# การใช้อำนาจอธิปไตยในโลกไซเบอร์

## A Using the sovereignty in Cyberspace

**[1]นัทธมน เพชรกล้า และ [2]สุมนทิพย์ จิตสว่าง**

**[1]Natthamon Petchkla and [1]Sumonthip Chitsawang**

สาขาวิชาอาชญาวิทยาและงานยุติธรรม คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Criminology and Justice Studies, Political Sciences, Chulalongkorn University

E-mail: [1]npetchkla@gmail.com, [2]sumonthip99@hotmail.com

**Received** January 16, 2023; **Revised** January 25, 2023; **Accepted** February 7, 2023

**บทคัดย่อ**

บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์อำนาจอธิปไตยทางไซเบอร์ โดยเริ่มต้นอธิบายพื้นฐานความเข้าใจเรื่องอำนาจอธิปไตยที่นำไปสู่การประยุกต์ใช้ในโลกไร้พรมแดน นอกจากนี้ในบทความได้ถอดบทเรียนจากนโยบายการรับมือภัยคุกคามไซเบอร์ของประเทศต่าง ๆ เพื่อขจัดปัญหาการรุกล้ำอำนาจอธิปไตยทางไซเบอร์ที่จะเกิดขึ้นในประเทศไทย โดยบทสรุปจะมีข้อเสนอแนะทางนโยบายเพื่อเป็นประโยชน์ต่อภาครัฐ บทความนี้มาจากการศึกษาแนวคิดทฤษฎี การทบทวนวรรณกรรม และบทสัมภาษณ์ของผู้เกี่ยวข้อง ประเด็นเหล่านี้ไม่ใช่เรื่องใหม่แต่เป็นการทวีคูณความรุนแรงของปัญหาในโลกแห่งไซเบอร์เมื่ออำนาจรัฐและเทคโนโลยีผนวกเข้าด้วยกัน เกิดเป็นมิติใหม่ของสนามรบที่อาจคาดไม่ถึง โลกแห่งไซเบอร์คู่ขนานไปกับโลกแห่งความจริงทำให้รัฐบาลของประเทศต่าง ๆ ไม่สามารถรับมือภัยคุกคามได้อย่างเต็มที่ การใช้กฎหมายภายในประเทศจับกุมคนกระทำความผิดทางไซเบอร์ แม้แต่การเรียกร้องความเป็นธรรมจากองค์กรสหประชาชาติหรือการใช้กฎหมายระหว่างประเทศอาจจะยังไม่ใช่คำตอบที่ดีที่สุดสำหรับการจัดการกับภัยคุกคามไซเบอร์ เพื่อที่จะป้องกันการแทรกแซงอำนาจรัฐในโลกไซเบอร์ บทความนี้ได้ให้คำตอบเพื่อเป็นแนวทางการศึกษาค้นคว้าต่อไป

**คำสำคัญ:** อธิปไตยไซเบอร์; โลกไซเบอร์; ความมั่นคงปลอดภัยไซเบอร์

## Abstract

This article aimed to analyze the cyber sovereignty by explaining the basics of understanding sovereignty and its application in a borderless world. In addition, in the article, lessons learned from the cyber threat response policies of the countries are listed for problems to eliminate, such as poaching the cyber sovereignty that will happen in Thailand. The conclusion will be proposed with policy recommendations for the benefit of the government sector. This article came from a study of theoretical concepts, a literature review, and interviews with relevant stakeholders. These issues may not be new, but they are becoming more serious troubles in cyberspace. When state power and technology are combined, a new dimension of the battlefield emerges that cannot be anticipated. The parallel between the cyber world and the real world has made governments unable to respond to threats effectively. Using domestic laws to arrest cyber criminals, demanding fairness from the United Nations, or applying international law may not be the best answer for dealing with cyber threats. In order to prevent the interference of state power in the cyber world, this article provides answers for further study and research.

**Keywords:** Cyber Sovereignty; Cyberspace; Cyber Security Government

## บทนำ

ปัญหาความคลุมเครือที่เกิดจากโลกไซเบอร์ที่ไร้พรมแดนทำให้รัฐชาติถูกแทรกแซงจากประเทศภายนอก บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์อำนาจอธิปไตยทางไซเบอร์ เพื่อให้เกิดคำนิยามที่ชัดเจนสามารถกำหนดนโยบายและออกกฎหมายเพื่อป้องกันการรุกล้ำทางอำนาจรัฐ โดยเริ่มต้นจากการทำความเข้าใจคำนิยามของอำนาจอธิปไตยที่มีอยู่เพื่อนำมาปรับใช้อย่างร่วมสมัยอำนาจอธิปไตย (Sovereignty) คือ การใช้อำนาจของรัฐเหนือเขตแดนทางกายภาพ มีสิทธิและเสรีภาพในการบริหารจัดการกิจกรรมต่าง ๆ ที่เกิดขึ้นบนพื้นที่อาณาเขตของตน อำนาจอธิปไตยมีองค์ประกอบหลัก 3 ประการด้วยกัน คือ อำนาจในการออกกฎหมาย อำนาจในการบริหาร และอำนาจในการตัดสินตีความ อำนาจอธิปไตยเป็นอำนาจสูงสุดในการปกครองรัฐ ดังนั้นสิ่งอื่นใดจะมีอำนาจยิ่งกว่าหรือขัดต่ออำนาจอธิปไตยหาได้ไม่ Encyclopedia Britannica (2019) ได้กำหนด อำนาจอธิปไตยในทางกฎหมาย (De jure Sovereignty) หมายถึง สิทธิอำนาจตามกฎหมายที่จะกระทำการหนึ่งใด และในทางปฏิบัติ อำนาจอธิปไตย (De facto Sovereignty) คือ ความสามารถในทางจริงที่จะกระทำการเช่นนั้น ลักษณะของอำนาจอธิปไตย มีลักษณะเด่นชัด 4 ลักษณะ ดังนี้ (เดชชาติ วงศ์โกมลเชษฐ์, 2515)

1. ความเด็ดขาด (absoluteness) เป็นอำนาจสูงสุดของรัฐ ไม่มีอำนาจใดเหนือกว่าอำนาจอธิปไตย

2. การทั่วไป (comprehensiveness) สามารถใช้ครอบคลุมได้ทั่วรัฐ เหนือบุคคลหรือองค์กรยกเว้นแต่เพียงผู้แทนอย่างเป็นทางการของรัฐต่าง ๆ ที่มาเยือนรัฐต้นทางจะอยู่เหนืออำนาจอธิปไตยของรัฐนั้น กระบวนการนี้ถือปฏิบัติกันมาช้านาน

3. ความถาวร (permanence) อำนาจอธิปไตยไม่มีวันสูญหายมีเพียงแต่การเปลี่ยนแปลงภายในรัฐ ตราบเท่าที่รัฐนั้นยังคงอยู่ เปรียบเสมือผู้ใช้อำนาจอธิปไตยภายในรัฐมีความเปลี่ยนแปลง อำนาจมีการเปลี่ยนผ่านแต่มิได้สุญหายไป

4. แบ่งแยกมิได้ (indivisibility) อำนาจอธิปไตยภายในรัฐหนึ่งจะไม่สามารถแบ่งแยกได้ ดังนั้นการแบ่งแยกดินแดนต่าง ๆ ภายในรัฐจะไม่สามารถเกิดขึ้นได้เพราะอำนาจอธิปไตยจะต้องมีหนึ่งเดียว การแบ่งแยกเท่ากับเป็นการทำลายอำนาจอธิปไตยนั้น ๆ

