“เทคโนโลยีสารสนเทศและการสื่อสารกับการเมืองระหว่างประเทศ : การเปลี่ยนแปลงอำนาจรัฐและระเบียบระหว่างประเทศในศตวรรษที่ยี่สิบเอ็ด”

ภาณุทัต วัชราภรณ์ [1]

บทคัดย่อ

บทความนี้จัดทำขึ้นเพื่ออภิปรายถึงความเปลี่ยนแปลงของอำนาจรัฐและการเมืองระหว่างประเทศในปัจจุบันที่เกิดขึ้นจากความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารหรือไอซีที

Abstract

This article aims to discuss the changes of state power and international politics by the advancement of Information and Communication Technology (ICT). By examining the use

[1]บทความนี้เป็นการศึกษาค้นคว้าประเด็นความมั่นคงรายบุคคล เรียงเรียงโดย นายภาณุทัต วัชราภรณ์ นักวิเคราะห์นโยบายและแผนปฏิบัติการกองความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ สำนักงานสภาความมั่นคงแห่งชาติ, รัฐศาสตร์บัณฑิต จุฬาลงกรณ์มหาวิทยาลัย

(Information and Communication Technology, ICT) โดยมีข้อเสนอหลักว่า เทคโนโลยีสารสนเทศและการสื่อสารได้สร้างความเปลี่ยนแปลงต่ออำนาจของรัฐในการเมืองระหว่างประเทศอย่างน้อยในสองระดับ ได้แก่ (1) ในระดับภายในประเทศ โดยรัฐในปัจจุบันกำลังสูญเสียความสามารถในการควบคุมเสถียรภาพทางยุทธศาสตร์ภายในประเทศจากการที่เทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่เข้ามามีบทบาทสร้างความรับรู้ของประชาชนภายในประเทศมากขึ้น ทั้งในกรณีของการทำสงครามที่ไม่ชอบธรรมของผู้นำรัฐและการถูกแทรกแซงทางการเมืองจากต่างชาติ และ (2) ในระดับระหว่างประเทศ ที่ “พื้นที่ทางไซเบอร์” หรือ “ไซเบอร์สเปซ” (cyber-space) ได้กลายมาเป็นอีกหนึ่งพื้นที่สำคัญในการปฏิสัมพันธ์กันระหว่างรัฐ ไม่ว่าจะเป็นในเชิงของการใช้เพื่อสั่งสมอำนาจ การใช้เพื่อกำหนดหรือควบคุมพฤติกรรมของรัฐอื่น และการใช้ทำสงครามรูปแบบใหม่

คำสำคัญ : การเมืองระหว่างประเทศ, ความมั่นคงทางไซเบอร์, สงครามไซเบอร์, สภาพจริงนิยมเชิงโครงสร้าง

of such technology, the article suggests that the state power and international politics have been affected by ICT in at least two levels. Firstly, the states are currently losing its power to control their domestic strategic stability as the ICT play a greater role in building public awareness. This can be seen through the case of an “unjust war” declared by state leader and the foreign electoral interference. Secondly, cyber space has become a new frontier for states to interact with each other. This can be seen from the states use of cyber tools as an arm race to the use to signaling and shaping to the others.

Keywords: International Politics, Cyber-security, Cyber War, Structural Realism

เทคโนโลยีเป็นต้นเหตุสำคัญของการเปลี่ยนแปลงต่างๆ รอบตัวเรา ด้วยความก้าวหน้าของเทคโนโลยี ชีวิตของเราจึงมีความสะดวกสบาย ความปลอดภัย ตลอดจนคุณภาพชีวิตที่ดีขึ้น แต่ในอีกแง่หนึ่งความก้าวหน้าทางเทคโนโลยีก็อาจนำมาซึ่งปัญหาและความท้าทายใหม่ๆ ตั้งแต่ในระดับชีวิตประจำวันของผู้คนไปจนถึงระดับความสัมพันธ์ระหว่างประเทศได้เช่นกัน

บทความนี้จัดทำขึ้นเพื่ออภิปรายถึงความเปลี่ยนแปลงของอำนาจรัฐและการเมืองระหว่างประเทศในปัจจุบันที่เกิดขึ้นจากความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารหรือไอซีที

(Information and Communication Technology, ICT) โดยมีข้อเสนอหลักว่า เทคโนโลยีสารสนเทศและการสื่อสารได้สร้างความเปลี่ยนแปลงต่ออำนาจของรัฐในการเมืองระหว่างประเทศอย่างน้อยในสองระดับ ได้แก่ (1) ในระดับภายในประเทศ โดยรัฐในปัจจุบันกำลังสูญเสียความสามารถในการควบคุมเสถียรภาพทางยุทธศาสตร์ภายในประเทศจากการที่เทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่เข้ามามีบทบาทสร้างความรับรู้ของประชาชนภายในประเทศมากขึ้น ทั้งในกรณีของการทำสงครามที่ไม่ชอบธรรมของผู้นำรัฐและการถูกแทรกแซงทางการเมืองจากต่างชาติ และ (2) ในระดับระหว่าง

ประเทศ ที่ “พื้นที่ทางไซเบอร์” หรือ “ไซเบอร์สเปซ” (Cyberspace) ได้กลายมาเป็นอีกหนึ่งพื้นที่สำคัญในการปฏิสัมพันธ์กันระหว่างรัฐ ไม่ว่าจะเป็นในเชิงของการใช้เพื่อสั่งสมอำนาจ การใช้เพื่อกำหนดหรือควบคุมพฤติกรรมของรัฐอื่น และการใช้ทำสงครามรูปแบบใหม่

ผู้เขียนได้แบ่งบทความฉบับนี้ออกเป็น 4 ส่วน เพื่อนำเสนอมุมมองดังกล่าว โดยส่วนแรก จะอธิบายถึงความสัมพันธ์ระหว่างเทคโนโลยีและการเมืองระหว่างประเทศ ผ่านการตั้งข้อสังเกตว่าเทคโนโลยีเป็นองค์ประกอบที่สำคัญ (important feature) ของระบบระหว่างประเทศมาโดยตลอด ส่วนที่สองจะกล่าวถึงการเปลี่ยนแปลงระดับภายในประเทศ ที่รัฐกำลังสูญเสียอำนาจในการควบคุมเสถียรภาพทางยุทธศาสตร์ในการควบคุมปัจจัยภายในประเทศต่างๆ อันเป็นผลมาจากการที่เทคโนโลยีสมัยใหม่เปิดโอกาสให้ประชาชนสามารถรับรู้ข้อมูลข่าวสารได้มากขึ้น จนสามารถสร้างแรงกดดันให้กับผู้ปกครองรัฐในการตัดสินใจดำเนินนโยบายต่างๆ ส่วนที่สาม จะกล่าวถึงการเปลี่ยนแปลงระดับระหว่างประเทศ โดยอธิบายถึงปฏิสัมพันธ์ระหว่างรัฐที่เริ่มเกิดขึ้นในพื้นที่ทางไซเบอร์ ทั้งในด้านการสั่งสมอำนาจ การใช้ขีดความสามารถในการกำหนดหรือควบคุมพฤติกรรมของรัฐอื่น และการใช้ทำสงครามรูปแบบใหม่ และส่วนสุดท้ายจะเป็นบทสรุปของบทความนี้

