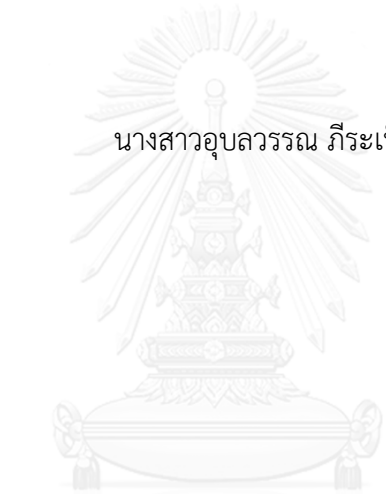
การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ : ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ

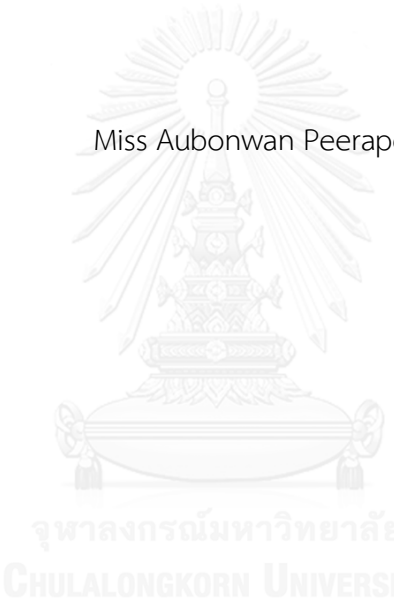
นางสาวอุบลวรรณ ภีระเป็ง



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

CYBER ATTACKS IN THE SITUATION OF ARMED CONFLICTS : STUDY ON THE APPLICATI ON OF INTERNATIONAL HUMANITARIAN LAW

Miss Aubonwan Peerapeng



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws Program in Laws
Faculty of Law
Chulalongkorn University
Academic Year 2015

หัวข้อวิทยานิพนธ์	การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ : ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ
โดย	นางสาวอุบลวรรณ ภีระเป็ง
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะนิติศาสตร์
(ศาสตราจารย์ ดร.นันทวัฒน์ บรมานันท์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์สุผานิต เกิดสมเกียรติ)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ)

.....กรรมการ
(รองศาสตราจารย์ จันตรี สินศุภฤกษ์)

.....กรรมการภายนอกมหาวิทยาลัย
(พันเอกปิยชาต เจริญผล)

อุบลวรรณ ภีระเป็ง : การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ : ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ (CYBER ATTACKS IN THE SITUATION OF ARMED CONFLICTS : STUDY ON THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร.ศารทูล สันติวาสะ, 262 หน้า.

วิทยานิพนธ์ฉบับนี้มีจุดประสงค์เพื่อศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศว่าสามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในฐานะเป็นวิธีการและปัจจัยในการสู้รบที่เกิดขึ้นใหม่ได้หรือไม่ เพียงใด ทั้งนี้ กฎหมายมนุษยธรรมระหว่างประเทศเป็นกฎหมายระหว่างประเทศบังคับใช้เมื่อมีการสู้รบหรือสถานการณ์การขัดกันทางอาวุธเกิดขึ้นประกอบด้วยหลักเกณฑ์เกี่ยวกับปฏิบัติการทางทหารรวมทั้งการให้ความคุ้มครองพลเรือน

จากการศึกษาวิจัยพบว่า แม้ว่าการโจมตีทางไซเบอร์จะเป็นวิธีการและปัจจัยในการสู้รบใหม่และไม่ปรากฏข้อบทที่เกี่ยวข้องกับการใช้เทคโนโลยีตามกฎหมายมนุษยธรรมระหว่างประเทศ แต่กฎหมายมนุษยธรรมระหว่างประเทศสามารถยืดหยุ่นครอบคลุมกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันเป็นการนำเอาเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์มาใช้ในปฏิบัติการทางทหารและการสู้รบได้ อย่างไรก็ตาม ด้วยลักษณะความเชื่อมต่อของเทคโนโลยีที่ใช้ในทางทหารและพลเรือน อีกทั้งการโจมตีทางไซเบอร์ยังเป็นการกระทำภายในห้วงไซเบอร์ที่ไม่มีลักษณะทางกายภาพก่อให้เกิดข้อท้าทายในบังคับใช้หลักการสำคัญตามกฎหมายมนุษยธรรมระหว่างประเทศ ไม่ว่าจะเป็นหลักการแยกแยะเป้าหมาย หลักความได้สัดส่วนในการโจมตี หลักการใช้ความระมัดระวังในการโจมตีอย่างมีนัยสำคัญจำเป็นจะต้องอาศัยความร่วมมือจากผู้ที่มีส่วนเกี่ยวข้องทั้งภาคประชาสังคม ภาครัฐ และความร่วมมือระหว่างประเทศในการพัฒนาแนวทางการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่จะนำไปสู่แนวทางปฏิบัติของรัฐที่ชัดเจนต่อไป เพื่อให้กฎหมายมนุษยธรรมระหว่างประเทศสามารถรองรับวิธีการและปัจจัยในการสู้รบใหม่ซึ่งมีความซับซ้อนของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ทวีขึ้นไปตามกาลเวลาได้อย่างมีประสิทธิภาพ

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2558 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

5586044734 : MAJOR LAWS
KEYWORDS: CYBER ATTACKS/ ARMED CONFLICT/ INTERNATIONAL HUMANITARIAN LAW

AUBONWAN PEERAPENG: CYBER ATTACKS IN THE SITUATION OF ARMED CONFLICTS : STUDY ON THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW. ADVISOR: ASST. PROF.SARATOON SANTIVASA, Ph.D., 262 pp.

The purpose of this thesis is to examines the applicability of International humanitarian law, whether it could be applied to cyber attacks in the situation of armed conflict, which is considered as “a new means and methods of warfare”, to what extent. It is worthy to note that the International humanitarian law is a branch of International law which enforcing in the wartime or when the situation of armed conflict has arisen, where as it is consisting of the restriction of military operations and the protection of civilians.

After studying and analyzing, it discovers that although the cyber attacks refers to a new means and methods of warfare and currently there are no specific regulations related to the use of technology under International humanitarian law. However, International humanitarian law is flexible in certain degree to covers the cyber attacks in the situation of armed conflict where the new technologies has been used in military operations, especially at wartime. Nevertheless, the interconnectivity of military and civilian technology and plus the cyber-attacks is an operation within the Cyberspace where no physical domain, accordingly, gives rise a significant challenges on the applicable of principles of International humanitarian law into the cyber attacks in the situation of armed conflict whether the principles of distinction, proportionality and precautions in attack, regarding to the cyber attacks in the situation of armed conflict. Such challenges are require the cooperation between the civil society, government and international organizations for developing approaches to address the cyber attacks in the situation of armed conflict and leading to the clearly state practice. So, that International humanitarian law can effectively respond to the new means and methods of warfare, which consist of complex technologies as the times goes by.

Field of Study: Laws Student's Signature .....

Academic Year: 2015 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สามารถสำเร็จลุล่วงไปได้ด้วยความกรุณาเป็นอย่างยิ่งจากท่านผู้ช่วยศาสตราจารย์ ดร. ศารทูล สันติวาสะ อาจารย์ที่ปรึกษาวิทยานิพนธ์ที่ได้ให้คำปรึกษาและชี้แนะแนวทางอันเป็นประโยชน์อย่างยิ่งต่อผู้เขียนตลอดระยะเวลาการศึกษาวิทยานิพนธ์จนกระทั่งวิทยานิพนธ์ฉบับนี้บรรลุผลสำเร็จ ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูงมา ณ ที่นี้

ผู้เขียนขอกราบขอบพระคุณท่านผู้ช่วยศาสตราจารย์สุผานิต เกิดสมเกียรติ ท่านรองศาสตราจารย์จันตรี สินศุภฤกษ์ และท่านพันเอกปิยชาต เจริญผล ประธานกรรมการและกรรมการสอบวิทยานิพนธ์ตามลำดับที่ได้กรุณาสละเวลารับเป็นกรรมการสอบวิทยานิพนธ์และให้คำแนะนำทางวิชาการในประเด็นต่างๆ อันเป็นประโยชน์ในการแก้ไขปรับปรุงต่อวิทยานิพนธ์ฉบับนี้

นอกจากนี้ ผู้เขียนขอขอบคุณเพื่อน พี่ น้อง หมวดวิชากฎหมายระหว่างประเทศ เจ้าหน้าที่คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยที่อำนวยความสะดวกตลอดการจัดทำวิทยานิพนธ์ เพื่อน พี่ น้อง มหาวิทยาลัยเชียงใหม่และที่ทำงานทุกคนที่ให้ความช่วยเหลือและให้กำลังใจในการทำวิทยานิพนธ์แก่ผู้เขียนเสมอมา

สุดท้ายนี้ หากวิทยานิพนธ์ฉบับนี้มีคุณค่าและประโยชน์ทางวิชาการใดๆ ผู้เขียนขอกราบเป็นกตเวทิกุลแก่บิดามารดา คณาจารย์และผู้มีพระคุณทุกท่านที่ให้การศึกษาและความรู้คุณธรรมแก่ผู้เขียนตลอดมา หากมีข้อบกพร่องประการใด ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

สารบัญ

หน้า

หน้า

หน้า

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน การพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์มีความก้าวหน้าและมีความสำคัญต่อการดำเนินกิจกรรมต่างๆ ของมนุษย์เป็นอย่างมาก มนุษย์นำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้ประโยชน์ในทุกกิจกรรมของมนุษย์ ทั้งภาครัฐและภาคเอกชน ไม่ว่าจะเป็นการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้ในการควบคุมระบบโครงสร้างพื้นฐานของรัฐ เช่น ระบบไฟฟ้า ระบบคมนาคมและการขนส่ง ระบบสื่อสาร ระบบการเงินการธนาคาร ระบบประปา หรือการใช้เทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการควบคุมระบบการดำเนินธุรกิจและติดต่อสื่อสารทางธุรกิจในภาคเอกชน เทคโนโลยีสารสนเทศและคอมพิวเตอร์ยังเป็นช่องทางในการติดต่อสื่อสารที่สำคัญ สามารถใช้อินเทอร์เน็ตในการเชื่อมต่อเครือข่ายคอมพิวเตอร์ทั่วโลก ศึกษาหาความรู้ทางการศึกษา ความบันเทิง ทำให้รับทราบข้อมูลข่าวสารจากทวีปอีกฝั่งของโลกได้อย่างรวดเร็วจากการใช้ประโยชน์จากการพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ถือได้ว่าเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือ “ไซเบอร์” มีบทบาทสำคัญอย่างมากต่อการเปลี่ยนแปลงทางเศรษฐกิจ การเมือง และสังคม

การพัฒนาทางเทคโนโลยีทางไซเบอร์ไม่เพียงแต่เข้ามามีบทบาทในการเปลี่ยนแปลงทางด้านเศรษฐกิจ การเมืองและสังคม ยังมีบทบาทสำคัญต่อการเปลี่ยนแปลงทางด้านปฏิบัติการทหารและการสู้รบอีกด้วย จากเดิมที่การสู้รบยุคเริ่มแรกเป็นความขัดแย้งต่อสู้เพื่อความอยู่รอด ความต้องการอาหาร การแก่งแย่งพื้นที่ที่ใช้เพื่อการเพาะปลูก เกษตรกรรมหรือปศุสัตว์ โดยใช้หอกดาบ เป็นอาวุธหรือปัจจัยในการสู้รบ ต่อมาในยุคอุตสาหกรรม แนวความคิดของการทำสู้รบเปลี่ยนแปลงไปเป็นการสู้รบเพื่อต้องการแสดงอำนาจ ลักษณะการสู้รบเป็นความขัดแย้งที่รุนแรงและมีการใช้อาวุธที่มีอานุภาพในการทำลายล้างสูง เช่น ปืน จรวด ลูกระเบิด จรวดนำวิถี ขีปนาวุธ หรืออาวุธร้ายแรงที่ทำอันตรายถึงตาย (Kinetic Weapons) อาวุธชีวภาพ (Biological Weapons) อาวุธเคมี (Chemical Weapons) อาวุธนิวเคลียร์ (Nuclear Weapons) จนในยุคปัจจุบันเทคโนโลยีทางไซเบอร์ได้ถูกนำมาใช้ร่วมกับอาวุธตามแบบ (Conventional Weapons) เพื่อเพิ่มประสิทธิภาพในการสู้รบหรือพัฒนาเป็นอาวุธเพื่อใช้ในการสู้รบหรือที่เรียกว่า อาวุธไซเบอร์

(Cyber Weapons) หรือการใช้เทคโนโลยีทางไซเบอร์ในปฏิบัติการทางทหารและการสู้รบ โดยเฉพาะการนำไซเบอร์มาใช้ในการโจมตีฝ่ายตรงข้ามในการสู้รบหรือการโจมตีทางไซเบอร์ (Cyber Attacks)

อย่างไรก็ตาม คำว่า “การโจมตีทางไซเบอร์” ถูกนำไปใช้อธิบายเหตุการณ์ไซเบอร์ซึ่งไม่จำกัดเฉพาะการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเท่านั้น ไม่ว่าจะเป็นในการจารกรรมข้อมูลไซเบอร์ (Cyber Espionage) สงครามไซเบอร์ (Cyber Warfare) อาชญากรรมทางไซเบอร์ (Cyber Crime)

ในไม่กี่ปีที่ผ่านมา หลายประเทศได้ให้ความสำคัญกับการพัฒนาขีดความสามารถทางไซเบอร์เพื่อนำมาใช้ในปฏิบัติการทางทหารและการสู้รบ มีการจัดตั้งกองกำลังไซเบอร์เป็นหน่วยปฏิบัติการเฉพาะทางทหาร อาทิ ประเทศสหรัฐอเมริกา จีน อังกฤษ รัสเซีย รวมทั้งนำเทคโนโลยีทางไซเบอร์มาใช้ในปฏิบัติการทางทหารเพื่อขัดขวางหรือทำลายความสามารถทางไซเบอร์ของฝ่ายตรงข้าม เห็นได้จากเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นต่อประเทศเอสโทเนียและซีเรียในปี ค.ศ. 2007 จอร์เจียในปี ค.ศ. 2008 ซึ่งการโจมตีทางไซเบอร์เหล่านั้นไม่เพียงแต่ก่อให้เกิดความเสียหายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ของเป้าหมายทางทหารโดยตรงแล้ว ยังก่อให้เกิดความเสียหายต่อคอมพิวเตอร์หรือระบบเครือข่ายของพลเรือนด้วยเช่นกัน การพัฒนาขีดความสามารถทางไซเบอร์ของหลายประเทศทุกภูมิภาคทั่วโลก ทำให้เกิดความกังวลว่าจะเกิดสมรภูมิในการสู้รบใหม่เพิ่มขึ้น เป็นสงครามไซเบอร์ (Cyber Warfare) ที่มีความรุนแรงและสร้างความเสียหายได้ไม่ต่างจากสงครามตามแบบ (Conventional Warfare)

จากการพัฒนาทางเทคโนโลยีทางไซเบอร์ถูกนำไปใช้งานทั้งในกิจการของพลเรือนและทางทหาร จึงทำให้พลเรือนมีความเสี่ยงที่จะได้รับผลกระทบจากการโจมตีทางไซเบอร์ ไม่ว่าจะเป็นการใช้ระบบคอมพิวเตอร์ควบคุมระบบโครงสร้างพื้นฐานสำคัญของพลเรือน (Civilian Infrastructure) อาทิ ระบบควบคุมและประเมินผลแบบศูนย์รวม (Supervisory Control And Data Acquisition หรือ SCADA) ระบบควบคุมแบบกระจายส่วน (Distributed Control Systems) ที่ใช้ในการติดตั้งโครงสร้างพื้นฐานที่สำคัญ เช่น โรงไฟฟ้า โรงงานนิวเคลียร์ เขื่อน การบำบัดน้ำเสียและระบบการกระจายน้ำ โรงกลั่นน้ำมัน ท่อก๊าซและท่อน้ำมัน ระบบธนาคาร ระบบโรงพยาบาล การควบคุมการจราจรทางอากาศและรถไฟต่างขึ้นอยู่กับระบบดังกล่าว

นอกจากนั้น การเชื่อมต่อทางอินเตอร์เน็ตยังเป็นต้นเหตุของภัยคุกคามต่อโครงสร้างพื้นฐานของพลเรือนได้ เนื่องมาจากเครือข่ายทางการทหารส่วนใหญ่ขึ้นอยู่กับโครงสร้างพื้นฐานคอมพิวเตอร์

ของพลเรือน เช่น เครือข่ายใยแก้วนำแสงใต้ทะเล ดาวเทียม ในขณะที่ ยานพาหนะของพลเรือน การขนส่งและการควบคุมการจราจรทางอากาศที่มีเพิ่มมากขึ้นพร้อมกับระบบกำหนดตำแหน่งบนโลก หรือจีพีเอส (Global Positioning System (GPS)) ถูกนำมาใช้ทางการทหารด้วยเช่นเดียวกัน

จากการพัฒนาเทคโนโลยีทางไซเบอร์ที่เปลี่ยนแปลงรูปแบบวิธีการสู้รบ ความกังวลของประชาคมระหว่างประเทศเกี่ยวกับความเป็นไปได้ของการเกิดสงครามไซเบอร์ที่เพิ่มมากขึ้น จึงทำให้เกิดความท้าทายต่อการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ ซึ่งเป็นกฎหมายที่กำหนดกฎเกณฑ์เกี่ยวกับปฏิบัติการทางทหารที่ใช้ในการสู้รบที่ได้รับการยอมรับทั่วไปว่ามีลักษณะเป็นกฎหมายจารีตประเพณีระหว่างประเทศ (Customary International Law) มีผลใช้บังคับเป็นการทั่วไป (Erga Omnes) โดยกฎเกณฑ์ตามกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ไม่ว่าจะเป็นกฎเกณฑ์ตามอนุสัญญาเจนีวาและอนุสัญญาเฮกต่างเป็นกฎเกณฑ์ที่บัญญัติไว้ก่อนที่จะมีการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์ หรือ ไซเบอร์ (Cyber) มาใช้ในทางการทหารและการสู้รบ วิธีการและปัจจัยในการสู้รบที่เปลี่ยนแปลงไปตามพัฒนาความก้าวหน้าทางไซเบอร์จะสามารถนำกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่มาบังคับใช้กับการโจมตีทางไซเบอร์ที่เกิดขึ้นสถานการณ์การขัดกันทางอาวุธนี้ได้หรือไม่ อย่างไร หลักการสำคัญตามกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ยืดหยุ่นครอบคลุมที่จะบังคับใช้เพื่อคุ้มครองพลเรือนหรือผู้ที่ไม่เกี่ยวข้องกับการสู้รบอันเป็นวัตถุประสงค์หลักของกฎหมายมนุษยธรรมระหว่างประเทศได้หรือไม่ หรือจำเป็นที่จะต้องพัฒนากฎหมายมนุษยธรรมระหว่างประเทศให้ขยายขอบเขตครอบคลุมถึงปฏิบัติการทางทหารที่อาศัยเทคโนโลยีทางไซเบอร์นี้หรือไม่ จำเป็นที่จะต้องมีข้อบทเกี่ยวกับสถานการณ์การขัดกันทางอาวุธที่อาศัยเทคโนโลยีทางไซเบอร์นี้ไว้เป็นการเฉพาะเจาะจงควบคุมเช่นเดียวกับที่มีสนธิสัญญาควบคุมอาวุธเคมี อาวุธนิวเคลียร์หรือไม่ สิ่งเหล่านี้เป็นประเด็นสำคัญที่เกิดขึ้นตามการพัฒนาและความก้าวหน้าของเทคโนโลยีทางไซเบอร์ที่เพิ่มขึ้นอย่างมีนัยสำคัญ

ดังนั้น วิทยานิพนธ์ฉบับนี้จะได้ทำการศึกษาเกี่ยวกับการโจมตีทางไซเบอร์ที่นำไปใช้ในปฏิบัติการทางทหารและการสู้รบหรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ความสัมพันธ์ระหว่างการโจมตีทางไซเบอร์กับกฎหมายมนุษยธรรมระหว่างประเทศ และการใช้หลักการของกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ เพื่อวิเคราะห์ข้อท้าทายในการบังคับใช้หลักการสำคัญตามกฎหมายมนุษยธรรมระหว่างประเทศต่อการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อเสนอแนวทางในการศึกษาวิจัยข้อท้าทายที่เกิดขึ้นจากการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศแก่ผู้สนใจศึกษาต่อไป

1.2 วัตถุประสงค์ในการศึกษาวิจัย

1. เพื่อศึกษาความสัมพันธ์ระหว่างการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธกับกฎหมายมนุษยธรรมระหว่างประเทศ
2. เพื่อศึกษาและวิเคราะห์ถึงการใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ตลอดจนข้อท้าทายเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ
3. เพื่อศึกษาและวิเคราะห์ข้อท้าทายเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ และแนวทางในการแก้ไขข้อท้าทาย

1.3 สมมติฐาน

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์ หรือ ไซเบอร์มาใช้ในปฏิบัติการทางทหารเพื่อเพิ่มศักยภาพในการสู้รบให้กับกองทัพ แม้กฎหมายมนุษยธรรมระหว่างประเทศจะไม่ได้มีข้อบทกำหนดว่าการโจมตีทางไซเบอร์เป็นวิธีการและปัจจัยในการสู้รบ แต่หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศสามารถยืดหยุ่นเพื่อให้ครอบคลุมกับวิธีการและปัจจัยในการสู้รบเหล่านี้ได้ แต่อย่างไรก็ตาม ยังมีข้อท้าทายบางประการเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศต่อกรณีการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

1.4 ขอบเขตของการวิจัย

การศึกษาวิทยานิพนธ์ฉบับนี้ ในส่วนแรกจะเป็นการศึกษาความสัมพันธ์ระหว่างการโจมตีทางไซเบอร์กับกฎหมายมนุษยธรรมระหว่างประเทศ ได้แก่ ความเบื้องต้นเกี่ยวกับการโจมตีทางไซเบอร์ ทั้งความหมายและรูปแบบของการโจมตีทางไซเบอร์ โดยศึกษาและวิเคราะห์จากกรณีศึกษาของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เกิดขึ้นจริง และความพยายามในทางระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์มาใช้ในสถานการณ์การขัดกันทางอาวุธ ตลอดจนแนวความคิดเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

จากนั้นในบทที่ 3 จะมุ่งศึกษาการใช้หลักการของกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ในส่วนแรกจะศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์แบ่งออกเป็นการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศในขณะที่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นแล้ว กับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ที่ก่อให้เกิดข้อพิพาททางอาวุธ ทั้งการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ (International Armed Conflict) และการโจมตีทางไซเบอร์ในสถานการณ์ขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ (Non-international Armed Conflict) ส่วนต่อมาจะศึกษาการบังคับใช้หลักการเกี่ยวกับปฏิบัติการทางทหาร และการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนตามกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อทำการวิเคราะห์ถึงข้อท้าทายในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธต่อไป

ในบทที่ 4 จะทำการวิเคราะห์ข้อท้าทายในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธว่ามีข้อท้าทายที่ต้องคำนึงถึงเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศอย่างไรบ้าง ตลอดจนแนวทางในการแก้ไขข้อท้าทายเหล่านั้น เพื่อเป็นแนวทางในการศึกษาวิจัยการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธแก่ผู้ที่สนใจศึกษาต่อไป

ในส่วนบทที่ 5 จะเป็นการนำความรู้ที่ได้จากการศึกษาค้นคว้าทั้งหมดข้างต้นมาหาข้อสรุปเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ พร้อมทั้งเสนอแนะแนวทางในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธให้เป็นไปได้จริง

1.5 วิธีการศึกษาและวิจัย

การศึกษาวิทยานิพนธ์นี้ใช้วิธีการศึกษาแบบการวิจัยเอกสาร (Documentary Research) ทั้งภาษาไทยและภาษาต่างประเทศ โดยศึกษาข้อมูลจากกฎหมายมนุษยธรรมระหว่างประเทศ ความเห็นของนักกฎหมาย จากหนังสือ บทความทางวิชาการ วิทยานิพนธ์ เอกสารที่เกี่ยวข้อง

รวมไปถึงข้อมูลทางอินเทอร์เน็ตที่เกี่ยวข้อง เพื่อนำมาศึกษาและวิเคราะห์ถึงข้อท้าทายและแนวทางในการปรับปรุงที่เหมาะสม

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษาวิจัย

1. เพื่อให้ทราบและเข้าใจถึงความสัมพันธ์ระหว่างการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธกับกฎหมายมนุษยธรรมระหว่างประเทศ
2. เพื่อให้ทราบถึงการใช้หลักการของกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ และข้อท้าทายเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ
3. เพื่อก่อให้เกิดประโยชน์และเป็นแนวทางแก่ผู้ที่สนใจทำการศึกษาในข้อท้าทายเกี่ยวกับการบังคับใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศต่อไป

บทที่ 2
ความสัมพันธ์ระหว่างการโจมตีทางไซเบอร์กับกฎหมายมนุษยธรรมระหว่างประเทศ

เนื้อหาในบทนี้จะทำการศึกษาความสัมพันธ์ระหว่างการโจมตีทางไซเบอร์กับกฎหมายมนุษยธรรมระหว่างประเทศโดยแบ่งเนื้อหาออกเป็นสามส่วน เริ่มต้นจากการศึกษาความเบื้องต้นเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธประกอบด้วยความหมายของการโจมตีทางไซเบอร์และรูปแบบการโจมตีทางไซเบอร์ที่ใช้ในสถานการณ์การขัดกันทางอาวุธที่เกิดขึ้นจริง เพื่อแสดงให้เห็นถึงลักษณะพิเศษของการโจมตีทางไซเบอร์ที่มีความซับซ้อนตามการพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์และส่งผลกระทบในทางกฎหมายเกี่ยวกับการควบคุมการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เกิดขึ้น

ในส่วนที่สองจะอธิบายถึงความพยายามในทางระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์ขัดกันทางอาวุธทั้งแนวทางของรัฐ ความร่วมมือระหว่างประเทศระดับทวิภาคีและระดับพหุภาคี เพื่อแสดงเห็นท่าที แนวโน้มการรับมือและความตระหนักในภัยคุกคามของการโจมตีทางไซเบอร์ของประชาคมระหว่างประเทศ จากนั้นในส่วนที่สาม จะกล่าวถึงแนวความคิดเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธซึ่งจะนำไปสู่การวิเคราะห์ในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เป็นลำดับถัดไป

2.1 ความเบื้องต้นเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

เนื่องจากการโจมตีทางไซเบอร์ยังไม่มีคำนิยามที่ชัดเจนถูกนำไปใช้อธิบายเหตุการณ์ไซเบอร์อย่างหลากหลาย ทั้งที่เกิดขึ้นในความสัมพันธ์ระหว่างประเทศในความสัมพันธ์ปกติหรือความสัมพันธ์ในลักษณะขัดแย้ง ดังนั้น จำเป็นที่จะต้องศึกษาความหมายและลักษณะของการโจมตีทางไซเบอร์เพื่อให้สามารถแยกแยะได้ว่าเหตุการณ์ไซเบอร์ใดเป็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

2.1.1 ความหมายของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

กรมวิทยาศาสตร์และเทคโนโลยีกลาโหมได้ให้ความหมายของคำว่า “ไซเบอร์” ว่าเป็นคำที่ใช้นำหน้าคำอื่น เพื่อสื่อความหมายว่ามีลักษณะที่เกี่ยวข้องกับคอมพิวเตอร์หรืออิเล็กทรอนิกส์[1] เป็นความหมายในเชิงนามธรรมหมายถึงขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ซึ่งครอบคลุมมากกว่าคอมพิวเตอร์ซึ่งมีความหมายในเชิงรูปธรรมของอุปกรณ์ระบบคอมพิวเตอร์ทั่วไป โดยไซเบอร์ (Cyber-) เป็นส่วนหนึ่งหรือ Subset ของระบบข้อมูลข่าวสาร (Information)[2]

ปัจจุบันมีรายงานเหตุการณ์ไซเบอร์ซึ่งเกิดจากการนำไซเบอร์เทคโนโลยีไปใช้ในหลากหลายบริบททั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธ คำว่า “การโจมตีทางไซเบอร์” ถูกนำไปใช้อธิบายเหตุการณ์ทางไซเบอร์ไม่จำกัดเฉพาะในสถานการณ์การขัดกันทางอาวุธเท่านั้น อาทิ สงครามไซเบอร์ (Cyber Warfare) การจารกรรมข้อมูลไซเบอร์ (Cyber Espionage) อาชญากรรมทางไซเบอร์ (Cyber-Crime) ทั้งหมดล้วนเป็นการกระทำที่มีความเกี่ยวข้องกับห้วงไซเบอร์[3] ที่อาศัยความก้าวหน้าและการพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์เช่นเดียวกัน โดยพิจารณาความหมายของแต่ละเหตุการณ์ไซเบอร์ได้ดังนี้

---

[1] รุ่งธรรม บัวแตง, "ความหมายของ ไซเบอร์ (Cyber) " http://www.dstd.mi.th/board/index.php?topic=887.0. [November 6, 2015]

[2] นิวัติ เนียมพลอย, "ไซเบอร์ กับการรักษาความปลอดภัยและการปฏิบัติการ (Cyber with Security and Operations)," https://nniwat.wordpress.com/2013/11/08/%E0%B9%84%E0%B8%8B%E0%B9%80%E0%B8%9A%E0%B8%AD%E0%B8%A3%E0%B9%8C-%E0%B8%81%E0%B8%B1%E0%B8%9A%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A3%E0%B8%B1%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/. [December 10, 2015]

[3] ปิยชาต เจริญผล, คู่มือกฎการใช้กำลัง (สถาบันกฎหมายมนุษยธรรมระหว่างประเทศ, 2554). หน้า 68.

ห้วงไซเบอร์หรือไซเบอร์สเปซ (Cyberspace) หมายถึงดินแดนทั่วโลกซึ่งมีลักษณะเฉพาะโดยการใช้อิเล็กทรอนิกส์ย่านความถี่คลื่นแม่เหล็กไฟฟ้า เพื่อที่จะเก็บ ปรับแต่งและแลกเปลี่ยนข้อมูลโดยระบบเครือข่ายรวมถึงอินเทอร์เน็ต ระบบโทรคมนาคม และรวมถึงระบบโครงสร้างที่เกี่ยวข้อง

อาชญากรรมไซเบอร์ (Cyber Crime) หรือ อาชญากรรมคอมพิวเตอร์ (Computer Crime) คือการกระทำใดๆ ที่เป็นความผิดต่อกฎหมายอาญาซึ่งต้องใช้ความรู้ความสามารถเกี่ยวกับคอมพิวเตอร์ในการกระทำความผิด โดยการกระทำดังกล่าวทำให้ผู้เสียหายได้รับความเสียหายและทำให้ผู้กระทำความผิดได้รับผลประโยชน์ด้วย[4] โดยกฎหมายที่บังคับใช้กับอาชญากรรมไซเบอร์จะขึ้นอยู่กับกฎหมายภายในของแต่ละรัฐแต่ละประเทศจะมีประมวลกฎหมายอาญาที่กำหนดว่าการกระทำทางไซเบอร์ใดถือเป็นอาชญากรรม[5] อย่างเช่นที่ประเทศสหรัฐอเมริกามีทั้งกฎหมายสารบัญญัติและกฎหมายวิธีพิจารณาความเกี่ยวกับอาชญากรรมไซเบอร์[6]

ประเภทความผิดเกี่ยวกับอาชญากรรมไซเบอร์หรืออาชญากรรมคอมพิวเตอร์ได้แก่ การเผยแพร่ภาพและสื่อลามกอนาจาร (Pornography) การเผยแพร่ภาพลามกอนาจารเด็ก (Child Pornography) การล่อลวงและอนาจารเด็ก (Pedophilia) การข่มขู่และคุกคามทางอินเตอร์เน็ต (Cyber-Stalking) การแสดงข้อความที่ก่อให้เกิดความเกลียดชังทางเชื้อชาติ (Hate Speech) การกระทำอันเป็นการกระทบต่อความมั่นคงของรัฐ (Threats to National Security) การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (Unauthorized Access) การจารกรรมข้อมูลคอมพิวเตอร์ (Computer Espionage) การทำให้เสียหายหรือทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ (Computer Sabotage) การฉ้อโกงทางคอมพิวเตอร์ (Computer Fraud)[7]

ส่วนการจารกรรมข้อมูลไซเบอร์ (Cyber-Espionage) หมายถึงการใช้เครื่องคอมพิวเตอร์หรือกิจกรรมการติดต่อสื่อสารทางดิจิทัลโดยเจตนา พยายามให้ได้มาซึ่งข้อมูลข่าวสารที่สำคัญเกี่ยวกับฝ่ายตรงข้ามหรือคู่แข่ง เพื่อวัตถุประสงค์ให้ได้รับความได้เปรียบหรือการขายข้อมูลที่สำคัญเพื่อ

---

[4] นันทชัย เพียรสนอง, "การใช้เทคโนโลยีสารสนเทศกับผลกระทบทางกฎหมาย" (งานวิจัยในการอบรมหลักสูตรผู้บริหารกระบวนการยุติธรรมระดับสูง (บ.ย.ส.), 2539). หน้า 27.

[5] David Weissbrodt, "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage," *Minnesota Journal of International Law* 22(2013). P. 366.

[6] CCIPS Compiled by Al Rees, "Computer Crime and Intellectual Property Section," ed. U.S. Department of Justice(2006).

[7] ตะวัน พึ่งพุทธารักษ์, "ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์" (จุฬาลงกรณ์มหาวิทยาลัย, 2546). หน้า 31.

ค่าตอบแทน[8] โดยการจารกรรมข้อมูลไซเบอร์ถือเป็นความผิดเกี่ยวกับอาชญากรรมไซเบอร์ประเภทหนึ่งตามที่ได้ศึกษาข้างต้น กฎหมายที่บังคับใช้กับการจารกรรมข้อมูลไซเบอร์จึงขึ้นอยู่กับกฎหมายภายในของแต่ละรัฐเช่นเดียวกับอาชญากรรมไซเบอร์

ในปัจจุบันคำว่า “สงครามไซเบอร์ (Cyber Warfare)” หรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ (Cyber Attacks in Armed Conflict) ยังไม่มีการให้ความหมายซึ่งเป็นที่ยอมรับกันเป็นสากล ด้วยเหตุกังกล่าวจึงมีความร่วมมือระหว่างประเทศ หน่วยงานภาครัฐ และนักวิชาการกฎหมายเสนอความหมายที่เฉพาะเจาะจง เพื่อให้สามารถนำไปใช้และให้ได้รับการยอมรับจากประชาคมระหว่างประเทศ ดังนี้

สงครามไซเบอร์ (Cyber Warfare) เป็นคำที่นิยามขึ้นโดย Richard A. Clarke ผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลสหรัฐ หมายถึง การดำเนินการโดยรัฐชาติแห่งหนึ่งเพื่อแทรกซึมคอมพิวเตอร์หรือเครือข่ายของอีกรัฐชาติหนึ่ง เพื่อวัตถุประสงค์ในการก่อให้เกิดความเสียหายหรือการรบกวน ขัดขวางกระบวนการดำเนินการตามปกติให้หยุดชะงัก[9]

คณะกรรมการกาชาดระหว่างประเทศ (International Committee of the Red Cross) กล่าวว่า สงครามไซเบอร์ หมายถึง ปฏิบัติการใดๆ ที่กระทำต่อเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ผ่านกระแสข้อมูล (Data Stream) ซึ่งนำมาใช้เป็นวิธีการและปัจจัยในการสู้รบ[10] และยังกล่าวว่า สงครามไซเบอร์หรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เป็นวิธีการที่เป็นปฏิปักษ์ใดๆ ต่อฝ่ายศัตรูที่ถูกออกแบบมา เพื่อค้นหา เปลี่ยนแปลง ทำลาย รบกวน หรือ

---

[8] Kevin G. Coleman, "Cyber Espionage Targets Sensitive Data," (2008), See more at: http://sip-trunking.tmcnet.com/topics/security/articles/47927-cyber-espionage-targets-sensitive-data.htm#sthash.6TTlz9qg.dpuf. [August 21, 2015]

[9] Richard A Clarke and Robert K Knake, *Cyber War: The Next Threat to National Security and What to Do About It*(HarperCollins, 2010). P. 11.

[10] ICRC, "Weapons: Icrc Statement to the United Nations, 2014," https://www.icrc.org/en/document/weapons-icrc-statement-united-nations-2014. [December 12, 2015]

การถ่ายโอนข้อมูลที่เก็บไว้ในคอมพิวเตอร์ การจัดการโดยคอมพิวเตอร์หรือส่งผ่านทางคอมพิวเตอร์[11] เช่น การโจมตีทางไซเบอร์ต่อระบบขนส่งมวลขน ระบบควบคุมการจราจรทางอากาศยาน ระบบแจกจ่ายน้ำมัน เครือข่ายอิเล็กทรอนิกส์ เขื่อน เคมีภัณฑ์ และโรงงงานนิวเคลียร์ เป็นต้น

องค์การความร่วมมือเซี่ยงไฮ้ (Shanghai Cooperation Organisation - SCO) กำหนดคำนิยามของคำว่า สงครามข้อมูลข่าวสารหรือสงครามสารสนเทศ (Information War)[12] คือ การปะทะกันระหว่างรัฐสองรัฐหรือมากกว่าสองรัฐขึ้นไปในห้วงสารสนเทศ (Information Space) โดยมีเป้าหมายในการทำลายระบบข้อมูลข่าวสาร การประมวลผลข้อมูลข่าวสาร แหล่งข้อมูลข่าวสาร และโครงสร้างอื่นๆ เพื่อบ่อนทำลายระบบการเมือง เศรษฐกิจและสังคม เป็นจิตวิทยาล้างสมองขนาดใหญ่ เพื่อทำให้เกิดความไม่มั่นคงทางสังคมและรัฐ ตลอดจนเพื่อบังคับให้รัฐตัดสินใจในสิ่งที่เป็นประโยชน์ของฝ่ายตรงข้าม[13] ปรากฏตามความตกลงระหว่างรัฐบาลประเทศสมาชิกขององค์การความร่วมมือเซี่ยงไฮ้ว่าด้วยความร่วมมือในด้านความมั่นคงปลอดภัยระบบสารสนเทศระหว่างประเทศ (Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security)[14]

[11] "Cyber Warfare," https://www.icrc.org/eng/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm. [September 3, 2015]

[12] สงครามไซเบอร์หรือ Cyber Warfare เป็นรูปแบบหนึ่งของ สงครามข้อมูลข่าวสาร Information Warfare ประกอบด้วย สงครามการควบคุมบังคับบัญชา (Command-and-Control Warfare) สงครามบนบรรทัดฐานของการข่าวกรอง (Intelligence-Based Warfare) สงครามอิเลคทรอนิคส์ (Electronic Warfare) สงครามจิตวิทยา (Psychological Warfare) สงครามแฮกเกอร์ (Hacker Warfare) สงครามสารสนเทศทางเศรษฐศาสตร์ (Economic Information Warfare) และสงครามไซเบอร์ (Cyber Warfare) ที่มา หน่วยบัญชาการและต่อสู้อากาศยานชายฝั่ง กองทัพเรือhttp://www.acdc.navy.mi.th/pdf/Information%20Warfare.pdf

[13] "Annex1 to the Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (Unofficial Translation)," ed. SCO(2 Dec 2008). P. 209.

[14] SCO, "Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (Unofficial Translation),"(2008). P. 202-203.