องค์ประกอบทั้ง 4 ประการ เป็นองค์ประกอบพื้นฐานที่ไม่สามารถขาดอันใดอันหนึ่งใด เพื่อให้เห็นความชัดเจนมากยิ่งขึ้น อำนาจอธิปไตยนั้นมีมาตั้งแต่โบราณ ในกรณีของไทยในอดีตอำนาจอธิปไตยเป็นของพระมหากษัตริย์ คือ กษัตริย์เป็นผู้มีอำนาจสูงสุดในการปกครองประเทศ ถือเป็นความเด็ดขาด (absoluteness) อำนาจอธิปไตยยังใช้ได้อย่างเป็นสากล (comprehensiveness) ไม่ว่าจะเป็นที่ใดในโลก การเคารพอำนาจอธิปไตยของประเทศนั้นๆ ถือเป็นเรื่องที่จะต้องปฏิบัติ เช่น การละเมิดอำนาจอธิปไตยที่เกิดขึ้นในประเทศจีน จะต้องใช้กฎหมายของประเทศจีนเป็นตัวตัดสิน กระบวนการทางกฎหมายที่เกิดขึ้นนั้นจะเป็นที่รับทราบกันโดยมิต้องมีลายลักษณ์อักษร นอกจากนี้ อำนาจอธิไตยจะไม่มีวันสูญหาย (permanence) ไม่ว่ารัฐบาลของประเทศนั้นๆ จะถูกโค่นล้มกี่ครั้ง แต่ผู้ที่เข้ามาปกครองใหม่จะต้องมีอำนาจอธิปไตยอยู่ในมือ และสุดท้ายอำนาจอธิปไตยจะไม่สามารถแบ่งแยกได้ ยกตัวอย่างของสหราชอาณาจักรในการแบ่งแยกดินแดนทุกครั้ง ไม่ว่าจะเป็นตั้งแต่สมัยล่าอาณานิคม หรือการแบ่งแยกประเทศไอร์แลน จะเกิดสงครามตามมาเสมอเพราะการแบ่งแยกอาณาเขต (indivisibility) ถือเป็นสิ่งที่ไม่สามารถยอมรับได้

จากการทำความเข้าใจพอสังเขปเกี่ยวกับหลักแนวคิดอำนาจอธิปไตยเบื้องต้นนั้น ทำให้ทราบว่าอำนาจอธิปไตยโดยสรุป คืออำนาจอันสูงสุดเหนือเขตแดนทางกายภาพของรัฐชาตินั้น ๆ แต่อย่างไรก็ตามในโลกปัจจุบันเทคโนโลยี ได้ให้กำเนิดมิติใหม่ หรือมิติทางไซเบอร์ ที่มีลักษณะพิเศษ คือ เป็นมิติที่ไร้ซึ่งพรมแดน ไร้ซึ่งรัฐชาติ ไร้ซึ่งตัวตนที่สมบูรณ์ ดังนั้นการรับมือกับภัยคุกคามที่จะเกิดขึ้นในมิติของไซเบอร์จึงเป็นเรื่องที่ท้ายทายเป็นอย่างมาก

## การใช้อำนาจอธิปไตยในโลกแห่งไซเบอร์

อย่างที่กล่าวมาข้างต้น โลกไซเบอร์เป็นโลกอิสระเหนืออำนาจอธิปไตยเพราะความไร้พรมแดน จึงทำให้เกิดเป็นคำถามขึ้นว่า รัฐจะรับผิดชอบต่อภัยคุกคามที่เกิดขึ้นในโลกไซเบอร์ได้อย่างไร รัฐจะใช้

อำนาจอธิปไตยที่มีอยู่นั้นบนโลกของไซเบอร์ได้หรือไม่โดยเฉพาะการปกป้องโครงสร้างพื้นฐานสำคัญต่าง ๆ เพื่อไม่ให้เกิดผลกระทบต่อประชาชน (Roscini, 2015)

กฎหมายระหว่างประเทศเป็นกฎหมายที่ถูกใช้เมื่อเกิดปัญหากระทบกระทั่งกันระหว่างรัฐชาติ โดยที่ไม่สามารถใช้กฎหมายภายในจัดการได้ กฎหมายต่างประเทศถึงแม้จะถือเป็นเสาหลักในการแก้ปัญหาในระดับสากลแต่ก็ยังไม่สามารถนำมาใช้กับปัญหาที่เกิดขึ้นในโลกแห่งไซเบอร์ได้เพราะลักษณะความพิเศษที่เปลี่ยนแปลงอย่างรวดเร็วเกิดขึ้นภายในโลกไซเบอร์ การขาดซึ่งความเชื่อมโยงทางภูมิศาสตร์ หรือการแบ่งลักษณะไม่ว่าจะเป็นตัวตน ปัจเจกหรือองค์กรในคราเดียวกันนั้นทำให้ปัญหาที่เกิดขึ้นในโลกไซเบอร์มีความซับซ้อนมากขึ้น การกำหนดนิยามของ อธิปไตยไซเบอร์จึงไม่สามารถเกิดขึ้นได้อย่างเป็นเอกฉันท์ในปัจจุบัน (Corn & Taylor, 2017; Brown, 2013) ซึ่งทำให้ปัญหาในการนิยามอธิปไตยไซเบอร์ยังคงเป็นข้อถกเถียงอยู่ ณ ขณะนี้ (Hare, 2009)

ในมุมมองของรัฐนั้น เป็นไปได้ยากที่จะรับผิดชอบภัยคุกคามที่เกิดขึ้นในโลกไซเบอร์ทั้งหมด ไม่ว่าจะเป็นในระดับปัจเจก องค์กร ระดับชาติ หรือระดับนานาชาติ เพราะยังไม่มีเขตแดนที่แน่นอน แต่อย่างไรก็ตามยังมีปรากฏการอ้างถึงการจู่โจมภายใต้ชื่อของรัฐชาติ เช่น ในกรณีของการจู่โจมประเทศเอสโตเนีย โดยประเทศรัสเซียได้อ้างว่าประเทศตนเป็นผู้จู่โจมเพื่อแสดงให้เห็นถึงอำนาจของตนที่มีเหนืออำนาจอธิปไตยรัฐชาติอื่น กรณีแบบนี้มักจะเกิดขึ้นในสภาวะสงครามหรือการสู้รบที่มีขั้วอำนาจอย่างชัดเจน การอ้างว่าตนเป็นฝ่ายโจมตีและการโจมตีนั้นสำเร็จ ถือเป็นการประกาศชัยชนะในการแทรกแซงอำนาจอธิปไตยเหนือรัฐชาติที่เป็นศัตรูได้ และอีกประการหนึ่งยังเป็นการข่มขู่ ยับยั้งไม่ให้อีกประเทศตอบโต้เพราะการแสดงให้เห็นถึงอำนาจที่เหนือกว่าจะเป็นกลยุทธ์ให้อีกประเทศที่ไม่มั่นใจในศักยภาพทางไซเบอร์ของตนอยู่การต่อสู้เพื่อหลีกเลี่ยงความเสียหายที่จะเกิดขึ้น

แต่การอ้างความรับผิดชอบดังกล่าวก็มิได้นำมาซึ่งความจริงที่สามารถเชื่อถือได้ การโจมตีของรัสเซียยังไม่ได้การพิสูจน์จากประเทศเอสโตเนียว่าเป็นการกระทำของรัสเซียอย่างที่กล่าวอ้าง การแทรกแซงอำนาจอธิปไตยของเกาหลีเหนือในสหรัฐอเมริกาก็เช่นกัน ยังไม่สามารถที่จะพิสูจน์ได้ว่าเป็นการกระทำของประเทศเกาหลีเหนืออย่างแท้จริง หรือถึงแม้อาจจะเป็นการกระทำของเกาหลีเหนือก็มิอาจทราบถึงจุดประสงค์ที่แน่นอนว่า อีกฝั่งหนึ่งต้องการประโยชน์อันใด บ้างอาจต้องการผลประโยชน์ ด้านการเงิน บ้างต้องการผลประโยชน์ทางการเมือง หรือไปจนกระทั่งการจู่โจมเพื่อเป็นแค่สัญลักษณ์ในการรุกรานมิได้ต้องการให้เกิดความเสียหายใดๆ การจู่โจมเช่นนี้ยังเกิดขึ้นได้ทั้งในระดับปัจเจก หรือระดับองค์กร ในภาคส่วนเอกชนเป็นผู้กระทำแต่อาศัยการพำนักอยู่ภายใต้รัฐชาตินั้น ๆ สร้างปัญหา ในกรณีนี้จะทำให้เกิดความสับสนกับการใช้อำนาจอธิปไตย เพราะไม่สามารถกล่าวหาได้เลยว่ารัฐเหล่านั้นเป็นผู้กระทำจริง หรือเพียงแค่บุคคลจากรัฐอื่นเข้ามาใช้พื้นที่ทางกายภาพของรัฐนั้นเป็นหน้ากากทางไซเบอร์สร้างความเข้าใจผิดให้เกิดความขัดแย้งขั้นระหว่างสองรัฐ หรือมากกว่านั้น (Liaropoulos, 2013)

