประกอบด้วย 6 ลำดับชั้น คือ ลำดับชั้นการจัดการ (management layer) ลำดับชั้นกำกับดูแล (supervisory layer) ลำดับชั้นเครือข่าย (network layer) ลำดับชั้นการสื่อสาร (communication layer) ลำดับชั้นควบคุม (control layer) และลำดับชั้นกายภาพ (physical layer) โดย ข้อมูลต่างๆที่เกิดขึ้นในลำดับชั้นกายภาพ (physical layer) รวมถึงพลังงานต่างๆที่เกิดขึ้นในลำดับชั้นนี้ จะถูกควบคุมโดยลำดับชั้นควบคุม (control layer) ที่ทำหน้าที่ในการตรวจจับข้อมูล การโจมตี และการบุกรุกทางไซเบอร์ต่างๆ ลำดับถัดมา ลำดับชั้นการสื่อสาร (communication layer) ทำหน้าที่ในการเชื่อมต่อระหว่างลำดับชั้นควบคุมไปยังเครือข่ายต่างๆ ซึ่งการลำเลียงข้อมูลจะถูกส่งต่อไปยังลำดับชั้นเครือข่าย (network layer) และถูกส่งต่อไปยังการวิเคราะห์ข้อมูลในลำดับชั้นกำกับดูแล (supervisory layer) ในท้ายที่สุด ข้อมูลที่ถูกวิเคราะห์จะถูกส่งไปยังลำดับชั้นการจัดการ (management layer) ในการตัดสินใจ รวมถึงการออกนโยบาย หลักเกณฑ์ และการควบคุมระบบต่างๆ (Cyber-Physical Power System Layers)

ดังนั้น ระบบพลังงานทางกายภาพของโลกไซเบอร์ เป็นปัจจัยสำคัญทางด้านลำดับชั้นทางกายภาพ เนื่องจาก ระบบพลังงานทางกายภาพของโลกไซเบอร์เป็นโครงสร้างของระบบพลังงานที่มีลักษณะกายภาพที่สร้างปฏิสัมพันธ์ในการทำงานในการสื่อสาร การควบคุม และทรัพยากรในการคำนวนต่างๆ ให้กับภาคเอกชน ภาคอุตสาหกรรม และ โครงสร้างพื้นฐานที่สำคัญของประเทศสหรัฐอเมริกา

การสื่อสารและการเชื่อมต่อ คือ องค์ประกอบที่สำคัญของโลกไซเบอร์ นอกจากการทำงานของระบบพลังงานทางกายภาพของโลกไซเบอร์ สายเคเบิ้ลโทรคมนาคมใต้ทะเล (Undersea Telecommunication) เป็นองค์ประกอบที่สำคัญของลำดับชั้นทางกายภาพของโลกไซเบอร์ด้วยเช่นกัน สายเคเบิ้ลใต้ทะเล เป็นสิ่งที่ทำให้ผู้บริโภค ภาคธุรกิจ และรัฐบาล รวมถึง กองกำลังทางการทหาร ใช้ในการติดต่อสื่อสารต่อกันและกัน และทำให้สามารถเข้าถึงอินเทอร์เน็ตด้วยเช่นกัน ภาคเอกชนและรัฐบาลที่เป็นเจ้าของธุรกิจโทรคมนาคม และธุรกิจประเภทเทคโนโลยี เป็นผู้ถือครองสายเคเบิ้ลโทรคมนาคมใต้ทะเลจำนวน 486 สาย ที่เป็นจุดเชื่อมต่อในทุกทวีปยกเว้ยทวีปแอนตาร์กติการ์ โดยภาคเอกชนเป็นผู้ถือครองสายเคเบิ้ลจำนวนอัตราส่วน 99 เปอร์เซ็นต์ ของธุรกิจสื่อดิจิทัลที่ใช้การแลกเปลี่ยนข้อมูลผ่านสายเคเบิ้ลใต้ทะเล อาทิเช่น ข้อมูลที่เป็นรูปแบบ เสียง ฐานข้อมูล และอินเทอร์เน็ต ที่ทำให้เกิด

การไหลเวียนเงินที่มีมูลค่าล้านล้านดอลลาร์สหรัฐในระบบกระแสการเงินรายวันของโลก และทำหน้าที่เป็นกระดูกสันหลังของระบบอินเทอร์เน็ตระดับโลก

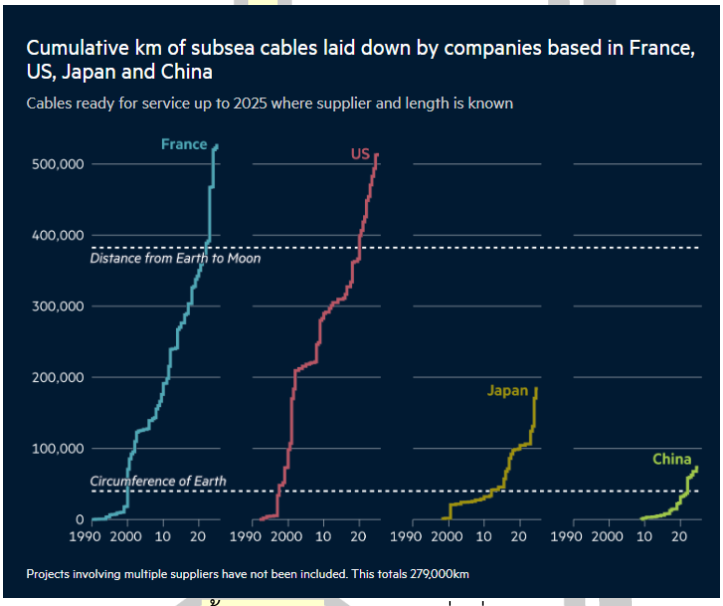
นอกจากประโยชน์ของสายเคเบิ้ลโทรคมนาคมใต้ทะเลแล้วนั้น ปัญหาของการใช้งานสายเคเบิ้ลโทรคมนาคมใต้ทะเลในทางการเมือง ก็เป็นจุดที่ก่อให้เกิดความเสียหายต่อระบบการเมืองระหว่างประเทศด้วยเช่นกัน การรุกรานของประเทศรัสเซียในสงครามยูเครนนั้น ได้เพิ่มข้อกังวลต่อความมั่นคงทางด้านการใช้สายเคเบิ้ลโทรคมนาคมใต้ทะเลในเชิงพาณิชย์ ที่กลุ่มผู้นำนาโต้ (North Atlantic Treaty Organization (NATO)) ให้ความสำคัญมากยิ่งขึ้น จากการรายงานในอดีตในเรื่องความสามารถของประเทศรัสเซียในการตัดสายเคเบิ้ลใต้ทะเลและพฤติกรรมอื่นๆที่เกิดขึ้นต่อโครงสร้างพื้นฐานของประเทศที่เป็นสมาชิกนาโต้ด้วยเช่นกัน ฝ่ายตุลาการของประเทศสหรัฐอเมริกาได้เพิ่มความสำคัญต่อปัญหาที่เกี่ยวข้องกับการเชื่อมต่อสายเคเบิ้ลโทรคมนาคมใต้ทะเลระหว่างประเทศสหรัฐอเมริกากับประเทศจีน โดยอ้างถึงการเพิ่มขึ้นของโอกาสที่รัฐบาลจีนจะทำการเข้าถึงระบบสายเคเบิ้ลโทรคมนาคมใต้ทะเลเพื่อรวบรวมข้อมูลส่วนบุคคล การสื่อสาร และข้อมูลอื่นๆที่สำคัญของประเทศสหรัฐอเมริกา รวมถึงการโจมตีทางไซเบอร์ผ่านการเชื่อมต่อสายเคเบิ้ลโทรคมนาคมใต้ทะเลในพื้นที่ภูมิภาคฮาวายและมหาสมุทรแปซิฟิก ได้เพิ่มความกังวลให้กับประเทศสหรัฐอเมริกาเกี่ยวกับความมั่นคงทางไซเบอร์ของสายเคเบิ้ลโทรคมนาคมใต้ทะเลด้วยเช่นกัน

รัฐบาลประเทศสหรัฐอเมริกาได้ทำการศึกษาความมั่นคงสำหรับสายเคเบิ้ลโทรคมนาคมใต้ทะเลในช่วงที่ผ่านมา โดยใน ค.ศ. 2017 มีการรายงานจากสำนักงานหน่วยข่าวกรองแห่งชาติ ระบุถึงความเสียหายที่เกิดขึ้นต่อสายเคเบิ้ลโทรคมนาคมใต้ทะเล ซึ่งส่วนมากมาจากพฤติกรรมของมนุษย์ อาทิเช่น การตกปลา การทอดสมอเรือ การขุดลอก และ เกิดจากภัยพิบัติทางธรรมชาติ โดยรัฐบาลได้แสดงออกในการปกป้องสายเคเบิ้ลโทรคมนาคมใต้ทะเลและเครือข่ายโทรคมนาคมของประเทศสหรัฐอเมริกาด้วยการเสริมสร้างความเข้มงวดมากยิ่งขึ้นในการประเมินสายเคเบิ้ลที่สามารถติดตั้งในประเทศสหรัฐอเมริกา อาทิเช่น สายเคเบิ้ลที่ผู้ครอบครองมาจากต่างประเทศ การห้ามใช้อุปกรณ์ที่ไม่น่าเชื่อถือในระบบสายเคเบิ้ลโทรคมนาคมใต้ทะเล การส่งเสริมการลงทุนทางด้านอุปกรณ์ที่ทำงานกับระบบสายเคเบิ้ลโทรคมนาคมใต้ทะเลที่น่าเชื่อถือในประเทศสหรัฐอเมริกาและทั่วโลก การสร้างระบบตัดการทำงานของสายเคเบิ้ลโทรคมนาคมใต้ทะเลในกรณีฉุกเฉิน และการขยายกองเรือที่ทำหน้าที่ซ่อมแซมสายเคเบิ้ลโทรคมนาคมใต้ทะเล (Gallagher, 2022)

พัฒนาการทางด้านเทคโนโลยีสายเคเบิ้ลโทรคมนาคมใต้ทะเลของประเทศสหรัฐอเมริกา มีการพัฒนาอย่างต่อเนื่องและล้ำหน้าเป็นอย่างมาก โดยเฉพาะเทคโนโลยีสายไฟเบอร์ออพติก ที่ใช้ในการเคลื่อนย้ายข้อมูล รับข้อมูล และการเพิ่มความเร็วของ

สัญญาณ ที่ได้เพิ่มความสามารถในการขนส่งสัญญาณผ่านสายเคเบิ้ลโทรคมนาคมใต้ทะเลที่มากยิ่งขึ้น จาก 25 เทอราบิทส์ ต่อ วินาที (terabits) เป็น 60 เทอราบิทส์ ต่อ วินาที ตั้งแต่ ค.ศ. 2014 จนถึง ค.ศ. 2019 การพัฒนาเทคโนโลยีล่าสุด คือการออกแบบระบบที่ทำให้เครื่องมือที่ใช้ในเครือข่ายอินเทอร์เน็ตมีความเร็วมากยิ่งขึ้น และเพิ่มจำนวนการจับขั้วสายเคเบิ้ลได้มากยิ่งขึ้น ทำให้การใช้งานร่วมกับสายเคเบิ้ลโทรคมนาคมใต้ทะเลสามารถเพิ่มเป็น 250 เทอราบิทส์ ต่อ วินาที (Gallagher, 2022)

ประเทศสหรัฐอเมริกา เป็นหนึ่งในประเทศที่บริษัทเอกชนมีความเป็นผู้นำทางด้านสายเคเบิ้ลโทรคมนาคมใต้ทะเล รวมถึงประเทศฝรั่งเศส และประเทศญี่ปุ่นด้วยเช่นกัน โดยสามารถจำแนกระยะสายเคเบิ้ลใต้ทะเลในอัตราส่วนกิโลเมตร ได้ดังนี้



ภาพประกอบ 12 ระยะสายเคเบิ้ลใต้ทะเลจากบริษัทที่มีถิ่นฐานอยู่ในประเทศฝรั่งเศส สหรัฐอเมริกา ญี่ปุ่น และจีน ภายใน ค.ศ. 1990 จนถึง ค.ศ. 2022

ที่มา: Gross et al. (2023)

ภาพประกอบ 13 สายเคเบิ้ลใต้ทะเลของประเทศสหรัฐอเมริการะหว่าง ค.ศ. 1989 ถึง ค.ศ. 2026

ที่มา: Gross et al. (2023)

จากภาพดังกล่าว ประเทศสหรัฐอเมริกามีสายเคเบิ้ลใต้ทะเล เป็นลำดับที่ 2 รองจากประเทศฝรั่งเศส และประเทศจีน เป็นลำดับสุดท้าย ในทศวรรษที่ 21 ประเทศจีนได้ประสบความสำเร็จในการสร้างผลประโยชน์ทางการค้าในระดับโลก แต่ด้วยความขัดแย้งทางด้านการเมือง ส่งผลให้สายเคเบิ้ลใต้ทะเลที่มีการเชื่อมต่อระหว่างประเทศสหรัฐอเมริกาและจีนถูกปิดกั้นจากรัฐบาลของประเทศสหรัฐอเมริกา ด้วยความกังวลของรัฐบาลประเทศสหรัฐอเมริกาเกี่ยวกับการแทรกแซงทางด้านการเมืองและทรัพย์สินโดยกลุ่มบริษัทที่ตั้งถิ่นฐานในประเทศจีน อาทิเช่น เหตุการณ์ใน ค.ศ. 2018 บริษัท Amazon Meta และ China Mobile ได้ทำข้อตกลงในการทำงานร่วมกันในการเชื่อมต่อสายเคเบิ้ลจากรัฐแคลิฟอเนียไปยังประเทศสิงคโปร์ มาเลเซีย และฮ่องกง แต่นโยบายจากทางภาครัฐในการปิดกั้นการมีส่วนร่วมในการลงทุนในสายเคเบิ้ลภายใต้ประเทศสหรัฐอเมริกา ทำให้บริษัท China Mobile จำเป็นต้องถอนตัวออกจากการลงทุนในครั้งนี้ ต่อมาใน ค.ศ. 2021 บริษัท Meta และ Amazon ได้ยื่นคำร้องการในการวางระบบการเชื่อมต่อสายเคเบิ้ลใหม่ โดยการวางระบบครั้งนี้ ไม่มีการลงทุนจากประเทศจีน ไม่มีการเชื่อมต่อจากประเทศฮ่องกง และใช้ชื่อใหม่ในชื่อ Cap-1 และในภายหลัง ระบบสายเคเบิ้ลใต้ทะเล Cap-1 ได้ถูกถอดถอนออกจากระบบ แม้ว่าสายเคเบิ้ลที่มีความยาวระยะ 12,000 กิโลเมตร ส่วนใหญ่จะถูกสร้างขึ้นแล้วก็ตาม การมีส่วนร่วมเริ่มแรกของจีนยังคงเป็นข้อกังวลด้านความปลอดภัยสำหรับรัฐบาลสหรัฐอเมริกา

รัฐบาลสหรัฐอเมริกามีความกังวลทางด้านความเสี่ยงจากการโจรกรรมข้อมูลจากประเทศจีน โดยรัฐบาลสหรัฐอเมริกามีนโยบายในการตัดขาดการเชื่อมต่อเครือข่ายสายอินเทอร์เน็ตที่ถูกพัฒนาจากการร่วมมือของบริษัทในระดับนานาชาติที่ประเทศจีนมีส่วนเกี่ยวข้อง รัฐบาลสหรัฐอเมริกาได้ประสบความสำเร็จในการกีดกันปักกิ่งในการเข้ามาเป็นผู้เล่นรายหลักในตลาดสายเคเบิ้ลใต้ทะเลในระดับโลก แต่ถึงกระนั้น จากการสัมภาษณ์ผู้บริหารในอุตสาหกรรมมากกว่า 20 ราย ชี้ให้เห็นว่านโยบายของรัฐบาลสหรัฐอเมริกาส่งผลให้มีการสั่งห้ามใช้การจัดซื้อจัดจ้างจากจีนโดยพฤตินัยทั่วทั้งภาคอุตสาหกรรม แม้แต่ในโครงการที่ไม่เกี่ยวข้องกับประเทศสหรัฐอเมริกาด้วยก็ตาม บางคนกังวลว่าสิ่งนี้อาจทำให้ระบบอินเทอร์เน็ตทั่วโลกเสียหายได้ เนื่องจากบริษัทจีนเริ่มสร้างเครือข่ายเคเบิลของตนเองที่ประเทศอื่นๆ (Gross et al., 2023)

2.4 ลำดับชั้นทางตรรกะ (Logical Layer)

ลำดับชั้นทางตรรกะ เปรียบเสมือนระบบประสาทส่วนกลางของโลกไซเบอร์ มีหน้าที่ในการนำส่งชุดข้อมูลไปยังจุดหมายปลายทาง ผ่านเส้นทางหลักที่เรียกว่า Domain name systems (DNS) ระบบปฏิบัติการอินเทอร์เน็ต เว็บไซต์ และ ซอฟต์แวร์ต่างๆ ที่มีพื้นฐานจากการเชื่อมต่อจากสายเคเบิ้ลไฟเบอร์ออพติก และระบบไซเบอร์ลำดับชั้นทางกายภาพขั้นพื้นฐานต่างๆ การโจมตีเป้าหมายโดยการใช้ไซเบอร์นั้น สามารถสร้างความเสียหายให้กับลำดับชั้นทางตรรกะของโลกไซเบอร์ในหลากหลายวิธี เพื่อทำให้เกิดการทำงานที่ผิดพลาด หรือ การปิดระบบการทำงานเพื่อหยุดยั้งระบบขนส่งของข้อมูลต่างๆในโลกไซเบอร์ด้วยเช่นกัน

ประเทศสหรัฐอเมริกาให้ความสำคัญในการปกป้องการโจมตีทางไซเบอร์เป็นอย่างมาก และเป็นประเทศที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์ในหลากหลายเหตุการณ์ ดังนั้น โลกไซเบอร์จึงเปรียบเสมือนเครื่องมือทางการทหารชนิดหนึ่งที่สำคัญของประเทศสหรัฐอเมริกา ในการปกป้องเพื่อป้องกันการตกเป็นเป้าหมายการโจมตีของศัตรู หรือการถูกใช้เพื่อการปฏิบัติการทางการทหารต่างๆ เครื่องมือทางไซเบอร์ (Cyber tools) สามารถถูกใช้ในรูปแบบของการปฏิบัติการทางการทหารแบบดั้งเดิม (Conventional operation) อาทิเช่น การใช้งานเครื่องมือทางไซเบอร์ในการต่อต้านรัฐอิสลาม ในรูปแบบการก่อกวนคำสั่งหรือการใช้งานทางไซเบอร์ของรัฐอิสลาม ที่ใช้ในการแพร่กระจายแนวคิดทางการเมืองของกลุ่มรัฐอิสลาม และนอกจากการโจมตีโดยการก่อกวนคำสั่งการใช้งานนั้น เครื่องมือทางไซเบอร์ ยังถูกใช้ในปฏิบัติการรูปแบบพิเศษด้วยเช่นกัน อาทิเช่น ปฏิบัติการไวรัสสตักซ์เน็ต (Stuxnet) ที่ใช้ในปฏิบัติการต่อต้านประเทศอิหร่าน

สำหรับการปฏิบัติการทางการทหารแบบดั้งเดิม ลำดับชั้นทางตรรกะ หรือ เครื่องมือทางไซเบอร์ สามารถถูกใช้งานในการเป็นแรงสนับสนุนและการสั่งการ ในการยืนยันถึงประสิทธิภาพในปฏิบัติการทางการทหารต่างๆที่เกี่ยวข้องกับโลกไซเบอร์ รวมถึงการใช้สัญญาณอินเทอร์เน็ตในการสั่งการ ทำให้เครื่องมือทางไซเบอร์ สามารถเป็นเครื่องมือที่สร้างผลประโยชน์ให้กับผู้ใช้งานได้เป็นอย่างมาก และมีความแตกต่างจากการใช้งานสนับสนุนจากรูปแบบอื่นๆ หากเปรียบเทียบกับการสนับสนุนทางกองทัพเรือ เครื่องมือทางไซเบอร์สามารถสร้างประสิทธิภาพได้เป็นอย่างมากในการต่อกรกับศัตรู ทั้งในด้านการเข้าถึงศัตรูและประสิทธิผลของการใช้งาน ปฏิบัติการของเครื่องมือทางไซเบอร์ได้เปรียบทั้งทางด้านเวลาและสถานที่ เนื่องจากปฏิบัติการทางไซเบอร์ สามารถโจมตีได้อย่างรวดเร็วได้ทั่วทุกมุมโลกและสามารถโจมตีได้อย่างรวดเร็ว ซึ่งแตกต่างจากการโจมตีทางการทหารแบบดั้งเดิม ที่ต้องใช้ระยะเวลาในการเคลื่อนพล รวมถึงการได้รับผลกระทบจากภูมิประเทศและสภาพอากาศและการป้องกันการถูกโจมตีทางด้านกายภาพด้วยเช่นกัน (Di Pane, 2024)

กองบัญชาการไซเบอร์สหรัฐ (U.S. Cyber Command) เป็นหนึ่งในหน่วยงานของกระทรวงกลาโหมสหรัฐ มีหน้าที่ในการกำหนดทิศทางทางการทหารในของโลกไซเบอร์ ทั้งการปฏิบัติการเชิงรุกและเชิงรับ เพื่อรักษาความมั่นคงในโลกไซเบอร์ของประเทศสหรัฐอเมริกา กองบัญชาการไซเบอร์สหรัฐ ก่อตั้งขึ้นใน ค.ศ. 2010 ภายใต้การกำกับดูแลของกองบัญชาการยุทธศาสตร์สหรัฐ (U.S. Strategic Command) และทำงานร่วมกับสำนักงานความมั่นคงแห่งชาติ (National Security Agency) ในประเด็นทางด้านหน่วยข่าวกรองและทางด้านการทหาร ภายหลังได้ถูกยกระดับขึ้นมาเป็นกองบัญชาการเต็มรูปแบบในช่วงสมัยของรัฐบาลอดีตประธานาธิบดี Donald Trump ใน ค.ศ. 2018 และได้มีแนวทางการทำงานที่มีความอิสระมากขึ้นจนถึงปัจจุบัน

ภารกิจของกองบัญชาการไซเบอร์สหรัฐ มีขอบเขตที่กว้างขวาง ตั้งแต่ระดับเชิงรุกและเชิงรับ ไปจนถึงการคอยตรวจสอบเครือข่ายอินเทอร์เน็ตของกระทรวงกลาโหมสหรัฐและการเข้าสนับสนุนการป้องกันระบบโครงสร้างพื้นฐานของประเทศ หน้าที่หลักของกองบัญชาการไซเบอร์สหรัฐ คือ

1. การรักษาความมั่นคงในขีดความสามารถของกระทรวงกลาโหมในการปฏิบัติงานในระดับโลกที่มีความเกี่ยวข้องกับโลกไซเบอร์มากยิ่งขึ้นในทุกๆวัน
2. การกำจัดภัยความมั่นคงของประเทศสหรัฐอเมริกาและการปกป้องผลประโยชน์แห่งชาติ
3. การสนับสนุนปฏิบัติการทางการทหารเพื่อให้บรรลุเป้าหมายผ่านโลกไซเบอร์

หน้าที่หลักที่ใช้ในการปฏิบัติหน้าที่ของกองบัญชาการไซเบอร์สหรัฐ คือ การปกป้องเชิงรุก (Defending forward) โดยมีการให้นิยามในกลยุทธ์ทางไซเบอร์ของ

กระทรวงกลาโหมสหรัฐใน ค.ศ. 2018 ไว้ว่า เป็นการทำงานร่วมกันกับภาคเอกชนและเครือข่ายประเทศพันธมิตร และคู่ค้าต่างๆ ในการเผชิญหน้ากับกิจกรรมทางไซเบอร์ที่สามารถเป็นภัยต่อการปฏิบัติภารกิจร่วมกันและ การป้องกันการรั่วไหลของข้อมูลสำคัญของกระทรวงกลาโหมสหรัฐ

การปกป้องเชิงรุก เป็นการปฏิบัติการที่ดำเนินการใกล้กับจุดเริ่มต้นของภัยคุกคามทางไซเบอร์ที่สามารถเกิดขึ้นได้ในอนาคต กล่าวคือ เป็นการทำงานแบบตัดไฟตั้งแต่ต้นลมก่อนที่ภัยคุกคามเหล่านั้นจะสร้างความเสียหายอย่างร้ายแรงให้กับประเทศสหรัฐอเมริกาไม่ว่าจะเป็นการจู่โจมเพื่อการได้มาซึ่งข้อมูล หรือ การโจมตีเพื่อให้เกิดความเสียหายต่างๆ

ความเสียหายจากการใช้ลำดับชั้นทางตรรกะ หรือ เครื่องมือไซเบอร์ ในสงครามยูเครน คือตัวอย่างที่มีบทบาทสำคัญและเห็นได้ชัดเจนจากผลกระทบที่เกิดขึ้นที่ส่งผลเหมือนการทำสงครามทางการทหารแบบดั้งเดิม การรุกรานครั้งนี้เปรียบเสมือนการเคลื่อนกำลังพลทางการทหาร และการใช้ปืนใหญ่ในการทำสงคราม โดยกองกำลังทหารรัสเซียได้สร้างผลกระทบต่างๆที่เกิดขึ้นผ่านการใช้ไซเบอร์ อาทิเช่น

- กองกำลังทหารรัสเซียได้ตั้งเป้าหมายการโจมตีไปยังดาวเทียมที่มีชื่อว่า Viasat ซึ่งเป็นดาวเทียมโทรคมนาคมของประเทศสหรัฐอเมริกา ที่ใช้ในการสนับสนุนกองกำลังทางการทหารของประเทศยูเครน โดยเป็นการโจมตีด้วยมัลแวร์ที่ออกแบบมาเพื่อลบข้อมูลต่างๆและปิดการทำงานของระบบทั้งหมด การโจมตีครั้งนี้ได้สร้างผลกระทบเป็นวงกว้างต่อดาวเทียมอื่นๆ โดยรอบด้วยเช่นกัน ทำให้ประชากรที่อาศัยภายนอกประเทศยูเครนได้รับผลกระทบจากการไม่มีไฟฟ้าใช้และการตัดขาดจากโลกอินเทอร์เน็ต
- การโจมตีทางไซเบอร์ต่อสภาเมือง Odessa ซึ่งเป็นเมืองท่าเรือหลักของประเทศยูเครนที่เชื่อมต่อกับทะเลดำ ที่มีการตั้งเวลาของขีปนาวุธในการโจมตีของประเทศยูเครน ในการตอบโต้การโจมตีของประเทศรัสเซีย
- การโจมตีทางไซเบอร์ยังสร้างผลกระทบต่อหลากหลายภาคส่วนของโครงสร้างพื้นฐานของประเทศยูเครน รัฐบาล และการใช้งานเครือข่ายอินเทอร์เน็ตของประชากรชาวยูเครน รวมถึง โรงพยาบาลด้วยเช่นกัน

เหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นต่างๆนั้น ทำให้เห็นถึงผลกระทบที่เกิดจากลำดับชั้นทางตรรกะ หรือ เครื่องมือทางไซเบอร์ ที่สามารถสร้างความเสียหายได้เปรียบเสมือนการทิ้งระเบิดในสงครามโลกครั้งที่ 2 ที่ส่วนมากเป็นการทิ้งระเบิดในพื้นที่โครงสร้างพื้นฐานของประเทศรวมถึงการทำลายเขตเศรษฐกิจต่างๆอย่างมีนัยะสำคัญ (Di Pane, 2024)

2.5 ลำดับชั้นทางข้อมูล (Information Layer)

ความเป็นผู้นำของประเทศสหรัฐอเมริกาในทศวรรษที่ 21 นอกจากความก้าวหน้าทางเทคโนโลยีและทางวัฒนธรรม การดำเนินการในการวางระเบียบและบรรทัดฐานทางสังคมในระดับโลก ทำให้ขอบเขตอำนาจการควบคุมข้อมูลของประเทศสหรัฐอเมริกา มีขอบเขตที่สามารถเข้าถึงข้อมูลได้ทั่วโลก Artur Victoria ได้นิยามความเป็นผู้นำทางด้านข้อมูลนี้ว่า “อำนาจนำของประเทศสหรัฐอเมริกา เกิดจากความเป็นผู้นำทางด้านการวางโครงสร้างเทคโนโลยีของโลกใบนี้” (Victoria, 2018)