กระทรวงกลาโหมของสหรัฐอเมริกาให้ความหมายของคำว่า “การโจมตีทางเครือข่ายคอมพิวเตอร์” (Computer Network Attacks - CNAs)[15] ไว้ว่าเป็นการกระทำผ่านการใช้งานเครือข่ายคอมพิวเตอร์ซึ่งมีเจตนาที่ปรับเปลี่ยน รบกวน หลอกลวง ลดค่า หรือทำลายระบบคอมพิวเตอร์หรือเครือข่ายหรือข้อมูลและ/หรือโปรแกรม หรือเปลี่ยนแปลงระบบหรือเครือข่ายเหล่านั้น[16]

องค์การสนธิสัญญาแอตแลนติกเหนือ (NATO) ได้ยอมรับเอาความหมายของสหรัฐอเมริกานี้ไว้ใน NATO Glossary of Terms and Definitions โดยหมายเหตุเพิ่มเติมไว้ว่าการโจมตีทางเครือข่ายคอมพิวเตอร์เป็นรูปแบบหนึ่งของการโจมตีทางไซเบอร์[17]

เป็นที่น่าสังเกตว่า การให้ความหมายของกระทรวงกลาโหมสหรัฐนี้เป็นการกำหนดความหมายจากคุณลักษณะของรูปแบบการโจมตีทางไซเบอร์ตามข้อเท็จจริงที่ว่าทั้งเครื่องมือหรืออาวุธที่ใช้ในการโจมตีและเป้าหมายในการโจมตีทางเครือข่ายคอมพิวเตอร์ก็คือเครือข่ายคอมพิวเตอร์และข้อมูลของฝ่ายอื่นที่บรรจุไว้ในเครือข่ายคอมพิวเตอร์เป้าหมายเหล่านั้น[18]

คู่มือทาลลินน์ (The Tallinn Manual) หรือ คู่มือทาลลินน์ว่าด้วยการบังคับใช้กฎหมายระหว่างประเทศต่อสงครามไซเบอร์กำหนดความหมายคำว่า “การโจมตีทางไซเบอร์” คือ ปฏิบัติการทางไซเบอร์ (Cyber Operation) ไม่ว่าจะเป็นการโจมตีหรือการป้องกันซึ่งคาดหมายอย่างมีเหตุผลได้ว่าจะก่อให้เกิดการบาดเจ็บหรือเสียชีวิตต่อบุคคลหรือความเสียหายหรือการทำลายต่อทรัพย์สิน

---

[15] ภายหลังนิยมเรียกว่า การโจมตีทางไซเบอร์ (Cyber Attacks) ซึ่งให้ความหมายครอบคลุมได้กว้างกว่าการโจมตีทางเครือข่ายคอมพิวเตอร์

[16] Joint Chiefs Of Staff Dod, "Department of Defense Dictionary of Military and Associated Terms,"(CreateSpace Independent Publishing Platform, 2009).

[17] NATO Standardization Agency, "Nato Glossary of Terms and Definitions,"(North Atlantic Treaty Organization, 2008).

[18] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*(the United States of America: Cambridge University Press, 2012). P. 4.

สิ่งของ[19] และให้ความหมายคำว่า ปฏิบัติการทางไซเบอร์ (Cyber Operation) ว่าเป็นการใช้ความสามารถของไซเบอร์โดยมีวัตถุประสงค์หลักในการบรรลุเป้าหมายในห้วงไซเบอร์หรือโดยการใช้ห้วงไซเบอร์[20] โดยคู่มือทาลลินน์ได้ยึดความหมายของการโจมตี (Attack) ตามข้อ 49 (1) แห่งพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ค.ศ. 1977[21] เป็นพื้นฐานในการให้ความหมายดังกล่าว

จากการศึกษาความหมายของเหตุการณ์ไซเบอร์ต่างๆ ข้างต้น สามารถสรุปได้ว่า อาชญากรรมไซเบอร์ (Cyber Crime) คือ การกระทำใดๆ ที่อาศัยความเชี่ยวชาญทางด้านเทคโนโลยีทางไซเบอร์ในการกระทำความผิดต่อกฎหมายอาญาส่วนการจารกรรมข้อมูลไซเบอร์ (Cyber Espionage) คือการใช้ความเชี่ยวชาญทางด้านเทคโนโลยีทางไซเบอร์ให้ได้มาซึ่งข้อมูลข่าวสารที่สำคัญถือเป็นรูปแบบอาชญากรรมไซเบอร์ประเภทหนึ่ง

ในส่วนความหมายของสงครามไซเบอร์หรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธผู้เขียนเห็นว่าเป็นวิธีการหรือปัจจัยในการสู้รบใดๆ ที่ดำเนินการต่อระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของฝ่ายที่เป็นปรปักษ์ภายในห้วงไซเบอร์ โดยเจตนาหรือคาดหมายได้ว่าจะก่อให้เกิดความเสียหายหรือผลกระทบต่อบุคคลหรือทรัพย์สินสิ่งของ อาจสรุปสั้นๆ ได้ว่า สงครามไซเบอร์คือการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์มาใช้ในการสู้รบ

---

[19] *Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts* ed. Michael N. Schmitt(Cambridge University Press, 2013).

Rule 30- Definition of Cyber Attack

"A cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."

[20] ibid.

"A cyber operation is defined as the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."

[21] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)," (8 June 1977).

Article 49 (1)

"Attacks" means acts of violence against the adversary, whether in offence or in defence."

2.1.2 รูปแบบการโจมตีทางไซเบอร์เกิดขึ้นในสถานการณ์การขัดกันทางอาวุธ

ในการศึกษารูปแบบการโจมตีทางไซเบอร์ที่ใช้ในสถานการณ์การขัดกันทางอาวุธพบว่าสามารถกระทำได้หลากหลายรูปแบบซึ่งในการศึกษาวิจัยเล่มนี้ ผู้เขียนขอหยิบยกเฉพาะรูปแบบการโจมตีทางไซเบอร์ที่เคยเกิดขึ้นในสถานการณ์การขัดกันทางอาวุธที่ผ่านมาแล้ว ได้แก่ การโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอส การฝังข้อมูลเท็จ และการแทรกซึมความปลอดภัยของเครือข่ายคอมพิวเตอร์ มีรายละเอียดดังต่อไปนี้

2.1.2.1 การโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอส

วิธีการโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอส (Distributed Denial of Service - DDoS) เป็นรูปแบบของการโจมตีทางไซเบอร์ที่พบบ่อยที่สุดในหลายๆ ปีที่ผ่านมาทั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธ โดยใช้วิธีการที่ทำให้คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์เป้าหมายไม่สามารถติดต่อกับคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์อื่นได้ ส่วนใหญ่จะมุ่งโจมตีต่อระบบเครือข่ายคอมพิวเตอร์ที่มีความสำคัญต่อทั้งภาครัฐและภาคเอกชน เช่น

- ระบบการสื่อสารโทรคมนาคม เช่น ระบบโทรศัพท์, ระบบการสื่อสารดาวเทียม, ระบบเครือข่ายอินเทอร์เน็ต, ระบบช่วยเหลือฉุกเฉิน 191
- ระบบการเงินการธนาคาร เช่น ธนาคารของภาครัฐและเอกชน สถาบันการเงิน ตลาดหลักทรัพย์
- ระบบไฟฟ้า เช่น ระบบที่ควบคุมการจ่ายไฟตามสายไฟฟ้า ระบบคอมพิวเตอร์ที่สถานีแจกจ่ายกระแสไฟฟ้า ระบบควบคุมเตาปฏิกรณ์นิวเคลียร์
- ระบบชลประทาน เช่น ระบบควบคุมระดับน้ำตามเขื่อนต่างๆ
- ระบบการแจกจ่ายก๊าซธรรมชาติและน้ำมันปิโตรเลียม เช่น ระบบควบคุมและประเมินผลแบบศูนย์รวม (Supervisor Control and Data Acquisition - SCADA) และระบบการจัดการพลังงาน (Energy Management Systems - EMS) ระบบควบคุมการผลิตและการขนส่ง[22]

[22] จตุชัย แพงจันทร์, "Cyber Warfare," ข่าวทหารอากาศ 72, no. 4 (2555).

ระบบเครือข่ายคอมพิวเตอร์ข้างต้นถือเป็นระบบเครือข่ายของโครงสร้างพื้นฐานที่สำคัญของรัฐ การโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอสต่อระบบเครือข่ายโครงสร้างพื้นฐานเหล่านั้นสามารถก่อให้เกิดความเสียหายทั้งทางตรงและทางอ้อม ความเสียหายที่เกิดขึ้นโดยตรงจากการโจมตีคือความเสียหายต่อระบบโครงสร้างพื้นฐานเป้าหมาย ส่วนความเสียหายทางอ้อมคือการก่อให้เกิดผลกระทบทางด้านจิตวิทยาต่อประชาชนอันเป็นผลกระทบต่อจิตใจที่เกิดขึ้นจากการโจมตีทางไซเบอร์อันเนื่องมาจากความหวาดกลัวและความไม่มั่นใจของประชาชนที่มีต่อความมั่นคงภายในรัฐ ยกตัวอย่าง การโจมตีแบบดีดีโอเอสต่อระบบการเงินของธนาคารจนเป็นเหตุให้การทำธุรกรรมทางการเงินล่ม ไม่สามารถใช้การได้ นอกจากความเสียหายที่เกิดขึ้นต่อระบบการเงินซึ่งจะต้องทำการแก้ไขปรับปรุงระบบและความเสียหายทางด้านเศรษฐกิจซึ่งสามารถวัดจำนวนความเสียหายเป็นตัวเลขได้แล้ว เมื่อระบบการเงินการธนาคารขัดข้องยังส่งผลกระทบทางด้านจิตวิทยาต่อความเชื่อมั่นของผู้ฝากเงินไว้ในธนาคารอาจเป็นสาเหตุให้ผู้คนจำนวนมากไม่มีความเชื่อมั่นต่อระบบการรักษาความปลอดภัยของธนาคารและถอนเงินออกจากธนาคารในเวลาเดียวกันจนนำไปสู่ความวุ่นวายโกลาหลภายในประเทศได้ ตัวอย่างเหตุการณ์การโจมตีแบบดีดีโอเอสที่ผ่านมา ได้แก่

กรณีการโจมตีทางไซเบอร์โดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอสต่อประเทศเอสโตเนีย (Estonia) นับว่าเป็นการโจมตีทางไซเบอร์ครั้งแรกของโลกซึ่งเกิดขึ้นในสถานการณ์ปกติ ประเทศเอสโตเนียเป็นหนึ่งในอดีตประเทศสาธารณรัฐของสหภาพโซเวียตซึ่งปัจจุบันเป็นทั้งสมาชิกกลุ่มสหภาพยุโรปและ NATO เหตุการณ์เกิดขึ้นในเดือนเมษายน ปี ค.ศ. 2007 พบว่าประเทศเอสโตเนียถูกโจมตีทางไซเบอร์โดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอสซึ่งการโจมตีดังกล่าวถูกกล่าวหาว่ามีสาเหตุเริ่มต้นมาจากการที่รัฐบาลเอสโตเนียสั่งเคลื่อนย้ายรูปปั้นอนุสรณ์และหลุมฝังศพทหารและผู้เสียชีวิตของรัสเซียใจกลางเมืองที่สร้างไว้ในช่วงต่อสู้ขับไล่พวกนาซีออกนอกประเทศในช่วงปลายสงครามโลกครั้งที่สองซึ่งรัสเซียยังปกครองอยู่ไปตั้งไว้ในสถานที่ซึ่งไม่สามารถมองเห็นได้ชัดเจนและไม่โดดเด่นในเมืองทาลลินน์ (Tallinn) เป็นเหตุให้เยาวชนซึ่งส่วนใหญ่มีต้นกำเนิดเชื้อชาติรัสเซียไม่พอใจรวมตัวกันประท้วง ณ สถานที่ตั้งอนุสรณ์ดังกล่าวและทวีความรุนแรงเพิ่มมากขึ้นจนทำให้ตำรวจต้องใช้กำลังเข้าปราบปราม โดยตำรวจจับกุมผู้ประท้วงราว 1300 คน โดยมีผู้บาดเจ็บจากเหตุการณ์ดังกล่าวประมาณ 100 คน และมีผู้เสียชีวิต 1 ราย[23]

[23] Kadri Kaska Eneken Tikk, Liis Vihul,, "International Cyber Incidents: Legal Considerations," *Cooperative Cyber Defence Centre of Excellence (CCD COE)* (2010). P.16.

จากเหตุการณ์จลาจลบนถนนในเมืองทาลลินน์ (Tallinn) นำไปสู่การก่อจลาจลในห้วงไซเบอร์ (Cyberspace) ในเวลาเพียงไม่กี่ชั่วโมง เว็บไซต์ของรัฐบาลเอสโตเนียและระบบพอร์ทัลเว็บไซต์ข่าวสารของเอสโตเนียที่เป็นทางเข้าสู่ระบบของธนาคารชั้นนำอยู่ภายใต้การโจมตีทางไซเบอร์หลายระลอก อีกทั้งยังโจมตีเว็บไซต์ที่รองรับการทำงานของเครือข่ายโทรศัพท์หลายๆ ภาคส่วน โดยการโจมตีทางไซเบอร์นี้กระทำต่อเว็บไซต์ของทั้งภาครัฐและภาคเอกชน

รูปแบบของการโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอสต่อประเทศเอสโตเนียคือการใช้คอมพิวเตอร์มากกว่าล้านเครื่องส่งคำสั่งพร้อมๆ กันไปยังเว็บไซต์เป้าหมายหลายๆ บอตเน็ต (Botnets) ให้ทำหน้าที่พร้อมๆ กัน จนทำให้เว็บไซต์ต่างๆ เกิดการน็อกหน้าเว็บ ไม่สามารถทำงานได้ นอกจากนี้ ยังทำให้เว็บไซต์สำคัญๆ หลายร้อยเว็บไซต์ภายในประเทศถูกโจมตีอย่างต่อเนื่องจนทำให้ไม่สามารถสำรองไฟล์เพื่อใช้เป็นการแบ็กอัพ (Back-up) ข้อมูลได้เป็นเหตุให้ระบบการสื่อสารและพาณิชย์ทั่วประเทศได้รับผลกระทบทันที เว็บไซต์ของหนังสือพิมพ์ที่สำคัญทั้งหมดถูกทำให้หยุดทำงาน ส่งกระทบต่อการติดต่อสื่อสารของรัฐบาล จนในที่สุดเว็บไซต์ของรัฐบาล หนังสือพิมพ์ มหาวิทยาลัยโรงพยาบาล ธนาคาร ไฟฟ้า และบริการทางการแพทย์ตกเป็นเหยื่อของการโจมตีทั้งหมด[24] การโจมตีดังกล่าวมีระยะเวลายาวนานกว่า 3 สัปดาห์ จนกระทั่งความตึงเครียดระหว่างเอสโตเนียและรัสเซียในเรื่องรูปปั้นอนุสรณ์และหลุมฝังศพทหารเริ่มผ่อนคลายลงในที่สุด[25] เหตุการณ์การโจมตีทางไซเบอร์ต่อประเทศเอสโตเนียดังกล่าวเป็นเหตุให้ผู้เชี่ยวชาญด้านความปลอดภัยบนอินเตอร์เน็ตจากทั้งยุโรปและอเมริกาเหนือต้องเดินทางไปยังเมืองทาลลินน์ (Tallinn) เพื่อให้ความช่วยเหลือเอสโตเนียในฐานะประเทศสมาชิก NATO[26]

จากการศึกษาพบว่า ผลกระทบของการโจมตีทางไซเบอร์ต่อประเทศเอสโตเนียดังกล่าวเป็นเหตุให้หน่วยงานราชการ ธนาคาร และภาคเอกชนของเอสโตเนียอยู่ในภาวะหยุดชะงักไม่สามารถทำงานได้ ส่งผลกระทบโดยตรงทางเศรษฐกิจและสังคมในวงกว้าง เนื่องจากหลายภาคส่วน

---

[24] ibid. pp. 24-25.

[25] ibid. P. 33.

[26] Richard A Clarke and Robert K Knake, Cyber War: The Next Threat to National Security and What to Do About It(HarperCollins, 2010). P. 14.

ของการพาณิชย์และอุตสาหกรรมต่างพึ่งพาโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศและการติดต่อสื่อสารและช่องทางการสื่อสารทางอิเล็กทรอนิกส์ในการดำเนินธุรกิจซึ่งนอกจากจะส่งผลกระทบต่อหน่วยงานขนาดใหญ่ๆ ไม่ว่าจะเป็น ธนาคาร บริษัทสื่อสารมวลชนและหน่วยงานของรัฐบาลยังส่งผลต่อธุรกิจประกอบการที่มีขนาดกลางและขนาดเล็กก็ได้รับผลกระทบจากการโจมตีครั้งนี้เช่นกัน[27]

ประเทศเกาหลีใต้เป็นอีกหนึ่งประเทศที่ประสบปัญหาการโจมตีทางไซเบอร์ด้วยวิธีการโดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอส ในปีค.ศ. 2009 เว็บไซต์รัฐบาลสหรัฐอเมริกาและเกาหลีใต้ รวมทั้งเว็บไซต์ของสื่อมวลชน ส่วนราชการและธนาคารหลายแห่งของประเทศเกาหลีใต้ถูกโจมตีทางไซเบอร์โดยการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอส[28] ต่อมาในเดือนมีนาคม ปี ค.ศ. 2013 มีรายงานว่าเว็บไซต์ของสถานีโทรทัศน์และธนาคารในประเทศเกาหลีใต้ถูกโจมตีทางไซเบอร์โดยการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอส ทำให้เว็บไซต์เหล่านั้นหยุดปฏิบัติงานรวมถึงการให้บริการทางการเงินทางอินเทอร์เน็ตไม่สามารถใช้การได้[29] และอีกครั้งในเดือนมิถุนายนปีเดียวกัน เว็บไซต์สื่อมวลชนและรัฐบาลรวมทั้งเว็บไซต์ของประธานาธิบดีและนายกรัฐมนตรีถูกทำให้หยุดปฏิบัติงานโดยการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอส[30] ทั้งนี้ ประเทศเกาหลีใต้เชื่อว่ารัฐบาลเกาหลีเหนือหรือเจ้าหน้าที่ของเกาหลีเหนือเป็นผู้รับผิดชอบอยู่เบื้องหลังเหตุการณ์โจมตีทางไซเบอร์ทั้งหมด[31]

---

[27] Kadri Kaska Eneken Tikk, Liis Vihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defence Centre of Excellence (CCD COE) (2010). pp. 24-25.

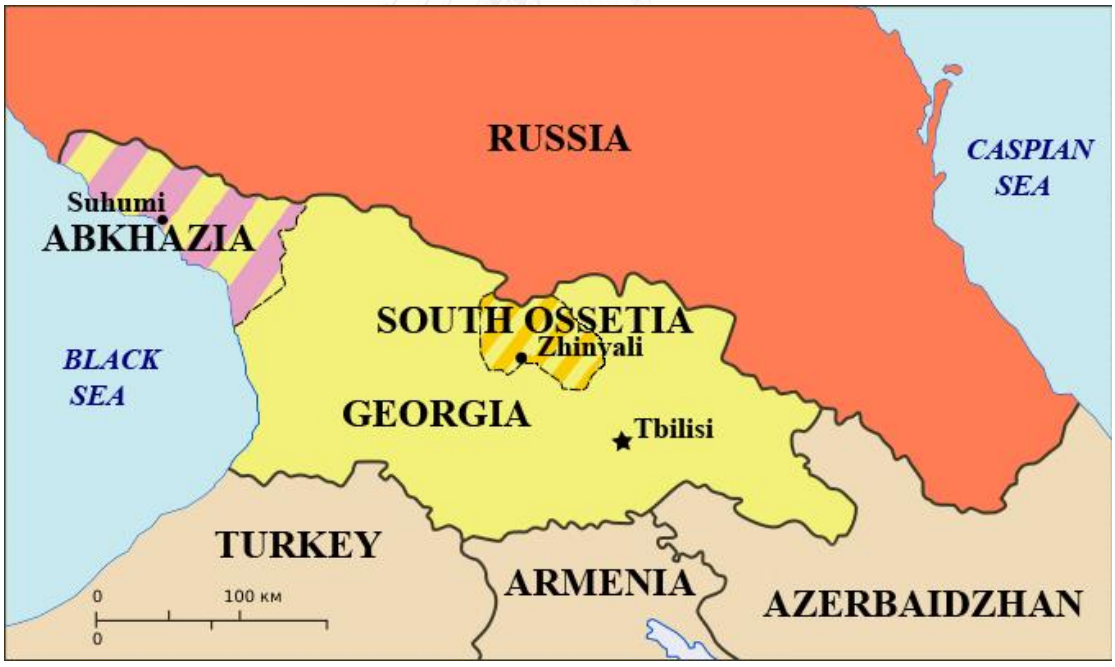
[28] Associated Press, "North Korea Launched Cyber Attacks, Says South " *The guardian*, 11 July 2009. Available at http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks

[29] CHOE SANG-HUN, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *The New York Times*, 20 March 2013. Available at http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=0 [July 2, 2015]

[30] Associated Press, "South Korea Blames North Korea for Cyberattack on Media, Government Sites," *Fox News*, 16 July 2013 Available at http://www.foxnews.com/world/2013/07/16/south-korea-blames-north-korea-for-cyberattack-on-media-government-sites/ [July 2, 2015]

[31] Richard A Clarke and Robert K Knake, Cyber War: The Next Threat to National Security and What to Do About It(HarperCollins, 2010). P. 20.

สำหรับเหตุการณ์โจมตีทางไซเบอร์ด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอสที่เกิดขึ้นในสถานการณ์การขัดกันทางอาวุธ ได้แก่ เหตุการณ์โจมตีทางไซเบอร์ต่อประเทศจอร์เจียเกิดขึ้น ในเดือนสิงหาคม ปีค.ศ. 2008 โดยมีที่มาของสถานการณ์การขัดกันทางอาวุธเริ่มต้นจากการที่เซาท์ออสเซเทีย (South Ossetia) ต้องการแบ่งแยกดินแดนประกาศตนเป็นเอกราชจากจอร์เจียในสงครามระหว่างจอร์เจียกับเซาท์ออสเซเทีย (South Ossetia) เมื่อปีค.ศ. 1991 อย่างไรก็ตาม ประชาคมระหว่างประเทศยังคงถือว่าเซาท์ออสเซเทีย (South Ossetia) เป็นส่วนหนึ่งของประเทศจอร์เจียอยู่[32] ถึงแม้ว่า ต่อมาจะมีประกาศหยุดยิงตั้งแต่ปีค.ศ. 1991 แต่ความตึงเครียดในบริเวณดังกล่าวยังคงไม่ได้รับการแก้ไข องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรป (OSCE) จึงได้จัดตั้งกองกำลังรักษาสันติภาพขึ้นในปีค.ศ. 1992 เพื่อรักษาความมั่นคงในเซาท์ออสเซเทีย (South Ossetia) โดยมีกองกำลังจากรัสเซีย จอร์เจียและเซาท์ออสเซเทีย (South Ossetia) ภายใต้อำนาจบังคับบัญชาของรัสเซีย ซึ่งในความเป็นจริงแล้ว กองกำลังรักษาสันติภาพดังกล่าวประสบความล้มเหลวในการทำงานร่วมกันและเกิดความตึงเครียดเพิ่มมากขึ้นระหว่างจอร์เจียฝ่ายหนึ่งกับกองกำลังแบ่งแยกดินแดนที่มีรัสเซียให้การสนับสนุนอีกฝ่ายหนึ่ง



รูปภาพที่ 1 แผนที่แสดงตำแหน่งทางภูมิศาสตร์ของออสเซเทีย (South Ossetia)

[32] Kadri Kaska Eneken Tikk, Liis Vihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defence Centre of Excellence (CCD COE) (2010). P. 67.

จนกระทั่ง วันที่ 7 สิงหาคม 2008 กองกำลังทางทหารของจอร์เจียเปิดฉากโจมตีต่อกองกำลังแบ่งแยกดินแดนโดยปราศจากการแจ้งเตือน มีการใช้อาวุธหนัก ระเบิดพวง เป็นภัยร้ายแรงต่อพลเรือนและมีการใช้กองกำลังทหารจอร์เจียอย่างไม่ได้สัดส่วนภายในเมืองซคินวาลี (Tskhinvali) รวมทั้งภายในดินแดนจอร์เจียซึ่งการกระทำดังกล่าวของประเทศจอร์เจียถือเป็นการละเมิดกฎหมายมนุษยธรรมระหว่างประเทศและพันธกรณีของจอร์เจียในการแก้ปัญหาความขัดแย้งอย่างสันติ[33]

ในวันที่ 8 สิงหาคม 2008 รัสเซียตอบโต้การกระทำของจอร์เจียด้วยปฏิบัติการทางทหารต่อดินแดนจอร์เจีย ทิ้งระเบิดลงที่กรุงทบิลิซี (Tbilisi) เมืองหลวงของจอร์เจีย โดยมีเป้าหมายที่จะสร้างความเสียหายต่อโครงสร้างทางเศรษฐกิจของจอร์เจียรวมไปถึง Black Sea Port และ Poti และถนนหลักที่เชื่อมทางใต้ของจอร์เจียกับตะวันออก โดยอ้างถึงหน้าที่ในการคุ้มครองประชาชนชาวรัสเซียต่างแดน[34] ต่อมาในวันที่ 9 สิงหาคม 2008 จอร์เจียประกาศภาวะสงคราม[35]

ในส่วนของการโจมตีทางไซเบอร์ด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการต่อจอร์เจียเกิดขึ้นทั้งก่อนและในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น ในวันที่ 20 กรกฎาคม 2008 เว็บไซต์ของประธานาธิบดีจอร์เจียอยู่ภายใต้การโจมตีทางไซเบอร์ด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือ ดีดีโอเอส โดยมีการสร้างคำสั่งเข้ามาสู่เว็บไซต์กว่าหลายล้านคำขอจนทำให้เว็บไซต์ทำงานมากเกินไปและหยุดปฏิบัติงานลงในที่สุด การโจมตีดังกล่าวเป็นผลให้เว็บไซต์ต้องปิดตัวลงเป็นเวลา 24 ชั่วโมง[36] ในวันที่ 8 สิงหาคม 2008 การโจมตีทางไซเบอร์ด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือ ดีดีโอเอสต่อเว็บไซต์ของรัฐบาลจอร์เจียได้เริ่มต้นในเวลาเดียวกับที่กองกำลังทหารรัสเซียต่อสู้กับกองกำลังทหารของจอร์เจีย[37]

---

[33] Council of Europe Parliamentary Assembly, "Resolution 1633 (2008):The Consequences of the War between Georgia and Russia "(2008).

[34] "Dmitry Medvedev Made a Statement on the Situation in South Ossetia (2008)," http://en.kremlin.ru/events/president/news/1043. [March 4, 2016]

[35] Kadri Kaska Eneken Tikk, Liis Vihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defence Centre of Excellence (CCD COE) (2010) P. 68.

[36] William C. Ashmore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review* 11(2009). P. 10.

[37] Ibid.

นอกเหนือจากการโจมตีทางไซเบอร์ต่อเว็บไซต์ประธานาธิบดีจอร์เจีย รัฐบาลกลาง กระทรวงการต่างประเทศและกระทรวงกลาโหมซึ่งทำให้เว็บไซต์เหล่านั้นไม่สามารถใช้งานได้ชั่วคราว[38] ระบบของธนาคารพาณิชย์ที่ใหญ่ที่สุดของประเทศจอร์เจียและสื่อต่างๆ ล้วนตกอยู่ภายใต้การโจมตีทางไซเบอร์ด้วยเช่นเดียวกัน โดยถูกรบกวน ปิดกั้นการเคลื่อนไหลของข้อมูล ขัดขวางการติดต่อสื่อสารและเกิดความสับสนไปทั่วทั้งประเทศซึ่งการโจมตีเหล่านี้มีเป้าหมายหลักอยู่ที่การขัดขวางความสามารถของรัฐบาลจอร์เจียในการติดต่อสื่อสารกับพลเมืองและรัฐอื่นๆ นำไปสู่ปัญหาการติดต่อสื่อสารตลอดทั่วทั้งประเทศเกิดขึ้นทั้งก่อนและในระหว่างที่มีการโจมตีทางกายภาพ (Physical Attack)[39] ในวันที่ 11 สิงหาคม 2008 รัฐมนตรีกระทรวงการต่างประเทศของจอร์เจียแถลงข่าวว่ารัสเซียทำสงครามไซเบอร์ขัดขวางการทำงานของเว็บไซต์จอร์เจียหลายเว็บไซต์รวมทั้งเว็บไซต์ของกระทรวงการต่างประเทศ[40]

แม้ว่าปฏิบัติการทางทหารจะสิ้นสุดลงเมื่อวันที่ 12 สิงหาคม 2008 ตามข้อตกลงหยุดยิง[41] แต่การโจมตีทางไซเบอร์ยังคงดำเนินการต่อไปตลอดทั้งเดือนสิงหาคม 2008 เซิฟเวอร์ (Server) ส่วนใหญ่ของจอร์เจียยังคงไม่สามารถกลับมาใช้งานได้อย่างเป็นปกติอาจถือได้ว่าเหตุการณ์โจมตีทางไซเบอร์ต่อประเทศจอร์เจียดังกล่าวเป็นครั้งแรกของโลกที่การโจมตีทางไซเบอร์ได้เกิดขึ้นร่วมกับปฏิบัติการทางทหารแบบดั้งเดิม (Conventional Military Action)[42]

---

[38] Steven Adair, "Georgian Websites under Attack - Ddos and Defacement," https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080811. [December 8, 2015]

[39] Lesly Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict," *Loyola of Los Angeles International and Comparative Law Review* 32, no. 2/5 (2010). P. 304.

[40] Ministry of Foreign Affairs, "Cyber Attacks Disable Georgian Websites," http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html. [April 5, 2016]

[41] BBC, "Russia 'Ends Georgia Operation' " http://news.bbc.co.uk/2/hi/europe/7555858.stm. [April 5, 2016]

[42] Lesly Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict," Loyola of Los Angeles International and Comparative Law Review 32, no. 2/5 (2010). P. 304.

2.1.2.2 การฝังข้อมูลที่ไม่ถูกต้อง

การฝังข้อมูลที่ไม่ถูกต้อง (Planting Inaccurate Information) คือรูปแบบหนึ่งของการโจมตีทางไซเบอร์ที่ต้องอาศัยความชำนาญมากกว่าการโจมตีด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอส โดยวิธีการแอบป้อนข้อมูลที่ไม่ถูกต้องลงในระบบคอมพิวเตอร์ หรือที่รู้จักในนามการโจมตีความหมาย (Semantic Attack) เป็นการทำให้ระบบคอมพิวเตอร์แสดงออกให้เหมือนว่ายังคงทำงานไปอย่างเป็นปกติซึ่งแท้จริงแล้ว ระบบคอมพิวเตอร์นั้นได้ทำงานผิดพลาด[43] โดยการใช้เทคนิคและความสามารถในการลักลอบเข้าไปยังระบบสารสนเทศของฝ่ายตรงข้ามเพื่อเปลี่ยนความหมายที่แท้จริงของสารสนเทศที่นำไปใช้งาน เช่น การเจาะระบบตรวจจับเรดาร์เพื่อทำการแก้ไขโปรแกรมให้ทำงานผิดพลาด โดยทำให้ระบบเรดาร์ที่สามารถตรวจจับตำแหน่งของเครื่องบินแสดงผลว่าเป็นเครื่องบินที่ตรวจจับตำแหน่งได้นั้นเป็นฝ่ายเดียวกันหรือตำแหน่งของเครื่องบินฝ่ายตรงข้ามไม่แสดงผลบนจอตรวจจับเรดาร์ หรือการเจาะระบบสารสนเทศทางทหารของฝ่ายตรงข้ามแล้วเข้าไปแก้ไขข้อมูลต่างๆ ที่ใช้ประกอบในการตัดสินใจ เพื่อทำให้มีการตัดสินใจที่ผิดพลาด เป็นต้น

ตัวอย่างการโจมตีทางไซเบอร์ด้วยวิธีการฝังข้อมูลที่ไม่ถูกต้องซึ่งนำมาใช้ในปฏิบัติการทางทหารเกิดขึ้นในปี ค.ศ. 1999 เมื่อสหรัฐอเมริกาได้พัฒนาแผนการที่จะป้อนข้อมูลที่ไม่เป็นความจริงลงในระบบเครือข่ายการออกคำสั่งการป้องกันทางอากาศของเซอร์เบีย เพื่อยับยั้งความสามารถของเซอร์เบียในการเล็งเป้าไปที่อากาศยานของ NATO[44] การโจมตีนี้เป็นการใช้ประโยชน์จากระบบเครือข่ายคอมพิวเตอร์ที่พัฒนาขึ้นมาจนกลายเป็นลักษณะหนึ่งของการสงครามสมัยใหม่ (Modern Warfare) แต่ในท้ายที่สุด กองกำลัง NATO ได้ยกเลิกแผนการนี้ไปเพราะหวั่นเกรงถึงปัญหาข้อกฎหมายในเรื่องผลกระทบต่อพลเรือน (Collateral Damage)

เมื่อวันที่ 6 กันยายน ค.ศ. 2007 กองทัพของอิสราเอลใช้วิธีการที่คล้ายการฝังข้อมูลที่ไม่ถูกต้อง ในระหว่างการโจมตีทางอากาศ (Operation Orchard) โจมตีต่อโรงงานผลิตนิวเคลียร์ในซีเรีย โดยอ้างว่าซีเรียเป็นภัยคุกคามต่ออิสราเอลจากการสร้างโรงงานผลิตนิวเคลียร์ซึ่งออกแบบและควบคุมโดยเกาหลีเหนือ แหล่งข่าวของรัฐบาลอิสราเอลระบุว่าสถานที่นั้นเป็นโรงงานผลิตอาวุธ

---

[43] Martin C. Libicki, *What Is Information Warfare?*(National Defense University, 1995). P. 77.

[44] William M. Arkin, "The Cyber Bomb in Yugoslavia," washingtonpost.com, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm. [July 7, 2015]

นิวเคลียร์ที่ออกแบบและควบคุมโดยเกาหลีเหนือ โดยเครื่องบินของอิสราเอลสามารถเข้าถึงเป้าหมายได้โดยไม่ถูกตรวจพบ เนื่องจากการโจมตีทางไซเบอร์ที่ได้กระทำการก่อนการโจมตีทางอากาศก่อกวนการทำงานของระบบป้องกันทางอากาศของซีเรียทำให้ไม่แสดงผลความผิดปกติใดๆ บนจอเรดาร์ น่านฟ้าซีเรียจึงดูเหมือนปลอดภัยและดูว่างเปล่าบนจอแสดงผล แต่ความจริงแล้ว ฝูงบินที่ประกอบด้วยอากาศยานอีเกิลและฟัลคอนบินแทรกซึมผ่านน่านฟ้าซีเรียเข้ามาจากทางตุรกีซึ่งเครื่องบินเหล่านี้ออกแบบและสร้างขึ้นเป็นครั้งแรกในทศวรรษที่ 1970 ไม่มีความสามารถในการล่องหนหรือหลีกเร้นจากการตรวจจับของเรดาร์ โครงสร้างของเครื่องบินทำจากไทเทเนียมและเหล็กกล้า มีขอบมุมที่แหลมคมและมีระเบิดและจรวดนำวิถีติดตั้งไว้ใต้ปีกเครื่องบินควรทำให้เกิดจุดสว่างบนจอตรวจจับเรดาร์ของซีเรีย แต่กลับไม่มีวี่แววปรากฏใดๆ แม้รายละเอียดของวิธีการในการโจมตีดังกล่าวจะไม่เป็นที่ปรากฏ แต่เห็นได้ชัดว่าอิสราเอลกระทำการป้อนข้อมูลเท็จลงในระบบตรวจจับเรดาร์ป้องกันทางอากาศเป็นเหตุให้ระบบเรดาร์แสดงผลการตรวจจับว่าไม่มีสิ่งปกติในน่านฟ้าในคืนที่มีการโจมตีทางอากาศเกิดขึ้น[45]

ซีเรียสรุปว่า ในคืนที่มีการโจมตีด้วยการทิ้งระเบิดของกองทัพอากาศอิสราเอล เครือข่ายระบบป้องกันทางอากาศถูกควบคุมดยอิสราเอล ทำให้จรวดนำวิถีต่อต้านอากาศยานเพื่อป้องกันทางอากาศของซีเรียไม่สามารถระดมยิงได้ เพราะไม่มีเป้าหมายในระบบให้จรวดนำวิถีต่อต้านอากาศยานออกไปค้นหา ฝูงบินป้องกันน่านฟ้าของซีเรียจึงไม่สามารถทะยานขึ้นเพื่อป้องกันน่านฟ้าของซีเรียได้ เนื่องจากระบบป้องกันทางอากาศของซีเรียที่สร้างโดยรัสเซียจำเป็นจะต้องอาศัยระบบควบคุมภาคพื้นดินคอยป้อนเส้นสมมุติที่ลากไปยังเครื่องบินเป้าหมายก่อนจึงจะทำงานได้ แต่กองบัญชาการควบคุมภาคพื้นดินของซีเรียไม่เห็นเป้าหมายที่ว่านั้นแม้แต่เป้าหมายเดียว[46]

2.1.2.3 การแทรกซึมความปลอดภัยทางเครือข่ายคอมพิวเตอร์

การแทรกซึมความปลอดภัยทางเครือข่ายคอมพิวเตอร์ (Infiltrating a Secure Computer Network) เป็นอีกรูปแบบหนึ่งของการโจมตีทางไซเบอร์ที่นำมาใช้ในสถานการณ์การขัดกันทางอาวุธ ตัวอย่าง การโจมตีทางไซเบอร์ด้วยการแทรกซึมความปลอดภัยทางเครือข่ายคอมพิวเตอร์ เช่น การโจมตีด้วยสตักซ์เน็ต การแทรกซึมระบบอีเมลล์

---

[45] Richard A Clarke and Robert K Knake, Cyber War: The Next Threat to National Security and What to Do About It(HarperCollins, 2010). P. 5.

[46] Ibid. P. 9.