**การก่อเกิดของอำนาจอธิปไตยไซเบอร์**

Betts (2011) เสนอแนวคิด อธิปไตยไซเบอร์ คือ การที่รัฐมีอำนาจในการควบคุมข้อมูลข่าวสาร เงินตรา สินค้าและบริการต่าง ๆ ในโลกไซเบอร์ที่เกิดขึ้นภายในอาณาเขตรัฐของตน แต่อย่างไรก็ตาม นักการเมืองและนักวิชาการด้านความมั่นคงปลอดภัยหลากหลายคนไม่เห็นด้วยกับนิยามแนวคิดนี้ (Humber, 2019) เพราะไม่สามารถขีดเส้นจำกัดเขตแดนรัฐชาติภายในโลกของไซเบอร์ได้

แนวคิดของอินเทอร์เน็ต คือ การเชื่อมต่อระหว่างกันแบบไม่จำกัด เน้นย้ำให้คำว่าอธิปไตยไซเบอร์ทำลายความเป็นอำนาจอธิปไตยของรัฐ เพราะเมื่อไหร่ก็ตามที่รัฐสร้าง อธิปไตยไซเบอร์ของตนเองจะทำให้เกิดปรากฏการณ์ตัดขาดทางไซเบอร์กับรัฐอื่น ๆ และจุดเป็นจุดกำเนิดความแตกหักของอินเทอร์เน็ต (Humber, 2019)

ความซับซ้อนของอินเทอร์เน็ตในโลกไซเบอร์ยังมีอีกมากเมื่อต้องประยุกต์ใช้กับทฤษฎีอธิปไตยทางไซเบอร์ โดยการวิเคราะห์นี้จะใช้กฎหมายระหว่างประเทศเป็นพื้นฐาน คำถามที่ว่าโลกไซเบอร์นั้นเป็นส่วนหนึ่งในการบังคับใช้อำนาจอธิปไตย หรือ โลกไซเบอร์นั้นมีอธิปไตยในตนเองมาตั้งแต่ต้น นักวิชาการและผู้เชี่ยวชาญด้านความมั่นคงยังเชื่อว่าโลกไซเบอร์ควรเป็นอิสระจากอำนาจอธิปไตย (Johnson & Post, 1996) โลกไซเบอร์ควรมีกฎหมายเป็นของตนและสามารถบังคับใช้กฎหมายได้อย่างอิสระตามกฎหมายที่ตนกำหนดไว้ ที่มากไปกว่านั้น ลักษณะพิเศษของไซเบอร์ในความไร้พรมแดนกลับตรงข้ามกับคำว่า อธิปไตย ดังนั้น อำนาจในการใช้กฎหมายของโลกไซเบอร์จึงไม่สามารถอยู่เหนือคนและอาณาเขตทางกายภาพได้ในความเป็นจริง (Johnson & Post, 1996)

แต่อย่างไรก็ตาม ผู้สนับสนุนแนวคิดอธิปไตยนำมาใช้ในโลกของไซเบอร์นั้นยังเชื่อว่า หากมีการศึกษาในทุก ๆ แง่มุมของอำนาจอธิปไตยแล้วจะสามารถนำมาใช้ในโลกไซเบอร์ได้อย่างแน่นอน (Tavenner, 2022) เห็นว่ามุมมองทางด้านอธิปไตยนั้นมีหลายมิติไม่เพียงแต่ในมุมทางกายภาพเท่านั้น แต่ยังแบ่งพื้นที่ของรัฐชาติกับการปฏิสัมพันธ์ของมนุษย์ที่เกิดขึ้นด้วย ดังนั้นการสร้างอธิปไตยทางไซเบอร์จึงเป็นการกระทำที่รัฐมีปฏิสัมพันธ์กับประชากรในรัฐด้วยกรอบทางกฎหมายที่ครอบคลุมพื้นที่มิติทางไซเบอร์ Joel (1996) อ้างว่า ผู้ที่มีส่วนร่วมในโลกอินเทอร์เน็ตจะเป็นผู้ที่ให้ความเห็นชอบกับการเป็นสมาชิกของกลุ่ม ๆ นั้น และยังให้สิทธิทางรัฐธรรมนูญผ่านทางเงื่อนไขการใช้บริการ

ประเทศไทยเป็นประเทศหนึ่งที่ประสบกับปัญหาการอำนาจอธิปไตยในโลกไซเบอร์ โดยเฉพาะการโจมตีจากตัวกระทำที่ไม่ใช่รัฐ เป็นผลทำให้ไม่ทราบถึงจุดประสงค์ของการโจมตีนั้น ๆ ขณะเดียวกันการโจมตีที่มีมากขึ้นทำให้เจ้าหน้าที่มีภาระงานที่ล้นมือ จนไม่สามารถหาหลักฐานในการจับกุมผู้กระทำความผิดทางไซเบอร์ได้หมด นอกจากจะเกิดผลเสียในระดับปัจเจกแล้ว การเกิดขึ้นของสงครามไซเบอร์ที่มีผลกระทบต่อผู้เสียหายยังไม่อาจนำ กฎหมายมนุษยธรรม มาใช้เอาผิดกับรัฐผู้กระทำได้

**แนวคิดอธิปไตยทางไซเบอร์ในต่างประเทศ**

**1. สาธารณรัฐประชาชนจีน**

รัฐบาลจีนให้ความสำคัญเป็นอย่างมากกับการแสดงถึงอำนาจอธิปไตยทางไซเบอร์ การแสดงถึงอำนาจอธิปไตยทางไซเบอร์นั้นเริ่มต้นจากการควบคุมเรื่องราว ข้อมูลสื่อสารต่าง ๆ ในประเทศให้เป็นระบบปิดอย่างชัดเจน มีจุดยืนโดยที่ประเทศอื่น ๆ ไม่สามารถใช้อำนาจอธิปไตยของตนผ่านเข้ามาได้ การควบคุมข้อมูลข่าวสารนี้จะเน้นไปยังข้อมูลที่เป็นภัยต่อความมั่นคงของประเทศ รัฐชาติ รวมถึงพรรคคอมมิวนิสต์ แนวคิดอำนาจอธิปไตยของรัฐบาลจีนสามารถแยกออกได้เป็น 2 แนวคิด (Lindsay, 2015)

– ยับยั้งขอมูลข่าวสารที่เป็นภัย

ข้อมูลข่าวสารต่างๆ ที่เป็นภัยต่อความมั่นคงของรัฐบาลจีน จะถูกยับยั้งโดยทันทีเมื่อผ่านเข้ามาสู่ระบบอินเทอร์เน็ต รวมไปถึงการควบคุมไม่ให้ประชาชนภายในประเทศของตนแสดงความคิดเห็นที่เป็นภัยต่อความมั่นคงของชาติ เป็นการรักษาความมั่นคงของอำนาจอธิปไตยทั้งภายในและภายนอกประเทศของตน

– ยกระดับธรรมาภิบาลของระบบอินเทอร์เน็ต

นโยบายการยกระดับธรรมาภิบาลของการใช้อินเทอร์เน็ตภายในอธิปไตยของรัฐชาติจีน รวมถึงการใช้อินเทอร์เน็ตในการศึกษา การค้าขาย บริษัทเอกชน หรือการประชุมระหว่างประเทศ เช่น องค์กรสหประชาชาติ การรวบอำนาจทั้งหมดนี้ถือเป็นการเปลี่ยนผ่านจากระดับปัจเจกและองค์กรไปสู่รัฐเพียงหนึ่งเดียว นครปักกิ่ง เมืองหลวงของประเทศจีน มีนโยบายที่เป็นแรงผลักดันสำคัญที่จะทำให้ธรรมา–ภิบาลในโลกไซเบอร์ของจีน อยู่คงอยู่สม่ำเสมอและต่อเนื่อง (Segal, 2020)