หากเปรียบเทียบที่มาของสิ่งที่ทำให้ประเทศใดประเทศหนึ่งมีความเป็นประเทศมหาอำนาจ สิ่งที่ทำให้ประเทศเหล่านั้นได้ก้าวขึ้นมาเป็นประเทศมหาอำนาจ นับตั้งแต่ทศวรรษที่ 16 อาทิเช่น อำนาจทางทะเล อำนาจทางการพาณิชย์ อำนาจทางด้านอุตสาหกรรม และ การทำงานร่วมกันทางการเมืองของหลากหลายประเทศ การก้าวขึ้นมาเป็นประเทศที่มีอำนาจนำในทางประวัติศาสตร์ มีการเปลี่ยนแปลงของhistorical primacy there is a shift in the power elements of the 21st century from the previous period. องค์ประกอบที่ทำหน้าที่หลักในการทำให้ประเทศนั้นๆก้าวขึ้นมามีอำนาจอย่างต่อเนื่องจนถึงทศวรรษที่ 21 รวมถึงการกล่าวอ้างของ Nye (2009: 78) เกี่ยวกับองค์ประกอบหลักที่ทำให้ประเทศสหรัฐอเมริกามีอำนาจ ประกอบด้วย ความเป็นผู้นำทางด้านเทคโนโลยี, ความเป็นผู้นำทางด้านการทหาร และความเป็นผู้นำทางด้านเศรษฐกิจ และการตั้งคำถามถึง “การเป็นแกนกลางสื่อสารข้ามชาติ” หรือ “transnational communication axis” ซึ่งนับตั้งแต่ที่ประเทศสหรัฐอเมริกามีจุดเด่นที่แข็งแกร่งทางด้านซอฟท์พาวเวอร์ (Soft power) ในขณะเดียวกัน โครงสร้างและการพัฒนาทางด้านเครือข่ายได้ถูกควบคุมโดยประเทศสหรัฐอเมริกา ข้อมูลต่างๆที่เกิดขึ้นในการใช้งานต่างๆไม่ว่าจะเป็นในโลกอินเทอร์เน็ต แอพลิเคชัน หรือสื่อออนไลน์ต่างๆ ล้วนเป็นการให้ข้อมูลกับประเทศสหรัฐอเมริกาด้วยเช่นกัน ทำให้ประเทศสหรัฐอเมริกาสามารถใช้เทคโนโลยีและข้อมูลในการทำงานที่เพื่อผลประโยชน์และในทางอื่นๆได้ด้วยเช่นกัน

การเป็นอันดับหนึ่งในการควบคุมข้อมูล สามารถอธิบายได้ถึงองค์ประกอบหลักที่สำคัญของโครงสร้างอำนาจสูงสุดของประเทศสหรัฐอเมริกา นอกจากการควบคุมข้อมูลทางด้านเครือข่ายในโลกไซเบอร์แล้วนั้น การเป็นศูนย์กลางทางด้านกายภาพในโลกไซเบอร์ ก็เป็นหนึ่งในปัจจัยสำคัญที่สร้างความเป็นอันดับหนึ่งของประเทศสหรัฐอเมริกาด้วยเช่นกัน อาทิเช่น การเป็นศูนย์กลางทางด้านโหนด (node) ของอินเทอร์เน็ต และโครงสร้างทาง

กายภาพของเครือข่ายทั่วโลก ที่ส่วนมากมีศูนย์กลางควบคุมอยู่ที่ทวีปอเมริกาเหนือเท่านั้น (Victoria, 2018)

กระทรวงกลาโหมควบคุมการใช้โลกไซเบอร์ในทางการทหาร และองค์กรความร่วมมือด้านการจัดสรรชื่อและหมายเลขทางอินเทอร์เน็ต “The Internet Corporation for Assigned Names and Numbers (ICANN)” ร่วมกับ VeriSign เป็นบริษัทให้บริการทางด้านการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ต และเป็นผู้ดูแลโดเมน .com ซึ่งทั้ง 2 องค์กรมีหน้าที่ในการควบคุมการใช้โลกไซเบอร์ในเชิงพาณิชย์ รับผิดชอบในการกำหนดพารามิเตอร์ในระบบปฏิบัติการอินเทอร์เน็ต การควบคุมดูแลระบบชื่อโดเมน การจัดสรรบล็อกของหมายเลขที่อยู่ IP และการจัดการระบบเส้นทางของเซิร์ฟเวอร์ต่างๆ

อำนาจในการควบคุมข้อมูลและการสื่อสารของเครือข่ายอินเทอร์เน็ตของประเทศสหรัฐอเมริกา ทำให้ประเทศ หรือ หน่วยงานต่างๆสามารถถูกห้ามไม่ให้เข้าถึงเครือข่ายอินเทอร์เน็ตและการเข้าถึงข้อมูลต่างๆในโลกอินเทอร์เน็ต ในขณะเดียวกัน การพาณิชย์ในโลกอินเทอร์เน็ตที่ได้รับการดูแลโดย ICANN กระทรวงพาณิชย์ และ VeriSign ซึ่งมีต้นกำเนิดในทวีปอเมริกาเหนือ ส่วนการควบคุมทางการทหาร ถูกดำเนินการโดยหน่วยงานทางด้านการป้องกันและหน่วยข้างกรองของกองทัพสหรัฐ

เซิร์ฟเวอร์ที่เป็นเซิร์ฟเวอร์หลักที่ใช้ในการเชื่อมต่ออินเทอร์เน็ตมีทั้งหมด 13 เซิร์ฟเวอร์ และเซิร์ฟเวอร์เหล่านี้มีหน้าที่ที่สำคัญในการกำหนดเซิร์ฟเวอร์อื่นๆ นับพันที่เชื่อมต่อกับเครือข่ายเพื่อเข้าสู่โลกไซเบอร์ ซึ่งจากเซิร์ฟเวอร์หลักที่กล่าวมาทั้ง 13 เซิร์ฟเวอร์นั้น มีเซิร์ฟเวอร์จำนวน 10 เซิร์ฟเวอร์ที่มีตำแหน่งอยู่ภายในประเทศสหรัฐอเมริกา ตามตำแหน่งตัวอักษรในรูป A B C D E F G H J และ L ส่วนอีก 3 เซิร์ฟเวอร์ประกอบด้วยตำแหน่ง K เป็นเซิร์ฟเวอร์ที่ก่อตั้งร่วมกับประเทศพันธมิตรในการรวบรวมข้อมูลในอดีต และตำแหน่ง M ในประเทศญี่ปุ่น ที่ยังคงเป็นรัฐที่สนับสนุนกองทัพสหรัฐอเมริกานับตั้งแต่การสิ้นสุดของสงครามโลกครั้งที่สอง และอีกตำแหน่ง คือตำแหน่ง I ที่เป็นเซิร์ฟเวอร์ที่ตั้งอยู่ในประเทศสวีเดน จากเซิร์ฟเวอร์ 10 ตำแหน่งในประเทศสหรัฐอเมริกา มี 6 ตำแหน่งที่ทำงานภายในโลกไซเบอร์ของประเทศสหรัฐอเมริกา (A, B, D, E, G, H) โดยมีวัตถุประสงค์ความปลอดภัยในการจัดการระบบในโลกไซเบอร์ ตำแหน่ง G ได้รับการควบคุมโดยตรงจากกระทรวงกลาโหมในการทำงานเกี่ยวกับศูนย์กลางข้อมูลเครือข่าย และตำแหน่ง H ทำหน้าที่ในการเป็นห้องปฏิบัติการวิจัยทางการทหารของกองทัพ

ภาพประกอบ 14 เซิร์ฟเวอร์หลักที่ใช้ในการเชื่อมต่ออินเทอร์เน็ต
ที่มา: Arthur Victoria (2018)

การกระจายตัวทั่วโลกของเซิร์ฟเวอร์หลัก ทำให้หลากหลายประเทศมีความสามารถในการเข้าถึงอินเทอร์เน็ตได้รวดเร็วมากยิ่งขึ้น และเป็นเหตุผลที่สามารถอธิบายถึงการขออนุญาตในการเข้าถึงข้อมูลต่างๆในโลกอินเทอร์เน็ต ที่ต้องได้รับการตรวจสอบและการอนุญาตจากเซิร์ฟเวอร์ที่เกี่ยวข้องและเซิร์ฟเวอร์หลักเพื่อตรวจสอบความถูกต้องของเนื้อหาต่างๆ จากที่กล่าวมา นั่นคือตัวชี้วัดในการระบุได้ว่า ในท้ายที่สุด ประเทศสหรัฐอเมริกาคือประเทศที่ได้รับข้อมูลต่างๆในโลกไซเบอร์ และยังเป็นสิ่งที่แสดงให้เห็นถึงความไม่จำเป็นในการก่อตั้งสถานที่ของหน่วยข่าวกรองสหรัฐในการปฏิบัติหน้าที่นอกเขตแดนประเทศด้วยเช่นกัน

นอกจากการวิเคราะห์ไปยังเซิร์ฟเวอร์หลักในการเข้าสู่โลกไซเบอร์เพื่อการได้มาซึ่งข้อมูลต่างๆแล้วนั้น ยังมีอีกมิติในการวิเคราะห์ด้วยเช่นกัน นั่นคือความเป็นผู้นำทางด้านเทคโนโลยีของบริษัทเอกชนของประเทศสหรัฐอเมริกา ที่มีสัดส่วนที่สำคัญของเว็บไซต์ที่จัดเก็บข้อมูลต่างๆในโลกอินเทอร์เน็ต รวมถึงการมีเซิร์ฟเวอร์ในระดับท้องถิ่นในประเทศต่างๆที่หลากหลาย อาทิเช่น บริษัท Google และ Yahoo

ความเป็นผู้นำทางด้านซอฟต์แวร์ คือมิติทางด้านการวิเคราะห์ความเป็นผู้นำทางด้านข้อมูลในโลกไซเบอร์ที่มักถูกมองข้าม เป็นมิติที่แสดงให้เห็นถึงความเป็นอำนาจนำในการสร้างโครงสร้างพื้นฐานที่สมบูรณ์แบบที่สุดในการใช้แพลตฟอร์มเพื่อสอดส่องข้อมูลต่างๆที่ถูกสร้างขึ้นมาโดยประชากรที่มีความแตกต่างในแต่ละประเทศ และข้อมูลดังกล่าวที่ถูกสร้างขึ้นมาได้ถูกนำไปสู่การใช้งานในประเทศสหรัฐอเมริกา และ เมื่อพิจารณาถึงความ

เชื่อมโยงของอุตสาหกรรมเทคโนโลยีสารสนเทศกับหน่วยงานทางด้านกลาโหมและข่าวกรองของสหรัฐฯ ซึ่งเมื่อนำผลประโยชน์ของบริษัทรวมเข้ากับความต้องการความร่วมมือของรัฐบาล อย่างน้อยก็เป็นไปได้ที่องค์กรเหล่านี้เต็มใจที่จะปฏิบัติตามข้อเรียกร้องของรัฐบาล

อำนาจนำทางด้านข้อมูลในโลกไซเบอร์ของประเทศสหรัฐอเมริกา คือสิ่งที่เห็นได้อย่างชัดเจน และอาจให้นิยามในการเป็นอันดับหนึ่งในการเข้าถึงข้อมูลต่างๆในโลกใบนี้ด้วยเช่นกัน และจากการวิเคราะห์ดังกล่าว ทำให้เห็นถึงระยะห่างของความเป็นอำนาจนำทางด้านข้อมูลของประเทศมหาอำนาจอย่างเห็นได้ชัด ไม่ว่าจะเป็นทางด้านการค้าขาย หรืออำนาจทางการทหาร ประเทศมหาอำนาจที่มีโครงสร้างที่ใหญ่กว่า จะสามารถได้รับประโยชน์และใช้ประโยชน์จากข้อมูลต่างๆได้เสมอ (Victoria, 2018)

สรุป

พื้นฐานสำคัญที่ทำให้ความก้าวหน้าทางเทคโนโลยีของประเทศสหรัฐอเมริกา ที่ได้รับผลประโยชน์จากอำนาจทางการเมือง คือ ความไม่สมมาตรทางเทคโนโลยี ที่มีพัฒนาการนับตั้งแต่ยุคสงครามโลกจนถึงปัจจุบัน และความเป็นประเทศมหาอำนาจทำให้ปัจจัยทางด้านพัฒนาการทางด้านเทคโนโลยี มีการพัฒนาและสร้างนวัตกรรมใหม่อย่างต่อเนื่อง และการใช้งานไซเบอร์ที่กลายมาเป็นการทำสงครามด้วยเทคโนโลยีและวิทยาศาสตร์ อย่างไรก็ตาม ความไม่สมมาตรที่เกิดขึ้น นำมาสู่ความท้าทายในความสำคัญเพื่อสร้างความมั่นคงทางไซเบอร์ เนื่องจากการขับเคลื่อนประเทศด้วยเทคโนโลยีไซเบอร์ ที่เป็นปัจจัยสำคัญต่อทั้งทางด้านเศรษฐกิจ และการเมือง ที่สามารถถูกแทรกแซงทางด้านข้อมูลที่บิดเบือน นำมาสู่การเป็นภัยต่อความมั่นคงในประเทศ

การแข่งขันทางด้านการพัฒนาและปรับใช้ไซเบอร์ในสังคม เพื่อให้ประชากรมีทักษะในการใช้งาน และสามารถนำไปต่อยอดทำให้เกิดการพัฒนาองค์ความรู้ใหม่ทางไซเบอร์ ส่งเสริมต่อการพัฒนาเศรษฐกิจ ที่สร้างความได้เปรียบทั้งทางด้านเทคโนโลยี และคุณภาพของระบบเศรษฐกิจภายในประเทศ อีกทั้งพัฒนาการที่เกิดขึ้น ยังได้สร้างความร่วมมือระหว่างภาครัฐและภาคเอกชนในการดำเนินการต่างๆที่จำเป็นต้องพึ่งพาซึ่งกันและกัน ประเทศสหรัฐอเมริกาให้ความสำคัญทางด้านความปลอดภัยทางด้านข้อมูลและการใช้ชีวิตประจำวันของประชากรในการใช้งานไซเบอร์ และโครงสร้างพื้นฐานประเทศที่พึ่งพาโลกไซเบอร์ จึงเป็นอีกปัจจัยที่ส่งเสริมให้ประเทศสหรัฐอเมริกา มีความจำเป็นในการพัฒนาไซเบอร์อย่างต่อเนื่องด้วยเช่นกัน

การกำหนดทิศทางการพัฒนาไซเบอร์ คือปัจจัยสำคัญในการขับเคลื่อนความก้าวหน้าทางเทคโนโลยีไซเบอร์ ประเทศสหรัฐอเมริกาให้ความสำคัญกับการพัฒนาเพื่อป้องกันการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ และการเป็นส่วนสำคัญต่อการผลักดันนโยบายเพื่อพัฒนาความมั่นคงของกระทรวงพลังงาน และการตอบโต้ฉุกเฉิน ก่อให้เกิดการร่วมมือกันระหว่างภาครัฐและเอกชน ที่ได้รวบรวมความร่วมมือจากทั้งผู้ประกอบการ ผู้ผลิต นักวิจัย และภาครัฐที่มี

ตัวแทนเป็นผู้นำประเทศ เข้ามาหารือร่วมกันในการผลักดันนโยบายต่างๆ รวมถึงการสร้างบุคลากรที่ผ่านการฝึกฝนและเรียนรู้ในความรู้วิศวกรรมไซเบอร์ เพื่อรองรับความหลากหลายของแรงงานที่จำเป็นต่อการพัฒนาไซเบอร์อย่างยั่งยืน

นอกจากการที่ประเทศสหรัฐได้รับผลประโยชน์ทางการเมืองจากการเป็นประเทศมหาอำนาจหลังสงครามโลกแล้วนั้น องค์ความรู้ที่ได้ส่งต่อมายังปัจจุบัน ได้สร้างข้อได้เปรียบให้กับประเทศสหรัฐด้วยการพัฒนาเทคโนโลยีเชิงกายภาพ ด้วยการพัฒนาความทันสมัยของกริด หรือระบบไฟฟ้า ที่สร้างข้อได้เปรียบต่อการดำเนินการทางไซเบอร์ ไม่ว่าจะเป็นกระบวนการสื่อสาร ควบคุม และการสร้างและจ่ายพลังงานไปยังระบบต่างๆ สร้างความท้าทายต่อการสร้างความมั่นคงในการปกป้องระบบไฟฟ้า ซึ่งเป็นหนึ่งในโครงสร้างพื้นฐานที่สำคัญของประเทศสหรัฐอเมริกา และการปกป้องพัฒนาการในการพัฒนาเทคโนโลยีเพื่อสร้างความก้าวหน้าในลำดับถัดไป อาทิเช่น การพัฒนาปัญญาประดิษฐ์อัจฉริยะ ที่จะมีบทบาทสำคัญต่อโลกไซเบอร์ ด้วยการทำงานที่ซับซ้อนมากยิ่งขึ้น อาทิเช่น การใช้ปัญญาประดิษฐ์ในการสร้างความมั่นคงทางไซเบอร์ เป็นต้น

การได้เปรียบเชิงกายภาพอีกหนึ่งข้อได้เปรียบ คือการเป็นหนึ่งในประเทศที่มีบริษัทเอกชนเป็นผู้นำทางด้านสายเคเบิ้ลใต้ทะเล แสดงให้เห็นถึงความสามารถในการเคลื่อนย้ายข้อมูล รับข้อมูล และการเพิ่มความเร็วของสัญญาณ ที่เป็นปัจจัยสำคัญต่อการใช้งานโลกไซเบอร์ เปรียบเสมือนระบบประสาทที่สามารถสั่งการระบบต่างๆในร่างกายได้อย่างรวดเร็ว และมีประสิทธิภาพในการทำงานของระบบการเคลื่อนไหวของร่างกาย รวมถึงการกระจายตัวของเซิร์ฟเวอร์หลักของประเทศสหรัฐอเมริกา ทั้งเซิร์ฟเวอร์ที่ก่อตั้งใหม่ และเซิร์ฟเวอร์ที่ถูกใช้งานเพื่อรวบรวมข้อมูลในอดีตสมัยสงครามโลก ยังคงทำหน้าที่ในการสนับสนุนกองทัพสหรัฐอเมริกาจนถึงปัจจุบัน และความพยายามปิดกั้นการเข้าแทรกแซงจากประเทศอื่นๆ ถือเป็นการสร้างความมั่นคงไซเบอร์ของประเทศสหรัฐอเมริกาด้วยเช่นกัน ดังนั้น ประเทศสหรัฐอเมริกาจึงมีการก่อตั้งกองบัญชาการไซเบอร์สหรัฐ เพื่อรองรับการปฏิบัติการการสร้างความมั่นคงทางไซเบอร์ทั้งเชิงรุกและเชิงรับ เพื่อป้องกันความเสียหายต่อโครงสร้างพื้นฐานของประเทศ ที่อาจนำมาสู่การทำลายเศรษฐกิจได้อย่างมหาศาล

3. ความเป็นมหาอำนาจไซเบอร์ทางวิทยาศาสตร์ (Cyber Science Power)

3.1 ลำดับชั้นทางด้านผู้ใช้งาน (User Layer)

ยุคสมัยที่เทคโนโลยีและมนุษย์ได้มีส่วนร่วมและมีความสัมพันธ์ซึ่งกันและกัน นั่นทำให้การพัฒนาทางด้านเทคโนโลยีไม่สามารถเกิดความก้าวหน้าได้โดยการปราศจากความรู้ความเชี่ยวชาญของมนุษย์ คือ ส่วนสำคัญของโลกไซเบอร์ ไม่ว่าจะเป็นในบทบาทของผู้สร้างและผู้ใช้งานโลกไซเบอร์ เทคโนโลยีไซเบอร์ ได้เข้ามามีบทบาทสำคัญในการใช้ชีวิตประจำวันของมนุษย์ และมนุษย์ได้พึ่งพาโลกไซเบอร์ไม่ว่าจะเป็นทางด้านความมั่นคงแห่งชาติ การ

พัฒนาเศรษฐกิจ และการพัฒนานวัตกรรม หากเปรียบเทียบกับภูมิศาสตร์อื่นๆที่มนุษย์ได้เข้าไปมีบทบาทและได้รับผลกระทบในการดำรงชีวิต อาทิเช่น ภูมิศาสตร์ทางด้านท้องฟ้า อวกาศ ทะเล หรือ พื้นดิน ปัจจุบันมนุษย์จำเป็นที่จะต้องพัฒนาองค์ความรู้ทางด้านโลกไซเบอร์อย่างต่อเนื่อง

แผนกลยุทธ์ความมั่นคงทางไซเบอร์แห่งชาติของประเทศสหรัฐอเมริกาในยุคสมัยการบริหารของประธานาธิบดี Joe Biden ใน ค.ศ. 2023 ได้มีการสร้างวิสัยทัศน์ที่สร้างความหนักแน่นในการให้คุณค่าในการสร้างความปลอดภัยในโลกไซเบอร์ และเพื่อให้บรรลุวิสัยทัศน์ดังกล่าว การเตรียมพร้อมบุคลากรหรือประชาชนให้เหมาะสมกับวิสัยทัศน์คือสิ่งที่จำเป็น จึงได้มีการเขียนแผนกลยุทธ์ทางด้านแรงงานและการศึกษาไซเบอร์แห่งชาติ (National Cyber Workforce And Education Strategy (NCS)) ซึ่งเป็นองค์ประกอบสำคัญตามแนวทางของประธานาธิบดีในการรักษาความปลอดภัยในโลกไซเบอร์

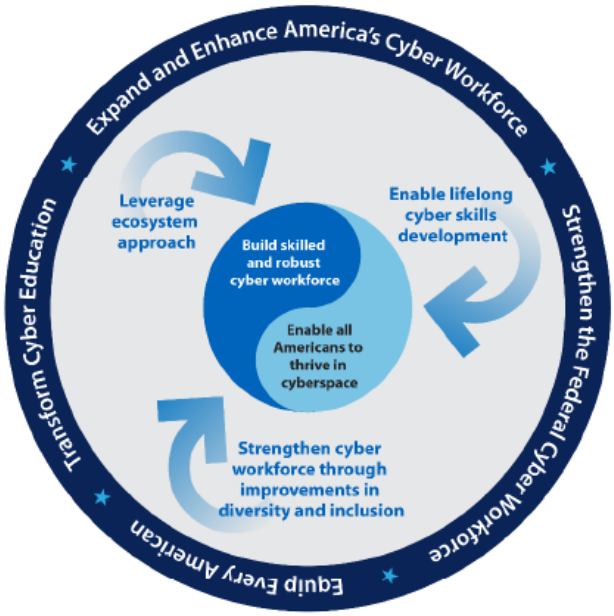
จุดประสงค์ของแผนกลยุทธ์ทางด้านแรงงานและการศึกษาไซเบอร์แห่งชาติ คือการเสริมสร้างความพร้อมทางด้านแรงงานที่มีความเชี่ยวชาญเกี่ยวกับโลกไซเบอร์ ทำให้แรงงานได้รับค่าตอบแทนที่ดี มีงานที่มีคุณภาพ และการส่งเสริมสวัสดิการ ความมั่นคงให้กับสังคมของประเทศสหรัฐอเมริกา กลยุทธ์นี้มีความตั้งใจในการปฏิรูปการศึกษาทางด้านไซเบอร์ โดยการสนับสนุนแนวทางที่เน้นทักษะเพื่อสร้างเส้นทางในการสร้างอาชีพทางไซเบอร์ที่มั่นคงยิ่งขึ้น และมีเป้าหมายเพื่อส่งเสริมความร่วมมืออย่างกว้างขวางระหว่างนายจ้าง นักการศึกษา รัฐบาล และผู้มีส่วนได้ส่วนเสียหลักอื่นๆ เพื่อตอบสนองความต้องการด้านแรงงานทั้งในระยะเร่งด่วนและระยะยาว

การศึกษาไซเบอร์และการพัฒนาบุคลากรไม่สามารถก้าวทันความต้องการและการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็วในปัจจุบัน นอกจากนี้ ทักษะที่เป็นที่ต้องการของพนักงานที่ทำงานเกี่ยวกับโลกไซเบอร์กำลังพัฒนาอย่างรวดเร็ว อาทิเช่น การพัฒนาปัญญาประดิษฐ์ (AI) และการเรียนรู้เกี่ยวกับเครื่องยนต์ (ML) อาจเปลี่ยนแปลงวิธีการปฏิบัติงานของแรงงานในทุกระดับชั้น ดังนั้น ประเทศสหรัฐอเมริกาจึงให้ความสำคัญเป็นอย่างมากในการเสริมสร้างทักษะที่จำเป็นให้กับประชากรชาวอเมริกันในการใช้คอมพิวเตอร์และอินเทอร์เน็ตอย่างมีประสิทธิภาพและเพื่อเพิ่มความมั่นใจในการใช้อินเทอร์เน็ตเพื่อทำกิจกรรมประจำวันมากขึ้น

แผนกลยุทธ์ความทางด้านแรงงานและการศึกษาไซเบอร์แห่งชาติของประเทศสหรัฐอเมริกา แบ่งออกเป็นสี่เสาหลักในการดำเนินงาน โดยเรียงลำดับดังนี้

1. การสร้างทักษะความรู้พื้นฐานทางไซเบอร์ให้กับประชากรชาวอเมริกันทุกคน
2. ปฏิรูปการศึกษาทางไซเบอร์

3. การขยายและเสริมสร้างแรงงานทางไซเบอร์ของประเทศสหรัฐอเมริกา
4. การเสริมสร้างบุคลากรทางไซเบอร์ของรัฐบาลกลาง



ภาพประกอบ 15 กลยุทธ์โดยภาพรวม

ที่มา: (The White House, 2023)

สองเสาหลักแรกมุ่งเน้นไปที่การพัฒนาทักษะทางไซเบอร์ที่จำเป็นในด้านแรงงานและสังคม เสาหลักที่สาม เกี่ยวกับประเด็นทางด้านความพยายามที่เกี่ยวข้องกับการเสริมสร้างแรงงานในโลกไซเบอร์ของประเทศ ในขณะที่เสาหลักสุดท้ายกล่าวถึงโอกาสและความท้าทายในการจ้างงานของรัฐบาลกลาง

ภายในการดำเนินงานของเสาหลักทั้งสี่นั้น มีแนวทางย่อยที่ช่วยชี้แนะแนวทางการปฏิบัติงานให้บรรลุเป้าหมายที่จำเป็น ประกอบด้วย แนวทางที่ 1 คือ การยกระดับการพัฒนาความร่วมมือระหว่างภาคแรงงานในระบบนิเวศ เพื่อตอบสนองความต้องการของแรงงานในโลกไซเบอร์ แนวทางที่ 2 คือ การสร้างโอกาสในการพัฒนาทักษะและความสามารถทางไซเบอร์แบบระยะยาวหรือตลอดชีวิต และแนวทางที่ 3 คือ การเสริมสร้างความแข็งแกร่งให้กับบุคลากรทางไซเบอร์ผ่านความหลากหลายและไม่แบ่งแยก (The White House, 2023)

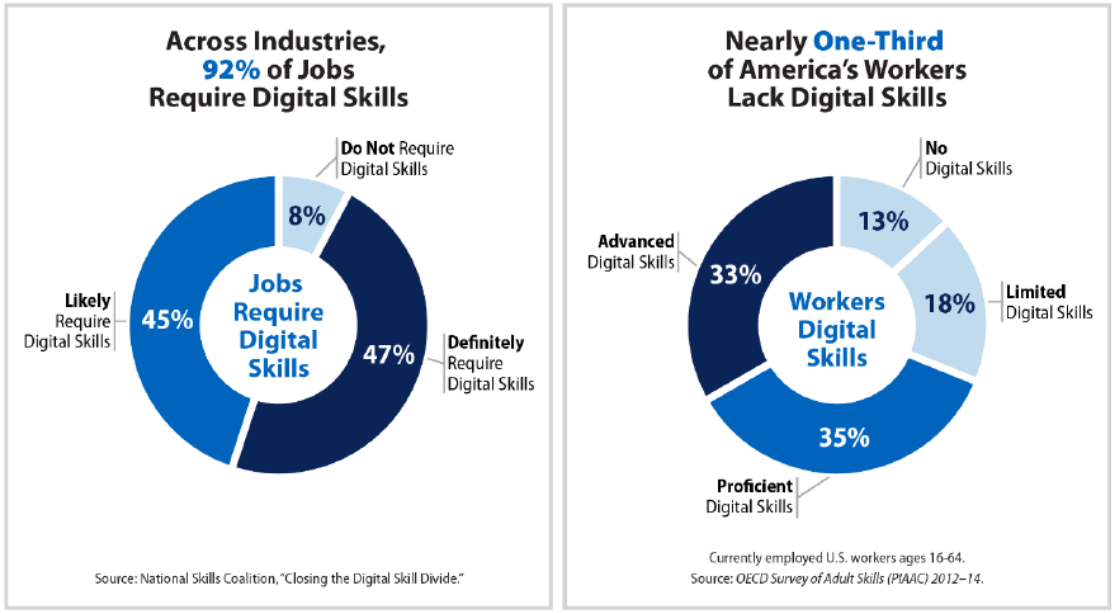
ประธานแผนกลยุทธ์ความทางด้านแรงงานและการศึกษาไซเบอร์แห่งชาติได้กำหนดทิศทางของแผนการดำเนินงานที่มีความท้าทายและถือเป็นโอกาสที่สำคัญในการพัฒนาการศึกษาไซเบอร์และแรงงานไปพร้อมกัน โดยมีข้อเรียกร้องไปยังรัฐบาลกลางของประเทศสหรัฐอเมริกาและพันธมิตรของประเทศ ในการให้ความสำคัญต่อการตัดสินใจในข้อเรียกร้องเหล่านี้ เพื่อเป็นการสร้างสภาพแวดล้อมดิจิทัลที่มีความปลอดภัย มีความยืดหยุ่น และ

สอดคล้องกับค่านิยมของสังคม ซึ่งช่วยเพิ่มความปลอดภัย ความเจริญรุ่งเรืองทางเศรษฐกิจ และพัฒนาการนวัตกรรมทางเทคโนโลยี