ส่วนที่หนึ่ง เทคโนโลยีและการเมืองระหว่างประเทศ

การเมืองระหว่างประเทศ (International Politics) นั้นเป็นการเมืองของความขัดแย้งระหว่างรัฐ หากสังเกตถึงความเป็นไปของการเมืองระหว่างประเทศตั้งแต่ในอดีตจวบจนถึงปัจจุบัน เราจะพบว่าตลอดระยะเวลามากกว่าสามร้อยปีที่ผ่านมาของการเมืองระหว่างประเทศ โลกต้องเผชิญกับความขัดแย้งระหว่างรัฐชาติในรูปแบบต่างๆ ไม่ว่าจะเป็นการต่อสู้กันทางทหารในรูปแบบของสงคราม การแข่งขันทางด้านเศรษฐกิจ หรือการคว่ำบาตรรัฐที่ไม่ปฏิบัติตามข้อตกลงระหว่างประเทศ

ในแง่หนึ่ง อาจกล่าวได้ว่าพฤติกรรมการแข่งขันกันแสวงหาอำนาจดังกล่าวของการเมืองระหว่างประเทศนั้นมีที่มาจาก “โครงสร้างของระบบระหว่างประเทศ” (International Structure) โดย เคนเนท วอลทซ์ (Kenneth Waltz) หนึ่งในนักวิชาการด้านความสัมพันธ์ระหว่างประเทศสำนักสภาพจริงนิยมเชิงโครงสร้าง (Structural Realism) ได้อธิบายถึงพฤติกรรมความขัดแย้งระหว่างรัฐชาติในการเมืองระหว่างประเทศไว้ตามแนวคิดดังกล่าว ซึ่งเขาได้เสนอว่าแท้จริงแล้วพฤติกรรมของรัฐชาติในการดำเนินกิจการต่างๆ นั้นมีที่มาจากโครงสร้างของระบบระหว่างประเทศ กล่าวคือ สำหรับวอลทซ์และสำนักสภาพจริงนิยมเชิงโครงสร้างแล้ว โครงสร้างของระบบจะเป็นตัวกำหนดบทบาทและพฤติกรรมของผู้นำและรัฐให้แสดงบทบาทที่คล้ายกันไม่ว่ารัฐเหล่านี้จะมีอุดมการณ์หรือระบบการเมืองที่แตกต่างกัน[2]

[2]Kenneth Waltz, Theory of International Politics (New York: Mcgraw Hill, 1979) , quoted in Cynthia Weber, “Realism: Is International Anarchy the Permissive Cause of War?,” in International Relations Theory: A Critical Introduction, 4th Edition (London and New York: Routledge, 2010), 16.

ซึ่งภายใต้ระบบระหว่างประเทศแบบเวสต์ฟาเลียที่ “ทุกๆ รัฐมีอำนาจสูงสุดเท่ากัน” สภาพแวดล้อมระหว่างประเทศนั้นมีลักษณะเป็น “อนาธิปไตย” เพราะทุกรัฐต่างถือว่าตนเองมีอำนาจอธิปไตยเป็นอำนาจสูงสุดและไม่ยอมรับว่ามีอำนาจอื่นใดที่เหนือกว่าตน ดังนั้น เพื่อความอยู่รอดและความมั่นคงของรัฐ ทุกๆ รัฐในการเมืองระหว่างประเทศจึงต้องพยายามปกป้องผลประโยชน์และช่วยเหลือตนเองด้วยการแสวงหาอำนาจให้ได้มากที่สุด หรืออาจกล่าวได้ว่าโครงสร้างอันเป็นอนาธิปไตยของระบบระหว่างประเทศคือที่มาของความขัดแย้งในการเมืองระหว่างประเทศ

อย่างไรก็ตาม การต่อสู้แย่งชิงอำนาจอย่างต่อเนื่องของรัฐไม่จำเป็นต้องลงเอยด้วยการประกาศสงครามอย่างเปิดเผยอยู่เสมอไป และรัฐในการเมืองระหว่างประเทศก็ไม่ได้ปรารถนาจะใช้สงครามเป็นวิธีการในการบรรลุเป้าหมายในทุกกรณี ทั้งนี้เพราะการตัดสินใจทำสงครามของรัฐต้องมาจากการวิเคราะห์ผลได้ผลเสียมาอย่างดีแล้วเท่านั้น โดยมากแล้วการใช้อำนาจทางการทหารหรือการทำสงครามมักจะถูกเก็บไว้เป็นตัวเลือกสุดท้ายเมื่อวิธีการอื่นๆ ในการดำเนินความสัมพันธ์ระหว่างประเทศไม่ได้ผล ซึ่งรัฐในการเมืองระหว่างประเทศสามารถที่จะหลีกเลี่ยงสงครามได้ด้วยการดำเนินนโยบาย “ถ่วงดุลอำนาจ” (Balance of Power) ซึ่งหมายถึงการที่รัฐที่ต้องการรักษาสันติภาพจะต้องเตรียมพร้อมที่จะทำสงครามด้วยการสะสมอำนาจให้มากที่สุดเท่าที่จะเป็นไปได้และใช้อำนาจนั้นเพื่อป้องกันและไขว่ขว้าผลประโยชน์แห่งชาติ โดยหวังว่าอำนาจทางการทหารที่ได้สั่งสมเอาไว้จะสามารถป้องปรามรัฐอื่น ๆ หรือรัฐที่เป็นศัตรูให้ไม่กล้าโจมตีหรือทำสงครามกับตนเอง