สตักซ์เน็ต (Stuxnet) ถือเป็นอาวุธไซเบอร์ที่ออกแบบเพื่อใช้ในการทำลายเป้าหมายทางทหาร โดย Ralph Lagner ผู้เชี่ยวชาญด้านความปลอดภัยคอมพิวเตอร์ชาวเยอรมัน อธิบายว่า สตักซ์เน็ตเป็นโปรแกรมที่เป็นอันตรายที่สุดซึ่งมีความซับซ้อนและพัฒนาขึ้นสำหรับการโจมตีเป้าหมายที่กำหนดอย่างเฉพาะเจาะจง รวมทั้งเป็นขีปนาวุธไซเบอร์ทางการทหารอย่างแม่นยำที่ใช้เพื่อการโจมตีทางไซเบอร์[47] Michael V. Hayden อดีตผู้อำนวยการหน่วยสืบราชการลับ (Central Intelligence Agency - CIA) และสภาความมั่นคงแห่งชาติของสหรัฐอเมริกา (National Security Agency - NSA) กล่าวว่า สตักซ์เน็ตเป็นการโจมตีทางไซเบอร์ครั้งแรกที่ถูกนำมาใช้เพื่อก่อให้เกิดความเสียหายทางกายภาพ (Physical Damage)[48]

สตักซ์เน็ตเป็นมัลแวร์ (Malware)[49] ชนิดหนึ่งที่ถูกค้นพบครั้งแรกเมื่อปี ค.ศ. 2010 โดยบริษัทรักษาความปลอดภัยคอมพิวเตอร์ที่ชื่อ ไวรัสบล็อกเอดา ในประเทศเบลารุส ซึ่งสตักซ์เน็ตออกแบบมาเพื่อโจมตีทำลายระบบควบคุมและประเมินผลแบบศูนย์รวม (Supervisory Control and Data Acquisition-SCADA) ที่ผลิตโดยบริษัทเยอรมัน Siemens AG. ซึ่งระบบดังกล่าวมักใช้ในการควบคุมและดูแลกระบวนการและระบบในโรงงานอุตสาหกรรมและโครงสร้างพื้นฐานสาธารณูปโภคหลักต่างๆ อาทิ ระบบควบคุมท่อส่งน้ำมัน และโรงงานผลิตกระแสไฟฟ้าพลังงานนิวเคลียร์ กล่าวได้ว่า สตักซ์เน็ตเป็นมัลแวร์ที่ออกแบบให้มุ่งโจมตีระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) โดยเฉพาะ[50]

การโจมตีของสตักซ์เน็ต (Stuxnet) ถูกออกแบบมาเพื่อแทรกซึมระบบและมีความสามารถในการควบคุมระบบจากระยะไกลในรูปแบบกึ่งอิสระและยังปิดบังการเปลี่ยนแปลง

---

[47] Mark Clayton, "Stuxnet Malware Is 'Weapon' out to Destroy ... Iran's Bushehr Nuclear Plant? ," http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant. [April 7, 2016]

[48] David E. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran," The New Yoek Times, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0. [April 7, 2016]

[49] Malware (มัลแวร์) ย่อมาจาก Malicious Software หมายถึง โปรแกรมคอมพิวเตอร์ใดๆ ที่เป็นอันตรายต่อคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ อาทิ ไวรัส (Virus) หนอนคอมพิวเตอร์ (Worm) โทรจัน (Trojan Horse) สตักซ์เน็ต (Stuxnet) สปายแวร์ (Spyware)

[50] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," *John Marshall Journal Of Computer & Information Law* 29, no. 1 (2011). P. 11.

ที่เกิดขึ้นกับระบบได้ โดยสตักซ์เน็ตจะแพร่กระจายผ่านทางอุปกรณ์ที่ใช้ในการเก็บข้อมูลหรือไฟล์จากคอมพิวเตอร์ (USB Thumb Drive) และใช้ประโยชน์จากช่องโหว่ของระบบปฏิบัติการ Microsoft Windows เพื่อเข้าไปควบคุมระบบก่อนจากนั้นจึงทำลายระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) เนื่องจากระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ส่วนใหญ่ไม่ได้เชื่อมต่อกับอินเทอร์เน็ต แต่มี USB Port เป็นช่องทางในการเชื่อมต่อและสื่อสารระหว่างคอมพิวเตอร์กับอุปกรณ์ภายนอกอื่นๆ เมื่อระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ติดเชื้อสตักซ์เน็ตเรียบร้อยแล้ว สตักซ์เน็ตจะทำการจัดเตรียมการติดต่อสื่อสารกับคอมพิวเตอร์ควบคุมจากระยะไกล (A Remote Server Computer) อย่างรวดเร็วซึ่งทำให้สามารถใช้สตักซ์เน็ตในการขโมยข้อมูลหรือควบคุมระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) [51] ทั้งนี้ สตักซ์เน็ตไม่ได้ถูกออกแบบมาให้สร้างความเสียหายหรือก่อให้เกิดความไม่สะดวกในการใช้งานในทันที แต่จะสร้างความเสียหายเป็นระยะเวลาต่อเนื่องตราบเท่าที่สตักซ์เน็ตยังคงไม่ถูกตรวจพบ ผู้โจมตีสามารถขโมยข้อมูล ทำให้ระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) หยุดการผลิตชั่วคราว เป็นอันตรายต่อระบบความปลอดภัยหรืออาจเป็นสาเหตุทำให้อุปกรณ์เสียหายหรือทำให้ผู้คนได้รับบาดเจ็บตามวัตถุประสงค์ของผู้โจมตี[52]

ในช่วงปลายปีค.ศ. 2009 หรือต้นปีค.ศ. 2010 Stuxnet ถูกปล่อยออกมาให้โจมตีโรงงานนิวเคลียร์ ในเมือง Natanz และ Bashir ของอิหร่านทำลายเครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์ (IR-1 Centrifuges) กว่า 1,000 เครื่อง จนเป็นเหตุให้การทำงานของเครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์เพื่อปรับปรุงคุณภาพยูเรเนียม (Uranium Enrichment) ต้องหยุดชะงักไปอย่างไม่มีกำหนด เนื่องจากปัญหาทางเทคนิคหลายประการที่เกิดขึ้นจากการทำลายของสตักซ์เน็ต สันนิษฐานว่าสตักซ์เน็ตเข้าสู่คอมพิวเตอร์ในโรงงานนิวเคลียร์ของอิหร่านผ่านทาง USB ที่ติดเชื้อเชื่อมต่อเข้าสู่เป้าหมาย เนื่องจากระบบควบคุมของโรงงานนิวเคลียร์ไม่ได้เชื่อมต่อกับอินเตอร์เน็ตจึงอาจเป็นไปได้ที่บุคลากรเจ้าหน้าที่ของโรงงานนิวเคลียร์เมือง Natanz จะนำสตักซ์เน็ตเข้าสู่ระบบควบคุมโดยไม่รู้ตัว หลังจากที่ใช้ USB กับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ติดเชื้อและคอมพิวเตอร์ของ

---

[51] Reuters, "Factbox: What Is Stuxnet?," http://www.reuters.com/article/us-security-cyber-iran-fb-idUSTRE68N3PT20100924. [April 7, 2016]

[52] Stacy Combest, "Building a Cyber Secure Plant," Siemens totally integrated automation, http://www.totallyintegratedautomation.com/2010/09/building-a-cyber-secure-plant/. [April 7, 2016]

โรงงาน[53] ซึ่งสตักซ์เน็ตดังกล่าวถูกออกแบบให้พยายามหาเป้าหมายสุดท้ายและสร้างความเสียหาย โดยทำให้เกิดการเปลี่ยนแปลงอย่างรวดเร็วของความเร็วในการหมุนรอบของมอเตอร์และทำลายการทำงานปกติของระบบควบคุม[54] โดยทางการอิหร่านออกมายอมรับว่า อิหร่านประสบปัญหาเกี่ยวกับอุปกรณ์ที่ใช้ในโครงการและสตักซ์เน็ตอาจจะเป็นสาเหตุของปัญหาดังกล่าว[55] ทั้งนี้ ไม่มีฝ่ายใดออกมาแสดงความรับผิดชอบต่อเหตุการณ์ไซเบอร์ที่เกิดขึ้น รวมทั้งในการตรวจสอบทางคอมพิวเตอร์ก็ไม่สามารถปรับความรับผิดให้แก่ฝ่ายใดได้ อย่างไรก็ตาม ประธานาธิบดีอิหร่าน Mahmoud Ahmadinejad กล่าวหาว่าประเทศอิสราเอลและประเทศทางตะวันตกอยู่เบื้องหลังการโจมตีทางไซเบอร์นี้[56]

การโจมตีด้วยสตักซ์เน็ตเป็นตัวอย่างรูปแบบของการโจมตีทางไซเบอร์ด้วยการแทรกซึมความปลอดภัยทางเครือข่ายคอมพิวเตอร์เพื่อก่อให้เกิดความเสียหายแก่เป้าหมายอย่างเฉพาะเจาะจง อย่างไรก็ตาม การโจมตีทางไซเบอร์รูปแบบการแทรกซึมความปลอดภัยทางเครือข่ายคอมพิวเตอร์ไม่จำเป็นที่จะต้องเป็นการทำลายเครือข่ายคอมพิวเตอร์หรือโครงสร้างพื้นฐานเสมอไป

ในปี ค.ศ. 2003 สหรัฐอเมริกาทำการแทรกซึมระบบอีเมลล์ของกระทรวงกลาโหมประเทศอิรัก เพื่อติดต่อกับเจ้าหน้าที่ของอิรักด้วยการส่งข้อความคำสั่งให้ทำการยอมแพ้อย่างสันติ ซึ่งเห็นได้ว่าข้อความดังกล่าวเป็นผลสำเร็จจากการที่กองกำลังทหารอเมริกันพบเจออุปกรณ์ทางการทหารถูกจัดเรียงทิ้งไว้ในลักษณะสอดคล้องตามข้อความที่ระบุในอีเมลล์[57] การโจมตีทางไซเบอร์รูปแบบดังกล่าวเป็นการโจมตีด้วยการควบคุมและบังคับบัญชา หมายความรวมถึงการโจมตีใดๆ ที่เป็นการแทรกแซงความสามารถในการควบคุมและบังคับบัญชาของกำลังทหารของศัตรู

---

[53] Paul Brannan David Albright, and Christina Walrond,, "Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?," Preliminary Assessment(2010). [October 8, 2015]

[54] William J. Broad and David E. Sanger, "Worm Was Perfect for Sabotaging Centrifuges," The New York Times, http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?_r=0. [April 7, 2016]

[55] Reuters, "Iran Says Cyber Foes Caused Centrifuge Problems," http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129. [April 8, 2016]

[56] ibid.

[57] Rebecca Crootof Oona A. Hathaway, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel,, "The Law of Cyber-Attack," *California Law Review* 100(2012). P. 24.

จากการศึกษารูปแบบของการโจมตีทางไซเบอร์ที่เกิดขึ้นทั้งในสถานการณ์ปกติและในสถานการณ์การขัดกันทางอาวุธข้างต้น จะเห็นได้ว่า การพัฒนาทางเทคโนโลยีถูกนำมาใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์หลากหลายรูปแบบ ทั้งรูปแบบที่ไม่มีความซับซ้อนและไม่ต้องอาศัยความรู้ทางเทคโนโลยีมากนัก เช่น การโจมตีทางไซเบอร์โดยการทำให้ระบบปฏิเสธการให้บริการ (DDOS) ไปจนถึงรูปแบบการโจมตีที่มีความยุ่งยากและซับซ้อนจำต้องอาศัยความก้าวหน้าทางเทคโนโลยีและความสามารถของผู้ออกแบบหรือผู้โจมตีเป็นอย่างมาก เช่น การโจมตีด้วยสตักซ์เน็ต

นอกจากนี้ การโจมตีทางไซเบอร์มีทั้งรูปแบบที่สามารถกำหนดเป้าหมายในการโจมตีได้อย่างเฉพาะเจาะจงและรูปแบบที่โจมตีต่อเป้าหมายทั่วไปอย่างไม่เฉพาะเจาะจง โดยการโจมตีทางไซเบอร์ที่เกิดขึ้นในสถานการณ์การขัดกันทางอาวุธที่ผ่านมาพบทั้งการโจมตีทางไซเบอร์ร่วมกับการโจมตีด้วยอาวุธตามแบบเพื่อสนับสนุน ช่วยเหลือให้ปฏิบัติการโจมตีด้วยอาวุธตามแบบบรรลุผล เช่น การโจมตีทางไซเบอร์ต่อระบบป้องกันทางอากาศของประเทศซีเรียที่ดำเนินการร่วมกับการโจมตีทางอากาศต่อโรงงานผลิตนิวเคลียร์ และการโจมตีทางไซเบอร์ต่อระบบเป้าหมายซึ่งมีวัตถุประสงค์ให้ระบบเป้าหมายเสียหาย โดยไม่มีรายงานการโจมตีด้วยอาวุธร่วมด้วย เช่น การโจมตีด้วยสตักซ์เน็ตต่อระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ที่ควบคุมการทำงานภายในโรงงานนิวเคลียร์ของประเทศอิหร่าน

เหตุการณ์ไซเบอร์เหล่านี้ แสดงให้เห็นอย่างชัดเจนว่าการโจมตีทางไซเบอร์หรืออาวุธไซเบอร์ซึ่งใช้เพียงปลายนิ้วสัมผัสเครื่องคอมพิวเตอร์ไม่ได้เป็นเพียงนิยายวิทยาศาสตร์หรือจินตนาการทางวิทยาศาสตร์ในอนาคตอีกต่อไป การพัฒนาเทคโนโลยีทางไซเบอร์ก่อให้เกิดวิธีการและปัจจัยในการสู้รบใหม่ที่สร้างความเสียหายได้เช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ ด้วยเหตุนี้ หลายประเทศจึงหันมาให้ความสำคัญกับประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเตรียมตัวรับมือกับสงครามไซเบอร์ที่อาจเกิดขึ้นในอนาคต ซึ่งผู้เขียนจะได้ศึกษาความพยายามในทางระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ทั้งในระดับรัฐ ความร่วมมือระหว่างประเทศระดับทวิภาคีและพหุภาคี ในส่วนต่อไป

2.2 ความพยายามในทางระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

จากการศึกษาส่วนที่ผ่านมา จะเห็นได้ชัดเจนว่า นอกจากความเสียหายที่เกิดขึ้นแก่ฝ่ายที่เป็นปรปักษ์ในการสู้รบแล้ว การโจมตีทางไซเบอร์ที่เกิดขึ้นยังก่อให้เกิดผลกระทบและสร้างความเสียหายให้แก่โครงสร้างพื้นฐานที่สำคัญของรัฐและทำให้พลเรือนได้รับผลกระทบจากการที่ไม่สามารถใช้งานโครงสร้างพื้นฐานเหล่านั้นอีกด้วย จากเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นได้ยกระดับความกังวลของรัฐเกี่ยวกับภัยคุกคามจากการโจมตีทางไซเบอร์และการเกิดสงครามไซเบอร์

จากการศึกษารายงานของสถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติ (United Nations Institute for Disarmament Research: UNIDIR) ในการศึกษาเบื้องต้นเกี่ยวกับนโยบายและการจัดระบบของประเทศสมาชิกองค์การสหประชาชาติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสงครามไซเบอร์[58] และรายการไซเบอร์เกี่ยวกับแนวโน้มและความเป็นจริงของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างประเทศ[59] โดยพิจารณาจากแหล่งข้อมูลที่เปิดเผยต่อสาธารณชนของรัฐ จากสื่อสารสนเทศระดับชาติ แหล่งข้อมูลตีพิมพ์ของรัฐบาลหรือในบางกรณีมาจากรายงานของรัฐบาลต่อองค์การระหว่างประเทศ[60] แสดงให้เห็นว่า ประเทศทั่วทุกภูมิภาคมีการริเริ่มในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยประเด็นเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธและสงครามไซเบอร์ถือเป็นประเด็นหนึ่งที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วยเช่นกันสะท้อนจากการกำหนดแผนการทางทหารหรือกองกำลังทางทหารสำหรับกิจกรรมไซเบอร์โดยเฉพาะ การจัดสรรงบประมาณในการพัฒนาศักยภาพด้านไซเบอร์ของทางการทหาร รวมทั้งความร่วมมือระหว่างประเทศเพื่อพัฒนาความสามารถในการป้องกันและรับมือกับการโจมตีทางไซเบอร์และสงครามไซเบอร์

ในส่วนนี้จะได้ศึกษาความพยายามในทางระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันเป็นการขับเคลื่อนทั้งในระดับรัฐ ความร่วมมือระหว่างประเทศ

---

[58] Center for Strategic and International Studies, "Preliminary Assessment of National Doctrine and Organization: Cybersecurity and Cyberwarfare,"(UNIDIR Resources Paper, 2011).

[59] UNIDIR, "The Cyber Index: International Security Trends and Realities,"(Geneva, Switzerland: United Nations, 2013).

[60] Ibid. P. 1.

ระดับทวิภาคีและระดับพหุภาคี เพื่อให้เห็นมุมมองของประชาคมโลกที่มีต่อการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธต่อไป

2.2.1 แนวทางของรัฐในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

จากเหตุการณ์การโจมตีทางไซเบอร์ที่ผ่านมาส่งผลให้รัฐต่างๆ ตระหนักในความสามารถของการใช้เทคโนโลยีทางไซเบอร์ในปฏิบัติการทางทหารและการสู้รบเพิ่มมากขึ้นและกำหนดแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อสร้างความเชื่อมั่นในความมั่นคงปลอดภัยของการดำเนินกิจกรรมใดๆ ในห้วงไซเบอร์ จากการศึกษาพบแนวทางของรัฐในการรับมือกับการโจมตีทางไซเบอร์และสงครามไซเบอร์ที่หลากหลาย ดังนี้

2.2.1.1 การกำหนดแผนพัฒนาขีดความสามารถทางไซเบอร์ในเชิงรุกหรือเชิงรับ

ด้วยศักยภาพของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ส่งผลให้หลายประเทศหันมาพัฒนาขีดความสามารถทางไซเบอร์ทั้งเชิงรุกหรือเชิงรับ (Defence and Offensive Capacibility) ในทางทหารขึ้นโดยเฉพาะโดยการพัฒนาขีดความสามารถทางไซเบอร์ผสมผสานเข้ากับกลยุทธ์ในการสู้รบแบบดั้งเดิม อาทิ

ประเทศแอลเบเนียมีความเห็นว่าการโจมตีทางไซเบอร์เป็นภัยคุกคามที่เกิดขึ้นใหม่ โดยในปีค.ศ. 2010 กระทรวงกลาโหมแอลเบเนียจัดตั้งศูนย์ปฏิบัติการสถาบันการเดินเรือนานาชาติเพื่อรับผิดชอบการควบคุมน่านฟ้า และการพัฒนาขีดความสามารถในการป้องกันไซเบอร์[61]

ประเทศเดนมาร์กกำหนดความตกลงเกี่ยวกับการป้องกันประเทศประจำปี ค.ศ. 2013-2017 จัดตั้งศูนย์ความมั่นคงปลอดภัยทางไซเบอร์ภายใต้กระทรวงกลาโหมรวมทั้ง

[61] ibid.

การเสริมสร้างขีดความสามารถทางการทหารในปฏิบัติการทางเครือข่ายคอมพิวเตอร์เพื่อเตรียมศักยภาพในการดำเนินปฏิบัติการทางทหารทั้งเชิงรุกและเชิงรับภายในห้วงไซเบอร์[62]

ประเทศเอสโตเนียกำหนดให้กระทรวงกลาโหมและกองกำลังป้องกันตนเองมีหน้าที่รับผิดชอบในการประสานงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในงานด้านการป้องกันแห่งชาติและการพัฒนาขีดความสามารถทางไซเบอร์[63]

2.2.1.2 การกำหนดหลักนิยมและยุทธศาสตร์ทางการทหาร

จากความสำคัญของการนำเทคโนโลยีทางไซเบอร์มาใช้ในการทหารทำให้รัฐต่างๆ หันมาปรับหลักนิยมและยุทธศาสตร์ทางการทหารของรัฐและกำหนดให้การโจมตีทางไซเบอร์หรือสงครามไซเบอร์เป็นภัยคุกคามต่อความมั่นคงของรัฐรูปแบบหนึ่ง อาทิ

ประเทศเบลารุสกำหนดหลักนิยมทางการทหารระบุว่า ความขัดแย้งทางไซเบอร์หรือสงครามไซเบอร์เป็นการเผชิญหน้าทางข้อมูลสารสนเทศ (Information Confrontation) ซึ่งเห็นว่าสงครามไซเบอร์มีศักยภาพที่จะเป็นหนึ่งในภัยคุกคามจากภายนอกรัฐ องค์ประกอบใหม่ของกองกำลังทางทหารรวมถึงกองกำลังปฏิบัติการพิเศษจะต้องสร้างขึ้นเพื่อรับมือกับภัยคุกคามและท้าทายใหม่ของการโจมตีทางไซเบอร์นี้[64] และมุ่งเน้นไปที่การบรรเทาความเสี่ยงภัยจากห้วงไซเบอร์ด้านความมั่นคงปลอดภัยทางทหาร เพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพในสมรภูมิรบใหม่ โดยทางการทหารจะพัฒนาขีดความสามารถด้านไซเบอร์สำหรับการป้องกันทางไซเบอร์และแจ้งเตือนการโจมตีทางไซเบอร์ล่วงหน้า ตลอดจนกองกำลังทางทหารมีหน้าที่รับผิดชอบในการสร้างมั่นใจด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในเวลาสงคราม

ประเทศบราซิลกำหนดยุทธศาสตร์การป้องกันแห่งชาติซึ่งประกาศในเดือนธันวาคม ปีค.ศ. 2008 ระบุว่า เทคโนโลยีทางไซเบอร์เป็นภาคเชิงยุทธศาสตร์สำหรับการป้องกันประเทศ

---

[62] Carmen-Cristina Cirlig, "Cyber Defence in the Eu: Preparing for Cyber Warfare?,"(European Parliament, European Union, October 2014). P. 16.

[63] ibid.

[64] Belarus News, "Belarusian Army to Combat Cyber Threats," Belarusian Telegraph Agency, http://eng.belta.by/society/view/belarusian-army-to-combat-cyber-threats-24388-2011. [April 14, 2016]

โดยยุทธศาสตร์ดังกล่าวเรียกร้องให้จัดตั้งองค์กรที่ทำขึ้นเพื่อยกระดับขีดความสามารถทางไซเบอร์ในภาคอุตสาหกรรมและการทหาร[65] ยุทธศาสตร์ดังกล่าวยังให้ความสำคัญเป็นพิเศษกับขีดความสามารถทางไซเบอร์และเทคโนโลยีที่พึ่งพาตนเองได้ โดยเทคโนโลยีที่ถือว่ามีความสำคัญอย่างยิ่งตามแผนยุทธศาสตร์คือเทคโนโลยีที่ใช้ในเรือดำน้ำและระบบอาวุธ นอกจากนี้ ประเทศบราซิลวางแผนที่จะพัฒนาขีดความสามารถทางไซเบอร์ โดยการสร้างศักยภาพในสถาบันการศึกษาและในกิจการทหารเพื่อเพิ่มช่องทางการติดต่อสื่อสารระหว่างหน่วยบัญชาการรบ[66]

ประเทศลิทัวเนียกำหนดหลักนิยมทางการทหารจัดให้ห้วงไซเบอร์เป็นสภาพแวดล้อมในการสู้รบและกำหนดให้การโจมตีทางไซเบอร์อย่างรุนแรงเป็นภัยคุกคามที่อาจเกิดขึ้นได้กับประเทศ[67] โดยในปีค.ศ. 2015 ประเทศลิทัวเนียดำเนินการจัดตั้งศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อเตรียมการสำหรับปฏิบัติการไซเบอร์ต่างๆ และเตรียมความพร้อมในการป้องกันตนเองจากการโจมตีทางไซเบอร์[68]

ประเทศยูเครนกำหนดบทบาททางทหารในการจัดการกับภัยคุกคามทางไซเบอร์ไว้ในสมุดปกขาว เมื่อเดือนมิถุนายน ปีค.ศ. 2012 สภาความมั่นคงและกลาโหมแห่งชาติของยูเครน (National Security and Defence Council of Ukraine) เห็นชอบในการกำหนดหลักนิยมทางทหารใหม่ระบุว่า ประเทศยูเครนจะพิจารณาการโจมตีทางไซเบอร์ต่อโรงงานนิวเคลียร์ อุตสาหกรรมเคมีและการป้องกัน พัสดุทางทหาร งเศรษฐกิจและข้อมูลสารสนเทศว่าเป็นพื้นฐานสำหรับสถานการณ์การขัดกันทางอาวุธ[69]

---

[65] The News Desk, "Brazilian Army Prepares Its Cdciber, the 'Cyber Defense Center'," Linha Defensiva, http://www.linhadefensiva.com/2012/05/brazilian-army-prepares-its-cdciber-the-cyber-defense-center/. [April 14, 2016]

[66] Brazilian Ministry of Defence, "National Strategy of Defense: Peace and Security for Brazil.,"(Ministry of Defense, 2008).

[67] Chief of Defence of the Republic of Lithuania, "Lithuanian Military Doctrine,"(2010).

[68] Carmen-Cristina Cirlig, "Cyber Defence in the Eu: Preparing for Cyber Warfare?,"(European Parliament, European Union, October 2014) P. 7.

[69] UNIDIR, "The Cyber Index: International Security Trends and Realities,"(Geneva, Switzerland: United Nations, 2013). P. 49.

2.2.1.3 การจัดตั้งหน่วยบัญชาการหรือกองกำลังไซเบอร์

แนวทางในการเตรียมตัวรับมือกับภัยคุกคามของสงครามไซเบอร์ของรัฐที่พบมากที่สุดคือ การจัดตั้งหน่วยบัญชาการหรือกองกำลังทหารทางไซเบอร์เพื่อรับมือกับการโจมตีทางไซเบอร์หรือสงครามไซเบอร์ขึ้น โดยจัดสรรบุคลากรทางการทหารให้ทำหน้าที่เสมือนทหารซึ่งทำการสู้รบในสนามรบเสมือนจริง (Virtual Battlefield) โดยมีทั้งที่ปฏิบัติหน้าที่ร่วมกับหน่วยงานข่าวกรองอื่นๆ และจัดตั้งเป็นหน่วยงานใหม่ภายในโครงสร้างทางการทหารมีหน้าที่เกี่ยวกับกิจกรรมด้านไซเบอร์โดยเฉพาะและมีภารกิจหลักในการป้องกันเครือข่ายทางการทหารและการปฏิบัติการทางทหารในห้วงไซเบอร์ อาทิ

ประเทศอาร์เจนตินาจัดตั้งหน่วยงานทางทหารที่ปฏิบัติภารกิจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ โดยหน่วยงานทางทหารของอาร์เจนตินาระบุว่าความสามารถในการทำสงครามสารสนเทศ (Information Warfare) จะต้องประกอบด้วยมาตรการเชิงรับในการป้องกันเครือข่ายภายในและมาตรการเชิงรุกในการขัดขวางเหล่าข้าศึกศัตรู[70] กำหนดให้หน่วยบัญชาการระบบคอมพิวเตอร์และการสื่อสารของกองทัพอาร์เจนตินา (The Argentine Army's Communications and Computing Systems Command) รวมถึงกองกำลังวิทยาศาสตร์คอมพิวเตอร์ (Computer Science Troops) ทำหน้าที่ครอบคลุมถึงปฏิบัติการทางไซเบอร์ประจำสมรภูมิรบในห้วงไซเบอร์[71]

ประเทศออสเตรียไม่ได้คาดการณ์ว่าการโจมตีทางทหารตามแบบ (Conventional Military Attack) จะเป็นภัยคุกคามที่สำคัญในอนาคตอีกต่อไปและมุ่งความสนใจไปที่การป้องกันความมั่นคงปลอดภัยทางไซเบอร์ และก่อตั้งโครงสร้างการป้องกันไซเบอร์ที่ประกอบไปด้วยทหาร 1,600 นาย โดยองค์กรข่าวกรองทางทหารของออสเตรียระบุว่า การป้องกันอิเล็กทรอนิกส์รวมทั้งการป้องกันมัลแวร์เป็นหนึ่งในงานสำคัญของการป้องกันไซเบอร์[72]

---

[70] Javier Ulises Ortiz, "Argentina: The Challenge of Information Operations," *IOSphere* Special Edition(2008). pp. 61-62.

[71] Ibid.

[72] Douglas Perry, "Austria Hires 1600 Soldiers for 'Cyber' Security," Tom's Guide, http://www.tomsguide.com/us/austria-cyber-crime-cyber-defense-secret-service,news-11077.html. [April 14, 2016]

ประเทศบราซิลจัดตั้งศูนย์การสื่อสารสงครามไซเบอร์เพื่อตอบโต้การโจมตีหลากหลายรูปแบบต่อเครือข่ายทางทหารและมีรายงานว่าศูนย์การสื่อสารสงครามไซเบอร์ (Cyber-Warfare Communications Centre) ซึ่งเป็นส่วนหนึ่งของศูนย์ป้องกันไซเบอร์ (Centre of Cyber Defence) ทำการสั่งซื้อโปรแกรมจำลองไวรัสและการโจมตีทางไซเบอร์เพื่อวัตถุประสงค์ในการฝึกทหารโดยเฉพาะ[73]

ประเทศแคนาดาจัดตั้งกลุ่มกองกำลังทางทหารให้ทำหน้าที่จัดการข้อมูลสารสนเทศเพื่อการป้องกันคอมพิวเตอร์และเครือข่ายการติดต่อสื่อสารของกองกำลังทางทหารโดยเฉพาะ ซึ่งในเดือนมิถุนายนปีค.ศ. 2011 ประเทศแคนาดาจัดตั้งกรมไซเบอร์เนติกส์ (The Directorate of Cybernetics) ที่มีภารกิจหลักเพื่อสร้างขีดความสามารถในการทำสงครามไซเบอร์ให้กับกองกำลังทางทหารของแคนาดาโดยเฉพาะ[74]

ประเทศอิหร่านประกาศเกี่ยวกับการวางแผนจัดตั้งหน่วยบัญชาการไซเบอร์สำหรับกองกำลังทางทหารเพื่อป้องกันการโจมตีทางไซเบอร์ในเดือนมิถุนายนปีค.ศ. 2011 [75] โดยหน่วยบัญชาการทางทหารของอิหร่านอ้างว่า หน่วยบัญชาการไซเบอร์ของอิหร่านเป็นกองทัพไซเบอร์ที่มีขนาดใหญ่เป็นอันดับสองของโลก[76]

ประเทศญี่ปุ่นให้ความสำคัญกับกิจกรรมไซเบอร์ในฐานะเป็นการพัฒนาของการสงครามแบบใหม่และอธิบายแนวโน้มเกี่ยวกับขีดความสามารถสงครามไซเบอร์ปรากฏตามรายงานสมุดปกขาวในปี 2010 โดยวางแผนจัดตั้งหน่วยป้องกันไซเบอร์ที่ประกอบด้วยสมาชิกจำนวน

---

[73] SecurityWeek News, "Cyberwarfare Brazilian Army to Get Cyberwarfare Training and Security Support from Panda Security," http://www.securityweek.com/brazilian-army-get-cyberwarfare-training-and-security-support-panda-security. [April 14, 2016]

[74] UNIDIR, "The Cyber Index: International Security Trends and Realities,"(Geneva, Switzerland: United Nations, 2013). P. 15.

[75] Xinhua, "Iran's Armed Forces to Launch 'Cyber Command'," China Daily, http://www.chinadaily.com.cn/world/2011-06/16/content_12707489.htm. [April 14, 2016]

[76] ExecutiveBiz, "Iranian Cyber Army Second-Largest in the World, Claims Iranian Commander," http://blog.executivebiz.com/2010/05/iranian-cyber-army-second-largest-in-the-world-claims-iranian-commander/. [April 14, 2016]

กว่า 100 คนในปีค.ศ. 2013 ซึ่งปัจจุบันกองกำลังป้องกันตนเองของญี่ปุ่นมีทั้งสิ้น 4 หน่วยงาน จำนวนสมาชิกกว่า 360 คนทำหน้าที่รับผิดชอบในการป้องกันระบบคอมพิวเตอร์ทางทหาร[77]

ประเทศสาธารณรัฐเกาหลีจัดตั้งหน่วยบัญชาการสงครามไซเบอร์อิสระทำหน้าที่รับผิดชอบในปฏิบัติการทั้งเชิงรุกและเชิงรับในห้วงไซเบอร์ภายใต้กระทรวงกลาโหมของสาธารณรัฐเกาหลี[78] โดยวางแผนพัฒนาอาวุธสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับรวมทั้งเพิ่มบุคลากรในหน่วยบัญชาการสงครามไซเบอร์ (Cyber Warfare Command) และมีเป้าหมายที่จะเพิ่มบุคลากรให้ได้จำนวนกว่า 1,000 คน[79]

ประเทศรัสเซียประกาศการพิจารณาจัดตั้งหน่วยบัญชาการความมั่นคงปลอดภัยทางไซเบอร์เพื่อป้องกันข้อมูลสารสนเทศสำหรับกองกำลังทางทหารโดยเฉพาะ ในเดือนมีนาคม ปีค.ศ. 2012[80]

ประเทศสหรัฐอเมริกาให้ความสำคัญกับการพัฒนาทางไซเบอร์เป็นอย่างมาก โดยกระทรวงกลาโหมของสหรัฐอเมริกาออกมายอมรับอย่างเป็นทางการว่า ระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตในห้วงไซเบอร์ (Cyberspace) เป็นรูปแบบสงครามแขนงใหม่ที่กลายเป็นวิกฤตอันตรายต่อปฏิบัติการทหาร[81]

นายลีออน พาเนตตา รัฐมนตรีว่าการกระทรวงกลาโหมของสหรัฐฯ ออกมาเตือนว่าประเทศสหรัฐอเมริกากำลังเผชิญกับความเป็นไปได้ที่จะเกิดสงครามไซเบอร์ เพิร์ล ฮาเบอร์ (Cyber-Pearl Harbor) และมีความเสี่ยงมากขึ้นที่จะถูกโจมตีจากกลุ่มแฮคเกอร์ (Hackers) ต่างชาติที่มีความสามารถในการรื้อถอนระบบพลังงานของประเทศ ระบบการขนส่งคมนาคม ระบบเครือข่ายทาง

---

[77] Japanese Ministry of Defence, "Defense of Japan 2010," ed. Ministry of Defence(2010).

[78] The Chosunilbo, "Cyber Security Is Vital for National Defense," http://english.chosun.com/site/data/html_dir/2009/11/02/2009110200788.html. [April 14, 2016]

[79] UNIDIR, "The Cyber Index: International Security Trends and Realities,"(Geneva, Switzerland: United Nations, 2013). P. 42

[80] RIA Novosti, "Russia Considering Establishing Cyber-Security Command " Atlantic Council, http://www.atlanticcouncil.org/blogs/natosource/russia-considering-establishing-cybersecurity-command. [April 14, 2016]

[81] William J. Lynn III, "Defending a New Domain,"(the Council on Foreign Relations, Foreign Affairs, 2010).

การเงิน และระบบเครือข่ายของรัฐและสามารถทำการโจมตีได้หลายรูปแบบต่อโครงสร้างพื้นฐานที่จำเป็นของสหรัฐในคราวเดียวกันกับการโจมตีทางกายภาพ (Physical Attack) ซึ่งผลลัพธ์โดยรวมของการโจมตีทั้งหมดมีความรุนแรงเป็นดั่งเช่นสงครามเพิร์ล ฮาเบอร์นำมาซึ่งความเสียหายทางด้านชีวิตและทรัพย์สินของประชาชนอาจทำให้ทั้งประเทศเป็นอัมพาตและสั่นสะเทือนความมั่นคงของชาติได้[82]

นายบารัค โอบามา ประธานาธิบดีแห่งสหรัฐอเมริกาให้ความสำคัญกับปฏิบัติการทางไซเบอร์โดยเรียกร้องให้สภาคองเกรสของสหรัฐอเมริกาสนับสนุนร่างกฎหมายด้านความปลอดภัยทางไซเบอร์[83] และจัดตั้งหน่วยบัญชาการไซเบอร์ (The United States Cyber Command - USCYBERCOM) ขึ้นในปีค.ศ. 2010 เพื่อทำหน้าที่จัดการกับภัยคุกคามทางไซเบอร์ต่อโครงสร้างพื้นฐานทางทหารทั้งปฏิบัติการเชิงรุกและเชิงรับ รวมทั้งทำหน้าที่ในการป้องกันทางไซเบอร์แห่งชาติอีกด้วย

2.2.1.4 การกำหนดให้องค์กรพลเรือนทำหน้าที่ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษาพบว่า บางประเทศกำหนดให้หน่วยงานพลเรือนมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยไซเบอร์ภายในประเทศ โดยการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในนาม CERT (Computer Emergency Response Team) CIRT (Computer Incident Response Team) หรือ CSIRT (Computer Security Incident Response Team) อย่างไรก็ตาม หากประเทศเหล่านี้ต้องการที่จะถ่ายโอนศักยภาพในการป้องกันไซเบอร์ของพลเรือนไปสู่ศักยภาพในการป้องกันไซเบอร์ทางทหารก็สามารถทำได้ไม่ยาก[84] อาทิ ประเทศอัฟกานิสถาน อาเซอร์ไบจาน บังคลาเทศ เบลเยียม ภูฏาน บรูไน บัลแกเรีย กัมพูชา ไอร์แลนด์ คูเวต เคนย่า นิวซีแลนด์ ฟิลิปปินส์ เนปาล โมร็อกโก ซาอุดิอาระเบีย สหรัฐอาหรับเอมิเรตส์ เป็นต้น

---

[82] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0. [July 7, 2015]

[83] Barack Obama, "Taking the Cyberattack Threat Seriously," *the Wall Street Journal* (2012). [December 14, 2015]

[84] UNIDIR, "The Cyber Index: International Security Trends and Realities,"(Geneva, Switzerland: United Nations, 2013).

ในส่วนของประเทศไทยกับการเตรียมความพร้อมในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ พบว่า ล่าสุดในปีพ.ศ. 2558 กองทัพไทยมีนโยบายในการจัดตั้งกองสงครามไซเบอร์ เพื่อรับมือกับประเด็นสงครามไซเบอร์ที่ทวีความรุนแรงเพิ่มมากขึ้น โดยกำหนดให้เป็นการป้องกันภัยคุกคามรูปแบบใหม่ทางด้านคอมพิวเตอร์ควบคู่ไปกับการจัดทำยุทธศาสตร์ทางด้านไซเบอร์ของกองทัพ[85] นอกจากนี้ ประเทศไทยยังจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team - ThaiCERT) ภายใต้สังกัดของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยเป็นสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ในภูมิภาคเอเชีย-แปซิฟิค (Asia Pacific Computer Emergency Response Team - APCERT) ด้วย[86]

จากการศึกษาแนวทางของรัฐในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ จะเห็นได้ว่า ความตระหนักในภัยคุกคามต่อความมั่นคงปลอดภัยของรัฐที่เกิดจากการนำเทคโนโลยีมาใช้ในการสู้รบหรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธส่วนใหญ่มุ่งเน้นไปที่การพัฒนาขีดความสามารถด้านไซเบอร์ของกองทัพและการจัดตั้งหน่วยงานทางทหารทำหน้าที่ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นการเฉพาะสะท้อนให้เห็นว่า รัฐต่างๆ เริ่มเตรียมความพร้อมในการเข้าสู่สมรภูมิการรบรูปแบบใหม่ภายในห้วงไซเบอร์อันเป็นสมรภูมิการรบเสมือนจริง (Virtual Battlefield) และแนวโน้มในการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้ในปฏิบัติการทางทหารและการสู้รบเพิ่มมากขึ้น

2.2.2 ความร่วมมือระหว่างประเทศระดับทวิภาคีในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

จากการศึกษา พบว่า ความร่วมมือระหว่างประเทศในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เป็นรูปธรรมยังมีไม่มากนักเมื่อเทียบกับแนวทางของรัฐในการรับมือ

---

[85] เดลินิวส์, "กองทัพเน้นปกป้องสถาบัน ตั้ง"กองสงครามไซเบอร์"สู้ " http://www.dailynews.co.th/politics/355320. [14 ธันวาคม 2558]

[86] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, "เกี่ยวกับไทยเซิร์ต," สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), https://www.thaicert.or.th/about.html. [April 13, 2016]

เรื่องเดียวกันนี้ โดยความพยายามในทางระหว่างประเทศระดับทวิภาคีในการริเริ่มความร่วมมือระหว่างประเทศเกิดขึ้นผ่านการพัฒนาความสามารถทางการทหารด้านไซเบอร์ร่วมกัน การแลกเปลี่ยนข้อมูลทางด้านไซเบอร์ รวมถึงการให้ความช่วยเหลือในการพัฒนาขีดความสามารถทางไซเบอร์และแก้ไขปัญหาเหตุการณ์ไซเบอร์ที่เกิดขึ้น โดยพบความร่วมมือระหว่างประเทศระดับทวิภาคีที่เกี่ยวข้องกับการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ดังนี้

ประเทศญี่ปุ่นและสหรัฐอเมริกาประกาศนโยบายยุทธศาสตร์ทวิภาคีในการสนทนาแลกเปลี่ยนประเด็นความมั่นคงปลอดภัยทางไซเบอร์ ในเดือนมิถุนายนปีค.ศ. 2011[87]

ประเทศอินเดียดำเนินความร่วมมือระหว่างประเทศในรูปแบบของบันทึกข้อตกลงความเข้าใจหรือการพัฒนาและการใช้ข้อมูลร่วมกันกับประเทศอื่นๆ เช่น อินเดียและเกาหลีใต้ลงนามในแถลงการณ์ร่วมสำหรับความร่วมมือทวิภาคีในเทคโนโลยีสารสนเทศ (IT) ในปีค.ศ. 2004 และนอกจากนี้ ประเทศอินเดียยังลงนามในบันทึกความเข้าใจกับประเทศเกาหลีใต้เพื่อสร้างการทำงานร่วมกันอย่างเป็นทางการทางด้านความมั่นคงปลอดภัยทางไซเบอร์[88]

ประเทศโมร็อกโกและมาเลเซียร่วมลงนามในบันทึกความเข้าใจว่าด้วยความมั่นคงปลอดภัยไซเบอร์ระหว่างการประชุมความมั่นคงปลอดภัยภูมิภาคที่โมร็อกโกในปีค.ศ. 2010 โดยบันทึกความเข้าใจดังกล่าวกำหนดความสัมพันธ์ในความร่วมมือระหว่างทั้งสองประเทศให้ครอบคลุมถึงการป้องกันข้อมูลโครงสร้างพื้นฐานที่สำคัญ การพัฒนากรอบความมั่นคงปลอดภัยทางไซเบอร์ การสร้างศักยภาพและการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกัน[89]

---

[87] Aaron Mehta and Paul Kallender-Umezu, "Us, Japan Strike New Military Agreement," DefenseNews, http://www.defensenews.com/story/breaking-news/2015/04/27/us-japan-new-military-agreement/26443297/. [April 14, 2016]

[88] Hamadoun I. Touré, The Quest for Cyber Peace, (International Telecommunication Union, 2011). pp. 94-95.