องค์กรแผนกลยุทธ์ความทางด้านแรงงานและการศึกษาไซเบอร์แห่งชาติ ได้เรียกร้องในการปรับเปลี่ยนทิศทางหลักที่สำคัญในการพัฒนาทางด้านแรงงานและการศึกษาไซเบอร์ ดังนี้ ข้อแรก ความรับผิดชอบต่างๆที่เกี่ยวข้องกับการปกป้องโลกไซเบอร์ ควรที่จะเปลี่ยนความรับผิดชอบจากบุคคลทั่วไป และกลุ่มธุรกิจขนาดเล็ก ไปยังตัวแสดงที่มีความสามารถที่มีประสิทธิภาพมากที่สุดในการดำเนินการเกี่ยวกับโลกไซเบอร์ เพราะความมั่นคงทางไซเบอร์ คือสิ่งที่เป็นรากฐานของโครงการที่ใช้ในการพัฒนาแรงงานและการศึกษาไซเบอร์ ซึ่งนำไปสู่การพัฒนาสภาพแวดล้อมดิจิทัลที่มีความมั่นคงและยั่งยืน และข้อที่สอง คือการพยายามในการเปลี่ยนแปลงแรงจูงใจในภาครัฐและเอกชนเพื่อสนับสนุนการลงทุนระยะยาวในด้านความมั่นคง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงนี้ จำเป็นต้องมุ่งเน้นไปที่ทักษะพื้นฐานทางไซเบอร์ การเปลี่ยนแปลงด้านการศึกษา และการศึกษาทางไซเบอร์ร่วมกันและระบบนิเวศต่างๆที่ใช้ในการพัฒนาบุคลากร

การเปลี่ยนแปลงในหลากหลายอย่าง ณ ปัจจุบัน เป็นสิ่งที่กำหนดความต้องการแรงงานทางไซเบอร์ของประเทศสหรัฐอเมริกา การตอบสนองความต้องการแรงงานทางไซเบอร์ที่มีทักษะถือเป็นเรื่องเร่งด่วน ผลการศึกษาในภาคอุตสาหกรรมชิ้นหนึ่ง ประเมินความต้องการที่ยังไม่ได้รับการตอบสนองสำหรับพนักงานที่มีหน้าที่รักษาความปลอดภัยทางไซเบอร์ จำนวน 411,000 คนใน ค.ศ. 2022 เพิ่มขึ้น 9.0% จาก ค.ศ. 2021 การศึกษาอีกชิ้นหนึ่ง ประมาณการถึงความต้องการของนายจ้างมีมากกว่าอุปทาน 32% และในมุมมองระดับโลก สถานการณ์ยิ่งเลวร้ายยิ่งขึ้น ความแตกต่างระหว่างอุปสงค์ทั่วโลกและขีดความสามารถของแรงงานในโลกไซเบอร์ใน ค.ศ. 2022 อยู่ที่ประมาณ 3.4 ล้านคน เพิ่มขึ้น 26% จากปีก่อนหน้า (The White House, 2023)

ทักษะทางไซเบอร์กำลังมีความสำคัญต่ออาชีพจำนวนมากในทุกภาคส่วนของเศรษฐกิจ ตัวอย่างเช่น มีการตีพิมพ์นิตยสารฉบับหนึ่งใน ค.ศ. 2023 พบว่า 92% ของงานในอุตสาหกรรมต่างๆ ในสหรัฐอเมริกาอย่างน้อยบุคลากรจำเป็นต้องมีทักษะด้านดิจิทัล ความต้องการนี้เกินกว่าอุปทาน เนื่องจากเกือบ 33% ของคนงานในสหรัฐฯ อายุระหว่าง 16 ถึง 64 ปี ขาดทักษะเหล่านี้ ทักษะทางไซเบอร์มีความสำคัญมากขึ้นต่อความสามารถในการแข่งขันทางเศรษฐกิจของสหรัฐฯ ในเศรษฐกิจโลก



ภาพประกอบ 16 การขาดแคลนอุปสงค์ต่ออุปทานของแรงงานในทักษะความรู้ทางด้านดิจิทัล

ที่มา: (The White House, 2023)

3.2 การอภิปรายทางวิชาการ (Academic Debates)

การอภิปรายทางวิชาการในประเทศมหาอำนาจไซเบอร์ครอบคลุมถึงการอภิปรายและการถกเถียงระหว่างนักวิชาการ นักวิจัย และผู้กำหนดนโยบายเกี่ยวกับแง่มุมต่างๆ ของอำนาจทางไซเบอร์ และผลกระทบต่อความมั่นคงของชาติ ความสัมพันธ์ระหว่างประเทศ เทคโนโลยี และสังคม การอภิปรายเหล่านี้มักเกี่ยวข้องกับคำถามและประเด็นสำคัญที่ส่งผลต่อความเข้าใจและการพัฒนาอำนาจทางไซเบอร์ภายในประเทศ หัวข้อสำคัญในการอภิปรายทางวิชาการ ได้แก่ คำจำกัดความและการวัดอำนาจทางไซเบอร์ บทบาทของเทคโนโลยีกับกลยุทธ์ในการกำหนดความสามารถทางไซเบอร์ การระบุแหล่งที่มาและการยับยั้งในโลกไซเบอร์ บรรทัดฐานและธรรมาภิบาลในไซเบอร์สเปซ ผลกระทบของอำนาจทางไซเบอร์ต่อสังคมและประชาธิปไตย และ ความสมดุลระหว่างความมั่นคงทางไซเบอร์และความผิดทางไซเบอร์ การอภิปรายเหล่านี้มีส่วนช่วยให้เกิดความเข้าใจที่ลึกซึ้งยิ่งขึ้นเกี่ยวกับโอกาสและความท้าทายที่เกี่ยวข้องกับการควบคุมอำนาจทางไซเบอร์ และการตัดสินใจเชิงนโยบายที่มุ่งนำทางไปสู่การสร้างอำนาจทางไซเบอร์ยอย่างมีประสิทธิภาพ

งานวิชาการเกี่ยวกับกลยุทธ์ทางไซเบอร์ มักจะเน้นไปที่ตัวแปรเชิงโครงสร้างและลัทธิเหตุผลนิยม (rationalism) อย่างไรก็ตาม งานวิจัยของ Lonergan and Schneider ได้บ่งชี้ถึงบทบาทสำคัญของแนวคิดในการกำหนดกระบวนการและนโยบายการตัดสินใจ

แนวความคิดต่างๆเหล่านั้น ได้ทำหน้าที่เป็นกรอบแนวทางในการชี้นำความไม่แน่นอน การอำนวยความสะดวกฉันทามติในการหาข้อตกลงร่วมกันในหน่วยงานภาครัฐ และการสร้างการพึ่งพานโยบายในระยะยาว ในบริบทของการก่อตั้งการป้องกันประเทศที่เผชิญกับภัยคุกคามและโอกาสที่เกิดขึ้น โลกไซเบอร์มีความโดดเด่นในฐานะโดเมนที่ได้รับอิทธิพลอย่างมาก กลยุทธ์ทางไซเบอร์ด้านกลาโหมของสหรัฐฯ ได้รับการเปลี่ยนแปลงที่สำคัญสองครั้งระหว่าง ค.ศ. 2011 ถึง ค.ศ. 2018 การเปลี่ยนจากการมองโลกในแง่ดีไปสู่การมองโลกในแง่ร้ายเกี่ยวกับอินเทอร์เน็ตและคุณค่าทางประชาธิปไตยเกิดขึ้นในช่วงรัฐบาลโอบามา โดยพื้นฐานนโยบายที่เกี่ยวกับการยกระดับ บรรทัดฐาน และ การสร้างความมั่นคงทางไซเบอร์ยังคงไม่เปลี่ยนแปลง อย่างไรก็ตาม ภายใต้การบริหารของอดีตประธานาธิบดีโดนัล ทรัมป์ มีการเปลี่ยนแปลงอย่างมากในความเชื่อเกี่ยวกับการแพร่กระจายทางไซเบอร์ บรรทัดฐานและความมั่นคงทางไซเบอร์ ส่งผลให้กระทรวงกลาโหมมีบทบาทใหม่ในโลกไซเบอร์ การศึกษาตรวจสอบต้นกำเนิดและวิวัฒนาการของแนวคิดเหล่านี้ผ่านการวิเคราะห์กลยุทธ์การป้องกันทางไซเบอร์สามกลยุทธ์ (Lonergan & Schneider, 2023) ดังนี้

ค.ศ. 2011 กลยุทธ์แห่งการมองโลกในแง่ดีและความคลุมเครือ

กระทรวงกลาโหมเปิดตัวยุทธศาสตร์ไซเบอร์ครั้งแรกในเดือนกรกฎาคม ค.ศ. 2011 หลังจากการจัดตั้งกองบัญชาการไซเบอร์ (Cyber Command) เป็นหน่วยบัญชาการรองย่อยภายใต้กองบัญชาการยุทธศาสตร์สหรัฐ กลยุทธ์นี้สอดคล้องกับยุทธศาสตร์โลกไซเบอร์ระหว่างประเทศ ของรัฐบาลโอบามา ซึ่งแสดงถึงการมองโลกในแง่ดีเกี่ยวกับไซเบอร์สเปซและศักยภาพของอินเทอร์เน็ตในการส่งเสริมสิทธิมนุษยชน ประชาธิปไตย และโอกาสทางเศรษฐกิจ การมองโลกในแง่ดีนี้เสริมด้วยเหตุการณ์ต่างๆ เช่น เหตุการณ์อาหรับสปริง (Arab Spring) ซึ่งโซเชียลมีเดียถูกมองว่าเป็นเครื่องมือสำคัญสำหรับการเคลื่อนไหวในระบอบประชาธิปไตย กลยุทธ์ของทำเนียบขาวมองว่าพื้นที่โลกไซเบอร์ที่เสรี ทำให้เปิดกว้าง สร้างความเป็นเอกภาพ มีความเชื่อถือได้ และปลอดภัย เป็นเป้าหมายที่เป็นประโยชน์ในระดับสากล โดยดำเนินการผ่านเครื่องมือที่ไม่ใช่ทางการทหารเป็นหลัก เช่น การทูต ความร่วมมือระหว่างประเทศ และการส่งเสริมบรรทัดฐาน แนวคิดเหล่านี้มีอิทธิพลอย่างมากต่อแนวทางการบริหารของโอบามาในการกำหนดบทบาทและความรับผิดชอบทางไซเบอร์ของหน่วยงานต่างๆ ของรัฐบาลในช่วงห้าปีต่อจากนี้

จากมุมมองของกระทรวงกลาโหม กลยุทธ์ทางไซเบอร์ของทำเนียบขาวไม่ได้ให้ความสำคัญทางการทหารเป็นหลักสำหรับความมีอำนาจทางการเมืองระหว่างประเทศ แต่เรียกร้องให้กระทรวงกลาโหมเข้าใจและปรับตัวให้เข้ากับความจำเป็นที่เพิ่มขึ้นสำหรับการใช้งานโลกไซเบอร์ที่ปลอดภัยและเชื่อถือได้ และการสนับสนุนพันธมิตรทางการทหารของ

กองทัพที่มีอยู่ในการสร้างความร่วมมือในโลกไซเบอร์ แม้ว่ากลยุทธ์ดังกล่าวเป็นการใช้แนวคิดความมั่นคงไซเบอร์ที่เน้นความร่วมมือเข้าด้วยกัน แต่การสนับสนุนกลับเป็นแนวทางการป้องกันเป็นส่วนใหญ่ โดยเน้นการเพิ่มประสิทธิภาพการป้องกันทางไซเบอร์และความยืดหยุ่นในการทำงานเพื่อสร้างความมั่นคงทางไซเบอร์ การอ้างอิงถึงมาตรการลงโทษเน้นย้ำถึงความสำคัญของความเป็นสัดส่วน และการพยายามลดการพึ่งพากำลังทหารทุกครั้งที่เป็นไปได้ ยุทธศาสตร์ดังกล่าวแสดงให้เห็นถึงพฤติกรรมที่กระทรวงกลาโหมใช้ทางเลือกทั้งหมดก่อนที่จะหันไปใช้ปฏิบัติการทางทหาร โดยพิจารณาอย่างรอบคอบถึงต้นทุนและความเสี่ยงของทั้งการกระทำและการไม่ปฏิบัติ และจัดลำดับความสำคัญของการกระทำที่สอดคล้องกับค่านิยมของประเทศ สนับสนุนความชอบธรรม และได้รับการสนับสนุนจากนานาชาติ

ความพยายามครั้งแรกของกระทรวงกลาโหมในการกำหนดกลยุทธ์ทางไซเบอร์ใน ค.ศ. 2011 สะท้อนความเข้าใจและความคลุมเครือของฝ่ายบริหารของโอบามาเกี่ยวกับบทบาทของกองทัพในขอบเขตที่มองว่ามีแนวโน้มที่ดีต่อการปกครองและความก้าวหน้าทางสังคม ด้วยเหตุนี้ กลยุทธ์ทางไซเบอร์ของกระทรวงกลาโหมชุดแรกจึงทำหน้าที่เป็นการรับรู้ถึงความสำคัญของโลกไซเบอร์ในการป้องกันมากกว่าการระบุรายละเอียดเกี่ยวกับลำดับความสำคัญ ภัยคุกคาม หรือความพยายามเชิงกลยุทธ์ โดยสรุปแผนริเริ่มเชิงกลยุทธ์ 5 ประการ ซึ่งรวมถึงการจัดกระทรวงกลาโหมเพื่อใช้ประโยชน์จากศักยภาพของโลกไซเบอร์อย่างเต็มที่ การปกป้องเครือข่ายและระบบของกระทรวง ส่งเสริมความร่วมมือกับหน่วยงานรัฐบาลกลางและภาคเอกชนอื่นๆ ยกระดับความปลอดภัยทางไซเบอร์โดยรวมในระดับสากลผ่านความร่วมมือกับพันธมิตรและพันธมิตร และปลูกฝังความมีประสิทธิผลกำลังคนและส่งเสริมนวัตกรรมภายในโดเมนไซเบอร์

กลยุทธ์ไซเบอร์ของกระทรวงกลาโหมแผนแรกขาดวาทกรรมที่สำคัญเกี่ยวกับการใช้อำนาจทางการทหารภายในโลกไซเบอร์ ไม่ได้ระบุศัตรูอย่างชัดเจนและจัดการกับผู้มีบทบาทที่ไม่ใช่รัฐและภัยคุกคามภายในอย่างเด่นชัดพอๆ กับรัฐชาติใดๆ นอกจากนี้ กลยุทธ์ยังคงคลุมเครือเกี่ยวกับวิธีที่กองทัพสหรัฐฯ ตั้งใจที่จะตอบโต้ภัยคุกคามที่มาจากไซเบอร์สเปซ ซึ่งสะท้อนถึงความไม่แน่นอนในวงกว้างเกี่ยวกับบทบาทของกองทัพในขอบเขตนี้และความสัมพันธ์กับหน่วยงานของรัฐบาลกลางอื่นๆ ในการต่อสู้กับภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม เอกสารดังกล่าวชี้ให้เห็นถึงความต่อเนื่องของกลยุทธ์ด้านไซเบอร์ของสหรัฐฯ ในทศวรรษต่อๆ ไป โดยเฉพาะอย่างยิ่งในการจัดลำดับความสำคัญของการปกป้องและยึดถือหลักการต่างๆ เช่น ความเป็นส่วนตัว เสรีภาพของพลเมือง การแสดงออกอย่างเสรี

และนวัตกรรม ขณะเดียวกันก็จัดการกับช่องโหว่ที่เกิดจากการพึ่งพาของกระทรวงกลาโหมกับการใช้งานเทคโนโลยีดิจิทัล (Lonergan & Schneider, 2023)

ค.ศ. 2015 : ความเป็นจริงของโลกไซเบอร์

ตามกลยุทธ์ ค.ศ. 2011 ขนาดความรุนแรง และเป้าหมายของเหตุการณ์ทางไซเบอร์พุ่งสูงขึ้นอย่างเห็นได้ชัด ซึ่งส่งผลกระทบต่อความมั่นคงของชาติและผลประโยชน์ด้านกลาโหมของสหรัฐฯ การจารกรรมทางไซเบอร์และการโจรกรรมทรัพย์สินทางปัญญาจากประเทศจีนเพิ่มขึ้นอย่างรวดเร็ว และเหตุการณ์โจมตีทางไซเบอร์หลากหลายเหตุการณ์ใน ค.ศ. 2014 ไม่ว่าจะเป็นเหตุการณ์ของ APT10 ที่ถูกกล่าวหาว่าเชื่อมโยงกับกระทรวงความมั่นคงแห่งรัฐของจีน โดยกำหนดเป้าหมายจากโจรกรรมข้อมูลบุคลากรกองทัพเรือสหรัฐฯ มากกว่า 100,000 คน ตลอดจนเหตุการณ์ Cloud Hopper (การโจมตีด้วยการส่งอีเมล์ปลอมเข้าสู่เป้าหมายและให้เป้าหมายติดตั้งมัลแวร์เพื่อการเข้าถึงข้อมูลต่างๆ) และการแฮ็กสิทธิในการเข้าถึงสำนักงานของการบริหารงานบุคคล เหตุการณ์ที่อิหร่านได้ทำการโจมตีทางไซเบอร์ รวมถึงการโจมตีภาคการเงินของสหรัฐฯ และการโจมตีแซนด์สคาสิโน เหตุการณ์ที่การโจมตีบริษัทโซนี่ พิคเจอร์สของเกาหลีเหนือ ทำให้เกิดความรุนแรงขึ้นอย่างมาก เหตุการณ์เหล่านี้กระตุ้นให้ฝ่ายบริหารของอดีตประธานาธิบดีโอบามา ประเมินมุมมองในแง่ดีก่อนหน้านี้เกี่ยวกับโลกไซเบอร์อีกครั้ง โดยภาพรวมภัยคุกคามทางไซเบอร์ได้พัฒนาไปจนถึงตัวแสดงที่มีความสามารถและมีแรงจูงใจจำนวนมาก ก่อให้เกิดความท้าทายที่สำคัญต่อความพยายามด้านความปลอดภัยทางไซเบอร์ของสหรัฐฯ เมื่อเทียบกับค.ศ. 2011 (Lonergan & Schneider, 2023)

แม้จะมีภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงขึ้น แต่ฝ่ายบริหารของโอบามายังคงลังเลที่จะพึ่งพากองทัพเพื่อจัดการกับความท้าทายเหล่านี้ โดยความไม่แน่นอนที่เพิ่มขึ้นในช่วงสี่ปีนับตั้งแต่ยุทธศาสตร์ ค.ศ. 2011 ฝ่ายบริหารเริ่มมีความกังวลมากขึ้นเกี่ยวกับความเสี่ยงที่จะบานปลาย และพยายามจำกัดบทบาทของอำนาจทางการทหารในโลกไซเบอร์ อดีตรัฐมนตรีกลาโหม Chuck Hagel เน้นย้ำถึงความมุ่งมั่นของเพนตากอนในการใช้ความยับยั้งชั่งใจในปฏิบัติการทางไซเบอร์นอกเหนือจากเครือข่ายของรัฐบาลสหรัฐฯ และสนับสนุนให้ประเทศอื่นๆ ปรับใช้แนวทางที่คล้ายกัน ด้วยเหตุนี้ การมุ่งเน้นของกองทัพจึงเปลี่ยนไปสู่การยับยั้งการโจมตีทางไซเบอร์ด้วยการแสดงให้เห็นถึงความพร้อมในการตอบสนอง แทนที่จะดำเนินการเชิงรับหรือเชิงป้องกันต่อภัยคุกคามที่อาจเกิดขึ้น ยุทธศาสตร์นี้มีจุดมุ่งหมายเพื่อเสริมสร้างบรรทัดฐานในการยับยั้งชั่งใจก่อนที่ฝ่ายใดฝ่ายหนึ่งจะทำการโจมตี ซึ่งสนับสนุนโดยฝ่ายบริหารผ่านช่องทางการทูต เช่น กลุ่มผู้เชี่ยวชาญ

ของรัฐบาลแห่งสหประชาชาติ และเวทีระหว่างประเทศต่างๆ รวมถึงกลุ่มประเทศ G7 G20 องค์การเพื่อความมั่นคงและความร่วมมือในยุโรป และองค์การรัฐอเมริกัน

กลยุทธ์ไซเบอร์ของกระทรวงกลาโหม ค.ศ. 2015 ตอกย้ำความตึงเครียดภายในฝ่ายบริหารของโอบามาระหว่างการรับรู้ถึงภาพรวมของภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงมากยิ่งขึ้น และความระมัดระวังเกี่ยวกับบทบาทของกองทัพในการจัดการกับความท้าทายเหล่านี้ เพื่อหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้น กลยุทธ์ ค.ศ. 2015 แตกต่างจาก ค.ศ. 2011 โดยมีการระบุศัตรูที่มีลำดับความสำคัญอย่างชัดเจน ซึ่งรวมถึงรัสเซีย จีน อิหร่าน เกาหลีเหนือ และตัวแสดงที่ไม่ใช่รัฐ ขณะเดียวกันก็สรุปเป้าหมายเชิงกลยุทธ์ 5 ประการ ประกอบด้วย การสร้างกองกำลังที่เตรียมพร้อม การปกป้องเครือข่ายข้อมูล การเตรียมปกป้องขอบเขตภายในประเทศสหรัฐฯ การพัฒนาทางเลือกทางไซเบอร์สำหรับการควบคุมความขัดแย้ง และการส่งเสริมพันธมิตรในการป้องปรามและการสร้างเสถียรภาพ กลยุทธ์เหล่านี้ถือเป็นการแตกต่างจากวิสัยทัศน์เชิงบวกของกลยุทธ์ ค.ศ. 2011 โดยเน้นแนวทางที่เน้นไปที่ภัยคุกคามทางไซเบอร์มากขึ้น เพื่อจัดการกับภัยคุกคามเหล่านี้ ยุทธศาสตร์ ค.ศ. 2015 อาศัยการป้องปรามอย่างหนัก โดยกองกำลังไซเบอร์ของกองทัพถูกสำรองไว้ แสดงให้เห็นถึงความสามารถในการตอบโต้ได้รับการพัฒนาอย่างเห็นได้ชัด นอกจากนี้ ฝ่ายบริหารของโอบามายังได้แนะนำการกำกับดูแลและควบคุมการปฏิบัติการทางไซเบอร์ทางการทหารที่สำคัญ รวมถึงการแสวงหาประโยชน์จากเครือข่ายคอมพิวเตอร์ การยอมรับในข้อผิดพลาดที่ผ่านมาในการขาดความชัดเจน และการสนับสนุนให้ระมัดระวัง และการกำกับดูแลในการปฏิบัติการทางไซเบอร์เชิงรุก (Lonergan & Schneider, 2023)

ค.ศ. 2018 : แนวทางที่กล้าแสดงออกมากขึ้น

คณะบริหารของทรัมป์เปลี่ยนจากช่วงเวลาแห่งการป้องกัน หรือการมีนโยบายเชิงรับไปสู่ท่าทีที่ยอมรับความเสี่ยงได้มากขึ้น โดยเฉพาะอย่างยิ่งที่เห็นได้ชัดเจนหลังจากการปฏิบัติการด้านข้อมูลทางไซเบอร์ของรัสเซียในช่วงการเลือกตั้งประธานาธิบดีสหรัฐฯ ค.ศ. 2016 เหตุการณ์นี้จุดประกายให้เกิดการถกเถียงอย่างเข้มข้นภายในฝ่ายบริหารของโอบามาเกี่ยวกับการตอบสนองที่เหมาะสม รวมถึงการกระทำทางไซเบอร์ที่อาจเกิดขึ้น รายงานระบุว่ามีการพิจารณาปฏิบัติการทางไซเบอร์เชิงรุก แต่ท้ายที่สุดก็ถูกยกเลิกด้วยความกังวลว่าจะกระตุ้นให้รัสเซียรุกรานต่อไป หนึ่งในตัวเลือกที่พิจารณาคือการปิดเว็บไซต์ที่โฮสต์เกิดข้อมูลที่รั่วไหล การโจมตีทางไซเบอร์ต่อสื่อรัสเซีย และการกำหนดเป้าหมายโครงสร้างพื้นฐานคำสั่งและการควบคุมที่ใช้โดยหน่วยข่าวกรองรัสเซีย อย่างไรก็ตาม การตอบสนองในท้ายที่สุดอาศัยมาตรการทางการทูต เศรษฐกิจ และการบังคับใช้กฎหมาย มากกว่าการตอบโต้ทางไซเบอร์โดยตรง

หลังจากเหตุการณ์ใน ค.ศ. 2016 และความกังวลที่เพิ่มมากขึ้นเกี่ยวกับภัยคุกคามทางไซเบอร์ มีการเปลี่ยนแปลงที่ชัดเจนในมุมมองภายในภาคเอกชนและกระทรวงกลาโหมเกี่ยวกับสมมติฐานก่อนหน้านี้เกี่ยวกับการบานปลายของการรุกรานทางไซเบอร์ ซึ่งนำไปสู่การเรียกร้องให้มีกลยุทธ์เชิงรุกมากขึ้น การเปลี่ยนแปลงนี้สะท้อนให้เห็นในเอกสารสำคัญสองฉบับ ประการแรก กองบัญชาการไซเบอร์ของสหรัฐฯ เปิดเผยวิสัยทัศน์ของคำสั่ง ซึ่งสนับสนุน "การมีส่วนร่วมอย่างต่อเนื่อง" เพื่อเผชิญหน้ากับศัตรูในโลกไซเบอร์อย่างต่อเนื่องแทนที่จะพึ่งพามาตรการตอบโต้เพียงอย่างเดียว วิสัยทัศน์นี้มีจุดมุ่งหมายเพื่อให้บรรลุ "ความเหนือกว่าทางไซเบอร์" โดยการมีส่วนร่วมและแข่งขันกับฝ่ายตรงข้ามอย่างต่อเนื่องเพื่อสร้างความได้เปรียบในการปฏิบัติงาน ต่อจากนั้น กระทรวงกลาโหมได้เผยแพร่บทสรุปสาธารณะของกลยุทธ์ทางไซเบอร์ใน ค.ศ. 2018 โดยแนะนำแนวคิด "การปกป้องไปข้างหน้า" เพื่อตอบโต้ภัยคุกคามทางไซเบอร์ล่วงหน้าที่อยู่นอกเครือข่ายของสหรัฐฯ และก่อนที่การโจมตีที่อาจเกิดขึ้นจะเกิดขึ้น

วิสัยทัศน์คำสั่งจากกองบัญชาการไซเบอร์ของสหรัฐฯ และยุทธศาสตร์ไซเบอร์ ค.ศ. 2018 ที่เผยแพร่โดยกระทรวงกลาโหม ได้ประกาศมุมมองใหม่ๆ เกี่ยวกับการแพร่กระจายทางไซเบอร์ และบทบาทของกองทัพในการกำหนดบรรทัดฐานของการยับยั้งการโจมตีที่อาจเกิดขึ้น แตกต่างจากแนวทางของรัฐบาลโอบามาซึ่งมุ่งเน้นไปที่กลยุทธ์การป้องกันความเสี่ยงและการป้องปรามโดยเน้นบรรทัดฐานทางการฑูตและการป้องกัน ความยืดหยุ่น และการตอบโต้ที่อาจเกิดขึ้น

ในช่วงเวลา ค.ศ. 2018 กระทรวงกลาโหม (DoD) ได้เห็นการขยายตัวและการพัฒนาที่โดดเด่น โดยกองบัญชาการไซเบอร์ของสหรัฐฯ ได้รับการยกระดับเป็นหน่วยบัญชาการรบแบบรวมศูนย์ ซึ่งสอดคล้องกับกองกำลังภารกิจไซเบอร์ (CMF) ที่สามารถปฏิบัติการได้เต็มรูปแบบ การเติบโตขององค์กรนี้มาพร้อมกับการมอบอำนาจในการปฏิบัติการทางไซเบอร์เชิงรุกภายใต้คำสั่งของประธานาธิบดี นอกจากนี้ กองบัญชาการไซเบอร์ของสหรัฐฯ ยังให้ความสำคัญกับการป้องกันการเลือกตั้ง โดยจัดตั้งกลุ่มรัสเซียกลุ่มเล็กขึ้นเพื่อปกป้องการเลือกตั้งใน ค.ศ. 2018 และ ค.ศ. 2020 และมีส่วนร่วมในการปฏิบัติการการต่อต้านทางไซเบอร์เพื่อขัดขวางหน่วยงานต่างๆ เช่น Internet Research Agency ที่เกี่ยวข้องกับการแทรกแซงการเลือกตั้ง กองบัญชาการไซเบอร์ของสหรัฐฯได้ขยายความร่วมมือไปยังพันธมิตร เช่น ประเทศเอสโตเนียและ ประเทศมอนเตเนโกร ผ่านภารกิจล่าภัยคุกคามเชิงรุกในเครือข่ายพันธมิตร กองบัญชาการไซเบอร์ของสหรัฐฯ ยังสนับสนุนภาคเอกชนผ่านโครงการริเริ่มใน “การฉีดวัคซีนป้องกันมัลแวร์ (malware inoculation) และโครงการนำร่องในภาคต่างๆ เช่น การบริการทางการเงินและพลังงาน

การส่งเสริมการฝึกอบรมร่วมกันและการแบ่งปันข้อมูล นอกจากนี้ กองบัญชาการไซเบอร์ของสหรัฐฯ ยังร่วมต่อสู้กับอาชญากรรมในโลกไซเบอร์ โดยมีส่วนร่วมในการดำเนินการเพื่อลงโทษสำหรับกลุ่มแรนซัมแวร์โดยความร่วมมือกับสหราชอาณาจักร ความพยายามเหล่านี้เน้นย้ำถึงการเปลี่ยนแปลงที่สำคัญไปสู่บทบาททางการทหารเชิงรุกและมีส่วนร่วมมากขึ้นในโลกไซเบอร์ ซึ่งถือเป็นการพัฒนาที่สำคัญจากมุมมองก่อนหน้านี้ (Lonergan & Schneider, 2023)

3.3 ความเป็นสถาบันนิยม (Institutionalization)

3.3.1 องค์กรความมั่นคงทางไซเบอร์ (Cybersecurity Agencies)