แม้ว่าตามแนวคิดของวอลทซ์และสำนักสภาพจริงนิยมเชิงโครงสร้างแล้ว โครงสร้างของระบบจะเป็นตัวกำหนดบทบาทและพฤติกรรมของผู้นำและรัฐให้แสดงบทบาทที่คล้ายกัน แต่การดำเนินไปของการเมืองระหว่างประเทศนั้นมีทั้งความต่อเนื่องและพลวัตการเปลี่ยนแปลงที่ “อาจจะไม่ได้ดำเนินไปแบบเส้นตรงเสียทีเดียว บางครั้งอาจจะเป็นวัฏจักร หรือบางครั้งอาจจะเป็นการตัดขาดจากเดิมและมีสิ่งใหม่เกิดขึ้นมา”[3] กล่าวคือ นับตั้งแต่อดีตกาลความขัดแย้งในการเมืองระหว่างประเทศนั้นไม่ได้เกิดขึ้นในรูปแบบใดรูปแบบหนึ่งโดยเฉพาะ แต่ความขัดแย้งดังกล่าวมีพลวัตที่เปลี่ยงแปลงไปมาอยู่ตลอดเวลา

เทคโนโลยีถือเป็นองค์ประกอบที่สำคัญ (Important Feature) ของระบบระหว่างประเทศมาโดยตลอด หากพิจารณาตามข้อสมมุติฐานของวอลทซ์ที่ว่า โครงสร้างของระบบจะเป็นตัวกำหนดบทบาทและพฤติกรรมของผู้นำและรัฐให้แสดงบทบาทที่คล้ายกัน เทคโนโลยีก็จะเป็นปัจจัยสำคัญในการเปลี่ยนแปลงรูปแบบหรือลักษณะของปฏิสัมพันธ์ระหว่างรัฐในการเมืองระหว่างประเทศ

หากพิจารณาคำอธิบายของผู้ช่วยศาสตราจารย์เจฟฟรีย์ เอร์เรร่า (Geoffrey Herrera) อาจารย์ประจำมหาวิทยาลัยเทมเพิล (Temple University) ที่ว่า

“ลองจินตนาการถึงระบบระหว่างประเทศสองระบบที่มีรูปแบบเหมือนกันทั้งหมด – ทั้งคู่มีลักษณะเป็นอนาธิปไตยและมีการกระจายของขีดความสามารถ (Capability) ของรัฐที่เหมือนกัน – แต่ในระบบแรกมีม้าและเรือเดินสมุทรเป็นเทคโนโลยีในการเดินทางและติดต่อสื่อสาร ส่วนระบบที่สองมีเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกันได้ทั่วโลก แน่นนอนว่าทั้งคุณภาพ ระดับ และความเอาจริงเอาจังของการดำเนินความสัมพันธ์ระหว่างรัฐในทั้งสองระบบย่อมแตกต่างกันโดยสิ้นเชิง”[4]

[3]จิตติภัทร พูนขำ, “การเมืองระหว่างประเทศยามผลัดปี: การสิ้นสุดของอะไร?,” The 101. World, แก้ไขล่าสุด 29 ธันวาคม 2560, https://www.the101.world/thoughts/world-at-year-end.

[4]Geoffrey Herrera, Technology and International Systems, accessed April 21, 2017, 565, http://journals.sagepub.com/doi/pdf/10.1177/0305829803032003100l.

จะพบว่า ความแตกต่างที่เกิดขึ้นระหว่างตัวอย่างทั้งสองกรณี ไม่ได้ขึ้นอยู่กับลักษณะของรัฐหรือกระทั่งกลุ่มของรัฐใดๆ แต่เป็นผลมาจากความสามารถที่เทคโนโลยีมีต่อการเมืองระหว่างประเทศ

อย่างไรก็ตาม การจะกล่าวว่าความก้าวหน้าของเทคโนโลยีทุกอย่างล้วนส่งผลให้เกิดการเปลี่ยนแปลงต่อการเมืองระหว่างประเทศนั้นก็ไม่ได้ถูกต้องเสียทีเดียว เพราะความก้าวหน้าของเทคโนโลยีบางอย่าง อาทิ เทคโนโลยีทางการแพทย์หรือเทคโนโลยีการเกษตร ก็ไม่ได้ก่อให้เกิดความเปลี่ยนแปลงใดๆ ต่อการเมืองระหว่างประเทศ ทั้งนี้เพราะเทคโนโลยีที่อาจก่อให้เกิดความเปลี่ยนแปลงต่อพลวัตของการเมืองระหว่างประเทศนั้นจะต้องประกอบไปด้วยสองลักษณะสำคัญ ประการแรกคือเทคโนโลยีดังกล่าวจะต้องถูกนำมาใช้จริงในสังคม เพราะ “เทคโนโลยีจะมีความหมายต่อสังคมเมื่อมันได้ถูกนำมาใช้จริง”[5] และเทคโนโลยีดังกล่าวจะต้องเป็นเทคโนโลยีที่เกี่ยวข้องกับปฏิสัมพันธ์ระหว่างรัฐ เช่น เทคโนโลยีการสื่อสาร (communication) เทคโนโลยีการขนส่ง (transportation) หรือเทคโนโลยีที่เกี่ยวข้องกับความรุนแรง (violence feature) อาทิ อาวุธหรือยุทธโธปกรณ์

การเปลี่ยนแปลงทางเทคโนโลยีครั้งใหญ่ๆ ย่อมส่งผลต่อปฏิสัมพันธ์ระหว่างรัฐในการเมืองระหว่างประเทศเสมอ อาวุธนิวเคลียร์เป็นตัวอย่างที่ดีที่สุดในการสนับสนุนข้อถกเถียงข้างต้น โดยนับแต่ช่วงครึ่งหลังศตวรรษที่ 20 มีนักวิชาการบางคนตั้งข้อสังเกตว่าอำนาจแข็ง (Hard Power) ทางการทหารและเศรษฐกิจซึ่งเคยเป็นสิ่งขี้ขาดอำนาจในการเมืองระหว่างประเทศ ได้ค่อยๆ เปิดทางให้แก่อำนาจอ่อน (Soft Power) ทางข่าวสารและการสื่อสารในการสร้างความยินยอมหรือการโน้มน้าวในการเมืองระหว่างประเทศมากขึ้น[7] ทั้งนี้เพราะความก้าวหน้าของเทคโนโลยีอาวุธ โดยเฉพาะอาวุธพลังทำลายล้างสูง (Weapon of Mass Destruction, WMD) อย่างอาวุธนิวเคลียร์นั้นมีอานุภาพที่มากเกินกว่าที่รัฐชาติจะสามารถใช้ต่อสู้ระหว่างกันได้อย่างบ่อยครั้ง