**2. สหพันธรัฐรัสเซีย**

รัฐบาลของรัสเซีย มีมุมมองแนวคิดในเรื่องอธิปไตยทางไซเบอร์เช่นเดียวกันกับประเทศจีน โดยที่รัฐบาลจะเป็นผู้ใช้อำนาจอธิปไตยในโลกไซเบอร์ ควบคุมการเปลี่ยนผ่านข้อมูลข่าวสารทั้งหมด อำนาจอธิปไตยทางไซเบอร์กำลังมีอิทธิพลเหนือการใช้อินเทอร์เน็ตภายในประเทศทั้งหมด แนวคิดอธิปไตยทางไซเบอร์ของรัสเซียถึงแม้จะเหมือนกับประเทศจีน แต่ก็ยังแตกต่างในเรื่องของการกำหนดคำนิยามและการใช้อำนาจเผด็จการผ่านโลกดิจิทัล นั่นหมายความว่า รัฐบาลสามารถคุกคามประชาชนผ่านการควบคุมข้อมูลในอินเทอร์เน็ต และโดดเดี่ยวประชากรจากโลกข้อมูลข่าวสารภายนอก แนวคิดนี้ใช้ชื่อว่า Kremlin’s cyber isolationist (Tavenner, 2022) แนวคิดอธิปไตยทางไซเบอร์ของรัฐบาลรัสเซียในช่วงแรกมีความเข้มงวดน้อยกว่าแนวคิดของรัฐบาลจีน โดยที่รัสเซียจะมุ่งปิดกั้นการติดต่อสื่อสารทางอินเทอร์เน็ตในโลกไซเบอร์ในรูปแบบของออฟไลน์เท่านั้น แต่หลังจากปี 2012 เมื่อรัสเซียประสบกับการประท้วงรัฐบาลครั้งใหญ่จากประชาชนที่ต้องการหลุดจากการคุกคาม จนทำให้รัฐบาลขาดเสถียรภาพ บทเรียนครั้งนั้นทำให้รัฐบาลรัสเซียเพิ่มขีดความสามารถในการใช้อำนาจอธิปไตยทางไซเบอร์ ปิดกั้นการติดต่อสื่อสารและคุกคามความเป็นส่วนตัวของประชาชนเทียบเท่ารัฐบาลจีน

มากไปกว่านั้นโครงสร้างพื้นฐานสำคัญทางอินเทอร์เน็ตของรัสเซีย มีความเหมือนกับต้นแบบของรัฐบาลจีน เทียบเท่าเป็น Proxy model (Weber, 2020) ทั้งจีนและรัสเซียนั้นเห็นพ้องต้องกันว่า

อำนาจอธิปไตยเหนือไซเบอร์จำเป็นจะต้องควบคุมแนวคิดเสรีประชาธิปไตยในการแลกเปลี่ยนสื่อสารข้อมูลสารสนเทศ จึงทำให้การควบคุมดังกล่าวของรัสเซีย ออกเป็นมติเห็นชอบด้วยกฎหมายเมื่อปี 2018 โดยรัสเซียได้เสนอเรื่องเข้าที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติ เน้นย้ำเรื่องการควบคุมข่าวสารจากภายนอก และการไม่แทรกแซงกิจการภายประเทศของรัสเซีย นักวิชาการบางกลุ่มเห็นว่านโยบายที่รัสเซียกำลังจะใช้นั้นทำเพื่อปกปิดการละเมิดสิทธิมนุษยชนที่รัสเซียได้กระทำไว้กับประชาชน

หลังจากที่รัสเซียได้ยื่นเสนอมติดังกล่าว ที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติ จึงได้มีการจัดตั้งคณะทำงานแบบเปิดว่าด้วยความปลอดภัยทางไซเบอร์ (Open-ended Working Group: OEWG) on the Topic of Cybersecurity เพื่อดำเนินการคู่ขนานกับกลุ่มผู้เชี่ยวชาญภาครัฐของสหประชาชาติ (UN Group of Governmental Experts: GGE) ที่มีอยู่แล้ว เพื่ออภิปรายเกี่ยวกับบรรทัดฐานทางไซเบอร์ จึงเป็นสาเหตุให้รัสเซียใช้ OEWG เป็นเวทีสำหรับการตีความการกำกับดูแลอินเทอร์เน็ตเพื่อให้สอดคล้องกับนโยบายของรัฐที่ออกมา

เนื่องจากจีนและรัสเซียมีความคล้ายคลึงในเรื่องของแนวคิดการปกครองและการเมือง จึงทำให้ในเวทีพหุภาคีหลายครั้ง จีนและรัสเซียจะแสดงภาพอำนาจอธิปไตยทางไซเบอร์เป็นสิ่งเดียวกันอย่างเป็นเอกฉันท์ ทั้งสองประเทศให้คำแนะนำบนเวทีพหุภาคี เรื่องของการใช้อำนาจอธิปไตยทางไซเบอร์อย่างจริงจัง แต่ไม่ได้นำเสนอนโยบายเฉพาะเจาะจงว่าจะดำเนินการดังกล่าวอย่างไร โดยส่วนใหญ่จะเป็นตัวเลือกการใช้เครื่องมือปราบปรามต่าง ๆ ที่เหมาะกับบริบทของแต่ละประเทศ ตั้งแต่กฎหมายการเซ็นเซอร์ที่เข้มงวดไปจนถึงการปิดเครือข่ายอินเทอร์เน็ต

**3. สหราชอาณาจักร**

จุดยืนของสหราชอาณาจักรนั้นยังไม่สามารถสรุปอย่างเป็นมติเอกฉันท์ได้ในเรื่องอธิปไตยทางไซเบอร์ มุมมองส่วนใหญ่ของสหราชอาณาจักรที่มีต่ออธิปไตยทางไซเบอร์นั้น คือการป้องกันยับยั้ง ไม่ให้เกิดภัยคุกคามทางไซเบอร์กับประชาชน ไม่ว่าจะเป็นการหลอกลวง การข่มขู่ การเรียกค่าไถ่ออนไลน์ รัฐบาลมีกฎหมายที่ชัดเจนในการจัดการกับผู้กระทำความผิด และได้รับความร่วมมือกับภาคเอกชนเป็นอย่างดี รัฐบาลกำหนดนโยบายการรับมือภัยคุกคามทางไซเบอร์ ผ่าน National Cyber Security Program โดยมีงบประมาณกว่า 650 ล้านปอนด์ ภายในเวลา 4 ปี นอกจากนี้ยังให้ความร่วมมือกับนานาชาติ เพื่อสร้างอำนาจอธิปไตยทางไซเบอร์ในรูปแบบที่สอดคล้องกับการปกครองของตน แต่ยังคงประสิทธิภาพของเทคโนโลยีเพื่อให้สามารถป้องกันภัยคุกคาม ตั้งแต่เล็กน้อยถึงขนาดใหญ่ให้ได้มากที่สุด

ใน London Conference on Cyberspace ปีล่าสุด รัฐบาลได้ให้ความร่วมมือกำหนดข้อตกลงระหว่างประเทศ ในชื่อ ‘Rules of the Road’ ในการใช้ประโยชน์ในโลกของไซเบอร์เป็นการแลกเปลี่ยนข้อมูลความมั่นคงปลอดภัยทางไซเบอร์กับภาคเอกชนและประเทศต่าง ๆ ที่มีสภาพแวดล้อมการกำหนดนิยามอธิปไตยทางไซเบอร์ในทิศทางเดียวกัน นอกจากนี้สหราชอาณาจักร ยังให้อำนาจสูงสุด

แก่รัฐบาลในการจัดการภัยคุกคามทางไซเบอร์และอาชญากรรมไซเบอร์ รวมถึงการสนับสนุนการวิจัยแก้ปัญหาเรื่องความตระหนักรู้ของประชาชน (The Cabinet Office, 2020)

**4. ประเทศไทย**

กระแสการประชาสัมพันธ์ Digital Government กำลังเป็นที่จับตามองในประเทศไทย นอกจากการบริหารงานภาครัฐแบบดิจิทัลแล้ว รัฐบาลไทยยังสนับสนุนความเป็นดิจิทัลในทุก ๆ มิติ ดังนั้นการตระหนักถึงการใช้อำนาจอธิปไตยทางไซเบอร์นั้น จึงเป็นหัวข้อที่ท้าทายกับสังคมไทย ประเทศไทยให้ความสำคัญเป็นอย่างมากสำหรับการให้เสรีภาพในการแสดงความคิดเห็นที่ไม่กระทบต่อความมั่นคงของชาติ Chachavalpongpun (2021) กล่าวไว้ว่า อำนาจอธิปไตยของไทยไม่ได้จำกัดอยู่ภายใต้เขตแดนทางกายภาพอีกแต่ไป แต่กลับขยายเข้าสู่โลกไซเบอร์อย่างชัดเจน ดังที่ได้เห็นในการจับกุมหลายคดีทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงของประเทศไทย อาจสรุปได้ว่า “อำนาจอธิปไตยทางไซเบอร์” มีความสำคัญอย่างยิ่งในการปกป้องประเทศจากภัยคุกคามทางไซเบอร์