การก่อตั้งโครงสร้างทางสถาบันเพื่อใช้ในการพัฒนาการศึกษาไซเบอร์ เริ่มต้นขึ้นใน ค.ศ. 1995 โดยการบริหารของอดีตประธานาธิบดี Bill Clinton ในการก่อตั้งคณะกรรมาธิการด้านการคุ้มครองโครงสร้างพื้นฐานที่สำคัญ (The Presidential Commission on Critical Infrastructure Protection (PCCIP)) ที่มีหน้าที่ในการรายงานรายละเอียดความมั่นคงที่ครอบคลุมของระบบโครงสร้างพื้นฐานทั้งหมดของประเทศสหรัฐอเมริกา ซึ่งการมอบหมายหน้าที่นี้ ไม่เพียงแต่ครอบคลุมความมั่นคงทางด้านข้อมูลและเครือข่ายโทรคมนาคมเท่านั้น แต่ยังรวมไปถึงภาคการเงิน การขนส่งพลังงาน และบริการฉุกเฉินด้วย โดยเน้นไปที่ความเสี่ยงทางไซเบอร์ โดยมีจุดประสงค์หลักในการก่อตั้งทั้งหมดสองจุดประสงค์ด้วยกัน คือ จุดประสงค์แรก เนื่องจากองค์ความรู้ทางไซเบอร์ยังเป็นเรื่องที่มีองค์ความรู้ที่ใหม่มากในช่วงเวลานั้น และจุดประสงค์ที่สอง โครงสร้างพื้นฐานต่างๆอาศัยการใช้ข้อมูลและเครือข่ายการเชื่อมต่อต่างๆจากโลกไซเบอร์ คณะกรรมาธิการด้านการคุ้มครองโครงสร้างพื้นฐานที่สำคัญ ประกอบไปด้วยตัวแทนจากหลากหลายหน่วยงานภาครัฐ รวมถึงการมีส่วนร่วมของภาคเอกชน แสดงให้เห็นถึงการดำเนินนโยบายความมั่นคงในขอบเขตทางด้านเทคโนโลยี ที่ไม่ใช่เพียงหน้าที่ของภาครัฐเพียงอย่างเดียว แต่เป็นการร่วมแบ่งปันความรับผิดชอบระหว่างภาครัฐและภาคเอกชน ทำให้เกิดการเปิดรับกลยุทธ์ที่เป็นไปได้ใหม่ๆในการพัฒนานโยบายความมั่นคง (Bendrath, 2001)

การทำงานร่วมกันระหว่างคณะกรรมาธิการด้านการคุ้มครองโครงสร้างพื้นฐานที่สำคัญและภาคเอกชน อดีตประธานาธิบดี Bill Clinton ยังได้ก่อตั้งคณะทำงานเฉพาะกิจด้านการปกป้องโครงสร้างพื้นฐาน (The Infrastructure Protection Task Force (IPTF)) ในการรับมือกับปัญหาที่เกิดขึ้นกระทันหันในการปกป้องโครงสร้างพื้นฐาน ก่อนที่จะทำการรายงานไปยัง PCCIP ซึ่งสมาชิกของ IPTF ได้ถูกคัดเลือกมาจากสำนักงานสืบสวนกลางสหรัฐอเมริกา (Federal Bureau of Investigation (FBI)), กระทรวงกลาโหมสหรัฐ (Department of Defense) และสำนักงานความมั่นคงแห่งชาติ (National Security

Agency) การทำงานของ IPTF สามารถอธิบายเปรียบเสมือนเป็นประสานการทำงานร่วมกันของ 2 รูปแบบการทำงาน โดยรูปแบบแรก คือ การทำงานระหว่างภาครัฐและภาคเอกชน ที่อยู่ใน PCCIP และรูปแบบการทำงานนโยบายความมั่นคงแบบดั้งเดิม ที่เป็นหน้าที่ของหน่วยงาน FBI หรือ กระทรวงกลาโหม IPTF มีสถานที่ตั้งการทำงานอยู่ที่กระทรวงยุติธรรมในการใช้งาน ศูนย์สืบสวนคอมพิวเตอร์และประเมินภัยคุกคามโครงสร้างพื้นฐาน (Computer Investigations and Infrastructure Threat Assessment Center (CITAC)) และเป็นสถานที่ทำงานเดียวกันกับ FBI ซึ่งทำให้กระบวนการตัดสินใจในการขั้นตอนใช้ทรัพยากรต่างๆของหน่วยงาน ขึ้นอยู่กับการตัดสินใจของหน่วยงาน FBI เป็นหลัก และมีการใช้กระบวนการตัดสินในในเชิงการทหารเป็นอย่างมากด้วยเช่นกัน (Bendrath, 2001)

ระบบราชการของรัฐบาลกลางสหรัฐนั้นมีขนาดที่กว้างใหญ่และซับซ้อน ไม่ทราบจำนวนที่แน่นอนของหน่วยงาน สำนักงาน คณะกรรมการ แผนกและหน่วยงานของรัฐบาลกลางทั้งหมดมีหน้าที่รับผิดชอบในการปกป้องระบบ ICT ของตนเอง และหลายแห่งมีหน้าที่รับผิดชอบเฉพาะภาคส่วนสำหรับโครงสร้างพื้นฐานที่สำคัญที่หน่วยงานนั้นๆรับผิดชอบอำนาจการกำกับดูแลของแผนกและหน่วยงานต่างๆ จะมีความแตกต่างกันออกไป หน่วยงานส่วนใหญ่มีหน้าที่รับผิดชอบทั่วไปในการควบคุมในขอบเขตของหน่วยงานของตนเอง ส่วนหน่วยงานอื่นๆ มีกฎระเบียบเฉพาะด้านความมั่นคงทางไซเบอร์ ในขณะที่บางหน่วยงานไม่มีขอบเขตอำนาจที่ชัดเจนในการกำกับควบคุมความมั่นคงทางไซเบอร์ นอกจากนี้ ในบางกรณีเอกสารกลยุทธ์ความมั่นคงไซเบอร์จะมอบหมายบทบาทและความรับผิดชอบระดับสูงให้กับหน่วยงานรัฐบาลกลาง แต่ให้รายละเอียดการดำเนินการขึ้นอยู่กับดุลยพินิจของหน่วยงาน

แม้ว่าความรับผิดชอบในการนำนโยบายไซเบอร์ไปปฏิบัติจะมีการกระจายไปในวงกว้าง บทบาทการประสานงานนโยบายหลักจะอยู่ภายใต้การดูแลของคณะกรรมการนโยบายระหว่างหน่วยงานโครงสร้างพื้นฐานสารสนเทศและการสื่อสาร (ICI-IPC) ของสภาความมั่นคงแห่งชาติในทำเนียบขาว ซึ่งเป็นการร่วมการดำเนินงานระหว่างสภาความมั่นคงแห่งมาตุภูมิ (Homeland Security Council) และหน่วยงานประสานงานความมั่นคงทางไซเบอร์ (Cyber Security Coordinator (CSC)) ที่สำนักงานความมั่นคงทางไซเบอร์ของสภาความมั่นคงแห่งชาติ โดย CSC ทำหน้าที่ในการพัฒนาแผนทางด้านยุทธศาสตร์และนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และกำกับดูแลการดำเนินงานของหน่วยงานตามนโยบายเหล่านั้น และทำหน้าที่เป็นที่ปรึกษาหลักของประธานสภาความมั่นคงแห่งชาติ รายงานต่อสภา และให้คำปรึกษาในทำเนียบขาว รวมถึงการประสานงานนโยบายและกิจกรรมที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกา (CCDCOE, 2015)

นอกเหนือจากบทบาทของหน่วยงานในทำเนียบขาวแล้ว กระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) ยังเป็นสถาบันหลักที่รับผิดชอบด้านความปลอดภัยทางไซเบอร์ภายในขอบเขตของประเทศสหรัฐอเมริกาแม้ว่าจะมีคำสั่งทางกฎหมายที่จำกัดในการปกป้องระบบข้อมูลของรัฐบาลกลางก็ตาม หน้าที่หลักของ DHS คือ เสริมสร้างความปลอดภัยและความยืดหยุ่นของโครงสร้างพื้นฐานที่สำคัญ , ช่วยเหลือหน่วยงานพลเรือนของรัฐบาลกลางในเรื่องการจัดซื้อจัดจ้างที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์และ, ส่งเสริมการนำนโยบายตามความเสี่ยงทั่วไปและแนวทางปฏิบัติที่ดีที่สุดในการนำไปปรับใช้, การบังคับใช้กฎหมายขั้นสูง, การตอบสนองต่อเหตุการณ์ และความสามารถในการรายงาน และการรักษาความปลอดภัยของระบบนิเวศไซเบอร์ที่ดี

กระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) ดำเนินการผ่านแผนกความมั่นคงทางไซเบอร์แห่งชาติเพื่อเสนอทิศทางเชิงกลยุทธ์และประสานความพยายามของรัฐบาลกลาง ที่มีจุดมุ่งหมายเพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญ ภายในหน่วยงาน 22 แห่งของ DHS นั้น คณะกรรมการป้องกันและคุ้มครองโครงการแห่งชาติ (National Protection and Programs Directorate (NPPD)) ซึ่งเป็นที่ตั้งของศูนย์บูรณาการความปลอดภัยทางไซเบอร์และการสื่อสารแห่งชาติ (National Cybersecurity & Communications Integration Centre (NCCIC)) ได้รับมอบหมายหน้าที่เป็นพิเศษในการริเริ่มด้านความปลอดภัยทางไซเบอร์ NPPD รับผิดชอบหลักในการดำเนินภารกิจความมั่นคงทางไซเบอร์ระดับชาติจากการมอบหมายงานโดย DHS โดยมุ่งเน้นไปที่วัตถุประสงค์ที่ไม่ใช่การบังคับใช้กฎหมายภายในขอบเขตของความมั่นคงทางไซเบอร์

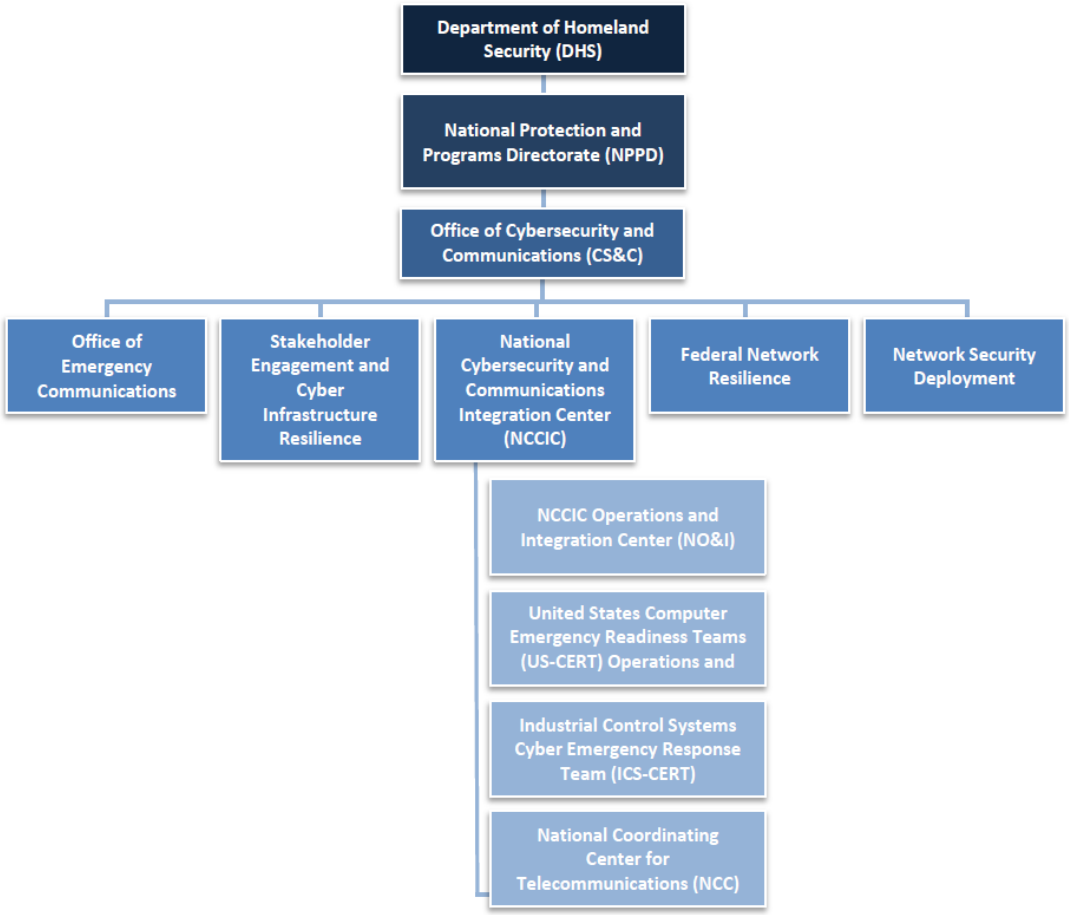
กระทรวงการต่างประเทศ (Department of State (DoS)) มีหน้าที่รับผิดชอบหลักในการเผยแพร่และปรับนโยบายความมั่นคงทางไซเบอร์ที่ได้รับมอบหมายจากประธานาธิบดีในระดับโลก นอกเหนือจากความมั่นคงทางไซเบอร์แล้ว DoS ยังกล่าวถึงประเด็นต่างๆ ที่เกี่ยวข้องกับไซเบอร์ รวมถึงความมั่นคงแห่งชาติ ข้อพิจารณาทางเศรษฐกิจ สิทธิมนุษยชนและเสรีภาพทางอินเทอร์เน็ต สำนักงานผู้ประสานงานสำหรับปัญหาไซเบอร์ (Office of the Coordinator for Cyber Issues) ที่อยู่ภายใน DoS มีบทบาทสำคัญในการประสานงานกิจการที่เกี่ยวข้องกับไซเบอร์ ให้คำปรึกษาแก่เจ้าหน้าที่อาวุโสเกี่ยวกับปัญหาไซเบอร์ที่เกี่ยวข้อง และทำหน้าที่เป็นผู้ประสานงานที่สำคัญระหว่างกระทรวงต่างๆ ทำเนียบขาว หน่วยงานรัฐบาลกลางอื่นๆ และภาคเอกชน

3.3.2 องค์กรที่เกี่ยวข้องกับกรอบกฎหมายและข้อบังคับความมั่นคงทางไซเบอร์ (Cybersecurity Legal and Regulatory Frameworks agencies)

กระทรวงยุติธรรม (Department of Justice (DoJ)) มีบทบาทสำคัญในการสนับสนุนกฎหมายความมั่นคงทางไซเบอร์และต่อต้านภัยคุกคามทางไซเบอร์ภายในประเทศสหรัฐอเมริกา โดยมุ่งเน้นที่การสืบสวนและการดำเนินคดีกรณีบุกรุก รวบรวมข้อมูลที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ต่อรัฐชาติ และให้การสนับสนุนทางกฎหมายและนโยบายแก่หน่วยงานต่างๆ ของรัฐบาล ความรับผิดชอบของ DoJ ได้แก่ การดำเนินคดีกับอาชญากรรมในโลกไซเบอร์ การขัดขวางภัยคุกคามทางไซเบอร์ การเป็นผู้นำการปฏิบัติการด้านความมั่นคงแห่งชาติเพื่อต่อต้านข่าวกรองต่างประเทศหรือกิจกรรมทางไซเบอร์ของผู้ก่อการร้าย และการรวบรวม วิเคราะห์ และเผยแพร่ข้อมูลภัยคุกคามทางไซเบอร์ภายในประเทศ เพื่อให้มั่นใจถึงแนวทางการรักษาความมั่นคงทางไซเบอร์ที่ครอบคลุม แผนกความมั่นคงแห่งชาติของ DoJ (National Security Division of DoJ) ได้จัดตั้งเครือข่ายผู้เชี่ยวชาญด้านความมั่นคงทางไซเบอร์แห่งชาติทั่วประเทศโดยร่วมมือกับหน่วยงานอื่น ๆ โดยมีเป้าหมายเพื่อจัดการกับการบุกรุกและการโจมตีทางไซเบอร์ที่กระทำโดยรัฐประเทศหรือองค์กรก่อการร้าย นอกจากนี้ แผนกอาชญากรรมคอมพิวเตอร์และทรัพย์สินทางปัญญาของ DOJ (Computer Crime and Intellectual Property Section) ยังทำงานร่วมกับหน่วยงานภาครัฐ ภาคเอกชน สถาบันการศึกษา และพันธมิตรระหว่างประเทศ เพื่อป้องกันสอบสวน และดำเนินคดีกับอาชญากรรมคอมพิวเตอร์อย่างมีประสิทธิภาพ (CCDCOE, 2015)

พระราชบัญญัติความมั่นคงแห่งมาตุภูมิ ค.ศ. 2002 ได้จัดตั้งกระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) โดยมีหน้าที่ดูแลการปกป้องโครงสร้างพื้นฐานที่สำคัญ โดยเฉพาะอย่างยิ่งในภาคส่วนไอทีและการสื่อสาร ภายในคณะกรรมการป้องกันและคุ้มครองโครงการแห่งชาติ (NPPD) ที่อยู่ในการกำกับดูแลของ DHS มีหน่วยงานสำนักงานความปลอดภัยทางไซเบอร์และการสื่อสาร (Office of Cybersecurity and Communications (CS&C)) ในการจัดการศูนย์บูรณาการความปลอดภัยทางไซเบอร์และการสื่อสารแห่งชาติ (National Cybersecurity & Communications Integration Centre (NCCIC)) ซึ่งทำหน้าที่ประสานงานด้านความมั่นคงทางไซเบอร์ที่เกี่ยวข้องกับการป้องกันโครงสร้างพื้นฐานที่สำคัญ คณะกรรมการป้องกันและคุ้มครองโครงการแห่งชาติ (NPPD) มีหน้าที่หลักในภารกิจรักษาความมั่นคงทางไซเบอร์ที่ไม่ใช่การบังคับใช้กฎหมาย จะดูแล CS&C ในการจัดการภาวะวิกฤติการตอบสนองต่อเหตุการณ์ และความสามารถในการป้องกันสำหรับโครงสร้างพื้นฐานทางไซเบอร์และการสื่อสารของสหรัฐอเมริกาทั้งหมด นอกจากนี้ CS&C ยังรับผิดชอบในการดำเนินโครงการเสริมสร้างความมั่นคงการบริการทางไซเบอร์ (Enhanced Cybersecurity

Services programme) ซึ่งมีเป้าหมายเพื่อสนับสนุนความปลอดภัยทางไซเบอร์ในภาคส่วนต่างๆที่สำคัญ



ภาพประกอบ 17 แผนผังองค์กรสำนักงานความปลอดภัยทางไซเบอร์และการสื่อสาร (CS&C)
ที่มา: (CCDCOE, 2015)

ศูนย์บูรณาการความปลอดภัยทางไซเบอร์และการสื่อสารแห่งชาติ (NCCIC) ทำหน้าที่เป็นศูนย์กลางรวมศูนย์สำหรับการบูรณาการทางไซเบอร์และการสื่อสารในระดับชาติ อำนวยความสะดวกในการทำงานร่วมกันระหว่างหน่วยงานรัฐบาลกลาง ชุมชนข่าวกรอง และการบังคับใช้กฎหมาย เพื่อแสดงให้เห็นถึงการให้ความสำคัญของความร่วมมือและการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชน แม้ว่า NCCIC จะร่วมมืออย่างใกล้ชิดกับผู้ดูแลโครงการและผู้ดำเนินการโครงสร้างพื้นฐานที่สำคัญต่างๆ แต่ก็ขาดอำนาจในการบังคับใช้ข้อบังคับด้านความมั่นคงทางไซเบอร์ต่างๆในภาคเอกชน ภารกิจหลักของ NCCIC ประกอบด้วย การให้ความตระหนักในสถานการณ์ที่เกี่ยวข้องกับช่องโหว่ การบุกรุก เหตุการณ์ต่างๆ และการสนับสนุนความพยายามในการบรรเทาผลกระทบทางไซเบอร์และการกู้คืนข้อมูล NCCIC ดำเนินงานผ่านสี่สาขา ประกอบด้วย สาขาปฏิบัติการและการบูรณา

การ (NCCIC Operations and Integration (NO&I)), ทีมเตรียมความพร้อมในกรณีฉุกเฉินทางคอมพิวเตอร์ของสหรัฐอเมริกา (US Computer Emergency Readiness Team (US-CERT)), ทีมเตรียมความพร้อมในกรณีฉุกเฉินทางคอมพิวเตอร์ระดับอุตสาหกรรมของสหรัฐอเมริกา (Industrial US Computer Emergency Readiness Team, (ICS-CERT)) และศูนย์ประสานงานแห่งชาติเพื่อการสื่อสาร (National Coordinating Centre for Communications (NCC)) ทั้งหมดนี้มุ่งเป้าไปที่การประสานงานของหน่วยงานรัฐบาลกลางในการรักษาความปลอดภัยระบบและแก้ไขปัญหาความมั่นคงทางไซเบอร์ตามที่ได้รับคำสั่งจากพระราชบัญญัติความมั่นคงแห่งมาตุภูมิ ค.ศ. 2002 (Federal Information Security Management Act of 2002 (FISMA))

สาขาปฏิบัติการและการบูรณาการ (NCCIC Operations and Integration (NO&I)) มุ่งเน้นไปที่การพัฒนาแผนปฏิบัติการ โปรแกรมการฝึกอบรม และแบบฝึกหัดสำหรับศูนย์บูรณาการความมั่นคงทางไซเบอร์และการสื่อสารแห่งชาติ (National Cybersecurity & Communications Integration Centre (NCCIC)) NO&I กำกับดูแลการฝึกหัดทางไซเบอร์หลากหลายรูปแบบที่ดำเนินการทั้งในระดับชาติและระดับนานาชาติ ตลอดจนภายในภาคเอกชน ครอบคลุมการฝึกหัดขนาดเล็กไปจนถึงการจำลองตามปฏิบัติการขนาดใหญ่ NO&I มีบทบาทสำคัญในการรับรองการเตรียมพร้อมและการประสานงานสำหรับเหตุการณ์ทางไซเบอร์และเหตุฉุกเฉิน ส่งเสริมการทำงานร่วมกันระหว่างผู้มีส่วนได้ส่วนเสียและเพิ่มประสิทธิภาพการตอบสนองในภาคส่วนต่างๆ (CCDCOE, 2015)

US-CERT มีบทบาทสำคัญในการตอบสนองต่อเหตุการณ์ทางไซเบอร์ ให้ความช่วยเหลือด้านเทคนิคแก่ผู้ปฏิบัติงาน และเผยแพร่การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ในปัจจุบันและที่อาจเกิดขึ้นในอนาคต ทำหน้าที่เป็นแพลตฟอร์มการแบ่งปันข้อมูลที่สำคัญ โดยการกระจายข้อมูลที่เกี่ยวข้องไปยังหน่วยงานภาครัฐ ภาคเอกชน ตลอดจนองค์กรและพันธมิตรระหว่างประเทศ US-CERT อำนวยความสะดวกในการแลกเปลี่ยนข้อมูลผ่านช่องทางต่างๆ รวมถึงเว็บไซต์สำหรับการแบ่งปันข้อมูลที่เกี่ยวข้องกับไซเบอร์กับภาครัฐและเอกชน เปรียบเสมือนกับ Cyber Security Bulletin รายสัปดาห์ที่สรุปช่องโหว่ใหม่ในทุกสัปดาห์ นอกจากนี้ US-CERT เป็นหน่วยงานริเริ่มการทำงานร่วมกัน เช่น สภา CIO ของรัฐบาลกลาง (Federal CIO Council), ฟอรัมของรัฐบาลด้านการตอบสนองเหตุการณ์และทีมรักษาความปลอดภัย (Government Forum of Incident Response and Security Teams), สภาศูนย์วิเคราะห์การแบ่งปันข้อมูลแห่งชาติ (the National Council of Information Sharing Analysis Centres) และ แหล่งข้อมูลชุมชน Software Assurance และสำนักหักบัญชีข้อมูล (Software Assurance Community Resources and

Information Clearinghouse) ซึ่งส่งเสริมความร่วมมือและการประสานงานระหว่างรัฐบาล หน่วยงานเกี่ยวกับประเด็นความมั่นคงทางไซเบอร์

ICS-CERT มีบทบาทสำคัญในการเพิ่มความปลอดภัยของระบบการควบคุมอุตสาหกรรม (Industrial Control Systems (ICS)) และลดความเสี่ยงต่อโครงสร้างพื้นฐานที่สำคัญผ่านความร่วมมือกับภาครัฐและเอกชน ด้วยการมุ่งเน้นไปที่การรับรู้สถานการณ์ การตอบสนองต่อเหตุการณ์ การประสานงานเกี่ยวกับช่องโหว่ และการส่งเสริมความร่วมมือด้านความปลอดภัยทางไซเบอร์ ICS-CERT ทำงานเพื่อเสริมสร้างปลอดภัยของโครงสร้างพื้นฐานที่สำคัญต่อภัยคุกคามทางไซเบอร์ โดยช่วยเหลือทางด้านทรัพยากรที่หลากหลายแก่เจ้าของโครงสร้างพื้นฐานและผู้ปฏิบัติงานที่สำคัญ รวมถึงการแจ้งเตือน คำแนะนำ จดหมายข่าว และการรายงาน เพื่อเพิ่มความเข้าใจเกี่ยวกับภัยคุกคามและช่องโหว่ที่เกิดขึ้นใหม่ในระบบการควบคุมอุตสาหกรรม ซึ่งช่วยให้การจัดการความเสี่ยงและกลยุทธ์การบรรเทาผลกระทบมีประสิทธิภาพมากขึ้น

ศูนย์ประสานงานแห่งชาติ (National Coordinating Centre for Communications (NCC)) มีบทบาทสำคัญในการดูแลโครงสร้างพื้นฐานโทรคมนาคมและการซ่อมแซมหรือขยายบริการทุกด้าน ด้วยความร่วมมือเชิงกลยุทธ์กับหน่วยงานภาครัฐและภาคเอกชนทั้งในประเทศและต่างประเทศ และ มีเป้าหมายในการจัดการกับความท้าทายต่างๆ การส่งเสริมนวัตกรรม และการรับประกันมั่นคงและการเติบโตของเครือข่ายและบริการทางด้านโทรคมนาคม

3.3.3 องค์กรบัญชาการไซเบอร์ทางการทหาร (Military Cyber Commands agencies)

กระทรวงกลาโหม (Department of Defense (DoD)) มีหน้าที่ปกป้องโดเมน และโครงสร้างพื้นฐานข้อมูลระดับโลกของกระทรวงกลาโหมจากภัยคุกคามทางไซเบอร์ นอกเหนือจากการปกป้องทรัพย์สินเหล่านี้แล้ว กระทรวงกลาโหมยังมีหน้าที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ต่างประเทศ การรักษาความมั่นคงของชาติและระบบทหาร และตรวจสอบอาชญากรรมทางไซเบอร์ภายในเขตอำนาจศาลทหาร บทบาทที่หลากหลายนี้ตอกย้ำถึงบทบาทที่สำคัญของกระทรวงกลาโหมในการรักษาความปลอดภัยทางไซเบอร์ของเครือข่ายและโครงสร้างพื้นฐานทางทหาร ตลอดจนความพยายามในวงกว้างในการตอบโต้ภัยคุกคามทางไซเบอร์ต่อความมั่นคงของชาติ

กระทรวงกลาโหมปฏิบัติตามบทบาทและความรับผิดชอบในการปฏิบัติงานด้านความปลอดภัยทางไซเบอร์ผ่านหน่วยงานต่างๆ รวมถึง ศูนย์ปฏิบัติการกองบัญชาการไซเบอร์สหรัฐ (USCYBERCOM Joint Operations Center) สำนักงานความมั่นคงแห่งชาติ/

ศูนย์บริการความมั่นคงแห่งชาติ (National Security Agency/Central Security Service Center) ศูนย์กลาโหมอาชญากรรมไซเบอร์ (Defense Cyber Crime Center) และสำนักงานระบบสารสนเทศกลาโหม (Defense Information Systems Agency (DISA)) โดย DISA มีหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศและการสื่อสารแก่เครือข่ายทางการทหาร ตลอดจนปกป้องเครือข่ายเหล่านี้จากภัยคุกคามทางไซเบอร์ องค์กรเหล่านี้มีบทบาทสำคัญในการรับรองความปลอดภัยและความมั่นคงของโครงสร้างพื้นฐานและเครือข่ายข้อมูลของกระทรวง ซึ่งมีส่วนช่วยในการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยรวมของกองทัพสหรัฐฯ

การปฏิบัติการทางการทหารแต่ละแห่งภายในสหรัฐอเมริกา มีหน่วยงานทางไซเบอร์โดยเฉพาะ ที่ทำหน้าที่ดำเนินงานภายใต้อำนาจของศูนย์ปฏิบัติการกองบัญชาการไซเบอร์สหรัฐ US Cyber Command (USCYBERCOM) ซึ่งเป็นคำสั่งย่อยภายใต้ US Strategic Command (USSTRATCOM) USCYBERCOM ตั้งอยู่ในเมืองฟอร์ตมีด รัฐแมริแลนด์ มีสำนักงานใหญ่ร่วมกับสำนักงานความมั่นคงแห่งชาติ (NSA) ผู้อำนวยการ NSA ทำหน้าที่สองบทบาทในฐานะผู้บัญชาการ USCYBERCOM ซึ่งสะท้อนถึงความเชื่อมโยงระหว่างหน่วยข่าวกรองแห่งชาติและขีดความสามารถทางไซเบอร์ทางทหาร สิ่งนี้เน้นย้ำถึงความสำคัญเชิงกลยุทธ์ของการปฏิบัติการทางไซเบอร์ในการสงครามสมัยใหม่และความมั่นคงของชาติ

