การสู้รบทางไซเบอร์: Uncertainty ในกฎหมายระหว่างประเทศ สู่ Uncharted ในกฎหมายไทย

รองศาสตราจารย์ ดร.วิณัฏฐา แสงสุข และคณะ

การสู้รบทางไซเบอร์: Uncertainty ในกฎหมายระหว่างประเทศ สู่ Uncharted ในกฎหมายไทย
Cyber Warfare: Uncertainty in International Law to Uncharted in Thai Law

รองศาสตราจารย์ ดร.วิณัฏฐา แสงสุข[*] และคณะ[**]
Associate Professor Dr.Winatta Saengsook *et. al*.

บทคัดย่อ

การสู้รบทางไซเบอร์ (Cyber Warfare) กลายเป็นอีกหนึ่งทางเลือกสำหรับความขัดแย้งในโลกยุคใหม่ นอกเหนือจากการรบแบบดั้งเดิม โดยสำหรับการสู้รบทางไซเบอร์ระหว่างรัฐกับรัฐนั้น กฎหมายระหว่างประเทศมีบทบัญญัติที่ครอบคลุมถึงวิธีการรบที่แปรเปลี่ยนไปเมื่อมีการใช้กำลัง

---

[*]อาจารย์ประจำสาขาวิชานิติศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา; น.บ. มหาวิทยาลัยรามคำแหง, น.บ.ท. สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา; น.ม. (กฎหมายธุรกิจ) มหาวิทยาลัยรามคำแหง, น.ด. สถาบันการศึกษานานาชาติ มหาวิทยาลัยรามคำแหง. E-mail: swinatta@aru.ac.th.

Lecturer in Law at Faculty of Humanities and Social Sciences, Phranakhon Si Ayutthaya Rajabhat University; LL.B. Ramkhamhaeng University; Barrister at Law at Thai Bar under The Royal Patronage; LL.M. in Business Law, Ramkhamhaeng University; LL.D. Ramkhamhaeng University.

[**]คณะผู้เขียนประกอบด้วยนางสาวณัฏฐธิดา วุ้นศิริ รองศาสตราจารย์พิมพ์ใจ รื่นเริง และผู้ช่วยศาสตราจารย์ภัทระ ลิมป์ศิระ.

The Co-Authors are Nuttathida Voonsiri, Associate Professor Pimjai Ruenrerng, Assistant Professor Patthara Limsira.

คณะผู้เขียนขอขอบคุณ นายนรินทร์ฤทธิ์ เปรมอภิวัฒโนกุล ที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ อุปนายกสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA) ประธานกรรมการบริหาร บริษัท เอฝน เพรเชียส จำกัด สำหรับคำแนะนำทางด้านความมั่นคงทางไซเบอร์.

The authors would like to express their appreciation to Narinrt Prem-apiwathanokul, A Chief Executive Officer, AFON Precious Co., Ltd., for his cybersecurity consulting.

วันที่รับบทความ (received) 19 มิถุนายน 2567, วันที่แก้ไขบทความ (revised) 7 กันยายน 2567, วันที่ตอบรับบทความ (accepted) 18 กันยายน 2567.

(Use of Force) และการขัดกันทางอาวุธ (armed conflict) อย่างไรก็ตาม การพัฒนาอย่างต่อเนื่องในรูปแบบภัยคุกคามทางไซเบอร์ (Cyber Threat) ส่งผลให้เกิดความไม่ชัดเจนในการบังคับใช้กฎหมายระหว่างประเทศ นอกจากนี้ กฎหมายในประเทศไทยเองก็ต้องมีการพัฒนากฎระเบียบเกี่ยวกับสู้รบทางไซเบอร์เพื่อปกป้องโครงสร้างสำคัญ และความมั่นคงทางไซเบอร์ของประเทศเพื่อรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงสู้รบทางไซเบอร์เพื่อรักษาผลประโยชน์ของประเทศชาติต่อไป ด้วยเหตุดังกล่าวบทความนี้มีวัตถุประสงค์เพื่อ 1) ศึกษากฎหมายระหว่างประเทศสามารถครอบคลุมถึงสู้รบทางไซเบอร์หรือไม่ 2) วิเคราะห์ว่าหน่วยงานทั้งภาครัฐ และเอกชนในประเทศไทยมีการเตรียมความพร้อมสำหรับการสู้รบทางไซเบอร์ภายใต้กรอบพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 และการดำเนินการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สมกช.) เป็นหน่วยงานรับผิดชอบตามพระราชบัญญัติแล้วหรือไม่ และ 3) เพื่อให้ข้อเสนอแนะในการปรับปรุงกฎหมายไทย รวมถึงแนวปฏิบัติด้านความมั่นคงทางไซเบอร์

คำสำคัญ: กฎหมายมนุษยธรรมระหว่างประเทศ, ความมั่นคงทางไซเบอร์, การสู้รบทางไซเบอร์

Abstract

Cyber warfare offers an alternative to traditional warfare in modern conflicts. Although international law has some provisions that may provide some guidance on the use of force and armed conflicts, there are still ongoing development in cyber threats. This has resulted in ambiguity in the enforcement of international law. Additionally, regulations in Thailand must be developed related to cyber warfare to protect its critical infrastructure and cyber security to deal with cyber threats, including cyber warfare, in order to preserve national interests. For this reason, the purpose of this article is to study 1) whether cyber warfare can be governed by international law, 2) whether both government and private agencies in Thailand is prepared for cyber warfare under the framework of the Cyber Security Act 2019 and the operations of the Office of the Security as the government agency responsible under such Act and 3) to provide suggestions for Thai law and practices regarding cyber security.

Keywords: international humanitarian law, cyber security, cyber warfare

1. บทนำ

ยามที่นึกถึงการสงครามหรือการสู้รบ ย่อมจินตนาการได้ถึงการนำอาวุธสงครามยุทโธปกรณ์เข้าประหัดประหารกันและเป็นเรื่องง่ายที่จะสามารถมองเห็นความเสียหายของสิ่งปลูกสร้าง และการเสียชีวิตล้มตายของผู้คน จุดเปลี่ยนของเทคโนโลยีการทหารถูกพัฒนามาถึงการกำเนิดของอาวุธนิวเคลียร์ในช่วงสงครามโลกครั้งที่ 2 หลังจากนั้น เทคโนโลยีก็เปลี่ยนไปอีกขั้นจนเข้ามาสู่ยุคที่เทคโนโลยีดิจิทัลก้าวล้ำหน้า และพัฒนาอย่างไม่มีจุดสิ้นสุด การทำสงครามจึงไม่ใช่การขนอาวุธมาสู้รบกันแบบดั้งเดิมอีกต่อไป[1] โดยอาวุธที่ถูกนำมาเป็นเครื่องมือสำคัญไม่ใช่อาวุธที่ใช้สำหรับการสังหารเป้าหมายโดยตรง แต่อาวุธที่ถูกนำมาเป็นเครื่องมือกลับเป็นเทคโนโลยีสารสนเทศและอินเทอร์เน็ตแทนเทคโนโลยีดิจิทัลต่างๆ เหล่านี้จึงเข้ามามีบทบาทในการต่อสู้กัน อีกทั้ง การป้องกันสงครามลักษณะเช่นนี้มิอาจทำได้ในวิธีการเหมือนกับการป้องกันสงครามนิวเคลียร์ ซึ่งสงครามลักษณะนี้ถูกเรียกว่าสงครามไซเบอร์ (Cyber War) เนื่องจากอาวุธที่ใช้ในสงครามไซเบอร์นี้มีวิธีการที่แตกต่างจากอาวุธแบบดั้งเดิม[2] สงครามไซเบอร์ คือ ความขัดแย้งระหว่างสองรัฐขึ้นไปที่ดำเนินการผ่านช่องทางไซเบอร์เป็นหลัก จึงเกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เครือข่าย และอินเทอร์เน็ตเพื่อโจมตีและป้องกันในทางระหว่างประเทศ ซึ่งโดยทั่วไปจะเกี่ยวข้องกับคำว่า สงคราม (War) ซึ่งโดยเนื้อแท้แล้วหมายถึงการกระทำขนาดใหญ่ โดยทั่วไป ในช่วงระยะเวลาที่ยืดเยื้อ และอาจรวมถึงวัตถุประสงค์ที่ต้องการใช้ความรุนแรงหรือจุดมุ่งหมายที่จะฆ่า ซึ่งสภาวะสงครามจะเกิดขึ้นได้จะต้องมีการประกาศสงครามเสียก่อน[3]

ในทางกลับกัน การสู้รบทางไซเบอร์ (Cyber Warfare) เป็นคำที่กว้างกว่าซึ่งหมายถึง การใช้วิธีดิจิทัล เทคนิค ยุทธวิธี และขั้นตอนที่อาจเกี่ยวข้องกับสงครามไซเบอร์ ซึ่งยังคงไม่ได้มีคำนิยาม

---

[1]Jan Angstrom and Jerker J. Widen, **Contemporary Military Theory: The dyanmics of war** (New York: Routledge, 2015), pp. 13-32; William W. Davis, George T. Duncan and Randolph M. Siverson, "The Dynamics of Warfare: 1816-1965," **American Journal of Political Science** 22, 4 (1978): 772-792.

[2]George Noel and Mark Reith, "Cyber Warfare Evolution and Role in Modern Conflict," **Journal of Information Warfare**, 20, 4 (2021): 30-44; Hans-Joachim Heintze and Pierre Thielbörger, Eds., **From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the last 25 Years** (Switzerland: Springer Cham, 2016), pp. 1-18, 107 ff.

[3]Section III of the Hague Convention of 1907; Andrew Clapham, "Declarations of War and Neutrality," In **War**, (Oxford: Oxford University Press, 2021), pp. 41-79.

ที่เป็นที่ยุติ[4] แต่คำนี้ไม่ได้หมายความถึงขนาด การยืดเยื้อ หรือความรุนแรง โดยการสู้รบ (Warfare) หมายถึง การกระทำอย่างหนึ่งของการทำสงคราม โดยการสู้รบเป็นส่วนหนึ่งของสงคราม แต่สงครามเป็นการแสดงความสัมพันธ์ระหว่างรัฐกับรัฐหรือในกรณีสงครามกลางเมืองระหว่างกลุ่มคนสองกลุ่ม ดังนั้น ความหมายของการสู้รบ (Warfare) กับสงคราม (War) จึงมีความแตกต่างกัน[5] ซึ่งการสู้รบจึงเป็นการกระทำที่คล้ายสงคราม (Warlike) จึงทำให้การสู้รบทางไซเบอร์จึงเป็นคำปลายเปิดมากกว่าและเป็นคำที่มีความหมายกว้างกว่า[6]

เนื่องมาจาก สงครามไซเบอร์จำเป็นจะต้องมีการประกาศสงครามก่อน แล้วจึงดำเนินการโจมตีทางไซเบอร์ ซึ่งอาจมีการปฏิบัติการทางทหารที่ใช้อาวุธอย่างแบบดั้งเดิมระหว่างรัฐที่ทำสงครามกัน โดยจนถึงขณะนี้ยังไม่มีการกระทำดังกล่าวเกิดขึ้นที่ดำเนินการครบตามหลักเกณฑ์ ซึ่งเป็นช่องว่างในทางกฎหมายในการที่จะต้องมีพัฒนาการต่อไปในอนาคต[7]

ดังนั้น บทความฉบับนี้จึงมีวัตถุประสงค์เพื่อศึกษาการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ พร้อมทั้งวิเคราะห์สถานะทางกฎหมายของการโจมตีทางไซเบอร์ตามกฎหมายระหว่างประเทศ เช่น กฎหมายมนุษยธรรมระหว่างประเทศ และการใช้กำลังตามกฎบัตรสหประชาชาติ เป็นต้น เพื่อพิจารณาว่าการสู้รบทางไซเบอร์จะถือว่าเป็นสงครามตามกฎหมายระหว่างประเทศได้หรือไม่ รวมถึงพิจารณาแนวคิด และหลักเกณฑ์ต่าง ๆ ที่อาจนำมาใช้เพื่อให้สามารถครอบคลุมการสู้รบทางไซเบอร์ และการใช้กำลังโดยวิธีการทางไซเบอร์ รวมถึงคู่มือทาลลินน์ด้วย สำหรับในส่วนของประเทศไทยได้มีการเตรียมความพร้อมในเรื่องการสู้รบทางไซเบอร์ ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 หรือไม่ เพียงใด โดยพิจารณาถึงคำนิยามที่เกี่ยวข้อง ขอบเขตการออกและใช้มาตรการสำหรับการสู้รบทางไซเบอร์ภายใต้พระราชบัญญัติดังกล่าว ทั้งนี้ ไม่รวมถึงประเด็นของอาชญากรรมทางคอมพิวเตอร์

---

[4]Jeffrey Carr, **Inside Cyber Warfare: Mapping the cyber underworld**, 2nd ed. (Sebastopol: O'Reilly, 2011), pp. 1-2; Lianne J. M. Boer, **International Law As We Know It: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship** (Cambridge: Cambridge University Press, 2021), pp. 1-25.

[5]ไพศาล นภสินธุวงศ์, "สงคราม และกฎการสงคราม War and Principles of War," **วารสารนาวิกาธิปัตย์สาร** 79 (กุมภาพันธ์-พฤษภาคม 2553): 76-93.

[6]Peter W. Singer and Allan Friedman, **Cybersecurity and Cyberwar: What everyone needs to know** (Oxford: Oxford University Press, 2014), p. 13.

[7]Martin C. Libicki, "Appendix A: What Constitutes an Act of War in Cyberspace?," In **Cyberdeterrence and Cyberwar** (Arlington, VA: RAND Corporation, 2009), pp. 179-182.

2. การโจมตีทางไซเบอร์

สนามรบไซเบอร์มาจากการโจมตีทางไซเบอร์ (Cyber Attack)[8] ซึ่งหมายความถึง การดำเนินการทางไซเบอร์ ไม่ว่าจะเป็นเชิงรุกหรือเชิงป้องกัน ที่คาดว่าจะก่อให้เกิดการบาดเจ็บหรือเสียชีวิตต่อบุคคล หรือความเสียหายหรือมีผลทำให้ทรัพย์สินถูกทำลาย ทั้งในทางกายภาพ และในโลกดิจิทัล[9] รวมไปถึงการโจมตีระหว่างรัฐบาลด้วยเพื่อทำลายเสถียรภาพทางการเมือง[10] โดยคำดังกล่าวต่างจากอาชญากรรมทางไซเบอร์ (Cybercrime) ซึ่งหมายถึง การกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหายแก่คอมพิวเตอร์หรือเครือข่ายอื่น ๆ หรือการให้เทคโนโลยีเพื่อช่วยเหลือ อำนวยความสะดวกหรือทำให้การกระทำความผิดนั้นมีผลเป็นวงกว้างยิ่งขึ้น ในกรณีที่มีการใช้เทคโนโลยีเข้าโจมตีหรือหลอกลวงมาจากต่างประเทศหรือเป็นคนต่างชาติก็ตามแต่ก็มิได้เข้าลักษณะเป็นสู้รบทางไซเบอร์ หากแต่เป็นการทำอาชญากรรมทางคอมพิวเตอร์ เช่น การหลอกผ่านอีเมลว่าได้รับรางวัล การหลอกขายสินค้าแต่ไม่ส่งสินค้าให้ แก๊งคอลเซ็นเตอร์ หลอกโอนเงินหรือดูดเงินจากบัญชีธนาคาร เป็นต้น

โดยที่จุดมุ่งหมายหลักของการโจมตีของการสู้รบทางไซเบอร์นั้นมี 5 ประการ คือ[11]

1) การหยุดชะงักของระบบไฟฟ้า (Power Failures) เมื่อไฟฟ้าขัดข้องอาจเป็นอันตรายต่อเศรษฐกิจของประเทศและส่งผลกระทบต่อประชาชน

---

[8]เมื่อวันที่ 2 พฤศจิกายน ค.ศ. 1988 ที่สหรัฐอเมริกา นายโรเบิร์ต มอร์ริส (Robert Morris) ปล่อยมัลแวร์ (Malware) ชื่อว่า หนอนมอร์ริส (Morris Worm) ได้สำเนาตัวเองและแพร่กระจายในอินเทอร์เน็ต ส่งผลให้คอมพิวเตอร์ประมาณ 3,000-4,000 เครื่องติดเชื้อ และถูกขัดขวางการทำงานให้ช้าลง สร้างความเสียหาย ประมาณ 98 ล้านดอลลาร์สหรัฐ ถือเป็นการโจมตีทางไซเบอร์เกิดขึ้นครั้งแรกในโลกอินเทอร์เน็ต. See, United States v. Morris (1991), 928 F.2d 504, 505 (2d Cir. 1991); Peter J. Denning, **The Internet Worm** (Mountain View: NASA Ames Research Center, 1989), pp. 1-2.

[9]International Committee of the Red Cross, **What limits does the law of war impose on cyber attacks?** [Online], available URL: https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.html, 2013 (June, 28).

[10]Valeriano Brandon and Ryan C. Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists," In **Cyber War versus Cyber Realities: Cyber Conflict in the International System** (Oxford: Oxford University Press, 2015), pp. 78-108.

[11]Oliver Buxton, **Cyber Warfare: Types, Examples, and How to Stay Safe** [Online], available URL https://www.avast.com/c-cyber-warfare, 2023 (July, 14).