[89] CyberSecurity Malaysia, "Malaysia and Morocco Are Now Partners in Cyber Security,"(2010). [April 15, 2016]

ประเทศจีนให้ความช่วยเหลือประเทศเมียนมาร์ในการจัดตั้งกองกิจการความมั่นคงปลอดภัยทางทหาร (Military Affairs Security) ที่มีภารกิจในการทำงานด้านสงครามศูนย์กลางเครือข่าย (Network-Centric Warfare) และพัฒนาขีดความสามารถทางไซเบอร์และสงครามอิเล็กทรอนิกส์[90]

ประเทศเนเธอร์แลนด์ลงนามในบันทึกความเข้าใจกับประเทศลักเซมเบิร์กและเบลเยียมว่าด้วยความร่วมมือในความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการแบ่งปันข้อมูลสารสนเทศและความเชี่ยวชาญร่วมกัน[91]

ประเทศแอลบาเนียริเริ่มปฏิบัติการร่วมกับสหรัฐอเมริกาภายใต้องค์กรเพื่อการพัฒนาระหว่างประเทศของสหรัฐฯ สำหรับการพัฒนาขีดความสามารถของแอลบาเนียในการป้องกันทางไซเบอร์และรับมือกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์[92]

จากการศึกษาข้างต้น จะเห็นได้ว่า ประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นประเด็นหนึ่งที่รัฐใช้ในการดำเนินความสัมพันธ์ระหว่างประเทศระดับทวิภาคี เพื่อหาแนวร่วมหรือกลุ่มประเทศพันธมิตรที่มีแนวความคิดเหมือนกัน (Like-minded States) เกี่ยวกับประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธผ่านการพัฒนาความร่วมมือระหว่างประเทศเพื่อแลกเปลี่ยนความรู้ ความเชี่ยวชาญ บุคลากรทางการทหารเกี่ยวกับเทคโนโลยีทางไซเบอร์ นับเป็นสัญญาณของการก้าวสู่ยุคใหม่ของสงครามที่สมรภูมิการรบทางไซเบอร์ (Cyber Domain) จะกลายเป็นสมรภูมิการรบอีกสมรภูมิหนึ่ง นอกเหนือจากสมรภูมิการรบ 4 ด้าน คือ ทางบก ทางทะเล ทางอากาศ และทางอวกาศ

---

[90] Brian McCartan, "Myanmar on the Cyber-Offensive," AsiaTimes, http://www.atimes.com/atimes/Southeast_Asia/JJ01Ae01.html. [April 15, 2016]

[91] Elizabeth Winkel, "Benelux Sign Memorandum of Understanding on Cyber Security," European Urban Knowledge Network, http://www.eukn.eu/e-library/project/bericht/eventDetail/benelux-sign-memorandum-of-understanding-on-cyber-security/. [April 15, 2016]

[92] Stephanie Pepi, "Usaid Launches the Albanian Cyber-Security Program," https://www.usaid.gov/news-information/press-releases/usaid-launches-albanian-cyber-security-program. [April 15, 2016]

2.2.3 ความร่วมมือระหว่างประเทศระดับพหุภาคีในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

นอกเหนือจากแนวทางของรัฐในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ และความร่วมมือระหว่างประเทศในระดับทวิภาคีแล้ว ความร่วมมือระหว่างประเทศระดับพหุภาคีภายใต้องค์การระหว่างประเทศนับว่ามีบทบาทสำคัญอย่างยิ่งในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ซึ่งผู้เขียนจะได้อธิบายรายละเอียดพร้อมทั้งประเมินผลลัพธ์ว่าความพยายามเหล่านี้มีบทบาทและแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอย่างไร

2.2.3.1 ความร่วมมือภายใต้กรอบกฎหมายมนุษยธรรมระหว่างประเทศ

คณะกรรมการกาชาดระหว่างประเทศนับเป็นองค์การความร่วมมือระหว่างประเทศภายใต้กรอบกฎหมายมนุษยธรรมระหว่างประเทศที่มีความสำคัญอย่างยิ่งในการส่งเสริมการบังคับใช้และการพัฒนากฎหมายระหว่างประเทศ โดยเฉพาะกฎหมายมนุษยธรรมระหว่างประเทศซึ่งเป็นกฎหมายระหว่างประเทศที่บังคับใช้เมื่อมีสถานการณ์การขัดกันทางอาวุธหรือการสู้รบหรือสงครามเกิดขึ้น โดยมีความพยายามภายใต้การดำเนินการของคณะกรรมการกาชาดระหว่างประเทศเกี่ยวกับประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหลายประการ ดังนี้

2.2.3.1.1 คณะกรรมการกาชาดระหว่างประเทศ

คณะกรรมการกาชาดระหว่างประเทศ (International Committee of the Red Cross) จัดตั้งขึ้นเมื่อปี ค.ศ. 1863 เป็นองค์กรไม่เลือกปฏิบัติ อิสระ เป็นกลางและปฏิบัติภารกิจทางด้านมนุษยธรรมเพื่อปกป้องคุ้มครองชีวิต และศักดิ์ศรีของผู้เดือดร้อนจากภัยสงครามและความไม่สงบภายในประเทศ[93] พร้อมทั้งให้ความช่วยเหลือบุคคลที่ได้รับผลกระทบจากการขัดกันทางอาวุธและความรุนแรงจากการขัดกันทางอาวุธและส่งเสริมกฎหมายเกี่ยวกับการให้ความคุ้มครองผู้ที่ตกเป็นเหยื่อของสงคราม โดยมีภารกิจในการดำเนินงานทั่วโลกภายใต้หลักการตามอนุสัญญาเจนีวา ค.ศ. 1949 เป็นหลัก มีสำนักงานใหญ่ตั้งอยู่ที่นครเจนีวา ประเทศสวิสเซอร์แลนด์และ

[93] Teerapat Asavasungsidhi, "Customary Law," *International Review of the Red Cross* 87, no. 857 (2005).

มีบุคลากรเจ้าหน้าที่กว่า 14,500 คนประจำการในประเทศมากกว่า 80 ประเทศทั่วโลก คณะกรรมการกาชาดระหว่างประเทศได้รับเงินทุนส่วนใหญ่จากการบริจาคโดยสมัครใจจากรัฐบาลของประเทศภาคีสมาชิกและจากสภากาชาดและสภาเสี้ยววงเดือนแดงของแต่ละประเทศ

การดำเนินงานของคณะกรรมการกาชาดระหว่างประเทศตั้งอยู่บนพื้นฐานหลักการตามอนุสัญญาเจนีวาปี ค.ศ. 1949 และพิธีสารเพิ่มเติมอนุสัญญาเจนีวาภายใต้มติที่ประชุมองค์กรกาชาดและเสี้ยววงเดือนแดงระหว่างประเทศ คณะกรรมการกาชาดระหว่างประเทศเป็นองค์การระหว่างประเทศด้านมนุษยธรรม เพื่อให้มั่นใจว่ามีการคุ้มครองด้านมนุษยธรรม ปกป้องชีวิตและศักดิ์ศรีและให้ความช่วยเหลือแก่เหยื่อของสงครามหรือผู้ที่ได้รับผลกระทบจากการสู้รบและความรุนแรงในสถานการณ์อื่นๆ ส่งเสริมให้มีการเคารพและการปฏิบัติตามกฎหมายมนุษยธรรมระหว่างประเทศและหลักการด้านมนุษยธรรม[94]

จากการยอมรับข้อบทของอนุสัญญาเจนีวา ค.ศ. 1949 อย่างเป็นสากล โดยข้อบทส่วนใหญ่ตามอนุสัญญาเจนีวา ค.ศ. 1949 ทั้ง 4 ฉบับเป็นส่วนหนึ่งของกฎหมายจารีตประเพณีระหว่างประเทศทำให้เมื่อมีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น รัฐทุกรัฐจะต้องปฏิบัติตามอนุสัญญาเจนีวา 1949 ในการให้ความคุ้มครองแก่ผู้ที่ได้รับบาดเจ็บ ผู้ป่วย และผู้ซึ่งเรืออับปาง เชลยศึกและพลเรือน การปฏิบัติภารกิจของคณะกรรมการกาชาดระหว่างประเทศจึงตั้งอยู่บนพื้นฐานของหลักกฎหมายตามอนุสัญญาเจนีวา ค.ศ. 1949 ทั้ง 4 ฉบับ ซึ่งอนุสัญญาเจนีวายังได้ให้สิทธิในการริเริ่ม (Right of Initiative) แก่คณะกรรมการกาชาดระหว่างประเทศ โดยในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ คณะกรรมการกาชาดระหว่างประเทศสามารถใช้สิทธิในการริเริ่มเพื่อปฏิบัติภารกิจด้านมนุษยธรรม ซึ่งได้รับการยอมรับในประชาคมระหว่างประเทศและตามข้อ 3 ร่วมแห่งอนุสัญญาเจนีวาทั้ง 4 ฉบับ ในกรณีสถานการณ์ความยุ่งยากภายในและความตึงเครียด หรือการกระทำอื่นที่มีลักษณะคล้ายกัน คณะกรรมการกาชาดระหว่างประเทศยังสามารถใช้สิทธิในการริเริ่มเพื่อปฏิบัติภารกิจด้านมนุษยธรรมได้เช่นเดียวกัน ดังนั้น เมื่อใดก็ตามที่กฎหมายมนุษยธรรมระหว่างประเทศไม่ได้นำไปบังคับใช้ คณะกรรมการกาชาดระหว่างประเทศอาจเสนอการให้ความช่วยเหลือแก่รัฐบาลโดยไม่ถือว่าการให้ความช่วยเหลือนั้นเป็นการแทรกแซงกิจการภายในของรัฐที่เกี่ยวข้องแต่อย่างใด[95]

---

[94] ICRC, "The Icrc's Mandate and Mission," https://www.icrc.org/en/mandate-and-mission. [February 29, 2016]

[95] ibid.

จากการศึกษาบทบาทของคณะกรรมการกาชาดระหว่างประเทศในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ พบว่า คณะกรรมการกาชาดระหว่างประเทศได้ตระหนักถึงความสำคัญของปัญหาสงครามไซเบอร์โดยกำหนดให้มีการส่งเสริมและปรับปรุงประสิทธิภาพของกฎหมายมนุษยธรรมในการบังคับใช้กับการโจมตีทางไซเบอร์อย่างต่อเนื่อง

ในที่ประชุมองค์กรกาชาดและเสี้ยววงเดือนแดงระหว่างประเทศเกี่ยวกับกฎหมายมนุษยธรรมระหว่างประเทศและความท้าทายของการขัดกันทางอาวุธที่มีอยู่ในปัจจุบัน ประเด็นเรื่องการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธถูกหยิบยกขึ้นเป็นประเด็นสำคัญอยู่ในวาระเรื่องวิธีการและปัจจัยในการสู้รบ หัวข้อ เทคโนโลยีใหม่ของการสู้รบ (New Technologies of Warfare) ซึ่งที่ประชุมองค์กรกาชาดและเสี้ยววงเดือนแดงระหว่างประเทศเห็นว่าสงครามไซเบอร์ (Cyber Warfare) เป็นหนึ่งในสองเทคโนโลยีใหม่ของการสู้รบที่ก่อให้เกิดประเด็นข้อท้าทายเกี่ยวกับกฎหมาย จรรยาบรรณและมนุษยธรรม โดยเฉพาะประเด็นที่ว่ากฎหมายที่มีอยู่ในปัจจุบันสามารถที่จะนำไปบังคับใช้หรือควรที่จะต้องอธิบายกฎหมายมนุษยธรรมระหว่างประเทศเพิ่มเติมหรือพัฒนา กฎใหม่ขึ้นมาจัดการกับข้อท้าทายต่างๆ ที่เกิดขึ้นหรือไม่ โดยคณะกรรมการกาชาดระหว่างประเทศได้ให้ผู้เชี่ยวชาญทางด้านกฎหมายมนุษยธรรมระหว่างประเทศพิจารณาแนวทางในการจัดการข้อท้าทายทางกฎหมายที่อาจเกิดขึ้นเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศต่อการโจมตีทางไซเบอร์อย่างต่อเนื่อง

คณะกรรมการกาชาดระหว่างประเทศจัดทำแถลงการณ์ไปยังองค์การสหประชาชาติ (ICRC Statement to the United Nations) ในการอภิปรายของคณะกรรมการที่หนึ่ง (First Committee) ของสมัชชาสหประชาชาติว่าด้วยการลดอาวุธและความมั่นคงระหว่างประเทศ (General Debate on All Disarmament and International Security

Agenda Items) ประเด็นเรื่อง อาวุธ ในปี ค.ศ. 2013[96] 2014[97] และล่าสุดในปี 2015[98] เกี่ยวกับสงครามไซเบอร์

ในแถลงการณ์ดังกล่าวข้างต้น คณะกรรมการกาชาดระหว่างประเทศเรียกร้องให้มีการจัดการกับสงครามไซเบอร์ซึ่งเป็นหนึ่งในเทคโนโลยีใหม่ของการสู้รบ (New Technologies of Warfare) ที่แม้จะไม่มีข้อห้ามหรือข้อบทใดๆ ตามสนธิสัญญาที่มีอยู่ในปัจจุบันควบคุมการใช้สงครามไซเบอร์ในการสู้รบไว้เป็นการเฉพาะ แต่หากรัฐจะนำเทคโนโลยีไซเบอร์มาใช้ในการขัดกันทางอาวุธจำต้องดำเนินการปฏิบัติให้สอดคล้องกับหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ โดยเฉพาะหลักการแยกแยะ หลักความได้สัดส่วนและหลักการใช้ความระมัดระวังในการโจมตี[99] ตลอดจนข้อห้ามโจมตีโดยตรงต่อทรัพย์สินและข้อห้ามการโจมตีโดยไม่เลือกเป้าหมาย[100] อีกทั้ง ระบุว่าสงครามไซเบอร์จะต้องอยู่ภายใต้ข้อจำกัดที่กำหนดโดยกฎหมายมนุษยธรรมระหว่างประเทศว่าด้วยอาวุธ วิธีการและปัจจัยในการสู้รบใหม่ทั้งหมด โดยเฉพาะข้อห้ามในการโจมตีโดยตรงต่อทรัพย์สินของพลเรือนและข้อห้ามโจมตีโดยไม่เลือกเป้าหมายและการโจมตีที่ไม่ได้สัดส่วน[101]

นอกจากนี้ ในแถลงการณ์ดังกล่าวคณะกรรมการกาชาดระหว่างประเทศยังต้องการเรียกร้องให้รัฐทำการประเมินว่าเทคโนโลยีใหม่นั้นเป็นไปตามกฎหมายมนุษยธรรมระหว่าง

[96] "Weapons: Icrc Statement to the United Nations, 2013," https://www.icrc.org/eng/resources/documents/statement/2013/united-nations-weapons-statement-2013-10-16.htm. [December 12, 2015]

[97] "Weapons: Icrc Statement to the United Nations, 2014". https://www.icrc.org/en/document/weapons-icrc-statement-united-nations-2014 [December 12, 2015]

[98] "Weapons: Icrc Statement to the United Nations, 2015," https://www.icrc.org/en/document/weapons-icrc-statement-united-nations-2015. [December 12, 2015]

[99] "Weapons: ICRC Statement to the United Nations, 2013," https://www.icrc.org/eng/resources/documents/statement/2013/united-nations-weapons-statement-2013-10-16.htm. [December 12, 2015]

[100] "Weapons: ICRC Statement to the United Nations, 2014". https://www.icrc.org/en/document/weapons-icrc-statement-united-nations-2014 [December 12, 2015]

[101] Ibid.

ประเทศก่อนที่จะพัฒนาหรือได้มาซึ่งปัจจัยในการสู้รบใหม่ซึ่งเป็นสิ่งจำเป็นเพื่อป้องกันการพัฒนาของอาวุธที่อาจจะละเมิดกฎหมายมนุษยธรรมระหว่างประเทศได้[102]

ยิ่งไปกว่านั้น คณะกรรมการกาชาดระหว่างประเทศยังได้แสดงความกังวลในคำแถลงการณ์เกี่ยวกับมิติทางด้านมนุษยธรรมของสงครามไซเบอร์ซึ่งเป็นวิธีการและปัจจัยในการสู้รบที่พึ่งพาเทคโนโลยีจากการเชื่อมต่อเทคโนโลยีสารสนเทศระหว่างเครือข่ายทางทหารและพลเรือน (Dual-use) ก่อให้เกิดข้อท้าทายในทางปฏิบัติที่สำคัญเป็นจำนวนมากในการให้ความคุ้มครองพลเรือนจากอันตรายของสงครามไซเบอร์ เช่น ความยากลำบากของฝ่ายในการสู้รบที่จะต้องแยกแยะระหว่างเป้าหมายทางทหารและทรัพย์สินของพลเรือนตลอดเวลาที่ดำเนินการโจมตีทางไซเบอร์ตามหลักการแยกแยะ หรือการประเมินผลกระทบทางอ้อม (Indirect Effect) ที่อาจเกิดขึ้นต่อเครือข่ายพลเรือนจากการโจมตีทางไซเบอร์นั้น อาทิ การโจมตีทางไซเบอร์ต่อระบบขนส่งมวลชน เครือข่ายอิเล็กทรอนิกส์ เขื่อน โรงงานเคมีและนิวเคลียร์อาจส่งผลกระทบร้ายแรงได้

นอกจากนี้ คณะกรรมการกาชาดระหว่างประเทศยังทำงานร่วมกับองค์การระหว่างประเทศอื่นในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ อาทิ องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือหรือนาโต โดยเข้าร่วมในฐานะผู้สังเกตการณ์ (Observer) ระหว่างการจัดทำคู่มือทาลลินน์ (The Tallinn Manual) ในฐานะผู้สังเกตการณ์เพื่อให้มั่นใจว่าคู่มือทาลลินน์จะสะท้อนแง่มุมทางกฎหมายที่มีอยู่เกี่ยวกับกฎหมายมนุษยธรรมระหว่างประเทศเท่าที่เป็นไปได้และจะรักษาหลักการคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศเกี่ยวกับการให้ความคุ้มครองเหยื่อในการสู้รบซึ่งคณะกรรมการกาชาดระหว่างประเทศได้เห็นด้วยกับกฎและความคิดเห็นตามคู่มือทาลลินน์เป็นส่วนใหญ่ แต่ก็มีข้อยกเว้นไม่เห็นด้วยในบางข้อ[103]

จากการศึกษาบทบาทของคณะกรรมการกาชาดระหว่างประเทศในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ จะเห็นได้ว่า คณะกรรมการกาชาดระหว่างประเทศพยายามพยายามแสดงจุดยืนเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่าง

---

[102] "Weapons: ICRC Statement to the United Nations, 2013," https://www.icrc.org/eng/resources/documents/statement/2013/united-nations-weapons-statement-2013-10-16.htm. [December 12, 2015]

[103] Laurent Gisel, "The Law of War Imposes Limits on Cyber Attacks Too," ICRC, https://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm. [January 20, 2015]

ประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยคณะกรรมการกาชาดระหว่างประเทศเห็นว่าการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบถือเป็นวิธีการและปัจจัยในการสู้รบใหม่ที่จะต้องปฏิบัติตามหลักการของกฎหมายมนุษยธรรมระหว่างประเทศ โดยกฎหมายมนุษยธรรมระหว่างประเทศสามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้ อย่างไรก็ตาม คณะกรรมการกาชาดระหว่างประเทศยังแสดงความกังวลเกี่ยวกับข้อท้าทายที่เกิดขึ้นจากการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยกำหนดให้ผู้เชี่ยวชาญทางด้านกฎหมายพิจารณาหาแนวทางในการจัดการกับข้อท้าทายต่างๆ ทั้งนี้ คณะกรรมการกาชาดระหว่างประเทศพยายามส่งเสริมให้รัฐต่างๆ เคารพและปฏิบัติตามหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธผ่านการเรียกร้องไปยังองค์การสหประชาชาติอย่างต่อเนื่องทุกปี ถือได้ว่าคณะกรรมการกาชาดระหว่างประเทศเป็นองค์การระหว่างประเทศที่มีบทบาทโดยตรงในการส่งเสริมและพัฒนากฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

2.2.3.2 ความร่วมมือภายใต้องค์การสหประชาชาติ

จากการที่องค์การสหประชาชาติกำหนดภารกิจเพื่อธำรงไว้ซึ่งสันติภาพและความมั่นคงระหว่างประเทศ การส่งเสริมการพัฒนาอย่างยั่งยืน การคุ้มครองสิทธิมนุษยชน การสนับสนุนกฎหมายระหว่างประเทศ และการให้ความช่วยเหลือด้านมนุษยธรรม[104] ความร่วมมือภายใต้องค์การสหประชาชาติจึงเป็นอีกกลไกความร่วมมือระหว่างประเทศที่มีบทบาทสำคัญในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธผ่านองค์กรดังต่อไปนี้

2.2.3.2.1 สมัชชาสหประชาชาติ

สมัชชาสหประชาชาติ (United Nations General Assembly – UNGA) ประกอบด้วยผู้แทนของรัฐสมาชิกทั้งหมดของสหประชาชาติ เป็นองค์กรหลักที่มีหน้าที่กำหนดนโยบาย พิจารณาตัดสินใจในญัตติสำคัญๆ จะต้องใช้การลงมติอย่างน้อยสองในสามของสมาชิก

[104] United Nations, "What We Do," https://www.un.org/en/sections/what-we-do/index.html. [March 19, 2016]

ทั้งหมดในที่ประชุม เช่น การรักษาสันติภาพและความมั่นคงระหว่างประเทศ การเลือกและรับสมาชิกใหม่ขององค์การ การพิจารณาจัดสรรและรับรองงบประมาณ ส่วนญัตติย่อยอื่นๆ จะใช้การลงมติคะแนนเสียงเกินกึ่งหนึ่งของสมาชิกในที่ประชุม โดยแต่ละรัฐมีมีคะแนนเสียงจำนวนหนึ่งเสียงเท่ากัน ทั้งนี้ หน้าที่และอำนาจของสมัชชาสหประชาชาติกำหนดไว้ในหมวดที่ 4 ข้อ 10 ของกฎบัตรสหประชาชาติ ดังนี้

"สมัชชาอาจอภิปรายปัญหาใดๆ หรือเรื่องใดๆ ภายในขอบข่ายแห่งกฎบัตรฉบับปัจจุบัน หรือที่เกี่ยวโยงไปถึงอำนาจและหน้าที่ขององค์การใดๆ ตามที่บัญญัติไว้ในกฎบัตรฉบับปัจจุบันได้ และอาจทำคำแนะนำไปยังสมาชิกของสหประชาชาติ หรือคณะมนตรีความมั่นคง หรือทั้งสองแห่งในปัญหาหรือเรื่องราวใดๆ เช่นว่านั้นได้ เว้นแต่ที่ได้บัญญัติไว้ใน ข้อ 12"

ด้วยอำนาจและหน้าที่ตามข้อ 10 ของกฎบัตรสหประชาชาติ ทำให้สมัชชาสหประชาชาติสามารถให้คำแนะนำในประเด็นต่างๆ ภายใต้ขอบเขตขององค์การสหประชาชาติ ยกเว้นประเด็นเกี่ยวกับการรักษาสันติภาพและความมั่นคงระหว่างประเทศซึ่งอยู่ภายใต้อำนาจของคณะมนตรีความมั่นคงแห่งสหประชาชาติ สมัชชาสหประชาชาติประกอบด้วยคณะกรรมาธิการใหญ่ทั้งหมด 6 คณะ ได้แก่ คณะกรรมาธิการที่หนึ่งเกี่ยวกับการลดอาวุธและความมั่นคงระหว่างประเทศ คณะกรรมาธิการที่สองเกี่ยวกับเศรษฐกิจและสังคม คณะกรรมาธิการที่สามเกี่ยวกับสังคม วัฒนธรรม และมนุษยธรรม คณะกรรมาธิการที่สี่เกี่ยวกับการเมืองและการปลดปล่อย คณะกรรมาธิการที่ห้าเกี่ยวกับบริหาร งบประมาณและการทั่วไป และคณะกรรมาธิการที่หกเกี่ยวกับกฎหมาย

จากการศึกษาพบว่า บทบาทของสมัชชาสหประชาชาติเกี่ยวกับประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอยู่ภายใต้คณะกรรมาธิการที่หนึ่ง (First Committee) เกี่ยวกับการลดอาวุธและประเด็นเกี่ยวกับความมั่นคงระหว่างประเทศที่น่าสนใจ ได้แก่ การดำเนินการภายใต้ข้อมติสมัชชาสหประชาชาติที่ 64/386[105] ว่าด้วยการพัฒนาด้านข้อมูลสารสนเทศและการสื่อสารโทรคมนาคมในบริบทของความมั่นคงระหว่างประเทศซึ่งข้อมติดังกล่าวเสนอให้มีการอภิปรายต่อเนื่องเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ในบริบทของความมั่นคงระหว่างประเทศและการประชุมของกลุ่มผู้เชี่ยวชาญซึ่งจะได้ออกคำแนะนำไปยังประเทศสมาชิกต่อไป

[105] UNGA, "Developments in the Field of Information and Telecommunications in the Context of International Security " in *A/64/386*(2009).

นอกจากนี้ สมัชชาสหประชาชาติยังได้จัดตั้งกลุ่มผู้เชี่ยวชาญภาครัฐ (Group of Governmental Experts - GGEs) เกี่ยวกับการพัฒนาด้านข้อมูลสารสนเทศและการสื่อสารโทรคมนาคมในบริบทของความมั่นคงระหว่างประเทศเพื่อเจรจาหารือและตรวจสอบภัยคุกคามที่มีอยู่และที่อาจเกิดขึ้นได้จากกิจกรรมในขอบเขตไซเบอร์เริ่มต้นขึ้นในปี ค.ศ. 2004 ประกอบด้วยผู้เชี่ยวชาญภาครัฐจาก 15 ประเทศ กลุ่มผู้เชี่ยวชาญภาครัฐ (GGEs) กลุ่มแรกประสบความล้มเหลวในการบรรลุข้อตกลง และได้จัดตั้งกลุ่มผู้เชี่ยวชาญภาครัฐขึ้นเป็นครั้งที่สองในปี ค.ศ. 2009 โดยมีอาณัติเพื่อการศึกษาอย่างต่อเนื่องถึงภัยคุกคามที่มีอยู่และอาจเกิดขึ้นได้ในขอบเขตของความมั่นคงปลอดภัยข้อมูลสารสนเทศและมาตรการความร่วมมือที่เป็นไปได้ในการจัดการกับปัญหาเหล่านั้น[106]

การจัดตั้งกลุ่มผู้เชี่ยวชาญภาครัฐ (GGEs) กลุ่มที่สองประสบความสำเร็จสามารถบรรลุความตกลงร่วมกันและจัดทำรายงานออกเผยแพร่เมื่อปีค.ศ. 2010 เรียกร้องให้นานาประเทศร่วมมือกันปรับปรุงความร่วมมือระหว่างประเทศและความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดยรายงานเสนอคำแนะนำให้ดำเนินการเจรจาระหว่างรัฐต่อไปในการหารือเกี่ยวกับบรรทัดฐานที่เกี่ยวข้องกับการใช้ข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อที่จะลดความเสี่ยงและป้องกันโครงสร้างพื้นฐานที่สำคัญระดับชาติและระหว่างประเทศ[107] นอกจากนี้ ยังให้คำแนะนำเกี่ยวกับมาตรการสร้างความไว้เนื้อเชื่อใจ (Confidence Building) เสถียรภาพ (Stability) และการลดความเสี่ยงในการเข้าใจผิดที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศและการสื่อสารในการจัดการกับผลกระทบจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารของรัฐ รวมทั้งการแลกเปลี่ยนความคิดเห็นของรัฐเกี่ยวกับการใช้เทคโนโลยีสารสนเทศและการสื่อสารในสถานการณ์ความขัดแย้ง[108]

นอกจากนี้ สมัชชาสหประชาชาติยังได้รับรองข้อมติเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารและความมั่นคงปลอดภัยทางไซเบอร์เป็นจำนวนมาก เพื่อดึงดูดความสนใจ

---

[106] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," in *A/65/201*(2010). ดูรายละเอียดได้ในภาคผนวก 1

[107] ibid.

[108] ibid.

ของรัฐสมาชิกในการจัดการกับความท้าทายทางไซเบอร์ในอนาคต ซึ่งผลการศึกษาล่าสุดเน้นความสำคัญไปที่กระบวนการสร้างบรรทัดฐานใหม่ภายในระบบสหประชาชาติ[109]

2.2.3.2.2 สถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติ

สถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติ (United Nations Institute for Disarmament Research - UNIDIR) เป็นทบวงชำนัญพิเศษแห่งสหประชาชาติก่อตั้งขึ้นเมื่อปี ค.ศ. 1980 มีสำนักงานตั้งอยู่ในนครเจนีวา ประเทศสวิตเซอร์แลนด์ เป็นองค์กรอิสระเป็นกลาง ปฏิบัติภารกิจในการวิจัยเกี่ยวกับการลดอาวุธและความมั่นคง เพื่อเป็นศูนย์กลางในการประชุมปรึกษาหารือเกี่ยวกับการลดอาวุธทั้งในระดับทวิภาคีและพหุภาคีและการเจรจาเพื่อการไม่แพร่ขยายอาวุธ นอกจากนี้ ยังทำหน้าที่เป็นศูนย์กลางในการช่วยเหลือประชาคมระหว่างประเทศในการพัฒนาหาวิธีการแก้ไขความท้าทายในการลดอาวุธและความมั่นคงผ่านการศึกษาและการวิจัย โดยสถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติพยายามที่จะควบคุมอาวุธและการลดอาวุธป้องกันไม่ให้เกิดความขัดแย้งและส่งเสริมการพัฒนาสันติภาพและความเจริญรุ่งเรืองของโลกตลอดจนมุ่งมั่นที่จะคาดการณ์ถึงข้อท้าทายเกี่ยวกับการรักษาความมั่นคงและภัยคุกคามใหม่และอธิบายรายละเอียดวิธีการที่เป็นไปได้ที่จะจัดการกับข้อท้าทายเหล่านั้นก่อนที่จะกลายเข้าสู่ขั้นวิกฤต UNIDIR ยังทำหน้าที่เป็นสะพานเชื่อมต่อระหว่างการลดอาวุธของสหประชาชาติกับองค์การด้านการพัฒนาและรักษาความมั่นคงและระหว่างระบบสหประชาชาติกับประชาคมด้านความมั่นคงอื่นๆ ในการสร้างความร่วมมือกันที่จำเป็นในการแก้ไขและบรรเทาผลกระทบจากความไม่มั่นคงทั้งในระดับระหว่างประเทศ ภูมิภาคและท้องถิ่น[110]

ในปัจจุบัน สถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติสำรวจประเด็นสำคัญที่เกี่ยวกับความหลากหลายของอาวุธยุทโธปกรณ์ที่มีอยู่ในปัจจุบันและในอนาคต ความตึงเครียดและความขัดแย้งในท้องถิ่นพร้อมกับการดำเนินการทางการทูตทั่วโลก โดยปฏิบัติภารกิจร่วมกับนักวิจัย นักการทูต เจ้าหน้าที่ของรัฐและองค์กรพัฒนาเอกชน และหน่วยงานสถาบันอื่นๆ การทำงานของสถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติตั้งอยู่บนพื้นฐานของข้อบทของ

---

[109] Tim Maurer, *Cyber Norm Emergence at the United Nations – an Analysis of the Un's Activities Regarding Cyber-Security*, Discussion Paper 2011-11 (Cambridge: Belfer Center for Science and International Affairs, 2011).

[110] UNIDIR, "The Institute," http://www.unidir.org/about/the-institute. [March 7, 2016]

เอกสารฉบับสมบูรณ์ของสมัยประชุมวิสามัญครั้งแรกของสมัชชาใหญ่แห่งสหประชาชาติเพื่อรองรับการลดอาวุธ (Final Document of the First Special Session of the UN General Assembly Devoted to Disarmament) และข้อเสนอแนะของสมัชชาแห่งสหประชาชาติ โดยมีโครงการในการตรวจสอบเป็นประจำทุกปีและอยู่ภายใต้การอนุมัติจากคณะกรรมการที่ปรึกษาของเลขาธิการสหประชาชาติว่าด้วยเรื่องการลดอาวุธ (UN Secretary-General's Advisory Board on Disarmament Matters) ซึ่งทำหน้าที่เป็นคณะกรรมาธิการอำนวยการของสถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติ (UNIDIR's Board of Trustees) ในการรายงานภารกิจของสถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติต่อสมัชชาใหญ่แห่งสหประชาชาติเป็นรายประจำปี[111]

บทบาทของสถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธมุ่งเน้นไปที่การสร้างขีดความสามารถทั้งในระดับชาติ ระดับภูมิภาคและพหุภาคีผ่านงานวิจัยและการวิเคราะห์ที่เกี่ยวข้องโดยกำหนดให้การโจมตีทางไซเบอร์เป็นหนึ่งในประเด็นภัยคุกคามต่อความมั่นคงปลอดภัยที่เกิดขึ้นใหม่ (Emerging Security Threats) จัดทำโครงการวิจัย การประชุม และสิ่งตีพิมพ์เกี่ยวกับภัยคุกคามทางไซเบอร์มากมาย ทั้งที่ยังดำเนินการอยู่ และที่เสร็จสิ้นไปแล้ว

จากการศึกษาแนวทางความร่วมมือระหว่างประเทศระดับพหุภาคีในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธภายใต้กรอบองค์การสหประชาชาติ จะเห็นได้ว่า สมัชชาสหประชาชาติถือว่าการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นหนึ่งในภัยคุกคามต่อความมั่นคงระหว่างประเทศ โดยมุ่งส่งเสริมความร่วมมือระหว่างประเทศในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศและโครงสร้างพื้นฐานที่สำคัญของรัฐและประชาคมโลก เนื่องจากข้อมูลสารสนเทศและโครงสร้างพื้นฐานล้วนพึ่งพาอาศัยเทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการควบคุมการดำเนินงานจึงมีความเสี่ยงที่จะถูกโจมตีทางไซเบอร์และหากเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือโครงสร้างพื้นฐานได้รับความเสียหายจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอาจส่งผลให้พลเรือนได้รับผลกระทบจากการไม่สามารถใช้งานโครงสร้างพื้นฐานที่สำคัญต่อการดำเนินชีวิตประจำวันเหล่านั้นได้ ตลอดจนกระตุ้นให้ประชาคมระหว่างประเทศให้ความสำคัญในการป้องกันตนเองจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ และส่งเสริมการอภิปรายแลกเปลี่ยนความคิดเห็นของรัฐเกี่ยวกับ

[111] UNIDIR, "Mandate," http://www.unidir.org/about/the-institute/mandate. [March 7, 2016]

การใช้เทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการสู้รบ เพื่อให้ทราบถึงมุมมองความเข้าใจของรัฐต่างๆ ที่มีเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

นอกจากนี้ สถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติยังทำหน้าที่ในการสำรวจวิจัยแง่มุมต่างๆ เกี่ยวกับภัยคุกคามทางไซเบอร์ซึ่งรวมถึงการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อกระตุ้นให้ประชาคมระหว่างประเทศตระหนักในภัยคุกคามที่เกิดจากการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบด้วย

2.2.3.3 ความร่วมมือภายใต้องค์การระหว่างประเทศต่างๆ

นอกเหนือจากความร่วมมือภายใต้กรอบกฎหมายมนุษยธรรมระหว่างประเทศและองค์การสหประชาชาติ องค์การระหว่างประเทศต่างๆ ให้ความสำคัญและเตรียมตัวรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในระดับที่แตกต่างกัน โดยมีรายละเอียดดังต่อไปนี้

2.2.3.3.1 องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรป

องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรป (Organization for Security Co-operation in Europe)[112] หรือ OSCE เป็นองค์การระหว่างประเทศระดับภูมิภาคเฉพาะกิจภายใต้กฎบัตรสหประชาชาติก่อตั้งขึ้นในช่วงสงครามเย็น องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรปพัฒนามาจากการประชุมว่าด้วยความมั่นคงและความร่วมมือในยุโรป (Conference on Security and Cooperation in Europe - CSCE) และเปลี่ยนชื่อเป็น “องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรป (Organization for Security Co-operation in Europe - OSCE)” เมื่อปี ค.ศ. 1994

ปัจจุบัน องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรปประกอบด้วยประเทศสมาชิกจำนวน 57 ประเทศ ครอบคลุมทวีปยุโรป ทวีปเอเชียกลาง และทวีปอเมริกา สำนักงานใหญ่ตั้งอยู่ ณ กรุงเวียนนา ประเทศออสเตรีย OSCE ถือเป็นองค์กรระหว่างรัฐบาล (Intergovernmental Organization) ด้านความมั่นคงระดับภูมิภาคขนาดใหญ่ที่สุดของโลกซึ่งปฏิบัติ

---

[112] OSCE, "40 Years of Osce," http://www.osce.org/whatistheosce. [March 15, 2016]

ภารกิจในมิติเกี่ยวกับความมั่นคง 3 ด้าน ได้แก่ มิติด้านความมั่นคงทางการเมืองและการทหาร (Politico-military Dimension) มิติความมั่นคงทางสิ่งแวดล้อมและเศรษฐกิจ (Economic and Environmental Dimension) และมิติด้านมนุษย์ (Human Dimension)

ในปี ค.ศ. 2008 องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรปเริ่มจัดการประชุมเจรจาหารือในระดับสูงเกี่ยวกับประเด็นความมั่นคงปลอดภัยทางไซเบอร์โดยเฉพาะการต่อต้านการก่อการร้ายและอาชญากรรมทางไซเบอร์ ในเดือนธันวาคม 2013 รัฐที่มีส่วนร่วม (Participating States) ได้ลงมติรับรองมาตรการเสริมสร้างความไว้เนื้อเชื่อใจในด้านความมั่นคงปลอดภัยและการใช้เทคโนโลยีสารสนเทศและการสื่อสาร[113] โดยมีวัตถุประสงค์เพื่อลดความขัดแย้งที่เกิดจากการใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICTs) รวมทั้งการแลกเปลี่ยนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ องค์กรแห่งชาติ กลยุทธ์ นโยบายรวมทั้งการให้ความร่วมมือระหว่างภาครัฐและภาคเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยและการใช้เทคโนโลยีสารสนเทศและการสื่อสาร การให้คำปรึกษาเพื่อลดความเสี่ยงของการเข้าใจผิดและความเป็นไปได้ในการเกิดความขัดแย้งตึงเครียดทางการเมืองหรือความตึงเครียดทางการทหารที่มีสาเหตุจากการใช้เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการโจมตีทางไซเบอร์ และปกป้องโครงสร้างพื้นฐานสำคัญด้านเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติ การแบ่งปันข้อมูลเกี่ยวกับมาตรการที่ดำเนินการเพื่อให้มั่นใจในอินเทอร์เน็ตที่เปิดกว้าง สามารถทำงานร่วมกัน มีความปลอดภัยและน่าเชื่อถือ

จากการศึกษาข้างต้นเป็นที่น่าสังเกตว่า องค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรปมุ่งเน้นประเด็นความมั่นคงปลอดภัยทางไซเบอร์จากการใช้เทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการก่อการร้ายและอาชญากรรมทางไซเบอร์มากกว่าการใช้ในสถานการณ์การขัดกันทางอาวุธ แม้ว่าหนึ่งในภารกิจหลักขององค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรปคือมิติด้านความมั่นคงทางการเมืองและทางการทหารก็ตาม

อย่างไรก็ดี การให้ความสำคัญกับการป้องกันโครงสร้างพื้นฐานสำคัญของรัฐถือเป็นแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่สำคัญ เนื่องจากโครงสร้างพื้นฐานสำคัญของรัฐมีความเสี่ยงที่จะตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ทั้ง

---

[113] "Decision No. 1106 Initial Set of Osce Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,"(2013).