กองบัญชาการไซเบอร์ของสหรัฐฯ (USCYBERCOM) มีหน้าที่รับผิดชอบหลักในการสั่งการและการควบคุมการปฏิบัติงานในโลกไซเบอร์แบบรวมศูนย์ ซึ่งครอบคลุมการวางแผนและการดำเนินการ รวมถึงการเป็นผู้นำการป้องกันและการปกป้องเครือข่ายข้อมูลของกระทรวงกลาโหมในแต่ละวัน การประสานงานการปฏิบัติการของกระทรวงกลาโหมเพื่อสนับสนุนภารกิจทางทหาร การควบคุมการปฏิบัติการและการป้องกันเครือข่ายข้อมูลของกระทรวงกลาโหม และการเตรียมที่จะมีส่วนร่วมในการปฏิบัติการทางโลกไซเบอร์ทางทหารเต็มรูปแบบ การแบ่งแยกบทบาทนี้ตอกย้ำบทบาทสำคัญของ USCYBERCOM ในการปกป้องเครือข่ายกระทรวงกลาโหม และความพร้อมในการตอบสนองต่อภัยคุกคามทางไซเบอร์ในทุกขอบเขตของความขัดแย้ง

กองบัญชาการไซเบอร์สหรัฐ (USCYBERCOM) ได้ระบุลำดับความสำคัญสำคัญ 5 ประการเพื่อเป็นแนวทางในการปฏิบัติงานและความคิดริเริ่มต่างๆ ลำดับความสำคัญเหล่านี้ประกอบด้วย การสร้างกองกำลังไซเบอร์ที่ได้รับการฝึกฝนและการเตรียมความพร้อม การใช้เครื่องมือเพื่อให้บรรลุการรับรู้สถานการณ์ที่ครอบคลุมในโลกไซเบอร์ การพัฒนาแนวคิดการบังคับบัญชาและการควบคุมและการปฏิบัติงานเพื่อปฏิบัติภารกิจอย่างมีประสิทธิภาพ การสร้างเครือข่ายป้องกันร่วมกันเพื่อเพิ่มความมั่นคงทางไซเบอร์ และการสร้างความมั่นใจว่า

คำสั่งต่างๆที่ได้รับมอบหมาย มีนโยบายและอำนาจที่จำเป็นในการดำเนินการเต็มรูปแบบในโลกไซเบอร์ ด้วยการมุ่งเน้นไปที่ลำดับความสำคัญเหล่านี้ USCYBERCOM มีเป้าหมายที่จะเพิ่มขีดความสามารถ เสริมสร้างการป้องกันทางไซเบอร์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพในสถานการณ์ต่างๆ

ค.ศ. 2016 กระทรวงกลาโหม (DoD) มีเป้าหมายที่จะจัดตั้งกองกำลังภารกิจไซเบอร์ (Cyber Mission Force (CMF)) ประกอบด้วยบุคลากรทางทหาร และพลเรือน กว่า 6,000 นายที่มาจากหน่วยงานทหารและองค์กรที่เกี่ยวกับด้านการป้องกันต่างๆ CMF จะถูกจัดเป็นทีมสี่ประเภท ประกอบด้วย ทีมงานภารกิจระดับชาติที่ได้รับมอบหมายให้ตอบสนองต่อการโจมตีทางไซเบอร์ที่สำคัญที่ส่งผลกระทบต่อประเทศ, ทีมป้องกันทางไซเบอร์ที่รับผิดชอบในการปกป้องเครือข่ายที่สำคัญของกระทรวงและสนับสนุนปฏิบัติการทางทหารทั่วโลก, ทีมงานภารกิจการต่อสู้ที่ช่วยเหลือแผนปฏิบัติการและการปฏิบัติการฉุกเฉิน และทีมสนับสนุนที่ให้ความช่วยเหลือด้านการวิเคราะห์และการวางแผน โดย 27 ทีมภารกิจการรบจะให้การสนับสนุนคำสั่งการรบต่างๆ เช่น กองบัญชาการกลางสหรัฐ กองบัญชาการแปซิฟิก และกองบัญชาการยุโรป นอกจากนี้ แผนยังรวมถึงการพัฒนาระยะการทดลองไซเบอร์ภายในประเทศเพื่อจำลองการดำเนินงานทางโลกไซเบอร์ และอำนวยความสะดวกในการทดสอบเทคโนโลยีและความสามารถใหม่ๆ

ศูนย์ปฏิบัติการร่วม (Joint Operations Centre) ที่เมืองฟอร์ตมีด มีผู้บัญชาการหน่วยรบที่ดูแล ศูนย์บัญชาการรบร่วมไซเบอร์สเปซ (Combatant Command Joint Cyberspace Centre) ได้รับการสนับสนุนจาก USCYBERCOM รวมถึงการจัดตั้งศูนย์ปฏิบัติการเครือข่ายและศูนย์รักษาความปลอดภัยระหว่างปฏิบัติการ กองบัญชาการไซเบอร์ของกองทัพบกสหรัฐฯ (US Army Cyber Command (ARCYBER)) ได้รับมอบหมายให้พัฒนากำลังเพื่อสนับสนุนหน่วยบัญชาการรบและกระทรวงกลาโหม (DoD) และขยายขีดความสามารถทางโลกไซเบอร์ไปยังทหารระดับชั้นที่ต่ำที่สุดของกองทัพบก กองทัพอากาศที่ 24 (The 24th Air Force (AFCYBER)) บรรลุขีดความสามารถในการปฏิบัติการอย่างเต็มรูปแบบใน ค.ศ. 2010 โดยมีภารกิจในการปฏิบัติการขยาย และปกป้องเครือข่าย ปกป้องระบบภารกิจหลัก และสร้างขีดความสามารถทางโลกไซเบอร์แบบเต็มรูปแบบ AFCYBER ดำเนินการปฏิบัติการทางโลกไซเบอร์ตลอด 24 ชั่วโมง โดยมีกำลังรบซึ่งประกอบด้วยกำลังประจำการ 5,400 นาย และกำลังพลสำรอง 11,000 นาย

เอกสารข้อมูลร่วมประจำ ค.ศ. 2013 (The 2013 Joint Information Environment White Paper) สรุปกลยุทธ์ในการรวมศูนย์ข้อมูลทั่วทั้งหน่วยงานทางการทหารเพื่อให้แน่ใจว่าผู้นำจะเข้าถึงข้อมูลที่แม่นยำที่สุด นอกจากนี้ มีการเสนอการเปลี่ยน

ศูนย์ข้อมูลเป็นระบบคลาวด์เพื่อเพิ่มการแบ่งปันข้อมูลและความคล่องตัวภายในกองทัพสหรัฐฯ แผนนี้มีจุดมุ่งหมายเพื่อปรับปรุงกระบวนการจัดการข้อมูล ปรับปรุงการเข้าถึงข้อมูลที่สำคัญ และส่งเสริมความร่วมมือที่มากขึ้นระหว่างหน่วยทหาร ซึ่งจะช่วยเพิ่มประสิทธิภาพการปฏิบัติงานและความสามารถในการตัดสินใจของกองทัพ (CCDCOE, 2015)

3.3.4 องค์กรหน่วยข่าวกรองไซเบอร์ (Cyber intelligence agencies)

องค์กรหน่วยข่าวกรองสหรัฐ นำโดยผู้อำนวยการหน่วยข่าวกรองแห่งชาติ (Director of National Intelligence (DNI)) มีบทบาทสำคัญในความมั่นคงทางไซเบอร์ เนื่องจากมีการไหลเวียนของข้อมูลที่กว้างขวางทั่วทั้งโครงสร้างพื้นฐานด้านไอทีทั่วโลก สำนักงานผู้อำนวยการข่าวกรองแห่งชาติประสานงานหน่วยงานและองค์กร 17 แห่ง ซึ่งหลายแห่งอยู่ภายใต้เขตอำนาจของกระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) และกระทรวงกลาโหม (DoD) แม้ว่า DNI จะกำหนดเป้าหมายสำหรับองค์กรหน่วยข่าวกรองแต่ก็ขาดการควบคุมโดยตรงต่อบุคลากรของหน่วยงาน สำนักงานความมั่นคงแห่งชาติ (NSA) ทำหน้าที่เป็นหน่วยงานหลักด้านความปลอดภัยทางไซเบอร์ในภาคความมั่นคงแห่งชาติ โดยมีผู้อำนวยการ รวมถึงผู้บัญชาการกองบัญชาการไซเบอร์ของสหรัฐฯ และหน่วยรักษาความปลอดภัยส่วนกลาง ซึ่งรายงานตรงต่อ DNI NSA มีหน้าที่ส่งสัญญาณข่าวกรองไปยังส่วนต่างๆ ของกระทรวงกลาโหม สำนักงานสืบสวนกลางแห่งสหรัฐอเมริกา (FBI) ซึ่งเป็นส่วนหนึ่งของโครงการริเริ่มการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบครอบคลุม (Comprehensive National Cybersecurity Initiative (CNCI)) และดูแลหน่วยงานเฉพาะกิจร่วมสืบสวนทางไซเบอร์แห่งชาติ (National Cyber Investigative Joint Task Force (NCIJTF)) โดยประสานงานจากหน่วยงานรัฐบาลกลาง 19 แห่งเพื่อคาดการณ์และป้องกันการโจมตีทางไซเบอร์ โดยรวมแล้ว องค์กรหน่วยข่าวกรองสหรัฐมีหน้าที่รับผิดชอบในการจัดหาและรักษาความปลอดภัยเทคโนโลยีข่าวกรองสำหรับกองทัพ เพื่อให้มั่นใจว่ามาตรการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพเพื่อปกป้องผลประโยชน์แห่งชาติ (CCDCOE, 2015)

สรุป

มนุษย์ คือผู้สร้างโลกไซเบอร์ และเป็นกำลังหลักในการส่งเสริมความก้าวหน้าทางไซเบอร์ให้กับประเทศนั้นๆ ประเทศสหรัฐอเมริกากำหนดนโยบายในการสร้างแรงงาน และการศึกษาไซเบอร์แห่งชาติ เพื่อให้ประชากรสามารถเป็นแรงงานที่มีประสิทธิภาพ ได้รายได้ที่ได้ และสวัสดิการที่รองรับความต้องการ บุคลากรและแรงงานไซเบอร์ เป็นแรงงานที่ขาดแคลน และไม่เพียงพอต่อการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว ณ ปัจจุบัน ดังนั้น ประเทศสหรัฐอเมริกาจึงกำหนดแผนกลยุทธ์

ที่ดึงดูดให้ประชากรเข้ามาเป็นส่วนหนึ่งของการเพิ่มแรงงานและการศึกษาไซเบอร์ เพื่อให้เพียงพอต่อความต้องการของประเทศ

แผนการดำเนินงานในการสร้างแรงงานไซเบอร์ เป็นสิ่งสำคัญในการกำหนดทิศทางในการขับเคลื่อนและพัฒนาองค์ความรู้ทางไซเบอร์ และการสร้างความร่วมมือภาคแรงงานระหว่างประเทศพันธมิตร ถือเป็นอีกหนึ่งปัจจัยเช่นกันในการสร้างระบบนิเวศไซเบอร์ที่ดี ไม่ว่าจะเป็นในแง่ของการพัฒนาทางเทคโนโลยีและวิทยาศาสตร์ หรือการสร้างสิ่งแวดล้อมทางวิชาการของเหล่านักวิชาการ ที่สามารถเข้ามาช่วยกันร่วมพัฒนาองค์ความรู้ทางไซเบอร์อย่างเป็นเอกภาพ

การก่อตั้งสถาบันเพื่อรองรับในการใช้เป็นสถานที่ในการพัฒนาองค์ความรู้ไซเบอร์ เป็นสิ่งที่จำเป็นในการสร้างและพัฒนาองค์ความรู้ใหม่ให้กับประเทศ รวมถึงการสร้างศูนย์กลางที่ใช้ในการทำงานร่วมกันระหว่างรัฐบาลกลาง และภาคเอกชน ที่ส่งเสริมการแบ่งปันข้อมูลระหว่างกัน รวมถึงการก่อตั้งหน่วยงานทางการทหาร และหน่วยข่าวกรองไซเบอร์ เพื่อใช้ในสถานการณ์ฉุกเฉินและการดำเนินการทางการทหารต่างๆด้วยเช่นกัน

บทที่ 6
ผลกระทบจากความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกาต่อความสัมพันธ์ระหว่างประเทศ

ความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่มีบทบาทสำคัญต่อความมั่นคงทางไซเบอร์และการเป็นส่วนสำคัญของโครงสร้างพื้นฐานของโลกไซเบอร์ ทำให้ประเทศสหรัฐอเมริกามีความเป็นศูนย์กลางของโลกไซเบอร์และมีความสามารถในการกำหนดทิศทางนโยบายที่เกี่ยวข้องกับไซเบอร์ในเวทีระหว่างประเทศ และการกำหนดมาตรฐานความมั่นคงทางไซเบอร์เพื่อสร้างความปลอดภัยจากภัยคุกคาม และความเป็นผู้นำทางด้านการสร้างนโยบายที่สร้างผลกระทบต่อรัฐอื่นๆ

งานวิจัยชิ้นนี้ใช้การวิเคราะห์ผลกระทบจากการเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกาต่อความสัมพันธ์ระหว่างประเทศโดยการใช้กรอบแนวคิดสัจนิยมใหม่ (Neorealism) แนวคิดสมองของโลก (Global Brain) และ การวิเคราะห์อำนาจทางไซเบอร์ (Cyber Power) โดยใช้กรณีศึกษาจากนโยบายต่างประเทศที่สร้างผลกระทบต่อความสัมพันธ์ระหว่างประเทศ สงครามไซเบอร์ การใช้เทคโนโลยีเพื่อควบคุมข้อมูล และบทบาทของประเทศสหรัฐอเมริกาในการสร้างความร่วมมือไซเบอร์ระหว่างประเทศ การบังคับใช้นโยบายที่เกี่ยวข้องกับไซเบอร์ของประเทศสหรัฐอเมริกา สร้างผลกระทบต่อความสัมพันธ์ระหว่างประเทศ โดยแบ่งผลกระทบที่เกิดขึ้น ดังนี้

ผลกระทบความมั่นคงทางไซเบอร์ต่อการแข่งขันทางเทคโนโลยี หมายถึง การที่ประเทศสหรัฐอเมริกาได้พัฒนานโยบายต่างๆเพื่อเข้าควบคุมและสร้างเสถียรภาพต่อการเป็นผู้นำทางไซเบอร์ ไม่ว่าจะเป็น การแข่งขันเทคโนโลยีไซเบอร์กับประเทศจีนและรัสเซีย เช่น เทคโนโลยี 5G และเครือข่ายโทรคมนาคม ในการออกนโยบายกีดกันอุปกรณ์อิเล็กทรอนิกส์ Huawei และการออกนโยบายส่งเสริมการสร้างผู้ผลิตภายในประเทศตนเอง การแข่งขันการสร้างปัญญาประดิษฐ์ (AI) และ IoT (Internet of Things) ที่กำลังกลายเป็นสนามรบใหม่ของสงครามไซเบอร์ในการใช้ประโยชน์เพื่อสร้างความมั่นคงทางไซเบอร์ รวมถึง สงครามข้อมูล (Information Warfare) ที่เป็นการแข่งขันการใช้ข้อมูลเพื่อสร้างความได้เปรียบทางด้านการเมือง

DeNardis (2020) ได้อธิบายถึงกฎหมาย CLOUD Act (Clarifying Lawful Overseas Use of Data Act) ของประเทศสหรัฐอเมริกา ซึ่งเป็นกฎหมายที่มีผลกระทบต่อความเป็นส่วนตัวของข้อมูล และมีจุดมุ่งหมายเพื่อสร้างความร่วมมือระหว่างประเทศกับบริษัทเอกชนในการบังคับใช้กฎหมาย โดยกฎหมายนี้ได้เริ่มใช้ในเดือนมีนาคม ค.ศ. 2018 เพื่อใช้ในการแก้ไขปัญหาความขัดแย้งของข้อกฎหมายในการเข้าถึงข้อมูลที่ถูกจัดเก็บไว้ในเซิร์ฟเวอร์ในอยู่ในต่างประเทศ โดยกฎหมายนี้ ได้

สร้างการขยายอำนาจของประเทศสหรัฐอเมริกาในแง่ของการบังคับใช้กฎหมายในการเข้าถึงข้อมูลในต่างประเทศ ซึ่งกฎหมายนี้อนุญาตให้หน่วยงานของรัฐของประเทศสหรัฐอเมริกาสามารถตรวจสอบข้อมูลผู้ใช้ของบริษัทเอกชนจากการบังคับให้บริษัทเหล่านั้นส่งมอบข้อมูลต่างๆมาให้กับหน่วยงานของรัฐ ไม่ว่าจะเป็น บริษัท Microsoft Google Apple ไม่ว่าเซิร์ฟเวอร์ที่ทำหน้าที่เก็บข้อมูล จะตั้งอยู่ที่ประเทศใดในโลกก็ตาม อีกทั้งกฎหมาย CLOUD Act สามารถใช้ในการสร้างข้อตกลงพิเศษกับรัฐบาลอื่นๆได้ เพื่อการอนุญาตให้เข้าถึงข้อมูลระหว่างกันและกัน ทำให้ประเทศสหรัฐอเมริกาสามารถเข้าถึงข้อมูลระหว่างประเทศได้รวดเร็วมากยิ่งขึ้น

บทบาทของกฎหมาย CLOUD Act ได้สร้างอิทธิพลทางด้านข้อมูลให้กับประเทศสหรัฐอเมริกา และทำให้มีอำนาจทางข้อมูลทั่วโลก แต่การสร้างอิทธิพลทางข้อมูลนี้ ได้ขัดกับความเป็นอธิปไตยของข้อมูล (Data Sovereignty) ที่สหภาพยุโรป (EU) ให้ความสำคัญเป็นอย่างมาก เนื่องจากสหภาพยุโรป มีการบังคับใช้กฎเกณฑ์การปกป้องข้อมูลทั่วไป (General Data Protection Regulation (GDPR)) โดยเป็นการกำหนดให้บริษัทต่างๆต้องให้ความสำคัญกับการรักษาข้อมูลส่วนตัวของผู้ใช้งานและจัดเก็บให้ปลอดภัย แต่กฎหมาย CLOUD Act ของประเทศสหรัฐอเมริกา เป็นการอนุญาตให้รัฐบาลเข้าแทรกแซงข้อมูลของผู้ใช้ได้ตามกฎหมาย และไม่จำกัดขอบเขตระหว่างประเทศด้วยเช่นกัน ทำให้เกิดข้อกังวลถึงการละเมิดสิทธิส่วนบุคคล และการเข้าถึงข้อมูลต่างๆโดยไม่ได้รับอนุญาตจากผู้ใช้งาน ส่งผลกระทบก่อให้เกิดการต่อต้านกฎหมาย CLOUD Act จากหลากหลายประเทศ และเริ่มมีการบังคับให้บริษัทต่างๆเก็บข้อมูลไว้ภายในประเทศเท่านั้น เพื่อลดอิทธิพลทางข้อมูลของประเทศสหรัฐอเมริกา (DeNardis, 2020)

การออกกฎหมายเป็นเพียงส่วนหนึ่งของการสร้างผลกระทบต่อความสัมพันธ์ระหว่างประเทศ การสร้างพันธมิตรระหว่างประเทศ เป็นอีกกลไกหนึ่งที่ช่วยเสริมสร้างอิทธิพลของประเทศสหรัฐอเมริกา โดยประเทศสหรัฐอเมริกามีกลุ่มพันธมิตร Five Eyes Alliance ซึ่งเป็นกลุ่มพันธมิตรทางข้อมูลข่าวกรองที่ถูกจัดตั้งขึ้นตั้งแต่สมัยสงครามโลกครั้งที่ 2 ร่วมกับประเทศสหราชอาณาจักร (United Kingdom) ซึ่งปัจจุบัน กลุ่มพันธมิตร Five Eyes มีสมาชิกทั้งหมด 5 ประเทศ ประกอบด้วย สหรัฐอเมริกา สหราชอาณาจักร แคนาดา (เข้าร่วมใน ค.ศ. 1948) ออสเตรเลีย และนิวซีแลนด์ (เข้าร่วมใน ค.ศ. 1956) ซึ่งองค์ประกอบสำคัญของกลุ่มพันธมิตรคือข้อมูลข่าวกรองทางด้านไซเบอร์ที่เกี่ยวข้องกับความมั่นคงของโครงสร้างพื้นฐานและการป้องกันภัยคุกคามจากรัฐอื่นๆและกลุ่มก่อการร้าย

ถึงแม้ว่ากลุ่มพันธมิตร Five Eyes Alliance จะมีความสัมพันธ์ที่ดีมาโดยตลอด แต่ข้อจำกัดในการแบ่งปันข่าวกรอง ก็เป็นอุปสรรคในการทำงานร่วมกัน เนื่องจากความกังวลในเรื่องต่างๆ เช่น ผลประโยชน์แห่งชาติ ข้อมูลลับเฉพาะของประเทศ และความเชื่อใจของหน่วยงาน อาทิเช่น เหตุการณ์ที่ประเทศสหรัฐอเมริกาและออสเตรเลีย มีข้อขัดแย้งในเรื่องการแบน Huawei ต่อความ

มั่นคงทางไซเบอร์ ถึงแม้ว่าจะมีข้อขัดแย้งระหว่างกันบ้างในบางเหตุการณ์ แต่กลุ่มพันธมิตร Five Eyes ก็ยังได้มีการขยายอำนาจการแบ่งปันข้อมูลไปยังประเทศอื่นๆด้วยเช่นกัน เช่น ประเทศฝรั่งเศส เยอรมนี และญี่ปุ่น แต่การขยายอำนาจนี้ เป็นเพียงการขยายอำนาจในบางขอบเขตของข้อมูล และจำกัดการแบ่งข้อมูลในบางส่วนด้วยเช่นกัน เนื่องจากปัญหาในความเชื่อมั่นของความสัมพันธ์ระหว่างประเทศ และผลกระทบจากการสร้างกลุ่มพันธมิตรนี้ ทำให้ประเทศจีนและรัสเซีย ได้มีการพัฒนาองค์ความรู้ทางเทคโนโลยีเพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นได้ ทำให้กลุ่มพันธมิตร Five Eyes Alliance มีความจำเป็นในการพัฒนากลยุทธ์ทางด้านความร่วมมือทางไซเบอร์มากยิ่งขึ้น (Pijovic, 2021)

ความร่วมมือของประเทศพันธมิตรของกลุ่ม Five Eyes Alliance ได้สร้างความตึงเครียดในความสัมพันธ์ระหว่างประเทศจากกรณีร่วมกันแบน Huawei และ ZTE โดยประเทศสหรัฐอเมริกาและพันธมิตรมีความกังวลต่อ Huawei และ ZTE ว่าอาจมีความสัมพันธ์กับรัฐบาลจีนและกองทัพจีน และอาจถูกใช้ในการสอดแนมและสร้างการโจมตีทางไซเบอร์ ทำให้ประเทศสหรัฐอเมริกาได้ออกคำสั่งห้ามใช้เทคโนโลยีที่มาจาก Huawei และ ZTE ในโครงสร้างพื้นฐาน 5G ของประเทศสหรัฐอเมริกา และได้กดดันประเทศพันธมิตร Five Eyes Alliance เช่น ประเทศอังกฤษ ออสเตรเลีย และแคนาดา ในการงดใช้สินค้าและเทคโนโลยีจาก Huawei และมีความกลัวว่า หากประเทศจีนได้เข้าควบคุมโครงสร้างโทรคมนาคมของโลก อาจก่อให้เกิดผลกระทบต่อความมั่นคงและความเป็นอิสระของโครงสร้างพื้นฐานทางไซเบอร์ของประเทศอื่นๆด้วยเช่นกัน

ประเทศสหรัฐอเมริกาได้ออกมาตรการต่างๆเพื่อต่อต้าน Huawei และ ZTE ไม่ว่าจะเป็นการออกคำสั่งให้กระทรวงพาณิชย์สหรัฐอเมริกา เพิ่ม Huawei และบริษัทที่เกี่ยวข้อง เข้าไปอยู่ในบัญชีเฉพาะ (Entity List) หมายถึง การที่บริษัทเอกชนของสหรัฐอเมริกาไม่สามารถทำธุรกิจร่วมกับ Huawei ได้หากไม่ได้รับการอนุญาตจากภาครัฐ รวมถึงการสั่งให้ Google งดให้การบริการซอฟต์แวร์ Android กับ Huawei ทำให้ Huawei จำเป็นต้องพึ่งพาระบบปฏิบัติการของตัวเองที่มีชื่อว่า HarmonyOS แต่ประสิทธิภาพก็ยังไม่สามารถเทียบเคียง Google ได้อย่างสมบูรณ์ ส่งผลกระทบให้ประเทศจีนจำเป็นต้องพึ่งพาเทคโนโลยีของตัวเองมากยิ่งขึ้น และยังส่งผลในแง่ของความสัมพันธ์ทางเศรษฐกิจและการทูตระหว่างประเทศที่มีความตึงเครียดมากยิ่งขึ้นด้วยเช่นกัน (Segal, 2020)

ปัญหาที่ส่งผลกระทบต่อทางด้านเศรษฐกิจจากความเป็นมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกาอีกหนึ่งเหตุการณ์ คือ การบังคับใช้กฎหมาย CHIPS and Science Act ที่เป็นกฎหมายในการสนับสนุนอุตสาหกรรมเซมิคอนดักเตอร์ของประเทศสหรัฐอเมริกา ซึ่งมีเป้าหมายในการบังคับใช้กฎหมายอยู่ 2 ประเด็น คือ

1. เพื่อกระตุ้นการผลิตเซมิคอนดักเตอร์ภายในประเทศตนเอง ซึ่งเป็นการให้งบในการสนับสนุนบริษัทที่ผลิตเซมิคอนดักเตอร์ในประเทศสหรัฐอเมริกา มากกว่า 52,000 ล้านดอลลาร์ จุดประสงค์คือความต้องการผลักดันในการขยายโรงงานผลิตภายในประเทศ รวมถึงการสนับสนุนการ

ลดหย่อนภาษีและให้งบสำหรับการทำวิจัยเพื่อคิดค้นและพัฒนาเทคโนโลยีชิปให้มีประสิทธิภาพขั้นสูงสุด โดยต้องการให้ภาคเอกชนในประเทศ พึ่งพาการใช้งานชิปภายในประเทศและลดการพึ่งพาการนำเข้าจากภายนอกประเทศ

2. เพื่อจำกัดการพัฒนาเทคโนโลยีของประเทศจีน ส่งผลกระทบต่อการออกข้อกำหนดจากกฎหมายข้อนี้ ในการห้ามให้บริษัทต่างๆที่ได้รับเงินสนับสนุนจากทางรัฐบาลของสหรัฐอเมริกา ลงทุนในอุตสาหกรรมเซมิคอนดักเตอร์ของประเทศจีนเป็นระยะเวลาทั้งหมด 10 ปี และประเทศสหรัฐอเมริกาได้บังคับใช้มาตรการในการเข้าควบคุมการส่งออกเพื่อจำกัดการเข้าถึงเทคโนโลยีของประเทศ เช่น ชิป AI และ อุปกรณ์ในการผลิตชิปขั้นสูง ทำให้กระทบต่อบริษัทของจีน เช่น Huawei และ SMIC อีกทั้งยังประสานขอความร่วมมือจากประเทศพันธมิตรต่างๆ เช่น ประเทศญี่ปุ่น เนเธอร์แลนด์ และเกาหลีใต้ ในการจำกัดการส่งออกอุปกรณ์การผลิตเซมิคอนดักเตอร์ไปยังประเทศจีนด้วยเช่นกัน

การออกกฎหมายที่เป็นการเอื้อประโยชน์ต่อประเทศสหรัฐอเมริกาและกีดกันการพัฒนาทางเทคโนโลยีต่อประเทศจีนนี้ ได้สร้างผลกระทบต่อความสัมพันธ์ระหว่างประเทศโดยตรง เพราะนอกจากทำให้เกิดความขัดแย้งกับประเทศจีนแล้วนั้น ก็ได้เกิดข้อโต้แย้งจากประเทศพันธมิตรต่อกระบวนการห่วงโซ่อุปทานทางเทคโนโลยีระหว่างประเทศ โดยเฉพาะบริษัทที่อยู่ในประเทศพันธมิตรต่างๆ ไม่ว่าจะเป็นภายในประเทศไต้หวัน และเกาหลีใต้ ที่ต้องปรับตัวจากนโยบายของประเทศสหรัฐอเมริกา รวมถึงความเสี่ยงที่เป็นการกดดันทำให้เกิดการแข่งขันที่ทวีความรุนแรงมากยิ่งขึ้น ทำให้อาจก่อให้เกิดสงครามเทคโนโลยีภายในอนาคต (Rasser, 2022)

ผลกระทบความมั่นคงทางไซเบอร์ต่อประเทศพันธมิตรและศัตรู หมายถึง ความขัดแย้งที่ได้รับผลจากนโยบายและกฎหมายทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่นอกจากจะเป็นการสร้างผลกระทบต่อประเทศที่ตนเองแล้วนั้น ยังส่งผลต่อประเทศพันธมิตรของประเทศสหรัฐอเมริกาด้วยเช่นกัน โดยผลกระทบที่เกิดขึ้นแบ่งออกได้เป็น 3 ประเด็น (Kaska et al., 2019) ดังนี้