ส่วนที่สอง การเปลี่ยนแปลงระดับภายในประเทศ

สำหรับผลกระทบที่เกิดขึ้นในระดับประเทศมักเกิดขึ้นจากคุณสมบัติสำคัญประการหนึ่งของเทคโนโลยีสารสนเทศและการสื่อสารในการประกอบสร้าง “ความรับรู้” (cognitive) ของผู้คนในสังคม ตัวอย่างของคุณสมบัติเช่นนี้ ได้แก่ การที่ผู้คนสามารถรับรู้และเผยแพร่ข่าวสารระหว่างกันได้อย่างง่ายดายผ่านสื่อสังคมออนไลน์ต่างๆ การกระทำในลักษณะนี้ไม่เพียงแต่เป็นการเผยแพร่ข้อมูลให้ผู้อื่น แต่ยังส่งผลต่อการประกอบสร้างความรู้ ความเข้าใจ รวมถึงไปมุมมองและทัศนคติของผู้คนอื่นๆ ต่อประเด็นหนึ่งๆ ในสังคมได้ด้วยเช่นกัน

[5]Herrera, Technology and International Systems, 578.
[6]William McNeill, The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000, (Chicago: University of Chicago Press, 1982) ; John Herz, International Politics in the Atomic Age, (New York: Columbia University Press, 1959); Benedict Anderson, Imagined Communities: Reflections on the Origins and Spread of Nationalism, (London: Verso, 1991); Daniel Headrick, Tools of Empire: Technology and European Imperialism in the Nineteenth Century, (NewYork: Oxford University Press, 1981), quoted in Herrera, Technology and International Systems, 565.
[7]Joseph Nye, “The Benefits of Soft Power,” Harvard Business School Working Knowledge, February 8, 2004, https://hbswk.hbs.edu/archive/the-benefits-of-soft-power.

คุณสมบัติประการนี้ของเทคโนโลยีสารสนเทศและการสื่อสารอาจก่อให้เกิดผลลัพธ์ได้ทั้งในแง่ดีและแง่ร้ายต่อสังคม ในแง่ดีที่ผู้กระจายข่าวสารทำไปเพื่อสร้างความรู้ความเข้าใจที่ถูกต้องให้กับผู้อื่น เช่น การเผยแพร่เนื้อหาเพื่อการเรียนรู้ ย่อมทำให้ผู้คนอื่นๆ ที่สามารถเข้าถึงองค์ความรู้และมีความรับรู้ที่มากขึ้นในประเด็นที่ยากจะเข้าถึงและทำความเข้าใจเองได้ แต่ในขณะเดียวกัน หากมีผู้ที่ประสงค์ร้ายนำเอาเทคโนโลยีมาใช้ประโยชน์ด้วยการเผยแพร่ข้อมูลที่ผิดเพี้ยน ไม่ว่าจะเป็นในแง่ของการสร้างข่าวปลอม (fake news) หรือการดัดแปลงข้อมูลเพื่อให้เกิดความเข้าใจผิด (disinformation) ก็ย่อมก่อให้เกิดความรับรู้ที่ผิดเพี้ยนขึ้นในสังคมขึ้นได้ ในส่วนนี้ของบทความจะกล่าวถึงผลกระทบที่เกิดขึ้นกับอำนาจของรัฐจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารทั้งในแง่ดีและแง่ร้าย ดังนี้

การต่อต้านการใช้อำนาจรัฐที่ไม่ชอบธรรม

ความสามารถในการเข้าถึงข้อมูลข่าวสารได้อย่างแพร่หลายของผู้คนด้วยเทคโนโลยีสารสนเทศและการสื่อสารในแง่หนึ่งก็ได้นำมาซึ่งปัญหาต่ออำนาจของรัฐในการเมืองระหว่างประเทศ ในยุคดิจิตอลที่ข้อมูลทุกอย่างถูกเก็บเอาไว้ในอินเทอร์เน็ต ปัจเจกบุคคลและภาคประชาสังคมที่สามารถเข้าถึงเทคโนโลยีดังกล่าวก็ได้เริ่มเข้ามามีส่วนร่วมในการเมืองทั้งภายในและระหว่างประเทศมากขึ้น

ปัจจุบันการรวมศูนย์อำนาจอย่างเบ็ดเสร็จของผู้นำจะเป็นไปได้ยากขึ้นในยุคที่ข้อมูลข่าวสารมีความเสรีด้วยอินเทอร์เน็ต เพราะ “ความสามารถในการเข้าถึงข้อมูลที่มากขึ้นช่วยสนันสนุนการระดมพลของผู้คน และมอบวิธีการรวมตัวที่ ดีกว่าให้แก่เหล่าผู้ต่อต้าน”[8] เหตุการณ์อาหรับสปริงที่มวลชนติดต่อกันผ่านโซเชียลมีเดียเพื่อรวมกลุ่มกันโค่นล้มผู้นำเผด็จการในอียิปต์จนสำเร็จในปี ค.ศ. 2011 เป็นข้อพิสูจน์ให้สังคมโลกได้เห็นถึงพลังของการรวมตัวกันผ่านเทคโนโลยีสารสนเทศและการสื่อสารอย่างสื่อสังคมออนไลน์และอินเทอร์เน็ต

นอกจากนี้ ผู้นำทางการเมืองภายในรัฐจะไม่สามารถทำสงครามตามรูปแบบด้วยวิธีการดั้งเดิมได้อย่างอิสระอีกต่อไป เพราะในปัจจุบันความเสรีของสื่อด้วยเทคโนโลยีสารสนเทศและการสื่อสารได้สร้างข้อจำกัดในการทำสงครามให้แก่รัฐ กล่าวคือ แม้ในเชิงทฤษฎีรัฐจะมีความชอบธรรมในการประกาศสงครามตามหลักสงครามที่ยุติธรรม (Just War) ทว่าในความเป็นจริง รัฐในปัจจุบันกลับไม่สามารถทำสงครามได้หากไร้ซึ่งแรงสนับสนุนจากประชาชนภายในประเทศ โดยสื่อที่มีความเสรีสูงย่อมนำมาซึ่งแรงต่อต้านต่อการทำสงครามที่สูงด้วยเช่นกัน ตัวอย่างเช่นในช่วงสงครามเวียดนามที่ “สหรัฐฯ แพ้สงครามเพราะสื่อ”[9] เนื่องจากในสมัยดังกล่าว สหรัฐไม่ได้จำกัดหรือตรวจสอบการนำเสนอข้อมูลของสื่ออย่างเข้มงวด ซึ่งการที่สื่อได้นำเสนอข่าวเกี่ยวกับการทำสงครามในเวียดนามอย่างตรงไปตรงมาทำให้เกิดกระแสต่อต้านจากประชาชนชาวสหรัฐฯ และกลายมาเป็นแรงกดดันและสาเหตุหนึ่งที่สหรัฐฯต้องยินยอมถอนกำลังออกจากสงครามเวียดนาม

ในขณะนี้แม้เราจะเห็นการทำสงครามตามแบบอยู่ เช่นในกรณีความขัดแย้งระหว่างรัสเซียและยูเครน แต่ก็เป็นเพราะว่า ประเทศผู้ริเริ่มสงครามมีความเข้าใจถึงข้อจำกัดทางอำนาจรัฐที่เกิดขึ้นจากเทคโนโลยีสารสนเทศและการสื่อสารอย่างดี จึงได้ทำการปิดกั้นและควบคุมการกระจายของข้อมูลภายในประเทศเพื่อลดแรงเสียดทานที่อาจเกิดขึ้นจากประชาชน

[8]Jan Pierskalla and Florian Hollenbach, “China’s ‘Networked Authoritarianism’,” in Journal of Democracy vol. 22, 32-46, quoted in Nils Weidmann, “Communication, Technology, and Political Conflict: Introduction to the Special Issue,” in Journal of Peace Research 2015 vol. 52, 265.