ในสถานการณ์ปกติและในสถานการณ์การขัดกันทางอาวุธ เนื่องมาจากการพึ่งพาเทคโนโลยีในการควบคุมโครงสร้างพื้นฐานเหล่านั้น

2.2.3.3.2 สหภาพยุโรป

สหภาพยุโรป (European Union -EU) เป็นความร่วมมือทางเศรษฐกิจการเมืองและสังคมระหว่างประเทศในทวีปยุโรปประกอบด้วยประเทศสมาชิก 28 ประเทศ ซึ่งทำงานเป็นอิสระจากรัฐบาลของประเทศสมาชิก ดำเนินการผ่านกลไกการเจรจาต่อรองระหว่างรัฐบาล (Intergovernmental) ในหมู่ประเทศสมาชิกและสถาบันอิสระเหนือรัฐ (Supranational) ได้แก่ สภายุโรป คณะกรรมาธิการยุโรป รัฐสภายุโรป และคณะมนตรีแห่งสหภาพยุโรป เน้นการทำงานตามสนธิสัญญามาสทริชท์ (The Treaty of Maastricht)ใน 3 เสาหลัก ได้แก่ (1) การรวมตัวทางเศรษฐกิจ (Economic Integration) (2) นโยบายร่วมด้านการต่างประเทศและความมั่นคง (Common Foreign and Security Policy - CFSP) และ (3) ความร่วมมือด้านกระบวนการยุติธรรมในคดีอาญา (Judicial Cooperation in Criminal Matters)

จากการศึกษาบทบาทของสหภาพยุโรปเกี่ยวกับประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ พบว่า สหภาพยุโรปเน้นไปที่การรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยเริ่มภารกิจด้านความมั่นคงปลอดภัยเครือข่ายและข้อมูลสารสนเทศจากการกำหนดนโยบายหลักด้านความมั่นคงปลอดภัยทางไซเบอร์ซึ่งมีความสัมพันธ์อย่างยิ่งกับสงครามไซเบอร์ ได้แก่ (1) มาตรการในการต่อสู้กับการโจมตีทางไซเบอร์ รวมทั้งอาชญากรรมทางไซเบอร์หรือการก่อการร้ายทางไซเบอร์และ (2) มาตรการในการสนับสนุนการป้องกันระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Protection - CIP) การป้องกันข้อมูลระบบโครงสร้างพื้นฐานสำคัญ (Critical Information Infrastructure Protection - CIIP) และความมั่นคงปลอดภัยทางเครือข่ายและระบบสารสนเทศ (Network and Information Security - NIS) ทั้งนี้ นโยบายทั้งสองมีความคาบเกี่ยวกันอย่างมีนัยสำคัญตามการศึกษาของรัฐสภายุโรป (European Parliament) เรื่องความมั่นคงปลอดภัยทางไซเบอร์และอำนาจไซเบอร์: แนวคิด เงื่อนไขและความสามารถสำหรับความร่วมมือในการดำเนินการภายในสหภาพยุโรป ปี ค.ศ. 2011[114] โดย EU ดำเนินนโยบาย ผ่านกลยุทธ์ การบังคับใช้กฎหมายและองค์กรต่างๆ ภายในสหภาพยุโรปมากมาย อาทิ

[114] Directorate-General for External Policies of the Union European Parliament, "Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the Eu,"(2011). P. 29.

- สหภาพยุโรปเริ่มต้นวิธีการในการป้องกันโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญขึ้นในปีค.ศ. 2007 ภายหลังเหตุการณ์การโจมตีทางไซเบอร์ต่อประเทศเอสโตเนีย โดยคณะกรรมการธิการยุโรปได้จัดตีพิมพ์เผยแพร่เอกสารมากมายสำหรับการริเริ่มป้องกันโครงสร้างพื้นฐานในเวลานั้น[115]

- กรอบการตัดสินใจว่าด้วยการโจมตีต่อระบบสารสนเทศ[116] กำหนดให้รัฐสมาชิกเสนอข้อบทในการจัดการประเภทของการโจมตีทางไซเบอร์ที่สำคัญและจัดให้มีคำนิยามทั่วไปสำหรับการโจมตีทางไซเบอร์ดังกล่าว นอกจากนี้ยังเรียกร้องให้มีการแลกเปลี่ยนข้อมูลร่วมกันระหว่างประเทศสมาชิกอีกด้วย ทั้งนี้ กรอบการตัดสินใจดังกล่าวพัฒนาไปเป็นแนวปฏิบัติว่าด้วยการโจมตีต่อระบบสารสนเทศ ในปีค.ศ. 2013[117]

- จัดตั้งสำนักงานรักษาความมั่นคงปลอดภัยเครือข่ายและระบบสารสนเทศยุโรป (The European Network and Information Security Agency - ENISA) เป็นหน่วยงานภายใต้การกำกับดูแลของสหภาพยุโรปในการช่วยเหลือคณะกรรมาธิการยุโรป รัฐสมาชิกและภาคธุรกิจในการจัดการ รับมือ และป้องกันปัญหาเกี่ยวกับความมั่นคงปลอดภัยของเครือข่ายและระบบสารสนเทศ นอกจากนี้ ยังทำหน้าที่ช่วยเหลือคณะกรรมาธิการยุโรปในการเตรียมงานด้านเทคนิคสำหรับการปรับปรุงและพัฒนากฎหมายของสหภาพยุโรปเกี่ยวกับประเด็นความมั่นคงปลอดภัยทางเครือข่ายและระบบสารสนเทศ

- จัดทำกลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรป (Cybersecurity Strategy of the European Union) ในปีค.ศ. 2013[118] ซึ่งกลยุทธ์ดังกล่าวแสดงวิสัยทัศน์ บทบาท หน้าที่ ความรับผิดชอบ และการดำเนินการที่จำเป็นสำหรับสหภาพยุโรปใน

---

[115] UNIDIR, "The Cyber Index: International Security Trends and Realities,"(Geneva, Switzerland: United Nations, 2013) P. 104.

[116] European Union, "Council Framework Decision 2005/222/Jha of 24 February 2005 on Attacks against Information Systems,"(16.3.2005).

[117] "Directive on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/Jha,"(2013).

[118] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,"(European Commission, 2013).

ขอบเขตของความมั่นคงปลอดภัยทางไซเบอร์ โดยเน้นย้ำบริบทของความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเห็นว่าการจัดการแบบรวมศูนย์อำนาจของสหภาพยุโรปไม่ใช่คำตอบในการแก้ปัญหาภัยคุกคามทางไซเบอร์ รัฐบาลแห่งชาติยังคงเป็นหน่วยงานหลักในการจัดระเบียบการป้องกันและรับมือกับเหตุการณ์ไซเบอร์ที่เกิดขึ้นในระดับชาติ โดยสหภาพยุโรปวาง 3 เสาหลักในการจัดการปัญหาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ (1) ความมั่นคงปลอดภัยทางเครือข่ายและระบบสารสนเทศ (Network and Information Security) (2) การบังคับใช้กฎหมาย (Law Enforcement) และ (3) การป้องกันตนเอง (Defence) ทั้งนี้ สหภาพยุโรปจะให้การช่วยเหลือ สนับสนุนในกรณีที่เกิดเหตุการณ์ไซเบอร์ที่สำคัญหรือเกิดการโจมตีทางไซเบอร์ขึ้น นอกจากนี้ ยังกำหนดหน่วยงานที่รับผิดชอบสำหรับการสร้างความมั่นใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

นอกจากนี้ สหภาพยุโรปยังผลักดันให้ประเทศสมาชิกตระหนักในความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้ความช่วยเหลือแก่ประเทศสมาชิกทั้งทางด้านเทคนิค และทางกฎหมาย รวมทั้งยังร่วมมือกับองค์การระหว่างประเทศอื่นเพื่อความร่วมมือในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยกำหนดให้การเสริมสร้างความร่วมมือกับพันธมิตรระหว่างประเทศที่เกี่ยวข้องเป็นหนึ่งในห้านโยบายสำคัญภายใต้กรอบนโยบายการป้องกันตนเองทางไซเบอร์ของสหภาพยุโรป[119] อาทิ ความร่วมมือกับองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (NATO) ในการแบ่งปันยุทธศาสตร์ในการจัดการกับวิกฤตการณ์ การพัฒนาขีดความสามารถและการให้คำปรึกษาทางการเมือง ซึ่งล่าสุดได้ลงนามในข้อตกลงทางเทคนิคว่าด้วยการป้องกันตนเองทางไซเบอร์ (Technical Arrangement on Cyber Defence)[120] เพื่อการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ การพัฒนาความร่วมมือในปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างสหภาพยุโรปและองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ

จากการศึกษาการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของสหภาพยุโรป แม้ว่าจะไม่พบการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เป็นรูปธรรม อย่างไรก็ตาม กลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Strategy of the European Union) ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรป อีกทั้งยังระบุว่าการเชื่อมต่อระหว่างวิธีการของพลเรือนและวิธีการทางทหารในการ

---

[119] Council of the European Union, "Eu Cyber Defence Policy Framework" (Brussels, 2014).

[120] European Union, "Eu and Nato Cyber Defence Cooperation,"

http://eeas.europa.eu/top_stories/2016/100216_eu-nato-cyber-defence-cooperation_en.htm. [March 14, 2016]

ป้องกันทรัพย์สินทางไซเบอร์ควรพัฒนาเพิ่มมากขึ้นซึ่งจะต้องได้รับการสนับสนุนโดยการวิจัยและการพัฒนาความร่วมมืออย่างใกล้ชิดระหว่างรัฐ ภาคเอกชนและสถาบันการศึกษาภายในสหภาพยุโรป ตลอดจนการพัฒนาความร่วมมือกับองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือซึ่งเป็นองค์การระหว่างประเทศทางการทหารโดยเฉพาะอาจพัฒนาไปสู่การรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เป็นรูปธรรมในอนาคตได้

2.2.3.3.3 องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ

องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (North Atlantic Treaty Organization - NATO)[121] ประกอบด้วยประเทศสมาชิกพันธมิตรทั้งหมด 28 ประเทศ ได้แก่ แอลเบเนีย เบลเยียม บัลแกเรีย แคนาดา โครเอเชีย สาธารณรัฐเชคฯ เดนมาร์ก เอสโตเนีย ฝรั่งเศส เยอรมณี กรีซ ฮังการี ไอซ์แลนด์ อิตาลี ลัตเวีย ลิทัวเนีย ลักเซมเบอร์ก เนเธอร์แลนด์ นอร์เวย์ โปแลนด์ โปรตุเกส โรมาเนีย สโลวาเกีย สโลวีเนีย สเปน ตุรกี อังกฤษ และสหรัฐอเมริกา[122] องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือเป็นความร่วมมือระหว่างประเทศของกลุ่มประเทศทวีปยุโรปและอเมริกาเหนือ วัตถุประสงค์ที่สำคัญขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ คือการเป็นพันธมิตรทางการเมืองและการทหารระหว่างประเทศสมาชิก การปกป้องเสรีภาพและการรักษาความปลอดภัยของประเทศสมาชิกด้วยวิธีการทางการเมืองและการทหาร ภารกิจทางด้านการเมืองขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือส่งเสริมค่านิยมประชาธิปไตยและกระตุ้นให้เกิดการประชุมปรึกษาหารือและให้ความร่วมมือในการป้องกันประเทศและปัญหาด้านความปลอดภัยในการสร้างความไว้วางใจและป้องกันการเกิดความขัดแย้งในระยะยาว ส่วนภารกิจทางด้านการทหารองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือมุ่งมั่นให้เกิดการแก้ไขปัญหาข้อพิพาทอย่างสันติ หากความพยายามทางด้านการทูตล้มเหลว องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือจะจัดตั้งกองกำลังทหารที่จำเป็นในการดำเนินการจัดการวิกฤต ภายใต้ข้อ 5 ของสนธิสัญญาวอชิงตัน (The Washington Treaty) ซึ่งเป็นสนธิสัญญาก่อตั้งนาโตหรือดำเนินการภายใต้อาณัติของสหประชาชาติ องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือถือเป็นพันธมิตรความร่วมมือทางการทหารที่ใหญ่ที่สุดในโลกในเรื่องงบประมาณทางการทหาร ระบบอาวุธและเครื่องมืออุปกรณ์ทันสมัยต่างๆ

---

[121] NATO, "What Is Nato?," http://www.nato.int/nato-welcome/index.html. [February 27, 2016]

[122] "Nato Member Countries " http://www.nato.int/cps/en/natohq/nato_countries.htm. [February 27, 2016]

บทบาทขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เริ่มต้นขึ้นภายหลังจากการโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการต่อองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือระหว่างสงครามโคโซโว ในช่วงปลายปี ค.ศ. 1990[123] ทำให้องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือเริ่มกำหนดภารกิจเกี่ยวกับการป้องกันทางไซเบอร์ (Cyber Defence) ไว้ในระเบียบวาระขององค์การ

ในการประชุมสุดยอดที่กรุงปราก ในปี ค.ศ. 2002 องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือรับรองนโยบายการป้องกันไซเบอร์โดยเริ่มดำเนินการจัดตั้ง NATO Computer Incident Response Capability เป็นศูนย์ประสานงานเหตุการณ์คอมพิวเตอร์ซึ่งรับผิดชอบในการรับมือกับการโจมตีทางไซเบอร์ต่อเครือข่ายคอมพิวเตอร์ขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ โดยมีศูนย์ประสานงานอยู่ที่กรุงบรัสเซลส์ ศูนย์เทคนิคในกรุงมงส์ (Mons) ประเทศเบลเยียมเพื่อจัดการกับการบุกรุกโดยไม่มีอำนาจ มาตรการในการป้องกัน กฎหมายดิจิทัล และการสนับสนุนอื่นๆไปยังประเทศสมาชิกถือเป็นส่วนหนึ่งของหน่วยบริการระบบสารสนเทศและการติดต่อสื่อสารของ องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ

นอกจากนี้ องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือยังจัดตั้งหน่วยงานจัดการป้องกันไซเบอร์ (Cyber Defence Management Authority - CDMA) ซึ่งเป็นส่วนหนึ่งของนโยบายการป้องกันไซเบอร์ขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ เพื่อประสานงานและเริ่มดำเนินภารกิจในการป้องกันไซเบอร์ที่เหมาะสมอย่างทันท่วงทีและมีประสิทธิภาพ เมื่อพันธมิตรที่ตกเป็นเหยื่อของการโจมตีไซเบอร์แจ้งความประสงค์มายังหน่วยงานจัดการป้องกันไซเบอร์ ซึ่งเตรียมความพร้อมและความสามารถในการประสานงานหรือการให้ความช่วยเหลือในความพยายามร่วมกัน โดยเจ้าหน้าที่ขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือยืนยันการพัฒนาทีมตอบสนองอย่างรวดเร็ว (Rapid-Reaction Teams - RRTs) ที่พร้อมสำหรับการปฏิบัติงานทันทีในกรณีฉุกเฉินเพื่อตอบโต้การโจมตีไซเบอร์ตามคำขอของรัฐสมาชิก ทั้งนี้ หากเป็นคำขอจากรัฐที่ไม่ใช่สมาชิกจะต้องได้รับการอนุมัติจากสภาองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (NATO Council) ก่อนดำเนินการ[124]

---

[123] NATO Parliamentary Assembly, "Nato and Cyber Defence," 173 DSCFC 09 E bis (NATO, 2009).

ในขณะที่ NATO ปฏิบัติการทางทหารต่อประเทศเซอร์เบีย กลุ่มแฮ็กเกอร์อาชีพของเซอร์เบียหลายกลุ่มโจมตีโครงสร้างพื้นฐานอินเทอร์เน็ตของ NATO เพื่อขัดขวางความสามารถในการทำสงครามต่อสู้ของ NATO

[124] ibid.

เป็นที่น่าสังเกตว่า การดำเนินนโยบายในการป้องกันไซเบอร์และปกป้องเครือข่ายคอมพิวเตอร์ขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ รวมทั้งการส่งเสริมและสนับสนุนให้รัฐสมาชิกสร้างระบบไซเบอร์แห่งชาติที่แข็งแกร่งขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือจำกัดเฉพาะด้านความมั่นคงแห่งชาติของรัฐสมาชิกเท่านั้น องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือไม่มีอำนาจจัดการกับปัญหาความมั่นคงปลอดภัยทางไซเบอร์ของพลเรือนแต่อย่างใด

จะเห็นได้ว่า องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือมุ่งเน้นไปที่การพัฒนานโยบายและการป้องกันประเทศสมาชิกจากการโจมตีทางไซเบอร์ โดยการจัดการกับสงครามไซเบอร์ขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือขณะนี้เป็นไปตามอำนาจแห่งข้อบทตามข้อ 4 ของสนธิสัญญานาโต (NATO Treaty)[125] กำหนดให้รัฐภาคีจะปรึกษาหารือกันเมื่อใดก็ตามความเห็นของภาคีสมาชิกว่าบูรณภาพแห่งดินแดน ความเป็นอิสระทางการเมือง หรือการรักษาความปลอดภัยใด ๆ ของรัฐภาคีสมาชิกถูกคุกคาม กล่าวคือ การผลักดันทางด้านกฎหมายต่างๆ ขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือเป็นเพียงการปรึกษาหารือในหมู่ประเทศรัฐสมาชิก อาทิ การจัดทำร่างคู่มือทาลลินน์ (Tallinn Manual) ซึ่งไม่มีผลผูกพันให้รัฐสมาชิกต้องปฏิบัติร่างคู่มือฯ ดังกล่าว นอกจากนี้ กลไกการจัดการกับการโจมตีทางไซเบอร์ในปัจจุบันขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือยังไม่ถือเป็นกรณีภายใต้เงื่อนไขของอำนาจแห่งข้อ 5 ของสนธิสัญญานาโต (NATO Treaty)[126] ซึ่งกำหนดเป็นพันธกรณีที่รัฐสมาชิกจะต้องร่วมมือกันช่วยเหลือรัฐสมาชิกแต่อย่างใด

---

[125] NATO, "The North Atlantic Treaty,"(North Atlantic Treaty Organization, 1949).

Article 4

"The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."

[126] ibid.

Article 5

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

จากการศึกษาพบว่าองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือดำเนินการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีนัยสำคัญ โดยในปีค.ศ. 2008 องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือจัดตั้งศูนย์ความร่วมมือป้องกันไซเบอร์แห่งองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (Cooperative Cyber Defence Centre of Excellence - CCDCOE) ณ กรุงทาลลินน์ ประเทศเอสโตเนีย[127] เพื่อพัฒนากรอบกฎหมาย นโยบาย ดำเนินการศึกษาวิจัย การฝึกอบรมและการเป็นเจ้าภาพจัดการประชุมเชิงปฏิบัติการในด้านความมั่นคงปลอดภัยไซเบอร์[128] ศูนย์ความร่วมมือป้องกันไซเบอร์แห่งองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (CCDCOE) ยังทำหน้าที่เป็นตัวประสานระหว่างสถาบันการศึกษา ภาคเอกชนและหน่วยทหารขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ โดยมีภารกิจในการจัดกิจกรรมฝึกอบรม การประชุมเชิงปฏิบัติการและการเผยแพร่ประชาสัมพันธ์รวมทั้งให้ความร่วมมือกับสหภาพยุโรปเพื่อความร่วมมือในการแลกเปลี่ยนวิธีปฏิบัติที่ดีที่สุดระหว่างกันและมีความพยายามในการจัดทำคำแนะนำเกี่ยวกับการบังคับใช้กฎหมายระหว่างประเทศกับสงครามไซเบอร์ภายใต้การดำเนินงานของศูนย์ความร่วมมือป้องกันไซเบอร์แห่งองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (CCDCOE) ดังนี้

- การจัดทำคู่มือทาลลินน์ (Tallinn Manual)

ในปีค.ศ. 2009 ศูนย์ความร่วมมือป้องกันไซเบอร์แห่งองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (CCDCOE) ได้เชื้อเชิญให้กลุ่มผู้เชี่ยวชาญระหว่างประเทศ (International Group of Experts) ประกอบด้วยผู้ประกอบวิชาชีพทางด้านกฎหมาย (Legal Practitioners) นักวิชาการ (Academics) และผู้เชี่ยวชาญทางด้านเทคนิค (Technical Experts) จัดทำคู่มือว่าด้วยกฎหมายที่ใช้บังคับกับสงครามไซเบอร์พิจารณาว่าข้อบทกฎหมายระหว่างประเทศที่มีอยู่จะสามารถนำไปบังคับใช้กับสงครามไซเบอร์ซึ่งเป็นสงครามรูปแบบใหม่ได้อย่างไร

ในการจัดทำคู่มือทาลลินน์มีตัวแทนจากสามองค์การระหว่างประเทศที่ได้รับเชิญเข้าร่วมการจัดทำคู่มือในฐานะผู้สังเกตการณ์ โดยผู้สังเกตการณ์มีส่วนร่วมอย่างเต็มที่ในการ

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

[127] "Nato Opens New Centre of Excellence on Cyber Defence," http://www.nato.int/docu/update/2008/05-may/e0514a.html. [March 17, 2016]

[128] CCDCOE, "About Cyber Defence Centre," https://ccdcoe.org/about-us.html. [March 17, 2016]

อภิปรายและจัดทำร่างคู่มือทาลลินน์ ตลอดทั้งกระบวนการ แต่ไม่มีสิทธิออกเสียงใดๆ ได้แก่ ผู้บัญชาการพันธมิตรปฏิรูปประจำนาโต (NATO's Allied Command Transformation) ผู้บัญชาการไซเบอร์ของสหรัฐอเมริกา (The U.S. Cyber Command's) และตัวแทนคณะกรรมการกาชาดระหว่างประเทศ (the International Committee of the Red Cross)

แหล่งที่มาที่สำคัญในการอ้างอิงและสนับสนุนกฎต่างๆ ตามคู่มือทาลลินน์มาจากกฎหมายสนธิสัญญา กฎหมายจารีตประเพณี การศึกษาจารีตประเพณีของกฎหมายมนุษยธรรมระหว่างประเทศของคณะกรรมการกาชาดระหว่างประเทศ (ICRC Customary IHL Study) HPCR Manual on International Law Applicable to Air and Missile Warfare (The AMW Manual) และ The Manual on the Law of Non-International Armed Conflict with Commentary (NIAC Manual)[129] ตลอดจนยังอ้างอิงจากคู่มือทหารของประเทศแคนาดา เยอรมนี สหราชอาณาจักร และสหรัฐอเมริกา

ภายหลังจากการเชื้อเชิญเป็นเวลา 3 ปี ศูนย์ความร่วมมือป้องกันไซเบอร์แห่งองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (CCDCOE) จึงเผยแพร่คู่มือว่าด้วยการบังคับใช้กฎหมายระหว่างประเทศต่อสงครามไซเบอร์หรือคู่มือทาลลินน์ (Manual on the International Law Applicable to Cyber Warfare หรือ Tallinn Manual)[130] คู่มือทาลลินน์กำหนดขอบเขตในการพิจารณากฎหมายระหว่างประเทศที่บังคับใช้กับสงครามไซเบอร์ประกอบด้วยหลักกฎหมายระหว่างประเทศเกี่ยวกับการใช้กำลังอาวุธโดยรัฐ (Jus ad Bellum) และกฎหมายระหว่างประเทศที่ใช้ในปฏิบัติทางการทหารในการขัดกันทางอาวุธ (Jus in Bello)

เมื่อพิจารณาคู่มือทาลลินน์ดังกล่าว ถือเป็นตราสารซึ่งกำหนดหลักการหรือคำแนะนำในทางกฎหมายระหว่างประเทศที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธซึ่งจัดทำขึ้นในขณะที่ยังไม่มีสนธิสัญญาหรืออนุสัญญาเกี่ยวกับสงครามไซเบอร์เป็นการเฉพาะ อย่างไรก็ดี คู่มือทาลลินน์มีฐานะเป็นเพียงความเห็นของนักนิติศาสตร์ อันเป็นที่มาลำดับรองของกฎหมายระหว่างประเทศไม่มีผลผูกพันทางกฎหมายหรือผูกพันรัฐสมาชิกขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือให้ต้องปฏิบัติตามแต่อย่างใด

---

[129] *Tallinn Manual on the International Law Applicable to Cyber Warfare* Prepared by the International Group of Experts ed. Michael N. Schmitt(Cambridge University Press, 2013). P. 7.

[130] *Tallinn Manual on the International Law Applicable to Cyber Warfare* Prepared by the International Group of Experts ed. Michael N. Schmitt(Cambridge University Press, 2013).

แม้ว่าคู่มือว่าด้วยการบังคับใช้กฎหมายระหว่างประเทศกับสงครามไซเบอร์หรือคู่มือทาลลินน์จะไม่มีผลบังคับใดๆ ในทางกฎหมาย อย่างไรก็ตาม คู่มือทาลลินน์อาจพิจารณาว่ามีฐานะเป็นแนวโน้มของกฎหมาย (Soft Law) ได้ หากว่ามีรัฐสมาชิกใดยึดถือเป็นแนวทางปฏิบัติอย่างต่อเนื่องและสม่ำเสมอและมีแนวโน้มที่จะเป็นที่ยอมรับกันในหมู่นานาประเทศในอนาคตจนเกิดเป็นแนวทางปฏิบัติของรัฐอันเป็นสิ่งที่รัฐยึดถือว่าเป็นกฎหมาย

อย่างไรก็ตาม เมื่อพิจารณาจากแหล่งที่มาในการอ้างอิงและสนับสนุนกฎต่างๆ ตามคู่มือทาลลินน์ส่วนที่เป็นคู่มือทางทหาร พบว่ามีการอ้างอิงเฉพาะคู่มือทหารของประเทศแคนาดา เยอรมณี สหราชอาณาจักรและสหรัฐอเมริกาเป็นที่น่าสงสัยว่าคู่มือทาลลินน์สะท้อนเฉพาะมุมมองทางทหารของประเทศในกลุ่มยุโรปและสหรัฐอเมริกาเท่านั้น โดยไม่ได้นำคู่มือทางทหารของประเทศกลุ่มตะวันออกอย่างประเทศรัสเซียหรือจีนมาใช้พิจารณาประกอบในการจัดทำคู่มือทาลลินน์แต่อย่างใด นอกจากนี้คณะกลุ่มผู้เชี่ยวชาญระหว่างประเทศผู้จัดทำคู่มือทาลลินน์ส่วนใหญ่เป็นนักนิติศาสตร์ที่มาจากกลุ่มประเทศยุโรปและสหรัฐอเมริกา กล่าวได้ว่า คู่มือทาลลินน์สะท้อนมุมมองเกี่ยวกับการบังคับใช้กฎหมายระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มาจากเฉพาะกลุ่มนักนิติศาสตร์ที่มีความคิดเหมือนกัน (Like-minded) เท่านั้น

2.2.3.3.4 การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก

การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก (ASEAN Regional Forum - ARF) ประกอบด้วยสมาชิก 27 ประเทศ ได้แก่ ประเทศสมาชิกอาเซียนทั้ง 10 ประเทศ คือ ไทย บรูไน กัมพูชา อินโดนีเซีย ลาว มาเลเซีย พม่า ฟิลิปปินส์ สิงคโปร์ และเวียดนาม ประเทศคู่เจรจาของอาเซียน ประเทศผู้สังเกตการณ์ของอาเซียน และประเทศอื่นในภูมิภาคเอเชีย-แปซิฟิก ได้แก่ ออสเตรเลีย บังคลาเทศ แคนาดา จีน อินเดีย ญี่ปุ่น สาธารณรัฐเกาหลี (เกาหลีใต้) สาธารณรัฐประชาธิปไตยประชาชนเกาหลี (เกาหลีเหนือ) มองโกเลีย นิวซีแลนด์ ปากีสถาน ปาปัวนิวกินี รัสเซีย ติมอร์-เลสเต ศรีลังกา สหรัฐอเมริกา และสหภาพยุโรป ก่อตั้งเมื่อปี ค.ศ. 1994 เป็นการประชุมเจรจาปรึกษาหารือในระดับพหุภาคีเพื่อส่งเสริมความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก

การดำเนินงานในกรอบของการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิกมีทั้งหมด 3 ขั้นตอน ได้แก่ มาตรการสร้างความไว้เนื้อเชื่อใจระหว่างกัน (Confidence Building Measures - CBMs) การดำเนินการทางการทูตเชิงป้องกัน (Preventive Diplomacy) และแนวทางแก้ไขปัญหาความขัดแย้ง (Approaches to Conflict Resolution) มีวัตถุประสงค์หลักที่จะมุ่งส่งเสริมสันติภาพผ่านการเสริมสร้างความไว้เนื้อเชื่อใจ ความร่วมมือระหว่างประเทศ และความสัมพันธ์อันดีระหว่างประเทศสมาชิกอาเซียน ประเทศอาเซียนกับคู่เจรจา และประเทศอื่น ๆ ในภูมิภาคเอเชีย-แปซิฟิก โดยมีทั้งผู้แทนฝ่ายการทูตและการทหารเข้าร่วมการประชุมการหารือด้านการเมือง และความมั่นคงในกรอบการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก ปัจจุบันดำเนินการตามขั้นที่หนึ่ง (CBMs) มีการประชุมกรอบย่อยต่างๆ มี 4 สาขาหลัก ได้แก่ (1) การบรรเทาภัยพิบัติ (Disaster Relief) (2) การต่อต้านการก่อการร้ายและอาชญากรรมข้ามชาติ (Counter-Terrorism and Transnational Crime) (3) ความมั่นคงทางทะเล (Maritime Security) และ (4) การลดและไม่แพร่ขยายอาวุธ (Non-Proliferation and Disarmament) [131]

สำหรับบทบาทของการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิกเกี่ยวกับประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธพบว่าการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิกเห็นว่าการโจมตีทางไซเบอร์ถือเป็นภัยคุกคามทางไซเบอร์อย่างหนึ่ง โดยประเทศสมาชิกให้ความร่วมมือในการต่อสู้กับภัยคุกคามทางไซเบอร์[132] อาทิ ในปีค.ศ. 2006 รัฐที่เข้าร่วมในแถลงการณ์ว่าด้วยความร่วมมือในการต่อสู้กับการโจมตีทางไซเบอร์ และการก่อการร้ายโดยการใช้ห้วงไซเบอร์ในทางมิชอบ (ARF Statement on Cooperation in Fighting Cyber Attacks and Terrorist Misuse of Cyber Space)[133] แถลงการณ์ดังกล่าวตระหนักถึงผลกระทบที่ร้ายแรงของการโจมตีผ่านทางห้วงไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญเกี่ยวกับความมั่นคงปลอดภัยของประชาชน เศรษฐกิจและความเป็นอยู่ทางกายภาพของประเทศในภูมิภาคนี้ ตลอดจนเน้นย้ำความจำเป็นสำหรับ

---

[131] กองการเมืองและความมั่นคง กรมอาเซียน, "การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก (Asean Regional Forum - Arf),"(2557).

[132] UNIDIR, "The Cyber Index: International Security Trends and Realities,"(Geneva, Switzerland: United Nations, 2013) P. 106.

[133] ARF, "Asean Regional Forum Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space," http://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html. [March 8, 2016] ดูรายละเอียดได้ในภาคผนวก 3

ความร่วมมือระหว่างภาครัฐและภาคเอกชนในการระบุตัวตน (Identifying) การป้องกัน (Preventing) และการบรรเทาให้น้อยลง (Mitigating) ของการโจมตีไซเบอร์และการก่อการร้ายโดยการใช้ห้วงไซเบอร์ในทางมิชอบ

ในเดือนมีนาคม ค.ศ. 2012 การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิกได้จัด Workshop on Proxy Actors in Cyber Space[134] ที่ประเทศเวียดนาม เน้นพัฒนาวิธีการในการอนุวัติแนวทางที่ตกลงร่วมกันและให้ความสำคัญในการกำหนดเวทีสำหรับเจรจาอภิปรายในประเด็นเกี่ยวข้องกับห้วงไซเบอร์ (Cyber Space) เพื่อขยายบทบาทของการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิกทางด้านไซเบอร์ผ่านขั้นตอนมาตรการสร้างความไว้เนื้อเชื่อใจระหว่างกัน (CBMs)

นอกจากนี้ ในการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก ครั้งที่ 19 ที่เมืองพนมเปญ ประเทศกัมพูชา เมื่อวันที่ 12 กรกฎาคม ค.ศ. 2012 รัฐมนตรีว่าการกระทรวงการต่างประเทศที่เข้าร่วมประชุมได้ยอมรับแถลงการณ์ว่าด้วยความร่วมมือในการดูแลความมั่นคงปลอดภัยทางไซเบอร์ (Statement on Cooperation in Ensuing Cyber Security)[135] ซึ่งสอดคล้องกับแถลงการณ์ว่าด้วยความร่วมมือในการต่อสู้กับการโจมตีทางไซเบอร์ และการก่อการร้ายโดยการใช้ห้วงไซเบอร์ในทางมิชอบ (ARF Statement on Cooperation in Fighting Cyber Attacks and Terrorist Misuse of Cyber Space) ที่จัดทำขึ้นก่อนหน้านี้ โดยรัฐสมาชิกการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิกตกลงที่จะกระชับความร่วมมือในการพัฒนากลยุทธ์ร่วมกันเพื่อเอาชนะภัยคุกคามทางไซเบอร์ นอกจากนี้ ยังประกาศความตั้งใจที่จะส่งเสริมความร่วมมือในระดับภูมิภาคเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ การป้องกันของโครงสร้างพื้นฐานของชาติที่สำคัญ (National Information Infrastructure) ซึ่งมีความเสี่ยงต่อภัยคุกคามเกี่ยวกับความ

---

[134] "Co-Chairs' Summary Report Arf Workshop on Proxy Actors in Cyberspace,"(Hoi An City, Viet Nam2012).

[135] "Asean Regional Forum Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security," (2012).

ปลอดภัยในห้วงไซเบอร์ต่างๆ และเห็นว่ารัฐมีภาระหน้าที่ในทางระหว่างประเทศและมีส่วนร่วมโดยตรงในการสร้างความมั่นใจในการรักษาความปลอดภัยทางไซเบอร์ทั่วโลก[136]

จากการศึกษาข้างต้น จะเห็นได้ว่า การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิกไม่ได้ให้ความสำคัญกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นการเฉพาะ อย่างไรก็ตาม นโยบายเกี่ยวกับการป้องกันโครงสร้างพื้นฐานของชาติที่สำคัญมีความเกี่ยวข้องกับการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอย่างมีนัยสำคัญ เนื่องจากโครงสร้างพื้นฐานที่สำคัญของชาติมีความเสี่ยงที่จะตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ทั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธ เนื่องจากการพึ่งพาอาศัยเทคโนโลยีในการควบคุมโครงสร้างพื้นฐานที่สำคัญเหล่านั้น

2.2.3.3.5 องค์การความร่วมมือเซี่ยงไฮ้

องค์การความร่วมมือเซี่ยงไฮ้ (Shanghai Cooperation Organisation - SCO)[137] ก่อตั้งขึ้นในปี พ.ศ. 2544 ปัจจุบันประกอบด้วยสมาชิกทั้งหมด 6 ประเทศ ได้แก่ คาซัคสถาน จีน คีร์กีซสถาน รัสเซีย ทาจิกิสถาน และอุซเบกิสถาน โดยอินเดียและปากีสถานมีกำหนดการเข้าเป็นสมาชิกถาวรในปี พ.ศ. 2559[138] มีต้นแบบจากความร่วมมือเซี่ยงไฮ้ 5 (Shanghai Five) ซึ่งประกอบด้วยประเทศในทวีปยูเรเชีย (Eurasian) 5 ประเทศ มีวัตถุประสงค์เพื่อเป็นองค์การความร่วมมือระหว่างประเทศทางด้านการเมือง เศรษฐกิจ และการทหาร โดยเฉพาะการต่อสู้กับกลุ่มลัทธิการก่อการร้าย (Terrorism) ลัทธิการแบ่งแยกดินแดน (Separatism) และลัทธิสุดโต่ง (Extremism) ปรากฏตามตราสารก่อตั้งองค์การฯ ปัจจุบันขยายขอบเขตความร่วมมือทั้งทางด้านการเมือง การค้าและเศรษฐกิจ วิทยาศาสตร์และเทคโนโลยี วัฒนธรรม ตลอดจนการศึกษา พลังงาน การขนส่ง การท่องเที่ยว สิ่งแวดล้อมและสาขาอื่นๆ

---

[136] "Co-Chairs' Summary Report of the Arf Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects,"(2013).