ผลกระทบทางด้านความมั่นคง หมายถึง ประเทศพันธมิตรของประเทศสหรัฐอเมริกา ได้รับผลกระทบจากการที่ประเทศสหรัฐอเมริกามองว่า Huawei คือภัยคุกคามทางไซเบอร์และสามารถส่งผลต่อโครงสร้างพื้นฐานสำคัญที่เชื่อมโยงต่อโลกไซเบอร์ ดังนั้น ประเทศพันธมิตรจึงถูกกดดันทางด้านการดำเนินนโยบายให้สอดคล้องกับแนวทางของประเทศสหรัฐอเมริกา และให้หันไปใช้เทคโนโลยีของอุปกรณ์ต่างๆจากแบรนด์ Huawei เป็นแบรนด์จากชาติตะวันตก เช่น แบรนด์ Ericsson (ประเทศสวีเดน) และ Nokia (ประเทศฟินแลนด์) และการปฏิบัติตามนโยบายการลดการพึ่งพาจากประเทศจีน ส่งผลกระทบให้หลากหลายประเทศพันธมิตรจำเป็นต้องลงทุนเพิ่มเติมด้วยงบประมาณของประเทศตนเอง

ผลกระทบทางด้านเศรษฐกิจและเทคโนโลยี หมายถึง ประเทศพันธมิตรของสหรัฐอเมริกาต้องเผชิญกับค่าใช้จ่ายของต้นทุนที่มากขึ้น เนื่องจาก Huawei เป็นหนึ่งในบริษัทเทคโนโลยีที่มีต้นทุนที่ถูกในการใช้เทคโนโลยีเข้ามาปรับใช้กับโครงสร้างพื้นฐาน สร้างความได้เปรียบสำหรับประเทศที่ต้องการพัฒนาโครงสร้างพื้นฐานในระบบดิจิทัล เช่น การพัฒนาระบบเครือข่าย 5G และอาจส่งผลให้การขยายเครือข่ายมีความล่าช้ากว่าประเทศที่เป็นพันธมิตรกับประเทศจีน และผลกระทบที่หลากหลายประเทศพันธมิตรของสหรัฐอเมริกาต้องเผชิญ คือ ความสัมพันธ์ทางเศรษฐกิจกับประเทศจีน เพราะการให้ความร่วมมือกับประเทศสหรัฐอเมริกาในการแบน Huawei อาจส่งผลต่อกระบวนการทำงาน การลงทุน และการค้าระหว่างประเทศกับประเทศจีน

ผลกระทบทางด้านภูมิรัฐศาสตร์ หมายถึง ผลกระทบที่เกิดขึ้นจากนโยบายของประเทศสหรัฐอเมริกา ก่อให้เกิดการแบ่งขั้วอำนาจระหว่างประเทศสหรัฐอเมริกา และประเทศจีน ความขัดแย้งทางด้านการแบน Huawei ได้ส่งผลให้ประเทศต่างๆจำเป็นต้องเลือกขั้วอำนาจระหว่างสองประเทศมหาอำนาจนี้ และในขณะที่ประเทศสหรัฐอเมริกาได้ดำเนินนโยบายการแบน Huawei ประเทศจีนได้เริ่มสร้างพันธมิตรจากความพยายามในการเผยแพร่อิทธิพลของตนเองผ่านโครงการต่างๆ อาทิเช่น โครงการ Belt and Road Initiative (BRI) ที่เป็นโครงการพัฒนาโครงสร้างพื้นฐานและการลงทุนในระดับโลกของประเทศจีน มีเป้าหมายในการสร้างการเชื่อมโยงกันระหว่างทวีปเอเชีย แอฟริกา และยุโรป ผ่านโครงสร้างพื้นฐานที่เกี่ยวข้องกับคมนาคม การค้า และพลังงาน ซึ่งส่งผลให้ประเทศต่างๆจำเป็นต้องเข้าร่วมกับการลงทุนของประเทศจีน และทำให้ประเทศจีนมีอิทธิพลทางเศรษฐกิจมากยิ่งขึ้น (Belt and Road Portal, 2024)

ผลกระทบทางไซเบอร์จากการบังคับใช้นโยบายของประเทศสหรัฐอเมริกาต่อความเป็นอธิปไตยของโลกไซเบอร์ในความสัมพันธ์ระหว่างประเทศ หมายถึง การบังคับใช้นโยบายไซเบอร์ สร้างผลกระทบต่อความเป็นอนาธิปไตยของโลกไซเบอร์ (Cyber Sovereignty) ที่แนวคิดและหลักการใช้โลกไซเบอร์ของแต่ละประเทศ มีความแตกต่างกัน โดยสามารถแบ่งหลักการใช้โลกไซเบอร์ได้ตามแนวคิด ดังต่อไปนี้

กลุ่มประเทศแนวคิดเสรีนิยม หมายถึง ประเทศที่ใช้แนวคิดเสรีนิยมในการใช้โลกไซเบอร์ โดยเป็นประเทศที่สนับสนุนการใช้โลกไซเบอร์แบบเปิดกว้าง (Open Internet) ไม่ว่าจะเป็นการให้เสรีภาพต่อประชาชนในการเข้าถึงข้อมูลของรัฐ การมีเสรีภาพในการแสดงความคิดเห็นในโลกอินเทอร์เน็ต และการปกครองที่ให้ความสำคัญจากการร่วมมือทั้งจากภาครัฐ ภาคเอกชน และภาคประชาชนในการร่วมกันกำหนดกฎเกณฑ์ในการใช้งานโลกไซเบอร์ เป็นกลุ่มประเทศที่มีแนวคิดต้องการลดการควบคุมจากภาครัฐ สามารถต่อต้านการจำกัดการใช้งานในประเด็นต่างๆที่ภาครัฐต้องการเข้าควบคุมหรือเซ็นเซอร์ได้ และเพิ่มการใช้งานอินเตอร์เน็ตให้สามารถเข้าถึงได้ในระดับสากล ประกอบด้วย ประเทศสหรัฐอเมริกา และประเทศสมาชิกกลุ่มสหภาพยุโรป

กลุ่มประเทศแนวคิดที่สนับสนุนความเป็นอธิปไตย์ทางไซเบอร์ หมายถึง ประเทศที่ให้ความสำคัญแก่การรักษาอำนาจอธิปไตยของประเทศตนเอง รวมถึงการรักษาอำนาจอธิปไตยของโลกไซเบอร์ ซึ่งเป็นกลุ่มประเทศที่มีความต้องการในการควบคุมการใช้งานโลกอินเทอร์เน็ต และสร้างสิทธิของรัฐบาลในการเข้าตรวจสอบข้อมูลต่างๆในโลกไซเบอร์ แนวคิดของกลุ่มประเทศเหล่านี้มองว่า โลกไซเบอร์ คือพื้นที่ที่ต้องถูกควบคุมและสอดส่องโดยภาครัฐ ความมั่นคงของรัฐและความปลอดภัยของข้อมูลคือสิ่งที่สำคัญมากกว่าสิทธิส่วนบุคคลของประชาชน เป็นการควบคุมเพื่อรักษาเสถียรภาพทางการเมืองของประเทศ อาทิเช่น ประเทศจีน รัสเซีย และประเทศที่ปกครองโดยระบอบเผด็จการต่างๆ (Segal, 2018)

สรุป

การวิเคราะห์ผลกระทบจากความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่ส่งผลต่อความสัมพันธ์ระหว่างประเทศสะท้อนให้เห็นถึงบทบาทสำคัญของประเทศสหรัฐอเมริกาในแง่ของความมั่นคงและอำนาจทางไซเบอร์ที่ใช้นโยบายต่างๆในการสร้างอิทธิพลให้กับประเทศตนเอง ไม่ว่าจะเป็นในด้านการแข่งขันทางด้านเทคโนโลยี การสร้างความมั่นคงร่วมกับประเทศพันธมิตร และการกำหนดนโยบายไซเบอร์ในระดับนานาชาติ การใช้นโยบายเพื่อกีดกันและกำจัดการมีส่วนร่วมของประเทศจีนภายในประเทศตนเอง อาทิเช่น การแบน Huawei และ ZTE ไปจนถึงการบังคับใช้กฎหมาย CLOUD Act และ CHIPS and Science Art ที่มีเป้าหมายในการเข้าควบคุมข้อมูลและการสนับสนุนให้มีการผลิตเซมิคอนดักเตอร์ภายในประเทศตนเอง ซึ่งนโยบายที่กล่าวมาก่อให้เกิดการแข่งขันทางด้านไซเบอร์มีการทวีความรุนแรงมากยิ่งขึ้น ทำให้ประเทศจีนมีการตอบโต้นโยบายดังกล่าวด้วยการเร่งพัฒนาเทคโนโลยีของประเทศตนเอง รวมถึงความพยายามในการสร้างอิทธิพลทางการเมืองระหว่างประเทศด้วยการสร้างโครงการ Belt and Road Initiative ก่อให้เกิดการแบ่งขั้วทางการเมืองระหว่างประเทศ ประกอบด้วย กลุ่มประเทศที่สนับสนุนแนวคิดเสรีที่นำโดยประเทศสหรัฐอเมริกา และประเทศพันธมิตร และกลุ่มประเทศที่สนับสนุนการมีอำนาจอธิปไตยในโลกไซเบอร์ของตนเอง เช่น ประเทศจีน และรัสเซีย แต่การดำเนินนโยบายต่างประเทศของประเทศสหรัฐอเมริกาก็ได้ส่งผลกระทบต่อประเทศพันธมิตรด้วยเช่นกัน ไม่ว่าจะเป็นการปรับตัวทางด้านเศรษฐกิจที่มีต้นทุนที่สูงมากขึ้นจากการดำเนินนโยบายตามที่ประเทศสหรัฐอเมริกาต้องการ ผลกระทบทางความสัมพันธ์ระหว่างประเทศที่เกิดจากการดำเนินนโยบายของประเทศสหรัฐอเมริกาแสดงให้เห็นถึงความพยายามในการรักษาดุลแห่งอำนาจของประเทศของตนเอง แต่ในขณะเดียวกัน ก็ได้สร้างผลกระทบให้กับความสัมพันธ์ระหว่างประเทศ ทั้งกลุ่มประเทศพันธมิตรที่ต้องปรับตัว และกลุ่มประเทศศัตรู ที่มีการแข่งขันทางเทคโนโลยีและความพยายามในการเผยแพร่อิทธิพล

บทที่ 7
สรุปผล อภิปรายผล และข้อเสนอแนะ

การวิจัยเรื่อง ความมั่นคงทางไซเบอร์กับความท้าทายของประเทศมหาอำนาจ: สหรัฐอเมริกาในศตวรรษที่ 21 ผู้วิจัยสามารถสรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ ตามลำดับดังต่อไปนี้

1. ความมุ่งหมายของการวิจัย
2. สรุปผล
3. อภิปรายผล
4. ข้อเสนอแนะ

1. ความมุ่งหมายของการวิจัย

การวิจัยครั้งนี้ ผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัย ดังนี้

1.1 เพื่อวิเคราะห์ความเป็นอนาธิปไตยในโลกไซเบอร์ที่ท้าทายอำนาจของประเทศสหรัฐอเมริกา

1.2 เพื่อวิเคราะห์บทบาทของไซเบอร์ที่ส่งผลต่อการสร้างความเป็นมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา

1.3 เพื่อวิเคราะห์ผลกระทบที่เกิดขึ้นของความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่ส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ และสมดุลแห่งอำนาจในการเมืองระหว่างประเทศ

2. สรุปผล

2.1 ความเป็นอนาธิปไตยในโลกไซเบอร์ที่ท้าทายอำนาจของประเทศสหรัฐอเมริกา

ความเป็นอนาธิปไตยในโลกไซเบอร์ คือ พื้นที่ที่ไม่มีมนุษย์อาศัยอยู่ แต่เป็นโลกที่มีการไหลเวียนของข้อมูลต่างๆที่เกิดขึ้นจากมนุษย์ และผลลัพธ์ที่เกิดขึ้นจากกระบวนการระหว่างโลกไซเบอร์ และ โลกทางกายภาพ คือ สิ่งสำคัญที่ทำให้เกิดผลกระทบจากโลกไซเบอร์ สู่โลกทางกายภาพ

โลกไซเบอร์ เกิดจากการสร้างของมนุษย์ และการเพิ่มขึ้นของการใช้งานในพื้นที่ของโลกไซเบอร์ ทำให้ความซับซ้อนของโลกไซเบอร์มีมากกว่าการแลกเปลี่ยนข้อมูล ซึ่งสำหรับตัวแสดงที่เป็นรัฐแล้วนั้น โลกไซเบอร์ คือ พื้นที่ในการสร้างความมั่นคงให้กับประชากรในประเทศ และเป็นพื้นที่ในการสร้างผลประโยชน์แห่งชาติด้วยเช่นกัน

ประเทศสหรัฐอเมริกา มีอำนาจทางด้านต่างๆเป็นพื้นฐาน ไม่ว่าจะเป็นอำนาจทางการทหาร เศรษฐกิจ และวิทยาศาสตร์ และการมีบทบาทสำคัญของการเป็นผู้พัฒนาและสร้างนวัตกรรมเทคโนโลยีโลกไซเบอร์ ทำให้ประเทศสหรัฐอเมริกาเป็นประเทศมหาอำนาจทางไซเบอร์

อย่างไรก็ตาม อำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ถูกท้าทายจากโลกไซเบอร์เนื่องจากความเป็นอนาธิปไตยที่ไร้พรมแดน ทำให้ประเทศสหรัฐอเมริกาไม่สามารถควบคุมการใช้งานอินเทอร์เน็ตทั่วทั้งโลกได้อย่างสมบูรณ์ อีกทั้งภัยคุกคามที่สามารถเกิดขึ้นได้จากทุกมุมโลก ทุกเวลา ไม่ว่าจะเป็นการแฮ็ก ที่สามารถเกิดจากตัวแสดงหลากหลายรูปแบบ ไม่ว่าจะเป็นกลุ่มก่อการร้ายข้ามชาติ กลุ่มอาชญากรทางไซเบอร์ กลุ่มนักเคลื่อนไหวทางการเมือง กลุ่มแฮ็กเกอร์มือสมัครเล่น รวมถึงตัวแสดงที่ถูกสนับสนุนโดยรัฐบาล

ความท้าทายที่เกิดขึ้น นอกจากเป็นผลกระทบทางด้านไซเบอร์ที่อยู่ในลำดับชั้นตรรกะแล้วนั้น ความท้าทายทางกายภาพของโลกไซเบอร์ของประเทศสหรัฐอเมริกาก็ได้รับผลกระทบเช่นกัน ขอบเขตของตำแหน่งที่ตั้งของสายเคเบิ้ลใต้ทะเลที่ยากที่จะควบคุมอย่างทั่วถึงและตลอดเวลา ส่งผลให้ประเทศที่มุ่งร้ายสามารถเข้าถึงและทำการโจมตี หรือการเชื่อมสายเคเบิ้ลเพื่อรวบรวมข้อมูลทางไซเบอร์ของประเทศสหรัฐอเมริกา และปัญหาที่เกิดจากปัจจัยภายนอก อาทิเช่น การทอดสมอเรือ การขุดลอด และภัยพิบัติทางธรรมชาติ ที่สามารถสร้างผลกระทบต่อสายเคเบิ้ลใต้ทะเล ทำให้เกิดความเสียหายได้เช่นกัน

ความท้าทายจากความเป็นอนาธิปไตยของโลกไซเบอร์ และความเป็นมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ได้ก่อให้เกิดสภาวะกลืนไม่เข้าคายไม่ออกทางด้านความมั่นคงทางไซเบอร์ในระดับนานาชาติ เนื่องจากพัฒนาการทางเทคโนโลยีของประเทศสหรัฐอเมริกาที่มีความล้ำหน้ามากกว่าประเทศอื่นๆ ซึ่งถึงแม้ว่าจะเป็นการพัฒนาโดยเพื่อการป้องกันภัยคุกคามเป็นหลัก แต่กลับเป็นสิ่งที่ทำให้ประเทศอื่นๆจำเป็นต้องเร่งพัฒนาเทคโนโลยีทางไซเบอร์ของตนเองมากยิ่งขึ้น อีกทั้งในทศวรรษที่ 21 รูปแบบการปกครองแบบเสรีนิยมประชาธิปไตย ที่ได้ถูกท้าทายด้วยการปกครองแบบสังคมนิยมคอมมิวนิสต์ อาทิเช่น ประเทศจีน เป็นประเทศที่มีประชากรจำนวนมาก ได้มีการสร้างองค์กรไซเบอร์ที่ใช้สำหรับทางการทหารอย่างเด่นชัด และสามารถเรียกได้ว่า เป็นกองทัพไซเบอร์ เพราะมีกำลังพลโดยรวมมากกว่า 45,000 คน (Hjortdal, 2011) และความเกรี้ยวกราดของประเทศรัสเซีย ที่ได้ทำการโจมตีทางไซเบอร์อย่างต่อเนื่อง ไม่ว่าจะเป็นการใช้ประเทศจอร์เจีย เปรียบเสมือนการทดสอบการโจมตีทางไซเบอร์ไปยัง สถาบันทางการเงิน ข้อมูลของภาครัฐ และอินเทอร์เน็ตภายในประเทศและ ก่อให้เกิดความพยายามในการถ่วงดุลทางอำนาจของประเทศที่มีแนวทางที่ตรงกันข้ามกับความเป็นประเทศเสรีนิยมประชาธิปไตย อาทิเช่น ประเทศจีน รัสเซีย และประเทศอิหร่าน

การเชื่อมต่อของข้อมูลในโลกไซเบอร์ ได้ท้าทายประเทศสหรัฐอเมริกาในแง่ของการเข้าถึงข้อมูลอย่างรวดเร็ว และประชาชนให้ความสนใจกับสื่อกระแสหลักน้อยลง มีทางเลือกในการรับฟังข้อมูลโดยไม่จำเป็นต้องพึ่งพารัฐบาล หรือบริษัทที่ทำหน้าที่เป็นสื่อต่างๆเหมือนในอดีต การเพิ่มขึ้นของช่องทางที่เผยแพร่ข้อมูล ทำให้เกิดความขัดแย้งระหว่างสื่อมีเดียต่างๆ ส่งผลให้การควบคุมข้อมูลของรัฐบาลมีประสิทธิภาพลดลง และการเพิ่มขึ้นของข้อมูลในโลกไซเบอร์ ที่มีจำนวนมหาศาลและยากที่จะควบคุม กลายเป็นสิ่งที่รัฐบาลต้องเผชิญในศตวรรษที่ 21

การไร้พรมแดนของอนาธิปไตยในโลกไซเบอร์ ได้สร้างอำนาจให้กับกลุ่มประเทศที่มีความต้องการใช้ไซเบอร์ทางการทหาร สามารถเข้ามามีบทบาทในโลกไซเบอร์ได้ด้วยเช่นกัน อาทิเช่น ประเทศเกาหลีเหนือ จีน รัสเซีย จอร์เจีย ลิทัวเนีย อิหร่าน และอื่นๆ ที่ทำให้ความพยายามในการสร้างอำนาจของประเทศสหรัฐอเมริกาในโลกใบนี้ มีความท้าทาย และด้วยการไร้พรมแดนนี้เอง ทำให้แนวคิดทางด้านความไม่สมมาตรทางด้านความก้าวหน้าทางเทคโนโลยีของประเทศสหรัฐอเมริกา ได้ถูกท้าทายจากการโจมตีทางไซเบอร์ของประเทศที่กำลังพัฒนา

ถึงแม้ว่ารัฐบาลสหรัฐอเมริกาจะเผชิญกับความท้าทายหลากหลายรูปแบบ แต่ด้วยความเป็นมหาอำนาจทางไซเบอร์ ทำให้ประเทศสหรัฐอเมริกามีรากฐานที่มั่นคงกว่าประเทศอื่นๆ อีกทั้งจากการวิเคราะห์ทำให้เห็นได้ถึงความพยายามในการเป็นสมองของโลก (Global Brain) ของประเทศสหรัฐอเมริกา ที่มีภาคเอกชนคอยสนับสนุนในการสร้างระบบนิเวศทางไซเบอร์ในระดับนานาชาติ อาทิเช่น Google Apple Facebook(Meta) Amazon Microsoft และการดำเนินนโยบายที่ทำให้บริษัทเหล่านี้ เปรียบเสมือนระบบประสาทของประเทศสหรัฐอเมริกา ที่สามารถรับรู้ข้อมูลและสั่งการได้จากการดำเนินนโยบายทางกฎหมายต่างๆ ไม่ว่าจะเป็น CLOUD Act และการบังคับใช้มาตรการ CHIPS and Science Act ของประเทศสหรัฐอเมริกา ในการกีดกันประเทศศัตรูเพื่อลดความสามารถในการพัฒนาเทคโนโลยีและทำให้ประเทศตนเองได้เปรียบนานาประเทศ

2.2 บทบาทของไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติ และความมั่นคงทางการทหารของประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกา มีศักยภาพในหลากหลายมิติ ที่ได้เปรียบประเทศมหาอำนาจอื่นๆ ไม่ว่าจะเป็นมิติทางด้านอำนาจทางการทหาร อำนาจทางเทคโนโลยี และอำนาจทางวิทยาศาสตร์ ที่มีผลพวงจากการขึ้นเป็นประเทศมหาอำนาจหลังสงครามโลกครั้งที่ 2 และการมีความสัมพันธ์อันดีระหว่างประเทศที่มีระบอบการปกครองแบบเสรีนิยมประชาธิปไตย และความร่วมมือของประเทศพันธมิตรทางด้านนโยบายไซเบอร์ระหว่างประเทศ

อำนาจไซเบอร์ได้รับประโยชน์จากการที่ประเทศสหรัฐอเมริกา มีอำนาจต่างๆด้วยเช่นกัน ไม่ว่าจะเป็นผลประโยชน์จากอำนาจทางการทหาร ที่ทำให้ประเทศสหรัฐอเมริกา มีความมั่นคง

ทางการเมืองอย่างยาวนาน ลักษณะความเป็นรัฐบาลที่ปกครองด้วยระบอบเสรีนิยมประชาธิปไตย คุณลักษณะของผู้นำประเทศที่ให้ความสำคัญกับการพัฒนาไซเบอร์ จุดประสงค์ทางการทหารที่ส่งเสริมในการใช้งานไซเบอร์ทางการทหาร อำนาจทางการทหารในพื้นที่การรบต่างๆ ไม่ว่าจะเป็นบนบก ในทะเล ในอากาศ ในอวกาศ และโลกไซเบอร์ ที่มีการเชื่อมโยงในการส่งเสริมการสร้างอำนาจไซเบอร์ให้ถูกใช้งานได้อย่างมีประสิทธิภาพ

การปกครองที่มีความมั่นคงทางการเมืองอย่างยาวนาน ส่งผลให้การพัฒนาทางเทคโนโลยีมีความต่อเนื่องมาหลายทศวรรษ และการปรับใช้เทคโนโลยีการสื่อสารตั้งแต่สมัยสงครามโลกครั้งที่ 1 จนถึงปัจจุบัน ทำให้ประเทศสหรัฐอเมริกามีความก้าวหน้าเป็นอย่างสูงในการสร้างองค์ความรู้ที่เข้าใจถึงการใช้งานเทคโนโลยีเหล่านี้ได้อย่างมีประสิทธิภาพ และการพัฒนาเทคโนโลยีจากหลายภาคส่วน ไม่ว่าจะเป็นภาครัฐ ภาคเอกชน และสังคม ที่มีอิสระทางด้านความคิดในการประยุกต์และสร้างนวัตกรรมใหม่ๆที่ส่งเสริมอำนาจไซเบอร์ให้กับประเทศสหรัฐอเมริกา การส่งเสริมการใช้งานอินเทอร์เน็ตจากภาครัฐ ที่ต้องการให้ประชากรได้รับการเข้าถึงอินเทอร์เน็ตอย่างทั่วถึงและปลอดภัย และการครอบครองเทคโนโลยีทางกายภาพต่างๆจากภาครัฐ และภาคเอกชน ที่ส่งผลต่อการใช้งานโลกไซเบอร์ในระดับนานาชาติ ไม่ว่าจะเป็นการครอบครองสายเคเบิ้ลโทรคมนาคมใต้ทะเล และการครอบครองเราท์เตอร์หลักที่ใช้ในการรวบรวมข้อมูลของโลกไซเบอร์ และข้อได้เปรียบทางด้านการเป็นผู้นำของประเทศสหรัฐอเมริกา ที่ได้สร้างบรรทัดฐานทางสังคมในระดับโลก ในการเข้าถึงข้อมูลได้ทั่วโลก และเป็นผู้วางโครงสร้างเทคโนโลยีให้กับโลกใบนี้ด้วยเช่นกัน ซึ่งการมีอำนาจในการควบคุมข้อมูล คือปัจจัยสำคัญในการกำหนดทิศทางข้อมูลในระดับโลก ที่สามารถสร้างผลประโยชน์ให้กับประเทศสหรัฐอเมริกาในการสื่อสารข้อมูลต่างๆออกไปยังนานาประเทศ

ปัจจัยสำคัญของการสร้างอำนาจไซเบอร์ คือการสร้างจากความรู้ความเข้าใจของประชากรในประเทศนั้นๆที่มีต่อโลกไซเบอร์ มนุษย์ คือ ผู้สร้างโลกไซเบอร์ และในขณะเดียวกัน มนุษย์ คือ ผู้ใช้งานโลกไซเบอร์ ทั้งในแง่ประโยชน์ส่วนตัว ประโยชน์ส่วนรวม และการใช้งานเพื่อการโจมตีต่างๆด้วยเช่นกัน ประเทศสหรัฐอเมริกาได้กำหนดแผนการพัฒนาบุคลากรและประชาชนให้มีทักษะและความรู้เรื่องโลกไซเบอร์ เพื่อเป็นประโยชน์ทั้งทางด้านแรงงาน และการศึกษาโลกไซเบอร์ด้วยเช่นกัน การสร้างแรงงานไซเบอร์ เปรียบเสมือนการปฏิรูปองค์ความรู้ทางด้านไซเบอร์ ให้มีการพัฒนาองค์ความรู้อย่างต่อเนื่อง และเป็นการเตรียมพร้อมเพื่อพัฒนาปัญญาประดิษฐ์ ในการสร้างความได้เปรียบทางด้านเทคโนโลยีอย่างต่อเนื่อง ประเทศสหรัฐอเมริกามีการกำหนดแผนกลยุทธ์ในการสร้างแรงงานไซเบอร์ที่ชัดเจน และการสร้างสิ่งแวดล้อมทางปัญญาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ ด้วยการให้พื้นที่ต่อการถกเถียงในประเด็นทางด้านไซเบอร์ของเหล่านักวิชาการต่างๆในหลากหลายประเด็น ไม่ว่าจะเป็นประเด็นทางด้านขอบเขตอำนาจทางไซเบอร์ ธรรมาภิ

บาลในโลกไซเบอร์ ผลกระทบของอำนาจทางไซเบอร์และประชาธิปไตย และอื่นๆ ทำให้องค์ความรู้ที่เกิดจากการถกเถียงทางไซเบอร์เหล่านี้ สามารถนำไปต่อยอดให้เกิดประโยชน์ต่อความมั่นคงไซเบอร์ได้ด้วยเช่นกัน

นวัตกรรมที่เกิดขึ้นจากการถกเถียงทางวิชาการ นำมาสู่การก่อตั้งสถาบันต่างๆที่มีความเกี่ยวข้องกับโลกไซเบอร์ เพื่อใช้ในการศึกษาและพัฒนาองค์ความรู้ต่างๆ ซึ่งไม่เพียงแต่เป็นการศึกษาเพื่อพัฒนาการทางด้านเครือข่ายโทรคมนาคมเพียงเท่านั้น แต่เป็นการศึกษาไปยังการสร้างความมั่นคงทางด้านการเงิน การขนส่งพลังงานของโครงสร้างพื้นฐานที่สำคัญ และการเตรียมพร้อมต่อสถานการณ์ฉุกเฉินต่างๆที่สามารถเกิดขึ้นจากผลกระทบทางไซเบอร์

รัฐบาลกลางและสภามีส่วนร่วมในการสร้างความร่วมมือของคณะกรรมาธิการทางด้านการคุ้มครองโครงสร้างพื้นฐานสำคัญ ร่วมกับภาคเอกชน และการก่อตั้งคณะทำงานที่ให้ความสำคัญต่อการปกป้องโครงสร้างพื้นฐาน รวมถึงการทำงานร่วมกันกับสำนักงานสืบสวนกลางสหรัฐอเมริกาและสำนักงานความมั่นคงแห่งชาติ ในการกำกับดูแลความมั่นคงทางไซเบอร์ของประเทศ และความปลอดภัยต่างๆ อีกทั้งการร่วมมือของกระทรวงต่างประเทศ ที่ทำหน้าที่ในการรับผิดชอบความมั่นคงทางไซเบอร์ ในประเด็นทางด้านสิทธิมนุษยชน และเสรีภาพทางอินเทอร์เน็ตด้วยเช่นกัน และกระทรวงยุติธรรม ที่มีบทบาทในการสนับสนุนกฎหมายความมั่นคงทางไซเบอร์และการต่อต้านภัยคุกคามทางไซเบอร์ ซึ่งเป็นการสร้างบรรทัดฐานให้กับสังคมในการกำหนดขอบเขตการใช้ไซเบอร์อย่างถูกต้อง และการขัดขวางการคุกคามทางไซเบอร์ต่างๆที่สามารถเกิดขึ้นได้ในอนาคต และกระทรวงกลาโหม มีหน้าที่หลักในการปกป้องโดเมน และโครงสร้างพื้นฐานข้อมูลระดับโลก จากภัยคุกคามทางไซเบอร์จากภายนอกประเทศ รวมถึงการรวบรวมข้อมูลต่างๆเพื่อการรักษาความมั่นคงของชาติและการทำงานของกองทัพ เพื่อการเตรียมพร้อมในการรับมือต่อภัยคุกคามต่างๆได้อย่างรวดเร็วและมีประสิทธิภาพ และองค์กรหน่วยข่าวกรองสหรัฐ ที่มีหน้าที่ในการรวบรวม และวิเคราะห์ข้อมูลที่ไหลเวียนในโลกไซเบอร์ทั่วโลก เพื่อการรักษาความปลอดภัยและความมั่นคงต่อประเทศสหรัฐอเมริกา