[9]Daniel Hallin, The ‘Uncensored War’: The Media and Vietnam (Oxford: Oxford University Press, 1986) quoted in Debbie Lisle, “How Do We Find Out What’s Going On in the World?,” in Global Politics: A New Introduction, 2nd Edition, eds. Jenny Edkins and Maja Zehfuss (London and New York: Routledge, 2014), 159.

ภายในประเทศ อย่างไรก็ตาม เรายังสามารถพบเห็นได้ว่าในหลาย ๆ พื้นที่ซึ่งการปิดกั้นข่าวสารไม่ประสบผลสำเร็จก็จะเกิดแรงต่อต้านต่อการทำสงครามของผู้นำขึ้นเป็นปกติ

การถูกแทรกแซงทางการเมืองจากต่างชาติ

แม้โดยพื้นฐานแล้วอินเทอร์เน็ตดูจะเป็นพื้นที่ที่มีความเสรี โดยเป็นพื้นที่สาธารณะที่ใครก็ล้วนสามารถเข้าไปใช้งานได้ ทว่าแท้จริงแล้วพื้นที่ดังกล่าวก็ถือเป็นพื้นที่ที่มีเจ้าของ มีการควบคุม ถูกทำให้เป็นเครื่องมือทางการตลาด การลงทุน การแสวงหากำไร หรือกระทั่งเป็นพื้นที่เพื่อผลประโยชน์ทางการเมืองมาตั้งแต่ต้น ทั้งยังมีแนวโน้มที่จะเป็นไปในทิศทางนี้มากขึ้นเรื่อยๆ ประเด็นสำคัญของคุณลักษณะนี้ของพื้นที่ทางอินเทอร์เน็ตจึงเป็นปัญหาที่ประชาชนสามารถถูกชักจูงให้คล้อยตาม (manipulate) จากการแทรกแซงผ่านช่องทางสื่อสังคมออนไลน์ได้ง่าย

ประเด็นปัญหาที่เกิดขึ้นและโด่งดังที่สุดของกรณีเช่นนี้คือ ประเด็นการถูกแทรกแซงการเลือกตั้งประธานาธิบดีสหรัฐอเมริกา ในปี ค.ศ. 2016 โดยทางการสหรัฐฯพบว่า คณะกรรมการแห่งชาติของพรรคเดโมแครต (Democrat National Committee, DNC) ได้ถูกกลุ่มแฮกเกอร์นิรนามเข้าถึงฐานข้อมูลในระบบ ทำให้ข้อมูลที่สมาชิกต่าง ๆ โต้ตอบกันในอีเมลหลุดรั่วออกไป และถูกนำไปเผยแพร่ให้เกิดความเสียหาย[10] รวมถึงการที่รัสเซียได้ทำปฏิบัติการข่าวสาร (Information Operation) ในการสร้างข่าวปลอม และใช้ประโยชน์จากการโฆษณาผ่านสื่อสังคมออนไลน์เพื่อชักจูงให้ผู้มีสิทธิ์ออกเสียง โดยเฉพาะกลุ่มที่ยังไม่ตัดสินใจเลือกผู้สมัครหันมาเลือกนายโดนัลด์ ทรัมป์ (Donald Trump) เป็นประธานิบดี[11]

แม้ว่าในท้ายที่สุด จะไม่มีบทสรุปว่าการที่นายโดนัลด์ ทรัมป์ชนะการเลือกตั้งประธานาธิบดีสหรัฐฯ เป็นผลจากการถูกแทรกแซงทางการเมืองผ่านระบบสารสนเทศจริงหรือไม่ และเทคโนโลยีดังกล่าวมีผลต่อการเลือกตั้งมากน้อยเพียงใด แต่เราก็ไม่อาจมองข้ามความสามารถของเทคโนโลยีสารสนเทศและการสื่อสารถูกใช้เป็นเครื่องมือในการเข้าแทรกแซงการเมืองภายในประเทศของรัฐอื่น รวมถึงผลกระทบต่อสังคมในการประกอบสร้างความคิดของผู้คนให้มีอคติ ทั้งในแง่ของความชอบหรือความเกลียด ต่อบุคคลหรือสถานการณ์หนึ่งๆ ซึ่งเป็นรากฐานสำคัญของการตัดสินใจทางการเมืองต่างๆ ภายในประเทศ และเป็นความท้าทายที่สำคัญของรัฐในการควบคุมเสถียรภาพทางการเมืองและความคิดของผู้คนภายในรัฐ

ส่วนที่สาม การเปลี่ยนแปลงระดับระหว่างประเทศ

การแพร่ขยายและความก้าวหน้าของเทคโนโลยีการสื่อสารและสารสนเทศอย่างอินเทอร์เน็ตได้ส่งผลให้เกิดพลวัตที่สำคัญขึ้นต่อการเมืองระหว่างประเทศ ดังเช่นที่ เฮนรี คิสซิงเจอร์ (Henry Kissinger) อดีตที่ปรึกษาด้านความมั่นคงและรัฐมนตรีว่าการกระทรวงการต่างประเทศชาวสหรัฐ กล่าวไว้ว่า “ไซเบอร์สเปซท้าทายประสบการณ์ทางประวัติศาสตร์ทั้งหมด”[12]

ในระดับระหว่างประเทศ เทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทในลักษณะของการเป็น “พื้นที่ในการปฏิสัมพันธ์” (Space of Interaction) ระหว่างรัฐ โดนในพื้นที่ที่เราเรียกว่า “พื้นที่ทางไซเบอร์” หรือ “ไซเบอร์สเปซ” รัฐได้ใช้พื้นที่ดังกล่าวในการสั่งสมอำนาจ และนำขีดความสามารถที่ตนเองมีไปใช้เพื่อกำหนดหรือควบคุมพฤติกรรมของรัฐอื่น รวมไปถึงการใช้ทำสงครามรูปแบบใหม่

[10]Ben Buchanan, The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics (Cambridge, Massachusetts: Harvard University Press, 2020), 211-239.
[11]Ibid., 231.
[12]Henry Kissinger, “Technology, Equilibrium, and Human,” in World Order (New York: Penguin, 2014), 344-345.