[137] SCO, "Brief Introduction to the Shanghai Cooperation Organisation " http://www.sectsco.org/EN123/brief.asp. [February 18, 2016]

[138] The Hindu, "India, Pakistan Become Full Sco Members," http://www.thehindu.com/news/international/india-gets-full-membership-of-the-shanghai-cooperation-organisation-along-with-pakistan/article7407873.ece. [February 18, 2016]

องค์การความร่วมมือเซี่ยงไฮ้แสดงความกังวลเกี่ยวกับภัยคุกคามที่เกิดจากการใช้เทคโนโลยีข้อมูลข่าวสารและการติดต่อสื่อสารและเครื่องมือเพื่อวัตถุประสงค์โจมตี โดยเฉพาะสงครามไซเบอร์ซึ่งขัดต่อการสร้างความมั่นคงระหว่างประเทศและเสถียรภาพทั้งในขอบเขตทางการทหารและพลเรือน รวมทั้งการเผยแพร่ข้อมูลที่เป็นอันตรายต่อระบบเศรษฐกิจสังคมและระบบการเมืองสังคม ตลอดจนศาสนา คุณธรรมและวัฒนธรรมตามความตกลงระหว่างรัฐบาลของประเทศสมาชิกขององค์การความร่วมมือเซี่ยงไฮ้ว่าด้วยความร่วมมือในด้านความมั่นคงปลอดภัยระบบสารสนเทศระหว่างประเทศ[139]

องค์การความร่วมมือเซี่ยงไฮ้ได้ออกปฏิญญาเยคาเตรินเบอร์กของผู้นำประเทศสมาชิกขององค์การความร่วมมือเซี่ยงไฮ้ในการประชุมผู้นำประเทศสมาชิกประจำปีค.ศ. 2009[140] กำหนดให้ประเทศสมาชิกขององค์การความร่วมมือเซี่ยงไฮ้ให้ความสำคัญกับประเด็นการสร้างความเชื่อมั่นในความมั่นคงปลอดภัยระบบสารสนเทศระหว่างประเทศในฐานะเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศระหว่างประเทศ

นอกจากนี้ บทบาทล่าสุดขององค์การความร่วมมือเซี่ยงไฮ้ในเวทีระหว่างประเทศ เมื่อวันที่ 9 มกราคม 2015 องค์การความร่วมมือเซี่ยงไฮ้ได้ยื่นแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับปรับปรุง[141] ต่อที่ประชุมสมัชชาแห่งสหประชาชาติ ซึ่งแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับเดิมนำเสนอต่อสหประชาชาติก่อนหน้านี้ในปีค.ศ. 2011 โดยเนื้อหาของแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศทั้งสองฉบับระบุถึงภัยคุกคามที่มีต่อเป้าหมายที่เป็นปัจเจกบุคคล ภาคธุรกิจ โครงสร้างพื้นฐานของชาติและรัฐบาลจากการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร เรียกร้องให้มีความร่วมมือระหว่างรัฐ และความร่วมมือภายในประเทศระหว่างรัฐ เอกชนและภาคประชาสังคมในการเผชิญหน้ากับภัยคุกคาม โดยแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับปรับปรุง

---

[139] SCO, "Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (Unofficial Translation)." P. 202-203.

[140] Shanghai Cooperation Organisation, "Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation,"(16 June 2009).

[141] UN, "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary (International Code of Conduct for Information Security),"(2015). ดูรายละเอียดได้ในภาคผนวก 2

ระบุถึงสิทธิและความรับผิดชอบของรัฐเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและเรียกร้องให้รัฐต่างๆ ดำเนินการตามความสมัครใจ อาทิ

- ปฏิบัติตามกฎบัตรสหประชาชาติโดยเน้นการเคารพอำนาจอธิปไตยและบูรณภาพแห่งดินแดน (Sovereignty and Territorial Integrity)

- ไม่ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology) เครือข่ายสารสนเทศและการสื่อสาร (Information and Communication Network) ในการดำเนินขัดแย้งกับการการรักษาสันติภาพและความมั่นคงระหว่างประเทศ

- ให้ความร่วมมือในการปราบปรามอาชญากรรมและการก่อการร้ายที่ใช้เทคโนโลยีสารสนเทศและการสื่อสารหรือไอซีที

- ส่งเสริมบทบาทสำคัญของสหประชาชาติในการกำหนดบรรทัดฐานระหว่างประเทศ

- เน้นให้รัฐมีบทบาทที่เท่าเทียมกันในการกำกับดูแลการใช้อินเทอร์เน็ตระหว่างประเทศ การรักษาความปลอดภัย การพัฒนาในทางที่จะส่งเสริมกลไกในการกำกับดูแลอินเทอร์เน็ตระหว่างประเทศในระดับพหุภาคีที่โปร่งใสและมีความเสมอภาคที่สร้างความมั่นใจในการกระจายความเท่าเทียมกันของทรัพยากรที่อำนวยความสะดวกในการเข้าถึงสำหรับทุกรัฐและทำให้มั่นใจว่าการทำงานของอินเทอร์เน็ตจะมีความมั่นคงและปลอดภัย

อย่างไรก็ตาม แนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับปรับปรุงดังกล่าวมีแนวโน้มว่าจะไม่ได้รับการสนับสนุนจากนานาประเทศจะไม่ได้รับการรับรองในระดับสากล แต่ถือเป็นสัญญาณที่ชัดเจนในความพยายามอย่างต่อเนื่องขององค์การความร่วมมือเซี่ยงไฮ้ในการสนับสนุนให้มีข้อตกลงระหว่างประเทศและ บรรทัดฐานใหม่ที่กำหนดหรือจำกัดพฤติกรรมของรัฐในการใช้เทคโนโลยีในด้านต่างๆ ซึ่งรวมถึงการใช้เทคโนโลยีในสถานการณ์การขัดกันทางอาวุธด้วย แม้แนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับปรับปรุงจะยังไม่ได้รับการยอมรับในระดับสากล แต่มีความเป็นไปได้ที่หลักการตามแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัย

ระบบสารสนเทศฉบับปรับปรุงจะถูกนำไปปรับใช้ในระดับภูมิภาคหรือใช้ในระหว่างรัฐที่มีความคิดเหมือนกัน เช่นที่ ประเทศรัสเซียรายงานการนำเสนออนุสัญญาการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศพิเศษ (A special Information Security Convention) ในการประชุมสุดยอดสมาชิกทั้งกลุ่มสมาชิก BRICS ซึ่งประกอบไปด้วยประเทศบราซิล รัสเซีย อินเดีย จีน และแอฟริกาใต้ และองค์การความร่วมมือเซี่ยงไฮ้[142]

นอกจากนี้ แนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับปรับปรุงดังกล่าวยังสะท้อนสัญญาณที่ชัดเจนในความพยายามอย่างต่อเนื่องขององค์การความร่วมมือเซี่ยงไฮ้ในการสนับสนุนให้มีข้อตกลงระหว่างประเทศและบรรทัดฐานใหม่ที่กำหนดหรือจำกัดพฤติกรรมของรัฐในการใช้เทคโนโลยีสารสนเทศ ซึ่งจะส่งผลให้มีการเจรจาหารือในระดับสากลเกี่ยวกับการควบคุมการใช้เทคโนโลยีสารสนเทศในสถานการณ์การขัดกันทางอาวุธต่อไปในอนาคต

เป็นที่น่าสังเกตว่า ความพยายามในการสร้างกฎเกณฑ์ทางกฎหมายเพื่อควบคุมการโจมตีทางไซเบอร์โดยเฉพาะขององค์การความร่วมมือเซี่ยงไฮ้มีลักษณะเป็นผลผลิตทางข้อตกลงทางการเมืองของรัฐที่มีผลประโยชน์ร่วมกัน เพื่อแย่งชิงอำนาจในการต่อรองในเวทีระหว่างประเทศของประเทศรัสเซียและจีนกับกลุ่มประเทศยุโรปและสหรัฐอเมริกามากกว่าความจำเป็นทางกฎหมาย

จากการศึกษาในส่วนนี้เกี่ยวกับความร่วมมือภายใต้องค์การระหว่างประเทศต่างๆ จะเห็นได้ว่า ประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นประเด็นหนึ่งในภัยคุกคามทางไซเบอร์ซึ่งองค์การระหว่างประเทศต่างแสดงความกังวลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับประเทศสมาชิกภายในองค์การระหว่างประเทศ โดยยังไม่มีความพยายามในการตั้งรับทางกฎหมายที่เป็นรูปธรรมมากนัก ส่วนใหญ่มุ่งเน้นไปที่การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ทั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธ โดยเฉพาะการป้องกันโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งอาจตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ เนื่องจากโครงสร้างพื้นฐานเหล่านั้นมีความสำคัญเป็นอย่างมากทั้งทางด้านเศรษฐกิจ การเมือง สังคม

---

[142] Henry Rõigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?," https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html. [March 15, 2016]

และการทหารจึงมีความเสี่ยงในการถูกโจมตีทางไซเบอร์ทั้งในสถานการณ์ปกติและในสถานการณ์การขัดกันทางอาวุธ

กล่าวได้ว่า องค์การระหว่างประเทศส่วนใหญ่เน้นไปที่การให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยทางไซเบอร์อันเป็นมาตรการเชิงป้องกัน ที่เป็นเช่นนี้เนื่องมาจากความสามารถของเทคโนโลยีในการปกปิดตัวตนของผู้กระทำและต้นตอที่มาของการโจมตีทางไซเบอร์ตลอดจนการพิสูจน์ว่าการโจมตีทางไซเบอร์ที่เกิดขึ้นเป็นการกระทำของฝ่ายใดด้วยเทคโนโลยีในขณะนี้ยังไม่มีเครื่องมือหรือวิธีการในการพิสูจน์ที่เป็นรูปธรรม การตั้งรับที่ดีที่สุดในขณะนี้จึงทำได้เพียงป้องกันระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ไม่ให้ถูกโจมตีทางไซเบอร์ผ่านมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั่นเอง

อย่างไรก็ตาม จากการศึกษาเกี่ยวกับความพยายามในทางระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธทั้งหมดข้างต้น ยังไม่พบความพยายามในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เป็นการตั้งรับในทางกฎหมายไม่ว่าจะภายในรัฐ ความร่วมมือระหว่างประเทศระดับทวิภาคี หรือในระดับพหุภาคีแต่อย่างใด ที่เป็นเช่นนี้อาจมีสาเหตุมาจากการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้ในการสู้รบเป็นประเด็นที่ค่อนข้างใหม่ แม้ว่าจะมีการหยิบยกขึ้นมาเจรจาหารือในทางทฤษฎีหรือมีการนำเทคโนโลยีไซเบอร์มาใช้ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในทางปฏิบัติแล้วก็ตาม จากตัวอย่างเหตุการณ์โจมตีทางไซเบอร์ที่เกิดขึ้นเห็นได้ว่าการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธยังไม่เป็นที่แพร่หลายและยังไม่ถึงขั้นเป็นสงครามไซเบอร์อย่างเต็มรูปแบบ ทำให้ความชัดเจนของประเด็นในทางกฎหมาย ผลกระทบเกี่ยวกับหลักการต่างๆ ตามกฎหมายระหว่างประเทศจึงไม่ชัดเจนเพียงพอที่จะสะท้อนแง่มุมหรือมิติของการละเมิดกฎหมายมนุษยธรรมระหว่างประเทศที่จะทำให้หน่วยงานต่างๆ หยิบยกประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธขึ้นมาเจรจาหารือในรายละเอียดอย่างเป็นรูปธรรมประกอบกับสถานการณ์การขัดกันทางอาวุธในปัจจุบันไม่ได้เกิดขึ้นอย่างแพร่หลายทำให้ในบางภูมิภาคจึงยังไม่เห็นความสำคัญของประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

อย่างไรก็ดี จากการศึกษาความพยายามในทางระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ทั้งในระดับรัฐ ความร่วมมือระหว่างประเทศระดับทวิภาคี และความร่วมมือภายใต้องค์การระหว่างประเทศสะท้อนให้เห็นความกังวลของประชาคมระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหรือสงครามไซเบอร์ที่อาจเกิดขึ้นในอนาคต โดยในระดับรัฐ ส่วนใหญ่จะมุ่งเน้นไปที่การเพิ่มขีดความสามารถทางด้านไซเบอร์ของกองทัพ

เช่นเดียวกับความร่วมมือระหว่างประเทศระดับทวิภาคีที่มีการแลกเปลี่ยนข้อมูล ความรู้ ความสามารถทางด้านไซเบอร์ ตลอดจนให้ความช่วยเหลือในการรับมือกับการโจมตีทางไซเบอร์ ในขณะที่ความร่วมมือภายใต้องค์การระหว่างประเทศส่วนใหญ่กำหนดให้การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นเพียงภัยคุกคามทางไซเบอร์อย่างหนึ่งและดำเนินการตั้งรับภายใต้มาตรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธ โดยไม่ได้ให้ความสำคัญกับบริบทการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นการเฉพาะแต่อย่างใด นอกจากนี้ ความพยายามในทางระหว่างประเทศเกี่ยวกับการสร้างกฎเกณฑ์หรือพัฒนากฎหมายระหว่างประเทศเพื่อควบคุมการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้น ยังไม่ได้รับความสำคัญในเวทีประชาคมระหว่างประเทศเท่าใดนัก

นอกเหนือจากการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในทางระหว่างประเทศแล้ว การควบคุมการโจมตีทางไซเบอร์ให้เป็นไปตามข้อบทของกฎหมายระหว่างประเทศเป็นอีกวิธีการหนึ่งที่ประชาคมระหว่างประเทศควรหันมาให้ความสำคัญ เมื่อหันมาพิจารณากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ในปัจจุบันกลับไม่พบว่ามีข้อบทเกี่ยวกับการใช้เทคโนโลยีในการสู้รบหรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธไว้แต่อย่างใดส่งผลให้เกิดแนวความคิดเกี่ยวกับการนำกฎหมายมนุษยธรรมระหว่างประเทศมาใช้บังคับกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่แตกต่างกันออกไป ซึ่งจะได้ศึกษาในส่วนต่อไป

2.3 แนวความคิดเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับกรณีการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

กฎหมายมนุษยธรรมระหว่างประเทศ (International Humanitarian Law) หรือกฎหมายว่าด้วยการขัดกันทางอาวุธ (Law of Armed Conflict) หรือ กฎหมายสงคราม (Law of War)[143]

[143] "What Is Ihl? (International Humanitarian Law: Answers to Your Questions)," (18 September 2015), https://www.icrc.org/en/document/what-ihl. [December 15, 2015]

กฎหมายมนุษยธรรมระหว่างประเทศ (International Humanitarian Law) หรือกฎหมายว่าด้วยการขัดกันทางอาวุธ (Law of Armed Conflict) หรือ กฎหมายสงคราม (Law of War) มีความหมายเดียวกัน โดยคณะกรรมการกาชาดระหว่างประเทศ องค์การระหว่างประเทศและรัฐต่างๆ นิยมเรียกว่า กฎหมายมนุษยธรรมระหว่างประเทศ (International Humanitarian Law)

เป็นสาขาหนึ่งของกฎหมายระหว่างประเทศบังคับใช้เมื่อเกิดสถานการณ์การขัดกันทางอาวุธ ไม่ว่าจะเป็นการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ (International Armed Conflict) หรือการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ (Non-International Armed Conflict) ประกอบด้วยหลักการเกี่ยวกับปฏิบัติการทางทหารสำหรับฝ่ายในการสู้รบ รวมทั้งหลักการเกี่ยวกับข้อจำกัดทางด้านวิธีการและปัจจัยในการสู้รบซึ่งมีที่มาจากทั้งสนธิสัญญาระหว่างประเทศและจารีตประเพณีระหว่างประเทศ เพื่อคุ้มครองพลเรือนและบุคคลที่ไม่ได้มีส่วนเกี่ยวข้องกับการสู้รบ แบ่งออกเป็น 2 กลุ่มใหญ่ๆ คือกลุ่มอนุสัญญาเจนีวาและกลุ่มอนุสัญญาเฮก โดยกลุ่มอนุสัญญาเจนีวาเป็นหลักการที่พื้นฐานสำคัญที่มุ่งคุ้มครองพลเรือนหรือผู้ที่ไม่มีส่วนเกี่ยวข้องในการสู้รบอีกต่อไปประกอบด้วยอนุสัญญาเจนีวา ค.ศ. 1949 ทั้ง 4 ฉบับ ได้แก่

- อนุสัญญาเจนีวาฉบับที่ 1 เพื่อฟื้นฟูสภาพของผู้ที่ได้รับบาดเจ็บและเจ็บป่วยของกองทัพในสนามรบ (Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949.)
- อนุสัญญาเจนีวาฉบับที่ 2 เพื่อฟื้นฟูสภาพของสมาชิกของกองทัพขณะอยู่ในทะเลซึ่งบาดเจ็บ เจ็บป่วยหรือผู้ซึ่งเรือต้องอับปาง (Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949.)
- อนุสัญญาเจนีวาฉบับที่ 3 เกี่ยวกับการปฏิบัติต่อเชลยศึก (Geneva Convention (III) relative to the Treatment of Prisoners of War of 12 August 1949.)
- อนุสัญญาเจนีวาฉบับที่ 4 เกี่ยวกับการคุ้มครองบุคคลพลเรือนในภาวะสงคราม (Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War of 12 August 1949.)

นอกจากนี้ยังมีพิธีสารเพิ่มเติมอนุสัญญาเจนีวาอีก 3 ฉบับ ได้แก่

- พิธีสารเพิ่มเติมอนุสัญญาเจนีวาลงวันที่ 12 สิงหาคม ค.ศ. 1949 เกี่ยวกับการคุ้มครองผู้ประสบภัยของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ (พิธีสารฉบับที่ 1) (Protocol Additional to the Geneva Conventions of 12 August 1949, and

relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.)

- พิธีสารเพิ่มเติมอนุสัญญาเจนีวาลงวันที่ 12 สิงหาคม ค.ศ. 1949 เกี่ยวกับการคุ้มครองผู้ประสบภัยของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ (พิธีสารฉบับที่ 2) (Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.)
- พิธีสารเพิ่มเติมอนุสัญญาเจนีวาลงวันที่ 12 สิงหาคม ค.ศ. 1949 เกี่ยวกับการเพิ่มสัญลักษณ์พิเศษของหน่วยงานกาชาดและสภาเสี้ยววงเดือนแดงระหว่างประเทศ (พิธีสารฉบับที่ 3) (Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem (Protocol III), 8 December 2005)

ส่วนกลุ่มอนุสัญญาเฮกเป็นหลักการพื้นฐานสำคัญเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบ (Means and Methods of Warfare) เนื่องจากการสู้รบไม่สามารถกระทำได้โดยปราศจากข้อจำกัดใดๆ และเพื่อจำกัดความเสียหายและความทุกข์ทรมานเกินความจำเป็นมีที่มาจากทั้งกฎหมายจารีตประเพณีระหว่างประเทศและกฎหมายสนธิสัญญาเป็นจำนวนมาก โดยกลุ่มอนุสัญญาเจนีวาและกลุ่มอนุสัญญาเฮกทั้งสองส่วนมีความเกี่ยวข้องกันอย่างใกล้ชิด[144] ตามที่ศาลยุติธรรมระหว่างประเทศกล่าวไว้ในความเห็นเชิงปรึกษา ค.ศ. 1996 คดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์ (Advisory Opinion of Legality of the Threat or Use of Nuclear Weapons)

เมื่อพิจารณาหลักการสำคัญตามกฎหมายมนุษยธรรมระหว่างประเทศครอบคลุมทั้งกลุ่มอนุสัญญาเจนีวาและกลุ่มอนุสัญญาเฮก จะเห็นได้ว่า ข้อบทกฎหมายตามกฎหมายมนุษยธรรมระหว่างประเทศล้วนมีอยู่ก่อนที่จะนำเทคโนโลยีเข้ามาใช้ในปฏิบัติการทางทหารและการสู้รบและไม่มีข้อบท

---

[144] ICJ, *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*, 1996. P. 256, Para. 75.

"These two (Hague Law and Geneva Law) branches of the law applicable in armed conflict have become so closely interrelated that they are considered to have gradually formed one single complex system, known today as international humanitarian law."

ตามกฎหมายมนุษยธรรมระหว่างประเทศใด ไม่ว่าจะเป็นจารีตประเพณีระหว่างประเทศหรืออนุสัญญากำหนดข้อบทเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธไว้เป็นการเฉพาะ

ด้วยเหตุดังกล่าว ส่งผลให้เกิดแนวความคิดที่แตกต่างกันเกี่ยวกับการนำกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ซึ่งเป็นกฎหมายที่ได้รับการยอมรับกันทั่วไปว่าเป็นกฎหมายระหว่างประเทศที่บังคับใช้เมื่อเกิดสภาวะสงครามหรือสถานการณ์การขัดกันทางอาวุธไปบังคับใช้กับการนำเทคโนโลยีมาใช้ในการสู้รบอย่างเช่นการโจมตีทางไซเบอร์ที่เกิดขึ้นในสถานการณ์การขัดกันทางอาวุธ ไม่ว่าจะในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศหรือการขัดกันทางอาวุธที่ไม่ลักษณะระหว่างประเทศ โดยกลุ่มแรกมีความเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้และ จำเป็นที่จะต้องกำหนดข้อบทกฎหมายบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธขึ้นเป็นการเฉพาะ เช่นเดียวกับอนุสัญญาที่ใช้ในการควบคุมอาวุธชีวภาพ อาวุธเคมี และอาวุธนิวเคลียร์[145]

ในขณะที่ อีกกลุ่มมีความเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้ โดยมีข้อท้าทายในการบังคับใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศบางประการ ดังมีรายละเอียดต่อไปนี้

2.3.1 กฎหมายมนุษยธรรมระหว่างประเทศไม่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

ด้วยลักษณะพิเศษของการโจมตีทางไซเบอร์ซึ่งเป็นการโจมตีที่ไม่มีลักษณะทางกายภาพและเป็นการโจมตีที่เกิดขึ้นในสมรภูมิห้วงไซเบอร์ซึ่งมีความแตกต่างจากสมรภูมิการรบอื่นทำให้นักวิชาการ

---

[145] อนุสัญญาห้ามอาวุธชีวภาพ (Biological Weapons Convention - BWC) อนุสัญญาห้ามอาวุธเคมี (Chemical Weapons Convention - CWC) สนธิสัญญาการไม่ขยายอาวุธนิวเคลียร์ Nuclear Non-Proliferation Treaty - NPT) และสนธิสัญญาว่าด้วยการห้ามทดลองนิวเคลียร์ (The Comprehensive Nuclear Test-Ban Treaty - CTBT)

กลุ่มนึง[146] มีความเห็นว่า กฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ไม่เพียงพอที่จะบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันเป็นเทคโนโลยีใหม่ได้ และเสนอให้มีการสร้างหลักการทางกฎหมายควบคุมการใช้เทคโนโลยีทางไซเบอร์ในปฏิบัติการทางทหารและการสู้รบไว้เป็นการเฉพาะเจาะจง

เหตุผลที่สำคัญในการสนับสนุนความเห็นดังกล่าวข้างต้นคือ ลักษณะพิเศษเกี่ยวกับการโจมตีทางไซเบอร์ ไม่ว่าจะเป็นอาวุธไซเบอร์มีราคาถูกเมื่อเทียบกับอาวุธประเภทอื่น โดยมีเพียงเครื่องคอมพิวเตอร์และอินเทอร์เน็ตก็สามารถทำการโจมตีทางไซเบอร์ได้ อาวุธไซเบอร์สามารถเข้าถึงได้ง่ายอย่างกว้างขวางไม่จำกัดเฉพาะรัฐเท่านั้น กลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรหรือตัวแสดงที่ไม่ใช่รัฐ (Non-state Actors) ล้วนสามารถเข้าถึงอาวุธไซเบอร์ได้อย่างเท่าเทียมกัน ลักษณะการโจมตีที่สามารถปกปิดหรืออำพรางตัวตนของผู้โจมตีและผู้ที่อยู่เบื้องหลังการโจมตีได้ การตรวจสอบหรือกลไกในการพิสูจน์ความจริงยังไม่มีประสิทธิภาพและเป็นรูปธรรม[147] ระยะทางอาณาเขต และดินแดนไม่เป็นอุปสรรคในการโจมตี ไม่ว่าจะอยู่ที่ใดโลกก็สามารถดำเนินการโจมตีทางไซเบอร์ได้

นอกจากนี้ กลุ่มที่มีความเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธยังให้เหตุผลว่ากฎเกณฑ์ตามกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ในปัจจุบันเป็นกฎเกณฑ์ที่ใช้ในการจัดการกับวิธีการและปัจจัยในการสู้รบที่ก่อให้เกิดการบาดเจ็บหรือเสียชีวิตหรือความเสียหายทางกายภาพต่อทรัพย์สิน โดยกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ไม่มีข้อบทในการจัดการกับความเสียหายทางไซเบอร์ที่อาจจะไม่ทำอันตรายต่อร่างกาย ชีวิตหรือความเสียหายต่อทรัพย์สิน[148]

---

[146] Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* (2011). Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict " *Harvard International Law Journal* 17, no. 1 (2006). Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," in *4th International Conferrence on Cyber Conflict*, ed. R. Ottis C. Czosseck, K. Ziolkowski(NATO CCD COE Publications, 2012). Oona A. Hathaway, "The Law of Cyber-Attack." Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86, no. 2 (2010). Stuart S. Malawer, "Cyber Warfare: Law and Policy Proposals for U.S. And Global Governance," *Virginia Lawyer* 58(2010).

[147] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," in 4th International Conferrence on Cyber Conflict, ed. R. Ottis C. Czosseck, K. Ziolkowski(NATO CCD COE Publications, 2012) P. 108.

[148] Olivia Solon, "Do We Need a Geneva Convention for Cyber Warfare?," wired.com, www.wired.co.uk/news/archive/2010-10/15/cyber-warfare-ethics. [March 30, 2016]

กลุ่มที่มีความเห็นว่า กฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ไม่เพียงพอที่จะใช้บังคับกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธยังเสนอความเห็นว่าจำเป็นที่จะต้องสร้างกฎเกณฑ์ระหว่างประเทศที่ควบคุมการโจมตีทางไซเบอร์ขึ้นเป็นการเฉพาะเช่นเดียวกับการทำสนธิสัญญาควบคุมอาวุธชีวภาพ อาวุธเคมี และอาวุธนิวเคลียร์ เพื่อลดการมีอยู่และจำกัดการใช้อาวุธไซเบอร์ พร้อมทั้งเสนอรูปแบบของสนธิสัญญาควบคุมอาวุธไซเบอร์จะต้องประกอบด้วยคำนิยามของการโจมตีทางไซเบอร์ ลักษณะการโจมตีทางไซเบอร์ และกฎเกณฑ์เกี่ยวกับการโจมตีทางไซเบอร์ซึ่งนำหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศต่างๆ เป็นพื้นฐานในการกำหนดกฎเกณฑ์ของสนธิสัญญาควบคุมอาวุธไซเบอร์[149] โดยประเทศรัสเซียถือเป็นประเทศแรกที่ผลักดันให้มีสนธิสัญญาควบคุมไซเบอร์ขึ้นในเวทีระหว่างประเทศทั้งในนามประเทศรัสเซีย และองค์การความร่วมมือเซี่ยงไฮ้ ตามที่ได้ศึกษามาแล้วข้างต้น ทั้งนี้ ประเทศรัสเซียเห็นว่าสนธิสัญญาระหว่างประเทศจะทำหน้าที่ในการจัดการกับความเสียเปรียบเกี่ยวกับการเข้าถึงอาวุธไซเบอร์[150] ในขณะที่สหรัฐอเมริกากลับมีความเห็นว่าสนธิสัญญาดังกล่าวไม่มีความจำเป็นแต่อย่างใด[151]

2.3.2 กฎหมายมนุษยธรรมระหว่างประเทศสามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้ โดยมีข้อท้าทายในการบังคับใช้บางประการ

นอกจากความเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ไม่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ได้ข้างต้น นักวิชาการอีกกลุ่มกลับมีความเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่สามารถที่จะบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้[152]

---

[149] Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict " Harvard International Law Journal 17, no. 1 (2006). P. 188.

[150] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," in *4th International Conferrence on Cyber Conflict*, ed. R. Ottis C. Czosseck, K. Ziolkowski(NATO CCD COE Publications, 2012) P. 96.

[151] John Markoff and Andrew E. Kramer, "U.S. And Russia Differ on a Treaty for Cyberspace," *The New York Times* 2009.[January 6, 2016]

[152] Erki Kodar, "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocal I," *ENDC Proceedings* 15(2012). Nils Melzer, "Cyber Operations and Jus in Bello," in *Confronting*

แม้ว่าจะไม่มีข้อบทตามกฎหมายมนุษยธรรมระหว่างประเทศที่กล่าวถึงการโจมตีทางไซเบอร์ไว้ก็ตาม อาทิ

คณะกรรมการกาชาดระหว่างประเทศภายใต้มติที่ประชุมองค์กรกาชาดและเสี้ยววงเดือนแดงระหว่างประเทศ ครั้งที่ 31[153] เห็นว่า ปฏิบัติการทางทหารใดที่ไม่ได้มีข้อบทกฎหมายควบคุมไว้เป็นการเฉพาะไม่ได้หมายความว่า ฝ่ายในการสู้รบจะสามารถใช้ปฏิบัติการทางทหารดังกล่าวได้อย่างไม่มีข้อจำกัด วิธีการและปัจจัยในการสู้รบ (Means and Method of Warfare) ที่มีการใช้เทคโนโลยีทางไซเบอร์อยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศ เมื่อปฏิบัติการไซเบอร์นั้นถูกนำมาใช้ในสถานการณ์การขัดกันทางอาวุธโดยฝ่ายในการสู้รบหรือในนามของฝ่ายในการสู้รบต่อฝ่ายตรงข้าม เพื่อที่จะทำให้เกิดความเสียหายแก่ฝ่ายตรงข้ามนั้น เช่น ใช้ปฏิบัติการไซเบอร์ในการจัดการระบบควบคุมการจราจรทางอากาศเป็นเหตุให้เกิดการชนกันของอากาศยานของพลเรือน การโจมตีดังกล่าวย่อมเป็นวิธีการในการสู้รบอย่างแท้จริงและอยู่ภายใต้บังคับข้อจำกัดตามกฎหมายมนุษยธรรมระหว่างประเทศ

ในทำนองเดียวกัน กลุ่มผู้เชี่ยวชาญผู้จัดทำร่างคู่มือทาลลินน์ (The Experts) มีความเห็นว่าการโจมตีทางไซเบอร์มีศักยภาพเทียบเท่ากับเป็นกองกำลังทางทหาร (Armed Force) และสามารถนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ได้ ปรากฏตามกฎข้อ 20 ของคู่มือทาลลินน์ระบุว่า “ปฏิบัติการทางไซเบอร์ที่ดำเนินการอยู่ภายในบริบทของการขัดกันทางอาวุธอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศ”[154]

Cyberconflict in Disarmament Forum, ed. Kerstin Vignard(Geneva: UNIDIR, 2011). Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.," *International Review of Red Cross* 94(2012). Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello," *International Review of the Red Cross* 84(2002). Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks," (2004), https://www.icrc.org/eng/resources/documents/misc/68lg92.htm. "Weapons: ICRC Statement to the United Nations, 2013," https://www.icrc.org/eng/resources/documents/statement/2013/united-nations-weapons-statement-2013-10-16.htm. [December 12, 2015]

[153] ICRC, "International Humanitarian Law and the Challenges of Contemporary Armed Conflict " in *31st International Conference of the Red Cross and Red Crescent*(Geneva, Switzerland2011). P. 36-37.

[154] *Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts* (2013)

Rule 20 – Applicability of the law of armed conflict

เหตุผลหลักที่ใช้สนับสนุนความคิดเห็นดังกล่าวมีที่มาจากหลักทั่วไปเกี่ยวกับอาวุธ วิธีการและปัจจัยในการสู้รบใหม่ตามข้อ 36 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1[155] บัญญัติว่า “ในการศึกษา การพัฒนา การได้มา หรือการยอมรับซึ่งอาวุธ วิธีการหรือปัจจัยในการสู้รบอันเป็นของใหม่ กำหนดให้คู่ภาคีผู้ทำสัญญาอยู่ภายใต้พันธกรณีในการพิจารณาว่าการใช้อาวุธหรือวิธีการหรือปัจจัยในการสู้รบอันเป็นของใหม่นั้น ในบางกรณีหรือทุกพฤติการณ์ จะถูกห้ามโดยพิธีสารฉบับนี้หรือกฎแห่งกฎหมายระหว่างประเทศอื่นๆ ที่ใช้บังคับกับอัครภาคีผู้ทำสัญญา”

จากข้อบทดังกล่าวข้างต้น ชี้ให้เห็นถึงการคาดการณ์ถึงการพัฒนาและใช้อาวุธ วิธีการหรือปัจจัยในการสู้รบใหม่ที่จะเกิดขึ้นของผู้ร่างพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 จากการที่กำหนดพันธกรณีให้รัฐพิจารณาความชอบด้วยกฎหมายของอาวุธ วิธีการและปัจจัยในการสู้รบซึ่งเป็นของใหม่ตามพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 และกฎหมายระหว่างประเทศอื่นๆ ถือเป็นการรับรองการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับเทคโนโลยีใหม่ที่จะเกิดขึ้นเหล่านั้น[156]

นอกจากนี้ เมื่อพิจารณาเหตุผลจากความเห็นของศาลยุติธรรมระหว่างประเทศเกี่ยวกับข้อโต้แย้งที่เสนอต่อศาลยุติธรรมระหว่างประเทศในความเห็นเชิงปรึกษาคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์ ค.ศ. 1996 (Advisory Opinion of Legality of the Threat or Use of Nuclear Weapons) ที่ระบุว่าการขาดข้อบทเกี่ยวกับอาวุธนิวเคลียร์ควรตีความว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่สามารถนำมาบังคับใช้กับการโจมตีด้วยอาวุธนิวเคลียร์ได้ แต่ถูกปฏิเสธในท้ายที่สุด โดยเทียบเคียงการขาดข้อบทเกี่ยวกับอาวุธนิวเคลียร์กับการขาดข้อบทเกี่ยวกับอาวุธไซเบอร์หรือการโจมตีทางไซเบอร์ในทำนองเดียวกัน

“Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.”

[155] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 36 - New weapons

“In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.”

[156] Heather Harrison Dinniss, Cyber Warfare and the Laws of War(the United States of America: Cambridge University Press, 2012). P. 128.

ศาลยุติธรรมระหว่างประเทศในความเห็นเชิงปรึกษาคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์สร้างบรรทัดฐานเพื่อหลีกเลี่ยงช่องว่างของกฎหมายโดยใช้วิธีการตีความและการเปรียบเทียบโดยให้เหตุผลว่าข้อกำหนดมาแตงส์ (Martens Clause) ซึ่งยังคงมีอยู่และนำไปบังคับใช้ได้อย่างไม่ต้องสงสัยนี้เป็นการยืนยันว่าหลักการและกฎเกณฑ์ของกฎหมายมนุษยธรรมระหว่างประเทศสามารถบังคับใช้กับอาวุธนิวเคลียร์ได้[157] ถือเป็นข้อสรุปในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ได้ด้วยเช่นกัน[158]

ทั้งนี้ เมื่อพิจารณาถึงวัตถุประสงค์ของข้อกำหนดมาแตงส์ที่ต้องการจำกัดขอบเขตสิทธิในการเลือกวิธีการและปัจจัยในการสู้รบ (Means and Methods of Warfare) ของฝ่ายในการสู้รบไม่ให้กระทำได้อย่างปราศจากข้อจำกัด และเพื่อกำจัดหรือขจัดเหตุการณ์ใดๆ ในสถานการณ์การขัดกันทางอาวุธที่ไม่ถูกควบคุมโดยข้อบทตามสนธิสัญญาหรือกฎหมายจารีตประเพณีระหว่างประเทศเป็นข้อยืนยันได้ว่า แม้จะปราศจากข้อบทไม่ว่าจะในสนธิสัญญาหรือกฎหมายจารีตประเพณีเกี่ยวกับการโจมตีทางไซเบอร์ไว้เป็นการเฉพาะ หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่สามารถนำไปบังคับใช้กับการโจมตีทางไซเบอร์ได้[159]

จากการศึกษาวิเคราะห์ความเห็นเกี่ยวกับการนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธทั้งสองความเห็นข้างต้น ผู้เขียนมีความเห็นว่า กฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้ แม้ว่าจะไม่มีข้อบทกฎหมายเกี่ยวกับการโจมตีทางไซเบอร์ตามกฎหมายมนุษยธรรมระหว่างประเทศก็ตาม โดยอ้างอิงจากข้อบทพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1 การเทียบเคียงความเห็นของศาลยุติธรรมระหว่างประเทศในความเห็นเชิงปรึกษาคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์ และวัตถุประสงค์ของกฎหมายมนุษยธรรมระหว่างประเทศในการให้คุ้มครองทางกฎหมายแก่พลเรือน

---

[157] ICJ. Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons, 1996. Para. 87.

"the Martens Clause, whose continuing existence and applicability is not to be doubted, as an affirmation that the principles and rules of humanitarian law apply to nuclear weapons."

[158] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello," International Review of the Red Cross 84(2002). P. 370.

[159] Erki Kodar, "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocal I," ENDC Proceedings 15(2012). P. 110.

นอกจากนี้ เมื่อพิจารณาร่างอนุสัญญาควบคุมอาวุธไซเบอร์ตามแนวความคิดที่เห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ก็ได้นำหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศมาเป็นกฎเกณฑ์ตามร่างอนุสัญญาควบคุมอาวุธไซเบอร์ที่นำเสนอด้วยเช่นกัน[160] จึงไม่อาจกล่าวได้ว่ากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ไม่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้

ยิ่งไปกว่านั้น สาเหตุที่มีสนธิสัญญาควบคุมอาวุธบางประเภทเป็นการเฉพาะ ไม่ว่าจะเป็นอาวุธเคมี อาวุธชีวภาพ อาวุธนิวเคลียร์เหล่านี้ล้วนมีพื้นฐานมาจากหลักการทั่วไปตามกฎหมายมนุษยธรรมระหว่างประเทศ ไม่ว่าจะเป็นอาวุธที่ก่อให้เกิดความทุกข์ทรมานโดยไม่จำเป็นหรือการบาดเจ็บเกินขนาด ไม่เหลือโอกาสในการรอดชีวิตก่อให้เกิดผลกระทบโดยไม่สามารถแยกแยะเป้าหมายได้[161] โดยเนื้อหาของสนธิสัญญาเหล่านั้นเป็นบริบทของการลดอาวุธ (Disarmament) และการไม่แพร่ขยายอาวุธ (Non-Proliferation) ไม่ใช่บริบทของสนธิสัญญาเกี่ยวกับหลักการด้านมนุษยธรรมแต่อย่างใด อีกทั้งการลดหรือไม่แพร่ขยายอาวุธไซเบอร์ไม่จำเป็นจะต้องอาศัยทรัพยากรหรือวิธีการยุ่งยากและไม่มีความเสี่ยงภัยใดๆ เหมือนเช่นการกำจัดอาวุธอื่นๆ อาทิ ทุ่นระเบิดสังหารบุคคล อาวุธเคมี อาวุธชีวภาพ อาวุธนิวเคลียร์ เพียงแค่ยกระดับหรืออัพเกรด (Upgrade) แทนที่ (Replace) หรือติดตั้งใหม่ (Installation) ระบบหรือเครือข่ายในการรักษาความปลอดภัยทางไซเบอร์ก็สามารถกำจัดหรือควบคุมอาวุธไซเบอร์ได้ ทั้งนี้ วิธีการในการควบคุมหรือจำกัดอาวุธไซเบอร์ที่มีประสิทธิภาพขึ้นอยู่กับการพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์ให้ทันกับการฉวยโอกาสจากช่องโหว่ของระบบปฏิบัติการหรือเครือข่ายที่จะเป็นช่องทางในการโจมตีทางไซเบอร์ได้

นอกจากนี้ ผู้เขียนเห็นว่าการจัดทำสนธิสัญญาระหว่างประเทศควบคุมการโจมตีทางไซเบอร์ยังมีข้อจำกัดหลายประการ อาทิ ความล่าช้าของกระบวนการในการจัดทำร่างสนธิสัญญา การลงนามและให้สัตยาบันสนธิสัญญาที่จะทำให้สนธิสัญญามีผลใช้บังคับซึ่งในเวลาที่สนธิสัญญาดังกล่าวมีผลใช้บังคับ เทคโนโลยีทางไซเบอร์นี้อาจพัฒนาไปไกลจนทำให้ข้อบทในสนธิสัญญาล้าสมัย อีกทั้ง

---

[160] Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict " Harvard International Law Journal 17, no. 1 (2006). P. 218.