โลกไซเบอร์ถูกบรรจุอยู่ในขอบเขตความมั่นคงของประเทศสหรัฐอเมริกา และการระบุถึงการเชื่อมโยงของโครงสร้างพื้นฐานของประเทศที่เป็นระบบดิจิทัล ในการใช้ในรูปแบบโทรคมนาคม เศรษฐกิจ และสังคม ทำให้ประเทศสหรัฐอเมริกามีการวางวิสัยทัศน์และดำเนินนโยบายไซเบอร์ที่เกี่ยวข้องกับความมั่นคงแห่งชาติไว้อย่างชัดเจน ทั้งประโยชน์ทางด้านการเมือง เศรษฐกิจ และสังคม ที่ประชาชนจำเป็นต้องได้รับความมั่นคงขั้นพื้นฐานในการใช้ชีวิตในประเทศสหรัฐอเมริกา และสิ่งแวดล้อมทางไซเบอร์ควรมีความปลอดภัยสำหรับการใช้งานทั้งภาครัฐ ภาคเอกชน และภาคประชาชน รวมถึงการให้ความสำคัญของผู้นำประเทศสหรัฐอเมริกา ที่มีส่วนร่วมในการกำหนดทิศทางการพัฒนาความมั่นคงทางไซเบอร์ของประเทศ ไม่ว่าจะเป็นการพัฒนาความมั่นคง

ทางไซเบอร์ ณ ปัจจุบัน และการต่อยอดเทคโนโลยีปัญญาประดิษฐ์ที่จะเป็นส่วนสำคัญในการขับเคลื่อนประเทศ อีกทั้งการให้ความสำคัญต่อการปกป้องความมั่นคงทางไซเบอร์จากตัวแสดงต่างๆที่มีพฤติกรรมมุ่งร้ายต่อประเทศ ทำให้ประเทศสหรัฐอเมริกาเป็นประเทศที่มีการเตรียมพร้อมสำหรับการเป็นประเทศมหาอำนาจทางไซเบอร์ทั้งปัจจัยทางด้านการเมืองในประเทศและระหว่างประเทศ (Domestic and International Politics) และลักษณะความเป็นรัฐบาล (Government Characteristic) อย่างสมบูรณ์แบบ

ประสิทธิภาพทางการเมืองของประเทศสหรัฐอเมริกา ส่งเสริมให้อำนาจทางการทหารของกองทัพมีความเป็นผู้นำในระดับระหว่างประเทศ ควบคู่ไปกับการใช้แผนความมั่นคงทางไซเบอร์ที่เป็นแผนการสร้างความมั่นคงเชิงรับ ซึ่งมีบทบาทสำคัญในการทำให้ประเทศสหรัฐอเมริกามีเสถียรภาพทางไซเบอร์ในการปกป้องโครงสร้างพื้นฐานที่สำคัญ การจำกัดการเข้าถึงโลกไซเบอร์ของตัวแสดงที่เป็นภัยต่อประเทศ การกำหนดทิศทางเศรษฐกิจในการขับเคลื่อนพัฒนาการเพื่อสร้างความมั่นคงทางไซเบอร์ การลงทุนเพื่อความมั่นคงทางไซเบอร์ และการสร้างความสัมพันธ์อันดีระหว่างประเทศเพื่อสร้างการพึ่งพาทางดิจิทัลให้กลายเป็นเครือข่ายที่มีความความมั่นคงทางไซเบอร์ที่มั่นคงร่วมกันระหว่างประเทศพันธมิตร

ความเป็นผู้นำทางการทหารของประเทศสหรัฐอเมริกา ไม่ว่าจะเป็นอำนาจทางบก อำนาจในทะเล อำนาจในอากาศ และอำนาจในอวกาศ แสดงให้เห็นถึงการเป็นผู้นำทางการทหารอย่างเห็นได้ชัด ในขณะเดียวกัน ความเป็นผู้นำทางการทหารก็ได้ถูกท้าทายจากการเปลี่ยนผ่านการทำสงครามด้วยเทคโนโลยี อาทิเช่น การยิงขีปนาวุธทางไกล สงครามอิเล็กทรอนิกส์ การโจมตีด้วยโดรน สงครามข้อมูล นวัตกรรมเทคโนโลยีที่ใช้ร่วมกับเรือรบ เรือดำน้ำ เครื่องบินรบ และเทคโนโลยีอวกาศ รวมถึงสงครามไซเบอร์ จำเป็นต้องพึ่งพาการใช้งานไซเบอร์อย่างหลีกเลี่ยงไม่ได้ รวมถึงความเป็นอนาธิปไตยของโลกไซเบอร์ ที่ไร้พรมแดน และไม่สามารถควบคุมได้ จึงทำให้ความเป็นมหาอำนาจของประเทศสหรัฐอเมริกา กำลังถูกท้าทายในศตวรรษที่ 21

2.3 ผลกระทบที่เกิดขึ้นของความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่ส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ

พฤติกรรมของประเทศสหรัฐอเมริกาในความเป็นประเทศมหาอำนาจทางไซเบอร์ สอดคล้องกับทฤษฎีสัจนิยมใหม่ของ Kenneth Waltz ในการให้ความสำคัญกับการดำเนินการเรื่องนโยบายระหว่างประเทศ การกระจายอำนาจผ่านนโยบายระหว่างประเทศ และการสร้างอำนาจในความเป็นอนาธิปไตย ซึ่งไม่เพียงแต่เป็นการสร้างอำนาจความเป็นอนาธิปไตยในการเมืองระหว่างประเทศเท่านั้น แต่เป็นการสร้างอำนาจอนาธิปไตยในโลกไซเบอร์ด้วยเช่นกัน ซึ่งสามารถใช้การวิเคราะห์เชิงระบบ (systemic approach) ผ่านรูปแบบทั้ง 3 ระดับได้ดังนี้

1. ระดับปัจเจกบุคคล (individual) บทบาทของผู้นำประเทศของประเทศสหรัฐอเมริกา ที่ให้ความสำคัญกับการดำเนินการนโยบายทางด้านไซเบอร์มาอย่างต่อเนื่อง และการส่งเสริมนโยบายทางด้านการพัฒนาความมั่นคงของโครงสร้างพื้นฐานที่เป็นการพึ่งพาโลกไซเบอร์ รวมถึงการส่งเสริมทางด้านนโยบายแรงงาน ที่ให้ความสำคัญในการผลิตแรงงานที่มีความเชี่ยวชาญในโลกไซเบอร์มากยิ่งขึ้นในทศวรรษที่ 21

2. ระดับระบบการเมือง (political system) การปกครองแบบเสรีนิยมประชาธิปไตย การสนับสนุนสิทธิเสรีภาพ และสิทธิมนุษยชน การส่งเสริมสิทธิในการเข้าถึงข้อมูลต่างๆ มีอิสระในการค้นคว้านวัตกรรมใหม่ๆ ที่ต่อยอดให้การพัฒนาทางด้านวิทยาศาสตร์ของประเทศมีความก้าวหน้าอย่างต่อเนื่อง ความโปร่งใสในการปกครองของรัฐ และการดำเนินนโยบายในการส่งเสริมให้ประชากรได้เข้าถึงอินเทอร์เน็ตได้อย่างทั่วถึง และมีความปลอดภัยในการทำกิจกรรมต่างๆในโลกไซเบอร์ ทำให้ประเทศสหรัฐอเมริกามีเสถียรภาพในการพัฒนาองค์ความรู้ทางด้านไซเบอร์ได้อย่างมีประสิทธิภาพในทศวรรษที่ 21

3. ระดับระบบการเมืองระหว่างประเทศ (international system) การปกครองแบบเสรีนิยม ได้รับอิทธิพลนับตั้งแต่การสิ้นสุดสงครามโลกครั้งที่สอง ทำให้อิทธิพลการปกครองแบบเสรีนิยมเป็นที่รู้จักและแพร่ขยายไปยังนานาประเทศ การดำเนินการต่างๆของประเทศมหาอำนาจอย่างประเทศสหรัฐอเมริกา จึงเป็นการดำเนินการด้วยความชอบธรรมอย่างหลีกเลี่ยงไม่ได้ และการดำเนินการเหล่านี้ นำมาซึ่งการสร้างผลประโยชน์แห่งชาติให้กับประเทศสหรัฐอเมริกาด้วยเช่นกัน ไม่ว่าจะเป็นในแง่ของผลประโยชน์ทางด้านเศรษฐกิจ หรือการทหาร และความสามารถในการกีดกันประเทศมหาอำนาจอื่นๆที่กำเนิดขึ้นในทวีปต่างๆ จากการสร้างพันธมิตรกับประเทศอื่นๆเพื่อประสิทธิภาพในการตอบโต้และการคงไว้ซึ่งอำนาจในการเมืองระหว่างประเทศ

ประเทศสหรัฐอเมริกา มีการขับเคลื่อนประเทศจากบทบาทที่ประเทศสหรัฐอเมริกาได้มีอิทธิพลมานับตั้งแต่หลังสงครามโลกครั้งที่ 2 ในการกำหนดขอบเขตและทิศทางต่างๆให้กับนานาชาติ รวมถึงการเป็นตัวกลางในการแก้ไขปัญหาทางการเมืองระหว่างประเทศแบบเสรีนิยม การสนับสนุนแนวคิดกฎระเบียบแบบเสรีนิยม และลักษณะของความเป็นรัฐบาล ที่สนับสนุนสิทธิเสรีภาพ ประชาธิปไตย และสิทธิมนุษยชน ส่งเสริมให้การดำเนินการทางการทหารของประเทศสหรัฐอเมริกา มีความชอบธรรมในปฏิบัติการทางการทหารต่างๆ ไม่ว่าจะเป็นการพยายามกีดกันการกำเนิดของประเทศมหาอำนาจใหม่ในแถบทวีปยูเรเซีย ทั้งการเข้าร่วมสงคราม และการสร้างพันธมิตรเพื่อควบคุมและสร้างอำนาจในแถบทวีปเอเชีย รวมถึงการก่อตั้งองค์กรความมั่นคงต่างๆ เพื่อการตอบโต้ที่รวดเร็ว และการดำเนินการทางการทูต ที่ใช้นโยบายทางการเมืองระหว่าง

ประเทศในการสร้างพันธมิตรและการเจรจาต่างๆเพื่อผลประโยชน์แห่งชาติและอำนาจของประเทศสหรัฐอเมริกา

ถึงแม้ว่าประเทศสหรัฐอเมริกาจะได้เปรียบในหลากหลายทางจากการสร้างผลประโยชน์โดยใช้ไซเบอร์ แต่การแบ่งขั้วทางอำนาจการเมืองระหว่างประเทศ คือสิ่งที่ได้รับผลกระทบจากการเป็นมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา การสร้างความขัดแย้งในเชิงภูมิรัฐศาสตร์ระหว่างประเทศสหรัฐอเมริกาและจีนจากการใช้นโยบายในการแบน Huawei และ ZTE โดยใช้เหตุผลการแบนว่าเป็นการปกป้องความมั่นคงทางไซเบอร์ และยังส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศสหรัฐอเมริกาและประเทศพันธมิตร ที่จำเป็นต้องปฏิบัติตามนโยบายของประเทศสหรัฐอเมริกา ไม่ว่าจะเป็นกลุ่มประเทศสหภาพยุโรป ออสเตรเลีย ไต้หวัน แคนาดา ทำให้ประเทศพันธมิตรเหล่านี้เกิดความตึงเครียดกับจีน และต้องแสดงจุดยืนทางไซเบอร์อย่างระมัดระวัง

นโยบายไซเบอร์ของประเทศสหรัฐอเมริกาได้สร้างอิทธิพลต่อความเป็นมหาอำนาจทางไซเบอร์ และได้ขยายอำนาจออกไปทั่วโลกจากการใช้กฎหมาย CLOUD Act จากการมีสิทธิเรียกร้องข้อมูลจากบริษัทเอกชนที่มีอิทธิพลต่อโลกไซเบอร์ อาทิเช่น Google Facebook(Meta) Microsoft และ Apple ที่มีที่ตั้งในแต่ละประเทศ ซึ่งในความเป็นจริงแล้ว กฎหมาย CLOUD Act ก็ได้ขัดกับหลักการ GDPR ของกลุ่มสหภาพยุโรป ที่ให้ความสำคัญกับการป้องกันข้อมูลส่วนบุคคลของประชาชน รวมถึงข้อกังวลในเรื่องการให้ความร่วมมือของกลุ่ม Five Eyes Alliance ที่เป็นการแบ่งปันข้อมูลข่าวกรองระหว่างประเทศสหรัฐอเมริกา อังกฤษ แคนาดา ออสเตรเลีย และนิวซีแลนด์ ที่มีข้อจำกัดทางบางข้อมูลที่ละเอียดอ่อนและปัญหาความเชื่อมั่นระหว่างกันและกัน

แรงกดดันที่เกิดจากผลกระทบต่อความสัมพันธ์ระหว่างประเทศ ส่งผลไปยังเศรษฐกิจและพัฒนาการทางเทคโนโลยี โดยนโยบาย CHIPS and Science Act ของประเทศสหรัฐอเมริกาในการสนับสนุนการผลิตเซมิคอนดักเตอร์ภายในประเทศ และความต้องการลดการพึ่งพาประเทศจีน รวมถึงการห้ามบริษัทต่างๆไปลงทุนหรือสนับสนุนบริษัทในประเทศจีน ทำให้เกิดผลกระทบต่อห่วงโซ่อุปทานของเซมิคอนดักเตอร์ และทำให้ประเทศพันธมิตรได้รับผลกระทบจนเกิดความขัดแย้ง อาทิเช่นประเทศไต้หวัน และเกาหลีใต้

ผลกระทบที่ทำให้เกิดการแบ่งขั้วทางความสัมพันธ์ระหว่างประเทศในทางไซเบอร์อีกด้านหนึ่ง คือการมีแนวคิดอธิปไตยทางไซเบอร์ที่แตกต่างกัน โดยนโยบายของประเทศสหรัฐอเมริกามีแนวคิดที่ขัดแย้งกับประเทศที่ต้องการรักษาอธิปไตยทางไซเบอร์ เช่น ประเทศจีนและรัสเซีย ที่ต้องการใช้ไซเบอร์ภายในประเทศเพื่อสร้างเสถียรภาพทางการเมือง ก่อให้เกิดการแบ่งขั้วในแนวคิดทางไซเบอร์ของประเทศกลุ่มเสรีนิยม และประเทศที่มีความต้องการควบคุมอินเทอร์เน็ตจากภาครัฐ ทำให้ความตึงเครียดของโลกไซเบอร์ในศตวรรษที่ 21 ทวีความรุนแรงมากยิ่งขึ้น

3. อภิปรายผล

งานวิจัยฉบับนี้ ได้ค้นพบการเชื่อมโยงกับงานวิจัยและวรรณกรรมที่เกี่ยวข้อง โดยความเป็นอนาธิปไตยของโลกไซเบอร์ ได้ชี้ให้เห็นถึงอำนาจการควบคุมของประเทศสหรัฐอเมริกา ที่ใช้ควบคุมข้อมูลของประชาชน ไม่ว่าจะเป็น Google Facebook(Meta) และ Microsoft โดยเป็นการใช้ข้อมูลเพื่อสร้างความมั่นคงให้กับรัฐ แต่ในขณะเดียวกันก็ถือว่าเป็นภัยต่อสิทธิเสรีภาพของประชาชน ได้เป็นการขยายความให้กับงานของ Andrea Monti & Raymond Wacks (2021) ที่ศึกษาผลกระทบของเทคโนโลยีต่อการเมือง อำนาจ และสิทธิส่วนบุคคล โดยงานวิจัยฉบับนี้ได้เติมเต็มงานของ Andrea Monti & Raymond Wacks (2021) ว่า ประเทศสหรัฐอเมริกาควรสร้างสมดุลระหว่างการสร้างความมั่นคงทางไซเบอร์และสิทธิเสรีภาพของประชาชน เพราะหากประเทศสหรัฐอเมริกาใช้อำนาจรัฐเพื่อควบคุมโลกไซเบอร์มากจนเกินไป จะสร้างผลกระทบต่อเสรีภาพประชาธิปไตย ที่เป็นภาพลักษณ์สำคัญในระดับนานาชาติ

การศึกษาความเป็นประเทศมหาอำนาจในแง่ของการเป็นผู้นำทางด้านเทคโนโลยี งานวิจัยของ Rikap & Lundvall (2021) ได้ชี้ให้เห็นถึงผลลัพธ์ของการที่ประเทศสหรัฐอเมริกา มีความเป็นผู้นำทางด้านเทคโนโลยีมาอย่างยาวนาน กำลังถูกท้าทายจากการแข่งขันพัฒนาเทคโนโลยีจากประเทศจีนและรัสเซีย และการแข่งขันทางเทคโนโลยีนี้สามารถนำไปสู่สงครามเทคโนโลยี ซึ่งงานวิจัยฉบับนี้ ได้ชี้ให้เห็นถึงการสร้างนโยบายเพื่อกีดกันคู่แข่งทางการเมืองระหว่างประเทศ โดยงานวิจัยฉบับนี้เสนอว่าประเทศสหรัฐอเมริกาควรพัฒนาเทคโนโลยี AI และ คอมพิวเตอร์ควอนตัม อย่างรวดเร็วที่สุด เพื่อรักษาการเป็นผู้นำทางด้านไซเบอร์ และควรพิจารณาถึงการใช้นโยบายในการสร้างการแข่งขันการพัฒนาเทคโนโลยีระหว่างประเทศ เนื่องจากเป็นการสร้างผลกระทบต่อเศรษฐกิจและการเมืองระหว่างประเทศ

การรักษาดุลแห่งอำนาจ คือสิ่งที่ท้าทายประเทศสหรัฐอเมริกาในศตวรรษที่ 21 โดยในงานของ Xuetong (2020) เกี่ยวกับการแข่งขันของระบบสองขั้วอำนาจทางเทคโนโลยี ที่เกี่ยวข้องกับการแบ่งขั้วทางเทคโนโลยีระหว่างประเทศจีนและสหรัฐอเมริกา และผลกระทบจากการที่ประเทศสหรัฐอเมริกาพยายามจะกีดกันอิทธิพลของประเทศจีนโดยใช้กฎหมายต่างๆในการแบนเทคโนโลยีของประเทศจีน อาทิเช่น Huawei และ Tiktok งานวิจัยฉบับนี้ได้ชี้ให้เห็นถึงความเสี่ยงจากการแบ่งขั้วอำนาจทางเทคโนโลยี ที่สามารถทวีความรุนแรง จนก่อให้เกิดสงครามไซเบอร์ขึ้นได้ง่ายมากยิ่งขึ้น และประเทศสหรัฐอเมริกา ควรให้ความสำคัญต่อการสร้างพันธมิตรและความสัมพันธ์กับประเทศพันธมิตรต่างๆ เพื่อเตรียมพร้อมสำหรับสงครามไซเบอร์ที่สามารถเกิดขึ้นได้ตลอดเวลา

ลำดับผู้ใช้งานของโลกไซเบอร์ คือปัจจัยสำคัญที่รัฐควรให้ความสำคัญ งานของ Oktavianto & Sibarani (2024) ได้อธิบายถึงความสำคัญของการให้ความรู้กับประชาชนและองค์กรต่างๆเกี่ยวกับ

ความมั่นคงทางไซเบอร์ โดยประเทศสหรัฐอเมริกาได้มีการจัดฝึกอบรมให้กับบุคลากรที่มีส่วนเกี่ยวข้องกับไซเบอร์ แต่ภายในองค์กรของภาครัฐ ก็ยังคงมีปัญหาทางด้านการขาดบุคลากรที่มีความรู้ทางไซเบอร์ โดยงานวิจัยฉบับนี้อภิปรายเพิ่มเติมในการที่ประเทศสหรัฐอเมริกา ควรจัดสรรงบประมาณเพิ่มเติมในการฝึกอบรมบุคลากรที่เกี่ยวข้องกับไวเบอร์ และควรให้ภาคเอกชนเข้ามามีบทบาทมากขึ้นสำหรับการให้ความรู้ถึงภัยคุกคามทางไซเบอร์

การโจมตีทางไซเบอร์ได้เพิ่มมากยิ่งขึ้นในศตวรรษที่ 21 งานของ Mahmood et al (2024) ได้อธิบายถึงการเพิ่มขึ้นของการโจมตีทางไซเบอร์ในช่วง COVID-19 อย่างมีนัยสำคัญ ทำให้ประเทศสหรัฐอเมริกาจำเป็นต้องรับมือกับการโจมตีทางไซเบอร์ในหลากหลายด้าน ซึ่งรวมไปถึงระบบโครงสร้างพื้นฐานทางด้านสาธารณสุขและการเงิน งานวิจัยฉบับนี้เสนอว่าประเทศสหรัฐอเมริกา ควรมีแผนการรับมือภัยคุกคามทางไซเบอร์ในช่วงวิกฤตให้มีประสิทธิภาพมากยิ่งขึ้น โดยการนำ AI และข้อมูลต่างๆที่ประเทศสหรัฐอเมริกาสามารถใช้งาน ในการตรวจจับการโจมตีทางไซเบอร์ก่อนที่จะถูกโจมตี

ความท้าทายของภัยคุกคามทางไซเบอร์ ได้ส่งผลไปในหลากหลายมิติ รวมถึงการทูตระหว่างประเทศ งานของ Rehman & Rassias (2024) ได้อธิบายถึงการที่ประเทศสหรัฐอเมริกาถูกกล่าวหาว่าใช้ไซเบอร์ในการแทรกแซงประเทศต่างๆ ทำให้ประเทศจีนและรัสเซียใช้ข้อกล่าวหานี้ในการโจมตีความชอบธรรมทางไซเบอร์ของประเทศสหรัฐอเมริกาเพื่อเป็นการทำลายภาพลักษณ์ของประเทศเสรีนิยมอย่างประเทศสหรัฐอเมริกา งานวิจัยฉบับนี้เสนอว่า ความมั่นคงทางไซเบอร์ควรได้รับการบรรจุอยู่ในประเด็นหลักที่ใช้ในการปรึกษาหารือถึงทางออกที่สันติและมีความเป็นไปได้ในทางการทูตระหว่างประเทศ และควรสร้างข้อตกลงในขอบเขตการใช้อำนาจทางไซเบอร์ระหว่างประเทศ เพื่อรักษาความสัมพันธ์ที่ดีต่อนานาประเทศ และหลีกเลี่ยงการแทรกแซงทางไซเบอร์ต่างๆ

งานวิจัยฉบับนี้ ได้ชี้ให้เห็นถึงความสำคัญของไซเบอร์ ในบทบาทของการเสริมความมั่นคงและอำนาจของประเทศสหรัฐอเมริกาในศตวรรษที่ 21 โดยไซเบอร์ได้มีส่วนในการเสริมสร้างประสิทธิภาพในหลากหลายด้าน ไม่ว่าจะเป็นทางด้านการทหาร เศรษฐกิจ และระบบโครงสร้างพื้นฐานสำคัญของประเทศ ประเทศสหรัฐอเมริกา ใช้ไซเบอร์เป็นเครื่องมือในการรักษาความได้เปรียบเชิงกลยุทธ์ทั้งในระดับประเทศและระดับนานาชาติ จากการมีโครงสร้างพื้นฐานทางไซเบอร์ที่ครอบคลุมอยู่ทั่วโลก

งานวิจัยได้แสดงให้เห็นถึงบทบาทของประเทศสหรัฐอเมริกา ที่มีความสามารถทางไซเบอร์ในด้านต่างๆ โดยได้ทำการวิเคราะห์ผ่านองค์ประกอบเหล่านี้

1. อำนาจทางไซเบอร์ด้านการทหาร (Cyber Military Power) หมายถึง การที่ประเทศสหรัฐอเมริกามีโครงสร้างพื้นฐานทางการทหารที่แข็งแกร่ง ส่งผลให้มีกองกำลังไซเบอร์ที่แข็งแกร่ง ที่สามารถใช้ในการโจมตีและป้องกันได้อย่างมีประสิทธิภาพ

2. อำนาจทางไซเบอร์ด้านเทคโนโลยี (Cyber Technology Power) หมายถึง พัฒนาการทางเทคโนโลยีไซเบอร์ของประเทศสหรัฐอเมริกา ที่มีความสามารถสูง ทำให้ประเทศสหรัฐอเมริกามีความสามารถในการควบคุมอินเทอร์เน็ตและเครือข่ายได้ทั่วโลก
3. อำนาจทางไซเบอร์ด้านวิทยาศาสตร์ (Cyber Science Power) หมายถึง การมีบุคลากรและสถาบันวิจัยที่รองรับและผลิตผู้เชี่ยวชาญทางไซเบอร์ที่มีประสิทธิภาพสูง

การวิเคราะห์ดังกล่าวทำให้เห็นถึงความมั่นคงทางไซเบอร์ของประเทศสหรัฐอเมริกาที่เป็นส่วนหนึ่งของแผนยุทธศาสตร์ของประเทศสหรัฐอเมริกา และเป็นสิ่งที่ช่วยให้ประเทศสหรัฐอเมริกาสามารถรักษาสถานะความเป็นประเทศมหาอำนาจของโลกใบนี้ ในช่วงเวลาที่มีการแข่งขันทางไซเบอร์ที่สูงมากยิ่งขึ้น

ความเป็นอนาธิปไตยของโลกไซเบอร์ คือสิ่งที่เหมือนกับระบบการเมืองระหว่างประเทศ ที่ไม่มีผู้กำหนดหรือควบคุมทิศทางต่างๆได้ ก่อให้เกิดความขัดแย้ง การแข่งขัน และความไม่เชื่อใจระหว่างประเทศ โดยสิ่งที่งานวิจัยฉบับนี้ได้ค้นพบ คือ การที่ประเทศสหรัฐอเมริกาได้ถูกท้าทายจากการโจมตีทางไซเบอร์จากรัฐอื่นๆ ไม่ว่าจะเป็นประเทศจีนและรัสเซีย โดยเฉพาะความเสียหายในระดับโครงสร้างพื้นฐานสำคัญของประเทศสหรัฐอเมริกาที่เคยถูกโจมตี ไม่ว่าจะเป็น พลังงานไฟฟ้า ท่อขนส่งน้ำมัน และหน่วยงานภาครัฐต่างๆ ความท้าทายที่เกิดจากความเป็นอนาธิปไตยทางไซเบอร์ คือสิ่งที่ท้าทายประเทศสหรัฐอเมริกา โดยเฉพาะการท้าทายทางด้านกฎหมาย ที่ขอบเขตของแต่ละประเทศมีการบังคับใช้กฎหมายทางไซเบอร์ที่แตกต่างกัน ทำให้สามารถสร้างความขัดแย้งให้กับความสัมพันธ์ระหว่างประเทศเกิดขึ้นได้ ทำให้ประเทศสหรัฐอเมริกาจำเป็นอย่างยิ่ง ที่จะต้องพัฒนาเทคโนโลยีไซเบอร์ เพื่อรักษาความมั่นคงทางไซเบอร์ รวมถึงการพัฒนานโยบายเพื่อรองรับความขัดแย้งและความเสี่ยงที่สามารถเกิดขึ้นได้ ไม่ว่าจะเป็นจากตัวแสดงที่เป็นรัฐ หรือ กลุ่มก่อการร้ายต่างๆ และตัวแสดงอื่นๆที่ไม่ใช่รัฐเช่นกัน

ความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ทำให้ประเทศสหรัฐอเมริกามีบทบาทในการกำหนดทิศทางของโลกไซเบอร์ในระดับนานาชาติ โดยใช้ความได้เปรียบทางโครงสร้างพื้นฐานที่สำคัญของโลกไซเบอร์ และความเป็นผู้นำทางเทคโนโลยีไซเบอร์ในศตวรรษที่ 21 โดยงานวิจัยฉบับนี้ได้ค้นพบสิ่งสำคัญที่ชี้ให้เห็นถึงผลลัพธ์ของความเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ที่ทำให้ประเทศสหรัฐอเมริกามีความสามารถควบคุมโครงสร้างพื้นฐานของโลกไซเบอร์ เช่น การมีฐานที่ตั้งเซิร์ฟเวอร์หลักของโลก และการมีสายเคเบิ้ลใต้ทะเล ทำให้สามารถตรวจสอบและควบคุมข้อมูลที่ไหลเวียนอยู่ในระบบได้ ประเทศสหรัฐอเมริกาได้มีนโยบายทางไซเบอร์ที่สร้างผลกระทบต่อความสัมพันธ์ระหว่างประเทศ อาทิเช่น การกำหนดหลักเกณฑ์พื้นฐานของการมีความมั่นคงทางไซเบอร์ การแบนเทคโนโลยีของประเทศคู่แข่ง และการใช้กฎหมายเพื่อยับยั้งการ

ลงทุนในประเทศคู่แข่ง อีกทั้งประเทศสหรัฐอเมริกามีฐานข้อมูลขนาดใหญ่ ผ่านการบังคับใช้กฎหมายและนวัตกรรมปัญญาประดิษฐ์ (AI) ที่เป็นเครื่องมือสำคัญในการแข่งขันเทคโนโลยีในอนาคต จากการค้นพบเหล่านี้ ทำให้เห็นถึงการที่ประเทศสหรัฐอเมริกา ใช้ไซเบอร์เป็นเครื่องมือเพื่อรักษาสถานะความเป็นประเทศมหาอำนาจในการเมืองระหว่างประเทศ