การใช้อำนาจอธิปไตยไซเบอร์ของจีน รัสเซีย สหราชอาณาจักร และไทย ถึงแม้จะมีความแตกต่างกันในส่วนของแนวคิดทางการเมือง โดยประเทศเสรีประชาธิปไตยจะให้ความสำคัญในเรื่องการปกป้องความเป็นส่วนตัวของประชาชน แต่ก็มิได้ละเลยถึงการป้องกันการแทรกแซงจากภายนอก เช่น การมีกฎหมายจับกุมผู้กระทำความผิดทางไซเบอร์อันก่อให้เกิดความเสียหายในชาติ อาศัยหลักการความเด็ดขาด (absoluteness) อันเป็นอำนาจสูงสุดของรัฐโดยรัฐอื่นจะไม่สามารถละเมิดได้ และการใช้อำนาจนั้นมีผลบังคับใช้ทั่วอาณาเขตของรัฐ สอดคล้องกับหลักการความทั่วไป (comprehensiveness) ของอำนาจอธิปไตยที่จะไม่มีข้อยกเว้นใด ๆ จากการรุกราน สำหรับประเทศที่มีความคิดทางการเมืองแบบสังคมนิยม ความมั่นคงของประเทศคือสิ่งสำคัญที่สุด สิทธิ์ในการเข้าถึงข้อมูลของประชาชนจึงเป็นสิ่งรองลงมา ไม่ว่าจะเป็น จีน หรือ รัสเซีย ถึงมีจะมีการเปลี่ยนแปลงการปกครองครั้งใหญ่เกิดขึ้นในอดีตแต่อำนาจอธิปไตยของรัฐมิเคยหายไป เฉกเช่นอำนาจอธิปไตยไซเบอร์ก็จะยังคงอยู่กับรัฐ รอการเปลี่ยนผ่านอำนาจของกลุ่มคนเท่านั้น หลักการนี้สอดคล้องกับความถาวร (permanence) ของอำนาจอธิปไตย และสิ่งที่สำคัญที่สุดคือการคำนึงถึงอำนาจอธิปไตยที่ไม่สามารถแบ่งแยกได้ (indivisibility) ถึงแม้ว่าอำนาจอธิปไตยไซเบอร์จะเป็นสิ่งนามธรรมต่างจากเขตแดน แต่อำนาจอธิปไตยไซเบอร์ยังต้องอาศัยความสำคัญทางกายภาพในการรักษาอำนาจของประเทศนั้น ๆ

สำหรับการใช้อำนาจอธิปไตยไซเบอร์ในบริบทของประเทศไทยนั้น งานวิจัยเรื่อง การรับมือการก่อการร้ายไซเบอร์ของภาครัฐไทย (Petchkla, 2022) นั้น พบว่าทั้งภาครัฐและภาคเอกชนมีอำนาจในการจัดการภัยคุกคามเป็นของตัวเอง โดยเฉพาะในภาครัฐได้ให้อำนาจกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหลักในการกำกับดูแล แต่อย่างไรก็ตาม พบว่าอำนาจในการจับกุมภัยคุกคามทางไซเบอร์ยังกระจายไปยังหน่วยงานความมั่นคงอื่น ๆ ไม่ว่าจะเป็น

สภาความมั่นคงแห่งชาติ, สำนักงานตำรวจแห่งชาติ และกองทัพไทย การกระจายอำนาจเหล่านี้มีส่วนสำคัญในการรักษาอำนาจอธิปไตยทางไซเบอร์ของรัฐ ถึงแม้รัฐจะออกกฎหมายภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ มีผลบังคับใช้จริงทางกฎหมาย แต่ก็มิอาจถือเป็นอำนาจอธิปไตยได้ เพราะมิได้มีหนึ่งเดียวอย่างชัดเจน และนอกจากนี้อำนาจดังกล่าวยังไม่มีความถาวร สามารถเปลี่ยนแปลงได้ตามขั้วอำนาจของผู้ปกครอง

**ข้อโต้แย้งของอธิปไตยทางไซเบอร์**

ปัจจุบันนี้ การแพร่หลายของกิจกรรมภายใต้โลกแห่งไซเบอร์ยิ่งซับซ้อน และยากที่จะยับยั้งด้วยกฎหมายต่างๆ ไม่ว่าจะเป็นกฎหมายที่ออกภายใต้อำนาจรัฐ หรือกฎหมายระหว่างประเทศก็ไม่สามารถที่จะใช้ผูกพันได้อย่างครอบคลุม ทั้งนี้เนื่องจากลักษณะพิเศษของไซเบอร์ที่ไร้ซึ่งพรมแดนทางกายภาพ จึงไม่สามารถคาดคะเนถึงอำนาจได้ว่ากิจกรรรมที่เกิดขึ้นนั้นเป็นความรับผิดชอบของรัฐใด (Jamnejad & Wood, 2009) และข้อจำกัดนี้ถือเป็นข้อจำกัดที่สำคัญยิ่งในการขัดขวางไม่ให้อำนาจอธิปไตยทางไซเบอร์เกิดขึ้นจริงอย่างสมบูรณ์ได้

กฎหลักของอำนาจอธิปไตย โดยเฉพาะอำนาจทางกายภาพ ควรจะต้องเป็นปัจจัยในหลักรองรับกิจกรรมหรือปฏิบัติการต่าง ๆ ในโลกไซเบอร์ทุก ๆ กิจกรรม ดังนั้นการขาดซึ่งปัจจัยทางกายภาพจึงไม่สามารถทำให้เกิดการสร้างมาตรฐานที่สมบูรณ์แบบ ควบคุมกิจกรรมทางไซเบอร์ที่เกิดขึ้นภายในรัฐใดรัฐหนึ่ง และส่งผลต่อโครงสร้างพื้นฐานทางไซเบอร์ของรัฐใดรัฐหนึ่ง เพราะการกระทำที่อยู่ภายในโลกของไซเบอร์ไม่สามารถที่จะบังคับใช้กฎหมายแทรกแซงทางกายภาพของรัฐทั้งสองได้ ดังนั้น อธิปไตยทางไซเบอร์จึงเปรียบเสมือน อธิปไตยคู่ขนานกับโลกแห่งความเป็นจริง (Jamnejad & Wood, 2009)

แต่อย่างไรก็ตาม ข้อโต้แย้งของอธิปไตยทางไซเบอร์ก็มิได้จบลงโดยง่าย โดย Egan (2016) ผู้เขียนหนังสือเรื่อง International Law and Stability in Cyberspace ให้ความเห็นว่า การใช้กฎหมายระหว่างประเทศผ่านอำนาจอธิปไตยในโลกของไซเบอร์สามารถเกิดขึ้นได้ สังเกตได้จากตัวอย่างปฏิบัติการของกลุ่มผู้ก่อการร้าย ISIS เนื่องจากคุณลักษณะการกระจายตัวอย่างไร้พรมแดนของโลกไซเบอร์ ทำให้ปฏิบัติการของกลุ่มผู้ก่อการร้าย ISIS ที่มุ่งเป้าไปยังสาธารณูปโภคสำคัญต่าง ๆ ของฝ่ายตรงข้าม จึงเป็นเรื่องง่ายที่จะโจมตี แต่สำหรับประเทศที่ตกเป็นกลุ่มเป้าหมายนั้นจะต้องใช้ข้ออ้างของอำนาจอธิปไตยในการปกป้องสาธารณูปโภคสำคัญของประเทศตน ด้วยเหตุนี้อำนาจอธิปไตยในโลกแห่งความจริ งจึงไม่อาจจะแยกขาดกับโลกไซเบอร์ได้

ISIS ที่รู้จักในนามกลุ่มองค์กรก่อการร้ายข้ามชาติ มีสื่อสังคมออนไลน์มากมายและใช้อินเทอร์เน็ตเป็นส่วนหลักในการสื่อสารกับสมาชิกและผู้สนับสนุน นอกจากนี้ยังใช้ประโยชน์จากอินเทอร์เน็ตในการรับสมัครบุคคล เพื่อจุดประสงค์ในการก่อการร้ายและส่งเสริมกิจกรรมก่อความไม่สงบไปยังผู้ก่อการร้ายรุ่นใหม่ ให้มีแนวคิดเดียวกันไปทั่วโลกโดยไร้พรมแดน มากไปกว่านั้น ISIS ยังสร้างฐานไซเบอร์ที่มีชื่อว่า Cyber Caliphate ดำเนินการทางไซเบอร์ที่เป็นอันตรายผ่านทางอินเทอร์เน็ต