การสั่งสมอำนาจทางไซเบอร์ (Cyber Arms race)

การสั่งสมอำนาจทางไซเบอร์เป็นปฏิสัมพันธ์ทางการเมืองรูปแบบหนึ่งของรัฐในปัจจุบัน ตัวอย่างที่เด่นชัดที่สุดของการสั่งสมอำนาจเช่นนี้ คือ เหตุการณ์ในปี ค.ศ. 2009 เมื่อรัฐบาลสหรัฐฯ ภายใต้ประธานาธิบดีบารัค โอบามา (Barack Obama) ได้จัดตั้ง “กองบัญชาการไซเบอร์แห่งสหรัฐ” (United States Cyber Command, USCYBERCOM) ขึ้นมาเพื่อป้องกันการถูกคุกคามทางไซเบอร์ ทั้งนี้หน่วยงานดังกล่าวของสหรัฐฯไม่ได้เกิดขึ้นมาเพื่อดำเนินการในเชิงป้องกันอย่างเดียว แต่ยังถูกจัดตั้งขึ้นมาเพื่อซักซ้อมการโจมตีทางไซเบอร์ในกรณีที่ต้องเผชิญสงครามไซเบอร์ด้วยเช่นกัน เพราะสำหรับการปฏิบัติการในพื้นที่ทางไซเบอร์แล้ว ในแง่หนึ่ง “การโจมตีก็คือการป้องกันที่ดีที่สุด”[13]

นอกจากฝ่ายสหรัฐฯที่มีการจัดตั้งหน่วยงานขึ้นมาปฏิบัติการอย่างเป็นทางการแล้ว ในช่วงสิบปีที่ผ่านมา ประเทศต่างๆ อาทิ จีน รัสเซีย อิหร่าน อิสราเอล และเกาหลีเหนือ ก็ได้พยายามสร้างนักรบไซเบอร์หรือกองทัพไซเบอร์ของตนเองขึ้นมาอย่างจริงจังเช่นกัน

การที่รัฐในปัจจุบันเลือกที่จะทำปฏิบัติการทางไซเบอร์ และพยายามสั่งสมกำลังในพื้นที่ดังกล่าวให้มากขึ้นมีสาเหตุสำคัญสองประการ

ประการแรก เป็นเพราะในพื้นที่ทางไซเบอร์ “โครงสร้างความสัมพันธ์เชิงอำนาจระหว่างรัฐชาติไม่ได้เป็นไปตามอำนาจในโลกทางกายภาพ” กล่าวคือ ในทางไซเบอร์ไม่ได้มีใครเป็นมหาอำนาจอย่างแท้จริง เพราะทุกคนต่างมีความเปราะบางและอาจตกเป็นเหยื่อของการโจมตีได้เสมอ นอกจากนี้ ปัจจุบันยังไม่มีข้อสรุปที่แน่ชัดว่าระหว่างแฮคเกอร์ฝีมือดีหนึ่งคนหรือแฮคเกอร์ฝีมือพอใช้หนึ่งร้อยคน ฝ่ายใดจะมีขีดความสามารถและสามารถปฏิบัติการทางไซเบอร์ได้อย่างมีประสิทธิภาพมากกว่ากัน[14] ด้วยเหตุนี้ ในบางกรณีรัฐเล็กๆ จึงอาจมีขีดความสามารถในการทำปฏิบัติการทางไซเบอร์มากกว่าหรือเท่ากับรัฐมหาอำนาจในโลกทางกายภาพได้

ประการที่สอง เป็นเพราะ การโจมตีทางไซเบอร์มีลักษณะของความลึกลับและยากในการระบุผู้กระทำผิด กล่าวคือ ในการถูกโจมตีครั้งหนึ่ง เป็นเรื่องยากมากสำหรับเหยื่อในการจะทราบว่าใครเป็นผู้ทำการโจมตีและการโจมตีมีต้นตอมาจากสถานที่ใด เพราะผู้โจมตีสามารถปลอมแปลงที่อยู่ของตนเพื่อให้เกิดความเข้าใจผิดของต้นตอการโจมตีให้กลายเป็นบุคคลที่สามได้ หรือแม้ว่าเหยื่อจะสามารถสืบทราบที่มาของการโจมตีทางไซเบอร์ แต่ก็ไม่มีอะไรที่สามารถพิสูจน์ได้ว่าการโจมตีนั้นเป็นไปตามคำสั่งของรัฐบาลหรือเป็นเพียงความต้องการส่วนบุคคลเช่นกัน

การกำหนดหรือควบคุมพฤติกรรมของรัฐอื่น

หลังจากที่รัฐสามารถสั่งสมอำนาจทางไซเบอร์ได้ระดับหนึ่งแล้ว อำนาจดังกล่าวยังสามารถนำมาใช้เพื่อให้เกิดผลกระทบทางการเมืองระหว่างประเทศได้หลายรูปแบบ ไม่ว่าจะเป็นในแง่ของการใช้เพื่อ “ส่งสัญญาน” (signaling) โดยเฉพาะในแง่ของการข่มขู่หรือแสดงความไม่พอใจต่อพฤติกรรมของรัฐอื่น หรือการใช้เพื่อ “กำหนดหรือควบคุมพฤติกรรม

[13]Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (New York: Public Affairs, 2017) 106-110.
[14]Segal, The Hacked World Order, 11-16.