2) การละเมิดความปลอดภัยทางไซเบอร์ (Cybersecurity Breaches) มักเป็นการโจมตีด้วยการแฮ็ก อาจทำให้ระบบซอฟต์แวร์เสียหายหรือรบกวนระบบเครือข่ายรัฐบาลที่ไม่ได้มีการป้องกัน

3) ข้อมูลรั่วไหล (Data Leaks) โดยการละเมิดข้อมูลขนาดใหญ่อาจส่งผลกระทบต่อข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ เช่น เวชระเบียนหรือรายละเอียดทางธนาคาร เป็นต้น

4) การก่อวินาศกรรมทางทหารหรือทางอุตสาหกรรม (Military or Industrial Sabotage) เป็นการโจมตีโดยตรงต่อความมั่นคงของชาติหรือโครงสร้างพื้นฐานทางเศรษฐกิจของประเทศทำให้ความสามารถทางทหารหรืออุตสาหกรรมลดลง

5) การหยุดชะงักของการสื่อสาร (Communications Disruption) ซึ่งกระทบต่อโทรศัพท์ โทรศัพท์มือถือ อีเมล หรือการสื่อสารดิจิทัลอื่น ๆ ที่อาจถูกปิด สกัดกั้น หรือดัดแปลงแก้ไขข้อมูลได้

โดยการโจมตีทางไซเบอร์นั้นไม่มีการดำเนินการที่เหมือนกัน และรูปแบบการโจมตีที่อาจเกิดขึ้นมีมากมายไม่มีที่สิ้นสุด แต่ท่ามกลางรูปแบบของการโจมตีทางไซเบอร์ที่หลากหลายนั้น การดำเนินการสู้รบทางไซเบอร์มักจะอยู่ในวิธีการโจมตีอย่างใดอย่างหนึ่งต่อไปนี้[12]

1) มัลแวร์ (Malware) หรือซอฟต์แวร์ที่เป็นอันตรายจะปลอมตัวเป็นไฟล์แนบอีเมลหรือโปรแกรมที่เชื่อถือได้ เช่น เอกสารหรือโฟลเดอร์ไฟล์ที่เข้ารหัส เพื่อแสวงหาประโยชน์จากไวรัสและอนุญาตให้แฮกเกอร์เข้าสู่เครือข่ายคอมพิวเตอร์ การโจมตีทางไซเบอร์ประเภทนี้มักจะทำให้ระบบเทคโนโลยีสารสนเทศทั้งเครือข่ายต้องหยุดชะงัก ตัวอย่างของมัลแวร์ ได้แก่

(1) ไวรัส (Virus) จะแทรกตัวเข้าไปในโปรแกรมหรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ให้มีสภาพเป็นพาหะในการแพร่กระจายไปยังเครื่องอื่นๆ โดยไวรัสจะทำงานก็ต่อเมื่อผู้ใช้เปิดโปรแกรมหรือไฟล์ที่ติดไวรัสเท่านั้น ไวรัสจะติดต่อตัวเองไปยังโปรแกรมหรือไฟล์อื่น ๆ ในระบบคอมพิวเตอร์ ทำให้เกิดความเสียหายต่อระบบ

(2) โทรจัน (Trojan) จะแฝงตัวมาในรูปแบบของโปรแกรมที่ดูน่าเชื่อถือและหลอกผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย เมื่อผู้ใช้เปิดโปรแกรมหรือติดตั้ง โทรจันจะเปิดช่องทางให้ผู้โจมตีเข้าถึงระบบคอมพิวเตอร์นำมาสู่ความเสียหายในภายหลัง คล้ายกับกลยุทธ์การรบด้วยม้าโทรจัน (Trojan Horse) ในเรื่องสงครามโทรจันที่เมืองทรอย (Troy)

(3) หนอนคอมพิวเตอร์ (Worm) สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่ายได้ เช่น อีเมล การแชร์ไฟล์ โดยไม่ต้องอาศัยไฟล์อื่น เวิร์มสามารถขโมยข้อมูล หรือทำลายระบบเครือข่ายได้

---

[12] ไมโครซอฟ, **การโจมตีทางไซเบอร์คืออะไร** [Online], available URL: https://www.microsoft.com/th-th/security/business/security-101/what-is-a-cyberattack, (ม.ป.ป.).

(4) แรนซัมแวร์ (Ransomware) จะทำการเข้ารหัส หรือล็อกไฟล์ ไม่ให้ผู้ใช้สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความหาผู้ใช้หรือองค์กร เพื่อเรียกค่าไถ่ (Ransom) แลกกับการถอดรหัสเพื่อปลดล็อกข้อมูลหรือกู้ข้อมูลคืนมา มักพบเจอบ่อยในระดับองค์กร หรือหน่วยงานรัฐบาล

(5) สปายแวร์ (Spyware) ติดตั้งบนระบบคอมพิวเตอร์ของผู้ใช้เพื่อแอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนบุคคล เช่น บัญชีชื่อผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น

(6) แบคดอร์ (Backdoor) คือ การเปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว

(7) รูทคิท (Rootkit) คือ การเปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

2) การโจมตีโดยปฏิเสธการให้บริการ (Denial-of-Service: DoS) เป็นการโจมตีเพื่อทำให้ระบบคอมพิวเตอร์ เครือข่าย หรือบริการไม่สามารถใช้งานได้ โดยการส่งข้อมูลจำนวนมหาศาลไปยังระบบเป้าหมาย วิธีการทำงานของ DoS จะมี 3 ขั้นตอน คือ

(1) โจมตีระบบด้วยข้อมูล ผู้โจมตีจะส่งข้อมูลจำนวนมหาศาลไปยังระบบเป้าหมาย ทำให้ระบบโอเวอร์โหลดและหยุดทำงาน

(2) โจมตีช่องโหว่ของระบบ ผู้โจมตีจะใช้ประโยชน์จากช่องโหว่ของระบบเพื่อทำให้ระบบหยุดทำงาน และ

(3) การโจมตีโดยปฏิเสธการให้บริการแบบกระจาย (Distributed Denial-of-Service: DDoS) เป็นการโจมตีแบบ DoS โดยการที่แฮกเกอร์จะทำการส่งคำขอเข้าถึงข้อมูล (Traffic) จากอุปกรณ์จำนวนมาก และหลากหลายแหล่งที่มา ไปยังเว็บไซต์ที่ต้องการโจมตีพร้อม ๆ กัน ซึ่งยากต่อการป้องกัน ส่งผลให้เว็บไซต์นั้นมีปริมาณคำขอเข้าถึงข้อมูลมากเกินกว่าที่ระบบเครือข่ายจะสามารถรองรับได้ ทำให้เว็บไซต์ไม่สามารถใช้งานได้ โดยวิธีนี้นั้นได้เคยถูกนำมาใช้โดยประเทศเอสโทเนีย อันเนื่องมาจากเหตุความขัดแย้งทางเชื้อชาติอย่างรุนแรงภายในประเทศส่งผลให้บริการทางการเงินในประเทศเอสโทเนีย ณ ขณะนั้นไม่สามารถใช้งานได้[13]

---

[13]Silpa, **สงครามไซเบอร์ครั้งแรก ๆ ของโลก และการก้าวข้ามนิยาม IO สู่ภัยจากรัฐชาติ...** [Online], available URL: https://www.silpa-mag.com/history/article_46065, 2564 (พฤศจิกายน, 11); Vsm365, **รูปแบบการโจมตีทาง Cyber ที่คุณควรรู้จัก** [Online], available URL: https://www.vsm365.com/th/articles/Types-of-cyber-attacks-you-should-know, 2567 (พฤษภาคม, 9).

โดยตัวอย่างการโจมตีแบบ DoS ได้แก่

- การโจมตีแบบ SYN flood ผู้โจมตีจะส่ง SYN packet จำนวนมหาศาลไปยังระบบเป้าหมาย ทำให้ระบบโอเวอร์โหลดและหยุดทำงาน

- การโจมตีแบบ Ping of Death ผู้โจมตีจะส่ง ICMP packet ขนาดใหญ่ไปยังระบบเป้าหมาย ทำให้ระบบหยุดทำงาน

- การโจมตีแบบ HTTP flood ผู้โจมตีจะส่ง HTTP request จำนวนมหาศาลไปยังเว็บไซต์เป้าหมาย ทำให้เว็บไซต์หยุดทำงาน

3) ฟิชชิ่ง (Phishing) คือ ภัยคุกคามที่ใช้เทคนิคทางวิศวกรรมสังคม (Social engineering) ด้วยการหลอกลวง ล่อหลอกผู้อื่น ใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล ตัวอย่างเช่น ผู้โจมตีส่งอีเมลที่ดูน่าเชื่อถือในนามของบริษัทที่มีชื่อเสียงให้ผู้ใช้งานกดคลิกลิงก์ และเข้าไปกรอกข้อมูลบัตรเครดิต หรือข้อมูลละเอียดอ่อนอื่น ๆ ในหน้าเพจที่ทำปลอมขึ้นมาอย่างแนบเนียน หรือให้ผู้ใช้ดาวน์โหลดไฟล์ที่แนบมากับอีเมลแล้วติดตั้งมัลแวร์ประเภทต่าง ๆ ในคอมพิวเตอร์ขององค์กร เพื่อเข้าถึงข้อมูลบนเครือข่ายส่วนตัวหรือของธุรกิจ

4) การโจมตีผ่าน Structured Query Language (SQL) ซึ่งเป็นภาษามาตรฐานในการเข้าถึงฐานข้อมูล โดยมี 2 รูปแบบ[14] คือ

(1) SQL injection คือ การใช้ช่องโหว่ด้านความปลอดภัยของเว็บแอปพลิเคชัน (Web Application) ที่ทำให้แฮกเกอร์สามารถแอบหาข้อมูล สืบค้นเว็บแอปพลิเคชันโดยทำกับฐานข้อมูล มักจะช่วยให้อาชญากรไซเบอร์ดูข้อมูลที่เราไม่สามารถค้นได้ และเป็นข้อมูลส่วนตัวของผู้อื่น อาชญากรไซเบอร์ยังสามารถแก้ไขหรือลบข้อมูลนี้ได้อีกด้วย

(2) NoSQL injection คือ การใช้ข้อบกพร่องของความปลอดภัยของเว็บแอปพลิเคชันที่ใช้ฐานข้อมูล โดยส่วนมากช่องโหว่ของ NoSQL injection นั้น เกิดเมื่อเว็บแอปพลิเคชันได้รับการป้อนข้อมูล (Input) ของ ผู้ใช้งานโดยตรงมา process โดยที่ไม่มีการตรวจสอบหรือกรอง Input ต่าง ๆ นั่นเอง

แม้ว่าการโจมตี SQL ของทั้งสองอย่างจะคล้ายคลึงกัน แต่ข้อแตกต่างหลักที่เห็นได้ชัดระหว่าง NoSQL และ SQL นั้น คือ วากยสัมพันธ์ (Syntax) และ ไวยกรณ์ (Grammar) ของการ

---

[14]Supawee Foitong, **NoSQL injection 101** [Online], available URL: https://datafarm-cybersecurity.medium.com/nosql-injection-101-e453d9856545, 2023 (March, 29); Kaori Takase, **SQLi : SQL Injection คืออะไร อธิบายช่องโหว่และการป้องกัน SQL Injection** [Online], available URL: https://kixoqxq59.medium.com/sqli-sql-injection-คืออะไร-อธิบายช่องโหว่และการป้องกัน-sql-injection-173113d91cdc, 2021 (June, 9).

กรองข้อมูลที่ต้องการจากฐานข้อมูลที่มีข้อมูลจำนวนมาก (Query) ซึ่ง NoSQL ไม่มีวากยสัมพันธ์และไวยกรณ์ที่เป็นกลางหรือแบบสำเร็จซึ่งรูปแบบของการกรองข้อมูลที่ต้องการจากฐานข้อมูลที่มีข้อมูลจำนวนมากนั้นขึ้นอยู่กับชนิดของฐานข้อมูลที่ใช้และภาษาที่ใช้เขียนของตัวเว็บ (Application Programing Interface: API) นั้น ซึ่งหมายความว่า การกรองข้อมูลที่ต้องการจากฐานข้อมูลที่มีข้อมูลจำนวนมากจะมีความหลากหลายไม่ได้ขึ้นอยู่ที่ฐานข้อมูลอย่างเดียว แต่ขึ้นอยู่กับภาษาที่ใช้เขียนด้วย เช่น Python PHP Node.js เป็นต้น หรือตัวของเฟรมเวิร์ก (framework) เช่น สปริงเฟรมเวิร์ก Spring Framework เป็นต้น

5) การเขียนสคริปต์ข้ามไซต์ (Cross Site Scripting: XSS) เกิดขึ้นเมื่ออาชญากรไซเบอร์ใช้จับตาดูเว็บไซต์ต่าง ๆ ที่มีจุดบกพร่องของระบบรักษาความปลอดภัย โดยแฮกเกอร์จะทำการส่งโค้ดคำสั่งเข้าไปในหน้าเว็บของผู้ใช้งานผ่านทางอีเมล์ เว็บบอร์ด เป็นต้น โดยหลอกให้ผู้ใช้กรอกข้อมูลสำคัญ เช่น ชื่อผู้ใช้งานและรหัสผ่าน เป็นต้น แล้วส่งกลับมาให้แฮกเกอร์ เกิดการเผยแพร่ข้อมูลส่วนบุคคลให้กับอาชญากรรายดังกล่าว เมื่อแฮกเกอร์ได้ข้อมูลนั้นก็จะทำการสวมรอยด้วยการใช้ข้อมูลของผู้ใช้ล็อกอินเข้าไปยังเว็บไซต์ต่าง ๆ ซึ่งก่อให้เกิดความเสียหายต่อผู้ใช้งานเป็นอย่างมาก

6) บอทเน็ต (Botnet) มาจากคำว่า Robot และ Network ใช้เรียกเครือข่ายเครื่องคอมพิวเตอร์ที่ถูกแฮกเกอร์ควบคุมเพื่อวัตถุประสงค์บางอย่าง เช่น นำไปใช้โจมตีเครือข่ายคอมพิวเตอร์อื่น สาเหตุที่กลายเป็นบอทเน็ต ส่วนมากมักเกิดจากการติดมัลแวร์ที่ปล่อยไปตามช่องทางต่าง ๆ เช่น อีเมล เว็บไซต์ รวมถึงโซเชียลมีเดีย เมื่อเปิดช่องทางให้แฮกเกอร์สามารถควบคุม หรือนำไปสร้างการจราจร (Traffic) ได้จากระยะไกล เช่น มัลแวร์ประเภท RAT (Remote Access Trojan) โดยเครื่องคอมพิวเตอร์ที่ถูกควบคุมจะเรียกว่า Zombie

7) โจมตีแบบดักกลางทาง (Man-in-the-middle attack) คือ การที่บุคคลภายนอกปลอมเป็นคนกลางเข้ามาแทรกสัญญาณในระหว่างที่มีการแลกเปลี่ยนข้อมูลในเน็ตเวิร์ค การโจมตีในรูปแบบนี้มักถูกใช้เพื่อขโมยข้อมูลเกี่ยวกับการเงิน และข้อมูลละเอียดอ่อนอื่น ๆ

8) ภัยคุกคามจากภายใน (Insider threat) เป็นภัยที่มาจากบุคคลภายในองค์กรที่ตั้งใจมุ่งประสงค์ร้ายต่อระบบความปลอดภัยขององค์กร โดยใช้อำนาจหน้าที่ หรือสวมรอยอำนาจหน้าที่เพื่อเข้าถึงระบบคอมพิวเตอร์ และทำให้ระบบการป้องกันภัยคุกคามอ่อนแอลง

9) การโจมตีของภัยคุกคามขั้นสูง (Advanced Persistent Threat: APT)[15] เป็นชุดของการโจมตีทางไซเบอร์ที่มีเป้าหมาย ซับซ้อน และยาวนาน เพื่อเข้าถึงระบบใช้เทคนิคการสอดแนม

---

[15]Amit Sharma and others, “Advanced Persistent Threats (APT): Evolution, anatomy, attribution and countermeasures,” **Journal of Ambient Intelligence and Humanized Computing** 14, 7 (2023): 9355-9381.

การค้นหาช่องโหว่ภายในระบบเพื่อเข้าถึงข้อมูลสำคัญ และการขโมยข้อมูลจากองค์กรหรือรัฐบาล ซึ่งแตกต่างจากการโจมตีทางไซเบอร์แบบดั้งเดิมที่มักมุ่งเน้นไปที่การสร้างความเสียหายแบบชั่วคราว หรือการปล้นทรัพยากรทางไซเบอร์ นอกจากนี้ การโจมตีนี้ในบางกรณียังได้รับการสนับสนุนจากรัฐบาล[16] โดยกลุ่ม APT ภาครัฐที่มักมุ่งเป้าหมายไปยังการเมือง เศรษฐกิจ หรือความมั่นคงของรัฐบาล องค์กรธุรกิจ หรือบุคคลสำคัญในต่างประเทศ

โดยที่รูปแบบการโจมตีทางไซเบอร์ที่กล่าวมาข้างต้นเป็นตัวอย่างเบื้องต้นเท่านั้น เนื่องจากทุกวันความเจริญก้าวหน้าทางเทคโนโลยียังไม่ถึงขีดจำกัด จึงอาจจะเกิดรูปแบบการโจมตีทางไซเบอร์ที่มีความสลับซับซ้อนเพิ่มมากขึ้นกว่านี้ที่ต่อยอดมาจากรูปแบบต่าง ๆ ที่กล่าวมาข้างต้น

3. หลักกฎหมายระหว่างประเทศ

ปัจจุบันยังไม่มีกฎหมายระหว่างประเทศฉบับเดียวที่มีเนื้อหาครอบคลุมในการกำกับการสู้รบทางไซเบอร์[17] แม้จะมีความพยายามในทางวิชาการในการผลักดันให้มีตราสารเป็นการเฉพาะขึ้นมาก็ตาม[18] ดังนั้น กฎหมายระหว่างประเทศที่มีอยู่ในปัจจุบันที่นำมาปรับใช้กับการสู้รบทางไซเบอร์ได้ คือ กฎหมายมนุษยธรรมระหว่างประเทศ แม้ว่าผู้ร่างมีเจตนาที่จะปรับใช้กับการขัดกันทางอาวุธแบบดั้งเดิม และคงมิได้คาดหมายว่าจะมาปรับใช้ควบคุมการสู้รบทางไซเบอร์กับคู่มือทาลลินน์ (Tallinn Manuals) จัดทำโดยศูนย์ความเป็นเลิศเพื่อความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ของเนโต้ (NATO Cooperative Cyber Defence Center of Excellence: CCDCOE) เมืองทาลลินน์ ประเทศเอสโตเนีย อย่างไรก็ตาม คู่มือทาลลินน์นั้น ไม่ได้มีสภาพบังคับเช่นเดียวกับกฎหมายระหว่างประเทศ อีกทั้ง คู่มือดังกล่าวยังอยู่ในระหว่างการปรับปรุง จึงยังมีความไม่ชัดเจนในทางปฏิบัติ

3.1 กฎหมายมนุษยธรรมระหว่างประเทศ

กฎหมายมนุษยธรรมระหว่างประเทศ (International Humanitarian Law: IHL) ที่เรียกกันในอีกชื่อว่า กฎหมายการขัดกันทางอาวุธ (Law of Armed Conflict) หรือ กฎหมาย

---

[16]Timo Steffens, **Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage** (Heidelberg: Springer Vieweg Berlin, 2020), pp. 3-21.

[17]Daniel B. Garrie, "Cyberwarfare, What Are the Rules?," **Journal of Law & Cyber Warfare** 1 (2012): 1-7.

[18]Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," **Philosophy & Technology** 31, 3 (2018): 379-407.