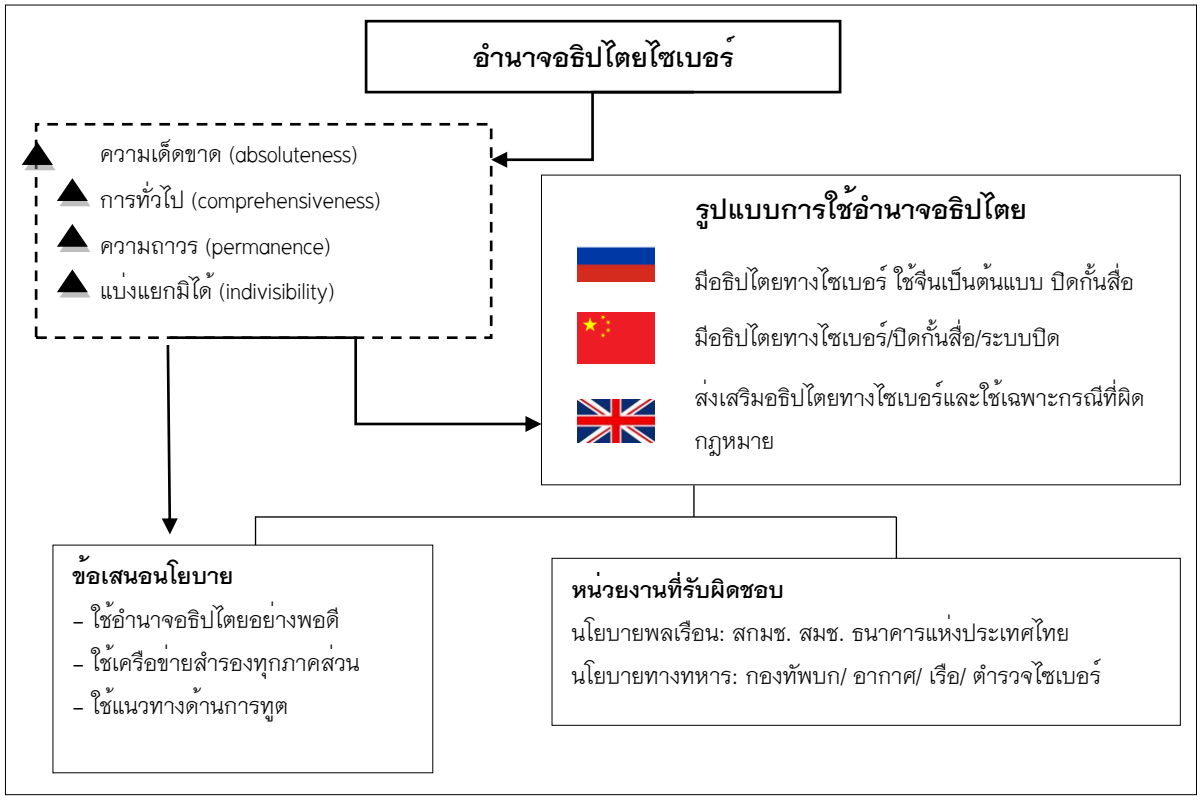
(Irshaid, 2016) ไม่มีประเทศใดสามารถล่วงรู้ได้ว่ากลุ่ม ISIS จะใช้อินเทอร์เน็ตดำเนินการบนเซิร์ฟเวอร์และโครงสร้างพื้นฐานของตนที่ไหนและเมื่อใด หรือถ้าหากมีระบบตรวจจับที่ดีก็สามารถสกัด ยับยั้งได้ทัน แต่ก็ไม่มีเครื่องมือใด ๆ ที่จะสามารถป้องกันได้อย่างเต็มที่และสมบูรณ์ การกระทำของกลุ่ม ISIS นั้นเป็นการละเมิดอธิปไตยของรัฐชาติต่าง ๆ โดยที่ปราศจากการตระหนักรู้ผ่านการใช้อินเทอร์เน็ต

หากการละเมิดอำนาจอธิปไตยทางไซเบอร์ของกลุ่ม ISIS ดังกล่าวนั้นสามารถระบุได้ว่าเป็นการกระทำที่ผิดกฎหมาย และละเมิดกฎหมายของรัฐได้อย่างแท้จริง รัฐดังกล่าวสามารถส่งต่อเรื่องให้คณะมนตรีความมั่นคง พิจารณาดำเนินการในระดับสากล และเป็นผลดีมากกว่าจะกำหนดให้อำนาจอธิปไตยทางไซเบอร์เกิดขึ้นจริง โดยอาจเริ่มใช้ในเขตพื้นที่ของสงครามเป็นตัวแบบ เพราะจะเห็นได้ชัดถึงผู้กระทำที่เป็นฝ่ายตรงข้าม (Egan, 2016)

การคำนึงถึงการแทรกแซงจากรัฐอื่นเพื่อปกป้องและยับยั้งกลุ่มก่อการร้าย ISIS นั้น ยังไม่มีมาตรการใด ๆ กีดกันรัฐดังกล่าวไม่ให้เข้ามามีส่วนร่วม เช่น สหรัฐอเมริกา พยายามที่จะเข้ามาแทรกแซงทางไซเบอร์เพื่อช่วยเหลือรัฐที่ตกเป็นเป้าหมายถูกกลุ่ม ISIS โจมตี ถึงแม้อาจจะยังไม่ได้รับความยินยอมจากรัฐนั้น ๆ แต่การกระทำของสหรัฐฯ จะไม่ถือว่าผิดกฎแห่งการแทรกแซงอำนาจอธิปไตย เว้นแต่การกระทำดังกล่าวเป็นการแทรกแซงที่ใช้กำลังที่ต้องห้าม (Schmitt, 2016) กลยุทธ์ส่วนใหญ่ที่สหรัฐฯ ใช้ในการยับยั้งกลุ่ม ISIS คือ การมุ่งโจมตีแหล่งเงินทุนของกลุ่มก่อการร้าย การปิดบัญชี หรือหยุดการเคลื่อนไหวในบัญชีของผู้ก่อการร้ายผ่านอินเทอร์เน็ตเป็นธุรกรรมทางการเงิน ซึ่งในบางกรณีสหรัฐฯ จำเป็นจะต้องขอความยินยอมจากรัฐปลายทางหรือรัฐที่ถูกโจมตีก่อน แต่อย่างไรก็ตาม ยังไม่มีกฎระเบียบหรือขั้นตอนใดทางกฎหมายที่จะต้องต้องปฏิบัติตามอย่างเคร่งครัด และในขณะเดียวกันรัฐปลายทางหรือรัฐที่ถูกโจมตี จะสามารถยับยั้งการกระทำของสหรัฐฯ ได้หากการกระทำของสหรัฐฯ ละเมิดต่อกฎหมายภายในประเทศของตน โดยรัฐดังกล่าวจะใช้อำนาจอธิปไตยภายในรัฐ แทนที่การใช้อำนาจจากกฎหมายระหว่างประเทศ (Schmitt, 2016)

นอกจากกลุ่ม ISIS และกลุ่มก่อการร้ายอื่น ๆ รัฐชาติเอง จะต้องใช้อินเทอร์เน็ตและสิ่งอำนวยความสะดวกทางไซเบอร์เป็นอาวุธต่อไปเพื่อยุติการมุ่งร้าย และตอบโต้กลุ่มผู้ไม่หวังดี ประสิทธิภาพในการใช้อาวุธเหล่านี้จะมีความสำคัญต่อความมั่นคงของประเทศและระหว่างประเทศ รัฐต้องประกันว่าการตอบสนองใด ๆ เป็นไปตามกฎหมายระหว่างประเทศ และคำนึงถึงอำนาจอธิปไตยของแต่ละรัฐ กฎหมายระหว่างประเทศ และแนวคิดเรื่องอำนาจอธิปไตยที่เข้าใจและนำไปใช้อย่างเหมาะสม ไม่ได้กีดกันกิจกรรมทางไซเบอร์ในระดับบุคคลและส่วนรวม แต่จะพุ่งเป้าไปที่ผู้ก่อการร้ายและพร้อมปกป้องโครงสร้างพื้นฐานที่กำลังตกเป็นเป้าหมายของการก่อการร้ายอยู่