ของรัฐ” (shaping) ในเชิงอ้อม อย่างการเข้าไปรบกวนโครงการภายในประเทศของรัฐอื่น[15]

ตัวอย่างที่สำคัญของการใช้เพื่อส่งสัญญาน คือ กรณีในปี ค.ศ. 2014 เมื่อ บริษัทผู้ผลิตภาพยนตร์ชื่อดังอย่าง “โซนี่ พิคเจอร์ส” (Sony Picture) ถูกกลุ่มแฮกเกอร์ปริศนาที่เรียกตนเองว่า “ผู้พิทักษ์สันติภาพ” (Guardian of Peace) กระหน่ำโจมตีฐานข้อมูลของตนอย่างหนักจนทำให้คอมพิวเตอร์ของทั้งบริษัทใช้การไม่ได้ และสร้างผลกระทบทางด้านการเงินต่อบริษัทจำนวนหนึ่ง การโจมตีดังกล่าวมักถูกมองว่าเป็นการโจมตีที่ได้รับการสนับสนุนจากประเทศเกาหลีเหนือ เนื่องจากในช่วงเวลาก่อนการถูกโจมตีระยะหนึ่งทางโซนี่ได้ปล่อยตัวอย่างภาพยนตร์เรื่อง The Independence ซึ่งมีเนื้อหาเสียดสีระบบการปกครองของเกาหลีเหนือและก่อให้เกิดความไม่พอใจจากทางการเกาหลีเหนืออย่างมากออกไป[16]

การโจมตีทางไซเบอร์ต่อบริษัทโซนี่จึงเปรียบเสมือนการส่งสัญญานเตือนจากตัวแสดงทางการเมืองระหว่างประเทศในการแสดงความไม่พอใจ และแสดงให้เห็นถึงขีดความสามารถในการลงโทษการกระทำที่ตนเองไม่เห็นด้วย ทั้งยังเป็นการข่มขู่ให้ผู้อื่นที่คิดจะกระทำเช่นเดียวกันเกิดความลังเลและไม่กล้ากระทำตามอีกด้วย

สำหรับตัวอย่างของการใช้เครื่องมือทางไซเบอร์ในการกำหนดหรือควบคุมพฤติกรรมของรัฐ คือ กรณีในปี ค.ศ. 2010 ที่สหรัฐฯได้ส่งมัลแวร์ (malware) ซึ่งหมายถึง “โปรแกรมประสงค์ร้ายที่ทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย หรือการโจรกรรมข้อมูล” ที่ชื่อ “สตักซ์เน็ต” (Stuxnet) ให้แทรกซึมและฝังตัวเข้าไปในระบบคอมพิวเตอร์ของโรงงานพัฒนาขีดความสามารถทางนิวเคลียร์ของอิหร่าน โดย สตักซ์เน็ตได้ถูกออกแบบมาให้รบกวนการทำงานของระบบการแยกยูเรเนียมให้บริสุทธิ์ของโรงงาน และส่งผลให้โครงการพัฒนานิวเคลียร์ของอิหร่านต้องชะลอลงไปอย่างมาก การใช้สตักซ์เน็ตได้สร้างความได้เปรียบทางการเมืองให้กับสหรัฐฯในการเจรจาต่อรองกับอิหร่าน เพราะยิ่งการพัฒนานิวเคลียร์ล่าช้ามากเท่าไหร่ สหรัฐฯ ก็จะยิ่งสามารถกดดันทางเศรษฐกิจต่ออิหร่านได้หนักมากขึ้นเรื่อยๆ และทำให้อิหร่านยอมหันมาเจรจาโดยดี

การใช้เครื่องมือทางไซเบอร์ในลักษณะนี้จะแตกต่างจากการใช้เพื่อส่งสัญญาณตรงที่ไม่ได้เกิดขึ้นอย่างเปิดเผย แต่กลับมีความสามารถในการจัดการกับพฤติกรรมของตัวแสดงอื่นได้ดีกว่า เพราะผู้ได้รับผลกระทบมักจะไม่ทราบว่าตัวเองกำลังตกเป็นเป้าหมาย และคิดว่าผลกระทบที่เกิดขึ้นเป็นเพราะข้อจำกัดภายในของตัวเอง และอาจก่อให้เกิดการเปลี่ยนทิศทางการดำเนินนโยบายของรัฐนั้นๆ ได้ รวมถึงเพิ่มความได้เปรียบในการเจรจาต่อรองบางกรณี ดังเช่นที่สหรัฐฯได้ทำกับอิหร่าน

การทำสงครามไซเบอร์ และประเด็นความท้าทายของรัฐในปัจจุบัน

ในปัจจุบันพื้นทางไซเบอร์ได้กลายมาเป็นพื้นที่ใหม่ในการต่อสู้กันระหว่างรัฐในการเมืองระหว่างประเทศนอกเหนือจากสมรภูมิรบทาง บก ทะเล อากาศ และอวกาศ โดย ริชาร์ด เอ.คลาร์ก (Richard A. Clarke) ได้ให้คำนิยามของ “สงครามไซเบอร์” ไว้ว่า

[15]Buchanan, The Hacker and the State, 3-7.
[16]Segal, The Hacked World Order, 57-31.

“เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก”[17] ซึ่งในสงครามดังกล่าวรัฐชาติไม่จำเป็นต้องเคลื่อนกำลังทางกายภาพอาทิ กำลังทหารหรืออุทธโธปกรณ์ ไปถล่มทำลายข้าศึก แต่สามารถทำร้ายข้าศึกได้ด้วยการนั่งอยู่หน้าจอคอมพิวเตอร์และเคาะแป้นคีย์บอร์ดเท่านั้น

สงครามไซเบอร์ถูกเชื่อว่าเกิดขึ้นอย่างเป็นทางการครั้งแรกช่วงปี ค.ศ. 2007 เมื่อเว็ปไซต์ของสถาบันต่างๆ ในประเทศเอสโทเนียไม่ว่าจะเป็นรัฐสภา กระทรวง ธนาคาร และสื่อมวลชนตกเป็นเป้าการโจมตีจากแฮ็คเกอร์ ด้วยวิธี “การปฏิเสธการให้บริการ” (Distributed Denial of Service, DDoS)[18] การโจมตีนี้ส่งผลให้การให้บริการทั้งหมดของเอสโทเนียต้องหยุดชะงักลงเป็นระยะเวลาหนึ่ง และส่งผลให้การพึ่งพาเทคโนโลยีสารสนเทศและการสื่อสารจำนวนมากซึ่งเป็นสิ่งที่เอสโทเนียเคยเชื่อว่าเป็นจุดแข็งของประเทศกลับกลายเป็นจุดอ่อนสำคัญในสมภูมิทางไซเบอร์ทันที

แม้ว่านักวิชาการในสำนักเคลาซวิทซ์นิยม (Clausewitzian) บางท่านจะเห็นว่าประเด็นความขัดแย้งทางด้านไซเบอร์นั้นอยู่เพียงแค่ในระดับของการทหาร[19] แต่หากเราพิจารณาถึงความจริงที่ว่ารัฐชาติในปัจจุบันล้วนมีระบบอันเป็นโครงสร้างพื้นฐานไม่ว่าจะเป็นระบบทางการเงิน ระบบสาธารณูปโภค หรือระบบขนส่งมวลชนที่ต้องพึ่งพาระบบคอมพิวเตอร์ ดังนั้นผลกระทบของการถูกโจมตีทางไซเบอร์จึงย่อมมีผลกระทบต่อการดำเนินชีวิตของประชาชนทั่วไปเป็นวงกว้างได้ไม่ต่างจากการถูกโจมตีทางกายภาพ สงครามไซเบอร์จึงถือเป็นภัยคุกคามสำคัญต่อความมั่นคงของรัฐในปัจจุบัน