[161] Robert Kolb and Richard Hyde, *An Introduction to the International Law of Armed Conflicts*(USA: Hart Publishing, 2008). P. 157.

สนธิสัญญาระหว่างประเทศดังกล่าวมีผลผูกพันเฉพาะรัฐเท่านั้นและบางรัฐอาจตั้งข้อสงวนในข้อบทบางประการทำให้สนธิสัญญาไม่สามารถบังคับใช้ได้อย่างเต็มที่และมีผลผูกพันเฉพาะรัฐที่ลงนามและให้สัตยาบันเท่านั้น ไม่รวมไปถึงกลุ่มที่ไม่ใช่รัฐ (Non-state Actors) ซึ่งเป็นฝ่ายในการสู้รบในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศที่สามารถเข้าถึงและใช้เทคโนโลยีทางไซเบอร์ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้เช่นเดียวกันกับรัฐ เนื่องจากกลุ่มติดอาวุธที่ไม่ใช่รัฐซึ่งเป็นฝ่ายในการสู้รบในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศไม่อาจเป็นภาคีของสนธิสัญญาได้ ข้อจำกัดเหล่านี้ส่งผลให้อาจเกิดสูญญากาศในการให้คุ้มครองพลเรือนและผู้บริสุทธิ์จากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธขึ้นได้

อย่างไรก็ตาม การบังคับใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ยังมีข้อท้าทายบางประการที่จำต้องพิจารณา ซึ่งผู้เขียนจะได้ศึกษาและวิเคราะห์การใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศในบทต่อไป

จากที่ได้ทำการศึกษาตลอดทั้งบทนี้ เห็นได้ชัดว่า การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธมีลักษณะพิเศษแตกต่างจากการโจมตีด้วยอาวุธตามแบบและมีสมรภูมิการรบเฉพาะคือห้วงไซเบอร์ซึ่งเป็นสมรภูมิการรบเสมือนจริง (Virtual Battlefield) ที่ไม่มีลักษณะทางกายภาพ ไม่มีพื้นที่ดินแดนหรืออาณาเขตของห้วงไซเบอร์ เป้าหมายในการโจมตีและ อาวุธหรือปัจจัยที่ใช้ในการโจมตีไม่ใช่พลรบ แต่มุ่งสร้างความเสียหายแก่ระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์อันเป็นเป้าหมายทางทหาร ลักษณะของการโจมตีทางไซเบอร์ในตัวเองไม่สามารถก่อให้เกิดการบาดเจ็บหรือเสียชีวิตของพลเรือนหรือพลรบได้ อาศัยความรู้ความเชี่ยวชาญเฉพาะทางด้านเทคโนโลยีในการโจมตี เครื่องมืออุปกรณ์หรืออาวุธไซเบอร์มีราคาถูก สามารถเข้าถึงได้ง่ายและเข้าถึงได้อย่างกว้างขวาง ไม่จำกัดเฉพาะรัฐ อาณาเขต ระยะทางดินแดนไม่เป็นอุปสรรคในการโจมตีทางไซเบอร์แต่อย่างใด โดยมีทั้งการโจมตีทางไซเบอร์ที่ดำเนินการร่วมกับการโจมตีด้วยอาวุธตามแบบเพื่อช่วยเหลือหรือสนับสนุนปฏิบัติการโจมตด้วยอาวุธตามแบบในการสร้างความเสียหายต่อเป้าหมายทางทหารและการโจมตีทางไซเบอร์เพียงลำพังที่ปราศจากการโจมตีด้วยอาวุธอื่นทั้งที่สามารถโจมตีต่อเป้าหมายได้อย่างเฉพาะเจาะจงและการโจมตีที่ไม่สามารถจำกัดเป้าหมายได้ด้วยลักษณะพิเศษและผลกระทบของการโจมตีทางไซเบอร์เหล่านี้ส่งผลให้มีการเปลี่ยนแปลงที่สำคัญทางการทหารหลายประการ ไม่ว่าจะเป็นการกำหนดหลักนิยม ยุทธศาสตร์ทางการทหาร การจัดตั้งหน่วยงานหรือกองกำลังทางทหารที่มีความรู้ความเชี่ยวชาญด้านเทคโนโลยีทางไซเบอร์เป็นการเฉพาะ

ตลอดจนความร่วมมือระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

ความพยายามในทางระหว่างประเทศในระดับพหุภาคีภายใต้องค์การระหว่างประเทศต่างๆ ส่วนใหญ่มุ่งเน้นไปที่การรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธ กล่าวได้ว่า ความร่วมมือระหว่างประเทศที่มีในขณะนี้ไม่ได้ให้ความสำคัญในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในทางกฎหมาย หรือการปรับปรุงกฎหมายระหว่างประเทศที่มีข้อบทควบคุมการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธแต่อย่างใด

แม้จะมีความร่วมมือระหว่างประเทศบางแห่ง เช่น องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ และองค์การความร่วมมือเซี่ยงไฮ้ได้พยายามดำเนินการพัฒนาและผลักดันทางด้านกฎหมายให้สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ แต่ยังไม่มีความชัดเจนและประสบความสำเร็จในเรื่องนี้เท่าใดนัก

อย่างไรก็ดี กลไกการรักษาความมั่นคงปลอดภัยทางไซเบอร์ผ่านความร่วมมือระหว่างประเทศนับเป็นก้าวสำคัญของการจัดการปัญหาสงครามไซเบอร์ที่มีอยู่ในปัจจุบัน องค์การระหว่างประเทศถือเป็นเวทีในการปรึกษาหารือและสะท้อนมุมมองของรัฐต่างๆ เกี่ยวกับการควบคุมการโจมตีทางไซเบอร์และเป็นจุดเริ่มต้นที่ดีของการควบคุมการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนี้

เมื่อหันมาพิจารณากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่กลับไม่มีข้อบทเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การณ์การขัดกันทางอาวุธ ส่งผลให้เกิดแนวความคิดเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศซึ่งเป็นกฎหมายระหว่างประเทศที่บังคับใช้เมื่อมีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นแตกต่างกันออกไป โดยมีทั้งแนวความคิดที่เห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่สามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ จำเป็นต้องมีสนธิสัญญาควบคุมอาวุธไซเบอร์หรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธขึ้นเป็นการเฉพาะและแนวความคิดที่เห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศสามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้

จากการที่กฎหมายมนุษยธรรมระหว่างประเทศไม่มีข้อบทเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธและมีอยู่ก่อนที่จะมีการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบดังที่ได้กล่าวมาแล้ว เมื่อการโจมตีทางไซเบอร์มีลักษณะพิเศษแตกต่างจากการโจมตีด้วยอาวุธตามแบบการนำกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่บังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจะสามารถบังคับได้หรือไม่ อย่างไร ลักษณะพิเศษของการโจมตีทางไซเบอร์ก่อให้เกิดข้อท้าทายในการบังคับใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ อย่างไร ซึ่งผู้เขียนจะได้ศึกษาในบทที่ 3 ต่อไป

บทที่ 3
การใช้หลักการของกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวเนื่องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

จากเนื้อหาบทที่แล้ว จะเห็นได้ว่า แม้แนวโน้มในการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบรวมทั้งความกังวลของประชาคมระหว่างประเทศเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหรือสงครามไซเบอร์จะมีเพิ่มมากขึ้น แต่ความพยายามในทางระหว่างประเทศของประชาคมระหว่างประเทศในการรับมือกับการโจมตีทางไซเบอร์ที่เห็นเป็นรูปธรรมในปัจจุบันมีเพียงการให้ความคุ้มครองแก่พลเรือนผู้บริสุทธิ์ผ่านนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ซึ่งเป็นมาตรการในการรับมือในทางปฏิบัติเท่านั้น ในส่วนของการรับมือทางกฎหมายเกี่ยวกับการส่งเสริมหรือปรับปรุงกฎหมายระหว่างประเทศเพื่อควบคุมการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นการเฉพาะยังไม่พบความพยายามที่เป็นรูปธรรมเท่าใดนักเมื่อเทียบกับภัยคุกคามไซเบอร์อย่างอื่น ไม่ว่าจะเป็นอาชญากรรมทางไซเบอร์ การก่อการร้ายทางไซเบอร์ อย่างไรก็ดีนอกจากการให้ความคุ้มครองผ่านกลไกความร่วมมือระหว่างประเทศ การให้ความคุ้มครองผ่านข้อบทกฎหมายมนุษยธรรมระหว่างประเทศซึ่งเป็นกฎหมายที่บังคับใช้เมื่อเกิดสถานการณ์การขัดกันทางอาวุธถือเป็นกลไกสำคัญหนึ่งที่เป็นหลักประกันในการให้ความคุ้มครองแก่พลเรือนจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

เนื้อหาในบทนี้จะทำการศึกษาและวิเคราะห์เกี่ยวกับการใช้หลักการของกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวเนื่องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยส่วนแรกจะศึกษาวิเคราะห์การนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยแบ่งการศึกษาออกเป็นการบังคับใช้เมื่อมีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นแล้วกับการบังคับใช้กับการโจมตีทางไซเบอร์ที่ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธทั้งการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ หลังจากนั้นจึงจะทำการศึกษาวิเคราะห์หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวเนื่องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้แก่หลักการเกี่ยวกับปฏิบัติการทางทหารและการให้ความคุ้มครองพลเรือนและทรัพย์สินพลเรือน เพื่อวิเคราะห์เกี่ยวกับข้อท้าทายในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในบทถัดไป ดังมีรายละเอียดดังต่อไปนี้

3.1 การนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

ในการพิจารณาการนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจำต้องแบ่งแยกการพิจารณาเป็น 2 กรณี ได้แก่ กรณีการโจมตีทางไซเบอร์ที่เกิดขึ้นในระหว่างสถานการณ์การขัดกันทางอาวุธตามแบบกับกรณีการโจมตีทางไซเบอร์ที่ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธขึ้น ซึ่งมีเงื่อนไขในการนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้แตกต่างกันพิจารณาได้ดังต่อไปนี้

3.1.1 การโจมตีทางไซเบอร์กับสถานการณ์การขัดกันทางอาวุธตามแบบ

กฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้เมื่อเกิดสภาวะสงครามระหว่างประเทศและใช้อยู่ตลอดเวลาที่มีการขัดแย้งทางอาวุธซึ่งเป็นสภาวะที่ไม่ปกติในความสัมพันธ์ทางกฎหมายระหว่างรัฐกับพลเมืองของฝ่ายตรงข้าม[162]

คำว่า “การขัดกันทางอาวุธ (Armed Conflict)” นั้น กฎหมายมนุษยธรรมระหว่างประเทศไม่ได้กำหนดคำนิยามที่ชัดเจนไว้ ไม่ว่าจะในอนุสัญญาเจนีวา 1949 ทั้ง 4 ฉบับและในพิธีสารเพิ่มเติมอนุสัญญาเจนีวา 1977 ทั้ง 2 ฉบับ เป็นเรื่องที่ผู้ร่างอนุสัญญาที่ต้องการหลีกเลี่ยงการโต้เถียงทางการเมืองหรือทางกฎหมายที่เกิดขึ้นในเรื่องคำนิยามทางกฎหมายของสงครามและความแตกต่างที่ตามมาระหว่างสภาวะสงความ การกระทำของตำรวจหรือการกระทำที่เป็นปฏิปักษ์ใดๆ ตั้งใจให้เป็นเรื่องของข้อเท็จจริงโดยไม่ประสงค์ที่จะจำกัดความหมายไว้ด้วยนิยามทางกฎหมาย[163]

---

[162] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 24.

[163] Jean S. Pictet, *Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.*(Switzerland: ICRC, 1952). P. 32.

อย่างไรก็ตาม คำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (The International Criminal Tribunal for the Former Yugoslavia: ICTY) ในคดี Prosecutor v. Dusko Tadic ได้ให้ลักษณะของการขัดกันทางอาวุธไว้ว่า “การขัดกันทางอาวุธมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหารระหว่างรัฐหรือการใช้ความรุนแรงทางทหารที่ยืดเยื้อระหว่างองค์กรของรัฐและกลุ่มขบวนการติดอาวุธหรือระหว่างกลุ่มดังกล่าวภายในรัฐ”

ดังนั้น จากการให้ลักษณะของการขัดกันทางอาวุธตามคำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวียข้างต้น กล่าวได้ว่า เงื่อนไขสำคัญในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศคือการมีอยู่ของการขัดกันทางอาวุธ (Existence of an Armed Conflict) ไม่ว่าฝ่ายในการสู้รบจะยอมรับการมีอยู่ของการขัดกันทางอาวุธหรือไม่ก็ตาม[164] และสิ้นสุดลงเมื่อมีการทำสนธิสัญญาสันติภาพหรือการยืนยันอย่างชัดแจ้งและเป็นทางการจากรัฐฝ่ายต่างๆ ที่เกี่ยวข้องเท่านั้น[165] โดยไม่คำนึงว่าจะเป็นการใช้กำลังทางทหารในรูปแบบใด ไม่ว่าจะเป็นปฏิบัติการทางบก ทางอากาศ ทางน้ำ ไม่ขึ้นอยู่กับอาวุธที่ใช้ อาจเป็นอาวุธปืนไปจนถึงระดับอาวุธนิวเคลียร์และอาวุธชีวภาพ โดยไม่คำนึงถึงความรุนแรงหรือร้ายแรงที่ฝ่ายตรงข้ามได้รับหรือความเสียหายมากน้อยเพียงใด[166]

ในสถานการณ์การขัดกันทางอาวุธตามแบบ (Conventional Armed Conflict) ซึ่งเป็นการขัดกันทางอาวุธด้วยการใช้วิธีการหรือปัจจัยในการสู้รบแบบดั้งเดิมในการเผชิญหน้าทางทหาร เช่น

---

[164] Common Article 2 of "The Geneva Conventions of 12 August 1949."

“..., even if the state of war is not recognized by one of them.”

[165] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 53.

[166] วราภรณ์ เหลืองทอง, "ปัญหาในการนิยามคำว่า "การขัดกันทางอาวุธ" อันเป็นเงื่อนไขสำหรับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ" (มหาวิทยาลัยธรรมศาสตร์, 2553). หน้า 30.

การระเบิด การยิงปืนใหญ่ หรือการเคลื่อนกำลังพลกองทหาร[167] เหล่านี้ถือเป็นการใช้กำลังทางทหารอย่างไม่มีข้อโต้แย้งและอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศ

จากการศึกษาข้างต้น เมื่อพิจารณาเงื่อนไขของการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์เป็นการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบเป็นวิธีการหรือปัจจัยในการสู้รบใหม่ แม้จะมีลักษณะพิเศษแตกต่างจากการโจมตีทางอาวุธตามแบบ (Conventional Weapons) หรืออาวุธร้ายแรงที่ทำอันตรายถึงตายซึ่งใช้ทั่วไปในการสู้รบปัจจุบัน เช่น ปืน จรวด หรือลูกระเบิด (Kinetic Weapons)[168] แต่การโจมตีทางไซเบอร์สามารถสร้างความเสียหายและผลกระทบต่อชีวิตและทรัพย์สินได้เช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ เช่น การโจมตีเครือข่ายคอมพิวเตอร์ต่อระบบควบคุมการจราจรทางอากาศของสนามบินขนาดใหญ่ เพื่อทำให้อากาศยานชนกัน การโจมตีต่อระบบในการปล่อยสารเคมีที่เป็นพิษจากโรงงานผลิตและจัดเก็บ ทำให้สารเคมีรั่วไหล จะเห็นได้ว่าเมื่อมีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น ไม่ว่าจะใช้วิธีการหรือปัจจัยในการสู้รบแบบใด ฝ่ายในการสู้รบจะต้องนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้เสมอ โดยไม่จำต้องคำนึงถึงอาวุธ วิธีการและปัจจัยในการสู้รบที่ใช้จะมีลักษณะพิเศษใดๆ ก็ตาม ดังนั้น การโจมตีทางไซเบอร์แม้จะเป็นการนำเทคโนโลยีมาใช้ในการสู้รบมีลักษณะพิเศษแตกต่างจากการโจมตีด้วยอาวุธตามแบบ หากดำเนินการโจมตีทางไซเบอร์ในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธตามแบบเกิดขึ้นอยู่ย่อมเข้าเงื่อนไขในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศและจะต้องอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกับการโจมตีด้วยอาวุธอื่นๆ

ยกตัวอย่าง การโจมตีทางไซเบอร์ซึ่งดำเนินการในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นแล้ว ได้แก่ การโจมตีทางไซเบอร์ที่เกิดขึ้นระหว่างสถานการณ์การขัดกันทางอาวุธระหว่างประเทศรัสเซียกับจอร์เจียในปี ค.ศ. 2008 การใช้กำลังทางทหารระหว่างจอร์เจียและรัสเซีย รวมทั้งการประกาศภาวะสงครามโดยจอร์เจียซึ่งนอกจากจะมีการโต้ตอบกันด้วยการโจมตีด้วยอาวุธตามแบบไม่ว่าจะเป็นการใช้อาวุธหนัก ระเบิดพวง การทิ้งระเบิดจากอากาศยาน ยังมีการโจมตีทางไซเบอร์ด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอสต่อประเทศจอร์เจียซึ่งเชื่อว่าเป็นการกระทำของรัสเซีย (ในขณะที่ทำการวิจัยนี้ ยังไม่มีการพิสูจน์ว่าเป็นการกระทำความผิดของรัสเซียจริง)

---

[167] Duncan B. Hollis, "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?," ed. Claire Findkelstein and Kevin Govern Jens David Ohlin, *CYBERWAR: LAW &ETHICS FOR VIRTUAL CONFLICTS* (Oxford University Press, 2014). P. 18.

[168] สหพงษ์ เครือเพ็ชร, "ระบบอาวุธเลเซอร์," วารสารหลักเมืองมกราคม 2558. หน้า. 18.

สถานการณ์การขัดกันทางอาวุธดังกล่าวนับว่าเป็นสถานการณ์การขัดกันทางอาวุธที่มีการใช้การโจมตีทางไซเบอร์ร่วมกับการโจมตีด้วยอาวุธตามแบบครั้งแรก[169]

เมื่อพิจารณากรณีการขัดกันทางอาวุธระหว่างประเทศรัสเซียกับจอร์เจียข้างต้น มีลักษณะเป็นการใช้กำลังทางทหารระหว่างรัฐสองรัฐ ได้แก่ประเทศรัสเซียและประเทศจอร์เจียและมีการประกาศภาวะสงครามโดยประเทศจอร์เจีย การโจมตีทางไซเบอร์ที่เกิดขึ้นในขณะที่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นจึงอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ เนื่องจากการโจมตีทางไซเบอร์ดำเนินการในระหว่างที่การขัดกันทางอาวุธยังคงมีอยู่อันเป็นเงื่อนไขในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศจึงสามารถนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ที่เกิดขึ้นในระหว่างสถานการณ์การขัดกันทางอาวุธระหว่างรัสเซียและจอร์เจียดังกล่าวได้

สรุปได้ว่า การโจมตีทางไซเบอร์ที่ดำเนินการในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธตามแบบ (Conventional Armed Conflict) เกิดขึ้น จะต้องอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ เนื่องจากการมีอยู่ของสถานการณ์การขัดกันทางอาวุธเป็นเงื่อนไขในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศโดยไม่ต้องคำนึงว่าอาวุธ วิธีการและปัจจัยในการโจมตีทางไซเบอร์นั้นจะมีลักษณะพิเศษแตกต่างจากการโจมตีด้วยอาวุธตามแบบอย่างไร

ส่วนการโจมตีทางไซเบอร์ซึ่งดำเนินการในขณะที่ยังไม่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น กรณีนี้จำเป็นต้องพิจารณาว่าการโจมตีทางไซเบอร์โดยลำพัง ปราศจากการการโจมตีด้วยอาวุธตามแบบร่วมด้วยสามารถเป็นชนวนเริ่มต้นในการเกิดสถานการณ์การขัดกันทางอาวุธอันเป็นเงื่อนไขสำคัญอย่างหนึ่งในการนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้หรือไม่ ซึ่งจะได้ศึกษาในส่วนต่อไป

---

[169] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (the United States of America: Cambridge University Press, 2012). P. 127.

3.1.2 การโจมตีทางไซเบอร์กับการเกิดสถานการณ์การขัดกันทางอาวุธ

ในกรณีที่ยังไม่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น หากรัฐหนึ่งเริ่มต้นดำเนินการโจมตีทางไซเบอร์ต่อเป้าหมายทางทหารของอีกรัฐหนึ่ง การโจมตีทางไซเบอร์ดังกล่าวจะอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่นั้น การพิจารณาในส่วนนี้ เป็นการพิจารณาว่าการโจมตีทางไซเบอร์เทียบได้กับการใช้กำลังทางทหาร (Armed Attack) ตามความหมายทั่วไปในกฎหมายระหว่างประเทศหรือไม่ มีนัยสำคัญ 2 ประการคือ

ในแง่มุมของกฎหมายระหว่างประเทศว่าด้วยสิทธิของรัฐในการใช้กำลังทางทหาร (Jus Ad Bellum) เพื่อพิจารณาว่ามีการโจมตีที่ถือว่าเป็นการละเมิดกฎหมายระหว่างประเทศตามที่กำหนดไว้ในข้อบทของกฎบัตรสหประชาชาติ[170]หรือไม่ เนื่องจากกฎบัตรสหประชาชาติและกฎหมายระหว่างประเทศทั่วไปตามการใช้กำลังทางอาวุธที่มีลักษณะเป็นการรุกรานและการละเมิดต่อสันติภาพซึ่งตามความหมายดังกล่าว การใช้กำลังทางอาวุธมีลักษณะเป็นการใช้กำลังทางอาวุธของกองทัพของรัฐและการใช้อาวุธตามแบบ[171] ซึ่งไม่อยู่ในกรอบการศึกษาวิเคราะห์ของวิทยานิพนธ์เล่มนี้

แต่ในขณะเดียวกันก็มีอีกนัยยะหนึ่งที่มีความสำคัญกับการพิจารณาในบริบทของกฎหมายมนุษยธรรมระหว่างประเทศ เนื่องจากการพิจารณาว่ากฎหมายมนุษยธรรมระหว่างประเทศจะเริ่มใช้บังคับหรือไม่นั้น ขึ้นอยู่กับว่ามีการขัดกันทางอาวุธ (Armed Conflict) เกิดขึ้นหรือไม่ ในปัจจุบันมีแนวทางในการพิจารณาซึ่งกำหนดไว้ตามคำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (The International Criminal Tribunal for the Former Yugoslavia: ICTY) ในคดี Prosecutor v. Dusko Tadic ให้ลักษณะของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศไว้ดังนี้

---

[170] United Nations, "Charter of the United Nations."

Article 2 (4)

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

(XXIX) United Nations General Assembly Resolution 3314, "Resolution 3314 (Xxix), Definition of Aggression,"(1970).

[171] *The Charter of the United Nations*, ed. Daniel-Erasmus Khan Bruno Simma, Georg Nolte, and Andreas Paulus, Third Edition, A Commentary (Oxford: Oxford University Press, 1995). pp. 609-610.

คือ “การขัดกันทางอาวุธมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหารระหว่างรัฐ...”[172] ซึ่งการพิจารณาดังกล่าวเป็นนัยยะในการพิจารณาที่ 2 ซึ่งเป็นข้อน่าสนใจในการพิจารณาว่า หากมีการเริ่มต้นด้วยการโจมตีทางไซเบอร์จะถือเป็นการตั้งต้นหรือชนวนเริ่มต้นให้มีการขัดกันทางอาวุธเกิดขึ้นได้หรือไม่ ในแง่ของการเทียบเคียงว่าการเริ่มต้นโจมตีทางไซเบอร์นั้นจะเทียบเคียงกับการโจมตีโดยใช้อาวุธแบบดั้งเดิมอันเป็นการใช้กำลังทางทหารได้หรือไม่

เนื่องจากกฎหมายมนุษยธรรมระหว่างประเทศสามารถแบ่งลักษณะการขัดกันทางอาวุธออกเป็น 2 ประเภทใหญ่ๆ ได้แก่ การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ (International Armed Conflict) และการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ (Non-International Armed Conflict) ซึ่งมีที่มาจากจารีตประเพณีระหว่างประเทศตามข้อบทในอนุสัญญาเจนีวา 1949 และพิธีสารเพิ่มเติมอนุสัญญาเจนีวา 1977 ดังนั้น ในการศึกษาวิทยานิพนธ์นี้ จะได้แบ่งการศึกษาการเกิดการขัดกันทางอาวุธ (Armed Conflict) จากการโจมตีทางไซเบอร์ออกเป็น 2 ประเภทใหญ่ๆ ได้แก่

1. การโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ
2. การโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ

ทั้งนี้ การโจมตีทางไซเบอร์ที่เคยเกิดขึ้นในสถานการณ์การขัดกันทางอาวุธ ส่วนใหญ่จะเป็นการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ และอาจจะมีบ้างที่เป็นการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ[173] การพิจารณาว่าการโจมตีทางไซเบอร์ใดก่อให้เกิดสถานการณ์การขัดกันทางอาวุธซึ่งอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศสามารถพิจารณาได้ดังต่อไปนี้

---

[172] *The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* 2 October 1995. Para. 70.

“...an armed conflict exists whenever there is a resort to armed force between States...”

[173] Erki Kodar, "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocal I," ENDC Proceedings 15(2012). P. 109.

3.1.2.1 การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ

การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ (International Armed Conflict) หรือที่เรียกอีกอย่างหนึ่งว่า ความขัดแย้งระหว่างรัฐต่อรัฐ (Inter-State Conflict) มีข้อบทเกี่ยวกับลักษณะของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศตามข้อ 2 ร่วมของอนุสัญญาเจนีวา 1949 กำหนดว่า “อนุสัญญานี้บังคับใช้กับทุกกรณีที่มีการประกาศสงครามหรือกรณีการขัดกันทางอาวุธใดๆ ที่เกิดขึ้นระหว่างสองรัฐหรือมากกว่าของรัฐภาคีสมาชิก แม้ว่ารัฐที่เป็นฝ่ายในการสู้รบฝ่ายหนึ่งฝ่ายใดจะไม่ยอมรับว่ามีภาวะสงครามเกิดขึ้น และอนุสัญญานี้บังคับใช้กับทุกกรณีที่มีการยึดครองดินแดนของรัฐภาคี ไม่ว่าทั้งหมดหรือเพียงบางส่วน แม้ว่าการยึดครองดังกล่าวไม่มีการใช้กำลังทางทหารต่อต้านก็ตาม”[174]

และมีคำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (The International Criminal Tribunal for the Former Yugoslavia: ICTY) ในคดี Prosecutor v. Dusko Tadic ได้ให้ลักษณะของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศไว้ว่า “การขัดกันทางอาวุธมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหารระหว่างรัฐ...”[175]

นอกจากนี้ คณะกรรมการกาชาดระหว่างประเทศ (International Committee of the Red Cross) เสนอคำนิยามของการขัดกันอาวุธที่มีลักษณะระหว่างประเทศว่าการขัดกันทาง

---

[174] "The Geneva Conventions of 12 August 1949."

Common Article 2.

“In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.”

[175] *The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* (2 October 1995), Para. 70.

“...an armed conflict exists whenever there is a resort to armed force between States...”

อาวุธที่มีลักษณะระหว่างประเทศมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหาร (Resort to Armed Force) ระหว่างสองรัฐหรือมากกว่าสองรัฐขึ้นไป[176]

จากการศึกษาข้อบทของอนุสัญญาเจนีวา 1949 ประกอบกับคำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (ICTY) และคำนิยามของคณะกรรมการกาชาดระหว่างประเทศดังกล่าวพอสรุปได้ว่า การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหาร ระหว่างรัฐสองรัฐหรือมากกว่าสองรัฐขึ้นไป โดยมีเงื่อนไขที่สำคัญของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ คือ จะต้องมีการใช้กำลังทางทหาร (Armed Force)[177]

เมื่อพิจารณาลักษณะของการโจมตีทางไซเบอร์ซึ่งดำเนินการภายในห้วงไซเบอร์ (Cyberspace) ที่ไม่มีลักษณะทางกายภาพ อาวุธไซเบอร์ (Cyber Weapons) ก็ไม่ถือเป็นอาวุธตามแบบ (Conventional Weapons) หรืออาวุธร้ายแรงที่ทำอันตรายถึงตายซึ่งใช้ทั่วไปในการสู้รบปัจจุบัน เช่น ปืน จรวด หรือลูกระเบิด (Kinetic Weapons) อย่างไรก็ตาม เป็นที่ชัดเจนว่าการโจมตีทางไซเบอร์สามารถสร้างความเสียหายและผลกระทบต่อพลเรือนได้เช่นเดียวกับอาวุธที่ใช้ในปัจจุบัน

ประเด็นสำคัญที่ต้องพิจารณาคือ การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศสามารถเกิดขึ้นโดยมีชนวนเริ่มต้นมาจากการโจมตีทางไซเบอร์โดยปราศจากการใช้กำลังทางทหารหรือการโจมตีด้วยอาวุธที่ทำอันตรายถึงตายอย่างอื่นประกอบได้หรือไม่ การพิจารณาการเกิดสถานการณ์การขัดกันทางอาวุธโดยการโจมตีทางไซเบอร์มีลักษณะเงื่อนไขเช่นเดียวกับการเกิดสถานการณ์การขัดกันทางอาวุธจากการใช้กำลังด้วยอาวุธตามแบบหรือไม่ อย่างไร ทั้งนี้ หากการโจมตีทางไซเบอร์ใดสามารถพิจารณาว่าเป็นการกระทำที่ก่อให้เกิดการขัดกันทางอาวุธได้เช่นเดียวกับการขัดกันทางอาวุธที่เกิดจากการใช้กำลังด้วยอาวุธ การโจมตีทางไซเบอร์ดังกล่าวย่อมอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศด้วยเช่นเดียวกัน

---

[176] ICRC Opinion paper, "How Is the Term "Armed Conflict" Defined in International Humanitarian Law? ,"(ICRC, 2008). P. 5.

[177] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (the United States of America: Cambridge University Press, 2012). P. 122.

เมื่อพิจารณาลักษณะเงื่อนไขของสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศกับลักษณะพิเศษของการโจมตีทางไซเบอร์ประกอบกันสามารถสรุปได้ว่า ลักษณะการโจมตีทางไซเบอร์ที่สามารถเป็นชนวนเริ่มต้นก่อให้เกิดสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องประกอบด้วยเงื่อนไขที่สำคัญสองประการ ได้แก่ (1) เป็นการกระทำของรัฐ (Attributable to the State) และ (2) เทียบเท่ากับการใช้กำลังทางทหาร (Amounts to a Resort of Armed Force)[178] โดยมีรายละเอียดดังต่อไปนี้

3.1.2.1.1 เป็นการกระทำของรัฐ

เงื่อนไขนี้สะท้อนจากความในข้อ 2 ร่วมของอนุสัญญาเจนีวา 1949 ที่ว่า “...การขัดกันทางอาวุธใดๆ ที่เกิดขึ้นระหว่างสองรัฐหรือมากกว่าของอัครภาคีผู้ทำสัญญา...”[179] แสดงว่าฝ่ายในการสู้รบที่เกิดขึ้นจะต้องเป็นประเทศหรือรัฐ เนื่องจาก “รัฐ” เท่านั้นที่สามารถเป็นภาคีอนุสัญญาเจนีวา 1949 ได้ เพียงแค่มีสถานะเป็นรัฐจะเป็นรัฐภาคีอนุสัญญาเจนีวาหรือไม่ก็ตาม เนื่องจากอนุสัญญาเจนีวาทั้ง 4 ฉบับ มีลักษณะเป็นจารีตประเพณีระหว่างประเทศซึ่งได้รับการยอมรับเป็นสากลแล้ว รัฐที่เกี่ยวข้องในการสู้รบจะต้องนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้เพื่อคุ้มครองพลเรือนผู้ที่ไม่มีส่วนเกี่ยวข้องกับการสู้รบหรือบุคคลอื่นตามที่กฎหมายมนุษยธรรมระหว่างประเทศให้ความคุ้มครอง แม้จะไม่ได้เป็นภาคีแห่งอนุสัญญาก็ตาม

นอกจากนี้ ผู้ทำคำอธิบายอนุสัญญาเจนีวา 1949 มีความเห็นว่า ความขัดแย้งใดๆ ที่เกิดขึ้นระหว่างสองรัฐและนำไปสู่การแทรกแซงของสมาชิกของกองกำลังติดอาวุธเป็น

---

[178] Michael N. Schmitt, "Classification of Cyber Conflict," *Journal of Conflict & Security Law* 17, no. 2 (2012).; Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks," (2004), Available at: https://www.icrc.org/eng/resources/documents/misc/68lg92.htm.; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (the United States of America: Cambridge University Press, 2012). ; Nils Melzer, "Cyberwarfare and International Law," *NUIDIR Resources Paper* (2011). Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.," International Review of Red Cross 94(2012).

[179] "The Geneva Conventions of 12 August 1949."

Common Article 2.

“...armed conflicts which may arise between two or more of the High Contracting Parties...”

การขัดกันทางอาวุธที่อยู่ภายในความหมายของข้อ 2 ของอนุสัญญาเจนีวา 1949 แม้ว่า ฝ่ายในการสู้รบฝ่ายหนึ่งฝ่ายใดจะปฏิเสธการมีอยู่ของภาวะสงครามก็ตาม โดยไม่ต้องคำนึงว่าความขัดแย้งจะมีอยู่ยาวนานเพียงใด หรือการฆ่าล้างจะเกิดขึ้นมากน้อยเพียงใด หรือว่ามีกองกำลังที่เข้าร่วมเป็นจำนวนเท่าใดก็ตาม[180]

เมื่อพิจารณาจากข้อ 2 ร่วมของอนุสัญญาเจนีวา 1949 ประกอบกับคำอธิบายข้อ 2 ร่วมของอนุสัญญาเจนีวา 1949 ข้างต้น สรุปได้ว่า การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นความขัดแย้งที่มีการใช้กำลังทางทหารระหว่างสองรัฐขึ้นไป โดยไม่คำนึงว่ารัฐที่เป็นฝ่ายในการสู้รบจะยอมรับหรือไม่ว่ามีการสู้รบเกิดขึ้น หรือไม่คำนึงว่าการสู้รบดังกล่าวจะมีระยะเวลายาวนานเพียงใด หรือไม่คำนึงว่าจะมีการสังหารฆ่าล้างเกิดขึ้นหรือไม่ก็ตาม ทั้งนี้ การขัดกันททางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นการใช้กำลังทางทหารที่ “เป็นการกระทำของรัฐ” เนื่องจากฝ่ายในการสู้รบของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นรัฐเท่านั้น

นอกจากนี้ การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องมีลักษณะระหว่างประเทศ (International) หมายความว่า จะต้องเป็นการกระทำที่ดำเนินการหรือควบคุมโดยรัฐ (Conducted by a State) หรือเป็นการกระทำของรัฐ (Attributable to a State)[181] ด้วยเงื่อนไขเดียวกันนี้ เมื่อพิจารณาการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นการโจมตีทางไซเบอร์ที่เป็นการกระทำของรัฐ ไม่ว่าจะดำเนินการหรือควบคุมโดยรัฐหรือเป็นการกระทำของรัฐ การโจมตีทางไซเบอร์ที่ดำเนินการโดยองค์กรอื่นของรัฐ เช่น หน่วยสืบราชการลับหรือหน่วยงานบังคับใช้กฎหมายของรัฐก็อยู่ในเงื่อนไขนี้เช่นกัน ทั้งนี้ องค์กรของรัฐให้หมายความรวมถึงบุคคลธรรมดาหรือนิติบุคคลซึ่งมีสถานะตามกฎหมายภายในของรัฐ[182] ตามความเห็นของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวียในคดี Tadic ซึ่งกล่าวว่า

---

[180] Jean S. Pictet, *Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. Geneva, 12 August 1949.(Switzerland: ICRC, 1952).P. 23.

[181] Michael Schmitt, "Classification of Cyber Conflict," Journal of Conflict & Security Law 17, no. 2 (2012). P. 252.

[182] ILC, "Responsibility of States for Internationally Wrongful Acts," in *Yearbook of the International Law Commission, 2001, vol. II (Part Two)* (UN, 2005). Article 4(2).

“ปัจเจกชนที่กระทำการภายในขอบข่ายหรือเกี่ยวกับกองกำลังทหารหรือสมรู้ร่วมคิดกับหน่วยงานของรัฐอาจจะพิจารณาว่าเป็นองค์กรของรัฐโดยพฤตินัยได้”[183]

ดังนั้น การโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นการโจมตีทางไซเบอร์ที่ดำเนินการโดยองค์กรของรัฐ (State Organs) หรือเป็นการกระทำของรัฐ (Attributable to the State) ซึ่งสอดคล้องตามกฎหมายระหว่างประเทศว่าด้วยความรับผิดของรัฐ ไม่จำกัดเฉพาะว่าจะต้องเป็นการกระทำของสมาชิกในกองกำลังทหารของรัฐ แต่รวมถึงการกระทำของบุคคลอื่นที่กระทำในนามรัฐหรือเป็นตัวแทนของรัฐด้วย เช่น พลเรือนที่ดำเนินการแทนกองกำลังทหารของรัฐ[184]

จากการศึกษาสรุปได้ว่า เงื่อนไขในการพิจารณาการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นการโจมตีทางไซเบอร์ที่สามารถพิจารณาได้ว่าเป็นการโจมตีทางไซเบอร์ที่ดำเนินการหรือควบคุมโดยรัฐ หรือเป็นการกระทำของรัฐกระทำต่ออีกรัฐหนึ่ง ไม่คำนึงว่าจะมีระยะเวลาในการโจมตีทางไซเบอร์ยาวนานเพียงใด หรือว่าการโจมตีทางไซเบอร์นั้นจะก่อให้เกิดการบาดเจ็บ เสียชีวิตหรือไม่ก็ตาม ดังเช่น เหตุการณ์การโจมตีทางไซเบอร์ด้วยวิธีการแทรกซึมความปลอดภัยทางเครือข่ายคอมพิวเตอร์ของโรงงานนิวเคลียร์ประเทศอิหร่านต่อระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) เป็นเหตุให้เครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์เสียหายตามที่ได้ศึกษาในบทที่ 2 มาแล้ว หากพบว่ากรณีดังกล่าว รัฐอยู่เบื้องหลังการโจมตีทางไซเบอร์นั้น ย่อมเข้าข่ายว่าเป็นการกระทำของรัฐอันเป็นเงื่อนไขของสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศได้

กรณีตัวอย่างข้างต้นเป็นการโจมตีทางไซเบอร์ที่ก่อให้เกิดความเสียหายทางกายภาพ แต่หากการโจมตีทางไซเบอร์ที่กระทำโดยรัฐหนึ่งต่ออีกรัฐหนึ่งไม่ก่อให้เกิดการบาดเจ็บหรือความเสียหายทางกายภาพจะเป็นจุดเริ่มต้นของการขัดกันทางอาวุธได้หรือไม่นั้น คณะกรรมการกาชาดระหว่างประเทศเห็นว่า ปฏิบัติการทางไซเบอร์ที่ทำให้วัตถุไร้ความสามารถ (Disable) ก็ถือเป็น

---

[183] *Prosecutor V . Tadic, (Appeal Judgment), Case It-94-1-A*, 15 July 1999 15 July 1999. Para. 144.