## การอภิปรายผลและองค์ความรู้ที่ได้รับ




**ภาพที่ 1** องค์ความรู้ที่ได้รับ

จากการวิเคราะห์อำนาจอธิปไตย ต้องประกอบไปด้วยความเด็ดขาด (absoluteness) การทั่วไป (comprehensiveness) ความถาวร (permanence) และแบ่งแยกมิได้ (indivisibility) คำนิยามเหล่านี้จะถูกนำมาประยุกต์ใช้ในการกำหนดรูปแบบของอำนาจอธิปไตยแต่ละประเทศ โดยจะต้องคำนึงถึงจุดยืนทางการเมืองของประเทศนั้น ๆ ด้วย สำหรับประเทศไทยนั้นถึงแม้จะมีกฎหมายไซเบอร์บังคับใช้จริง แต่ก็ไม่ได้ระบุความต้องการที่ชัดเจนว่าจะต้องการให้รูปแบบการใช้อำนาจอธิปไตยไซเบอร์เป็นไปในรูปแบบใด บทความนี้จึงเสนอข้อคิดเห็นในส่วนท้ายเพื่อสามารถกำหนดเป็นแนวทางนโยบายในอนาคตได้ว่า การใช้อำนาจอธิปไตยของไทย ควรมีการศึกษาถึงช่องว่างระหว่างบริบทความเป็นจริง กับสิ่งที่เกิดขึ้นในโลกไซเบอร์ ว่ามีความแตกต่างกันอย่างไร และการใช้อำนาจอธิปไตยนั้นไม่ควรใช้มากไปหรือน้อยไป แต่ควรจะมีจุดยืนตามระบบการปกครองของตนเองในโลกความจริง พร้อมทั้งเสนอแนวทางแก้ปัญหาการใช้การทูตในการต่อรองเจรจา และแสดงออกถึงความคิดเห็น และจุดยืนของตนในเวทีโลกมากขึ้น โดยใช้อำนาจผ่านทางทั้งหน่วยงานที่เป็นระบบของพลเรือนและหน่วยงานที่เป็นระบบของฝ่ายทหาร

## สรุป

สรุปในภาพรวมของบทความ รวบรวมแนวคิดเรื่องอำนาจอธิปไตยซึ่งเป็นพื้นฐานในการวิเคราะห์อำนาจอธิปไตยทางไซเบอร์ไว้ในส่วนแรก โดยพบว่าลักษณะพิเศษบางอย่างของโลกไซเบอร์เป็นอุปสรรคต่อการกำหนดเขตแดนอธิปไตย ไม่ว่าจะเป็นการเปลี่ยนแปลงอย่างรวดเร็ว ความไร้ตัวตน ไร้ซึ่งพรมแดน จะไม่สามารถกำหนดได้ว่าอำนาจอธิปไตยที่แท้จริงของแต่ละรัฐชาตินั้นเป็นอย่างไร และจากอุปสรรคดังกล่าวจึงเป็นที่มาของการค้นคว้า พัฒนาคำนิยามในการใช้อำนาจอธิปไตยไซเบอร์ของรัฐให้สอดคล้องตามยุคสมัยโดย รัฐจะต้องใช้อำนาจอธิปไตยอย่างพอดี ไม่มากเกินที่จะละเมิดความเป็นส่วนตัวของประชาชน และไม่น้อยเกินไปเพื่อที่จะยังคงซึ่งอำนาจรัฐไว้แม้แต่ในโลกที่ไร้พรมแดน การใช้อำนาจอธิปไตยในโลกไซเบอร์ที่แท้จริงจะผ่านการกำหนดกฎหมายและนโยบายต่าง ๆ ที่ไม่ให้รัฐอื่นสามารถแทรกแซงรัฐของตนได้ แต่เมื่อใดที่มีการแทรกแซง รัฐจำเป็นจะต้องมี เครือข่ายสำรองทุกภาคส่วนเพื่อรับมือการโจมตีทางไซเบอร์ที่เกิดขึ้น ในกรณีที่สัญญาณอินเทอร์เน็ตของรัฐถูกโจมตีจากภายนอก เครือข่ายสำรองจากภาคเอกชนจะถูกนำมาใช้แทนทันทีเพื่อไม่ให้เกิดความชะงักงันในการใช้ชีวิตของประชาชน และสุดท้ายการใช้แนวทางด้านการทูตเพื่อเป็นเครื่องมือในการต่อรองในเวทีโลก บทความนี้ได้ยกตัวอย่างของประเทศจีนและประเทศรัสเซีย ที่มีความต้องการในการสนับสนุนการใช้อำนาจอธิปไตยในโลกไซเบอร์อย่างชัดเจน เพราะไม่ต้องการให้ประเทศอื่น ๆ เข้ามาละเมิดอำนาจของรัฐตนได้ ทั้งสองประเทศได้เสนอแนวคิดผ่านองค์กรสหประชาชาติ เพื่อแสดงจุดยืนของตนอย่างชัดเจนเพื่อไม่ให้รัฐอื่นเข้ามาแทรกแซง ประการสุดท้าย การกำหนดนโยบายสอดคล้องกับรูปแบบการปกครองในโลกความเป็นจริงที่คู่ขนาดกับโลกไซเบอร์ จึงมีแนวโน้มว่าประเทศเสรีประชาธิปไตยอย่าง สหรัฐอเมริกา หรือสหราชอาณาจักร จะมีท่าทีที่จะกำหนดอำนาจอธิปไตยทางไซเบอร์ของตนอิงตามรูปแบบการปกครองทางการเมือง เคารพสิทธิมนุษยชนของประชาชนในประเทศตน และพยายามจะใช้วิธีทางการทูตในการแก้ไขปัญหาการละเมิดอำนาจอธิปไตยของตน

## ข้อเสนอแนะ

### ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

**– อธิปไตยทางไซเบอร์ที่มากเกินพอดี**

จากกรณีของประเทศจีน ที่ได้กำหนดนโยบายทางอินเทอร์เน็ตต่อต้านสื่อสังคมออนไลน์ต่างจากประเทศสหรัฐอเมริกา ไม่ว่าจะเป็น Google Facebook Instagram หรือ WhatsApp เพราะเกรงว่าสื่อสังคมออนไลน์เหล่านี้จะเป็นเครื่องมือให้สหรัฐล่วงรู้ข้อมูลความลับหรือละเมิดอธิปไตยของประเทศตน แต่ผลกระทบของนโยบายนี้ทำให้ประชาชนในประเทศนั้นไม่สามารถติดต่อสื่อสารกับสังคมภายนอกได้ และที่สำคัญไปกว่านั้นการใช้สื่อออนไลน์ที่รัฐบาลตนเองสร้างขึ้นกลับละเมิดความเป็นส่วนตัวของ

ประชาชนโดยใช้เหตุผลด้านความมั่นคงปลอดภัยเป็นข้ออ้าง การกระทำของรัฐบาลจีนจึงสร้างความไม่พอใจให้ทั้งภายในและภายนอกประเทศ โดยทั้งนี้ยังมีการรณรงค์จากประเทศสหรัฐฯ ที่พยายามจะโน้มน้าวประเทศอื่น ๆ ให้คว่ำบาตรสินค้าจีน เพื่อเป็นการตอบโต้ต่อนโยบายดังกล่าวและแบนโทรศัพท์มือถือจากสัญญาณเครือข่าย 5G และบริษัทสัญชาติอเมริกันอย่าง Apple ยังมีนโยบายลบแอปพลิเคชันออกจาก App Store (Sherman, 2019) การกำหนดเขตแดนอธิปไตยทางไซเบอร์ที่ชัดเจนของประเทศจีน สามารถถอดบทเรียนให้กับประเทศไทยในอนาคตได้ว่า การแบ่งเส้นเขตแดนอธิปไตยที่ชัดเจนและเข้มงวดเกินไปทางไซเบอร์ จะทำให้เกิดการตอบโต้จากประเทศอื่น ๆ และคนภายในประเทศที่ได้รับผลกระทบ

