ความมั่นคงทางไซเบอร์และผลประโยชน์แห่งชาติ: กรณีศึกษาประเทศสหรัฐอเมริกา, รัสเซีย, จีน และ เกาหลีเหนือ*

Cyber Security and National Interest: Case Studies of U.S.A., Russia, China and North Korea

[1]อลงกรณ์ ศิลปดอนบม

[1]Alongkorn Sillapadonbom

[1]มหาวิทยาลัยมหาสารคาม

[1]Mahasarakham University, Thailand

[1]Corresponding Author's E-mail: alongkorn.liberty@gmail.com

บทคัดย่อ

ความมั่นคงทางไซเบอร์ กลายมาเป็นประเด็นสำคัญต่อการดำรงอยู่ของรัฐต่างๆ เนื่องด้วยกระแสโลกาภิวัตน์ที่นำพาการพัฒนาเทคโนโลยีกระจายสู่นานาประเทศ ทำให้เกิดการเข้าถึงของข้อมูลต่างๆ และการนำไซเบอร์เข้ามามีส่วนเกี่ยวข้องในกระบวนการและดำเนินนโยบายต่างๆของประเทศ เพื่อผลประโยชน์แห่งชาติ บทความวิชาการชิ้นนี้ เป็นการนำกรณีศึกษาของประเทศสหรัฐอเมริกา รัสเซีย จีน และเกาหลีเหนือ ที่มีเนื้อหาเกี่ยวกับความมั่นคงทางไซเบอร์ ผลประโยชน์แห่งชาติ และการทำสงครามไซเบอร์ วิเคราะห์ผ่านแนวคิดผลประโยชน์แห่งชาติและทฤษฎีสัจนิยมแบบดั้งเดิม ผลการวิเคราะห์ทำให้เห็นถึงบริบทของประเทศที่แตกต่างกันในการนำไซเบอร์มาใช้ในการดำเนินกิจการภายในประเทศและการทำสงครามด้วยไซเบอร์ โดยการกระทำทั้งหมดนั้น เป็นการกระทำเพื่อผลประโยชน์แห่งชาติ ดังนั้น แต่ละประเทศจึงต้องรักษาความมั่นคงทางไซเบอร์เพื่อเป็นการรักษาผลประโยชน์แห่งชาติด้วยวิธีการที่แตกต่างกันออกไป

คำสำคัญ: สงครามไซเบอร์; ผลประโยชน์แห่งชาติ; ความมั่นคงทางไซเบอร์

Abstract

Cyber security has significantly become important for some countries. Globalization had been spreading innovation technology through global included cyber. Data accessibility and cyber operations get involved in every activities and policy-making process creates national interest for every country. This article illustrates case studies from the U.S.A, Russia, China, and North Korea about their cyber security, national interest, and cyber warfare and analyzes through the concept of national interest and traditional realism. The result shows

*Received December 15, 2021; Revised December 22, 2021; Accepted December 29, 2021

that contextually defined, dependent on various activities that some countries operate cyber to their demands for anything whether it is for domestically or cyber warfare. All cyber actions are being utilized to create national interest. Then each country must secure its cyber security to ensure by using different strategies.

Keywords: Cyber warfare; National interest; Cyber security

บทนำ

นิยามของคำว่า “cyber” นั้นมีความซับซ้อนกว่าที่คนในยุคปัจจุบันเข้าใจ เดิมทีต้นกำเนิดมาจากคำว่า “Cyberspace” ในนวนิยายวิทยาศาสตร์ของ Gibson ใน ค.ศ. 1984 ที่ให้นิยามว่า “Cyberspace” ว่า “เป็นการแสดงถึงสิ่งแวดล้อมที่สมมุติขึ้นมา” ต้นกำเนิดของคำว่า cyber มีรากศัพท์มาจากภาษากรีกโบราณคำว่า “kybereo” ที่มีความหมายว่า การช่วยเหลือ, การควบคุมทาง, การแนะนำ, การควบคุม, การบริหาร (Lehto, 2013) และจากการที่ Gibson ได้นำคำศัพท์นี้มาใช้ในคำว่า Cyberspace ซึ่งได้ให้ความหมายของ cyberspace ในนวนิยายวิทยาศาสตร์ของเขาว่า “เป็นการแสดงภาพของข้อมูลจากคอมพิวเตอร์ทุกเครื่องในการใช้งานของมนุษย์” หลังจากนั้นทำให้การใช้คำที่เกี่ยวกับ Cyber ได้ถูกหยิบยกขึ้นมาในฐานะของการแสดงออกถึงนามธรรมหรือสิ่งแวดล้อมต่างๆที่เกิดขึ้นในโลกของอินเตอร์เน็ตและคอมพิวเตอร์ ในปัจจุบันคำว่า “ไซเบอร์” ได้กลายเป็นคำที่นิยมและคุ้นชินสำหรับสังคม ณ ปัจจุบัน การติดต่อสื่อสาร เทคโนโลยี การเก็บข้อมูล การเงิน เศรษฐกิจและสังคมต้องพึ่งพาไซเบอร์ การเชื่อมต่อของไซเบอร์ ได้สร้างสิ่งที่เรียกว่า “พื้นที่ของไซเบอร์” หรือ Cyberspace ที่เป็นพื้นที่สำหรับการเชื่อมต่อต่างๆ ที่ของเทคโนโลยีไซเบอร์ พัฒนาการของเทคโนโลยีสร้างความแปลกใหม่ในการดำรงชีวิตของมนุษย์ในการพึ่งพาไซเบอร์ในการใช้ชีวิตประจำวันในด้านต่างๆ แต่อีกด้านหนึ่งของไซเบอร์นั้น สามารถเป็นภัยร้ายแรงสำหรับการใช้ชีวิตประจำวันได้ด้วยเช่นกัน ไม่ว่าจะเป็นการเกิดจาก Digital Hacking หรือ การแฮ็กข้อมูลเพื่อนำข้อมูลไปใช้เพื่อประโยชน์ส่วนตน Digital Stalking หรือ การเฝ้าดูการเคลื่อนไหวของผู้ใช้งาน Viruses หรือ การทำลายข้อมูลทางไซเบอร์ด้วยไวรัสทางไซเบอร์ และ Encryption หรือ การทำให้ข้อมูลที่มีอยู่หายไปและสามารถดูได้เพียงผู้ส่งสารและผู้รับสาร (Mitra, 2010) การถูกโจมตีทางไซเบอร์หรือที่เรียกว่าสงครามไซเบอร์นั้น สามารถสร้างความเสียหายต่อประเทศได้ภายในระยะเวลาไม่กี่ชั่วโมง เช่น การทำลายสถาบันทางการเงิน การระงับการเข้าถึงการเงิน รวมไปถึงการแฮ็กเอาข้อมูลมาเพื่อใช้ในทางการทหารโดยใช้ไซเบอร์ ล้วนแต่ส่งผลต่อความมั่นคงของภาครัฐและอธิปไตยของประเทศ ดังนั้นแต่ละประเทศจึงใช้ความสามารถของไซเบอร์ในการสร้างผลประโยชน์ให้กับรัฐของตน หรือใช้เพื่อป้องกันการถูกโจมตีทางไซเบอร์ระหว่างประเทศที่ไม่คาดคิดในอนาคต

บทความวิชาการชิ้นนี้อาศัยวิธีวิจัยเชิงเอกสาร (Documentary Research Method) มีวัตถุประสงค์เพื่อวิเคราะห์การใช้ไซเบอร์เพื่อผลประโยชน์แห่งชาติของแต่ละประเทศ และจุดประสงค์ที่แตกต่างกันในการใช้ไซเบอร์ของแต่ละประเทศ และการทำสงครามไซเบอร์ โดยศึกษาจากเอกสารวิจัยต่างๆ ที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ การทำสงครามไซเบอร์ และผลประโยชน์แห่งชาติของแต่ละประเทศ และนำมาวิเคราะห์

เปรียบเทียบถึงพฤติกรรมการใช้ไซเบอร์ของแต่ละประเทศ โดยการศึกษาความสัมพันธ์ระหว่างประเทศ คือ การศึกษาความสัมพันธ์ระหว่างรัฐแต่ละรัฐ ที่มีการแลกเปลี่ยนเชิงนโยบายต่างประเทศ รวมถึงการตัดสินใจต่างๆ ไม่ว่าจะเป็นความร่วมมือหรือความขัดแย้ง โดยคำนึงถึง “ผลประโยชน์แห่งชาติ” ในการเป็นเหตุผลเพื่อสนับสนุนอุดมการณ์ของตนในการกระทำสิ่งต่างๆ รวมถึงการก่อสงครามด้วยเช่นกัน อาทิเช่น การที่สหรัฐอเมริกาประกาศทำสงครามการค้ากับจีนเพื่อรักษาผลประโยชน์แห่งชาติ หรือการพัฒนาอาวุธนิวเคลียร์เพราะอาวุธนิวเคลียร์เป็นผลประโยชน์แห่งชาติของเกาหลีเหนือ (Putthiwanich, 2021)