ภาคสงคราม (Law of War) คือ กฎหมายระหว่างประเทศที่ใช้บังคับเกี่ยวกับวิธีการทำสงคราม และการปฏิบัติต่อพลรบและพลเรือนอย่างมีมนุษยธรรมในระหว่างการทำสงคราม (*Jus in bello*)[19] ซึ่งถือว่ากฎหมายมนุษยธรรมระหว่างประเทศเป็นกฎหมายระหว่างประเทศที่มีสถานภาพเป็นกฎหมายพิเศษ (*lex specialis*)[20] และกฎหมายสิทธิมนุษยชนระหว่างประเทศ (International Human Rights Law) เป็นกฎหมายที่ใช้ในทุกสถานการณ์ โดยกฎหมายทั้งสองกลุ่มนี้มีการทับซ้อนกันอยู่บ้างตามแนวคำวินิจฉัยต่าง ๆ ของศาลยุติธรรมระหว่างประเทศ (International Court of Justice)[21] โดยความสัมพันธ์ของกฎหมายมนุษยธรรมระหว่างประเทศกับกฎหมายสิทธิมนุษยชนระหว่างประเทศต่างก็มีวัตถุประสงค์ร่วมกันในการเคารพและปกป้อง (Respect and Protect) ศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) และปัจเจกชน (Individual)[22]

โดยการขัดกันทางอาวุธนั้นแบ่งได้เป็น 2 กรณี คือ การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ (International Armed Conflict) และการขัดกันทางอาวุธ ที่ไม่มีลักษณะระหว่างประเทศ (Non-International Armed Conflict)[23] โดยมีหลักการพื้นฐานที่สำคัญ 5 หลัก[24] ได้แก่

---

[19]International Committee of the Red Cross, **What are jus ad bellum and jus in bello?** [Online], available URL: https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0%EF%BB%BF, 2015 (January, 22).

[20]Cordula Droege, "The Interplay between International Humanitarian law and International Human Rights Law in Situation of Armed Conflict," **Israel Law Review** 40, 2 (2007): 310-355.

[21]E.g. Legality of the Use by a State of Nuclear Weapons in armed Conflict, Advisory Opinion, I.C.J. Reports 1996, p. 226, para. 25; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 136, para. 106; Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168, paras. 216-221.

[22]Daniel Moeckli, Sangeeta Shah, and Sandesh Sivakumaran, **International Human Rights Law**, 3rd ed., (Oxford: Oxford University Press, 2018), p. 503.

[23]Office of the High Commissioner of United Nations Human Rights, **International legal Protection of Human Rights in Armed Conflict** [Online], available URL: https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict.pdf, 2011 (May, 12).

[24]Redcross, **Introduction to International Humanitarian Law** [Online], available URL: https://www.redcross.org.uk/about-us/what-we-do/protecting-people-in-armed-conflict/international-humanitarian-law, (n.d.).

1) หลักการแบ่งแยกพลรบกับพลเรือน (Principle of Distinction) ห้ามผู้มีส่วนร่วมโจมตีพลเรือนในสถานการณ์การขัดกันทางอาวุธ โดยมีการแยกแยะระหว่างพลเรือนกับทหาร

2) หลักความได้สัดส่วน (Proportionality) ห้ามผู้มีส่วนร่วมทำการโจมตีซึ่งคาดว่าจะทำให้เกิดการสูญเสียชีวิต ความสูญเสีย ความเสียหายต่อวัตถุพลเรือน แก่พลเรือนในสถานการณ์การขัดกันทางอาวุธ เพื่อความได้เปรียบทางการทหารโดยตรง และเป็นรูปธรรม

3) หลักการเตือนภัยก่อนการโจมตี (Precaution) ให้ผู้มีส่วนร่วมดำเนินการเพื่อหลีกเลี่ยงการเกิดความเสียหาย และความสูญเสียแก่พลเรือนในสถานการณ์การขัดกันทางอาวุธ

4) หลักความจำเป็นทางทหาร (Military Necessity) ผู้มีส่วนร่วมในสถานการณ์การขัดกันทางอาวุธจะสามารถใช้อาวุธเท่าที่ไม่ขัดกับกฎหมายมนุษยธรรมระหว่างประเทศ และให้ใช้อาวุธเพื่อให้บรรลุ “วัตถุประสงค์ทหารที่มีการรองรับทางกฎหมาย (Legitimate Military Purpose)” โดยมีผลกระทบต่อชีวิตและทรัพยากรของพลเรือนน้อยที่สุด

5) หลักมนุษยธรรม (Humanity) ห้ามให้มีการสูญเสีย และ/หรือความเสียหายเพื่อบรรลุวัตถุประสงค์ทางการทหารที่มีการรองรับทางกฎหมาย (Legitimate Military Purpose)

ในบริบทของการปฏิบัติการทางไซเบอร์ แนวคิดของการโจมตีทางไซเบอร์ จึงหมายถึงปฏิบัติการทางไซเบอร์ที่สามารถคาดหมายได้อย่างสมเหตุสมผลว่าจะส่งผลให้ความเสียหาย ทั้งทางตรงและทางอ้อม รวมถึงมีการปิดใช้งาน หรือการทำลายวัตถุ เช่น โครงสร้างพื้นฐาน และข้อมูลที่อาจเป็นไปได้ หรือการบาดเจ็บหรือเสียชีวิตของบุคคล แต่จะไม่รวมถึงการดำเนินการทางไซเบอร์ที่มุ่งเป้าไปที่การเข้าถึงเฉพาะข้อมูลโดยไม่ได้รับอนุญาต โดยเมื่อนำหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศมาพิจารณา อาจพิจารณาได้ว่า พลเรือนจะต้องไม่ถูกโจมตีหรือวัตถุพลเรือนคือวัตถุทั้งหมดที่ไม่ใช่วัตถุประสงค์ทางทหาร ซึ่งรวมถึงโครงสร้างพื้นฐานของพลเรือน บริการสาธารณะ บริษัท ทรัพย์สินส่วนตัว และข้อมูลพลเรือนเพื่อหลีกเลี่ยงหรือลดผลกระทบที่ปฏิบัติการอาจมีต่อพลเรือน ตัวอย่างเช่น หากมีการตั้งเป้าที่จะขัดขวางบริการไฟฟ้าหรือรถไฟที่กองกำลังทหารใช้ ต้องพิจารณาหลีกเลี่ยงหรือลดผลกระทบที่การปฏิบัติงานเช่นนั้นอาจมีต่อพลเรือนให้เหลือน้อยที่สุด รวมถึงผลกระทบจากเหตุที่ไม่ได้ตั้งใจก่อนที่จะดำเนินการด้วย อีกทั้ง ยังเป็นการเพื่อลดผลกระทบที่ปฏิบัติการอาจมีต่อพลเรือน และหยุดการโจมตีหากความเสียหายต่อพลเรือนที่จะมีความเสี่ยงที่มากเกินไปหากสามารถเข้าถึงระบบปฏิบัติการได้

3.1.1 อาวุธทางไซเบอร์

ตามกฎหมายมนุษยธรรมระหว่างประเทศแล้ว ไม่ได้มีนิยามของอาวุธบัญญัติเอาไว้ แต่ความหมายโดยทั่วไปจึงหมายถึง รายการอุปกรณ์ใด ๆ ที่รัฐหรือกลุ่มติดอาวุธจัดหาให้กับกองทัพหรือสมาชิกของตน เพื่อว่าในการขัดกันด้วยอาวุธ พวกเขาสามารถดำเนินการอย่างรุนแรงต่อศัตรูและใช้งานภายในขอบเขตที่สมเหตุสมผลโดยความจำเป็นทางทหารและกฎเกณฑ์ของกฎหมาย

มนุษยธรรมระหว่างประเทศ ซึ่งกฎหมายมนุษยธรรมระหว่างประเทศมีหลักการและกฎพื้นฐานที่ควบคุมการเลือกอาวุธ และห้ามหรือจำกัดการใช้อาวุธบางชนิด หรือมีเป็นตราสารเฉพาะ[25] เช่น ลูกปืนที่มีน้ำหนักน้อยกว่า 400 กรัม[26] กระสุนที่ขยายหรือแผ่ในร่างกายมนุษย์[27] ยาพิษและอาวุธอาบยาพิษ[28] อาวุธเคมี[29] อาวุธชีวภาพ[30] อาวุธที่เศษชิ้นส่วนไม่สามารถตรวจจับในร่างกายได้ด้วยรังสีเอกซ์[31] อาวุธเพลิง[32] อาวุธเลเซอร์ที่ทำให้ตาบอด[33] ทุ่นระเบิดสังหารบุคคล[34] เศษซากระเบิดจากสงคราม[35] และระเบิดลูกปราย[36] เป็นต้น

---

[25]International Committee of the Red Cross, **Weapons** [Online], available URL: https://www.icrc.org/en/document/weapons, 2011 (November, 30).

[26]1868 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight (Declaration of Saint Petersburg).

[27]1899 Declaration concerning the prohibition of the use of bullets which can easily expand or change their form inside the human body such as bullets with a hard covering which does not completely cover the core, or containing indentations.

[28]1907 Convention respecting the Laws and Customs of War on Land.

[29]1925 Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (Geneva Protocol 1925); 1993Convention on the prohibition of chemical weapons.

[30]1925 Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (Geneva Protocol 1925); 1972 Convention on the prohibition of biological weapons.

[31]1980 Protocol I on Non-Detectable Fragments to the Convention on Certain Conventional Weapons.

[32]1980 Protocol III on Incendiary Weapons to the Convention on Certain Conventional Weapons.

[33]1995 Protocol IV on Blinding Laser Weapons to the Convention on Certain Conventional Weapons.

[34]1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (Ottawa Treaty).

[35]1995 Protocol V on Explosive Remnants of War to the Convention on Certain Conventional Weapons.

[36]2008 Convention on Cluster Munitions.

นอกจากนี้ ความหมายของอาวุธทางไซเบอร์ที่ยังไม่มีนิยามในทางกฎหมายระหว่างประเทศ หากแต่ความหมายโดยทั่วไป คือ ซอฟต์แวร์ที่เป็นอันตราย (Malicious Software Entities) นำไปใช้เพื่อก่อให้เกิดอันตรายต่อเครือข่ายและระบบคอมพิวเตอร์ของฝ่ายตรงข้าม ซอฟต์แวร์เหล่านี้คุกคามต่อการทำงานของระบบดิจิทัลที่ทำให้เกิดวงจรการสื่อสารและการแลกเปลี่ยนทั่วโลก โดยอาจส่งผลกระทบอย่างมีนัยสำคัญต่อระเบียบทางสังคม เศรษฐกิจ และการเมือง[37] ดังนั้น ความหมายของอาวุธทางไซเบอร์แตกต่างไปจากอาวุธอย่างดั้งเดิม

ในการพิจารณาว่าการใช้อาวุธทางไซเบอร์ (Cyberweapons) ในสงครามนั้นยังไม่มีหลักเกณฑ์ในเรื่องดังกล่าวเป็นการเฉพาะ จึงให้พิจารณาจากหลักเกณฑ์การใช้อาวุธอย่างดั้งเดิม โดยต้องมีการคำนึงว่า

1) อาวุธนั้นชอบด้วยกฎหมายหรือไม่ กล่าวคือ มีกฎหมายห้ามการใช้อาวุธดังกล่าวหรือไม่ โดยอนุสัญญาว่าด้วยการห้ามหรือการจำกัดการใช้อาวุธตามแบบฉบับบางประเภทซึ่งอาจถือว่าเป็นอันตรายมากเกินไปหรือมีผลกระทบตามอำเภอใจ ค.ศ. 1980 (1980 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects: CCW)[38] มีหลักการทั่วไปอันเป็นแนวทางปฏิบัติในทางกฎหมายระหว่างประเทศ ได้แก่ (1) ห้ามการใช้อาวุธที่ไม่จำกัดผลลัพธ์ (use of weapons that are indiscriminate) และ (2) ห้ามการใช้อาวุธที่ทำให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น (use of weapons of a nature to cause unnecessary suffering or superfluous injury)[39] นอกจากนี้ ยังมิได้มีการจำแนกอาวุธต้องห้ามออกเป็นประเภทต่าง ๆ เป็นการเฉพาะ[40] เช่น อาวุธใดก็ตามที่มีผลเบื้องต้นทำให้บุคคลได้รับบาดเจ็บจากสะเก็ดระเบิดซึ่งหากอยู่ในร่างกายจะไม่สามารถตรวจพบได้ด้วยการเอ็กซ์เรย์ อาวุธเพลิง อาวุธแสงเลเซอร์ ที่ออกแบบมาโดยเฉพาะเพื่อทำให้ตาบอดถาวร (blinding laser weapons) เป็นต้น

---

[37]Tim Stevens, “Cyberweapons: power and the governance of the invisible,” **International Politics** 55, 3-4 (2018): 482-502.

[38]United Nations, **Treaty Series**, vol. 1342, p. 137.

[39]International Committee of the Red Cross, **1980 Convention on Certain Conventional Weapons** [Online], available URL: https://www.icrc.org/en/document/1980-convention-certain-conventional-weapons#.VKkpP2SG-rY, 2021 (May, 21).

[40]1980 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I); 1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II).

2) การใช้อาวุธนั้นชอบด้วยกฎหมายหรือไม่ เช่น หากใช้อาวุธนอกเหนือจากอาวุธต้องห้ามถูกนำไปใช้ในเหตุการณ์ที่ได้รับการกำหนดว่าชอบด้วยกฎหมาย ตามมาตรา 36 ของพิธีสารเพิ่มเติม ฉบับที่ 1 ค.ศ. 1977 ของอนุสัญญาเจนีวา ค.ศ. 1949 (1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)) กำหนดให้รัฐภาคีพิจารณา วิธีการหรือปัจจัยใหม่ในการทำสงครามว่าเป็นการต้องห้ามตามกฎหมายระหว่างประเทศหรือไม่ ซึ่งในทางปฏิบัตินั้น ยังไม่มีการกำหนดหลักเกณฑ์ที่ชัดเจนในประเด็นดังกล่าว เนื่องจากขึ้นอยู่กับการตีความของแต่ละรัฐภาคี อย่างไรก็ตาม การตีความดังกล่าวมีหลักควรพิจารณาว่าอาวุธ วิธีการหรือปัจจัยดังกล่าว (1) ต้องห้ามหรือถูกจำกัดตามพิธีสารหรืออนุสัญญาระหว่างประเทศใดเป็นการเฉพาะหรือไม่ (2) ต้องห้ามตามพิธีสาร อนุสัญญาระหว่างประเทศที่มีสถานะผูกพันรัฐภาคีหรือกฎหมายจารีตประเพณีระหว่างประเทศใดตามหลักกฎหมายมนุษยธรรมหรือไม่ และ (3) ขัดต่อหลักมนุษยธรรม (Principle of Humanity) หรือข้อกำหนดแห่งมโนธรรมของสาธารณะโดยรวม (the dictates of public conscience) หรือไม่ นอกจากนี้ รัฐภาคีควรพิจารณาการใช้โดยปกติหรือที่คาดหมายได้จากอาวุธ วิธีการหรือปัจจัยนั้น และบริบทในการใช้อาวุธ วิธีการหรือปัจจัยดังกล่าวประกอบด้วย[41]

การใช้อาวุธทางไซเบอร์ครั้งแรก ๆ ที่ปรากฏเป็นข่าวใหญ่ คือ ในปี ค.ศ. 2010 เชื่อว่าสตักซ์เน็ต (Stuxnet)[42] ถูกปล่อยโดยสหรัฐอเมริกาและอิสราเอล[43] ซึ่งเป็นหนอนคอมพิวเตอร์เพื่อโจมตีโรงงานนิวเคลียร์ของอิหร่าน จึงทำให้สตักซ์เน็ตถือเป็นอาวุธทางไซเบอร์หลักตัวแรก ๆ ที่ถูกนำมาโจมตี และเชื่อว่าอิหร่านได้ใช้อาวุธทางไซเบอร์เพื่อตอบโต้ไปยังสถาบันการเงินชั้นนำของสหรัฐอเมริกา รวมถึงตลาดหลักทรัพย์นิวยอร์ก (New York Stock Exchange)[44]

---

[41]Vincent Boulanin, **Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon System** [Online], available URL: https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1501.pdf, 2015 (November, 2).

[42]Kim Zetter, **Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon** (New York: Crown Publishers, 2014), pp. 52-68.

[43]David E. Sanger, **Obama Order Sped Up Wave of Cyberattacks Against Iran** [Online], available URL: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html, 2012 (June, 1).

[44]Sue Halpern, **How Cyber Weapons Are Changing the Landscape of Modern Warfare** [Online], available URL: https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare, 2019 (July, 18); Saeid Reza Ameli, Hassan Hosseini, and Farnaz Noori, "Militarization of Cyberspace, Changing Aspects of War in the 21st Century: The Case of Stuxnet Against Iran," **Iranian Review of Foreign Affairs** 10, 29 (2019): 99-136.

จากพลวัตรของอาวุธทางไซเบอร์ที่แตกต่างไปอย่างมากจากอาวุธตามกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ จึงมีข้อเสนอทางวิชาการถึงความจำเป็นที่จะต้องสร้างกฎหมายเฉพาะขึ้นมากำกับอาวุธทางไซเบอร์ โดยกฎหมายที่มีอยู่ไม่ทันสมัยต่อการปรับใช้กับอาวุธทางไซเบอร์[45] ซึ่งบทบาทของสังคมระหว่างประเทศจึงต้องมาร่วมกันสร้างหลักกฎหมาย มิใช่ต้องรอคอยให้มหาอำนาจเป็นผู้กำหนดกติกาเพียงฝ่ายเดียว[46] ซึ่งเป็นแนวทางปกติของกฎหมายมนุษยธรรมระหว่างประเทศที่จะมีพัฒนาเป็นตราสารเฉพาะสำหรับอาวุธแต่ละชนิด

3.1.2 การใช้กำลัง

ในความสัมพันธ์ระหว่างประเทศสมาชิกทั้งปวงจักต้องละเว้นการคุกคามหรือการใช้กำลัง[47] ซึ่งเป็นหลักการอันเป็นพื้นฐานของกฎบัตรสหประชาชาติ[48] โดยคำว่าการใช้กำลัง (Use of force) โดยทั่วไป หมายความถึง การใช้กำลังทางกายภาพ อย่างไรก็ตาม การตีความถ้อยคำดังกล่าวนั้นอาจมีการเปลี่ยนแปลงได้ตามยุคสมัยในกรณีที่อนุสัญญาที่นั้นมีผลบังคับใช้มาเป็นเวลานานแล้ว[49] เนื่องจากการโจมตีทางไซเบอร์นั้น อาจไม่ได้ทำให้เกิดความเสียหายทางกายภาพมาก จึงต้องมีหลักการพิจารณาโดยคำนึงถึงผลที่เกิดขึ้นจากการโจมตีทางไซเบอร์อาจทำให้เกิดความเสียหายทางกายภาพหรือกระทบต่อความมั่นคงของประเทศนั้น ๆ[50]

---

[45]Nicholas Tsagourias and Giacomo Biggio, “The regulation of cyber weapons,” In: Eric P.J. Myjer and Thilo Marauhn eds., **Research Handbook on International Arms Control Law** (United Kingdom: Edward Elgar, 2022), pp. 440-455; Dennis Broeders and others, “Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards lines in the sand?,” **Journal of Cyber Policy** 7, 1 (2022): 97-135; Jonathan F. Lancelot, “Cyber-Diplomacy: Cyberwarfare and the rules of engagement,” **Journal of Cyber Security Technology** 4, 4 (2020): 240-254.

[46]Lucas Kello, “Cyber Legalism: Why it fails and what to do,” **Journal of Cybersecurity** 7, 1 (2021). 1-9.

[47]Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, paras. 47-48.

[48]Charter of United Nations, Article 2(4).

[49]Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2009, p. 213.

[50]Marco Roscini, **Cyber Operations and the Use of Force in International Law** (Oxford: Oxford University Press 2014), p. 55.

ทั้งนี้ ยังมีความเห็นที่หลากหลายของนานาประเทศในเรื่องดังกล่าวว่าจะถือว่าการโจมตีทางไซเบอร์ที่ไม่มีผลในทางกายภาพเลยจะถือเป็นการใช้กำลังตามกฎบัตรสหประชาชาติได้หรือไม่ โดยรัฐภาคีหลายประเทศเห็นควรให้มีการขยายขอบเขตของการใช้คำว่า “การใช้กำลัง” ให้ครอบคลุมถึงการโจมตีทางไซเบอร์ โดยในมุมมองของรัฐภาคีนั้นสามารถแบ่งออกเป็น 2 แนวคิด ดังนี้

1) กลุ่มแรกมีแนวคิดว่า ควรมีการประเมินนั้นถือว่าการโจมตีทางไซเบอร์จะเป็นการใช้กำลังหรือไม่จากผลลัพธ์ (Effect-based Approach) กล่าวคือ การกระทำนั้นก่อให้เกิดหรือน่าจะก่อให้เกิดความเสียหายทางกายภาพต่อทรัพย์สิน การสูญเสียชีวิต หรือการบาดเจ็บของบุคคล[51] ซึ่งเป็นการประเมินที่เป็นรูปธรรมที่สุดและถูกบรรจุไว้ในคู่มือทาลลินน์ด้วย[52] ในการพิจารณาว่าการกระทำโดยรัฐนั้นเป็นการใช้กำลังหรือไม่นั้น ให้พิจารณาปัจจัย 7 ประการ[53] ดังต่อไปนี้

(1) ความรุนแรง โดยหากมีการก่อให้เกิดความเสียหายทางกายภาพ ให้ถือว่าเป็นการใช้กำลัง

(2) ความฉับพลัน โดยหากการกระทำของรัฐนั้นทำให้เกิดผลทันที ให้ถือว่าเป็นการใช้กำลัง

(3) ผลโดยตรงจากการกระทำ โดยหากผลลัพธ์เป็นผลที่ชัดเจนจากการกระทำโดยรัฐ ให้ถือว่าเป็นการใช้กำลัง

(4) การเข้าถึง โดยหากการกระทำของรัฐเข้าถึงหรือล่วงล้ำอำนาจอธิปไตยของรัฐอื่น ให้ถือว่าเป็นการใช้กำลัง

(5) การประเมินความเสียหาย โดยหากมีความเสียหายจากการกระทำของรัฐให้ถือว่าเป็นการใช้กำลัง

(6) ความต้องห้ามตามกฎหมาย โดยหากการกระทำดังกล่าวนั้นมีกฎหมายใดห้ามไว้ ให้ถือว่าเป็นการใช้กำลัง และ

(7) การรับผิดชอบ โดยหากรัฐภาคีมีความเกี่ยวข้องกับการกระทำดังกล่าวให้ถือว่าเป็นการใช้กำลัง

นอกจากการประเมินโจมตีทางไซเบอร์จากผลลัพธ์แล้วนั้น ในการพิจารณาถึงการโจมตีทางไซเบอร์นั้น ยังมีหลักการสำหรับการประเมินโจมตีทางไซเบอร์จากเป้าหมาย (Target-based Approach) ซึ่งให้ถือว่ามีการใช้กำลังเมื่อมีการมุ่งเป้าไปยังโครงสร้างสำคัญของประเทศ และ

---

[51]Ibid., p. 53.

[52]Huseyin Kuru, “Prohibition of Use of Force and Cyber Operations as Force,” **Journal of Learning and Teaching in Digital Age** 2, 2 (2017): 49-53.

[53]Ibid., p. 53.

การประเมินโจมตีทางไซเบอร์จากวิธีการ (Instrument-based Approach) ซึ่งให้ถือว่ามีการใช้กำลังเมื่อการโจมตีทางไซเบอร์มีความคล้ายคลึงกับอาวุธแบบดั้งเดิม อย่างไรก็ตาม แนวคิดทั้งสองยังขาดความชัดเจนในทางปฏิบัติ เมื่อเทียบกับแนวคิดการประเมินโจมตีทางไซเบอร์จากผลลัพธ์[54] โดยแนวคิดนี้เป็นแนวคิดที่ได้รับความนิยมมากที่สุดในหมู่ประเทศต่าง ๆ[55] เช่น ประเทศแคนาดาถือว่าการกระทำทางไซเบอร์ที่อาจเทียบได้กับการคุกคามหรือการใช้กำลังโดยมีขนาดและผลกระทบที่เทียบเคียงได้กับผลจากสถานการณ์อื่น ๆ เป็นการใช้กำลัง[56] และสหราชอาณาจักรถือว่าการกระทำใดเป็นการใช้กำลังเมื่อการกระทำนั้นมีหรือจะมีผลเหมือนหรือคล้ายคลึงกันกับการกระทำโดยทางกายภาพ[57] เป็นต้น

2) กลุ่มที่สองมีแนวคิดว่า การโจมตีทางไซเบอร์ที่ถือเป็นการใช้กำลังหากเข้าองค์ประกอบตามที่แต่ละรัฐภาคีกำหนดโดยไม่จำเป็นต้องมีความเสียหายทางกายภาพเพียงประการเดียว เช่น ประเทศเนเธอร์แลนด์นำความเสียหายทางด้านอื่นนอกเหนือจากการเสียหายทางกายภาพมาพิจารณาด้วย เช่น ความเสียหายทางเศรษฐกิจและความเสียหายทางการเงิน เป็นต้น[58] และประเทศนอร์เวย์ถือว่าการกระทำที่เป็นอุปสรรคต่อการดำเนินการของโครงสร้างของรัฐหรือโทรคมนาคมก็อาจเป็นการใช้กำลังได้เช่นกัน[59]

---

[54]Ibid., p. 48.

[55]Marco Roscini, op. cit., pp. 46-47.

[56]Government of Canada, **International Law applicable in cyberspace** [Online], available URL: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, 2022 (April, 22).

[57]Commonwealth & Development Office, **Application of international law to states' conduct in cyberspace: UK statement** [Online], available URL: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement, 2021 (June, 3).

[58]Dutch Ministry of Foreign Affairs, **Letter to the parliament on the international legal order in cyberspace** [Online], available URL: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, 2019 (July, 5).

[59]United Nations, **Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States** [Online], available URL: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf, 2021 (July, 13).

เมื่อการโจมตีทางไซเบอร์ครอบคลุมถึงเทคนิค เป้าหมาย และผลที่ตามมา ซึ่งส่งผลต่อเศรษฐกิจ สังคม การเมือง และโครงสร้างพื้นฐาน ซึ่งผลพวงของจากสู้รบทางไซเบอร์จำเป็นต้องมีกลยุทธ์เพื่อบรรเทาอันตรายที่เกิดจากการโจมตีดังกล่าว โดยเน้นความสำคัญของการรวบรวมข้อมูลเชิงลึกจากกลยุทธ์เหล่านี้ และขัดขวางภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต[60]

3.1.3 การป้องกันตนเอง

การใช้กำลังที่ชอบด้วยกฎหมายที่สอดคล้องกับเป้าหมายของสหประชาชาติ[61] มี 2 ประการ คือ การใช้สิทธิป้องกันตนเอง (Self-Defense) ตามข้อ 51 ของกฎบัตรสหประชาชาติ กับการใช้มาตรการรักษาสันติภาพร่วมกันภายใต้หมวด 7 ของกฎบัตรสหประชาชาติ โดยประเด็นที่เกี่ยวข้องกับการสู้รบทางไซเบอร์ที่รัฐสามารถใช้สิทธิของตนตอบโต้ได้นั้น น่าจะเหมาะกับการปรับใช้สิทธิป้องกันตนเองตามข้อ 51 ของกฎบัตรสหประชาชาติ ซึ่งถือว่าเป็นหลักการที่ตกผลึกมาจากหลักกฎหมายจารีตประเพณีระหว่างประเทศ[62]

โดยการที่จะก่อให้เกิดสิทธิป้องกันตนเองได้นั้น รัฐต้องถูกการโจมตีด้วยอาวุธ (Armed Attack) กล่าวคือ มีการโจมตีด้วยอาวุธข้ามแดนระหว่างประเทศ และกลุ่มผู้ใช้อาวุธโจมตีรัฐอื่นอย่างรุนแรงเทียบเท่ากับการโจมตีด้วยอาวุธโดยกลุ่มทหารปกติ คือ ขนาดและผลของการโจมตีรุนแรงมากกว่าขนาดหรือลักษณะที่เป็นเพียงการพิพาทเล็กน้อยตามแนวชายแดนเท่านั้น จึงหมายความว่าสิทธิในการป้องกันตนเองเกิดขึ้นหลังจากที่มีการโจมตีด้วยกำลังอาวุธบังเกิด (Occurs) ขึ้นแล้ว ซึ่งเป็นไปตามหลักกฎหมายจารีตประเพณีระหว่างประเทศที่ปรากฏในกรณีพิพาทคาโรไลน์ (Caroline)[63] แต่การช่วยเหลือผู้ก่อความไม่สงบโดยการสนับสนุนอาวุธหรือการสนับสนุนรูปแบบอื่น ๆ อาจเป็นการข่มขู่คุกคามอันตรายหรือการใช้กำลัง (Threat or Use of Force) หรืออาจก่อให้เกิดการเข้าแทรกแซงของรัฐอื่น แต่ไม่ใช่การโจมตีด้วยอาวุธ แม้ว่าจะไม่ก่อให้เกิดสิทธิในการใช้กำลังป้องกัน

---

[60]Ridge A. Atrews, “Cyberwarfare: Threats, Security, Attacks, and Impact,” **Journal of Information Warfare** 19, 4 (2020): 17-28.

[61]Charter of United Nations, Article 2(4).

[62]Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14.

[63]Craig Forcese, **Destroying the Caroline: The Frontier Raid that Reshaped the Right to War** (Toronto: Irwin Law, 2018); Michael Wood, “The Caroline Incident-1837,” In: Tom Ruys, Olivier Corten, Alexandra Hofer eds., **The Use of Force in International Law: A Case-Based Approach** (Oxford: Oxford University Press, 2018), pp. 5-14; Edward Jr. Collins and Martin A. Rogoff, “The Caroline Incident of 1837, the McLeod Affair of 1840-1841, and the Development of International Law,” **American Review of Canadian Studies** 20, 1 (1990): 81-107.

ตนเอง แต่รัฐที่กระทำการดังกล่าวก็จะถือว่าละเมิดต่อการที่รัฐภาคีต้องละเว้นที่จะไม่ใช้การข่มขู่คุกคามอันตรายหรือการใช้กำลังตามมาตรา 2(4) ของกฎบัตรสหประชาชาติ

โดยที่หลักการของการป้องกันตนเองที่สำคัญมี 2 ประการ[64] คือ

1) หลักการได้สัดส่วน (Proportionality) ไม่มีการระบุว่ามาตรการตอบสนองต่อการป้องกันตนเองที่เหมาะสมต่อการป้องกันตนเองอย่างแน่ชัดว่าเป็นเช่นไร โดยที่การได้สัดส่วนไม่ได้หมายความว่ารัฐต้องกระทำเหมือนกัน แต่เป็นการกระทำเพื่อให้ยุติการโจมตี และป้องกันมิให้มีการโจมตีต่อรัฐ ดังนั้น จึงต้องมีการพิจารณาตามแต่ละกรณี

2) ความจำเป็น (Necessary) การป้องกันตนเองจะกระทำเพียงเท่าที่จำเป็นเท่านั้น และต้องมีการพิสูจน์ให้สามารถเห็นได้ด้วยว่ากระทำการเพียงเท่าที่จำเป็นเท่านั้น[65]

จากเหตุความไม่สงบในโลกท่ามกลางการก่อการร้าย จึงมีการใช้กำลังการโจมตีโดยกลุ่มที่ไม่ใช่รัฐ (Non-State Actor) แต่ทว่าสิทธิของรัฐที่จะใช้การป้องกันตนเองได้นั้น ภายใต้กฎบัตรสหประชาชาติบังคับใช้เฉพาะระหว่างรัฐเท่านั้น จุดเปลี่ยนจึงเกิดขึ้นหลังจากเหตุการณ์ 9/11 คณะมนตรีความมั่นคงแห่งสหประชาชาติจึงเรียกประชุมด่วน และออกมติคณะมนตรีความมั่นคงที่ 1368 (2001) Threats to international peace and security caused by terrorist acts (12 September 2001) ให้สิทธิป้องกันตนเองต่อการก่อการร้ายและภัยคุกคามต่อสันติภาพ และความมั่นคงระหว่างประเทศ ผลจากมตินี้จึงสะท้อนว่า สหประชาชาติให้รัฐภาคีสามารถใช้สิทธิป้องกันตนเองตามมาตรา 51 ได้ โดยไม่จำเป็นจะต้องจำกัดแต่เพียงเฉพาะการกระทำที่มาจากรัฐเท่านั้น โดยจะต้องเป็นการก่อการร้ายที่มีแหล่งกำเนิดมาจากนอกรัฐ[66]

การใช้สิทธิป้องกันตนเองตามกฎบัตรสหประชาชาติ ในทางทฤษฎีรัฐที่ใช้สิทธิจะต้องรายงานให้คณะมนตรีความมั่นคงรับทราบ และรัฐนั้นก็ควรจะหยุดการกระทำ แต่ทว่าในทางปฏิบัติ รัฐก็มักจะอ้างว่าการดำเนินการของคณะมนตรีความมั่นคงไม่เพียงพอ รัฐนั้นจึงยังคงต้องดำเนินการใช้สิทธิป้องกันตนเองต่อไป รวมไปถึงรัฐก็ถือว่าการรายงานให้คณะมนตรีความมั่นคงทราบนั้นไม่ใช่องค์ประกอบของการป้องกันตนเองตามหลักกฎหมายจารีตประเพณีระหว่างประเทศแต่อย่างใด[67]

---

[64]Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168.

[65]Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, p. 161.

[66]Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 136.

[67]Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14.

การที่รัฐถูกการโจมตีทางไซเบอร์แล้วจึงใช้สิทธิของตนตอบโต้ด้วยการป้องกันตนเองนั้น ความเสียหายที่เกิดขึ้นจะมากมายเกินกว่าที่จะเยียวยาให้กลับคืนมาได้หรือไม่ ซึ่งหากเทียบกับอันตรายจากการใช้อาวุธนิวเคลียร์เพื่อป้องกันตนเองแล้วก็ยังคงไม่มีความชัดเจนในกฎหมายระหว่างประเทศในปัจจุบัน ถึงการใช้อาวุธนิวเคลียร์เพื่อป้องกันตนเองที่ชอบด้วยกฎหมาย[68] การสู้รบทางไซเบอร์ที่รัฐจะต้องยอมให้ถูกโจมตีก่อนจึงจะสามารถใช้สิทธิในการป้องกันตนเองจะทันต่อการหยุดยั้งหายนะทางไซเบอร์ได้หรือไม่

3.1.4 อาชญากรรมสงคราม

ศาลอาญาระหว่างประเทศ (International Criminal Court: ICC) เป็นศาลระหว่างประเทศถาวรที่จัดตั้งขึ้นตามธรรมนูญกรุงโรมของศาลอาญาระหว่างประเทศ (Rome Statute of the International Criminal Court) ค.ศ. 1998 เพื่อตรวจสอบ ดำเนินคดี และพิจารณาคดีบุคคลที่ถูกกล่าวหาว่าก่ออาชญากรรมร้ายแรงที่สุดที่ประชาคมระหว่างประเทศกังวล[69] โดยที่ศาลมีเขตอำนาจใน 5 ฐานความผิด ได้แก่ อาชญากรรมการฆ่าล้างเผ่าพันธุ์ (Genocide)[70] อาชญากรรมต่อมนุษยชาติ (Crimes Against Humanity)[71] อาชญากรรมสงคราม (War Crimes)[72] อาชญากรรมการรุกราน (Crime of Aggression)[73] และความผิดต่อกระบวนการยุติธรรม (Offences against the Administration of Justice)[74]

อาชญากรสงคราม รวมถึงการละเมิดอนุสัญญาเจนีวาอย่างร้ายแรง การละเมิดกฎหมายและจารีตประเพณีอย่างร้ายแรงอื่น ๆ ที่บังคับใช้ในการสู้รบระหว่างประเทศ และในความขัดแย้งที่ไม่มีลักษณะระหว่างประเทศที่ระบุไว้ในธรรมนูญกรุงโรม เมื่อมีการกระทำโดยเป็นส่วนหนึ่งของแผน หรือนโยบายหรือในวงกว้าง ดังนั้น เมื่อมีการก่ออาชญากรรมตามแผนการหรือนโยบายหรือเป็นส่วนหนึ่งของอาชญากรรมขนาดใหญ่ โดยหากกิจกรรมทางไซเบอร์เป็นไปตามเงื่อนไขดังกล่าวจึงจะถือว่าเป็นอาชญากรรมสงคราม[75]

---

[68]Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226.

[69]Rome Statute of the International Criminal Court, Preamble.

[70]Ibid., Article 6.

[71]Ibid., Article 7.

[72]Ibid., Article 8.

[73]Ibid., Article 8 bis.

[74]Ibid., Article 70.

[75]Victor Tsilonis, “Cyber Warfare: International Criminal Law in the Digital Era,” In **The**

3.2 คู่มือทาลลินน์

ปี ค.ศ. 2007 ช่วงปลายเดือนเมษายนถึงพฤษภาคม ประเทศเอสโตเนียตัดสินใจย้ายรูปปั้นทหารโซเวียตนิรนามออกไปจากที่ตั้งเดิมซึ่งอยู่ใจกลางกรุงทาล์ลินน์ เมืองหลวงของประเทศเอสโตเนีย โดยรูปปั้นนี้เป็นอนุสรณ์สงครามโลกครั้งที่ 2 ที่รำลึกถึงทหารโซเวียต การย้ายรูปปั้นนี้นำมาซึ่งความโกรธเคืองในหมู่ประชากรเชื้อสายรัสเซียที่อาศัยอยู่ในเอสโตเนียนำมาสู่การประท้วงที่กรุงทาลลินน์ จนเกิดเป็นจลาจล ต่อมาเหตุการณ์นี้ถูกเรียกว่า คืนบรอนซ์ (Pronksiöö) เนื่องจากรูปปั้นดังกล่าวมีชื่อเรียกอย่างไม่เป็นทางการว่ารูปปั้นทหารบรอนซ์ นอกจากนี้ การย้ายรูปปั้นทหารบรอนซ์ยังทำให้รัสเซียไม่พอใจ ในช่วงเวลาเดียวกันนี้ ประเทศเอสโตเนียเผชิญกับการโจมตีทางไซเบอร์ต่อเนื่องนาน 3 สัปดาห์ เว็บไซต์ของหน่วยงานภาครัฐ และเอกชน โดยเฉพาะอย่างยิ่งธนาคาร ถูกโจมตี ส่งผลให้การให้บริการภาครัฐของเอสโตเนียซึ่งพึ่งพาการทำงานบนพื้นที่ไซเบอร์ไม่สามารถดำเนินการได้ ความเสียหายทางธุรกิจก็เกิดขึ้นเนื่องจากต้องระงับการทำธุรกรรมทางการเงิน ซึ่งรูปแบบของการโจมตีทางไซเบอร์นี้เป็นการโจมตีแบบ DoS[76]

จากเหตุการณ์ข้างต้น ศูนย์ความเป็นเลิศด้านการป้องกันทางไซเบอร์ของสหกรณ์ของนาโต (NATO Cooperative Cyber Defence Center of Excellence: CCDCOE) จึงจัดตั้งคณะทำงานผู้เชี่ยวชาญระหว่างประเทศ (International Group of Experts: IGE) ขึ้นมาทำความเข้าใจเกี่ยวกับความสัมพันธ์ระหว่างกฎหมายระหว่างประเทศกับไซเบอร์[77] โดยขอบเขตอำนาจหน้าที่นั้น ผลงานของคณะทำงานจะไม่มีผลผูกมัดทางกฎหมาย ซึ่งผลงานที่ได้รับการยอมรับอย่างกว้างขวาง

Jurisdiction of the International Criminal Court (Switzerland: Springer Cham, 2024), pp. 315-339; Sarah Zarmsky, "Is International Criminal Law Ready to Accommodate Online Harm?: Challenges and Opportunities," **Journal of International Criminal Justice** 22, 1 (2024): 169-184; Simon McKenzie, "Cyber Operations against Civilian Data: Revisiting War Crimes against Protected Objects and Property in the Rome Statute," **Journal of International Criminal Justice** 19, 5 (November 2021): 1165-1192.

[76]Mark Landler and John Markoff, **Digital Fears Emerge After Data Siege in Estonia** [Online], available URL: https://www.nytimes.com/2007/05/29/technology/29estonia.html, 2007 (May, 29); Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," **Journal of Strategic Security** 4, 2 (2011): 49-60.

[77]Matthew Hoisington, Regulating Cyber Operations Through International Law: In, Out or Against the Box? In: Ludovica Glorioso and Mariarosaria Taddeo eds., **Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative** (Switzerland: Springer Cham, 2016), pp. 87-98.

คือ คู่มือทาลลินน์ (Tallinn Manual) ซึ่งเป็นผลงานทางวิชาการที่มีการพัฒนามากที่สุดที่พยายามจะจัดระเบียบหลักการต่าง ๆ ทางกฎหมายระหว่างประเทศ โดยหลักการแล้วคู่มือนี้จะเน้นที่กิจกรรมทางไซเบอร์ในความขัดแย้งทางอาวุธในบริบทของกฎหมาย[78] สะท้อนถึงกฎหมายที่มีผลผูกพัน (*lex lata*) ที่ใช้กับการปฏิบัติงานทางไซเบอร์และหลีกเลี่ยงการแสดงกฎหมายที่ยังไม่มีผลผูกพัน (*lex ferenda*) โดยฉบับปัจจุบัน คือ คู่มือทาลลินน์ 2.0 ว่าด้วยกฎหมายระหว่างประเทศที่ใช้กับการปฏิบัติการทางไซเบอร์ (The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations) ฉบับปี ค.ศ. 2017[79] โดยมีเนื้อหาเพิ่มจากคู่มือทาลลินน์ฉบับปี ค.ศ. 2013[80] คือ จากเดิมที่เน้นการปฏิบัติการต่อภัยคุกคามที่มีผลกระทบร้ายแรง ซึ่งอาจนำไปสู่การละเมิดการใช้กำลังทหารตามกฎหมายระหว่างประเทศ รวมถึงสิทธิของแต่ประเทศในการป้องกันตนเอง ฉบับใหม่เพิ่มบทวิเคราะห์ทางกฎหมายในการใช้อำนาจรัฐจัดการกับภัยคุกคามทางไซเบอร์ที่มีโดยทั่วไป รวมทั้งการใช้กำลังทหารจัดการ/รับมือเท่าที่จำเป็น จึงมีการอธิบายทางกฎหมายระหว่างประเทศที่เกี่ยวข้องกับไซเบอร์ทั้งในยามสงบและสงคราม เนื้อหาของคู่มือทาลลินน์ 2.0 จึงมีความครอบคลุมประเด็นต่าง ๆ ทางกฎหมายระหว่างประเทศ ดังนี้ อำนาจอธิปไตย (Sovereignty) การตรวจสอบ (Due Diligence) เขตอำนาจรัฐ (Jurisdiction) กฎหมายความรับผิดชอบระหว่างประเทศ (Law of International Responsibility) การดำเนินการทางไซเบอร์ที่ไม่ได้รับการควบคุมโดยตรง (Cyber Operations Not Per Se Regulated) กฎหมายสิทธิมนุษยชนระหว่างประเทศ (International Human Rights Law) กฎหมายการทูตและกงสุล (Diplomatic and Consular Law) กฎหมายทะเล (Law of the Sea) กฎหมายอากาศ (Air Law) กฎหมายอวกาศ (Space Law) กฎหมายโทรคมนาคมระหว่างประเทศ (International Telecommunications Law) การระงับข้อพิพาทอย่างสันติ (Peaceful Settlement of Disputes) และการห้ามการแทรกแซง (Prohibition of Intervention)

แต่อย่างไรก็ตาม คู่มือทาลลินน์ 3.0 อยู่ในระหว่างดำเนินการ ซึ่งเปิดรับฟังข้อคิดเห็นและพยายามที่จะแก้ไขเนื้อหาที่มีอยู่เพื่อตอบสนองต่อการพัฒนาใหม่ ๆ รวมทั้งแนะนำการอภิปรายในหัวข้อใหม่ ๆ ที่เกี่ยวข้องกับกิจกรรมของรัฐในพื้นที่ไซเบอร์ รวมถึงกระบวนการปรับปรุงเกี่ยวกับ

---

[78]Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," **Georgetown Journal of International Law** 48, 3 (Spring 2017): 735-778.

[79]Michael N. Schmitt ed., **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, 2nd Ed., (New York: Cambridge University Press, 2017).

[80]Michael N. Schmitt ed., **Tallinn Manual on the International Law Applicable to Cyber Warfare**, (New York: Cambridge University Press, 2013).

ผู้เชี่ยวชาญด้านกฎหมายระหว่างประเทศที่หลากหลาย[81] จึงสะท้อนให้เห็นได้ว่ากฎหมายระหว่างประเทศในปัจจุบันที่ใช้ในการกำกับปฏิบัติการทางไซเบอร์นั้นยังคงไม่ยุติ มีพลวัตรในการพัฒนาหลักกฎหมายที่เกี่ยวข้องให้ก้าวหน้าขึ้นอย่างต่อเนื่องและรวดเร็ว

4. การโจมตีทางไซเบอร์ในประเทศไทย

ตั้งแต่ปี พ.ศ. 2561 - 2566 จากที่ปรากฏเป็นข่าวว่าการโจมตีทางไซเบอร์ที่เกิดขึ้นกับองค์กรภาครัฐและเอกชนของไทยมีเหตุการณ์ที่สำคัญ 9 ครั้ง[82]

ครั้งที่ 1 เดือนเมษายน พ.ศ. 2561 ฐานข้อมูลลูกค้า TrueMove H ที่ลงทะเบียนซิมผ่านช่องทาง iTrueMart หลุดบนคลาวด์เก็บข้อมูล Amazon Web Service S3 ทำให้บุคคลภายนอกสามารถเข้าถึงข้อมูลรูปสำเนาบัตรประชาชน ใบขับขี่ และพาสปอร์ตของลูกค้า

ครั้งที่ 2 เดือนกันยายน พ.ศ. 2563 คอมพิวเตอร์ของโรงพยาบาลสระบุรีถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่ ส่งผลให้ทางโรงพยาบาลไม่สามารถดึงข้อมูลคนไข้เพื่อทำการรักษาได้ เป็นการโจมตีทางไซเบอร์ที่สร้างผลกระทบต่อการให้บริการของโรงพยาบาลสระบุรีอย่างมาก แม้ที่ผ่านมาทางโรงพยาบาลสระบุรีมีการแบ็กอัปข้อมูลไว้ตลอดเวลา แต่ไวรัสได้เจาะเข้าไปในฐานข้อมูลในช่วงนั้นพอดี

ครั้งที่ 3 เดือนมกราคม พ.ศ. 2564 เมื่อบริษัทในกลุ่ม Jasmine International ซึ่งเป็นบริษัทแม่ของ 3BB ผู้ให้บริการอินเทอร์เน็ต และช่อง MONO ออกประกาศชี้แจงข้อมูลกรณีแฮกเกอร์โจรกรรมข้อมูลส่วนบุคคลของลูกค้า พร้อมเรียกร้องให้ชำระค่าไถ่กว่า 550,000 เหรียญดอลลาร์สหรัฐเพื่อแลกเปลี่ยนกับข้อมูลดังกล่าว แต่ Jasmine หลีกเลี่ยงการชำระค่าไถ่ แฮกเกอร์จึงโต้ตอบด้วยการแฮกข้อมูลเพิ่มเติม โดยหลังเกิดเหตุ Jasmine ได้เปิดหน้าเว็บไซต์ให้ลูกค้า 3BB และช่อง MONO ตรวจสอบได้ด้วยตัวเอง อีกทั้งยืนยันว่า ข้อมูลส่วนบุคคลที่รั่วไหลไม่เกี่ยวกับข้อมูลทางการเงินหรือบัตรเครดิต พร้อมจะเร่งเพิ่มมาตรการป้องกันการโจมตีทางไซเบอร์ให้หนาแน่นมากยิ่งขึ้น

ครั้งที่ 4 เดือนสิงหาคม พ.ศ. 2564 สายการบิน Bangkok Airways ได้ออกประกาศว่าถูกโจมตีทางไซเบอร์ด้วย Lockbit Ransomware ทำให้ระบบสารสนเทศของบริษัทฯ อาจถูกเข้าถึงจากผู้ไม่หวังดี ซึ่งหลังเกิดเหตุทางบริษัทฯ ได้ดำเนินการสืบสวนเพื่อระบุว่ามีข้อมูลส่วนไหนบน Database ที่ได้รับความเสียหาย รวมถึงผู้โดยสารที่ได้รับผลกระทบ พร้อมกันนี้ได้เร่งปรับปรุงการป้องกันการโจมตีทางไซเบอร์ให้มีความรัดกุมมากยิ่งขึ้นกว่าเดิมด้วย

---

[81]The NATO Cooperative Cyber Defence Centre of Excellence, **The Tallinn Manual** [Online], available URL: https://ccdcoe.org/research/tallinn-manual, 2012 (September, 20).

[82]Sosecure, **สรุป 9 เหตุการณ์การโจมตีทางไซเบอร์ครั้งใหญ่ในไทย** [Online], available URL: https://www.sosecure.co.th/2024/04/29/cyber-attack, 2567 (เมษายน, 29).

ครั้งที่ 5 เดือนกันยายน พ.ศ. 2564 หลังสถาบันโรคไตภูมิราชนครินทร์ตรวจพบว่า ระบบข้อมูลของโรงพยาบาลถูกบล็อก และมีความพยายามเจาะข้อมูลส่วนตัว เช่น ข้อมูลการฟอกไตของคนไข้ ผลเอกซเรย์ และประวัติการรักษาของคนไข้ เป็นต้น โดยคาดว่าผู้ก่อเหตุเจาะระบบด้วยวิธีการควบคุมระยะไกลจากภายนอกโรงพยาบาล

ครั้งที่ 6 เดือนกันยายน พ.ศ. 2564 ผู้ใช้ THJAX ประกาศขายข้อมูลส่วนบุคคลโดยอ้างว่ามาจากเว็บไซต์ CP Freshmart จากนั้นไม่นานทาง CP Freshmart ออกแถลงการณ์ยืนยันว่าข้อมูลลูกค้าถูกแฮกจริง แต่ยืนยันว่าข้อมูลที่หลุดออกไปมีเพียงชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ และอีเมล แต่ไม่มีข้อมูลบัตรเครดิตหรือข้อมูลด้านการเงิน ทั้งนี้ได้ชี้แจงเพิ่มเติมว่า การโจมตีทางไซเบอร์ครั้งนี้ไม่มีผลกระทบต่อการดำเนินธุรกิจและระบบความปลอดภัยด้านอื่น ๆ พร้อมขอให้ลูกค้าระมัดระวังการหลอกลวงทางโทรศัพท์ และการหลอกลวงทางอีเมล (Phishing) ที่อาจเกิดขึ้นได้จากการนำข้อมูลไปใช้ต่อ และย้ำว่าไม่มีนโยบายติดต่อลูกค้าเพื่อขอข้อมูลทางด้านการเงิน

ครั้งที่ 7 เดือนตุลาคม พ.ศ. 2564 เซ็นทรัล เรสตอรองส์ กรุ๊ป (Central Restaurant Group: CRG) ได้ออกหนังสือยืนยันว่ามีแฮกเกอร์ได้เข้าโจมตีระบบสารสนเทศของเซ็นทรัล เรสตอรองส์ กรุ๊ป จริง โดยการโจมตีทางไซเบอร์ครั้งนี้แฮกเกอร์ได้ข้อมูลบางส่วนของลูกค้าไป แต่ข้อมูลสำคัญเกี่ยวกับการซื้อสินค้า ข้อมูลบัตรเครดิต และธุรกรรมทางการเงินยังอยู่ในสถานะที่ปลอดภัย

ครั้งที่ 8 เดือนกุมภาพันธ์ พ.ศ. 2565 ระบบการคัดเลือกกลางบุคคลเข้าศึกษาในสถาบันอุดมศึกษา (Thai University Central Admission System: TCAS) ยืนยันว่ามีข้อมูลส่วนตัวบางส่วนของนักเรียนปี 2564 ที่ยื่นเพื่อรับการคัดเลือกเข้าศึกษาต่อ รอบ 3 Admission 1 รั่วไหลจากเว็บไซต์ mytcas.com จำนวนกว่า 23,000 รายการ โดยข้อมูลชื่อ-นามสกุล เลขประจำตัวประชาชน โปรแกรมที่สมัครและรอบที่สมัครถูกวางขายในเว็บมืด

ครั้งที่ 9 เดือนมีนาคม พ.ศ. 2566 แฮกเกอร์ชื่อ 9Near ประกาศขายข้อมูลบนเว็บไซต์แห่งหนึ่งระบุว่าเป็นข้อมูลและรายชื่อคนไทย 55 ล้านคน โดยมีรายละเอียดตั้งแต่ชื่อและนามสกุล ที่อยู่ วันเกิด เลขบัตรประชาชน เบอร์โทรศัพท์ที่เป็นเบอร์ใช้งานจริงและลงทะเบียนไว้กับหน่วยงานรัฐ ถือเป็นข่าวการโจมตีทางไซเบอร์ที่สร้างผลกระทบต่อความเชื่อมั่นของประชาชนไม่น้อยเลยทีเดียว

จากข่าวการโจมตีสถาบันการเงิน ภาคธุรกิจต่าง ๆ หรือหน่วยงาน ภาครัฐในข้างต้น จะเห็นได้ว่าประเทศไทยเป็นหนึ่งในเป้าหมายการโจมตีทางไซเบอร์ในรูปแบบของมัลแวร์เรียกค่าไถ่ และการโจรกรรมข้อมูล ซึ่งหลังเกิดเหตุหน่วยงานที่เกี่ยวข้องต่างเร่งปรับปรุงมาตรการป้องกันการโจมตีทางไซเบอร์ เพื่อให้พร้อมรับมือและป้องกันตนเองจากภัยที่อาจเกิดขึ้น เพื่อไม่ให้ตกเป็นเหยื่อของมิจฉาชีพซ้ำสอง ทั้งนี้ แม้เหตุการณ์ทั้ง 9 นั้น จะไม่มีเหตุการณ์ใดที่ถือได้ว่าเป็นสู้รบทางไซเบอร์และเป็นเพียงแค่โจมตีทางไซเบอร์เท่านั้น เหตุการณ์ดังกล่าวเป็นตัวอย่างให้เห็นถึงความเสียหายเชิงเศรษฐกิจ ความเชื่อมั่นต่อระบบการป้องกันและมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

เมื่อพิจารณารูปแบบการโจมตีทางไซเบอร์ที่เกิดขึ้นแล้ว เห็นว่ามักมาในรูปแบบของการใช้มัลแวร์เรียกค่าไถ่ และการโจรกรรมข้อมูลโดยการเจาะระบบข้อมูลหรือวิธีการอื่นใดด้วยมิชอบเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลเป็นไปตามองค์ประกอบภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มาตรา 60 วรรคสอง (2) และ/หรือมาตรา 60 วรรคสอง (3)(ข) เนื่องจากเป็นภัยคุกคามทางไซเบอร์ที่มุ่งเพื่อโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศและความสงบเรียบร้อยของประชาชนเสียหาย เช่น โรงพยาบาลหรือสถานพยาบาล บริษัทด้านโทรคมนาคม หรือหน่วยงานรัฐอื่น ๆ เป็นต้น ซึ่งยังไม่ครอบคลุมถึงกรณีการโจมตีทางไซเบอร์เนื่องจากการโจมตีไปยังโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง 8 ด้าน การโจมตีดังกล่าวจึงเป็นเพียงแค่การโจมตีทางไซเบอร์ นอกจากนี้ เหตุการณ์ดังกล่าวยังอาจทับซ้อนกับความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อีกด้วย โดยในปัจจุบันนั้น ประเทศไทยยังไม่มีแนวทางของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่วางความเห็นอย่างชัดเจนตามหลักเกณฑ์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562

5. กองบัญชาการไซเบอร์ (Cyber Command)

จากสถานการณ์ความรุนแรงของภัยคุกคาม และการโจมตีทางไซเบอร์ นับวันจะทวีความเข้มข้นและความรุนแรงเพิ่มขึ้นตามลำดับและส่งผลกระทบต่อความมั่นคงของประเทศ ทั้งด้านการเมือง เศรษฐกิจ สังคมจิตวิทยา และการทหาร หลายประเทศได้มีความตระหนัก และมีการตื่นตัวในการเตรียมความพร้อมเพื่อรับมือกับภัยคุกคาม และการโจมตีดังกล่าวโดยเริ่มปรับหลักนิยมทางทหารใหม่ด้วยการเพิ่มสมรภูมิการรบที่ 5 คือ ไซเบอร์โดเมน ให้เทียบเท่ากับสมรภูมิรบที่มีอยู่เดิม คือ บก ทะเล อากาศ และอวกาศ ดังนั้น การกำหนดให้ไซเบอร์เป็นอีกหนึ่งสมรภูมิแห่งการสู้รบนั้น เพื่อที่จะได้จัดตั้งกองกำลังที่รับผิดชอบในการรบในสมรภูมินี้

5.1 สหรัฐอเมริกา

ก่อตั้งกองบัญชาการไซเบอร์ของสหรัฐอเมริกา (United States Cyber Command: USCYBERCOM)[83] เป็นศูนย์บัญชาการรบร่วมที่รับผิดชอบเกี่ยวกับการปฏิบัติการทางทหารในไซเบอร์โดเมนทั้งหมด มีสถานะเป็นกองบัญชาการรบร่วมระดับรอง (Sub-unified command) ขึ้นตรงกับกองบัญชาการด้านยุทธศาสตร์ (US STRATCOM) หน่วยบัญชาการไซเบอร์ตั้งอยู่ในฐานทัพฟอร์ทมีด

[83]U.S. Cyber Command, **Our History** [Online], available URL: https://www.cybercom.mil/About/History. (n.d.)

(Fort Meade) ณ มลรัฐแมร์รี่แลนด์ (Maryland) หน้าที่หลักของกองบัญชาการไซเบอร์นี้ คือ การปกป้องระบบเครือข่ายที่ทหารเป็นผู้รับผิดชอบ ในขณะที่ระบบเครือข่ายของรัฐบาลฝ่ายพลเรือนนั้น จะเป็นหน้าที่ของกระทรวงความมั่นคงแห่งมาตุภูมิของสหรัฐอเมริกา (United States Department of Homeland Security) ซึ่งสหรัฐอเมริกาเป็นหนึ่งในตัวอย่างของประเทศที่มีความพร้อมและโดดเด่นในการก่อตั้งกองทัพไซเบอร์

5.2 สหราชอาณาจักร

ก่อตั้งกองกำลังไซเบอร์แห่งชาติ (National Cyber Force: NCF)[84] ภายใต้การควบคุมโดยหน่วยงานข่าวกรองของสหราชอาณาจักร (Government Communications Headquarters: GCHQ) กับกระทรวงกลาโหม กองกำลังไซเบอร์แห่งชาติตั้งอยู่ที่หมู่บ้านแซมเลสเบอรี (Samlesbury) ในเซาธ์ ริบเบิล (South Ribble) แลงคาเชียร์ (Lancashire) มีจุดมุ่งหมายเพื่อรวมกิจกรรมทางไซเบอร์ที่อันตรายต่อสหราชอาณาจักร ซึ่งไม่ได้มีหน้าที่เพียงปฏิบัติงานด้านข่าวสารเท่านั้น แต่ยังทำหน้าที่ต่อต้านภัยคุกคามจากผู้ก่อการร้าย รวมถึงป้องกันประเทศจากศัตรูในเงามืดด้วย สำหรับภารกิจสำคัญที่ NCF จะเข้าร่วม คือ เจาะเข้าแนวป้องกันทางอากาศของศัตรูเพื่อปกป้องการปฏิบัติงานของกองทัพอากาศของสหราชอาณาจักร (Royal Air Force: RAF) ในการขัดขวาง และทำลายระบบการสื่อสารที่อาจเป็นภัยคุกคามความมั่นคงแห่งสหราชอาณาจักร รวมถึงสนับสนุนงานภาคสนามทางไซเบอร์ด้วย[85] ซึ่งมีข้อสังเกตการปฏิบัติการของกองกำลังไซเบอร์ถือเป็นความลับระดับประเทศ จึงทำให้รายชื่อของบุคลากรและรายละเอียดโครงสร้าง รวมถึงรายละเอียดของการปฏิบัติงานของ NCF ไม่ค่อยเปิดเผยต่อสาธารณะ[86] ซึ่งอาจจะเป็นประเพณีของหน่วยงานด้านความลับ และความมั่นคงที่ชื่อของเอ็ม (M)[87] ก็ยังคงเป็นความลับ

---

[84]National Cyber Force, **National Cyber Force Explainer** [Online], available URL: https://assets.publishing.service.gov.uk/media/61b9f526d3bf7f05522e302e/Force_Explainer_20211213_FINAL__1_.pdf, 2021 (December, 13).

[85]National Cyber Force, **The National Cyber Force: Responsible Cyber Power in Practice** [Online], available URL: https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf, 2023 (April, 3).

[86]Emma Woollacott, **UK's National Cyber Force Reveals How It Works** [Online], available URL: https://www.forbes.com/sites/emmawoollacott/2023/04/04/uks-national-cyber-force-reveals-how-it-works/?sh=5eafcb6b29f5., 2023 (April, 4).

[87]"เอ็ม" เป็นรหัสเรียกตำแหน่งหัวหน้าหน่วยงานสืบราชการลับของสหราชอาณาจักรในนิยายชุดเจมส์ บอนด์ (James Bond) ประพันธ์โดยเอียน แลนแคสเตอร์ เฟลมมิง (Ian Lancaster Fleming).

5.3 ประเทศไทย

จากเดิมที่กองทัพแต่ละภาคส่วนก็จะมีหน่วยงานที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ แต่กลับสร้างความเคลือบแคลงใจให้แก่สังคม เนื่องจากความพยายามต่าง ๆ ของกองทัพมักจะถูกตั้งคำถามจากสังคม ไม่ว่าจะเป็นการพยายามจะผลักดันระบบอินเทอร์เน็ตในรูปแบบของเกตเวย์แห่งชาติ ซึ่งก็คือ Single Gateway เช่นเดียวกับประเทศจีนและเกาหลีเหนือ[88] หรือการมีปฏิบัติการข่าวสาร (Information Operation: IO)[89] ในสื่อสังคมออนไลน์ จนกลายเป็นประเด็นทางการเมืองแทนความมั่นคงไปแทน[90] และบดบังความตั้งใจในการดำเนินการจัดการกับภัยคุกคามทางไซเบอร์ของกองทัพไทย ซึ่งเป็นปัจจัยที่สำคัญต่อการดำเนินงานด้านความมั่นคงทางไซเบอร์ของกองทัพในอนาคต

จากการที่กองทัพไทยได้จัดส่งเจ้าหน้าที่ที่เกี่ยวข้องไปศึกษาดูงานหน่วยงานด้านไซเบอร์ของมิตรประเทศ เพื่อนำมาเป็นแนวทางในการพัฒนาขีดความสามารถด้านไซเบอร์ของกองทัพไทยมุ่งสู่การเป็นศูนย์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อความเป็นเลิศ (Cyber Security Academy) เพื่อการพัฒนาบุคลากรทางไซเบอร์ของประเทศโดยร่วมมือกับทุกกระทรวง ทบวง กรม สถาบันการศึกษา ภาคธุรกิจ เอกชน และหน่วยงานความมั่นคง โดยพัฒนาการล่าสุดกองทัพไทยมีนโยบายในการดำเนินงานด้านความมั่นคงทางไซเบอร์มีดังนี้[91]

---

[88]สาวตรี สุขศรี, **นโยบาย Single Internet Gateway เพื่อรัฐ เพื่อประชาชน หรือเพื่อใคร?** [Online], available URL: https://prachatai.com/journal/2015/10/61774, 2558 (ตุลาคม, 6).

[89]กองบรรณาธิการ, “การปฏิบัติการข่าวสารในยุคแห่งสงครามสารสนเทศ,” **วารสารสถาบันวิชาการป้องกันประเทศ** 7, 1 (2559): 9-15; ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, **เอกสารศึกษาเฉพาะกรณี “การสื่อสารทางยุทธศาสตร์ (Strategic Communication : SC) และการปฏิบัติการข่าวสาร (Information Operations : IO) ของกองทัพไทย : แนวทางการดำาเนินงานในอนาคต** (กรุงเทพมหานคร: ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, 2559).

[90]บีบีซี, **ไอโอ : คณะก้าวหน้าเปิดโปงข้อมูลเครือข่ายปฏิบัติการข่าวสารกองทัพ ด้านเอกชนแถลงโต้ชี้ข้อมูลบิดเบือน** [Online], available URL: https://www.bbc.com/thai/thailand-55145803, 2563 (ธันวาคม, 1); สปริงนิวส์, **IO #ทหารมีไว้ทำไม ที่มาและเรื่องราว ปฏิบัติการข่าวสารสร้างสรรค์!?** [Online], available URL: https://www.springnews.co.th/news/hot-issue/847064, 2567 (มกราคม, 19).

[91]กรุงเทพธุรกิจ, **‘สุทิน’ สั่งทุกเหล่าทัพตั้ง ‘กองบัญชาการไซเบอร์’ ต้านภัยคุกคามใหม่** [Online], available URL: https://www.bangkokbiznews.com/politics/1128462, 2567 (มิถุนายน, 15); ไทยรัฐออนไลน์, **“กองทัพ” รุกตั้งหน่วยไซเบอร์ทหาร รับภัยคุกคาม เริ่มผลิตนักรบ 1 ต.ค.นี้** [Online], available URL: https://www.thairath.co.th/news/local/bangkok/2787536, 2567 (พฤษภาคม, 22); ประชาไทย, **ก.กลาโหม เตรียมตั้งกองบัญชาการสงครามไซเบอร์** [Online], available URL: https://prachatai.com/journal/2024/05/109345, 2567 (พฤษภาคม, 25).

5.3.1 จัดตั้งหน่วยบัญชาการไซเบอร์ทหารมีเป้าหมายหลักให้เป็นศูนย์ความมั่นคงปลอดภัยทางไซเบอร์และเพื่อการพัฒนาบุคลากรทางไซเบอร์ของประเทศไทย และปรับโครงสร้างหน่วยไซเบอร์ภายใต้หน่วยปฏิบัติการดิจิทัล กองทัพบกเพิ่มกองสงครามอิเล็กทรอนิกส์ กองทัพเรือเพิ่มศูนย์ไซเบอร์กองทัพเรือ กองทัพอากาศปรับย้ายกองสงครามเครือข่ายไปอยู่ภายใต้ศูนย์ไซเบอร์กองทัพอากาศ และปรับศูนย์ไซเบอร์กองทัพอากาศไปอยู่ภายใต้กรมเทคโนโลยีสารสนเทศ และการสื่อสารทหารอากาศ เพื่อรองรับและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ทั้งในระดับกองทัพ และในระดับประเทศ หากเกิดเหตุการณ์สำคัญ กองทัพก็จะมีความสามารถในการเตรียมการจัดทีมรับผิดชอบระบบสาธารณูปโภคสำคัญของประเทศได้

5.3.2 ก่อตั้งโรงเรียนดิจิทัลโรงเรียนไซเบอร์ทหารเพื่อเป็นหน่วยสายวิทยาการด้านไซเบอร์ และเป็นแหล่งผลิตบุคลากรด้านไซเบอร์ให้แก่กองทัพ และหน่วยงานภายนอก โดยจะร่วมมือกับทุกหน่วยงานราชการ สถาบันการศึกษา และเอกชน รวมทั้งหน่วยงานความมั่นคงต่าง ๆ ของประเทศไทยมีเป้าหมาย เพื่อผลิตบุคลากรที่มีความชำนาญในด้านนี้ปีละประมาณ 300-500 นาย

5.3.3 การตั้งสถาบันป้องกันและตอบโต้สถานการณ์วิกฤตนานาชาติ (International Crisis Prevention and Response Academy: ICPRA) พร้อมรับมือปัญหาก่อการร้าย ก่อเหตุร้ายในประเทศ และการแก้ไขวิกฤตการณ์ระดับชาติ โดยยกระดับเป็นศูนย์ปฏิบัติการพิเศษร่วม (Joint Special Operations Command: JSOC)

หากเกิดสถานการณ์วิกฤตทางการเมืองในอนาคต หน่วยงานทางทหารที่กำลังจะตั้งขึ้นใหม่นั้น ต้องพึงระวังการกำหนดบทบาทที่ต้องดำเนินการเพื่อความมั่นคงปลอดภัยทางไซเบอร์ตลอดจนการป้องกันและตอบโต้สถานการณ์วิกฤตของชาติให้เป็นไปตามวัตถุประสงค์ของการจัดตั้งหน่วยงานดังกล่าวด้วย

6. กฎหมายเกี่ยวกับการสู้รบทางไซเบอร์ในประเทศไทย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 เป็นกฎหมายที่มีวัตถุประสงค์ เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้มีผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สมกช.) เป็นหน่วยงานรับผิดชอบตามพระราชบัญญัติดังกล่าว และประสานการปฏิบัติงานร่วมกัน และรับมือภัยทางไซเบอร์อย่างมีประสิทธิภาพ[92] แต่ความพร้อมในการรับมือภัยคุกคามที่เข้ามา

---

[92]กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. **เกี่ยวกับ สกมช. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม** [Online], available URL: https://www.mdes.go.th/mission/detail/2481, (ม.ป.ป.).

ในเขตแดนแห่งความมั่นคงปลอดภัยทางไซเบอร์ หรือการตอบโต้หรือตอบสนองต่อ “ภัยคุกคามทางไซเบอร์” หรือ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องในลักษณะเป็นเชิงสงครามนั้น[93] ยังขาดความชัดเจนในทางมาตรการตามกฎหมายและการกำหนดขั้นตอนดำเนินการทั้งทางภาครัฐ และเอกชนดังนี้

6.1 ขอบเขตของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562

ตามมาตรา 3 ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 นั้น “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง ทั้งนี้ หากพิจารณาถึงภัยคุกคามทางไซเบอร์ตาม NIST Cybersecurity Framework (NIST CSF)[94] โดยในปัจจุบัน คือ NIST CSF 2.0[95] นั้น หมายถึง

---

[93]พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562, มาตรา 3.

[94]เป็นกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่ถูกกำหนดโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (The National Institute of Standards and Technology: NIST) ภายใต้กระทรวงพาณิชย์ของสหรัฐอเมริกา เป็นหนึ่งในกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นที่นิยมใช้อย่างมากในปัจจุบัน จึงไม่เพียงแค่องค์กรในสหรัฐ แต่เป็นที่แพร่หลายไปยังทุกภูมิภาคทั่วโลกรวมไปถึงประเทศไทย มาใช้เป็นแนวทางและกรอบการอ้างอิงในการสร้างความปลอดภัยให้กับระบบการทำงานของหน่วยงานต่าง ๆ ที่จำเป็นของรัฐและเอกชนที่มีระบบการทำงานพื้นฐานอยู่บนเทคโนโลยีสารสนเทศเพื่อรับมือกับภัยคุกคามไซเบอร์ กรอบทำงานนี้นำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุดของการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับรวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว และเป็นระบบ. Dietmar P. F. Möller, “NIST Cybersecurity Framework and MITRE Cybersecurity Criteria,” In **Guide to Cybersecurity in Digital Transformation. Advances in Information Security** (Switzerland: Springer, Cham, 2023), pp. 231-271; Marion Toussaint, Sylvère Krima and Hervé Panetto, “Industry 4.0 Data Security: A cybersecurity frameworks review,” **Journal of Industrial Information Integration** 39 (March 2024): 100-604.

[95]The National Institute of Standards and Technology, **The NIST Cybersecurity Framework (CSF) 2.0** [Online], available URL: https://doi.org/10.6028/NIST.CSWP.29, 2024 (February, 26).

พฤติการณ์หรือสถานการณ์ที่อาจทำให้เกิดผลในด้านลบต่อการดำเนินงานขององค์กร (รวมถึงภารกิจ หน้าที่ ภาพลักษณ์ หรือชื่อเสียง) ทรัพย์สิน บุคคลขององค์กรนั้น หรือ องค์กรอื่น หรือของชาติผ่านทางระบบข้อมูลสารสนเทศที่มีการเข้าถึง ทำลาย เปิดเผย หรือดัดแปลงข้อมูล และ/หรือการปฏิเสธการให้บริการ[96] จะเห็นได้ว่านิยามตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 นั้นไม่ได้ระบุถึง “พฤติการณ์หรือสถานการณ์ที่อาจทำให้เกิดผลในด้านลบทางไซเบอร์” แต่กลับกล่าวถึงการกระทำโดยมีจุดมุ่งหมาย ซึ่งอาจทำให้เกิดความสับสนต่อเมื่อมีการบังคับใช้และตีความกฎหมายในมาตราที่เกี่ยวข้องได้ นอกจากนี้ ขอบเขตตามพระราชบัญญัติดังกล่าวอาจมีกรณีที่อาจทับซ้อนกับกรณีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ว่าจะเป็นคำนิยามของคำว่า “ภัยคุกคามทางไซเบอร์” ซึ่งอาจรวมถึงกรณีการใช้มัลแวร์หรือเวิร์มที่สร้างความเสียหายแก่ระบบคอมพิวเตอร์เกี่ยวกับความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ[97] กล่าวคือ แม้จะมีการกล่าวถึงบริบทของความมั่นคงในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 แต่การไม่ได้กล่าวถึงความมั่นคงของชาติอย่างชัดแจ้งอาจทำเกิดความสับสนได้เช่นกัน

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ได้กำหนดภัยคุกคามทางไซเบอร์นั้นแบ่งออกได้เป็น 3 ประเภท คือ

---

[96]Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

U.S. Department of Commerce and National Instituted of Standards and Technology, “**NIST Special Publication 800-30 Rev. 1 : Guide for Conducting Risk Assessments** [Online], available URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, 2012 (September, 20).

[97]พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560, มาตรา 12 วรรคแรก ถ้าการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 หรือมาตรา 11 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท และ มาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ.

(1) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่ส่งผลให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลง[98]

(2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศโดยมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้[99]

(3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ที่มีลักษณะ ดังต่อไปนี้ (ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศที่เป็นวงกว้างล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยา ตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ[100] (ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือ การสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง[101]

---

[98]เรื่องเดียวกัน, มาตรา 60 วรรคสอง (1).

[99]เรื่องเดียวกัน, มาตรา 60 วรรคสอง (2).

[100]เรื่องเดียวกัน, มาตรา 60 วรรคสอง (3)(ก).

[101]เรื่องเดียวกัน, มาตรา 60 วรรคสอง (3)(ข).

จากบทบัญญัติดังกล่าว สังเกตได้ว่า ความร้ายแรงของภัยคุกคามตั้งแต่มาตรา 60 วรรคสอง (1) จนถึง มาตรา 60 วรรคสอง (3)(ก) นั้นแปรเปลี่ยนไปตามความเสียหายของโครงสร้างพื้นฐานสำคัญของประเทศหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศซึ่งมีลักษณะของการประเมินภัยคุกคามทางไซเบอร์จากเป้าหมาย ซึ่งตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) “โครงสร้างพื้นฐานสำคัญ” หมายความถึง บรรดาหน่วยงาน หรือองค์กร หรือส่วนงานหนึ่งส่วนงานใด ของหน่วยงานหรือองค์กรซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงาน หรือองค์กร หรือส่วนงานของหน่วยงาน หรือองค์กรนั้นมีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน[102] ในขณะที่ “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายถึง คอมพิวเตอร์หรือระบบคอมพิวเตอร์ของหน่วยงานรัฐหรือเอกชนที่ใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความปลอดภัยเกี่ยวกับความมั่นคงของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างอันเป็นประโยชน์สาธารณะ[103] ซึ่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 กำหนดให้หน่วยงานด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิกส์ติก ด้านพลังงาน และสาธารณูปโภค ด้านสาธารณสุข และด้านอื่น ๆ ที่คณะกรรมการประกาศกำหนดเพิ่มเติม เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[104] จึงอาจกล่าวได้ว่า หากพื้นฐานสำคัญของประเทศหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้นั้นย่อมมีผลต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน ในขณะที่มาตรา 60 วรรคสอง (3)(ข) กล่าวถึงลักษณะผลกระทบจากการโจมตีทางไซเบอร์โดยไม่ได้คำนึงถึงโครงสร้างพื้นฐานสำคัญของประเทศหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศซึ่งมีลักษณะของการประเมินภัยคุกคามทางไซเบอร์จากผลลัพธ์ จะเห็นได้ว่า บทบัญญัติดังกล่าวมีความสอดคล้องกันทางหลักการ อีกทั้ง การนำโครงสร้างพื้นฐานสำคัญทางสารสนเทศมากำหนดความร้ายแรงของภัยคุกคามอาจทำให้ขาดความชัดเจนในทางปฏิบัติ เนื่องจากความรุนแรงของภัยคุกคามทางไซเบอร์ไม่ได้ขึ้นอยู่กับว่าองค์ใดถูกโจมตี หากแต่เป็นผลกระทบที่ตามมา นอกจากนี้ ผู้เขียนมีข้อสังเกตว่า มาตรา 60 วรรคสอง (2) และ มาตรา 60 วรรคสอง (3)(ข) มีถ้อยคำในทำนองเดียวกัน เช่น ถ้อยคำว่า

---

[102]ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) เล่ม 139 ตอนพิเศษ 288 ง ราชกิจจานุเบกษา 9 ธันวาคม 2565.

[103]พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562, มาตรา 3.

[104]เรื่องเดียวกัน, มาตรา 49 (1) – (8).

“ความมั่นคงของรัฐ” และ “ความสงบเรียบร้อยของประชาชน” เป็นต้น จึงอาจเกิดความไม่ชัดเจนเมื่อบังคับใช้กฎหมายดังกล่าวว่าในกรณีที่เกิดความเสียหายต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ให้ใช้มาตราใดและจะถือได้ว่ากรณีตามมาตรา 60 วรรคสอง (2) นั้น เป็นภัยคุกคามในระดับวิกฤติด้วยได้หรือไม่

6.2 การออกและใช้มาตรการเพื่อรักษาความมั่นคงทางไซเบอร์

ในส่วนของการปรับใช้มาตรการเพื่อรักษาความมั่นคงทางไซเบอร์นั้น มีข้อสังเกตว่ามีการนำถ้อยคำและหลักการจากพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 มาใช้กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 นี้ด้วย ดังจะเห็นจากการแบ่งประเภทของภัยคุกคามทางไซเบอร์ ซึ่งมีระดับไม่ร้ายแรง ระดับร้ายแรงเช่นเดียวกันกับพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 อย่างไรก็ตาม การนิยามของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 จะมุ่งเน้นความเสียหายที่เกิดต่อระบบคอมพิวเตอร์ของโครงสร้างพื้นฐานสำคัญหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ อีกทั้ง มีการเพิ่มภัยคุกคามทางไซเบอร์ในระดับวิกฤตเข้ามาด้วย ในขณะที่การนิยามของพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 จะเน้นไปที่ลักษณะความเสียหาย[105] ในส่วนภัยคุกคามทางไซเบอร์ในระดับวิกฤติตามมาตรา 60 (3)(ข) นั้น มีถ้อยคำที่คล้ายคลึงกับคำนิยามของคำว่า “สถานการณ์ฉุกเฉิน” พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548[106] ซึ่งสถานการณ์ฉุกเฉินนั้นมีหลายรูปแบบ และนำมาใช้เพื่อแก้ไขปัญหาที่เกิดจากภัยพิบัติสาธารณะในบางกรณี เช่น การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19)[107] กล่าวคือ กรณีตามมาตรา 60(3) นั้น

---

[105]พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548, มาตรา 11.

[106]“สถานการณ์ฉุกเฉิน” หมายถึง สถานการณ์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวมหรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง.

[107]เป็นช่วงเวลาที่มีการก่อภัยในทางไซเบอร์เพิ่มมากขึ้น. Harjinder Singh Lallie and others, “Cyber Security in the Age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” **Computers & Security** 105 (2021): 102-248.

สามารถปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 อีกทั้งยังให้อำนาจนายกรัฐมนตรี หน่วยงานราชการ และเจ้าหน้าที่รัฐโดยไม่ต้องผ่านความเห็นชอบของรัฐสภาตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติ และกฎหมายอื่นที่เกี่ยวข้องได้ แม้การใช้พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 เพื่อลดขั้นตอนทางราชการในช่วงต้นของวิกฤตจะเป็นการอำนวยความสะดวกแก่หน่วยงานที่เกี่ยวข้อง อย่างไรก็ตาม จากประกาศคณะกรรมการที่มีการออกแนวปฏิบัตินั้นมีการมอบหมายให้หน่วยงานต่าง ๆ ของรัฐร่วมกันออกแนวทางเพื่อจัดทำมาตรการเองโดยไม่ได้คำนึงความพร้อมทางด้านทรัพยากรของแต่ละหน่วยงาน จึงอาจนำมาสู่ความล่าช้าในการออกมาตรการ ตลอดจนความไม่เป็นเอกภาพของมาตรการรักษาความมั่นคงทางไซเบอร์

ทั้งนี้ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มาตรา 53 และ 54 ได้กำหนดมาตรการให้หน่วยงานภาครัฐได้ดำเนินการ คือ กำหนดให้หน่วยงานควบคุมหรือกำกับดูแล (Regulator) จะต้องตรวจสอบ (Audit) โดยจะกระทำด้วยตนเองหรือโดยหน่วยงานอื่นก็ได้ มาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับควบคุมดูแลของตน ซึ่งจะต้องไม่น้อยกว่าประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ที่สำนักงานฯ กำหนดอีกทั้ง “ต้องมีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมินด้านความมั่นคงปลอดภัยสารสนเทศ และต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าเป็นผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอกก็ได้”[108] ทั้งนี้ หน่วยงานอาจใช้หลักการประเมินความเสี่ยงด้านไซเบอร์และการตรวจสอบ ซึ่งเป็นที่ยอมรับในอุตสาหกรรม (Best Practices) อาทิ ISO/IEC 27001, ISO 19011, NIST SP 800-30 และ NIST SP 800-53A เป็นต้น โดยในขณะนี้ยังไม่ได้มีการออกตรวจอย่างจริงจังหรือการลงโทษทางอาญา[109] ซึ่งแม้จะมีแนวปฏิบัติที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศนั้นมีลักษณะเป็นแนวปฏิบัติพื้นฐาน (Security Control Baselines) ซึ่งระบุถึงหลักเกณฑ์การพิจารณาลักษณะของภัยคุกคามทางไซเบอร์ทั้ง 4 ปัจจัย ได้แก่ 1) ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน 2) ลักษณะผลกระทบต่อข้อมูลในระบบ 3) แนวโน้มในการกู้คืนระบบ และ 4) ลักษณะ

---

[108]สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), **กรณีศึกษาจากการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานของรัฐ** [Online], available URL: https://cc.ubru.ac.th/backend/file-download/02-10-20231537966296.pdf, 2566 (กันยายน, 13).

[109]กองทัพบก, **EP. 3 หน่วยงานรัฐพร้อมหรือไม่? ที่จะรับมือกับภัยคุกคามครั้งนี้!** [Online], available URL: https://rta.mi.th/ep-3-หน่วยงานรัฐพร้อมหรือไม่, 2566 (พฤศจิกายน, 18).

ผลกระทบต่อลูกค้าหรือผู้ใช้บริการ นอกจากนี้ พระราชบัญญัติดังกล่าวได้กำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไว้ทั้งสิ้น 8 ประเภท โดยกฎหมายฉบับนี้เปิดช่องให้บัญญัติหน่วยงานในลักษณะอื่นนอกเหนือจากประเภท 1-7 อาจเข้าข่ายเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งแต่ละประเภทจะกำหนดหน่วยงานกำกับดูแลและตรวจการดำเนินการตามมาตรการและออกมาตรการตรงกับลักษณะของภารกิจและบริการหน่วยงาน เช่น ให้ธนาคารแห่งประเทศไทยดูแลมาตรการทางไซเบอร์ของหน่วยงานด้านการเงินการธนาคาร เป็นต้น โดยมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ดูแลมาตรการทางไซเบอร์ในภาพรวม[110]

7. ข้อเสนอแนะ

ในปัจจุบันมีภัยคุกคามข้อมูลของประชาชนในรูปแบบใหม่ที่หลากหลาย จึงมีความจำเป็นอย่างยิ่งที่ประเทศไทยจะมีกฎหมายที่รับมือภัยคุกคามความมั่นคงทางไซเบอร์ โดยเฉพาะอย่างยิ่งการสู้รบทางไซเบอร์ อย่างไรก็ตาม เพื่อให้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 นั้น มีความครอบคลุมอย่างครบถ้วนและสามารถนำไปใช้ปฏิบัติได้อย่างมีประสิทธิภาพยิ่งขึ้น ผู้เขียนขอเสนอแนวทางปรับปรุงแก้ไขกฎหมายดังกล่าวดังนี้

1) กฎหมายฉบับนี้ถูกบังคับใช้กับหน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมทั้งสิ้น 8 กลุ่ม ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงาน และสาธารณูปโภค ด้านสาธารณสุข และด้านอื่น ๆ ตามที่คณะกรรมการฯ ประกาศกำหนดเพิ่มเติม เพื่อป้องกันภัยคุกคามทางไซเบอร์ตามมาตรา 60 ซึ่งสามารถครอบคลุมถึงการโจมตีในไซเบอร์ที่เคยเกิดขึ้นในประเทศไทย รวมถึงการสู้รบทางไซเบอร์ แต่ทว่าการบัญญัตินิยามศัพท์ทางกฎหมายในระดับสากลก็ยังคงไม่มีคำนิยามที่ตกผลึก และเป็นที่ยอมรับอย่างชัดเจน ดังนั้น หากการที่นิยามคำศัพท์ตามแต่เฉพาะในกฎหมายฉบับนี้อาจนำไปสู่ข้อจำกัด จึงควรเปิดกว้างให้สามารถตีความ พัฒนา หรือปรับเปลี่ยนได้ เพื่อให้ทันต่อการเปลี่ยนแปลงของนวัตกรรมที่พัฒนาอย่างรวดเร็วของเทคโนโลยี

2) การรับมือกับภัยคุกคามทางไซเบอร์นั้น เป็นความรับผิดชอบและความพร้อมหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ในกรณีของการบริการโอนเงินผ่านแอพพลิเคชั่นธนาคาร ธนาคารแห่งประเทศไทยมีมาตรการสำหรับการดูแลบริการดังกล่าว อีกทั้ง ยังมีการลงพื้นที่ตรวจการดำเนินการของธนาคารพาณิชย์ เป็นต้น จึงอาจมีข้อห่วงกังวลว่า

---

[110]เรื่องเดิม.

ในกรณีที่หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่ได้มีมาตรการป้องกันภัยคุกคามทางไซเบอร์ที่เป็นรูปธรรมและไม่ได้มีทรัพยากรบุคคลในการออกตรวจการดำเนินการตามมาตรการนั้น หน่วยงานดังกล่าวจะต้องดำเนินการอย่างไร และควรมีการลงรายละเอียดให้แก่หน่วยงานที่เกี่ยวข้องว่าต้องมีการกำหนดมาตรการ หรือส่งเสริมกิจกรรมลักษณะใด เพื่อรักษาความมั่นคงทางไซเบอร์ในเชิงเทคนิคเพื่อให้หน่วยงานที่เกี่ยวข้องนำไปปฏิบัติตามได้อย่างเป็นรูปธรรมและมีเอกภาพหรือไม่ จึงนำมาสู่คำถามว่าแนวปฏิบัติพื้นฐานหรือมาตรการดังกล่าวจะใช้บังคับกับหน่วยงานที่เกี่ยวกับระบบบริการสาธารณะหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างไร รับมือกับสถานการณ์สงครามที่เกิดจากการโจมตีทางไซเบอร์ได้หรือไม่ มีมาตรการที่ชัดเจน มีการเตรียมความพร้อมในแต่ละด้านแล้วหรือไม่ เพราะธนาคารพาณิชย์มีธนาคารแห่งประเทศไทยกำกับดูแลหรือธนาคารที่เป็นต่างประเทศก็จะอยู่ภายใต้การกำกับของกฎหมายต่างประเทศ รวมไปถึงธนาคารยังต้องมีมาตรการต่าง ๆ ให้สอดคล้องกับมาตรฐานของรัฐปลายทางของธุรกรรมอีกด้วย ซึ่งไม่น่าเป็นห่วงเท่ากับหน่วยงานของภาครัฐและภาคเอกชนที่ขาดความพร้อม และจะเป็นเป้าหมายของการโจมตี ภาครัฐจึงต้องเข้ามากำกับดูแลตั้งแต่ต้นตามบทบาทหน้าที่ เพราะหากเกิดสถานการณ์เช่นนั้นแล้วความเสียหายอาจมีผลรุนแรงและแก้ไขได้ยาก

3) แนวปฏิบัติพื้นฐาน (Security Control Baselines) ไม่ได้แบ่งมาตรการตามระดับองค์กรอย่างเป็นรูปธรรม ให้แต่ละประเภทมีหน่วยงานควบคุม จึงอาจทำให้เกิดคำถามว่าในกรณีหน่วยงานภาครัฐเป็นผู้รับผิดชอบระบบสาธารณสุข หรือ ระบบสาธารณูปโภค เช่น กระทรวงสาธารณสุขจะต้องดำเนินการ มาตรการความมั่นคงปลอดภัยทางไซเบอร์ที่โรงพยาบาลระดับจังหวัดต้องดำเนินการอย่างไร มาตรการความมั่นคงปลอดภัยทางไซเบอร์ที่ระดับโรงพยาบาลประจำตำบลต้องดำเนินการอย่างไร และมาตรการความมั่นคงปลอดภัยทางไซเบอร์ที่โรงพยาบาลของแต่ละหน่วยสังกัดอื่น ๆ ที่มิใช่กระทรวงสาธารณสุขต้องดำเนินการอย่างไร ซึ่งแต่ละหน่วยงานย่อมต้องพิจารณาให้ชัดเจนถึงระดับของมาตรการความมั่นคงทางไซเบอร์ที่อาจไม่สามารถใช้ระดับมาตรการเดียวกันได้ รวมไปถึงงบประมาณและการมีผู้เชี่ยวชาญในด้านความมั่นคงปลอดภัยทางระบบไซเบอร์มาดูแลอย่างจริงจังเป็นต้น

4) จากแนวคิดสากลดั้งเดิมของการป้องกันตนเองที่จะต้องถูกโจมตีก่อน แต่ประเทศกำลังพัฒนาอย่างไทยไม่ได้เป็นผู้นำในการคิดค้นทางด้านเทคโนโลยี แต่เป็นเพียงผู้ใช้เทคโนโลยีเท่านั้น การที่จะต้องรอคอยให้ถูกกระทำก่อนแล้วจึงตอบโต้ได้ อาจส่งผลให้ความเสียหายจากการสู้รบทางไซเบอร์มากเกินกว่าที่ประเทศไทยจะแบกรับเอาไว้ได้ ดังนั้น เพื่อความอยู่รอดของรัฐ (State survival) อันเป็นหลักการที่สำคัญที่สุด ในการป้องกันตนเองจากกรณีการสู้รบทางไซเบอร์นั้น ประเทศไทยจึงควรผลักดันแนวทางการปฏิบัติของไทยในการอ้างสิทธิในการป้องกันตนเองล่วงหน้าโดยที่ไม่จำเป็นจะต้องรอให้มีการถูกโจมตีทางไซเบอร์ก่อน และพัฒนาให้เป็นกฎหมายโดยที่ใช้อำนาจอธิปไตยของตน

ในการดำเนินมาตรการต่าง ๆ ที่เคารพในอำนาจในอธิปไตยของรัฐอื่น ๆ ด้วย เพื่อไม่ให้เป็นการแทรกแซงรัฐอื่น ซึ่งประเทศไทยก็เป็นผู้นำในการพัฒนาหลักการป้องกันตนเองจากกรณีการสู้รบทางไซเบอร์นี้ให้กลายมาเป็นหลักการหรือหลักกฎหมายจารีตประเพณีระหว่างประเทศในอนาคตก็ได้

5) การดำเนินการต่าง ๆ ของกองบัญชาการไซเบอร์ของทหารนั้น จะสร้างความเชื่อมั่นให้ประชาชนได้อย่างไรว่าดำเนินการเพื่อให้กิจกรรมทางไซเบอร์มิใช่เพื่อผลประโยชน์ทางด้านการเมือง การสร้างความโปร่งใสที่ต้องสมดุลกับการรักษาความลับ และท้ายที่สุดแล้วกองทัพไทยจึงต้องปลอดจากการเมือง

8. บทสรุป

จากการพิจารณากฎหมายระหว่างประเทศเห็นว่าการโจมตีทางไซเบอร์นั้นมีบางลักษณะที่ยังยึดโยงกับสงครามรูปแบบดั้งเดิม กล่าวคือ ต้องถูกโจมตีก่อน จึงจะสามารถใช้สิทธิการป้องกันตนเองได้และต้องมีการประกาศสงครามก่อนนั้น กฎหมายระหว่างประเทศและคู่มือทาลลินด์ซึ่งยังอยู่ในระหว่างการปรับปรุงเนื้อหายังขาดความชัดเจนต่อความหมายและขอบเขตของการสู้รบทางไซเบอร์ อาวุธทางไซเบอร์ และการใช้กำลังที่ใช้วิธีทางไซเบอร์เมื่อเทียบกับการสู้รบแบบดั้งเดิม ถึงแม้จะยังคงสามารถใช้กฎหมายที่เทียบเคียงต่อไปได้ แต่จากการสู้รบที่เปลี่ยนไป เห็นควรมีการปรับปรุงให้ทันสมัยเพื่อให้มีกฎหมายระหว่างประเทศในเรื่องดังกล่าวเป็นการเฉพาะ ทั้งนี้ หลายประเทศยังมีความเห็นที่หลากหลายเกี่ยวกับขอบเขตและผลกระทบจากการสู้รบทางไซเบอร์ และมีบางประเทศที่เห็นควรให้บัญญัติกฎหมายขึ้นมาเป็นการเฉพาะด้วยการกำหนดหลักเกณฑ์ใหม่เพื่อรับมือกับรูปแบบภัยคุกคามที่เปลี่ยนไป

จากการพิจารณาถึงกฎหมายภายในของประเทศไทย กล่าวคือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 นั้นทำให้เข้าใจได้ว่า ประเทศไทยนั้นได้ตระหนักถึงภัยคุกคามทางไซเบอร์ ตลอดจนถึงความสำคัญของระบบและเสถียรภาพของความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ตาม อาจยังมีข้อห่วงกังวลในส่วนของการกำหนดนิยามและขอบเขตของภัยคุกคามทางไซเบอร์ที่ยังมีถ้อยคำที่ทับซ้อนกับกฎหมายอื่น เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 เป็นต้น และใช้ถ้อยคำที่สับสนจึงเกิดความไม่ชัดเจนว่า เมื่อเกิดการโจมตีทางไซเบอร์หรือการสู้รบทางไซเบอร์นั้นจะต้องนำบทบัญญัติในกฎหมายใดและมาตราใดมาปรับใช้ นอกจากนี้ ควรมีการลงรายละเอียดการดำเนินการทางด้านความมั่นคงทางไซเบอร์ว่าจะสามารถพัฒนาได้อย่างเป็นรูปธรรมให้รับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ทั้งในภาพรวม และในแต่ละด้านได้อย่างรวดเร็วและมีประสิทธิภาพเพียงใด และกฎหมายที่บัญญัตินั้นจะมีบทบาท และถูกนำไปบังคับใช้กับหน่วยงาน

ต่าง ๆ ทั้งในภาครัฐและภาคเอกชนได้มากน้อยเพียงใด ทั้งนี้ หน่วยงานควบคุมหรือกำกับดูแล (Regulator) พึงต้องตรวจสอบ กำกับ และสนับสนุนการดำเนินการที่เกี่ยวข้องกับการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับผู้ที่เกี่ยวข้องทั้งภาครัฐและเอกชน พร้อมทั้งพิจารณาด้วยว่าการจะมีระบบและมาตรการความมั่นคงปลอดภัยทางไซเบอร์ที่เสถียรและมีประสิทธิภาพนั้นนอกเหนือไปจากหลักการสำคัญในด้านกฎหมายและด้านไซเบอร์แล้ว ต้องคำนึงถึงปัจจัยแวดล้อมอื่น ๆ เช่น ทรัพยากรบุคคล องค์ความรู้ รวมถึงลักษณะภารกิจหรือการบริการ และการดำเนินของแต่ละหน่วยงาน เป็นต้น

บรรณานุกรม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. **เกี่ยวกับ สกมช. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม** [Online]. Available URL: https://www.mdes.go.th/mission/detail/2481, (ม.ป.ป.).

กรุงเทพธุรกิจ. **'สุทิน' สั่งทุกเหล่าทัพตั้ง 'กองบัญชาการไซเบอร์' ต้านภัยคุกคามใหม่** [Online]. Available URL: https://www.bangkokbiznews.com/politics/1128462, 2567 (มิถุนายน, 15)

กองทัพบก. **EP. 3 หน่วยงานรัฐพร้อมหรือไม่? ที่จะรับมือกับภัยคุกคามครั้งนี้!** [Online]. Available URL: https://rta.mi.th/ep-3-หน่วยงานรัฐพร้อมหรือไม่, 2566 (พฤศจิกายน, 18).

กองบรรณาธิการ. "การปฏิบัติการข่าวสารในยุคแห่งสงครามสารสนเทศ." **วารสารสถาบันวิชาการป้องกันประเทศ** 7, 1 (2559): 9-15.

ไทยรัฐ ออนไลน์. **"กองทัพ" รุกตั้งหน่วยไซเบอร์ทหาร รับภัยคุกคาม เริ่มผลิตนักรบ 1 ต.ค.นี้** [Online]. Available URL: https://www.thairath.co.th/news/localbangkok/2787536, 2567 (พฤษภาคม, 22).

บีบีซี. **ไอโอ : คณะก้าวหน้าเปิดโปงข้อมูลเครือข่ายปฏิบัติการข่าวสารกองทัพ ด้านเอกชนแถลงโต้ชี้ข้อมูลบิดเบือน** [Online]. Available URL: https://www.bbc.com/thai/thailand-55145803, 2563 (ธันวาคม, 1).

ประชาไทย. **ก.กลาโหม เตรียมตั้งกองบัญชาการสงครามไซเบอร์** [Online]. Available URL: https://prachatai.com/journal/2024/05/109345, 2567 (พฤษภาคม, 25).

ไพศาล นภสินธุวงศ์. "สงครามและกฎการสงคราม War and Principles of War." **วารสารนาวิกาธิปัตย์สาร** 79 (กุมภาพันธ์-พฤษภาคม 2553): 76-93.

ไมโครซอฟ. **การโจมตีทางไซเบอร์คืออะไร** [Online]. Available URL: https://www.microsoft.com/th-th/security/business/security-101/what-is-a-cyberattack, (ม.ป.ป.).

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. **เอกสารศึกษาเฉพาะกรณีการสื่อสารทางยุทธศาสตร์ (Strategic Communication : SC) และการปฏิบัติการข่าวสาร (Information Operations : IO) ของกองทัพไทย : แนวทางการดำเนินงานในอนาคต**. กรุงเทพมหานคร: ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, 2559.

สปริงนิวส์. **IO #ทหารมีไว้ทำไม ที่มาและเรื่องราว ปฏิบัติการข่าวสารสร้างสรรค์!?** [Online]. Available URL: https://www.springnews.co.th/news/hot-issue/847064, 2567 (มกราคม, 19).

สาวตรี สุขศรี. **นโยบาย Single Internet Gateway เพื่อรัฐ เพื่อประชาชน หรือเพื่อใคร?** [Online]. Available URL: https://prachatai.com/journal/2015/10/61774, 2558 (ตุลาคม, 6).

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.). **กรณีศึกษาจากการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานของรัฐ** [Online]. Available URL: https://cc.ubru.ac.th/backend/file-download/02-10-20231537966296.pdf, 2566 (กันยายน, 13).

Ameli, Saeid Reza. Hassan Hosseini and Farnaz Noori. "Militarization of Cyberspace, Changing Aspects of War in the 21st Century: The Case of Stuxnet Against Iran." **Iranian Review of Foreign Affairs** 10, 29 (2019): 99-136.

Angstrom, Jan. and Jerker J. Widen. **Contemporary Military Theory: The dynamics of war**. New York: Routledge, 2015.

Atrews, Ridge A. "Cyberwarfare: Threats, Security, Attacks, and Impact." **Journal of Information Warfare** 19, 4 (2020): 17-28.

Boer, Lianne J. M. **International Law As We Know It: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship**. Cambridge: Cambridge University Press, 2021.

Boulanin, Vincent. **Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon System** [Online]. Available URL: https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1501.pdf, 2015 (November, 2).

Brandon, Valeriano and Ryan C. Maness. "The Dynamics of Cyber Conflict Between Rival Antagonists." In **Cyber War versus Cyber Realities: Cyber Conflict in the International System**. Oxford: Oxford University Press, 2015.

Broeders, Dennis and others. "Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards lines in the sand?." **Journal of Cyber Policy** 7, 1 (2022): 97-135.

Buxton, Oliver. **Cyber Warfare: Types, Examples, and How to Stay Safe** [Online]. available URL https://www.avast.com/c-cyber-warfare, 2023 (July, 14).

Carr, Jeffrey. **Inside Cyber Warfare: Mapping the cyber underworld**. 2nd ed. Sebastopol: O'Reilly, 2011.

Clapham, Andrew. “Declarations of War and Neutrality.” In **War**. Oxford: Oxford University Press, 2021.

Collins, Edward Jr., and Martin A. Rogoff. “The Caroline Incident of 1837, the McLeod Affair of 1840–1841. And the Development of International Law.” **American Review of Canadian Studies** 20, 1 (1990): 81-107.

Commonwealth & Development Office. **Application of international law to states’ conduct in cyberspace: UK statement** [Online]. Available URL: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement, 2021 (June, 3).

Davis, William W. George T. Duncan and Randolph M. Siverson. “The Dynamics of Warfare: 1816-1965.” **American Journal of Political Science** 22, 4 (1978): 772–792.

Denning, Peter J. **The Internet Worm**. Mountain View: NASA Ames Research Center, 1989.

Droege, Cordula. “The Interplay between International Humanitarian law and International Human Rights Law in Situation of Armed Conflict.” **Israel Law Review** 40, 2 (2007): 310-355.

Dutch Ministry of Foreign Affairs. **Letter to the parliament on the international legal order in cyberspace** [Online]. Available URL: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, 2019 (July, 5).

Eilstrup-Sangiovanni, Mette. “Why the World Needs an International Cyberwar Convention.” **Philosophy & Technology** 31, 3 (2018): 379-407.

Foitong, Supawee. **NoSQL injection 101** [Online]. Available URL: https://datafarm-cybersecurity.medium.com/nosql-injection-101-e453d9856545, 2023 (March, 29).

Forcese, Craig. **Destroying the Caroline: The Frontier Raid that Reshaped the Right to War**. Toronto: Irwin Law, 2018.

Garrie, Daniel B. “Cyberwarfare, What Are the Rules?.” **Journal of Law & Cyber Warfare** 1 (2012): 1-7.

Government of Canada. **International Law applicable in cyberspace** [Online]. Available URL: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, 2022 (April, 22).

Halpern, Sue. **How Cyber Weapons Are Changing the Landscape of Modern Warfare** [Online]. Available URL: https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare, 2019 (July, 18).

Heintze, Hans-Joachim and Pierre Thielbörger. Eds. **From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the last 25 Years**. Switzerland: Springer Cham, 2016.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” **Journal of Strategic Security** 4, 2 (2011): 49-60.

Hoisington. Matthew. Regulating Cyber Operations Through International Law: In Out or Against the Box? In: Ludovica Glorioso and Mariarosaria Taddeo eds., **Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative**. Switzerland: Springer Cham, 2016.

International Committee of the Red Cross. **What limits does the law of war impose on cyber attacks?** [Online]. Available URL: https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.html, 2013 (June, 28).

_____. **1980 Convention on Certain Conventional Weapons** [Online]. Available URL: https://www.icrc.org/en/document/1980-convention-certain-conventional-weapons#.VKkpP2SG-rY, 2021 (May, 21).

_____. **Weapons** [Online]. Available URL: https://www.icrc.org/en/document/weapons, 2011 (November, 30).

_____. **What are jus ad bellum and jus in bello?** [Online]. Available URL: https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0%EF%BB%BF, 2015 (January, 22).

Jensen, Eric Talbot. “The Tallinn Manual 2.0: Highlights and Insights.” **Georgetown Journal of International Law** 48, 3 (Spring 2017): 735-778.

Kello, Lucas. “Cyber Legalism: Why it fails and what to do.” **Journal of Cybersecurity** 7, 1 (2021). 1-9.

Kuru, Huseyin. “Prohibition of Use of Force and Cyber Operations as Force.” **Journal of Learning and Teaching in Digital Age** 2, 2 (2017): 49-53.

Lallie, Harjinder and others. “Cyber Security in the Age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.” **Computers & Security** 105, (2021): 102-248.

Lancelot, Jonathan F. “Cyber-Diplomacy: Cyberwarfare and the rules of engagement.” **Journal of Cyber Security Technology** 4, 4 (2020): 240-254.

Landler, Mark and John Markoff. **Digital Fears Emerge After Data Siege in Estonia** [Online]. Available URL: https://www.nytimes.com/2007/05/29/technology/29estonia.html, 2007 (May, 29).

Libicki, Martin C. “Appendix A: What Constitutes an Act of War in Cyberspace?.” In **Cyberdeterrence and Cyberwar**. Arlington, VA: RAND Corporation, 2009.

McKenzie, Simon. “Cyber Operations against Civilian Data: Revisiting War Crimes against Protected Objects and Property in the Rome Statute.” **Journal of International Criminal Justice** 19, 5 (November 2021): 1165-1192.

Moeckli, Daniel, Sangeeta Shah and Sandesh Sivakumaran. **International Human Rights Law**. 3rd ed. Oxford: Oxford University Press, 2018.

Möller, Dietmar. “P. F. NIST Cybersecurity Framework and MITRE Cybersecurity Criteria.” In **Guide to Cybersecurity in Digital Transformation. Advances in Information Security**. Switzerland: Springer, Cham, 2023.

National Cyber Force. **National Cyber Force Explainer** [Online]. Available URL: https://assets.publishing.service.gov.uk/media/61b9f526d3bf7f05522e302e/Force_Explainer_20211213_FINAL__1_.pdf, 2021 (December, 13).

_____. **The National Cyber Force: Responsible Cyber Power in Practice** [Online]. Available URL: https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_ Power_in_Practice.pdf, 2023 (April, 3).

Noel, George and Mark Reith. "Cyber Warfare Evolution and Role in Modern Conflict." **Journal of Information Warfare** 20, 4 (2021): 30-44.

Office of the High Commissioner of United Nations Human Rights. **International legal Protection of Human Rights in Armed Conflict** [Online]. Available URL: https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict.pdf, 2011 (May, 12).

Redcross. **Introduction to International Humanitarian Law** [Online]. Available URL: https://www.redcross.org.uk/about-us/what-we-do/protecting-people-in-armed-conflict/international-humanitarian-law, (n.d.).

Roscini, Marco. **Cyber Operations and the Use of Force in International Law**. Oxford: Oxford University Press 2014.

Sanger, David E. **Obama Order Sped Up Wave of Cyberattacks Against Iran** [Online]. Available URL: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html, 2012 (June, 1).

Schmitt Michael N. ed. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**. 2nd ed. New York: Cambridge University Press, 2017.

_____. **Tallinn Manual on the International Law Applicable to Cyber Warfare**. New York: Cambridge University Press, 2013.

Sharma, Amit and others. "Advanced Persistent Threats (APT): Evolution, anatomy, attribution and countermeasures." **Journal of Ambient Intelligence and Humanized Computing** 14, 7 (2023): 9355-9381.

Silpa. **สงครามไซเบอร์ครั้งแรก ๆ ของโลก และการก้าวข้ามนิยาม IO สู่ภัยจากรัฐชาติ...** [Online]. Available URL: https://www.silpa-mag.com/history/article_46065, 2564 (พฤศจิกายน, 11).

Singer, Peter W., and Allan Friedman. **Cybersecurity and Cyberwar: What everyone needs to know**. Oxford: Oxford University Press, 2014.

Sosecure. **สรุป 9 เหตุการณ์การโจมตีทางไซเบอร์ครั้งใหญ่ในไทย** [Online]. Available URL: https://www.sosecure.co.th/2024/04/29/cyber-attack, 2567 (เมษายน, 29).

Steffens, Timo. **Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage**. Heidelberg: Springer Vieweg Berlin, 2020.

Stevens, Tim. "Cyberweapons: power and the governance of the invisible." **International Politics** 55, 3-4 (2018): 482–502.

Takase, Kaori. **SQLi : SQL Injection คืออะไร อธิบายช่องโหว่และการป้องกัน SQL Injection** [Online]. Available URL: https://kixoqxq59.medium.com/sqli-sql-injection-คืออะไร-อธิบายช่องโหว่และการป้องกัน-sql-injection-173113d91cdc, 2021 (June, 9).

The National Institute of Standards and Technology. **The NIST Cybersecurity Framework (CSF) 2.0** [Online]. Available URL: https://doi.org/10.6028/NIST.CSWP.29, 2024 (February, 26).

The NATO Cooperative Cyber Defence Centre of Excellence. **The Tallinn Manual** [Online]. Available URL: https://ccdcoe.org/research/tallinn-manual, 2012 (September, 20).

Toussaint, Marion. Sylvère Krima, and Hervé Panetto. "Industry 4.0 Data Security: A cybersecurity frameworks review." **Journal of Industrial Information Integration** 39 (March 2024): 100-604.

Tsagourias, Nicholas and Giacomo Biggio. "The regulation of cyber weapons." In Eric P.J. Myjer and Thilo Marauhn eds., **Research Handbook on International Arms Control Law**. United Kingdom: Edward Elgar, 2022.

Tsilonis, Victor. "Cyber Warfare: International Criminal Law in the Digital Era." In **The Jurisdiction of the International Criminal Court**. Switzerland: Springer Cham, 2024.

U.S. Cyber Command. **Our History** [Online]. Available URL: https://www.cybercom.mil/About/History. (n.d.)

U.S. Department of Commerce and National Instituted of Standards and Technology. "**NIST Special Publication 800-30 Rev. 1 : Guide for Conducting Risk Assessments** [Online]. Available URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, 2012 (September, 20).

United Nations. **Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States** [Online]. Available URL: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf, 2021 (July, 13).

Vsm365. **รูปแบบการโจมตีทาง Cyber ที่คุณควรรู้จัก** [Online]. Available URL: https://www.vsm365.com/th/articles/Types-of-cyber-attacks-you-should-know, 2567 (พฤษภาคม, 9).

Wood, Michael. "The Caroline Incident-1837." In Tom Ruys, Olivier Corten, Alexandra Hofer eds. **The Use of Force in International Law: A Case-Based Approach**. Oxford: Oxford University Press, 2018.

Woollacott, Emma. **UK's National Cyber Force Reveals How It Works** [Online]. Available URL: https://www.forbes.com/sites/emmawoollacott/2023/04/04/uks-national-cyber-force-reveals-how-it-works/?sh=5eafcb6b29f5., 2023 (April, 4).

Zarmsky, Sarah. "Is International Criminal Law Ready to Accommodate Online Harm?: Challenges and Opportunities." **Journal of International Criminal Justice** 22, 1 (2024): 169-184.

Zetter, Kim. **Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon**. New York: Crown Publishers, 2014.