ถึงแม้ประเทศจีนจะเป็นประเทศมหาอำนาจ แต่กรณีการออกนโยบายเหล่านี้สามารถมาประยุกต์ใช้กับประเทศไทยได้ ไม่ว่าจะเป็นแนวคิด Single Gateway ที่เคยเกิดขึ้นในอดีต จนเป็นเหตุให้เกิดความไม่พอใจของคนภายในประเทศ ร่วมกันตอบโต้รัฐบาลไทยผ่านการโจมตีเว็บไซต์ด้วยแบบ DDOS Attack กับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) ในขณะนั้นล่มและไม่สามารถใช้การได้ การแบ่งเส้นอธิปไตยทางไซเบอร์ที่เข้มข้นเกินความพอดี อาจจะเป็นผลให้เกิดความขัดแย้งตามมาภายหลัง

**– สนับสนุนอธิปไตยทางไซเบอร์ในเวทีสากล**

การวางนโยบายจำเป็นจะต้องประกอบไปด้วยปัจจัยตั้งต้นที่เหมาะสม ในกรณีนี้การแสดงออกให้เห็นว่าประเทศไทยมิได้ละเลยการสร้างโลกไซเบอร์ที่โปร่งใสต่อสายตานานาชาตินั้น รัฐบาลจะต้องสนับสนุนการกำหนดอธิปไตยทางไซเบอร์ผ่านองค์ที่ชื่อถือได้ ไม่ว่าจะเป็น United Nations Internet Governance Forum, Asia Pacific Computer Emergency Response Team (AP CERT), Cooperative Cyber Defense and Center of Excellence (CCDCOE) หรือภาคส่วนเอกชน รวมทั้งบังคับใช้คู่มือ Tallinn Manual 2.0 ให้สอดคล้องกับนโยบายด้านไซเบอร์

**– นำวิธีทางการทูตมาปรับใช้ในการต่อรองทางไซเบอร์**

การทูตถูกนำมาใช้เป็นวิธีแก้ปัญหาในหลายยุคหลายสมัยและได้ผลอย่างมีประสิทธิภาพ โดยปราศจากความรุนแรง ในกรณีนี้หากประเทศไทยพบว่า มีการละเมิดต่ออำนาจอธิปไตยของรัฐไทยจากต่างประเทศ รัฐบาลควรใช้ความสัมพันธ์ทางการทูตในการเจรจาแก้ปัญหากับประเทศที่สงสัยว่าเป็นคู่กรณี หรือหากพบว่าประเทศไทยถูกใช้เป็นฐานในการจู่โจมทางไซเบอร์ ในกรณีบริษัท Sony Pictures ที่พบหลักฐานระบุการใช้เซิร์ฟเวอร์ในประเทศไทยในการโจมตี ควรนำเอาหลักการเจรจาต่อรองกับประเทศที่ได้รับความเสียหาย และพร้อมให้ความช่วยเหลือในการตามจับกุมผู้กระทำอย่างเต็มที่เพื่อสร้างพันธมิตรกับประเทศนั้น ๆ

**ข้อเสนอแนะในการทำวิจัยครั้งต่อไป**

จากการศึกษาครั้งนี้ได้ข้อค้นพบองค์ความรู้ที่สำคัญ คือ ช่องว่างระหว่างพื้นที่ทางกายภาพและพื้นที่ทางไซเบอร์ โดยเร่งศึกษาช่องว่างระหว่างพื้นที่ทางกายภาพและพื้นที่ทางไซเบอร์ที่มีผลต่อ

การใช้อำนาจอธิปไตย จากการเก็บข้อมูลและผลการวิจัยชี้ให้เห็นว่าอำนาจหน้าที่ในการป้องกันโครงสร้างพื้นฐานสำคัญเชิงกายภาพของประเทศไทยนั้น ขึ้นต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) พร้อมที่จะเป็นเจ้าภาพหลักในการศึกษา และกำหนดขอบเขตของอธิปไตยไซเบอร์ ในส่วนของการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) มีเจ้าภาพหลักเป็นสภาความมั่นคงแห่งชาติ ซึ่งได้จัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) เป็น 6 กลุ่ม ได้แก่ 1.กลุ่มความมั่นคงและบริการภาครัฐ 2. กลุ่มการเงิน 3. กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม 4. กลุ่มการขนส่งและโลจิสติกส์ 5. กลุ่มพลังงานและสาธารณูปโภค 6. กลุ่มสาธารณสุข (ETDA, 2018) และจะต้องเร่งศึกษาในเรื่องของขอบเขตอำนาจ ต่อไป

## เอกสารอ้างอิง

เดชชาติ วงศ์โกมลเชษฐ์. (2515). *หลักรัฐศาสตร์.* (พิมพ์ครั้งที่ 8). กรุงเทพฯ: โรงพิมพ์สมาคมสังคหศาสตร์แห่งประเทศไทย.

Betts, A. (2009). Sovereignty and the State System. *Forced Migration and Global Politics*, *2*(3), 43–45.

Brown, G.D. (2013). The Wrong Questions About Cyberspace. *The Newly Formed United States Cyber Command*, *1*(217), 214–233.

Chachavalpongpun, P. (2022). *Nationhood in the Cloud: Cyber Sovereignty in Thailand*, Retrieved October 31, 2022, from https://doi.org/10.1080/10357823.2022.2109591

Corn, G., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound*, *1*(111), 207–212.

Egan, B. (2016). Legal Adviser, U.S. Dep't of State. *International Law and Stability in Cyberspace, 1*(35), 169–180.

Encyclopedia Britannica. (2019). *Britannica.* Retrieved September 24, 2022, from https://web.archive.org/web/20061020084752//corporate.britannica.com/company_info.html

Electronic Transactions Development Agency [ETDA]. (2018). *การรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญ*. Retrieved December 24, 2022, from https://www.etda.or.th/th/Useful-Resource/documents-for-download/ETDA-Annual-Report-2018.aspx

Hare, F. (2009). *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?*. Retrieved October 22, 2022, from https://ccdcoe.org/uploads/2018/10/06_HARE_Borders-in-Cyberspace.pdf

Humber, K. (2019). *Crimean Tatars and the Politics of Sovereignty: Small State Instrumentalization of Ethnic Minority Sovereignty Claims in Geopolitically Disputed Territory*(Doctoral dissertation). University of British Columbia.

Irshaid, F. (2016). *How ISIS Is Spreading Its Message Online*. Retrieved September 15, 2022, from https://www.bbc.com/news/world-middle-east-27912569

ITU. (2020). *Organizations and Institutions that Address International Cybersecurity*. Retrieved October 22, 2022, from https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf

Jamnejad, M., & Wood, M. (2009). The Principle of Non-intervention. *Leiden Journal of International Law*, *22*(2), 345-381.

Joel, R. (1996). "Governing Networks and Rule-Making in Cyberspace". *Emory Law Journal, 45*(2), 928-950.

Johnson, D.R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402.

Liaropoulos, A. (2013). *Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?*. Retrieved September 20, 2022, from https://www.researchgate.net/publication/287453182_Exercising_state_sovereignty_in_cyberspace_An_international_cyber-order_under_construction

Lindsay, J. (2015). Engagement Without Recognition: The Limits of Diplomatic Interaction with Contested States. *International Affairs, 91*(2), 267-285.

Petchkla, N. (2022). Government Sector's Response in Counter-Cyberterrorism in Thailand. *International Journal of Crime, Law and Social Issues, 9*(2), 1-14.

Roscini, M. (2015). Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*, *50*(2-3), 233-274.

Schmitt, M. (2016). *US Transparency Regarding International Law in Cyberspace, JUST SECURITY*. Retrieved November 25, 2022, from https://www.justsecurity.org/34465/transparency-international-law-cyberspace/

Segal, A. (2020). *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*. Retrieved September 14, 2022, from https://www.nbr.org/publication/chinasvision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/

Sherman, J. (2019). *How Much Cyber Sovereignty is Too Much Cyber Sovereignty?*. Retrieved November 5, 2022, from https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

Tavenner, E. (2022). *Russian Cyber Sovereignty: Global Implications of an Authoritarian RuNet.* Retrieved November 25, 2022, from https://www.american.edu/sis/centers/security-technology/russian-cyber-sovereignty.cfm

The Cabinet Office. (2020). *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World.* Retrieved October 16, 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Weber, V. (2020). *The Sinicization of Russia's Cyber Sovereignty Model.* Retrieved May 31, 2022, from https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model