ผลประโยชน์แห่งชาติมีนิยามที่แตกต่างกัน อาทิเช่น Morgenthau (1952) ได้ให้ความหมายว่า “ผลประโยชน์แห่งชาติ คือ ความอยู่รอด ซึ่งหมายถึงการปกป้องหรือรักษาไว้ซึ่งอัตลักษณ์ทางกายภาพ การเมือง และวัฒนธรรมให้รอดพ้นจากการรุกรานโดยชาติอื่นๆ” (Morgenthau, 1952 as cited in Putthiwanich, 2021) ในขณะเดียวกัน Dyke (1962) ให้นิยามว่า “ผลประโยชน์แห่งชาติ คือสิ่งที่รัฐต้องปกป้องหรือบรรลุเมื่อเปรียบเทียบกับผลประโยชน์อื่นๆ ซึ่งหมายถึงความปรารถนาในส่วนของการไม่ขึ้นต่อใคร” (Dyke, 1962 as cited in Putthiwanich, 2021) ผลประโยชน์แห่งชาติ สามารถแบ่งตามประเภทต่างๆตามการพิจารณาถึงปัจจัยที่ใช้มองผลประโยชน์แห่งชาติ ดังนี้ 1) พิจารณาจากระดับความสำคัญของผลประโยชน์แห่งชาติ สามารถจำแนกเป็น ผลประโยชน์ปฐมภูมิ หมายถึง ผลประโยชน์ที่ไม่สามารถใช้ในการต่อรองได้ เป็นผลประโยชน์ที่จะเกิดความเสียหายต่อรัฐและอธิปไตยโดยตรง และ ผลประโยชน์ทุติยภูมิ หมายถึง ผลประโยชน์ที่สำคัญต่อการดำรงอยู่ของรัฐ แต่ไม่สำคัญเท่าผลประโยชน์ปฐมภูมิ ซึ่งสามารถต่อรองด้วยการเจรจาได้ เช่น ผลประโยชน์ด้านเศรษฐกิจ การช่วยเหลือระหว่างประเทศ การรักษาข้อตกลงระหว่างประเทศ เป็นต้น 2) พิจารณาจากระยะหวังผล สามารถแบ่งได้เป็นผลประโยชน์ระยะยาว หมายถึง ผลประโยชน์ที่เปลี่ยนแปลงได้ยากและมีความสำคัญในการใช้ระยะเวลาในการดำเนินการ และระยะสั้น หมายถึง ผลประโยชน์ที่ไม่ถาวร และเป็นเพียงบางโอกาส มีความผันแปรในการเปลี่ยนแปลงสูง 3) พิจารณาความเฉพาะเจาะจงของผลประโยชน์แห่งชาติ สามารถแบ่งได้เป็น ผลประโยชน์ทั่วไป หมายถึง ผลประโยชน์ที่มีความกว้างขวางและครอบคลุม ซึ่งส่วนมากเป็นเรื่องทั่วไปของประชาคมระหว่างประเทศ เช่น ประชาธิปไตย หลักสิทธิมนุษยชน และการค้าเสรี และ ผลประโยชน์เฉพาะด้าน คือ ผลประโยชน์ที่มีความชัดเจนในข้อตกลงต่างๆที่เกิดขึ้น รวมถึงมีการกำหนดเงื่อนไขที่ชัดเจน 4) พิจารณาจากการได้มาของผลประโยชน์นั้นๆ แบ่งได้เป็น ผลประโยชน์จากการได้มาโดยเปรียบเทียบ (Relative Gains) หมายถึง การได้ผลประโยชน์จากการสูญเสียของอีกฝ่าย หรือแบบ “Zero-sum Game” ซึ่งเป็นเรื่องที่เกี่ยวกับความมั่นคงของรัฐ เช่น การครอบครองอาวุธ ที่ต่างฝ่ายต่างแข่งกันครอบครองอาวุธเพื่ออำนาจในการต่อรอง หรือ ความมั่นคงแห่งชาติของประเทศตน และ ผลประโยชน์จากการได้มาโดยสัมบูรณ์ (Absolute Gains) หมายถึง การได้รับผลประโยชน์ซึ่งกันและกัน โดยไม่มีการคำนึงถึงฝ่ายตรงข้ามว่าจะได้ผลประโยชน์มากหรือน้อยเพียงใดเป็นการตั้งเป้าหมายเพียงเพื่อได้ผลประโยชน์บางอย่างเท่านั้น (Putthiwanich, 2021)

บทความนี้นำแนวคิดผลประโยชน์จากการได้มาโดยเปรียบเทียบ มาใช้ในการอธิบายความมั่นคงทางไซเบอร์และผลประโยชน์แห่งชาติของแต่ละประเทศ รวมไปถึงการทำสงครามระหว่างรัฐเพื่อผลประโยชน์แห่งชาติของตน ซึ่งโยงไปถึง ทฤษฎีสัจนิยมแบบดั้งเดิม (Classical Realism) เป็นทฤษฎีที่ให้ความสำคัญกับ

การดำรงอยู่ของ “อำนาจ” (Power) ของรัฐ ที่เป็นเครื่องมือในการอยู่รอดและความมั่นคงของรัฐ และในขณะเดียวกัน อำนาจ ก็ถูกใช้ในการเมืองระหว่างประเทศในรูปแบบของ “การต่อสู้ช่วงชิงอำนาจ” (Struggle for Power) ด้วยเช่นกัน โดยจุดเชื่อมโยงของผลประโยชน์แห่งชาติ และอำนาจนั้น สามารถอธิบายได้ 3 รูปแบบคือ นโยบายขยายอำนาจ (Imperialism) เป็นการได้มาของอำนาจโดยการขยายดินแดน, การกำจัดภัยคุกคามต่อชาติ และการเข้าครอบงำผู้อื่น นโยบายรักษาสถานะอำนาจ (Status Quo Ante Bellum) เป็นการรักษาสถานะความสัมพันธ์ระหว่างประเทศเพื่อหลีกเลี่ยงสงคราม และนโยบายเพื่อเกียรติยศ (Policy for Prestige) คือการให้ความสำคัญต่อความต้องการหรือความคาดหวังของประชาชนที่มีต่อรัฐบาลของตน (Putthiwanich, 2021) สำหรับบทความนี้ผู้เขียนจะใช้ทฤษฎีดังกล่าวมาวิเคราะห์ประเทศสหรัฐอเมริกา จีน รัสเซีย และเกาหลีเหนือ ตามลำดับ

ประเทศสหรัฐอเมริกา

ภายหลังการโจมตีของกลุ่มก่อการร้าย Al Qaeda ในเหตุการณ์ 911 รัฐบาลของประเทศสหรัฐอเมริกาได้ประกาศถึงการให้ความสำคัญต่อการปกป้อง Cyberspace ว่าเป็นเรื่องสำคัญสำหรับความมั่นคงของประเทศ และเป็นสิ่งที่ท้าทายประเทศมหาอำนาจอย่างสหรัฐอเมริกาในการพัฒนาโครงสร้างพื้นฐานทางดิจิทัลเพื่อรองรับและป้องกันภัยคุกคามต่าง ๆ ที่จะเกิดขึ้นภายในอนาคต และยังได้มีการออกเอกสารทางการสำคัญต่าง ๆ ในการระบุว่าการปกป้อง Cyberspace คือสิ่งที่ต้องให้ความสำคัญอย่างเร่งด่วนเป็นอันดับต้นๆ รวมถึงการบริหารในยุครัฐบาลของ Barrack Obama ในเดือนพฤษภาคม ค.ศ. 2010 ในเอกสารยุทธศาสตร์แผนความมั่นคงระดับชาติ (National Security Strategy, (NSS)) ที่มีการระบุถึงการให้ความสำคัญต่อกการปกป้อง Cyberspace เป็นครั้งแรก (Peritz, and Sechrist, 2010) จากการกล่าวมาข้างต้น Peritz, and Sechrist (2010) ไม่เห็นด้วยสำหรับการที่ประเทศสหรัฐอเมริกาได้ประกาศว่าการปกป้อง Cyberspace จะกลายเป็นคำสั่งที่สำคัญอันดับต้นๆของภัยความมั่นคงระดับชาติ และภัยที่ส่งผลกระทบต่อโครงสร้างพื้นฐานของระบบดิจิทัลในประเทศนั้น คือ Cybercrime, Cyberespionage และ Cyberterrorism สิ่งที่ถูกประเมินว่าเป็นปัจจัยที่สำคัญต่อภัยความมั่นคงระดับประเทศ คือ Cyberwar ซึ่งเป็นความขัดแย้งระหว่างประเทศ และเป็นส่วนหนึ่งของการทำสงครามด้วยเช่นกัน

ในปี ค.ศ. 2000 คณะกรรมาธิการด้านผลประโยชน์แห่งชาติของสหรัฐอเมริกาจากทั้งสองพรรคการเมืองได้มีการให้ความสำคัญเกี่ยวกับ “ผลประโยชน์แห่งชาติที่สำคัญอย่างยิ่ง” ที่ต้องมีการปกป้องอย่างรัดกุมและเข้มงวดเพื่อความอยู่รอดของประชาชนชาวอเมริกันและการเป็นอยู่อย่างอิสระและอำนาจอธิปไตยของรัฐ โดยในการบริหารของรัฐบาล Bush และ Obama ได้มีการสรุปเนื้อหาเอกสารเกี่ยวกับยุทธศาสตร์ความมั่นคงของประเทศได้เป็น 3 รูปแบบ คือ 1) การสยบรัฐคู่อริ การชนะความขัดแย้ง และการปกป้องประชากร 2) การกีดกันรัฐคู่อริในการคิดค้นและใช้งานอาวุธทำลายล้างที่มีประสิทธิภาพสูง และ 3) การเตรียมพร้อมและวางแผนสำหรับภัยคุกคามในรูปแบบต่างๆอย่างทันท่วงทีต่อสถานการณ์ฉุกเฉิน (Peritz, and Sechrist, 2010) ความมั่นคงทางไซเบอร์ของสหรัฐอเมริกา เกี่ยวข้องกับความมั่นคงแห่งชาติของสหรัฐอเมริกาประกอบด้วยความมั่นคงทางการเงิน พลังงาน ระบบคมนาคม ความมั่นคงทางการทหาร และ ระบบ

สารสนเทศ อาศัยระบบการจัดการข้อมูลทางไซเบอร์ ดังนั้น ความมั่นคงในการวางโครงสร้างรากฐานระบบการจัดการข้อมูลจึงเป็นสิ่งที่รัฐบาลให้ความสำคัญ รวมถึงการที่ทำให้หน่วยข่าวกรองและกระทรวงกลาโหมสหรัฐฯ มีความเห็นตรงกันในเรื่องการปกป้องความมั่นคงทางไซเบอร์นั้น เพราะ Cyberspace ถือเป็นเรื่องสำคัญต่อการทำงานในระบบราชการต่างๆ ยกตัวอย่าง เอกสารรายงานด้านความมั่นคงของหน่วยงานกระทรวงกลาโหมสหรัฐฯ ได้ระบุเอาไว้ในเอกสารว่า “ความล้มเหลวของหน่วยงานกระทรวงกลาโหมในการปกป้อง Cyberspace จะทำให้เกิดความเสี่ยงต่อความสามารถในการปฏิบัติการภารกิจต่างๆทั้งใน ปัจจุบัน และอนาคต” (Peritz, and Sechrist, 2010) ดังเช่นตัวอย่างจากการถูกแฮ็กเข้าระบบเพื่อดาวน์โหลดเทคโนโลยีการออกแบบเครื่องบินแบบใหม่ล่าสุดของประเทศสหรัฐอเมริกาในปี 2009 (Mount, 2009)

ประเทศสหรัฐอเมริกา นำอาวุธทางไซเบอร์มาประยุกต์ใช้ในยุทธศาสตร์ทางการทหารและการใช้ความสามารถทางไซเบอร์ในการโจมตีค่าเงิน โดยภายหลังจากที่ ISIS ได้ก่อการร้าย และมีการฆ่านักข่าวชาวอเมริกัน ประธานาธิบดี Barrack Obama ได้เริ่มทำสงครามกับกลุ่มก่อการร้าย โดยเป้าหมายสำคัญคือการตั้งเป้าไปที่สถาบันการเงินของรัฐอิสลาม พุ่งทำลายค่าเงินด้วยการโจมตีทางอากาศ ผลลัพธ์ที่เกิดขึ้นคือ สงครามในการทำลายค่าเงินนั้น ปรากฏเห็นอย่างเด่นชัดมากขึ้น และถูกพูดถึงอย่างมากในการลดทอนกำลังของฝ่ายศัตรูด้วยการใช้สงครามทำลายเงินตรา การทำลายประสิทธิภาพในการเข้าถึงเงินตราโดยการใช้ความสามารถทางไซเบอร์ เพื่อโจมตีการเข้าถึงแหล่งเงินทุนของกลุ่มก่อการร้าย ส่งผลให้กลุ่มก่อการร้ายไม่สามารถเข้าถึงการจัดซื้ออาวุธจากตลาดค้าอาวุธนานาชาติต่างๆ รวมถึงการใช้ระบบไซเบอร์ในการตัดการเข้าถึงเงินของกลุ่มก่อการร้ายที่มีการพยายามปกปิดโดยนำเงินตราต่างๆแปรรูปไว้ในรูปแบบค่าเงินดิจิทัล หรือ บิทคอยน์ และมีการใช้ Dark Web เพื่อเพิ่มค่าเงินของบิทคอยน์อีกด้วย และการลดค่าเงินของรัฐอิสลาม เป็นการกระทำที่สหรัฐอเมริกาพยายามโจมตีศัตรูจากตัวอย่างที่ได้กล่าวไปนั้น ประเทศสหรัฐอเมริกา ได้ใช้ความมั่นคงทางไซเบอร์และความสามารถทางไซเบอร์ ในการทำสงครามค่าเงิน โดยได้สร้างยุทธศาตร์ใหม่ในการโจมตีนั่นคือการโจมตีค่าเงินในช่วงสภาวะสงครามจากการใช้ไซเบอร์ และจากตัวอย่างที่กล่าวไปนั้น การพุ่งเป้าหมายไปยังสถาบันการเงิน กลายเป็นแผนการหนึ่งในการดำเนินการทางทหาร การเปลี่ยนแปลงทางเทคโนโลยี ได้ทำให้เกิดการสร้างสงครามค่าเงินขึ้นมา และความซับซ้อนของอำนาจทางไซเบอร์ กลายเป็นปัจจัยสำคัญของแต่ละประเทศในการสร้างอำนาจทางการเมือง และการให้ความสำคัญกับการเปลี่ยนแปลงของธรรมชาติของค่าเงิน สถาบันการเงิน และอัตราการแลกเปลี่ยนค่าเงิน ที่จะเป็นเป้าหมายในอนาคตหากเกิดสภาวะสงครามเกิดขึ้น ทำให้สหรัฐอเมริกาได้สร้างผลประโยชน์ระหว่างประเทศจากการทำสงครามทางไซเบอร์ขึ้นมาจากการทำสงครามค่าเงิน (Crespo, 2018)

ประเทศรัสเซีย

ประเทศรัสเซียมีความสามารถทางไซเบอร์ ไม่ว่าจะเป็นการโจมตีประเทศยูเครนและจอร์เจีย หรือการแฮ็กและแอบสอดส่องขั้นตอนการทำงานของประเทศสหรัฐอเมริกา และการแทรกแซงการเลือกตั้งในทวีปยุโรป พัฒนาการทางไซเบอร์ของประเทศรัสเซียได้มีการพยายามปิดและป้องกันข้อมูลทางดิจิทัลของประเทศตนเอง โดยใช้กฎหมายและขั้นตอนต่างๆ ในความพยายามควบคุมโครงสร้างพื้นฐานทางดิจิทัล รวมถึงเนื้อหา

ต่างๆ ที่สามารถทำให้ระบบไซเบอร์ของประเทศรัสเซีย เป็นอิสระจากการสอดส่องหรือตรวจสอบจากทั่วโลก ในมุมมองของประเทศรัสเซียที่มีต่อ Cyberspace นั้น คือการเผชิญหน้าของข้อมูล (Information confrontation) ที่สามารถทำให้เกิดผลประโยชน์ได้ไม่ว่าจะเป็นในทางโครงสร้างพื้นฐานแบบกายภาพ และองค์ความรู้ที่สามารถนำไปใช้ในการบิดเบือนข้อมูลจนำให้เกิดความเสียหายต่อรัฐได้ เพราะการเผชิญหน้าของข้อมูลต่างๆ จะเป็นการนำข้อมูลไปสู่ความคิดของประชาชนและมุมมองต่อเหตุการณ์ต่างๆ ไม่ว่าจะเป็นภายในประเทศหรือนานาชาติ โดยประเทศรัสเซียได้ให้คุณค่าของคำว่า “Information Confrontation” มากกว่า “ Cyberspace” โดยการจำกัดขอบเขตของคำว่า Cyberspace ให้เป็นเพียงส่วนหนึ่งของ Information Confrontation ซึ่งนิยามที่กระทรวงความมั่นคงของประเทศรัสเซีย ได้ให้คำนิยามว่า การเผชิญหน้าของข้อมูล Information Confrontation นั้น คือการโจมตีโครงสร้างชุดข้อมูลที่ส่งผลกระทบต่อผลประโยชน์แห่งชาติและอุดมคติของชาติ และในขณะเดียวกัน ก็เป็นการปกป้องผลประโยชน์แห่งชาติและอุดมคติของชาติด้วยเช่นกัน (Hakala, and Melnychuk, 2021)

ผลประโยชน์แห่งชาติของประเทศรัสเซีย คือ 1) เพื่อป้องกันไม่ให้เกิดการใช้อาวุธนิวเคลียร์หรืออาวุธต่างๆ ที่มีประสิทธิภาพทำลายล้างสูงต่อประเทศรัสเซียและป้องกันการแพร่ขยายอาวุธนิวเคลียร์และระบบเคลื่อนย้ายนิวเคลียร์ในเขตประเทศพื้นที่หลังจากการล่มสลายของสหภาพโซเวียต 2) เพื่อสร้างความมั่นคงความสามารถในการยับยั้งนิวเคลียร์ของประเทศรัสเซีย 3) เพื่อเป็นการรักษาอำนาจอธิปไตยของรัสเซียและการคงไว้ซึ่งการเป็นประเทศมหาอำนาจ เพื่อป้องกันการก่อการร้ายที่มีภัยต่อประเทศรัสเซีย 4) เพื่อรักษาอิทธิพลของประเทศรัสเซียในเขตประเทศพื้นที่หลังจากการล่มสลายของสหภาพโซเวียต 5) การสร้างหลักประกันในการสร้างผลกำไรจากการส่งออกพลังงานและการสร้างความมั่นใจว่าจะไม่มีรัฐอื่นๆ ส่งผลกระทบต่อการส่งออกพลังงานของประเทศรัสเซีย 6) การรักษาความมั่นคงและปลอดภัยของระบบการเมืองรัสเซีย และ 7) การป้องกันและสนับสนุนผลประโยชน์ทางเศรษฐกิจกับกลุ่มผลประโยชน์ทางธุรกิจการเมืองที่เป็นพันธมิตรกับชนชั้นนำของประเทศรัสเซีย (Allison, and Blackwill, 2011)

สำหรับรัฐบาลของประเทศรัสเซียนั้น การนิยามคำที่เกี่ยวข้องกับคำว่า Cyber เป็นการปกป้องข้อมูลที่เป็นองค์ความรู้และวัฒนธรรมของชาติและการทำให้การไหลเวียนของข้อมูลเป็นไปอย่างราบรื่นในการทำงาน โดยใน ค.ศ. 1992 ประเทศรัสเซียได้มีการก่อตั้งสภาความมั่นคงของประเทศรัสเซีย และต่อมาได้มีการก่อตั้งองค์กรที่รับผิดชอบเกี่ยวกับความมั่นคงทางไซเบอร์ ได้แก่ The Security Council, The Federal Security Service (FSB), The Federal Guard Service, The Federal Technical and Export Control Service และ The Ministry of Information Technologies and Communications ซึ่งมีการแบ่งหน้าที่ความรับผิดชอบอย่างชัดเจนในแต่ละภาคส่วน โดย กระทรวงการต่างประเทศ รับผิดชอบในส่วนของอาชญากรรมทางไซเบอร์ (Cyber Crime) กระทรวงกลาโหม รับผิดชอบในส่วนของสงครามไซเบอร์ (Cyber Warfare) และ FSB ทำหน้าที่รับผิดชอบในส่วนของการก่อการร้ายทางไซเบอร์ (Cyber Terrorism) รวมถึงความมั่นคงทางไซเบอร์ภายในประเทศ โดยรัฐบาลให้ความสำคัญหลักๆ 3 ประเด็นคือ 1) อาชญากร 2) ผู้ก่อการร้าย และ 3) ภัยคุกคามทางการทหารและการเมือง จาก Cyberspace (Gady, and Austin, 2010)

สงครามไซเบอร์ของรัสเซีย มีจุดเริ่มต้นจากสงครามรุสโซ่จอร์เจีย ค.ศ. 2008 เริ่มต้นขึ้นหลังสงครามเย็น โดยรัสเซียได้เริ่มกลับมามีอำนาจและถูกเปรียบเทียบว่าเป็นประเทศมหาอำนาจเทียบเท่ากับสหรัฐอเมริกา รัฐบาลรัสเซียมีความเกรงกลัวว่ารัฐต่างๆ โดยรอบที่เป็นอดีตสหภาพโซเวียตจะมีความพัฒนาทางด้านเศรษฐกิจและความมั่นคงจนอาจเป็นภัยต่อรัสเซีย ทางรัสเซียจึงได้ดำเนินการใช้กองกำลังทั้งที่เป็นแบบทางการทหารและไม่เป็นทางการทหาร เช่น การนำความสามารถในการใช้ไซเบอร์ ในแผนการกู้คืนเขตแดนหรือเขตพื้นที่ที่เคยเป็นของรัสเซียในสมัยจักรวรรดิ จุดเริ่มต้นของสงคราม รุสโซ่ จอร์เจียน คือ การที่จอร์เจียยิงปืนใหญ่ ในการต่อกรกับเมือง ซคินวาลี ซึ่งเป็นเมืองหลวงของประเทศเซาท์ออสซีเชีย หนึ่งในเขตที่มีข้อพิพาทกับประเทศจอร์เจีย โดยประเทศ อับคาเซีย และ เซาท์ออสซีเชีย นั้น ได้รับการสนับสนุนทางทหารจากรัสเซีย เหตุผลในการที่รัสเซียเข้ามามีส่วนเกี่ยวข้องในความขัดแย้งนั้น เพราะความกังวลของปูตินที่มีต่อประธานาธิบดีของจอร์เจียที่ได้เปิดรับนโยบายของชาวตะวันตกที่มีความสนใจในการเข้าร่วมกับ NATO และ EU การขยายอิทธิพลของ NATO เข้าสู่ประเทศจอร์เจียนั้น อาจเป็นความพยายามในการรุกล้ำเข้าหาประเทศรัสเซีย (Crespo, 2018) ต่อมาหลังจากที่การยิงปืนใหญ่ของจอร์เจียในเมือง ซคินวาลี ของประเทศเซาท์ออสซีเชีย รัสเซียเริ่มรุกรานจอร์เจีย รัสเซียได้ทำการใช้ความสามารถทางไซเบอร์ในการตัดสัญญาณเว็บไซต์ต่างๆของรัฐบาลจอร์เจียและสถาบันการเงิน เช่น ธนาคารแห่งชาติ รวมถึงการแฮ็กข้อมูลทางด้านมีเดีย การเงิน ข้อมูลคณะรัฐมนตรี ตำรวจ กองกำลังทางทหาร และระบบอินเทอร์เน็ตทั้งประเทศ แสดงให้เห็นถึงความพยายามในการใช้ไซเบอร์ในการทำสงครามและโจมตีสถาบันทางการเงินในสนามรบ (Crespo, 2018) อีกหนึ่งตัวอย่างคือ สงครามยูเครนตั้งแต่ ค.ศ. 2014 เป็นต้นมา เกิดจากการที่รัสเซียมีความกลัวในการถูกคุกคามจากฝั่งยุโรปตะวันตกเข้าสู่ยุโรปตะวันออก และด้วยความสัมพันธ์ทางประวัติศาสตร์ของยูเครนและรัสเซีย โดยปูตินเชื่อว่ายูเครนคือส่วนหนึ่งของประเทศรัสเซีย ดังนั้น เมื่อการตัดสินใจของยูเครนในการสนใจเข้าร่วมกับฝั่งตะวันตกจึงส่งผลกระทบโดยตรงต่ออำนาจในภูมิภาคและอัตลักษณ์ของประเทศรัสเซีย และ ปูตินต้องการผนวกยูเครนเข้ามาเป็นส่วนหนึ่งของรัสเซีย รัสเซียได้ใช้ความขัดแย้งดังกล่าวในการเป็นสนามทดลองการใช้ปฏิบัติการสงครามไซเบอร์ โดยมีการโจมตีโดยใช้สงครามไซเบอร์ในยูเครนเป็นระยะเวลากว่า 3 ปี เป็นการโจมตีสื่อมีเดีย สถาบันการเงิน ระบบคมนาคมขนส่ง กองกำลังทหาร การเมือง และพลังงาน รวมถึงการลดทอนอำนาจอธิปไตยของยูเครนและความชอบธรรมในเขตแดนของประเทศยูเครน นอกจากการโจมตีทางไซเบอร์แล้ว ยังมีการโจมตีค่าเงินโดยใช้ไซเบอร์ด้วยเช่นกัน (Crespo, 2018)

ประเทศจีน

ความกว้างใหญ่ของประเทศจีน และจำนวนประชากรที่มากถึง 1,446,463,533 คน (Worldometers, 2021) ซึ่งเป็นจำนวนประชากรที่มากที่สุดในโลก ได้นำมาสู่ปัญหาด้วยเช่นกัน โดยภายหลังจากการที่เทคโนโลยีอินเทอร์เน็ตได้กลายเป็นสิ่งที่ถูกใช้ในชีวิตประจำวันอย่างกว้างขวางนั้น ความมั่นคงและความปลอดภัยทางไซเบอร์จึงกลายมาเป็นปัญหาต่อมาของประเทศจีน โดยใน ค.ศ. 2011 มีประชากรชาวจีนถูกแฮ็กคอมพิวเตอร์จำนวน 8,531 ล้านเครื่องต่อวัน และจากผลสำรวจชิ้นหนึ่งแสดงให้เห็นว่า ร้อยละ 60 จากจำนวนประชากร 2,500 คน เคยถูกขโมยข้อมูลส่วนบุคคลจากการโจรกรรมทางไซเบอร์ (Yuxiao, 2011) การดำเนิน

นโยบายในการพัฒนาประเทศของจีนนั้น ในช่วงรัฐบาลหูจิ่นเทา ได้มีการประกาศกลยุทธ์ “การพัฒนาแบบวิทยาศาสตร์” โดยมีเนื้อหาในการตั้งเป้าหมายให้ประเทศจีนก้าวข้ามผ่านสถานะการเป็นประเทศพัฒนาแล้วในระดับกลางสู่ระดับอื่นภายใน ค.ศ. 2050 โดยตั้งเป้าไปยังการส่งเสริมและป้องกัน “ผลประโยชน์แกนกลาง” ซึ่งหมายถึงอำนาจอธิปไตยของประเทศ ความมั่นคง ความสงบสุขของเขตแดน และการพัฒนาภายในประเทศให้เป็นไปอย่างราบรื่น รวมถึงการรักษาความมั่นคงทางสังคม อัตราการเติบโตของเศรษฐกิจ และความสามารถทางการทูตและการทหารในการปกป้องการแพร่ขยายของโลกาภิวัตน์ที่ส่งผลต่อการเจริญเติบโตของผลประโยชน์แห่งชาติ การพัฒนาและกระแสของ Cyberspace ได้กลายมาเป็นประเด็นหลักในแผนการพัฒนาแบบวิทยาศาสตร์ของประเทศจีน โดยมีการกล่าวถึงการทำให้เกิดระบบการควบคุมแบบอัตโนมัติผ่านการวางโปรแกรม (Automation) และความต้องการทางข้อมูลในการใช้ประโยชน์กับเศรษฐกิจ การเมือง ความมั่นคงของระบบสาธารณะ และทางการทหาร (Cooper III, 2011) ในด้านความมั่นคงทางข้อมูลไซเบอร์ของจีน ประเทศจีนให้ความสำคัญอย่างมากในการรวบรวมข้อมูลและองค์ความรู้โดยเจริญรอยตามการใช้ยุทธศาสตร์ของจีน เช่น การใช้วิธีคิดแบบพิชัยสงครามซุนจื่อ ดังนั้นแล้ว การรวบรวมข้อมูลให้มากที่สุด จึงเป็นองค์ประกอบที่สำคัญสำหรับความคิดทางการทหารของประเทศจีน การศึกษาความมั่นคงทางไซเบอร์ของจีนสามารถสืบค้นจากเอกสารทางการทหารที่อธิบายถึง “ความพยายามของกองกำลังทหารของจีนในการพัฒนายุทธศาสตร์ที่เกี่ยวข้องกับ Cyberspace ในเอกสาร แนวปฏิบัติยุทธศาสตร์ทางการทหาร (The Military Strategic Guidelines)” ระบุว่าประเทศจีนให้ความสำคัญอย่างมากในการศึกษาความขัดแย้งในรูปแบบเครือข่ายอินเทอร์เน็ต และการศึกษาเชิงลึกเกี่ยวกับการพัฒนาเทคโนโลยีขั้นสูงสำหรับใช้ในความขัดแย้งในประเทศ และมีการประกาศในเอกสารถึงความสามารถของประเทศจีนที่เกี่ยวข้องกับความเชี่ยวชาญในการทำสงครามในรูปแบบเครือข่ายไซเบอร์ ไม่ว่าจะเป็นทางการทหาร หรือ การปกครองประชาชนภายในรัฐและเอกสารทางการ ความคิดเห็นเกี่ยวกับการสร้างความเข้มแข็งทางการทหารด้วยความมั่นคงทางข้อมูลในอนาคต ที่เป็นความคิดเห็นของประธานาธิบดี สีจิ้นผิง และ คณะกรรมการทหารส่วนกลาง (Raud, 2016)

ใน ค.ศ. 2015 กระทรวงกลาโหมได้ออกเอกสาร ยุทธศาสตร์ทางการทหารของประเทศจีน ที่มีเนื้อหาเกี่ยวกับการให้ความสำคัญอย่างมากในการศึกษาการทำสงครามด้วยความสามารถทางข้อมูล และประเทศจีนได้ประกาศถึงการพัฒนาอย่างต่อเนื่องของกองกำลังไซเบอร์และการส่งเสริมประสิทธิภาพของการศึกษา Cyberspace การปกป้องทางไซเบอร์ รวมถึงการสนับสนุนการมีส่วนร่วมในการทำงานในโลกไซเบอร์ระดับนานาชาติอีกด้วย และประเด็นสำคัญคือ การตั้งเป้าหมายในการสร้างกองกำลังทางข้อมูลที่มีประสิทธิภาพสูงในการชนะสงครามทางไซเบอร์และสงครามทางข้อมูลที่สามารถเกิดขึ้นในอนาคต ความทะเยอทยานในการพัฒนาความสามารถทางไซเบอร์ของประเทศจีนนั้น สามารถตีความได้ถึงความต้องการในการทำลายระบบการทำงานของรัฐคู่อริในช่วงสงครามเพื่อนำพามาซึ่งชัยชนะที่รวดเร็ว เอกสารต่างๆที่กล่าวมาทำให้เห็นถึงการที่ประเทศจีนต้องการใช้สงครามไซเบอร์เป็นส่วนหนึ่งทางยุทธศาสตร์ทางการทหาร การสร้างสนามรบไซเบอร์โดยที่กระทรวงกลาโหมของจีนจะต้องเป็นผู้ชนะอย่างมีประสิทธิภาพ และการเตรียมพร้อมทั้งระยะสั้นและระยะยาวในการโจรกรรมทางไซเบอร์ต่อรัฐคู่อริและภาคเอกชน ไม่ว่าจะเป็นการรวบรวมข้อมูลสำคัญต่างๆ

รวมถึงกลุ่มผู้ต่อต้านรัฐบาลภายในประเทศ เช่น กลุ่มเห็นต่างทางการเมือง และกลุ่มนักกิจกรรมรณรงค์เพื่อประชาธิปไตยเพื่อเป็นการรักษาเสถียรภาพในการควบคุมทางการเมืองภายในระบบคอมมิวนิสต์(Raud, 2016)

ในปี ค.ศ. 2009 ประเทศสหรัฐอเมริกาได้รับรู้ถึงการถูกแฮ็กเครือข่ายพลังงานไฟฟ้า ทำให้เครือข่ายต่างๆสามารถถูกปิดการทำงานเมื่อไรก็ตามที่แฮ็กเกอร์ต้องการจะปิด จากการติดตามต้นทางของการแฮ็กครั้งนี้ปรากฏว่าเป็นการแฮ็กจากประเทศจีน แสดงให้เห็นถึงความไม่มีประสิทธิภาพในการปกป้องระบบเครือข่ายพลังงานไฟฟ้าของประเทศสหรัฐอเมริกา ณ ขณะนั้น และ เหตุการณ์ที่ฐานทัพอากาศยานของสหรัฐอเมริกาถูกรุกรานโดยการตัดการทำงานของเครือข่ายทั้งหมดและการหยุดการทำงานของการปล่อยเครื่องบิน ซึ่งเกิดจากการโจมตีโดยไวรัสจำนวนมากโดยมีต้นทางจากประเทศจีน ในปี ค.ศ. 2009 ได้มีการแฮ็กข้อมูลจำนวนมากเกี่ยวกับเครื่องบินขับไล่โจมตีร่วมของสหรัฐอเมริกา (The Joint Strike Fighter) และการแฮ็กครั้งนี้เป็นการแฮ็กเพื่อคัดลอกข้อมูลต่างๆ โดยกระทรวงกลาโหมได้เปิดเผยว่าต้นทางการแฮ็กมาจากประเทศจีน, เหตุการณ์ที่กระทรวงกลาโหม สหรัฐฯได้มีสถานการณ์ที่กระทบต่อความมั่นคงทางคอมพิวเตอร์ จึงมีการยับยั้งการใช้แท่งเสียบหน่วยความจำ หรือ USB และประเทศจีนเป็นผู้ผลิตรายใหญ่ที่สุดในโลก สหรัฐฯเกรงว่าการใช้ USB นี้จะเป็นการถูกแฮ็กเพื่อส่งข้อมูลกลับไปยังต้นทางของประเทศที่ผลิต ซึ่งแสดงให้เห็นถึงความกลัวและความตึงเครียดจากการทำสงครามไซเบอร์และการแฮ็ก การแฮ็กเข้าสู่คอมพิวเตอร์ของนายกรัฐมนตรี อังเกลา แมร์เคิล ของประเทศเยอรมนี โดยเป็นการแฮ็กเพื่อเข้าโจรกรรมข้อมูลที่เป็นความลับของอุตสากรรมจำนวนมาก รวมถึงความสามารถของการแฮ็กที่อาจส่งผลต่อการก่อวินาศกรรมต่อระบบโครงสร้างพื้นฐานทั้งหมด อาทิเช่น ระบบพลังงานของประเทศเยอรมนี และตัวอย่างสุดท้ายที่น่าสนใจ ใน ค.ศ. 2009 การที่แฮ็กเกอร์จำนวนมหาศาล ทำการแฮ็กเข้าสู่บัญชีลูกค้าของบริษัท Google ซึ่งถูกใช้งานโดยบริษัทเอกชนต่างๆ การบริหารจัดการของสหรัฐ รวมถึง ผู้ผลิตสินค้าต่างๆให้กับกระทรวงกลาโหมสหรัฐ หรือแม้กระทั่งการทำงานของสมาชิกในสภาคองเกรส โดยมีรายงานว่าการแฮ็กครั้งนี้มาจากสถาบันการศึกษาของประเทศจีนทั้งหมดสองสถาบัน คือ สถาบันอาชีวะชานเชียงในจี่หนาน และ มหาวิทยาลัยเซี่ยงไฮ้เจียวทง ในขณะเดียวกัน รายงานเอกสารลับของสำนักงานสอบสวนกลาง หรือ FBI ข้อมูลได้รั่วไหลที่ระบุถึงการที่ประเทศจีนกำลังพัฒนา “กองทัพไซเบอร์” ประกอบด้วย หน่วยสอดแนมทางไซเบอร์จำนวน 30,000 นาย และอีก 15,000 นายจากการจ้างจากภาคเอกชน ในรายงานระบุว่า ภารกิจหลักของหน่วยงานนี้ คือการขโมยข้อมูลทางการทหารของประเทศสหรัฐฯและความลับทางเทคโนโลยี (Hjortdal, 2011)

ประเทศเกาหลีเหนือ

ประเทศเกาหลีเหนือ เป็นหนึ่งในประเทศที่มีตัวตนบนโลกอินเทอร์เน็ตน้อยที่สุด เป็นประเทศที่มีระบบเครือข่ายอินเทอร์เน็ตสำหรับใช้งานภายในประเทศโดยเฉพาะชื่อว่า กวางมยอง หรือ Kwangmyon ที่ใช้สำหรับการใช้งานอีเมล์ เว็บไซต์ และการเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในประเทศ รัฐบาลเกาหลีเหนือได้ทุ่มงบประมาณในการพัฒนาระบบการทำงานด้วยไซเบอร์ ทำให้ประเทศเกาหลีเหนือมีขีดความสามารถสูงในการใช้ไซเบอร์โจมตีเป้าหมายต่างๆ โดยมีนักวิเคราะห์กล่าวว่า ประเทศเกาหลีเหนือกำลังพัฒนาความสามารถทางไซเบอร์ในการโจมตีที่ทำลายล้างได้แบบวงกว้างโดยเป็นการโจมตีเข้าสู่ระบบ

โครงสร้างพื้นฐานที่สำคัญจนสามารถนำไปสู่สงครามไซเบอร์ได้ในอนาคต (Avery et al. 2017) ปัญหานิวเคลียร์ที่เกิดจากการไม่ยอมปลดอาวุธนิวเคลียร์ซึ่งการครอบครองและการผลิตนิวเคลียร์ของประเทศเกาหลีเหนือ ถือเป็นผลประโยชน์แห่งชาติของเกาหลีเหนือ (Powcharoen, 2021) ในแง่ของการใช้ไซเบอร์ในทางการทหารเพื่อผลประโยชน์แห่งชาติ สามารถบ่งบอกได้ถึงความพยายามในการเข้าถึงข้อมูลของรัฐคู่อริต่างๆ ในการใช้ประโยชน์จากการแฮ็กเพื่อผลประโยชน์แห่งชาติ รวมถึงการใช้อาวุธทางไซเบอร์เพื่อจู่โจมสถาบันทางการเงินเพื่อผลประโยชน์ทางการเงิน หรือแม้กระทั่งการจู่โจมทางไซเบอร์เพื่อตอบโต้ข้อมูลต่างๆ ที่ไม่เหมาะสมอันจะก่อให้เกิดภาพลักษณ์ที่ไม่ดีต่อประเทศ การใช้ระบบปฏิบัติการทางไซเบอร์ของประเทศเกาหลีเหนือนั้นเป็นเครื่องมือที่มีประสิทธิภาพแก่ระบอบครอบครัวของผู้นำคิมจองอึน ในการคุกคามระบบทางการทหาร เศรษฐกิจ และอำนาจทางการเมืองของรัฐคู่อริต่างๆด้วยเช่นกัน (Ha, and Maxwell, 2018)

ประเทศเกาหลีเหนือให้ความสำคัญไปยังการพัฒนานิวเคลียร์ อาวุธเคมี และ อาวุธชีวภาพที่มีประสิทธิภาพในการทำลายล้างโดยกว้าง ความสามารถทางไซเบอร์ได้กลายมาเป็นยุทธศาสตร์ทางการทหารที่สำคัญของประเทศเกาหลีเหนือ โดยนาย คิม จอง อึน ได้กล่าวว่า “สงครามทางไซเบอร์ พร้อมด้วยอาวุธนิวเคลียร์และมิซไซล์ คือดาบประกาศิต (All-Purpose Sword) ที่ยืนยันในความสามารถของกองกำลังของเกาหลีเหนือในการโจมตีอย่างไม่อ่อนข้อ” หน่วยสืบราชการลับของเกาหลีเหนือมีชื่อเรียกว่า The Reconnaissance General Bureau หรือ RGB เป็นหน่วยสืบราชการลับที่รับผิดชอบต่อกิจกรรมทางไซเบอร์ต่างๆ ก่อตั้งระหว่าง ค.ศ. 2009 ถึง 2010 เป็นช่วงกลางระหว่างการปรับโครงสร้างองค์ความรู้ของประเทศและความมั่นคงภายในของประเทศเกาหลีเหนือ หน่วย RGB เป็นหน่วยงานที่รายงานข่าวกรองอิสระจากกองทัพและมอบอำนาจในการตัดสินใจให้กับคณะกรรมการกิจการประเทศโดยตรง ซึ่งนำโดย คิม จอง อึน หน่วยงาน RGB ทำหน้าที่คอยตรวจสอบกิจการทางการทหารที่เกี่ยวข้องกับไซเบอร์ภายในประเทศ รวมถึงการป้องกันการก่อการร้ายต่อประเทศเกาเหลีเหนือ หน่วย RGB มีโครงสร้างการทำงานที่มีหน่วยย่อยต่างๆ โดยหนึ่งในหน่วยงานใต้การบังคับบัญชาของหน่วย RGB คือหน่วย Bureau 121 ซึ่งเป็นหน่วยงานหลักของหน่วย RGB ในหน้าที่ทางไซเบอร์ กล่าวคือ หน่วย Bureau 121 คือเครื่องมือทางไซเบอร์ในการดำเนินการกิจกรรมทางไซเบอร์ อาทิเช่น การโจมตีเครือข่ายคอมพิวเตอร์ การแฮ็กเพื่อคัดลอกองค์ความรู้ของรัฐที่ต้องการข้อมูล และ การลอบวางไวรัสในระบบคอมพิวเตอร์ของรัฐคู่อริ และหน่วย Unit 180 คือหน่วยงานไซเบอร์อีกหน่วยหนึ่งของประเทศเกาหลีเหนือ ที่มีหน้าที่โจมตีสถาบันทางการเงินของประเทศต่างๆ ซึ่งจากการกล่าวของ คิม ฮุง กวาง ผู้ลี้ภัยจากเกาหลีเหนือ ได้กล่าวว่า การทำงานของหน่วย Unit 180 คือการขโมยเงินจากธนาคารจากต่างประเทศ (Ha, and Maxwell, 2018)

ในปี ค.ศ. 2010 ประเทศเกาหลีใต้รายงานว่า ถูกโจมตีทางไซเบอร์จากประเทศเกาหลีเหนือเป็นจำนวน 6,000 ครั้ง และสร้างความเสียหายทางเศรษฐกิจและการฟื้นฟูโดยคิดเป็นต้นทุนอยู่ที่จำนวน 650 ล้านดอลลาร์สหรัฐ (Avery et al. 2017) ใน ค.ศ. 2017 มีรายงานถึงการถูกแฮ็กด้วย Ransomware หรือ มัลแวร์เรียกค่าไถ่ ที่ใช้ในการล็อคการเข้าถึงข้อมูล โดยจะเกิดการล็อครหัสผ่านเกิดขึ้นกับข้อมูลของเหยื่อ และหากเหยื่อต้องการเข้าถึงข้อมูล จะต้องทำการจ่ายเงินให้กับแฮ็กเกอร์เพื่อเข้าถึงข้อมูลที่ต้องการ มีการรายงานจากบริษัททั่วโลกว่าถูกแฮ็กด้วย ransomware จำนวน 300,000 ผู้ใช้งานจากอย่างน้อย 150 ประเทศทั่วโลก

ซึ่ง Ransomware นี้มีชื่อว่า WannaCry ซึ่งประเทศเกาหลีเหนือถูกต้องสงสัยว่าเป็นผู้ออกแบบ WannaCry จากการตรวจสอบของหน่วยงานความมั่นคงแห่งชาติสหรัฐอเมริกา ระบุว่าไวรัส WannaCry มีต้นทางมาจากประเทศเกาหลีเหนือ โดยจุดประสงค์ของการแฮ็กครั้งนี้คือการสร้างรายได้ให้กับประเทศเป็นจำนวน 140,000 ดอลลาร์สหรัฐผ่านบิทคอยน์

ใน ค.ศ. 2016 ได้มีการโจมตีทางไซเบอร์กับธนาคารในประเทศบังกลาเทศและประเทศในแถบทวีปเอเชียตะวันออกเฉียงใต้ เกิดการโจรกรรมเงินเป็นจำนวนประมาณ 81 ล้านดอลลาร์สหรัฐ มีต้นทางมาจากการแฮ็กในประเทศเกาหลีเหนือ แฮ็กเกอร์ได้ใช้ the Society for Worldwide Interbank Financial Telecommunication หรือ SWIFT ซึ่งเป็นหน่วยงานที่ให้บริการในการส่งข้อความสู่ธนาคารกลางสหรัฐแห่งเมืองนิวยอร์กในการแลกเปลี่ยนเงินจากธนาคารกลางประเทศต่างๆ แฮ็กเกอร์ได้ทำการใส่มัลแวร์ หรือซอฟท์แวร์ที่เป็นอันตรายเข้าสู่ระบบคอมพิวเตอร์ของ SWIFT ที่ถูกใช้งานโดยธนาคารกลางประเทศบังกลาเทศ หลังจากการแฮ็กเข้าสู่การแลกเปลี่ยนเงินระหว่าง SWIFT มีรายงานว่าประเทศเกาหลีเหนือได้ทำงานเชื่อมต่อการโจมตีทางไซเบอร์นี้ไปยังอีก 18 ประเทศด้วยเช่นกัน และกรณีการแฮ็กบริษัท Sony Pictures Entertainment เรื่อง The Interview ที่มีเนื้อหาเกี่ยวกับการลอบสังหารผู้นำประเทศเกาหลีเหนือ ในเดือนพฤศจิกายนของปีเดียวกัน บริษัท Sony Pictures Entertainment ได้ถูกโจมตีทางไซเบอร์ด้วยการปิดระบบการเข้าถึงข้อมูลทางเทคโนโลยีต่างๆ การทำลายข้อมูล และการแฮ็กเข้าถึงข้อมูลภายในและนำมาเปิดเผยต่อสาธารณะ ประเทศเกาหลีเหนือออกมาปฏิเสธในการมีส่วนเกี่ยวข้องกับเรื่องราวที่เกิดขึ้น แต่ FBI และหน่วยงาน DNI ได้ระบุว่าเป็นการโจมตีทางไซเบอร์จากรัฐบาลเกาหลีเหนือ (Avery et al. 2017)

บริบทการใช้ความสามารถทางไซเบอร์ของแต่ละประเทศที่กล่าวมา ทำให้เห็นถึงจุดประสงค์ต่างๆในการดำเนินการทางไซเบอร์ต่างๆ ไม่ว่าจะเป็นในด้านการใช้ไซเบอร์เพื่อผลประโยชน์แห่งชาติของประเทศตนเองรวมไปถึงในการทำสงคราม ซึ่งสามารถวิเคราะห์ได้ดังตารางที่ 1 ดังนี้

ตารางที่ 1 ตารางเปรียบเทียบผลประโยชน์แห่งชาติและความสำคัญของไซเบอร์ในแต่ละประเทศ

ประเทศ	**ผลประโยชน์แห่งชาติ**	**ความมั่นคงไซเบอร์แห่งชาติ**	**จุดประสงค์ในการใช้อาวุธไซเบอร์**
สหรัฐอเมริกา	ปกป้องประเทศและกีดกันประเทศที่ใช้อาวุธทำลายล้างสูง	การเงิน พลังงาน ระบบคมนาคม ความมั่นคงทางการทหาร และระบบสารสนเทศ รวมถึงไซเบอร์	เพื่อตอบโต้การก่อการร้ายที่เกิดขึ้นจากการเป็นผู้ถูกกระทำ
รัสเซีย	ปกป้องประเทศและกีดกันประเทศที่ใช้อาวุธทำลายล้างสูง รักษาอิทธิพลในเขตล่มสลายจากสหภาพโซเวียต	การปกป้องข้อมูลที่เป็นองค์ความรู้และวัฒนธรรมของชาติและการทำให้การไหลเวียนของข้อมูลเป็นไปอย่างราบรื่น	เพื่อสอดแนม จู่โจม สร้างผลประโยชน์ทางข้อมูลและการเงิน และการสร้างอำนาจทางไซเบอร์

จีน	อำนาจอธิปไตยของประเทศ ความมั่นคง ความสงบสุขของเขตแดน และการพัฒนาภายในประเทศให้เป็นไปอย่างราบรื่น	การสร้างประสิทธิภาพทางไซเบอร์ทั้งในการปกครองและการทำสงคราม	เพื่อสอดแนมและเข้าถึงข้อมูลของรัฐต่างๆด้วยการแฮ็กข้อมูล และการสร้างอำนาจทางไซเบอร์
เกาหลีเหนือ	การครอบครองอาวุธนิวเคลียร์ อัตลักษณ์ของชาติ และ ความมั่นคงทางด้านการทหาร	การสร้างประสิทธิภาพทางไซเบอร์ทั้งในการปกครองและการทำสงคราม	เพื่อสอดแนม จู่โจม สร้างผลประโยชน์ทางข้อมูลและการเงินและการเข้าถึงข้อมูลของรัฐต่างๆด้วยการแฮ็กข้อมูล และการสร้างอำนาจทางไซเบอร์

จากตารางที่ 1 แสดงให้เห็นถึงบริบทของแต่ละประเทศในการใช้ความสามารถทางไซเบอร์ ปรากฏว่าแต่ละประเทศมีลักษณะที่แตกต่างกันออกไป อาทิเช่น ประเทศสหรัฐอเมริกามีความต้องการในการใช้ไซเบอร์เพื่อการบริหารจัดการสาธารณ, การบริหารสาธารณูปโภคขั้นพื้นฐาน รวมถึงทางด้านการทหาร แต่ในประเทศรัสเซีย จีน และเกาหลีเหนือ ให้ความสำคัญกับความมั่นคงไซเบอร์ไปในทิศทางที่คล้ายกันคือ ความต้องการที่จะสร้างประสิทธิภาพทางไซเบอร์ทั้งทางการปกครองและทางการทำสงคราม และเมื่อนำทฤษฎีสัจนิยมแบบดั้งเดิม (Putthiwanich, 2021) มาวิเคราะห์พฤติกรรมและบริบทของการใช้ไซเบอร์นั้น จะเห็นได้ว่า Cyberspace นั้น เปรียบเสมือนความเป็น อนาธิปไตย ที่เหมือนกับ ความสัมพันธ์ระหว่างประเทศ ที่ไม่มีใครเป็นมหาอำนาจแบบผูกขาด ดังนั้น แต่ละประเทศต่างใช้พื้นที่ Cyberspace ในการทำสงครามไซเบอร์ หรือการแฮ็กข้อมูลด้วยวิธีการต่างๆ เพื่อผลประโยชน์แห่งชาติของตนเอง ซึ่งเปรียบเสมือนผลประโยชน์จากการได้มาโดยเปรียบเทียบ (Relative Gains) เป็นการได้ผลประโยชน์จากการสูญเสียของอีกฝ่าย อาทิเช่น การแฮ็กข้อมูลต่างๆของประเทศเกาหลีเหนือ การโจมตีการเข้าถึงเงินทุนของผู้ก่อการร้ายสำหรับประเทศสหรัฐอเมริกา การแฮ็กข้อมูลเครื่องบินจู่โจมของประเทศจีน และการโจมตีด้วยไซเบอร์ของประเทศรัสเซีย

ทฤษฎีสัจนิยมแบบดั้งเดิมนั้น เมื่อนำมาใช้ในการมองปรากฏการณ์ทางไซเบอร์ที่เกิดขึ้น ทำให้เห็นได้ว่า ความร่วมมือทางไซเบอร์ของแต่ละประเทศนั้นยังคงเป็นไปได้ยาก และแต่ละประเทศ ต่างต้องการสร้างความมั่นคงและปลอดภัยให้กับประเทศตนเอง อีกทั้งมีความต้องการในการเสริมความสามารถในการใช้ไซเบอร์ให้เป็นอาวุธเพื่อที่ประเทศของตนจะได้มี “อำนาจ” (Power) ของประเทศตนเองเพื่อความอยู่รอดและความมั่นคงของรัฐ อาทิเช่นประเทศเกาหลีเหนือที่ประกาศว่า อาวุธทางไซเบอร์ คือ ดาบประกาศิต (All-Purposes Sword) ของประเทศตนเอง และเมื่อนำความเชื่อมโยงของทฤษฎีสัจนิยมแบบดั้งเดิมมาวิเคราะห์ร่วมกับผลประโยชน์แห่งชาติ (Putthiwanich, 2021) นำบริบทของแต่ละประเทศมาอธิบายตามแนวคิดได้ดังนี้

1. นโยบายขยายอำนาจ (Imperialism) : ประเทศแต่ละประเทศใช้ความสามารถทางไซเบอร์ในความต้องการขยายอำนาจและดินแดน เช่นกรณีของประเทศรัสเซีย ที่มีความต้องการยึดเอาประเทศยูเครนกลับมา

อยู่ในอาณาเขตของตน และใช้อาวุธทางไซเบอร์จู่โจมเป็นระยะเวลากว่า 3 ปี การโต้ตอบผู้ก่อการร้ายของประเทศสหรัฐอเมริกา ความพยายามใช้ไซเบอร์ในการครอบงำการทำงานของประเทศอื่นๆจากการแฮ็กของประเทศจีนและประเทศเกาหลีเหนือ

2. นโยบายรักษาสถานะอำนาจ (Status Quo Ante Bellum) : ในส่วนของนโยบายนี้ ผู้เขียนวิเคราะห์ว่า ยังไม่มีความร่วมมือเพื่อสร้างหรือรักษาสถานะความสัมพันธ์อันดีระหว่างประเทศในรูปแบบไซเบอร์อย่างเป็นทางการและชัดเจน อันเนื่องมาจากความต้องการที่จะรักษาข้อมูลที่เป็นความลับของแต่ละประเทศ

3. นโยบายเพื่อเกียรติยศ (Policy for Prestige) : ประเทศที่เห็นได้ชัดว่าการใช้ไซเบอร์เพื่อนโยบายนี้คือประเทศจีน และเกาหลีเหนือ กล่าวคือ การใช้ไซเบอร์ในการควบคุมความคิดความคาดหวังต่างๆของประชาชนที่มีต่อรัฐบาล เพื่อรักษาอำนาจของรัฐตนให้มีความมั่นคง

สรุป

ความสามารถทางไซเบอร์ สามารถนำมาใช้เพื่อผลประโยชน์ส่วนบุคคล รวมไปถึงผลประโยชน์แห่งชาติดังที่บทความได้กล่าวถึง แต่ความสามารถทางไซเบอร์นั้น ก็สามารถนำมาใช้ในส่วนของการโจรกรรมทางข้อมูล การแฮ็กข้อมูล รวมไปถึงการก่อการร้ายจนนำมาซึ่งสงคราม ความสามารถทางไซเบอร์ได้กลายมาเป็นสิ่งที่เป็นอาวุธและสามารถสร้างความร่วมมือหรือความขัดแย้งได้เพียงชั่วข้ามคืน อย่างไม่เป็นทางการเช่น การประกาศการโจมตี และสามารถทำได้ถึงระดับบุคคลธรรมดาด้วยเช่นกัน นานาประเทศต่างให้ความสำคัญในการพัฒนาทางด้านไซเบอร์อย่างเห็นได้ชัด อันเนื่องมาจากการได้รับผลกระทบทางไซเบอร์ และความสามารถของประเทศที่สามารถใช้ไซเบอร์เพื่อสร้างประโยชน์ให้กับชาติตนเอง ดังนั้น ความสามารถทางไซเบอร์เป็นสิ่งที่หลีกเลี่ยงไม่ได้ที่จะต้องเผชิญในอนาคต และในแง่ของประเด็นทางการเมืองระหว่างประเทศ เป็นสิ่งที่ต้องทำการศึกษาค้นคว้าเพิ่มเติม อาทิเช่น หากเกิดความร่วมมือระหว่างประเทศในการใช้ความสามารถทางไซเบอร์ในการโจมตีรัฐคู่อริ จะเกิดอะไรขึ้น? หรือ หากเกิดความขัดแย้งระหว่างประเทศในการทำสงครามไซเบอร์ ผลกระทบที่เกิดขึ้นจะสร้างความเสียหายจนถึงขั้นสูญเสียอำนาจอธิปไตยหรือไม่ ? ความสามารถทางไซเบอร์และผลประโยชน์แห่งชาตินั้น จึงเป็นสิ่งที่ควรศึกษาต่อไปอย่างยิ่งทั้ง ณ ปัจจุบันและอนาคตอันใกล้

ข้อเสนอแนะ

จากผลการศึกษาในครั้งนี้ ผู้ศึกษามีข้อเสนอแนะเพื่อการนำไปใช้ประโยชน์ของหน่วยงานเทคโนโลยีสารสนเทศภาครัฐถึงการพัฒนาประสิทธิภาพส่วนบุคคล ตลอดถึงการเสนอแนะเพื่อการวิจัยต่อยอดสำหรับผู้ที่สนใจ

1. ข้อเสนอแนะจากการศึกษา

บทความนี้ เป็นประโยชน์ต่อผู้ที่ต้องการศึกษา ดังนี้

1.1 เพื่อศึกษาความแตกต่างของความมั่นคงทางไซเบอร์ในแต่ละประเทศ

1.2 เพื่อศึกษาการใช้ไซเบอร์เป็นอาวุธสงครามเพื่อผลประโยชน์แห่งชาติ

1.3 เพื่อศึกษาจุดประสงค์การใช้ไซเบอร์เพื่อเป็นอาวุธสงครามในแต่ละประเทศ

2. ข้อเสนอแนะในการศึกษาครั้งต่อไป

2.1 การศึกษาครั้งต่อไป บทความนี้สามารถนำไปใช้วิเคราะห์สำหรับการศึกษาความมั่นคงทางไซเบอร์ของประเทศต่างๆ และความสัมพันธ์ระหว่างความมั่นคงทางไซเบอร์ สงครามทางไซเบอร์ และผลประโยชน์แห่งชาติ

References

Allison, G., & Blackwill, R. D. (2011). *Russia and U.S. National Interests: Why Should Americans Care?*. Retrieved October 11, 2021, from https://www.cfr.org/report/russia-and-us-national-interests-why-should-americans-care.

Avery, E. M. et al. (2017). *North Korean Cyber Capabilities: In Brief*. Retrieved October 11, 2021, from https://sgp.fas.org/crs/row/R44912.pdf.

Azmi, R., & Kautsarina, K. (2019). *Revisiting Cyber Definition*. Retrieved October 11, 2021, from https://www.researchgate.net/publication/334989724_Revisiting_Cyber_Definition.

Cooper III, C. A. (2011). Chinese Perceptions of and Strategic Response to Threats in Cyberspace. In J. Lindsay (Ed.), *IGCC Workshop Report on China and Cybersecurity* (pp.1-36). San Diego: University of California San Diego.

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

Gady, F. S., & Austin, G. (2010). *Russia, The United States, And Cyber Diplomacy*. Retrieved October 13, 2021, from https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf

Ha, M., & Maxwell, D. (2018). *Kim Jong Un's 'All-Purpose Sword' North Korean Cyber-Enabled Economic Warfare*. Retrieved October 13, 2021, from https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf

Hakala, J., & Melnychuk, J. (2021). *Russia's Strategy in Cyberspace*. Riga: NATO Strategic Communications Centre of Excellence.

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, 4(2), 1–24.

Lehto, M. (2013). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. *International Journal of Cyber Warfare and Terrorism*, 3(3), 1-18.

Mitra, A. (2010). *Digital Security: Cyber Terror and Cyber Security*. New York: Infobase.

Mount, M. (2009). *Hackers stole data on Pentagon's newest fighter jet*. Retrieved October 17, 2021, from https://edition.cnn.com/2009/US/04/21/pentagon.hacked/.

Peritz, A. J., & Sechrist, M. (2010). *Protecting Cyberspace and the US National Interest*. Retrieved October 17, 2021, from https://www.belfercenter.org/sites/default/files/legacy/ files/cyber-vital-national interest.pdf+&cd=2&hl=th&ct=clnk&gl=th

Powcharoen, P. (2021). *Economy and Nuclear Development: The Case of North Korea*. *Journal of Political Economy*, 9(1), 107 – 123.

Putthiwanich, K. (2021). National Interest and International Relations Theories. *Political Science Critique*, 8(15), 1-24.

Raud, M. (2016). *China and Cyber: Attitudes, Strategies, Organisation*. Retrieved October 17, 2021, from https://ccdcoe.org/library/publications/china-and-cyber-attitudes-strategies-organisation/

Worldometers. (2021). *China Population*. Retrieved October 19, 2021, from https://www.worldometers.info/world-population/china-population/

Yuxiao, L. (2011). Cyberspace Security and International Cooperation in China. In J. Lindsay (Ed.), *IGCC Workshop Report on China and Cybersecurity* (pp.56 - 78). San Diego: University of California San Diego.