ถึงแม้ว่าประเทศสหรัฐอเมริกา จะเป็นประเทศมหาอำนาจทางไซเบอร์ แต่ความท้าทายต่างๆได้สร้างข้อจำกัดบางประการให้กับประเทศมหาอำนาจนี้ ไม่ว่าจะเป็นภัยคุกคามจากการโจมตีโดยแฮ็กเกอร์ที่ได้การสนับสนุนจากภาครัฐอื่นๆ โดยประเทศสหรัฐอเมริกาถูกตั้งเป้าให้เป็นเป้าหมายหลักในการโจมตี ไม่ว่าจะเป็นจากประเทศจีน รัสเซีย เกาหลีเหนือ และอิหร่าน และมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง การขาดแคลนบุคลากรทางด้านไซเบอร์ของประเทศสหรัฐอเมริกา ซึ่งถึงแม้ว่าจะเป็นประเทศที่ล้ำหน้ากว่าประเทศอื่นๆ แต่ปัญหาทางด้านการผลิตบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์ในระดับสูง ก็เป็นปัญหากับประเทศเช่นกัน ความขัดแย้งในความสัมพันธ์ระหว่างประเทศที่เกิดจากนโยบายไซเบอร์ ทำให้ประเทศสหรัฐอเมริกามีความขัดแย้งเพิ่มมากยิ่งขึ้น ไม่เพียงแต่กับประเทศคู่แข่ง แต่ความไม่เชื่อใจจากประเทศพันธมิตรก็ได้เริ่มทวีความรุนแรงขึ้นด้วยเช่นกัน

งานวิจัยฉบับนี้ ได้ยืนยันถึงการเป็นประเทศมหาอำนาจทางไซเบอร์ของประเทศสหรัฐอเมริกา ในการเป็นประเทศมหาอำนาจทางไซเบอร์อันดับหนึ่งของโลก และในขณะเดียวกัน ก็ได้เผชิญหน้ากับความท้าทายในศตวรรษที่ 21 จากภัยคุกคามทางไซเบอร์ที่มีเพิ่มมากยิ่งขึ้น ความเป็นประเทศที่มีอำนาจทางไซเบอร์ ส่งผลต่อความสำคัญในการเมืองระหว่างประเทศ และเป็นปัจจัยที่ส่งเสริมให้ประเทศสหรัฐอเมริกา รักษาสถานการณ์เป็นผู้นำในการเมืองระหว่างประเทศด้วยเช่นกัน แต่อย่างไรก็ตาม ความเป็นอนาธิปไตยในโลกไซเบอร์ และการเพิ่มขึ้นของประเทศคู่แข่งที่เป็นผลจากการแบ่งขั้วอำนาจทางไซเบอร์ ไม่ว่าจะเป็นประเทศจีน และรัสเซีย ส่งผลให้ประเทศสหรัฐอเมริกาจำเป็นต้องพัฒนาเทคโนโลยีไซเบอร์อย่างรวดเร็วมากกว่าในอดีต เพื่อป้องกันภัยคุกคามทางไซเบอร์ และความเป็นผู้นำในการเป็นประเทศมหาอำนาจทางไซเบอร์ในศตวรรษที่ 21

4. ข้อเสนอแนะ

4.1 ข้อเสนอแนะเชิงนโยบาย

งานวิจัยชิ้นนี้ มีข้อเสนอแนะต่อหน่วยงานที่เกี่ยวข้องกับการกำหนดนโยบายไซเบอร์และหน่วยงานความมั่นคงแห่งชาติ ดังนี้

4.1.1 ส่งเสริมการสร้างแรงงานทางไซเบอร์ที่มีประสิทธิภาพ รวมถึงการสร้างความมั่นคงให้กับอาชีพที่เกี่ยวข้องกับไซเบอร์ ให้ประชากรมีความต้องการเป็นส่วนหนึ่งของแรงงานไซเบอร์ เนื่องจากประเทศไทย ถือเป็นประเทศที่ขาดความพร้อมทางด้านแรงงานไซเบอร์เป็นอย่างมาก และความเป็นที่

ต้องการทางแรงงานไซเบอร์เพื่อรองรับการเตรียมพร้อมจากภัยคุกคามทางไซเบอร์ที่สามารถเกิดขึ้นได้ทุกเมื่อ

4.1.2 สร้างกองกำลังทางไซเบอร์ที่พร้อมสำหรับการโจมตีไม่ว่าจะเป็นภายในประเทศหรือภัยคุกคามจากนอกประเทศ เพื่อความพร้อมในสถานการณ์ฉุกเฉินที่สามารถสร้างความเสียหายให้กับประเทศได้ และส่งเสริมสวัสดิการให้กับกองกำลังทางไซเบอร์ เพื่อการเป็นกองกำลังที่มีประสิทธิภาพและยั่งยืน

4.1.3 ส่งเสริมการดำเนินกิจกรรมที่พัฒนาองค์ความรู้ทางไซเบอร์ และการผลักดันให้คนรุ่นใหม่ เข้าใจและสามารถใช้งานไซเบอร์ได้อย่างมีประสิทธิภาพ ไม่ปิดกั้นเสรีภาพทางไซเบอร์ ไม่ว่าจะเป็นการเรียนรู้ หรือการแสดงออกทางความคิด ที่เป็นส่วนสำคัญต่อการสร้างนวัตกรรมทางไซเบอร์เพื่อความพัฒนาที่ยั่งยืน

4.1.4 การให้ความสำคัญต่อนโยบายไซเบอร์จากผู้นำประเทศ ที่มีความรู้และเข้าใจต่อความสำคัญที่แท้จริงของโลกไซเบอร์ ไม่ว่าจะเป็นการใช้ไซเบอร์ทางการทหาร นโยบายไซเบอร์ระหว่างประเทศ ความสำคัญต่อโครงสร้างพื้นฐานที่ต้องการความมั่นคงและปลอดภัย การสร้างแรงงานไซเบอร์เพื่อรองรับความต้องการในอนาคต การวางเครือข่ายและส่งเสริมการสร้างการเข้าถึงโลกไซเบอร์ให้กับภาคประชาชน

4.1.5 การให้ทุนสนับสนุนกับนักวิชาการทางไซเบอร์ เพื่อเป็นแรงผลักดันให้นักวิชาการมีความต้องการในการพัฒนาองค์ความรู้เพื่อส่งต่อองค์ความรู้ไปยังคนรุ่นต่อไป ให้มีความยั่งยืน

4.1.6 ทำให้ประเทศมีเสถียรภาพทางการเมือง เพื่อให้ประชากรมีความใส่ใจกับการพัฒนาองค์ความรู้ และการดำเนินนโยบายต่างๆให้เป็นไปอย่างราบรื่น

4.2 ข้อเสนอต่องานวิจัยในอนาคต

4.2.1 งานวิจัยชิ้นนี้ ให้ความสำคัญกับประเทศมหาอำนาจ คือ ประเทศสหรัฐอเมริกา

ซึ่งเป็นประเทศที่มีระบอบการปกครองแบบประชาธิปไตย ยังขาดการวิเคราะห์ในประเทศที่มีระบอบการปกครองที่แตกต่างกัน ไม่ว่าจะเป็นการปกครองแบบสังคมนิยมหรือ คอมมิวนิสต์

4.2.2 งานวิจัยชิ้นนี้ เป็นการศึกษาประเทศมหาอำนาจและเป็นประเทศที่พัฒนาแล้ว ยังขาดการศึกษาประเทศที่กำลังพัฒนา ที่ได้รับผลกระทบจากโลกไซเบอร์ รวมถึงประเทศที่ด้อยพัฒนา ในการมีส่วนร่วมกับโลกไซเบอร์และความมั่นคงทางไซเบอร์

4.3.3 การศึกษาประเทศไทยสามารถได้รับผลกระทบอย่างไร จากโลกไซเบอร์และการวิเคราะห์ในการสร้างอำนาจทางไซเบอร์ให้กับประเทศที่กำลังพัฒนา ว่ามีความเป็นไปได้มากน้อยเพียงใด จากความเป็นอนาธิปไตยของโลกไซเบอร์

บรรณานุกรม

สุรชาติ บำรุงสุข. (2545). **กระบวนทัศน์ความมั่นคงใหม่ : ความเปลี่ยนแปลงของทฤษฎีและกรณีประเทศไทย**. กรุงเทพฯ : วารสารสังคมศาสตร์ : 25 ปี 6 ตุลา.

Abdelmalak, M., Bhusal, N., Gautam, M., & Benidris, M. (2023). **Cyber-Physical Power System Layers: Classification, Characterization, and Interactions**. 2023 IEEE Texas Power and Energy Conference (TPEC). https://doi.org/10.1109/TPEC56611.2023.10078602

AFCEA Cyber Committee. (n.d.). **The evolution of U.S. cyberpower. AFCEAinternational.** Retrieved from https://www.afcea.org/committees/cyber/documents/theevolutionofuscyberpower.pdf

Amoroso, E. 2006. **Cyber Security**. New Jersey: Silicon Press

Andress, J., & Winterfeld, S. (2013). **Cyber warfare: techniques, tactics and tools for security practitioners**. Elsevier.

Asadi, H. (2022). **The economic impact of cyberattacks in the United States [Master's thesis, City University of New York]**. CUNY Academic Works. https://academicworks.cuny.edu/jj_etds/255

Aslanoglu, R., & Tekir, S. (2012). **Recent cyberwar spectrum and its analysis**. Proceedings of the 11th European Conference on Information Warfare and Security, 45–52.

Arslan, A. S. (2023). **Neorealist analysis of security dilemma in cyberspace: A quantitative study**. APSA Preprints. https://preprints.apsanet.org/engage/api-gateway/apsa/assets/orp/resource/item/642f46b9736114c9630aa93f/original/neorealist-analysis-of-security-dilemma-in-cyberspace-a-quantitative-study.pdf

Azmi, R., & Kautsarina. (2019). **Revisiting Cyber Definition**. Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS). https://www.researchgate.net/publication/334989724_Revisiting_Cyber_Definition Baezner, M. (2018). **Hotspot analysis: Cyber disruption and cybercrime: Democratic people's Republic of Korea**. Zurich: Center for Security Studies (CSS), ETH Zurich.

Baezner, M., & Robin, P. (2017). **Hotspot analysis: Stuxnet. Zurich: Center for Security Studies (CSS)**. ETH Zurich.

Baezner, M., & Robin, P. (2017). **Cyber-conflict between the United States of America and Russia. Zurich: Center for Security Studies (CSS)**. ETH Zurich.

Belt and Road Portal. (2024). **Belt and Road Initiative**. Retrieved from www.yidaiyilu.gov.cn

Bendrath, R. (2001). **The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection**. Information & Security: An International Journal, 7, 80-103. https://doi.org/10.11610/isij.0705

Benkler, Y. (2016). **Networked Publics and the Global Information Society**. MIT Press.

Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). **Security: A new framework for analysis**. Lynne Rienner Publishers.

Canongia, C., & Mandarino, R. (2014). **Cybersecurity: The New Challenge of the Information Society**. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global. http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

Carayannis, E. G., Campbell, D. F. J., & Efthymiopoulos, M. P. (Eds.). (2014). **Cyber-development, cyber-democracy and cyber-defense: Challenges, opportunities and implications for theory, policy and practice**. Springer. https://doi.org/10.1007/978-1-4939-1028-1

Carnegie endowment. (n.d.). **Timeline of Cyber Incidents Involving Financial Institutions**. Retrieved September 16, 2022 from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Carr, J. (2012). **Inside Cyber Warfare: Mapping the Cyber Underworld**. O'Reilly Media, Inc., Sebastopol.

Cavelty, M. D. & Wenger, A. (2020). **Cyber security meets security politics: Complex technology, fragmented politics, and networked science**. *Contemporary Security Policy*, 41(1), 5-32, DOI: 10.1080/13523260.2019.1678855

CCDCOE. (2015). **Cyber Security: United States Organisation**. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf

Center for Strategic and International Studies (CSIS). (n.d.). **Significant Cyber Incidents Since 2006**. Retrieved September 16, 2022 from https://csis-websiteprod.s3.amazonaws.com/s3fspublic/220906_Significant_Cyber_Incidents.pdf?OSKTnneXKCxI_Qx1Y7An4JGjm6DiTB0_

Clark, D. D. (2010). **Characterizing cyberspace: Past, present and future (ECIR Working Paper No. 2010-3)**. MIT Political Science Department.

CNSS. 2010. **National Information Assurance Glossary**. Committee on National Security Systems (CNSS) Instruction No. 4009: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

Crespo, R. A. (2018). **Currency warfare and cyber warfare: The emerging currency battlefield of the 21st century**. *Comparative Strategy*, 37(3), 235-250.

Dalio, R. (2022). **The Changing World Order: Country Power Index 2022**.

DeNardis, L. (2020). **The Internet in everything: Freedom and security in a world with no off switch**. Yale University Press.

Di Pane, J. (2 0 2 4). **Cyber Warfare and U.S. Cyber Command**. The Heritage Foundation. Retrieved from https://www.heritage.org/military-strength/assessment-us- military-power/cyber-warfare-and-us-cyber-command

DHS. (2014). **A Glossary of Common Cybersecurity Terminology**. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1 , 2 0 1 4 : http://niccs.us-cert.gov/glossary#letter_c

Dunn Cavelty, M. (2018). **Cybersecurity in the Age of Digital Politics**. Routledge.

Floridi, L. (2014). **The Fourth Revolution: How the Infosphere is Reshaping Human Reality**. Oxford University Press.

Foulon, M., & Meibauer, G. (2024). **How cyberspace affects international relations: The promise of structural modifiers**. Contemporary Security Policy. https://doi.org/10.1080/13523260.2024.2365062

Finszter, G., & Sabjanics, I. (Eds.). (2018). **Security challenges in the 21st century**. Dialóg Campus Publishing.

Freeman, C. (2007). **The political economy of the long wave**. The evolution of economic institutions, 75-97.

Gady, F. S., & Austin, G. (2010). **Russia, the United States, and cyber diplomacy**. Opening the Doors, East West Institute: New York.

Gallagher, J. C. (2022). **Undersea Telecommunication Cables: Technology Overview and Issues for Congress (CRS Report No. R47237)**. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R47237

Gartzke, E., & Lindsay, J. R. (2022). **Is there a cyber security dilemma?**.Journal of Cybersecurity, 8 (1) , tyac0 1 2 . https://academic.oup.com/cybersecurity/article/8/1/tyac012/6705410

Ghincea, M. (2023). **Great powers, foreign policy, and the Russo-Ukrainian war**. Brill.

Ginter, A. (2018). **The Top 20 Cyberattacks on Industrial Control Systems, chapter Andrew Ginter**. Waterfall Security Solutions.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). **2005 CSI/FBI computer crime and security survey**. Computer Security Journal, 21(3), 1.

Gross, A., Heal, A., Campbell, C., Clark, D., Bott, I., & de la Torre Arenas, I. (2023). **Subsea cables: how the US is pushing China out of the internet's plumbing**. Financial Times. Retrieved from https://ig.ft.com/subsea-cables/

Hamourtziadou, L. (2019). **Security challenges of the 21st century: New challenges and perspectives**. Journal of Global Faultlines, 6(2), 121-123.

Heylighen, F. (2011). **Conceptions of a Global Brain: an historical review**. Evolution: Cosmic, biological, and social, 274-289.

Hjortdal, M. (2011). **China's use of cyber warfare: Espionage meets strategic deterrence**. *Journal of Strategic Security*, 4(2), 1-24.

Hurley, M. M. (2012). **For and from cyberspace: Conceptualizing cyber intelligence, surveillance, and reconnaissance**. AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST.

ITU. 2009. **Overview of Cybersecurity**. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Kaska, K., Beckvard, H., & Minárik, T. (2019). **Huawei, 5G, and Security**. NATO CCD COE.

Katz, M. N. (2018). **Great powers in the twenty-first century**. nSzoriHo, Winter 2018(10), 122-133.

Kaviani, R. (2017). **The concept of power in international relations**. International Journal of Political Science, 7(2), 29-36.

Kello, L. (2018). **Realism and cyber conflict: Security in the digital age**. E-International Relations. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

Kemmerer, R. A. 2003. **Cybersecurity**. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257

Klipstein, M., & Breuer, P. (2021). **Powering the DIME: Unlearned lessons of asymmetric national power in cyberspace**. The Cyber Defense Review, 7(1), 129–135.

Kuusisto, T., Kuusisto, R. (2015). **Cyber World as a Social System**. In: Lehto, M., Neittaanmäki, P. (eds) **Cyber Security: Analytics, Technology and Automation**. Intelligent Systems, Control and Automation: Science and Engineering, vol 78. Springer, Cham. https://doi.org/10.1007/978-3-319-18302-2_2

Kyriazis, M. (2015). **Systems neuroscience in focus: From the human brain to the global brain?**. Frontiers in Systems Neuroscience, 9 (7). https://doi.org/10.3389/fnsys.2015.00007

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). **Cyber security in the age of COVID-19: A timeline and**

analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

Landau, S. (2022). **Cyberwar in Ukraine: What You See Is Not What's Really There.** Retrieved from: https://www.lawfareblog.com/cyberwar-ukraine-what-you-see-not-whats-really-there

Lehto, M. (2013). **The cyberspace threats and cyber security objectives in the cyber security strategies**. International Journal of Cyber Warfare and Terrorism (IJCWT), 3(3), 1-18.

Lewis, J. A. (2006). **Cybersecurity and Critical Infrastructure Protection**. Washington, DC: Center for Strategic and International Studies. http://csis.org/publication/cybersecurity-and-criticalinfrastructure- protection

Libicki, M. (2009). **Cyberdeterrence and Cyberwar**. RAND Corporation.

Lonergan, E. D., & Schneider, D. (2023). **The power of beliefs in US cyber strategy: The evolving role of deterrence, norms, and escalation**. *Journal of Cybersecurity, 9*(1), Article tyad006. https://doi.org/10.1093/cybsec/tyad006

Mahmood, S., Chadhar, M., & Firmin, S. (2024). **Addressing cybersecurity challenges in times of crisis: Extending the sociotechnical systems perspective**. Applied Sciences, 14(11610). https://doi.org/10.3390/app142411610:contentReference[oaicite:1]{index=1}.

Mitra, A. (2010). **Digital security: cyber terror and cyber security**. Infobase Publishing.

Nye, J. S. Jr. (2011). **The Future of Power**. Issues & Insights, 11(8), Pacific Forum CSIS.

Nye, J. (2017). **The Future of Power**. PublicAffairs.

Oktavianto, R., & Sibarani, B. E. (2024). **Building Cyber-savvy Generation: 15 Years of Research on Cybersecurity Education and Future Research Agendas**. SSRN. Retrieved from https://ssrn.com/abstract=5004673

Owen, R. S. (2007). **Infrastructures of cyber warfare**. In Cyber warfare and cyber terrorism (pp. 35-41). IGI Global.

Oxford University Press. (2014). **Oxford Online Dictionary**. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity

Peritz, A. J., & Sechrist, M. (2010). **Protecting Cyberspace and the US National Interest**. Belfer Center for Science and International Affairs, Cambridge, MA, USA.

Pijovic, N. (2021). **Cyber intelligence sharing and the Five Eyes: The politics of sharing and withholding**. 13th International Conference on Cyber Conflict (CyCon), 133–148.

Pitrelli, M. (2022). **Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia.** Retrieved November 30, 2022 from https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html

Powell, R. (1994). **Anarchy in international relations theory: The neorealist-neoliberal debate**. International Organization, 48(2), 313-344. Retrieved from JSTOR.

Public Safety Canada. (2014). **Terminology Bulletin 281: Emergency Management Vocabulary**. Ottawa: Translation Bureau, Government of Canada. http://www.bt-tb.tpsgcpwgsc.gc.ca/publications/documents/urgence-emergency.pdf

Rasser, M. (2022). **The CHIPS and Science Act: Strengthening America's Semiconductor Industry and Countering China**. Center for a New American Security (CNAS).

Raud, M. (2016). **China and Cyber: Attitudes**. *Strategies, Organisation', for Nato Cooperative Cyber Defence Centre of Excellence, Tallinn*.

Rehman, S., & Rassias, M. (2024). **Security challenges in the 21st century: Addressing cybersecurity threats in international diplomacy**. ResearchGate. https://www.researchgate.net/publication/386341180

Rikap, C., & Lundvall, B. Å. (2021). **China's Catching-Up Process and Its Emergence as a Potential Lead Country in Artificial Intelligence**. In The Digital Innovation Race (pp. 121-144). Palgrave Macmillan, Cham.

Robinson, J. (2022). **Cyberwarfare statistics: A decade of geopolitical attacks**. Retrieved September 7, 2022 fromhttps://www.privacyaffairs.com/geopolitical-attacks/

Sadler, B. D. (2023). **2024 Index of U.S. Military Strength**. The Heritage Foundation. Retrieved fromhttps://www.heritage.org/sites/default/files/2024-01/2024_IndexOfUSMilitaryStrength.pdf

Sailio, M., Latvala, O.-M., & Szanto, A. (2020). **Cyber threat actors for the factory of the future**. Applied Sciences, 10(12), 4334. https://doi.org/10.3390/app10124334

Schweller, R. L. (2016). **Balancing in neorealism**. International Security, 40(2), 51-86. https://doi.org/10.1162/ISEC_a_00216

Segal, A. (2018). **The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age**. PublicAffairs.

Segal, A. (2020). **China, Huawei, and the Global Battle for 5G**. Council on Foreign Relations. Retrieved from https://www.cfr.org

Sharma, R. (2020). **The Rise of Digital Sovereignty: Cyber Power and Geopolitics**. Springer.

Shier, J. (2020). **CYBERTHREATS: A 20-YEAR RETROSPECTIVE**. Retrieved fromhttps://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-cyberthreats-20-year-retrospective-wp.pdf

Sigholm, J. (2016). **Non-state actors in cyberspace operations**. Journal of Military Studies, 4(1), 1-37.

Spoehr, T. W. (2023). **2024 Index of U.S. Military Strength**. The Heritage Foundation. Retrieved from https://www.heritage.org/sites/default/files/2024-01/2024_IndexOfUSMilitaryStrength.pdf

Sumari, A. D. W., Gunawan, D., & Munthaha, F. (2014). **Cyberspace operations as multiplier power in asymmetric conflict**. Retrieved from https://scholar.ui.ac.id/en/publications/cyberspace-operations-as-multiplier-power-in-asymmetric-conflict

The White House. (2023). **National cybersecurity strategy**. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The White House. (2023). **National Cyber Workforce and Education Strategy (NCWES)**. The White House. https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

Tsakanyan, V. T. (2017). **The role of cybersecurity in world politics**. Vestnik RUDN. International Relations, 17(2), 339-348. doi: 10.22363/2313-0660-2017-17-2-339-348

United Nations Security Council Counter-Terrorism Committee. (2025). **Technology and terror: The new arsenal of anarchy**. Retrieved from https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/new_delhi_-ict-_statement_by_resolve_network.pdf

U.S. Department of Energy. (2022). **National cybersecurity strategy for critical infrastructure energy sector. U.S. Department of Energy**. Retrieved from https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

Van Haaster, J. (2016). **Assessing cyber power**. In 2016 8th International Conference on Cyber Conflict (CyCon) (pp. 7-21). IEEE.

Venable, J. (2023). **2024 Index of U.S. Military Strength**. The Heritage Foundation. https://www.heritage.org/sites/default/files/2024-01/2024_IndexOfUSMilitaryStrength.pdf

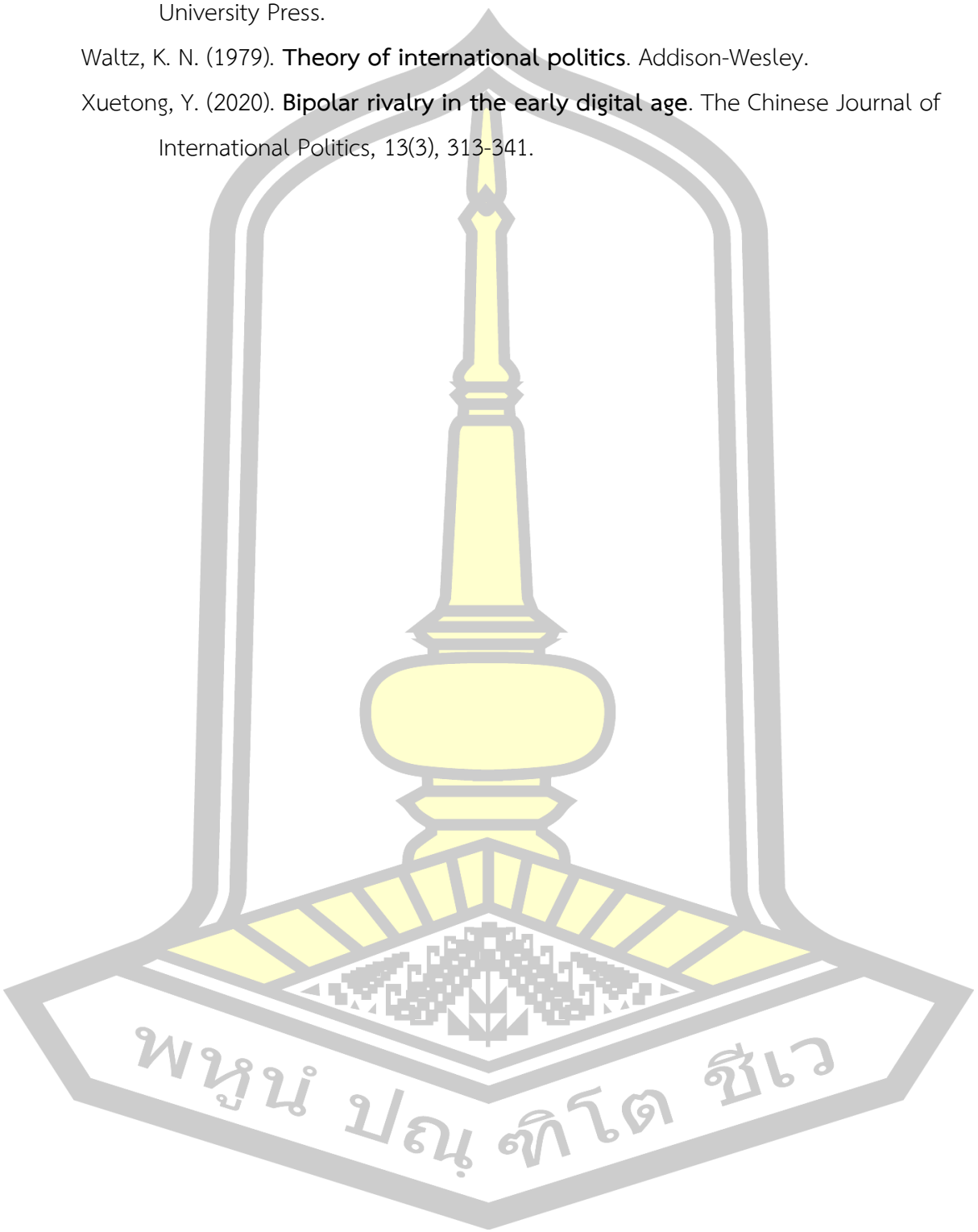
Victoria, A. (2018). **Cyber Information - US**. ResearchGate. https://doi.org/10.13140/RG.2.2.13202.96968

Voo, J., Hemani, I., & Cassidy, D. (2022). **National cyber power index 2022**. Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

Waltz, K. N. (1959). **Man, the state, and war: A theoretical analysis**. Columbia University Press.

Waltz, K. N. (1979). **Theory of international politics**. Addison-Wesley.

Xuetong, Y. (2020). **Bipolar rivalry in the early digital age**. The Chinese Journal of International Politics, 13(3), 313-341.



บรรณานุกรม

พหุน ปณฺ ฑิโต ชีเว

ประวัติผู้เขียน

ชื่อ	อลงกรณ์ ศิลปดอนบม
วันเกิด	วันพฤหัสบดีที่ 15 กรกฎาคม พ.ศ.2536
สถานที่เกิด	กรุงเทพมหานคร
สถานที่อยู่ปัจจุบัน	10/19 ม.14 ถ.มิตรภาพ ต.ในเมือง อ.เมือง จ.ขอนแก่น 40000
ตำแหน่งหน้าที่การงาน	ธุรกิจส่วนตัว
สถานที่ทำงานปัจจุบัน	10/19 ม.14 ถ.มิตรภาพ ต.ในเมือง อ.เมือง จ.ขอนแก่น 40000
ประวัติการศึกษา	พ.ศ. 2555 มัธยมศึกษาตอนปลาย (ม.6) โรงเรียนมหาไถ่ศึกษาภาคตะวันออกเฉียงเหนือ จังหวัด ขอนแก่น พ.ศ. 2559 ปริญญาบริหารธุรกิจบัณฑิต (การจัดการ) สาขา ธุรกิจระดับโลก คณะวิทยาลัยนานาชาติ มหาวิทยาลัยขอนแก่น พ.ศ. 2563 ปริญญารัฐประศาสนศาสตรมหาบัณฑิต วิทยาลัยการปกครองท้องถิ่น มหาวิทยาลัยขอนแก่น พ.ศ. 2568 ปริญญารัฐศาสตรดุษฎีบัณฑิต สาขา รัฐศาสตร์ วิทยาลัยการเมืองการปกครอง มหาวิทยาลัยมหาสารคาม