นอกจากนี้ หากเรานำเอานิยามสงครามไซเบอร์ของ ริชาร์ด เอ.คลาร์ก มาพิจารณาอีกครั้ง ก็จะพบว่าหลายๆ กรณีที่ผู้เขียนได้หยิบยกมาอธิบายในบทความชิ้นนี้ไม่ว่าจะเป็น การใช้สตักซ์เน็ตของสหรัฐฯ การโจมตีบริษัทโซนี่ หรือกระทั่งการแทรกแซงทางการเมืองของรัสเซีย ก็ยังสามารถถูกตีความให้ลักษณะเป็นสงครามไซเบอร์ได้ด้วยเช่นกัน

ประเด็นท้าทายที่เกิดขึ้นต่อการเมืองระหว่างประเทศในปัจจุบันจึงเป็นประด็นที่ว่า “อะไรคือความถูกผิดในสงครามไซเบอร์” ทั้งนี้เพราะในปัจจุบัน ยังไม่มีกฎหมายหรือบรรทัดฐานใดๆ ที่สามารถรองรับหรืออธิบายสิ่งที่ควรจะเป็นของการเมืองระหว่างประเทศในพื้นที่ทางไซเบอร์ได้

แนวคิดเรื่องสงครามที่ยุติธรรมนั้นไม่สามารถนำมาประยุกต์ใช้กับสงครามไซเบอร์ได้ เพราะตัวแสดงที่สามารถทำสงครามไซเบอร์ได้นั้นไม่ได้เป็นเพียงแค่รัฐอีกต่อไป โดยองค์กร กลุ่มบุคคล หรือบุคคลเพียงคนเดียวที่มีทักษะและความสามารถในด้านนี้ก็ล้วนสามารถก่อสงครามไซเบอร์ได้ นอกจากนี้โจมตีทางไซเบอร์ยังสามารถปกปิดตัวตนของตนเองได้จากการปลอมแปลงที่อยู่ และแม้ว่าเหยื่อจะสามารถสืบทราบที่อยู่ของผู้กระทำการได้ แต่ก็ยังไม่มีสิ่งใดที่สามารถอธิบายเจตนารมย์ของการโจมตีนั้นๆ ได้ว่ามีที่มาจากคำสั่งของรัฐหรือความต้องการส่วนบุคคล

[17]ริชาร์ด คลาร์ก และ โรเบิร์ต ดเนค, สงครามไซเบอร์, แปลโดย ไพรัตน์ พงศ์พานิชย์ (กรุงเทพฯ: มติชน, 2010).
[18]Segal, The Hacked World Order, 2-3, 67-73.

ในแง่หนึ่ง เราอาจถือได้ว่าการที่สหรัฐลอบส่งมัลแวร์สตักซ์เน็ตไปทำให้แผนการแยกยูเรเนียมให้บริสุทธิ์ของอิหร่านต้องชะลอลงไปเป็นการกระทำที่ถูกต้องในเชิงศีลธรรม เพราะที่ผ่านมาสหรัฐฯ ก็ได้พยายามหยุดโครงการนิวเคลียร์ของอิหร่านด้วยวิธีการอื่นๆ มาโดยตลอด แต่อิหร่านก็ยังไม่ได้มีท่าทีจะล้มเลิกแผนการดังกล่าว และการที่อิหร่านสามารถพัฒนาอาวุธนิวเคลียร์ได้สำเร็จย่อมก่อให้เกิดปัญหาในเชิงความสัมพันธ์ระหว่างประเทศและปัญหาความมั่นคงของประชาคมโลก แต่ในอีกแง่หนึ่ง การกระทำดังกล่าวของสหรัฐฯก็อาจไม่ถูกต้องในเชิงบรรทัดฐานของการเมืองระหว่างประเทศ เพราะการกระทำดังกล่าวถือเป็นการละเมิดบรรทัดฐานในการไม่เข้าไปแทรกแซงกิจการภายในของรัฐอื่น

บทสรุป

จากประเด็นทั้งหมดที่กล่าวมา ประเด็นเรื่อง “ความมั่นคงทางไซเบอร์” (Cybersecurity) จึงเป็นสำคัญที่รัฐควรให้ความสำคัญเพื่อรับมือกับความขัดแย้งภายใต้การเมืองระหว่างประเทศร่วมสมัย

อย่างไรก็ดี ผู้ปกครองรัฐและผู้มีส่วนเกี่ยวข้องกับกิจการด้านความมั่นคงทางไซเบอร์ควรตระหนักรู้ถึงลักษณะสำคัญของความขัดแย้งทางไซเบอร์ประการหนึ่ง นั่นคือการที่ ประเด็นทางไซเบอร์แม้จะเกิดขึ้นในพื้นที่ทางไซเบอร์ แต่จำเป็นต้องได้รับการแก้ไขจากพื้นที่ทางกายภาพ ทั้งนี้ เพราะ “การโจมตีทางไซเบอร์เป็นเพียงอาการของโรค”[20] (Cyberattacks are a Symptom) กล่าวคือ การโจมตีทางไซเบอร์เป็นผลพวงของขัดแย้งระหว่างรัฐในพื้นที่กายภาพ ไม่ว่าจะเป็นความขัดแย้งทางด้านผลประโยชน์ อุดมการณ์ หรือเป็นเพียงการแข่งขันเชิงอำนาจตามธรรมชาติของการเมืองระหว่างประเทศ ดังนั้น การจะป้องกันและแก้ไขปัญหาทางไซเบอร์ที่จะเกิดขึ้นจึงต้องอาศัยความสามารถของผู้นำในการรับรู้และรักษาโรคให้ถูกวิธี นั่นคือการแก้ปัญหาที่ประเด็นด้านภูมิรัฐศาสตร์ และใช้ทักษะทางด้านการเมืองนำทักษะทางด้านเทคนิคในการแก้ไขปัญหา

[19]Marco Cepik, Diego Canabarro, and Thiago Borne Ferreira, Cyberwar: Clausewitzian Encouters, accessed April 1, 2017, http://professor.ufrgs.br/marcocepik/files/cepik__canabarro__borne_-_2015_-_cyberwar.pdf.
[20]Dmitri Alperovitch, “The Case for Cyber-Realism: Geopolitical Problems Don’t Have Technical Solutions,” Foreign Affairs, accessed May 5, 2022, https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism.