



ความขัดแย้งทางไซเบอร์²¹ ในมุมมองเชิงยุทธศาสตร์ (Strategic View of Cyber Conflicts)²²

ภาณุภัต วัชรภรณ์²³

บทคัดย่อ

บทความนี้อธิบายการใช้เครื่องมือทางไซเบอร์เพื่อบรรลุวัตถุประสงค์เชิงยุทธศาสตร์ของรัฐ โดยพิจารณาถึงปัจจัยต่าง ๆ ที่ผลักดันให้รัฐหันมาใช้เครื่องมือเหล่านี้ ได้แก่ พื้นที่และโอกาสในการโจมตีที่เพิ่มขึ้น ต้นทุนที่ลดลง การปกปิดตัวตน การปฏิเสธความรับผิดชอบ และความคลุมเครือของกฎหมายระหว่างประเทศ บทความนี้ยังวิเคราะห์ถึงความเป็นไปได้ ข้อจำกัด และความท้าทายที่รัฐต้องเผชิญในการดำเนินกลยุทธ์ทางไซเบอร์ ประกอบด้วย การส่งสัญญาณ (Signaling) การกำหนดทิศทางสถานการณ์ (Shaping) การป้องปราม (Deterrence) การบีบบังคับ (Coercion) และการบรรลุวัตถุประสงค์ของ

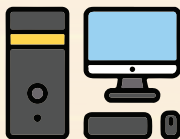
²¹ การใช้เครื่องมือทางไซเบอร์เพื่อผลลัพธ์ทางยุทธศาสตร์อาจถูกดำเนินการอย่างแอบแฝงและแนบเนียน โดยไม่จำเป็นต้องมุ่งหวังผลลัพธ์ทางกายภาพในทันที เพื่อคงไว้ซึ่งนัยดังกล่าว ในข้อบทความนี้ผู้เขียนจึงขอหลีกเลี่ยงการใช้คำว่า “การโจมตีทางไซเบอร์” (cyber attack) และขอใช้ คำว่า “ความขัดแย้งทางไซเบอร์” (cyber conflicts) ซึ่งหมายถึง การใช้เครื่องมือทางไซเบอร์โดยรัฐหนึ่งเพื่อสร้างความได้เปรียบทางยุทธศาสตร์เหนือ รัฐอื่น เพื่อให้สอดคล้องกับนัยที่แท้จริงของกลยุทธ์ทางไซเบอร์ของรัฐชาติ

²² บทความนี้มีการใช้ Large Language Model (LLM) เพื่อช่วยในการเรียบเรียงข้อความ โดยเนื้อหาและข้อคิดเห็นมาจากการค้นคว้าและวิเคราะห์โดยผู้เขียนเองทั้งหมด

²³ นักวิเคราะห์นโยบายและแผนปฏิบัติการ กองความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ สำนักงานสภาความมั่นคงแห่งชาติ, ด (ความสัมพันธ์ระหว่างประเทศ) คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Master of National Security Policy, National Security College, Crawford School of Public Policy, the Australian National University.

สงคราม โดยแม้ว่าเครื่องมือทางไซเบอร์จะมีศักยภาพในการบรรลุวัตถุประสงค์เชิงยุทธศาสตร์ แต่กลับมีข้อจำกัดที่สำคัญบางประการ เช่น ปัญหาในการระบุแหล่งที่มาของการโจมตีและความยากลำบากในการตีความเจตนาทำให้มีความไม่แน่นอนในการบรรลุเป้าหมายเชิงยุทธศาสตร์ นอกจากนี้ยังนำไปสู่การยกระดับความขัดแย้งโดยไม่ตั้งใจด้วยเหตุนี้รัฐไทยจึงควรศึกษาบทบาทของเครื่องมือทางไซเบอร์ในความขัดแย้งระหว่างประเทศต่าง ๆ เพื่อถอดบทเรียนและวางแผนนโยบายในการรับมือ ตอบโต้ หรือเลือกใช้เครื่องมือทางไซเบอร์เพื่อรักษาผลประโยชน์แห่งชาติของไทยท่ามกลางการแข่งขันทางภูมิรัฐศาสตร์โลกต่อไป

บทนำ



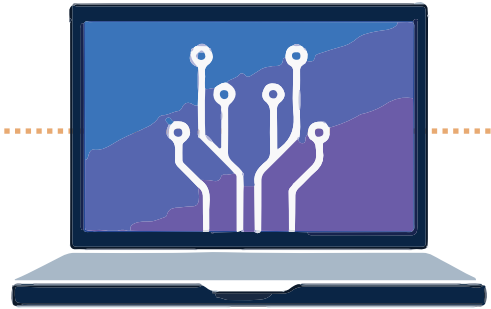
การใช้เครื่องมือทางไซเบอร์เพื่อผลลัพธ์ทางการเมืองระหว่างประเทศสามารถพบเห็นได้บ่อยครั้งในปัจจุบัน²⁴ ไม่ว่าจะเป็นการใช้เพื่อสอดแนมทางการข่าว (Cyber Espionage) การลบสร้างความเสียหายต่อเป้าหมาย (cyber sabotage) หรือการสนับสนุนปฏิบัติการทางทหารในรูปแบบ “สงครามผสมผสาน” (Hybrid Warfare) จากมุมมองเชิงยุทธศาสตร์ ซึ่งมุ่งเน้นการสร้าง “คุณค่าหรือผลลัพธ์ที่ตอบสนองความต้องการของรัฐ” เครื่องมือไซเบอร์เหล่านี้มีบทบาทสำคัญในการดำเนินกลยุทธ์ต่าง ๆ เช่น การส่งสัญญาณ (Signaling) การกำหนดทิศทางสถานการณ์ (Shaping) การป้องปราม (Deterrence) การบีบบังคับ (Coercion) หรือการบรรลุวัตถุประสงค์ของสงคราม เป็นต้น

บทความนี้มุ่งอธิบายปัจจัยที่ผลักดันให้รัฐชาติหันมาใช้เครื่องมือทางไซเบอร์เพื่อบรรลุเป้าประสงค์ทางยุทธศาสตร์ และวิเคราะห์ความเป็นไปได้ ข้อจำกัด และความท้าทายต่าง ๆ ที่รัฐชาติต้องเผชิญในการดำเนินกลยุทธ์ทางไซเบอร์ ประกอบด้วย (1) การส่งสัญญาณ (2) การป้องปรามและการบีบบังคับ (3) การกำหนดทิศทางสถานการณ์ และ (4) การบรรลุวัตถุประสงค์ของสงคราม

ขอบเขตของบทความนี้ให้ความสำคัญกับการกระทำของรัฐชาติเป็นหลัก โดยการวิเคราะห์จะไม่เน้นการใช้เครื่องมือทางไซเบอร์ที่ไม่สามารถหาความเชื่อมโยงกับรัฐชาติ (เช่น การแฮกเพื่อวัตถุประสงค์ทางการเงินโดยกลุ่มอาชญากรไซเบอร์) หรือจากตัวแสดงที่เป็นเอกเทศจากรัฐอย่างชัดเจน (เช่น กลุ่มก่อการร้าย) มาเกี่ยวข้อง นอกจากนี้ การวิเคราะห์นี้ให้ความสำคัญกับมิติด้านตรรกะ (Logical Aspects) ของความมั่นคงปลอดภัยไซเบอร์เป็นหลัก กล่าวคือ การวิเคราะห์จะสนใจประเด็นไซเบอร์ในแง่ของการโจมตีต่อระบบคอมพิวเตอร์เป็นหลัก มากกว่าการสนใจมิติทางกายภาพ (Physical Aspects) อย่างเช่นการทำลายโครงสร้างพื้นฐานสำคัญของระบบอินเทอร์เน็ต หรือ มิติด้านข้อมูล (Information Aspects) ในรูปแบบปฏิบัติการข้อมูลข่าวสาร (Information Operation)

²⁴ สามารถสืบค้นปฏิบัติการทางไซเบอร์ที่มีความเกี่ยวข้องกับรัฐนับตั้งแต่ ค.ศ. 2005 ได้ที่ “Cyber Operation Tracker,” Council on Foreign Relations, <https://www.cfr.org/cyber-operations/>.

ทำไมเครื่องมือทางไซเบอร์ ถึงน่าสนใจสำหรับรัฐ



ปัจจัยที่เอื้อให้รัฐหันมาใช้เครื่องมือทางไซเบอร์ เพื่อบรรลุเป้าประสงค์ทางยุทธศาสตร์ ประกอบด้วย อย่างน้อย 5 ปัจจัยสำคัญ ได้แก่ พื้นที่และโอกาส โจมตีที่กว้างขึ้น ต้นทุนที่น้อยลง ความสามารถในการปกปิดตัวตน (Anonymity) ความสามารถในการปฏิเสธความเกี่ยวข้อง (Deniability) และความคลุมเครือในการบังคับใช้กฎหมายระหว่างประเทศ

พื้นที่และโอกาสโจมตีที่กว้างขึ้น หมายถึง การที่รัฐทุกรัฐสามารถตกเป็นเป้าการโจมตีทางไซเบอร์ได้เหมือนกันหมด อันเป็นผลมาจากการที่วิถีชีวิตของผู้คนในปัจจุบันต้องพึ่งพาเทคโนโลยีสารสนเทศและการสื่อสารอย่างหลีกเลี่ยงไม่ได้ เช่น การที่บริการภาครัฐ ระบบธนาคาร การสื่อสาร ไปจนถึงโครงสร้างพื้นฐานสำคัญ อาทิ ระบบโทรคมนาคม พลังงาน สาธารณสุข และคมนาคม ต้องอาศัยระบบคอมพิวเตอร์ในการบริหารจัดการ ไม่มากก็น้อย

ในแง่นี้ จึงหมายความว่าประเทศมหาอำนาจที่มีขีดความสามารถในการป้องกันประเทศอย่างสหรัฐอเมริกาก็สามารถตกเป็นเป้าหมายการ

โจมตีทางไซเบอร์จากรัฐอื่น ๆ ได้ โดยแม้ว่าหน่วยงานภาครัฐจะกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ แต่ระบบคอมพิวเตอร์ของภาคเอกชน หรือปัจเจกบุคคลก็ยังสามารถตกเป็นเป้าการโจมตีทางไซเบอร์ที่สามารถส่งผลกระทบทางการเมืองระหว่างประเทศ เช่น กรณีที่ระบบซอฟต์แวร์ของบริษัท SolarWinds ที่ถูกแทรกแซงและลักลอบขโมยข้อมูลที่เกี่ยวข้องกับรัฐบาลสหรัฐฯ²⁵ หรือการที่ผู้นำประเทศอย่างอดีตนายกรัฐมนตรีนองเกลามาเคิล ของเยอรมนี ตกเป็นเป้าหมายของสปายแวร์โดยหน่วยข่าวกรองของรัฐอื่น²⁶

ความเปราะบางของประเทศมหาอำนาจจากการโจมตีทางไซเบอร์ยังมีคุณค่าในเชิงยุทธศาสตร์มากขึ้นไปอีก เมื่อเปรียบเทียบกับการโจมตีทางกายภาพซึ่งแทบจะเป็นไปไม่ได้เลยที่รัฐอื่นๆ จะสามารถโจมตีและสร้างความเสียหายให้กับมหาอำนาจอย่างสหรัฐฯได้สำเร็จ และไม่ถูกตอบโต้กลับอย่างรุนแรง

²⁵ Cybersecurity & Infrastructure Security Agency. (n.d.). Fact sheet: Russian SVR activities related to SolarWinds compromise. Accessed October 25, 2024, from https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf

Zscaler. (n.d.). What is the SolarWinds cyberattacks? Accessed October 25, 2024, from <https://www.zscaler.com/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack#how-the-attack-works%20%20https://www.theguardian.com/world/2021/may/31/denmark-helped-us-spy-on-angela-merkel-and-european-allies-report>

²⁶ Henley, J. (2021, May 31). Denmark helped US spy on Angela Merkel and European allies – Report. The Guardian. Accessed October 25, 2024, from <https://www.theguardian.com/world/2021/may/31/denmark-helped-us-spy-on-angela-merkel-and-european-allies-report>



ในแง่ของต้นทุน การใช้เครื่องมือทางไซเบอร์ • ใช้ Stuxnet
บางรูปแบบสามารถกระทำได้ด้วยต้นทุนที่ต่ำ เช่น เพื่อลอบสร้าง
การโจมตีด้วยวิธี Denial-of-Service Attack ความเสียหาย
(DDoS Attack) ที่ต้องการเพียงอุปกรณ์จำนวน ต่อโครงการพัฒนา
มากในการส่งคำขอเข้าถึงเป้าหมายพร้อมกัน โดย
รัฐส่วนใหญ่ก็มีทรัพยากรเพียงพอในการดำเนินการ
การอยู่แล้ว และหากเลือกเป้าหมายที่เหมาะสม
การโจมตีเช่นนี้ก็สามารถสร้างผลกระทบเป็นวงกว้างได้
ดังเช่นกรณีทีเอสโตเนียและจอร์เจียเคยประสบ
ในอดีต²⁷

อย่างไรก็ตาม ปัจจัยว่าด้วยต้นทุนที่ลดลงนี้
อาจไม่เป็นจริงเสมอไป จากการที่ระบบการรักษา
ความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบันมี
มาตรฐานที่สูงขึ้นจากอดีตมาก รวมถึงการที่รัฐที่
เคยโดนโจมตีในอดีตเริ่มพัฒนาขีดความสามารถ
ในการป้องกันประเทศทางไซเบอร์เพิ่มมากขึ้น²⁸
ดังนั้น รูปแบบการโจมตีด้วยต้นทุนที่ต่ำอย่าง
DDoS Attack ไม่น่าจะก่อให้เกิดผลกระทบได้
มากเท่ากับเหตุการณ์ในอดีตข้างต้น นอกจากนี้
หากรัฐต้องการใช้เครื่องมือทางไซเบอร์เพื่อ
ให้ได้ผลลัพธ์ทางยุทธศาสตร์ที่มีประสิทธิภาพ
ยังจำเป็นต้องอาศัยเครื่องมือทางไซเบอร์ที่มี
ขีดความสามารถสูงซึ่งมักต้องใช้ทรัพยากร
จำนวนมากตามไปด้วย ดังเช่น กรณีของการ •
ใช้ Stuxnet เพื่อลอบสร้าง ความเสียหาย ต่อโครงการพัฒนา
อาวุธนิวเคลียร์ของอิหร่านที่ต้องอาศัยช่องโหว่
ที่เพิ่งเคยถูกค้นพบและไม่เคยได้รับการแก้ไข
(Zero-Day Vulnerability) อย่างน้อย 5 ช่องโหว่²⁹
หรือการซื้อบริการสปายแวร์ Pegasus ของบริษัท
NSO Group ที่มีราคาสูง³⁰ เป็นต้น



ความสามารถในการปกปิดตัวตน (Anonymity) หมายถึง การที่ผู้กระทำการสามารถปกปิด
ต้นตอของการโจมตีทางไซเบอร์ได้ ด้วยเทคนิค
เช่น การใช้ VPN, Proxy Server, การใช้บอทเน็ต,
หรือการปลอมแปลง IP เป็นต้น ส่งผลให้เกิด
ความยุ่งยากและไม่แน่นอนในการระบุแหล่งที่มา
ของการโจมตี หรือที่เรียกว่า “ปัญหาในการระบุ
ตัวตนผู้กระทำผิด” (Attribution Problem) และ
แม้ว่าการทำนิติวิทยาศาสตร์ทางไซเบอร์ (Cyber
Forensic) จะเป็นไปได้ แต่ก็ต้องอาศัยทรัพยากร
ที่มากและอาจไม่คุ้มค่าหากรัฐที่ตกเป็นเหยื่อ
ไม่มีแนวทางการตอบโต้ที่ชัดเจน ผลลัพธ์เบื้องต้น
ของความไม่แน่นอนและความลำบากในการชี้
ผู้กระทำผิดส่งผลให้รัฐที่ทำการโจมตีทางไซเบอร์
มีโอกาสถูกตอบโต้กลับในระดับต่ำมาก

²⁷ Pernik, P., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., et al. (2018). The early days of cyberattacks: The cases of Estonia, Georgia, and Ukraine. In N. Popescu & S. Secieru (Eds.), Hacks, leaks and disruptions: Russian cyber strategies (pp. [page numbers]). European Union Institute for Security Studies (EUISS). <https://www.jstor.org/stable/resrep21140.9>

²⁸ NBC News. (2009, July 9). A look at Estonia's cyber attack in 2007. NBC News. Retrieved October 28, 2024, from https://www.nbcnews.com/id/wbna31801246#.WNLFP2_yuUk

²⁹ Black Hat. (n.d.). A decade after Stuxnet's printer vulnerability: Printing is still the stairway to heaven. Retrieved October 28, 2024, from <https://www.blackhat.com/html/webcast/05202021-a-decade-after-stuxnets-printer-vulnerability-printing-is-still-the-stairway-to-heaven.html>

³⁰ Benenav, J. (2022, November 12). Internal documents show how close the F.B.I. came to deploying spyware. The New York Times. Retrieved October 28, 2024, from <https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html>



ความสามารถในการปฏิเสธความเกี่ยวข้อง เป็นประเด็นที่ตามมาจากความสามารถในการปกปิดตัวตน โดยแม้ว่ารัฐที่เป็นเหยื่อจะสามารถระบุที่มาของการโจมตีได้สำเร็จ รัฐที่เป็นผู้กระทำการยังมีความได้เปรียบทางการเมืองในการปฏิเสธความเกี่ยวข้องกับการโจมตีทางไซเบอร์ได้โดยการอ้างว่าผู้กระทำ การเป็นเพียงกลุ่มบุคคลที่ไม่ได้มีความเกี่ยวข้องกับรัฐและเบี่ยงเบนประเด็นให้เป็นการจัดการกับกลุ่มอาชญากร ไซเบอร์ภายในประเทศแทน



ความคลุมเครือในการบังคับใช้กฎหมายระหว่างประเทศ ในประเด็นความขัดแย้งทางไซเบอร์เป็นอีกข้อจำกัดสำคัญที่เอื้อให้การโจมตีทางไซเบอร์ยังถูกใช้เป็นเครื่องมือทางการเมือง

ระหว่างประเทศ โดยแม้ว่ารัฐภาคีขององค์การสหประชาชาติจะมีมติยอมรับว่ากฎหมายระหว่างประเทศสามารถบังคับใช้ได้ในพื้นที่ทางไซเบอร์³¹ รวมถึงกฎบัตรของสหประชาชาติ ข้อ 2(4) ว่าด้วย “การละเว้นการคุกคามหรือการใช้กำลัง” ต่อรัฐอื่น³² แต่แนวทางการตีความการโจมตีทางไซเบอร์ในลักษณะของการใช้กำลังยังไม่ได้ได้รับความเห็นพ้องในเวทีระหว่างประเทศ โดยเฉพาะเมื่อมีการใช้เครื่องมือทางไซเบอร์เพื่อเป้าประสงค์ทางยุทธศาสตร์บางรูปแบบ เช่น การสอดแนมเพื่อการข่าว หรือการลอบสร้างความเสียหายนั้นไม่ได้ก่อให้เกิดผลกระทบในเชิงกายภาพในทันทีตามที่หลาย ๆ ประเทศตั้งคำถามเกี่ยวกับการใช้กำลังทางไซเบอร์เอาไว้³³

³¹ United Nations. (2013, June 24). Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security. Retrieved October 25, 2024, from https://dig.watch/wp-content/uploads/A_68_98_E.pdf.

³² United Nations. (n.d.). UN Charter. Retrieved October 28, 2024, from <https://www.un.org/en/about-us/un-charter/chapter-1>.

³³ Cyber Defence Centre of Excellence. (2024, June 17). Use of force. Retrieved October 28, 2024, from https://cyber-law.ccdcoe.org/wiki/Use_of_force#:~:text=A%20cyber%20activity%20constitutes%20a,an%20unlawful%20use%20of%20force.



ในอีกมุมมองหนึ่ง ความคลุมเครือของการบังคับใช้กฎหมายระหว่างประเทศยังเปิดโอกาสให้รัฐสามารถใช้เครื่องมือทางไซเบอร์ในฐานะ “ทางเลือกอื่นนอกจากสงคราม” (Alternative to War) เพื่อยุติข้อขัดแย้งระหว่างประเทศ³⁴ กล่าวคือ เครื่องมือทางไซเบอร์ได้กลายมาเป็นเครื่องมือในการหลีกเลี่ยงการจู่โจมทางสงครามเต็มรูปแบบของรัฐในการสร้างความเสียหาย หรือตอบโต้กับรัฐอื่น ๆ

ด้วยปัจจัยทั้งห้าประการข้างต้น ส่งผลให้เครื่องมือทางไซเบอร์เป็นตัวเลือกเชิงกลยุทธ์ที่น่าสนใจ โดยเฉพาะสำหรับมหาอำนาจ (Great Power) และรัฐอภิมหาอำนาจ (Superpower) ที่มีขีดความสามารถทางไซเบอร์มากเพียงพอสำหรับใช้เป็นเครื่องมือทางยุทธศาสตร์ โดยในส่วนถัดไปจะอธิบายความเป็นไปได้ และข้อจำกัดของความขัดแย้งทางไซเบอร์ในมุมมองเชิงยุทธศาสตร์

รัฐใช้เครื่องมือทางไซเบอร์ในทางยุทธศาสตร์ได้อย่างไรบ้าง



1. เพื่อส่งสัญญาณให้อีกฝ่าย (Signaling)

การส่งสัญญาณ ในที่นี้หมายถึง การสื่อสารเชิงสัญลักษณ์อย่างโจ่งแจ้งเพื่อให้อีกฝ่ายตีความสารของผู้สื่อสาร ยกตัวอย่างเช่น การเคลื่อนกำลังพลไปยังเขตชายแดนเพื่อส่งสัญญาณไม่ให้รัฐข้างเคียงละเมิดเข้ามายังอาณาเขต การร่วมซ้อมรบเพื่อแสดงให้เห็นความร่วมมือที่ดีระหว่างประเทศพันธมิตร และความตั้งใจในการใช้กำลังเพื่อตอบโต้สถานการณ์ที่อาจเกิดขึ้น หรือการซ้อมยิงขีปนาวุธเพื่อแสดงขีดความสามารถและข่มขู่ประเทศอื่น ๆ เป็นต้น³⁵

ในกรณีของการส่งสัญญาณด้วยเครื่องมือทางไซเบอร์ สามารถเกิดขึ้นในลักษณะของการโจมตีเพื่อแสดงความไม่พอใจต่อการกระทำบางอย่างของรัฐอื่น ตัวอย่างในอดีต เช่น เหตุการณ์ในปี ค.ศ. 2007 ที่เอสโตเนียประสบกับการถูกโจมตีด้วย DDoS Attack อันเป็นผลมาจากความไม่พอใจของแอกเกอร์ชาวรัสเซียที่ไม่พอใจรัฐบาลเอสโตเนียที่ต้องการย้ายรูปปั้นวีรบุรุษชาวโซเวียตออกจากกรุงทาลินน์³⁶ หรือเหตุการณ์ที่กลุ่มแฮกเกอร์ชาวเกาหลีเหนือทำการขโมยและลบข้อมูลสำคัญของบริษัทโซนี่ ในปี ค.ศ. 2014 เพื่อตอบโต้กับการที่บริษัทได้ถ่ายทำภาพยนตร์ที่มีเนื้อหาหมิ่นผู้นำเกาหลีเหนือ³⁷ เป็นต้น โดยทั้งสองเหตุการณ์แสดงให้เห็นถึงการโจมตีทางไซเบอร์ที่มีแรงจูงใจและผลประโยชน์เชื่อมโยงกับรัฐโดยตรง

³⁴ Harknett, R. J., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45(4), 534–567. <https://doi.org/10.1080/01402390.2020.1732354>.

³⁵ Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal geopolitics*. Harvard University Press.

³⁶ Council on Foreign Relations. (n.d.). Estonia denial of service incident. *Cyber Operation Tracker*. Retrieved October 25, 2024, from <https://www.cfr.org/cyber-operations/estonian-denial-service-incident>.

³⁷ Council on Foreign Relations. (n.d.). Compromise of Sony Pictures Entertainment. *Cyber Operation Tracker*. Retrieved October [insert date], 2024, from <https://www.cfr.org/cyber-operations/compromise-sony-pictures-entertainment>. 25, 2024, <https://www.cfr.org/cyber-operations/compromise-sony-pictures-entertainment>.

แม้ว่าเครื่องมือไซเบอร์จะมีศักยภาพในการส่งสัญญาณทางยุทธศาสตร์ แต่มีข้อจำกัดสำคัญ คือ ความยากลำบากในการตีความสารของฝ่ายผู้รับ เนื่องจากการระบุตัวตนผู้โจมตีในโลกไซเบอร์นั้นมีความคลุมเครือ ต้องใช้เวลาและผู้ถูกโจมตีอาจไม่สามารถเชื่อมโยงการโจมตีนั้นเข้ากับข้อเรียกร้องทางการเมืองระหว่างประเทศได้อย่างถูกต้องและทันท่วงที่ยิ่งไปกว่านั้น ความแตกต่างทางวัฒนธรรมและข้อจำกัดในการรับรู้ยังเพิ่มโอกาสในการตีความสัญญาณทางการเมืองระหว่างประเทศที่ผิดพลาด³⁸ ดังนั้น การใช้เครื่องมือไซเบอร์เพื่อการส่งสัญญาณจึงอาจไม่บรรลุผลตามเจตนา หากฝ่ายผู้รับไม่สามารถเข้าใจความหมายที่แท้จริงของการกระทำนั้น ๆ ได้

ฉะนั้น ในการแก้ไขปัญหาคำถามการตีความสัญญาณที่ผิดพลาด ผู้โจมตีอาจเลือกใช้ ช่องทางการสื่อสารอื่น ๆ ควบคู่ไปกับการโจมตีทางไซเบอร์เพื่อประกาศตัวตนและแสดงเจตนาอย่างชัดเจน ตัวอย่างเช่น กรณีที่รัฐมนตรีว่าการกระทรวงกลาโหมสหรัฐฯ มีแถลงการณ์ว่า สหรัฐฯ เป็นผู้โจมตีระบบควบคุมและสั่งการของกลุ่มไอเอสในอิหร่านและซีเรีย⁴⁰ แม้กรณีนี้จะไม่ใช่การโจมตีรัฐโดยตรง แต่ก็แสดงให้เห็นว่ารัฐสามารถใช้ช่องทางการสื่อสารแบบเปิดเผยเพื่อประกาศตัวเป็นผู้โจมตีได้ นอกจากนี้ การสื่อสารดังกล่าวยังสามารถทำผ่านช่องทางลับได้เช่นกัน

อย่างไรก็ตาม การตัดสินใจใช้ช่องทางการสื่อสารประกอบกับการโจมตีเพื่อส่งสัญญาณอาจไม่ได้เป็นทางเลือกที่ดีในเชิงยุทธศาสตร์เสมอไปด้วยข้อจำกัดอีกหนึ่งประการนั้นคือ

การที่ขีดความสามารถทางไซเบอร์ต้องอาศัยความลับทั้งในส่วน of เครื่องมือและเทคนิคที่ใช้การเปิดเผยตัวตนของผู้ถูกโจมตีจึงเท่ากับการเปิดเผยขีดความสามารถทางไซเบอร์ที่รัฐนั้น ๆ ครอบครองอยู่ ยิ่งไปกว่านั้น การเปิดเผยช่องโหว่บางอย่างที่รัฐสามารถเข้าถึงได้อาจนำไปสู่การแก้ไขช่องโหว่ดังกล่าวได้แต่อาจส่งผลให้ความได้เปรียบทางไซเบอร์ในภาพรวมของรัฐนั้น ๆ ลดลงในที่สุด⁴¹



³⁸ Jervis, R. (1976). Perception and misperception in international politics. Princeton University Press.

³⁹ Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. Security Studies, 26(3), 450–475. <https://doi.org/10.1080/09636412.2017.1306396>.

⁴⁰ Paletta, D., & Schwartz, F. (2016, February 2). Pentagon deploys cyberweapons against Islamic State. The Wall Street Journal. Retrieved October 28, 2024, from <https://www.wsj.com/articles/pentagon-deploys-cyberweapons-against-islamic-state-1456768428>.

⁴¹ Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. Security Studies, 26(3), 450–475. <https://doi.org/10.1080/09636412.2017.1306396>.

จุดแตกต่างสำคัญระหว่างการส่งสัญญาณแบบดั้งเดิม เช่น การเคลื่อนกำลังพล หรือ การทดสอบขีปนาวุธ กับการใช้เครื่องมือไซเบอร์ คือ ผลกระทบที่เกิดขึ้น โดยวิธีแบบดั้งเดิมมักไม่ก่อให้เกิดความเสียหายต่อทรัพย์สินของฝ่ายตรงข้ามโดยตรง ในขณะที่การส่งสัญญาณด้วยวิธีไซเบอร์ จำเป็นต้องสร้างความเสียหายในระดับหนึ่ง เช่น การรบกวนระบบ หรือการขโมยข้อมูล เพื่อให้สัญญาณนั้น ๆ ปรากฏชัด

อย่างไรก็ตาม ความเสียหายที่เกิดขึ้น แม้จะอยู่ในระดับที่จำกัด ก็อาจนำไปสู่ความเสี่ยงในการยกระดับความขัดแย้งโดยไม่ได้ตั้งใจ (Unintended Escalation) หากฝ่ายรับสารตีความการกระทำดังกล่าวเป็นการรุกราน และตัดสินใจตอบโต้ ⁴² ด้วยเหตุนี้ ความคลุมเครือในการสื่อสารของการใช้เครื่องมือทางไซเบอร์ จึงเป็นความท้าทายสำคัญในการส่งสัญญาณทางยุทธศาสตร์



2. เพื่อการป้องปราม (Deterring) และการบีบบังคับ (Coercion)

การป้องปรามและการบีบบังคับเป็นยุทธศาสตร์ที่มีความต่อเนื่องจากการส่งสัญญาณ โดย “การป้องปราม” หมายถึง การทำให้รัฐอื่นไม่ยอมทำสิ่งที่เราไม่ต้องการ (discourage) โดยเฉพาะการใช้กำลังทหาร ด้วยการแสดงให้เห็นว่า หากลงมือกระทำ จะต้องเจอกับผลลัพธ์ที่ร้ายแรงจนไม่คุ้มค่า ⁴³ ตัวอย่างเช่น การเสริมสร้างแสนยานุภาพทางทหารให้แข็งแกร่ง เพื่อป้องปรามไม่ให้ประเทศเพื่อนบ้านรุกราน ส่วน “การบีบบังคับ” คือ การกดดันหรือบีบบังคับให้อีกฝ่ายยอมทำตามที่เราต้องการ โดยทำให้เขาเห็นว่าหากไม่ทำตามจะต้องเผชิญกับผลเสียที่ร้ายแรงกว่า (cost-benefit calculation) ⁴⁴ เช่น การขู่คว่ำบาตรทางเศรษฐกิจเพื่อบีบบังคับให้รับข้อตกลงสันติภาพ

⁴² Ibid., 461.

⁴³ RAND Corporation. (2018). Understanding deterrence. Retrieved October 11, 2023, from https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

⁴⁴ Borghard and Lonergan, “The Logic of Coercion in Cyberspace” 460.

แม้ยุทธศาสตร์ทั้งสองแบบมีความคล้ายคลึงกัน แต่มีความแตกต่างกันตรงที่การป้องปรามจะเน้นการทำให้รัฐอีกฝ่ายยอมรับกับสถานะปัจจุบัน (status quo) และไม่ต้องการจะทำหายหรือเปลี่ยนแปลง ส่วนการบีบบังคับจะผลักดันให้อีกฝ่ายต้องเปลี่ยนแปลงสถานะปัจจุบัน ซึ่งถือเป็นการกระทำที่ยากกว่า

ปัจจัยสำคัญที่สุดของยุทธศาสตร์ทั้งสอง คือ “ความน่าเชื่อถือ” (credibility) ของรัฐผู้ดำเนินการ ซึ่งประกอบด้วย 2 องค์ประกอบหลัก คือ “ความมุ่งมั่น” (resolve) และ “ขีดความสามารถ” (capability) โดยทั่วไปแล้ว ในมุมมองเชิงยุทธศาสตร์ รัฐมักประสบปัญหาเกี่ยวกับ “ความมุ่งมั่น” ซึ่งเป็นเรื่องของการรับรู้และวิจารณ์ญาณ (subjectivity) มากกว่า “ขีดความสามารถ” ซึ่งเป็นเรื่องที่วัดผลได้ชัดเจน (objectivity)⁴⁵ เช่น การครอบครองอาวุธที่สามารถนำมาเปรียบเทียบขีดความสามารถระหว่างกันได้อย่างเป็นรูปธรรมการป้องปรามจะเน้นการละเว้น

เมื่อพิจารณาในมุมทางไซเบอร์ แม้ว่ารัฐจะมีความมุ่งมั่นที่จะใช้เครื่องมือทางไซเบอร์เพื่อการป้องปรามหรือบีบบังคับแต่ด้วยข้อเท็จจริงที่ว่า การครอบครองอาวุธทางไซเบอร์ต้องอาศัยความลับและไม่เปิดเผย⁴⁶ ทำให้เกิด “ความเหลื่อมล้ำระหว่างขีดความสามารถและความมุ่งมั่นของรัฐ” ส่งผลต่อความน่าเชื่อถือของยุทธศาสตร์

ยกตัวอย่างเช่น ยุทธศาสตร์การป้องปรามด้วยการลงโทษ (Deterrence by Punishment) และยุทธศาสตร์บีบบังคับที่ต้องแสดงให้เห็นถึงขีดความสามารถในการสร้างความเสียหาย แต่ในกรณีของไซเบอร์กลับปรากฏว่า การเปิดเผยข้อมูลดังกล่าวอาจเป็นการเปิดเผยข้อมูลสำคัญที่ทำให้อีกฝ่ายป้องกันตนเองได้ดีขึ้น และลดทอนประสิทธิภาพของยุทธศาสตร์ลง

นอกจากนี้ ยุทธศาสตร์การป้องปรามโดยการสกัดกั้น (Deterrence by Denial) ซึ่งเน้นการป้องกันไม่ให้ฝ่ายตรงข้ามบรรลุเป้าหมาย โดยการทำให้การกระทำนั้นเป็นไปได้หรือยากที่จะประสบความสำเร็จ ด้วยวิธีการ เช่น การเสริมการป้องกัน การปกปิดเป้าหมาย หรือการป้องกันไม่ให้ฝ่ายตรงข้ามเข้าถึงทรัพยากรที่สำคัญ อันเป็นสิ่งที่กระทำได้ยากในเชิงไซเบอร์⁴⁷ เพราะในพื้นที่ทางไซเบอร์ ผู้กระทำการโจมตีมักจะมีควมได้เปรียบอย่างไม่สมมาตร (Asymmetrical Advantage) จากความสามารถปรับแต่งเครื่องมือโจมตีให้เข้ากับเป้าหมายได้อย่างเฉพาะเจาะจง ในขณะที่ฝ่ายป้องกันมักขาดความรู้เกี่ยวกับขีดความสามารถ รูปแบบการทำงาน และวิธีการป้องกันภัยคุกคามไซเบอร์ของฝ่ายตรงข้าม⁴⁸ ด้วยเหตุนี้ การรักษาความลับในขณะเดียวกันกับการแสดงศักยภาพเพื่อสร้างความน่าเชื่อถือ จึงเป็นความท้าทายสำคัญของการใช้เครื่องมือไซเบอร์เพื่อการป้องปรามหรือบีบบังคับ⁴⁹

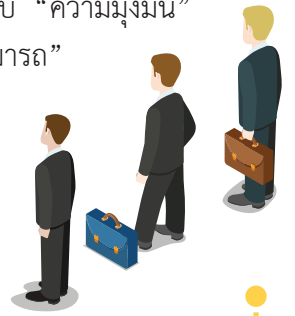
⁴⁵ Schelling, T. (1966). The art of commitment. In Arms and influence (pp. 35–91). Yale University Press.

⁴⁶ Borghard and Lonergan, “The Logic of Coercion in Cyberspace” 465.

⁴⁷ Ibid., 474.

⁴⁸ Dmitri Alperovitch, “The Case for Cyber-Realism: Geopolitical Problems Don’t Have Technical Solutions,” Foreign Affairs, 2021, accessed August 31, 2023, <https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism>.

⁴⁹ Buchanan, The Hacker and the State, 217.



3. เพื่อกำหนดทิศทางสถานการณ์ (Shaping)



ลักษณะของการใช้เครื่องมือทางไซเบอร์เพื่อกำหนดสถานการณ์ คือ การแอบใช้ขีดความสามารถทางไซเบอร์ในทางลับ เพื่อสร้างความได้เปรียบให้กับประเทศผู้ใช้⁵⁰ ไม่ว่าจะเป็นการใช้เพื่อบั่นทอนขีดความสามารถบางอย่างของอีกฝ่าย หรือเพื่อให้ได้มาซึ่งข้อมูลที่สำคัญในการประกอบการตัดสินใจ หรือเพื่อสนับสนุนการวางแผนเพื่อการเจรจาต่อรอง ตัวอย่างของการใช้เครื่องมือทางไซเบอร์ในลักษณะนี้ มีดังเช่น การใช้เพื่อลักลอบสร้างความเสียหาย การแอบขโมยข้อมูล หรือการบ่อนทำลาย (subversion)⁵¹ โดยในที่นี้จะอธิบายเพียงสองรูปแบบแรกเนื่องจากการบ่อนทำลายมีความเกี่ยวข้องกับมิติเชิงข้อมูลมากกว่าในเชิงตรรกะ

ตัวอย่างที่ดีที่สุดสำหรับ การใช้เครื่องมือทางไซเบอร์เพื่อลักลอบสร้างความเสียหาย คือกรณีของ Stuxnet ที่นักวิเคราะห์เชื่อว่ารัฐบาลสหรัฐฯ ร่วมกับรัฐบาลอิสราเอลในการลอบฝังมัลแวร์เข้าไปในโรงงานสกัดแร่ยูเรเนียมของอิหร่านเพื่อชะลอความสามารถในการพัฒนาขีดความสามารถด้านนิวเคลียร์ของอิหร่าน⁵² ความได้เปรียบเชิงยุทธศาสตร์ที่สหรัฐฯ อาจได้รับจากปฏิบัติการดังกล่าวมีคุณค่าอย่างมาก เนื่องจาก นอกจากสหรัฐฯ จะสามารถชะลอการพัฒนาอาวุธนิวเคลียร์ของอิหร่านไปได้กว่า 2 ปี เมื่อการชะลอดังกล่าวมีมาตรการการกีดกันทางการค้าช่วยเสริมด้วย ยังอาจช่วยกดดันให้อิหร่านต้องยอมกลับมาเจรจาข้อตกลง ว่าด้วยอาวุธนิวเคลียร์ในปี ค.ศ. 2015⁵³ สำเร็จ



สำหรับ การสร้างความได้เปรียบทางสถานการณ์ด้วยการแอบขโมยข้อมูล เช่น กรณีที่สหรัฐฯ ลอบเข้าถึงข้อมูลภายในสถานทูตของ บอสเนีย กาบอง ยูกันดา และไนจีเรีย เพื่อนำมาประเมินและสนับสนุนท่าทีในการเจรจาต่อรองในการประชุมคณะมนตรีความมั่นคงแห่งสหประชาชาติ ในปี ค.ศ. 2010⁵⁴ โดยข้อมูลที่รั่วออกมาภายหลังเปิดเผยว่า ผู้แทนสหรัฐฯ ในวงประชุมดังกล่าวอธิบายความได้เปรียบจากปฏิบัติการดังกล่าวว่า “ช่วยให้เขารู้ว่าประเทศอื่นกำลังพูดความจริงหรือไม่ ... ช่วยเปิดเผยจุดยืนที่แท้จริงของอีกฝ่าย ... และให้ข้อมูลเกี่ยวกับ ‘จุดที่ยอมรับไม่ได้’ (red lines) ของหลาย ๆ ประเทศ”⁵⁵

⁵⁰ Buchanan, The Hacker and the State, 2-5.

⁵¹ Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5–32. <https://doi.org/10.1080/01402390.2011.608939>.

⁵² Council on Foreign Relations. (n.d.). Stuxnet. Cyber Operation Tracker. Retrieved October 25, 2024, from <https://www.cfr.org/cyber-operations/stuxnet>.

⁵³ Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.

⁵⁴ Buchanan, The Hacker and the State, 9-11.

⁵⁵ Greenwald, G. (2014, May 14). Documents from No place to hide [Snowden NSA archive]. Retrieved from [source URL if available]. Cited in Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal geopolitics (p. 10). Harvard University Press.



ในขณะที่นักวิชาการมักตั้งข้อสงสัยเกี่ยวกับการใช้เครื่องมือไซเบอร์เพื่อเป้าหมายทางยุทธศาสตร์รูปแบบอื่น ๆ แต่กลับมีความเห็นพ้องต้องกันว่าการใช้เครื่องมือไซเบอร์เพื่อกำหนดทิศทางสถานการณ์นี้เป็นยุทธศาสตร์ที่เหมาะสมและมีประสิทธิภาพมากกว่าเพื่อจุดประสงค์อื่น ๆ เนื่องจากธรรมชาติของเครื่องมือทางไซเบอร์นั้นต้องเป็นความลับซึ่งสอดคล้องกับวัตถุประสงค์ของการกำหนดทิศทางสถานการณ์อยู่แล้ว นอกจากนี้ธรรมชาติของพื้นที่ทางไซเบอร์ยังมีความใกล้ชิดกับมิติด้านข้อมูล ซึ่งเมื่อรัฐหนึ่งสามารถเข้าถึงข้อมูลของอีกรัฐได้ย่อมก่อให้เกิดความได้เปรียบเชิงยุทธศาสตร์

ทั้งนี้ จะเห็นได้ว่าการใช้เครื่องมือทางไซเบอร์เพื่อสร้างความได้เปรียบทางสถานการณ์ให้กับรัฐผู้กระทำการนั้นจำเป็นต้องอาศัยเครื่องมือในการดำเนินนโยบายการต่างประเทศอื่น ๆ เช่น เครื่องมือทางเศรษฐกิจหรือการทูตควบคู่ไปด้วย

อย่างไรก็ตาม การใช้เครื่องมือไซเบอร์เพื่อกำหนดทิศทางสถานการณ์มีข้อจำกัดสำคัญคือรัฐผู้ใช้ต้องมีขีดความสามารถทางไซเบอร์ขั้นสูงเนื่องจากเครื่องมือที่ใช้ต้องมีความซับซ้อนและต้องออกแบบมาเฉพาะเจาะจงสำหรับระบบเป้าหมาย ซึ่งอาจรวมถึงการที่ผู้กระทำการต้องมีข้อมูลเชิงลึกเกี่ยวกับระบบของเป้าหมายด้วย



4. เพื่อสนับสนุนปฏิบัติการทางทหาร



รูปแบบสุดท้ายของการใช้เครื่องมือทางไซเบอร์เพื่อเป้าประสงค์ทางยุทธศาสตร์ คือ การใช้เพื่อสนับสนุนปฏิบัติการทางทหาร ในที่นี้ได้แก่ การโจมตีทางไซเบอร์ต่อระบบข้อมูลหรือโครงสร้างพื้นฐานสำคัญของรัฐอื่น เพื่อสร้างความเสียหายให้แก่อีกฝ่ายและสร้างความได้เปรียบในการเข้าปฏิบัติการของรัฐผู้กระทำการ

ตัวอย่างของการใช้เครื่องมือทางไซเบอร์ในการสู้รบทางทหารที่ชัดเจนที่สุด ณ ขณะนี้ ได้แก่ สมรภูมিরะหว่างรัสเซีย-ยูเครน นับตั้งแต่การบุกเข้ายึดพื้นที่บางส่วนของยูเครนในเดือน ก.พ. ปี ค.ศ. 2022 โดยพบว่า รัสเซียได้ใช้ปฏิบัติการโจมตีทางไซเบอร์ควบคู่ไปกับการโจมตีทางกายภาพ เช่น การรวบรวมระบบการสื่อสารหนึ่งชั่วโมงก่อนการยิงขีปนาวุธเข้าไปในพื้นที่ ส่งผลให้การโจมตีปกติมีแนวโน้มก่อความเสียหายต่อชีวิตและทรัพย์สินได้มากขึ้น⁵⁶ นอกจากนี้ยังพบการใช้ไวเปอร์แวร์ (wiperware) เพื่อลบข้อมูลภายในระบบคอมพิวเตอร์ออก ส่งผลให้การให้บริการภาครัฐที่สำคัญในยูเครนได้รับผลกระทบ⁵⁷ และการโจมตีแบบ DDoS Attack มุ่งเป้าไปที่ภาคการเงินการธนาคารของยูเครน⁵⁸

แม้การใช้เครื่องมือทางไซเบอร์จะดูเหมือนมีประสิทธิภาพในการช่วยเหลือปฏิบัติการทางทหาร แต่กลับสร้างข้อกังวลที่สำคัญให้กับประชาคมระหว่างประเทศในประเด็นของการเป็น “สงครามที่ยุติธรรม” (Just War) เนื่องจาก ตามกฎหมายมนุษยธรรมระหว่างประเทศ (International Humanitarian Law) – ที่รัฐภาคีของสหประชาชาติให้การยอมรับว่ามีผลบังคับใช้ในพื้นที่ทางไซเบอร์ – มองว่าการสู้รบยามสงครามจะต้องคำนึงถึงหลักการว่าด้วย “การแบ่งแยกระหว่างพลเรือนและทหาร” (Distinction) แต่ในความเป็นจริงโครงสร้างพื้นฐานทางด้านไซเบอร์มักมีลักษณะของการใช้ร่วมกันระหว่างภาคพลเรือนและทหาร ส่งผลให้การโจมตีหลาย ๆ ครั้งมีผู้ได้รับผลกระทบที่เป็นพลเรือนจำนวนมาก ในขณะเดียวกัน ผู้กระทำการโจมตีทางไซเบอร์ก็ไม่ได้จำกัดอยู่แค่กำลังพลทหารของรัฐแต่กลับ



⁵⁶ Duguin, S., & Pavlova, P. (n.d.). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. European Parliament. Retrieved October 28, 2024, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf#page12](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf#page12).

⁵⁷ Foreign Policy. (n.d.). Digital front lines: A sharpened focus on the risks of, and responses to, hybrid warfare. Retrieved October 28, 2024, from <https://digitalfrontlines.io>.

⁵⁸ Ibid.

มีพลเรือนที่มีความสามารถเข้าร่วมเป็นส่วนหนึ่งของปฏิบัติการ⁵⁹ โดยแม้ว่ากฎหมายระหว่างประเทศจะอนุญาตให้ผู้มีส่วนร่วมในลักษณะดังกล่าวสามารถตกเป็นเป้าหมายของการโจมตีได้ แต่ด้วยข้อเท็จจริงที่ว่าผู้ทำการโจมตีทางไซเบอร์ไม่จำเป็นต้องยึดโยงกับสภาพทางกายภาพ แต่สามารถดำเนินการโจมตีจากที่ไหนก็ได้ กลับทำให้การควบคุมหลักการในสมรภูมิรบเป็นเรื่องยุ่งยากมากขึ้น

ด้วยเหตุที่กล่าวมาข้างต้น การใช้เครื่องมือทางไซเบอร์ในสมรภูมิรบจึงเป็นความท้าทายสำคัญของประชาคมระหว่างประเทศในการกำหนดกฎเกณฑ์ทางมนุษยธรรมที่เหมาะสมต่อไป

ทั้งนี้ ในความขัดแย้งทางการทหาร ยังมีมิติของการสร้างความเสียหายทางกายภาพ เช่น การทำลายสายเคเบิลใต้ทะเล และมิติของปฏิบัติการด้านข้อมูลข่าวสาร (ซึ่งมีบทบาทอย่างมากในสงครามรัสเซีย-ยูเครนปัจจุบัน) ซึ่งเป็นมิติอื่น ๆ ของความมั่นคงปลอดภัยไซเบอร์ควบคู่ไปด้วย ทว่าทั้งสองมิติอยู่นอกเหนือขอบเขตในการวิเคราะห์ของบทความชิ้นนี้

สรุป

แม้ประเด็นความขัดแย้งทางไซเบอร์จะฟังดูเป็นเรื่องใหม่สำหรับผู้กำหนดนโยบายด้านความมั่นคง แต่ในความเป็นจริง ประเด็นความขัดแย้งทางไซเบอร์กลับเป็นประเด็นที่มีบทบาทต่อการเมืองระหว่างประเทศมาเป็นระยะเวลาหนึ่ง ทั้งยังมีการศึกษาจำนวนมากให้ผู้กำหนดนโยบายได้นำมาเป็นบทเรียน โดยเฉพาะ เมื่อเปรียบเทียบกับประเด็นเทคโนโลยีเกิดใหม่อย่าง ปัญญาประดิษฐ์หรือเทคโนโลยีชีวภาพ ที่ยังไม่ปรากฏข้อมูลในเชิงนโยบายให้ค้นคว้าได้มากนัก

บทความนี้ได้นำเสนอความเป็นไปได้ ข้อจำกัด และความท้าทายในการใช้เครื่องมือทางไซเบอร์เพื่อเป้าประสงค์ทางยุทธศาสตร์ของรัฐ โดยทุกวิธีการล้วนมีความสำคัญสำหรับประเทศไทยในการศึกษาเพื่อถอดบทเรียน และวางแผนนโยบายในการรับมือ ตอบโต้ หรือกระทั่งเลือกใช้เครื่องมือทางไซเบอร์และเครื่องมือทางการเมืองระหว่างประเทศอื่น ๆ เพื่อรักษาผลประโยชน์แห่งชาติของไทยเอาไว้ท่ามกลางการแข่งขันทางภูมิรัฐศาสตร์โลกต่อไป

การกำหนดนโยบายทางไซเบอร์ที่มีประสิทธิภาพจำเป็นต้องมองประเด็นทางไซเบอร์ให้กว้างกว่าการเป็นแค่ “ปัญหาเชิงเทคนิค” ที่ต้องแก้ไขเฉพาะหน้า และตระหนักว่าประเด็นและเครื่องมือทางไซเบอร์คือกลไกสำคัญในการขับเคลื่อนผลประโยชน์แห่งชาติ ซึ่งต้องอาศัยทั้งมิติทางการเมืองและการทูตในการกำหนดทิศทางต่อไป

⁵⁹ Duguin, S., & Pavlova, P. (n.d.). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. European Parliament. Retrieved October 28, 2024, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf).



บรรณานุกรม

Black Hat. (n.d.). *A decade after Stuxnet's printer vulnerability: Printing is still the stairway to heaven*. Retrieved October 28, 2024, from <https://www.blackhat.com/html/webcast/05202021-a-decade-after-stuxnets-printer-vulnerability-printing-is-still-the-stairway-to-heaven.html>

Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, 26(3), 450–474. <https://www.tandfonline.com/doi/citedby/10.1080/09636412.2017.1306396?scroll=top&needAccess=true>

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal geopolitics*. Harvard University Press.

Council on Foreign Relations. (n.d.-a). *Compromise of Sony Pictures Entertainment*. Cyber Operation Tracker. Retrieved October 25, 2024, from <https://www.cfr.org/cyber-operations/compromise-sony-pictures-entertainment>

Council on Foreign Relations. (n.d.-b). *Cyber Operation Tracker*. Retrieved October 25, 2024, from <https://www.cfr.org/cyber-operations/>

Council on Foreign Relations. (n.d.-c). *Estonia denial of service incident*. Cyber Operation Tracker. Retrieved October 25, 2024, from <https://www.cfr.org/cyber-operations/estonian-denial-service-incident>

Council on Foreign Relations. (n.d.-d). *Stuxnet*. Cyber Operation Tracker. Retrieved October 25, 2024, from <https://www.cfr.org/cyber-operations/stuxnet>

Cybersecurity & Infrastructure Security Agency. (n.d.). *Fact sheet: Russian SVR activities related to SolarWinds compromise*. Retrieved October 25, 2024, from https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf

Alperovitch, D. (2021). The case for cyber-realism: Geopolitical problems don't have technical solutions. *Foreign Affairs*. Retrieved August 31, 2023, from <https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism>

Duguin, S., & Pavlova, P. (n.d.). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. European Parliament. Retrieved October 28, 2024, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf)

Foreign Policy. (n.d.). *Digital front lines: A sharpened focus on the risks of, and responses to, hybrid warfare*. Retrieved October 28, 2024, from <https://digitalfrontlines.io>

Greenwald, G. (2014, May 14). *Documents from No place to hide*. [Snowden NSA archive]. Cited in Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal geopolitics* (p. 10). Harvard University Press.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2013, June 24). *United Nations*. Retrieved October 25, 2024, from https://dig.watch/wp-content/uploads/A_68_98_E.pdf

Harknett, R. J., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45(4), 534–567. <https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354>

Henley, J. (2021, May 31). Denmark helped US spy on Angela Merkel and European allies – Report. *The Guardian*. Retrieved October 25, 2024, from <https://www.theguardian.com/world/2021/may/31/denmark-helped-us-spy-on-angela-merkel-and-european-allies-report>

Jervis, R. (1976). *Perception and misperception in international politics*. Princeton University Press.

NBC News. (2009, July 9). *A look at Estonia's cyber attack in 2007*. Retrieved October 28, 2024, from https://www.nbcnews.com/id/wbna31801246#.WNLFP2_yuUk

Paletta, D., & Schwartz, F. (2016, February 2). Pentagon deploys cyberweapons against Islamic State. *The Wall Street Journal*. Retrieved October 28, 2024, from <https://www.wsj.com/articles/pentagon-deploys-cyberweapons-against-islamic-state-1456768428>

Pernik, P., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., et al. (2018). *The early days of cyberattacks: The cases of Estonia, Georgia, and Ukraine*. In N. Popescu & S. Secieru (Eds.), *Hacks, leaks, and disruptions: Russian cyber strategies* (pp. 9–20). European Union Institute for Security Studies (EUISS). Retrieved from <https://www.jstor.org/stable/resrep21140.9>

RAND Corporation. (2018). *Understanding deterrence*. Retrieved October 11, 2023, from https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32. <https://www.tandfonline.com/doi/full/10.1080/01402390.2011.608939>

Schelling, T. (1966). *Arms and influence*. Yale University Press.

Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs.