[184] Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks," (2004), Available at: https://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

การโจมตี แม้จะไม่ก่อให้เกิดความเสียหายทางกายภาพก็ตาม[185] ทั้งนี้ คณะกรรมการกาชาดระหว่างประเทศยังได้กล่าวต่อไปว่าคำตอบที่แน่ชัดในประเด็นดังกล่าวจะต้องอาศัยแนวทางปฏิบัติของรัฐ (State Practice) ในอนาคตต่อไป

เมื่อพิจารณาเงื่อนไขการเป็นการกระทำของรัฐประกอบกับลักษณะของการโจมตีทางไซเบอร์ข้างต้น สรุปได้ว่าการโจมตีทางไซเบอร์ที่ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศหรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นการโจมตีทางไซเบอร์ที่เป็นการกระทำของรัฐดำเนินการหรือควบคุมโดยรัฐหนึ่งปฏิบัติการโจมตีต่อระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของอีกรัฐหนึ่ง (หรือมากกว่าหนึ่งรัฐขึ้นไป) ภายในห้วงไซเบอร์ โดยไม่คำนึงว่าจะมีรัฐยอมรับว่ามีการขัดกันทางอาวุธเกิดขึ้นหรือไม่ หรือว่าการโจมตีทางไซเบอร์จะมีระยะเวลายาวนานเพียงใด

อย่างไรก็ตาม ด้วยศักยภาพของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่สามารถปกปิดตัวตน ที่มาของการโจมตี ตลอดจนปกปิดร่องรอยในการพิสูจน์ว่าเป็นการกระทำของรัฐ ซึ่งในขณะที่ทำการศึกษาวิจัยวิทยานิพนธ์เล่มนี้ยังไม่พบว่ามีเครื่องมือหรือวิธีการที่สามารถแกะรอยการโจมตีทางไซเบอร์และพิสูจน์ว่าเป็นการกระทำของฝ่ายใดที่เป็นรูปธรรมและเป็นที่ยอมรับก่อให้เกิดข้อท้าทายเกี่ยวกับเงื่อนไขในการพิจารณาว่าเป็นการกระทำของรัฐ ซึ่งจะได้อธิบายรายละเอียดข้อท้าทายดังกล่าวในบทถัดไป

3.1.2.1.2 เทียบเท่ากับการใช้กำลังทางทหาร

จากข้อ 2 ร่วมของอนุสัญญาเจนีวา 1949 เพียงแค่มีการใช้กำลังทางทหารระหว่างรัฐสองรัฐขึ้นไปก็เพียงพอที่จะพิจารณาว่าเป็นการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศได้[186] โดยไม่ต้องคำนึงถึงสาเหตุหรือความรุนแรงในการเผชิญหน้า อีกทั้งไม่จำต้องมีการประกาศสงครามหรือการยอมรับว่ามีสถานการณ์การสู้รบ โดยยืนยันตามคำอธิบายอนุสัญญาเจนีวาของ

---

[185] ICRC, "International Humanitarian Law and the Challenges of Contemporary Armed Conflict " in 31st International Conference of the Red Cross and Red Crescent(Geneva, Switzerland2011). P. 37.

[186] Geneva Academy of International Humanitarian Law and Human Rights, "Qualification of Armed Conflicts," (2012), http://www.geneva-academy.ch/RULAC/qualification_of_armed_conflict.php. [September 23, 2015]

คณะกรรมการกาชาดระหว่างประเทศที่มีต่อข้อ 2 ร่วม โดยสรุปว่า “ความขัดแย้งใดๆ ที่เกิดขึ้นระหว่างรัฐสองรัฐและนำไปสู่การแทรกแซงของการใช้กำลังทางทหาร (Intervention of Armed Forces) คือ การขัดกันทางอาวุธภายในความหมายของข้อ 2 ร่วมของอนุสัญญาเจนีวา 1949 แม้ว่าหนึ่งในรัฐคู่กรณีจะปฏิเสธการมีอยู่ของภาวะสงครามก็ตาม โดยไม่คำนึงว่าความขัดแย้งจะมีอยู่เป็นเวลานานแค่ไหนหรือการฆ่านองเลือดจะเกิดขึ้นมากน้อยเพียงใด”[187]

นอกจากนี้ คำอธิบายของคณะกรรมกากาชาดระหว่างประเทศในข้อ 1 พิธีสารเพิ่มเติมอนุสัญญาเจนีวา 1977 ฉบับที่ 1 อธิบายว่า กฎหมายมนุษยธรรมระหว่างประเทศครอบคลุมถึงการขัดแย้งใดๆ ระหว่างสองรัฐที่เกี่ยวข้องกับการใช้กำลังทางทหารของพวกเขา (Use of their Armed Force) โดยทั้งระยะเวลาของความขัดแย้งและความรุนแรงของความขัดแย้งไม่มีบทบาทสำคัญ[188] และคำอธิบายของคณะกรรมการกาชาดระหว่างประเทศที่มีต่อข้อบทของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2 อธิบายการขัดกันทางอาวุธไว้ว่าเป็น “การมีอยู่ของการสู้รบระหว่างกองกำลังทางทหาร ซึ่งมีการจัดรูปแบบลักษณะองค์กรในระดับมากหรือน้อย[189]

เมื่อพิจารณาจากคำอธิบายอนุสัญญาเจนีวา 1949 และพิธีสารเพิ่มเติมอนุสัญญาเจนีวา 1977 ข้างต้นแสดงให้เห็นว่า เงื่อนไขที่จำเป็นของการขัดกันทางอาวุธที่มีลักษณะ

---

[187] Jean S. Pictet, Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.(Switzerland: ICRC, 1952).P. 32.

“Any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place.”

[188] Jean DE PREUX Claude PILLOUDt, Yves SANDOZ, Bruno ZIMMERMANN, Philippe Eberlin, Hans-Peter Gasser and Claude F. Wenger, , "Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949," ed. ICRC(Netherlands Martinus Nijhoff Publishers 1987).Para. 62.

“...humanitarian law...covers any dispute between two States involving the use of their armed forces. Neither the duration of the conflict, nor its intensity, play a role;... “

[189]ibid., Para. 4341.

"armed conflict" ... existence of open hostilities between armed forces which are organized to a greater or lesser degree.”

ระหว่างประเทศคือการใช้กำลังทางทหาร[190] ดังนั้น การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องสามารถพิจารณาได้ว่าเทียบเท่ากับการใช้กำลังทางทหารตามเงื่อนไขของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ

จากการศึกษา ไม่พบว่ามีข้อบทกฎหมายหรือคำพิพากษาของศาลระหว่างประเทศใดกล่าวว่าการโจมตีทางไซเบอร์เทียบเท่ากับการใช้กำลังทางทหารตามกฎหมายมนุษยธรรมระหว่างประเทศไว้อย่างชัดเจน อย่างไรก็ตาม ผู้เชี่ยวชาญทางด้านกฎหมายส่วนใหญ่มีความเห็นว่าการโจมตีทางไซเบอร์สามารถพิจารณาเทียบเท่ากับการใช้กำลังทหารตามกฎหมายมนุษยธรรมระหว่างประเทศได้ ดังนี้

Cordula Droege ผู้เชี่ยวชาญทางด้านกฎหมายของคณะกรรมการกาชาดระหว่างประเทศให้ความเห็นว่าในกรณีที่ปราศจากการใช้กำลังร้ายแรงที่ทำอันตรายถึงตาย (Kinetic Force) และอาวุธดั้งเดิม (Traditional Weapons) การโจมตีทางไซเบอร์สามารถพิจารณาว่าเทียบเท่ากับการใช้กำลังทางทหารได้ โดยการเปรียบเทียบความคล้ายคลึงกันของผลกระทบจากการโจมตีทางไซเบอร์กับผลกระทบจากการใช้กำลังทางทหารร้ายแรงที่ทำอันตรายถึงตาย (Kinetic Force) ซึ่งการเปรียบเทียบดังกล่าวเป็นประโยชน์สำหรับการพิจารณาการโจมตีทางไซเบอร์ที่นำไปสู่การเสียชีวิต การบาดเจ็บของบุคคล หรือความเสียหายทางกายภาพ หรือการทำลายโครงสร้างพื้นฐานที่สำคัญ[191] ยกตัวอย่าง การโจมตีทางไซเบอร์ที่ทำให้เครื่องบินหรือรถไฟพุ่งเข้าชนกันเป็นสาเหตุให้เกิดการสูญเสียชีวิตหรือบาดเจ็บของพลเรือนได้เช่นเดียวกับการโจมตีด้วยอาวุธที่ทำอันตรายถึงตาย (Kinetic Weapons)

ทั้งนี้ Cordula Droege เห็นว่าการเปรียบเทียบผลกระทบที่เกิดขึ้นอาจไม่เพียงพอที่จะพิจารณาว่าการโจมตีทางไซเบอร์เป็นการใช้กำลังทางทหาร เนื่องจากลักษณะการโจมตีทางไซเบอร์ส่วนใหญ่ไม่ได้ถูกใช้เพื่อทำลายหรือสร้างความเสียหายทางกายภาพต่อโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructures) โดยตรง แต่ใช้เพื่อให้เกิดผลกระทบต่อปฏิบัติการทางทหารและการทำงานของโครงสร้างพื้นฐานมากกว่า เช่น การโจมตีทางไซเบอร์ต่อโครงข่ายไฟฟ้าทำให้ไม่

---

[190] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello," International Review of the Red Cross 84(2002). P. 372.

[191] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.," International Review of Red Cross 94(2012). P. 546.

สามารถทำงานได้ โดยที่ไม่มีความเสียหายทางกายภาพเกิดขึ้น การโจมตีเหล่านี้ย่อมไม่มีความเสียหายทางกายภาพเกิดขึ้นในทันที

การพิจารณาว่าการโจมตีทางไซเบอร์ที่ไม่ก่อให้เกิดความเสียหายทางกายภาพขึ้นในทันทีมีศักยภาพเทียบเท่ากับการใช้กำลังทางทหารหรือไม่นั้น Cordula Droege เสนอวิธีการพิจารณา 2 วิธีการ ดังนี้

วิธีการแรก เป็นการพิจารณาว่าการโจมตีทางไซเบอร์ก่อให้เกิดผลกระทบต่อปฏิบัติการทางทหารหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญของพลเรือนดั่งเช่นการใช้กำลังทางทหารหรือไม่ หากการโจมตีทางไซเบอร์ใดก่อให้เกิดผลกระทบต่อปฏิบัติการทางทหารหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญแล้ว การโจมตีทางไซเบอร์ดังกล่าวสามารถพิจารณาได้ว่าเทียบเท่ากับการใช้กำลังทางทหาร วิธีการนี้เป็นไปตามวัตถุประสงค์ของกฎหมายมนุษยธรรมระหว่างประเทศในการให้ความคุ้มครองแก่พลเรือนและผู้ที่ไม่มีส่วนเกี่ยวข้องจากการสู้รบและหลีกเลี่ยงช่องว่างในการให้ความคุ้มครอง ดังนั้น การโจมตีทางไซเบอร์โดยรัฐที่มีจุดมุ่งหมายในการทำให้ปฏิบัติการทางทหารหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญของพลเรือนเหล่านั้นไร้ความสามารถ ถือเป็นการใช้กำลังทางทหารอันเป็นเงื่อนไขสำคัญของการเกิดสถานการณ์การขัดกันทางอาวุธได้[192]

วิธีการที่สอง เป็นการพิจารณาปัจจัยต่างๆ เกี่ยวกับการใช้กำลังทางทหารรวมกัน ไม่เน้นเฉพาะการพิจารณาผลกระทบของการโจมตีทางไซเบอร์เหมือนเช่นวิธีการแรก ปัจจัยเกี่ยวกับการใช้กำลังทางทหารที่ต้องพิจารณา อาทิ ความรุนแรงของผลกระทบที่เกิดจากการโจมตีทางไซเบอร์ อาวุธเครื่องมือที่ใช้ในการโจมตีทางไซเบอร์ ความเกี่ยวข้องของกองกำลังทหารหรือหน่วยงานอื่นของรัฐในการโจมตีทางไซเบอร์ ลักษณะของเป้าหมาย (ว่าเป็นเป้าหมายทางทหารหรือไม่) และระยะเวลาของการโจมตี เช่น เมื่อผู้บัญชาการกองกำลังทหารของรัฐหนึ่งถูกสังหารจากการโจมตีทางอากาศโดยรัฐอื่นหรือถูกสังหารโดยการส่งจดหมายอาบยาพิษ การกระทำเหล่านี้สามารถพิจารณาว่า

---

[192] Ibid.

เป็นการใช้กำลังทางทหารในสถานการณ์การขัดกันทางอาวุธได้[193] หรือการที่มีบุคคลถูกยิงหรือถูกจับกุมตามคำสั่งของรัฐภายใต้สถานการณ์ที่มีกองกำลังทางทหารของสองรัฐเข้ามาเกี่ยวข้องถือได้ว่าเป็นการใช้กำลังทางทหารอันเป็นเงื่อนไขในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ ในขณะที่กรณีอื่น อาจจำเป็นจะต้องมีความรุนแรงของสถานการณ์ระดับสูง (A High Level of Violence) ประกอบในการพิจารณาว่าเป็นการใช้กำลังทางทหาร เช่น การส่งข้อมูลโดยสายลับที่ถูกส่งมาจากรัฐบาลของเขาจากต่างประเทศ[194]

เมื่อพิจารณาตามวิธีการที่สองนี้ การโจมตีทางไซเบอร์ที่เกิดขึ้นในระยะเวลาสั้นๆ สามารถพิจารณาเป็นกองกำลังทางทหารได้ หากว่าการโจมตีดังกล่าวทำให้เกิดผลกระทบที่รุนแรง ยกตัวอย่าง การโจมตีทางไซเบอร์ด้วยสตักซ์เน็ต (Stuxnet) ก่อให้เกิดความเสียหายต่อเครื่องหมุนเหวี่ยง (IR-1 Centrifuges) ประมาณ 1000 ตัวตามที่มีการรายงานข่าว จนเป็นเหตุให้ต้องมีการเปลี่ยนเครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์เพื่อปรับปรุงคุณภาพยูเรเนียม (Uranium Enrichment) ในโรงงานนิวเคลียร์ ที่เมือง Natanz อิหร่าน[195] หากเครื่องหมุนเหวี่ยงเหล่านั้น ถูกทำลายด้วยการใช้ระเบิดหรือปืนที่มีอานุภาพร้ายแรงโดยกองกำลังทางอากาศของรัฐอื่น การโจมตีดังกล่าวย่อมพิจารณาได้ว่าเป็นการใช้กองกำลังทางทหารและเป็นจุดเริ่มต้นของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศอย่างชัดเจนได้ Cordula Droege ยังให้ข้อสังเกตว่าในการจัดหมวดหมู่ของการขัดกันทางอาวุธไม่ได้ขึ้นอยู่กับท่าทีของรัฐที่เกี่ยวข้องว่ามีความเห็นอย่างไร แต่แนวทางปฏิบัติของรัฐ (State Practice) และความเชื่อว่าเป็นกฎหมาย (Opinion Juris) ของรัฐ เป็นตัวกำหนดการตีความกฎหมายระหว่างประเทศในเรื่องคำนิยามของการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ การจัดหมวดหมู่ของการขัดกันทางไซเบอร์ (Cyber Conflicts) เหล่านี้จะกำหนดให้ชัดเจนได้จากแนวทางปฏิบัติของรัฐในอนาคตต่อไป

---

[193] Ibid.

[194] Antoine A. Bouvier and Anne Quintin Marco Sassòli, *How Does Law Protect in War?*, ed. Third, vol. I(Geneva: ICRC, 2011). P. 122.

[195] David Albright, "Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?."

Nils Melzer ผู้เชี่ยวชาญทางด้านกฎหมายของศูนย์นโยบายด้านความมั่นคงปลอดภัยแห่งนครเจนีวา (Geneva Centre for Security Policy) และที่ปรึกษากฎหมายของคณะกรรมการกาชาดระหว่างประเทศ เห็นว่าปฏิบัติการไซเบอร์สามารถก่อให้เกิดผลกระทบเช่นเดียวกับการใช้กำลังร้ายแรงที่ทำอันตรายถึงตาย (Kinetic Force) กล่าวคือ ก่อให้เกิดการเสียชีวิต การบาดเจ็บของบุคคล หรือความเสียหาย การทำลายซึ่งทรัพย์สินได้ โดยปฏิบัติการไซเบอร์ของรัฐสามารถยกระดับไปสู่การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศได้ หากวางแผนให้เกิดความเสียหายต่อรัฐอื่น ไม่เพียงแต่ทำให้เกิดการเสียชีวิต การบาดเจ็บ ของบคุล หรือการทำลาซึ่งทรัพย์สินเท่านั้น แต่ยังรวมถึงการทำให้ส่งผลกระทบโดยตรงต่อปฏิบัติการทางทหารหรือความสามาร ถทางทหารของรัฐอื่น โดยการโจมตีทางไซเบอร์เพียงลำพังจะสามารถเป็นการขัดกันทางอาวุธได้หรือไม่นั้นอาจจะได้รับการพิจารณาอย่างชัดเจนผ่านแนวทางปฏิบัติของรัฐในอนาคตเท่านั้น[196]

Michael Schmitt ผู้เชี่ยวชาญด้านกฎหมายประจำวิทยาลัยการทัพเรือของสหรัฐอเมริกา (United States Naval War College) เห็นว่าปฏิบัติการไซเบอร์ (Cyber Operations) เทียบเท่ากับการโจมตีที่มีลักษณะ“ติดอาวุธ” (Armed) ตามกฎหมายมนุษยธรรมระหว่างประเทศ โดยข้อ 49 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ให้คำนิยาม การโจมตี (Attacks) ว่าเป็นการกระทำรุนแรงต่อฝ่ายตรงข้ามในการสู้รบที่เป็นปฏิปักษ์ ไม่ว่าในการรุกรานหรือการป้องกัน[197] ถึงแม้ว่าปฏิบัติการไซเบอร์ (Cyber Operations) จะไม่ได้มีความรุนแรงในตัวมันเอง แต่ปฏิบัติการไซเบอร์สามารถก่อให้เกิดผลกระทบที่มีความรุนแรงได้ (Violent Consequences) กล่าวคือ สามารถทำให้เกิดการบาดเจ็บ การเสียชีวิตของบุคคล หรือการทำลาย ความเสียหายต่อทรัพย์สินได้ การโจมตีทางไซเบอร์ที่ก่อให้เกิดผลกระทบดังกล่าวย่อมอยู่ในเกณฑ์ “ติดอาวุธ” (Armed) ในการขัดกันทางอาวุธ[198] ยกตัวอย่าง ถ้ารัฐอยู่เบื้องหลังการโจมตีด้วยสตักซ์เน็ต (Stuxnet) ต่อระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ซึ่งควบคุมเครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์ใน

---

[196] Nils Melzer, "Cyberwarfare and International Law," NUIDIR Resources Paper (2011). P. 24-25.

[197] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 49 (1)

“Attacks” means acts of violence against the adversary, whether in offence or in defence.”

[198] Michael Schmitt, "Classification of Cyber Conflict," Journal of Conflict & Security Law 17, no. 2 (2012). P. 251.

โรงพลังงานนิวเคลียร์ของอิหร่าน เมื่อปี ค.ศ. 2010 อันเป็นการก่อให้เกิดความเสียหายทางกายภาพต่อทรัพย์สิน ย่อมอยู่ภายในเกณฑ์ของการโจมตีตามกฎหมายมนุษยธรรมระหว่างประเทศ อย่างไรก็ตาม ปฏิบัติการไซเบอร์โดยรัฐหนึ่งที่กระทำต่อรัฐอื่นที่ไม่ก่อให้เกิดความการบาดเจ็บหรือความเสียหายทางกายภาพจะเป็นจุดเริ่มต้นให้เกิดการขัดกันทางอาวุธได้หรือไม่นั้น ขึ้นอยู่กับแนวทางปฏิบัติของรัฐ (State Practice) ว่าเป็นไปในทิศทางใด

นอกจากนี้ คู่มือทาลลินน์ (Tallinn Manual) ให้ลักษณะของการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศไว้ตามกฎข้อ 22 คู่มือทาลลินน์ไว้ว่าการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศมีอยู่เมื่อใดก็ตามที่มีการสู้รบซึ่งเกิดขึ้นระหว่างสองรัฐหรือมากกว่าสองรัฐขึ้นไป ซึ่งอาจรวมถึงหรือถูกจำกัดโดยปฏิบัติการทางไซเบอร์[199] โดยการให้ลักษณะของคู่มือทาลลินน์เป็นการนำเอาเงื่อนไขตามข้อ 2 ร่วมของอนุสัญญาเจนีวาซึ่งมีที่มาจากกฎหมายจารีตประเพณีระหว่างประเทศใช้เป็นพื้นฐานของกฎข้อนี้

ในส่วนของการพิจารณาว่าการโจมตีทางไซเบอร์เป็นการใช้กำลังทางทหารหรือเทียบเท่าการใช้กำลังทางทหารหรือไม่นั้น ผู้เขียนมีความเห็นว่าแม้ว่าการโจมตีทางไซเบอร์จะเป็นการกระทำที่มุ่งโจมตีต่อเป้าหมายที่เป็นเครื่องคอมพิวเตอร์ เครือข่ายหรือระบบทางสารสนเทศและคอมพิวเตอร์ภายในห้วงไซเบอร์ไม่ได้เป็นการกระทำที่มุ่งกระทำเพื่อให้เกิดการบาดเจ็บหรือเสียชีวิตของบุคคลหรือการทำลายทรัพย์สินโดยตรง แต่การโจมตีทางไซเบอร์สามารถพิจารณาว่าเทียบเท่ากับการใช้กำลังทางทหารได้ พิจารณาจากความเสียหายหรือผลกระทบที่เกิดขึ้นจากการโจมตีทางไซเบอร์ ซึ่งหากการโจมตีทางไซเบอร์ใดสามารถสร้างความเสียหายทางกายภาพต่อทรัพย์สินและเป็นเหตุให้เกิดการบาดเจ็บหรือเสียชีวิตของบุคคลได้เช่นเดียวกับการโจมตีด้วยอาวุธต่างๆ การโจมตีทางไซเบอร์นั้นย่อมพิจารณาได้ว่าเทียบเท่ากับการใช้กำลังทางทหาร ยกตัวอย่าง การโจมตีทางไซเบอร์ต่อระบบ

---

[199] *Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts*

Rule 22 – Characterisation as International Armed Conflict

"An international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more States."

การจัดการจราจรทางอากาศยานเพื่อเข้าควบคุมเครื่องบิน เพื่อทำให้เครื่องบินชนกันหรือเครื่องบินตกเป็นเหตุให้ผู้โดยสารได้รับบาดเจ็บหรือเสียชีวิตอันเป็นความเสียหายเช่นเดียวกับการยิงขีปนาวุธโจมตีเครื่องบินกลางอากาศ การโจมตีทางไซเบอร์ต่อระบบการจัดการจราจรทางอากาศยานดังกล่าวย่อมพิจารณาได้ว่าเทียบเท่าการใช้กำลังทางทหาร

เมื่อพิจารณาเงื่อนไขการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศทั้งหมด สรุปได้ว่า การโจมตีทางไซเบอร์ที่ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศซึ่งสามารถนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้ได้นั้นจะต้องเป็นการโจมตีทางไซเบอร์ที่เทียบเท่ากับการใช้กำลังทางทหารซึ่งดำเนินการหรือควบคุมหรือเป็นการกระทำของรัฐหนึ่งโจมตีต่อระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของอีกรัฐหนึ่ง (หรือมากกว่าหนึ่งรัฐขึ้นไป) ภายในห้วงไซเบอร์

ยกตัวอย่างเช่น หากรัฐ A ดำเนินการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ B จนเป็นเหตุให้โครงสร้างพื้นฐานที่สำคัญของรัฐ B ไม่สามารถใช้การได้ การติดต่อสื่อสารขัดข้องทั้งหมด ไม่สามารถติดต่อขอความช่วยเหลือจากรัฐอื่นได้ โรงงานผลิตกระแสไฟฟ้า น้ำ พลังงานของรัฐ B ขัดข้องเสียหายใช้การไม่ได้เป็นเหตุให้ประชาชนได้รับบาดเจ็บหรือเสียชีวิตจากการขาดสาธารณูปโภคพื้นฐานที่สำคัญ หรือหากกองกำลังทหารของรัฐ A ดำเนินการโจมตีทางไซเบอร์ต่อระบบการจัดการจราจรทางอากาศยานและอากาศยานรบของรัฐ B จนเป็นเหตุให้อากาศยานชนกันกลางอากาศหรือเข้าบังคับระบบการบินอัตโนมัติของอากาศยานรบเป็นเหตุให้อากาศยานพุ่งชนอาคารก่อสร้างของรัฐ B จนทำให้พลเรือนได้รับบาดเจ็บหรือเสียชีวิตและอาคารก่อสร้างทรัพย์สินต่างๆ ได้รับความเสียหายหรือถูกทำลาย ทั้งสองกรณีอาจพิจารณาได้ว่าเป็นการโจมตีทางไซเบอร์ซึ่งก่อให้เกิดสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศได้ อย่างไรก็ตาม ความแน่ชัดของการเกิดสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจากการโจมตีทางไซเบอร์นี้จำเป็นจะต้องอาศัยแนวทางปฏิบัติของรัฐในอนาคตต่อไป

ในส่วนต่อไปจะได้ศึกษาวิเคราะห์ว่าการโจมตีทางไซเบอร์ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศซึ่งเป็นเงื่อนไขสำคัญในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศได้หรือไม่ เพียงใด มีเงื่อนไขในการพิจารณาอย่างไรบ้าง

3.1.2.2 การโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ

การบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศมิได้ใช้บังคับเฉพาะกับการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศเท่านั้นยังขยายขอบเขตของการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศไปยังกรณีการขัดกันทางอาวุธภายในประเทศอันเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ (Not of an International Character) หรือที่เรียกว่า “การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ” (Non-international Armed Conflict) เพื่อให้ความคุ้มครองพลเรือนที่ไม่เกี่ยวข้องกับการสู้รบปรากฏตามข้อ 3 ร่วมของอนุสัญญาเจนีวา 1949 ความว่า ในกรณีการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศเกิดขึ้นภายในดินแดนของรัฐภาคี...”[200]

ลักษณะของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศปรากฏตามคำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (The International Criminal Tribunal for the Former Yugoslavia: ICTY) คดี Prosecutor v. Dusko Tadic อธิบายว่าเป็น “การขัดกันทางอาวุธมีอยู่เมื่อใดก็ตามที่มีการใช้ความรุนแรงทางอาวุธอย่างยืดเยื้อระหว่างองค์กรของรัฐบาลและกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรหรือระหว่างกลุ่มดังกล่าวภายในรัฐ”[201]

ความหมายเดียวกันนี้ได้รับการรับรองไว้ในข้อ 8 (2) (f) ของธรรมนูญกรุงโรมว่าด้วยศาลอาญาระหว่างประเทศ (The Rome Statute of the International Criminal Court)[202] ระบุว่า “(ข้อ 8 (2) (e)) บังคับใช้กับการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศและไม่นำไปบังคับ

---

[200] "The Geneva Conventions of 12 August 1949."

Common Article 3, para 1.

“In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:...”

[201] *The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* Para. 70.

“A non-international armed conflict exists “whenever there is ... protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.”

[202] Elizabeth Wilmshurst, *International Law and the Classification of Conflicts*(United Kingdom: Oxford University Press, 2012).

ใช้กับสถานการณ์ความยุ่งยากภายในและความตึงเครียด เช่น การจลาจล การแบ่งแยกดินแดน สถานการณ์ความรุนแรงที่มีลักษณะเป็นครั้งคราวหรือการกระทำอื่นที่มีลักษณะคล้ายกัน โดยบังคับใช้กับการขัดกันทางอาวุธที่เกิดขึ้นภายในดินแดนของรัฐที่เป็นการขัดกันทางอาวุธที่ยืดเยื้อระหว่างหน่วยงานของรัฐกับกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรหรือระหว่างกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร[203] และได้รับการรับรองจากศาลระหว่างประเทศต่างๆ ได้แก่ ศาลอาญาระหว่างประเทศ (the International Criminal Court : ICC)[204] ศาลอาญาระหว่างประเทศสำหรับรวันดา (the International Criminal Tribunal for Rwanda : ICTR)[205] และศาลพิเศษสำหรับสาธารณรัฐเซียร์ราลีโอน (the Special Court for Sierra Leone : SCSR)[206]

นอกจากนี้ คณะกรรมการกาชาดระหว่างประเทศ (International Committee of the Red Cross) เสนอคำนิยามของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศว่าเป็นการเผชิญหน้าทางอาวุธอย่างยืดเยื้อเกิดขึ้นระหว่างกองกำลังทหารของรัฐบาลและกลุ่มกองกำลังติดอาวุธหนึ่งกลุ่มหรือมากกว่าหนึ่งกลุ่ม หรือระหว่างกองกำลังติดอาวุธเกิดขึ้นในดินแดนของรัฐ (รัฐภาคีแห่งอนุสัญญาเจนีวา) การเผชิญหน้าทางอาวุธนั้นจะต้องเกินระดับความรุนแรงในขีดต่ำสุดและฝ่ายในการสู้รบที่เกี่ยวข้องในการขัดกันทางอาวุธจะต้องมีลักษณะเป็นองค์กร มีการจัดตั้งอย่างมีระบบ[207]

---

[203] "Rome Statute of the International Criminal Court," (opened for signature 17 July 1998, entered into force 1 July 2002).

Article. 8 (2) (f)

"Paragraph 2 (e) applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature. It applies to armed conflicts that take place in the territory of a State when there is protracted armed conflict between governmental authorities and organized armed groups or between such groups."

[204] *The Prosecutor V. Lubanga (Decision on Confirmation of Charges) Icc-01/04-01/06* 29 January 2007. Para 233; *The Prosecutor V. Bemba Gombo (Decision on Confirmation of Charges) Icc-01/05-01/08* 15 June 2006. Para 229.

[205] *The Prosecutor V. Jean-Paul Akayesu, Ictr-96-4-T, Trial Chamber I*, 2 September 1998., para 619; *The Prosecutor V. Rutaganda, Ictr-96-3-T, Judgment*, 6 December 1999., para 92.

[206] *Prosecutor V. Fofana (Decision on Appeal against Decision on Prosecutor's Motion for Judicial Notice and Admission of Evidence) Scsl-04-14-T-398, Separate Opinion of Judge Robertson*, 16 May 2005. para 32.

[207] ICRC, "How Is the Term "Armed Conflict" Defined in International Humanitarian Law? Icrc Opinion Paper, (March 2008),"(ICRC, 2008).

จากการศึกษาข้อ 3 ร่วมของอนุสัญญาเจนีวา 1949 และคำพิพากษาของศาลระหว่างประเทศต่างๆ ข้างต้น จะเห็นได้ว่า เงื่อนไขสำคัญของการมีอยู่ซึ่งการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะต้องประกอบไปด้วย (1) กลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร (An Organized Armed Group) และ (2) ระดับความรุนแรง (A Level of Intensity)[208] รายละเอียดเงื่อนไขของการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ มีดังต่อไปนี้

3.1.2.2.1 ฝ่ายในการสู้รบจะต้องเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร

จากการศึกษาการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศภายใต้ข้อ 3 ร่วมของอนุสัญญาเจนีวา 1949 เป็นการขัดกันทางอาวุธระหว่างรัฐกับกลุ่มที่ไม่ใช่รัฐ (Non-state Groups) หรือเป็นการขัดกันทางอาวุธระหว่างกลุ่มที่ไม่ใช่รัฐด้วยกันเอง กล่าวคือ การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะต้องมีกลุ่มที่ไม่ใช่รัฐ (Non-state Groups) อย่างน้อยฝ่ายหนึ่งเป็นฝ่ายในการสู้รบ (A Party to an Armed Conflict)[209]

กลุ่มที่ไม่ใช่รัฐ (A Non-State Group) ต้องเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร (An Organized Armed Group) จึงจะสามารถเป็นฝ่ายในการสู้รบภายในความหมายของกฎหมายมนุษยธรรมระหว่างประเทศได้ โดยจะต้องมีระดับของการจัดตั้งองค์กร (A Level of Organisation) ที่จะช่วยให้ดำเนินการสู้รบได้อย่างต่อเนื่องและปฏิบัติตามกฎหมายมนุษยธรรมระหว่างประเทศได้[210] ปัจจัยที่บ่งชี้การเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรตามคำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (ICTY) กล่าวไว้ในคำพิพากษาหลายคดี อาทิ

---

[208] Michael Schmitt, "Classification of Cyber Conflict," Journal of Conflict & Security Law 17, no. 2 (2012). P. 255.

[209] Elizabeth Wilmshurst, International Law and the Classification of Conflicts(United Kingdom: Oxford University Press, 2012). P. 51.

[210] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," International Review of Red Cross 94 (2012). P. 550.

คดี Prosecutor V. Ramash Haradinaj ระบุว่า ปัจจัยที่บ่งชี้การเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรนั้น ... “ต้องมีอยู่ซึ่งแบบแผนสายการบังคับบัญชาและกฎระเบียบวินัยและวิธีการทำงานภายในกลุ่ม มีกองบัญชาการ มีข้อเท็จจริงที่ว่ากลุ่มนั้นควบคุมดินแดนบางส่วนเป็นกลุ่มที่มีความสามารถในการเข้าถึงอาวุธ อุปกรณ์ทางทหารอื่นๆ มีการรับสมัครและมีการฝึกหัดทางทหาร มีความสามารถในการวางแผนประสานงานและดำเนินการปฏิบัติการทางทหาร รวมทั้งการเคลื่อนกำลังและส่งกำลังบำรุงทางทหาร มีความสามารถในการกำหนดยุทธศาสตร์รวมทางทหารและใช้ยุทธวิธีทางการทหาร และมีความสามารถในการพูดเป็นหนึ่งเสียงและเจรจาและสรุปข้อตกลง เช่น การหยุดยิงหรือสนธิสัญญาสันติภาพ”[211] โดยปัจจัยเหล่านี้เป็นปัจจัยที่ค่อนข้างเป็นตัวบ่งชี้ลักษณะของการจัดตั้งองค์กร แต่ไม่ได้เป็นปัจจัยขั้นต่ำที่จะต้องมีในการพิจารณาลักษณะการจัดตั้งเป็นองค์กร

นอกจากนี้ ในคดี Prosecutor v. Limaj ศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (ICTY) พิจารณาปัจจัยบางส่วนในการตัดสินว่ากองทัพปลดปล่อยโคโซโว (The Kosovo Liberation Army) มีคุณสมบัติเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรในการสู้รบกับสหพันธ์สาธารณรัฐยูโกสลาเวีย (The Federal Republic Of Yugoslavia) ได้แก่ การมีอยู่ของแบบแผนคำสั่งอย่างเป็นทางการ การสร้างพื้นที่กองกำลังในการปฏิบัติการ การออกคำสั่ง การจัดตั้งกองบัญชาการและการประกาศใช้คำสั่งทางวินัย[212]

จากการศึกษาข้อ 3 ร่วมของอนุสัญญาเจนีวา 1949 และคำพิพากษาของศาลระหว่างประเทศต่างๆ ข้างต้น สรุปได้ว่าการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะต้องประกอบด้วยกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรอย่างน้อยหนึ่งฝ่าย เมื่อพิจารณาเงื่อนไขของการบ่งชี้

---

[211] *The Prosecutor V. Ramush Haradinaj, Judgement (Trial Chamber), Case No. It*-04-84-*T*, 3 April 2008 3 April 2008. Para. 60.

“...the existence of a command structure and disciplinary rules and mechanisms within the group; the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits and military training; its ability to plan, coordinate and carry out military operations, including troop movements and logistics; its ability to define a unified military strategy and use military tactics; and its ability to speak with one voice and negotiate and conclude agreements such as cease-fire or peace accords.”

[212] *Prosecutor V. Fatmir Limaj, Haradin Bala and Isak Musliu, Judgement (Trial Chamber Ii), Case No. It-03-66-T*, 30 November 2005. Paras 94-129.

ว่าเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรข้างต้นกับเหตุการณ์การโจมตีทางไซเบอร์ที่กระทำโดยกลุ่มแฮคเกอร์ เป็นที่ชัดเจนว่าปัจเจกบุคคลที่กระทำการโจมตีทางไซเบอร์ต่อรัฐหรือกลุ่มติดอาวุธเพียงลำพังไม่เป็นไปตามเงื่อนไขลักษณะการเป็นองค์กร ยกตัวอย่าง การโจมตีทางไซเบอร์ต่อเอสโตเนีย แม้จะมีแฮคเกอร์จำนวนมากที่มีส่วนร่วมในปฏิบัติการไซเบอร์ต่อเอสโตเนีย แต่แฮคเกอร์เหล่านั้นขาดปัจจัยในการบ่งชี้การเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร ดังนั้น กลุ่มแฮคเกอร์ดังกล่าวจึงไม่ถือเป็นฝ่ายในการสู้รบของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ

นอกจากจะต้องมีลักษณะการจัดตั้งกลุ่มอย่างมีระบบเป็นองค์กร (Organisation) แล้วจะต้องเป็นกลุ่มที่มีการจัดตั้งเป็นองค์กรนั้นจะต้องเป็นกลุ่ม “ติดอาวุธ” (Armed) ด้วยซึ่งความหมายของ“ติดอาวุธ” (Armed) ในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศนั้นมีความหมายสอดคล้องกับการพิจารณาว่าการโจมตีทางไซเบอร์เทียบเท่ากับการใช้กำลังทางทหารซึ่งเป็นเงื่อนไขในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศที่ได้ศึกษามาแล้วข้างต้น เนื่องจากกลุ่มที่มีลักษณะเป็นองค์กรนั้นจะต้องเป็นการกระทำของกลุ่มติดอาวุธ หากสมาชิกของกลุ่มที่มีลักษณะเป็นองค์กรเลือกปฏิบัติการโจมตีทางไซเบอร์ด้วยตนเอง ไม่ได้ปฏิบัติการในนามกลุ่ม การกระทำของสมาชิกของกลุ่มดังกล่าวย่อมไม่มีลักษณะเป็นการกระทำของกลุ่มติดอาวุธซึ่งต่างจากกรณีการกระทำของรัฐที่แม้สมาชิกของหน่วยงานรัฐบาลปฏิบัติการโจมตีทางไซเบอร์ด้วยตนเอง อาจจะพิจารณาว่าเป็นการกระทำของรัฐได้[213]

3.1.2.2.2 ระดับความรุนแรง

การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศภายใต้ข้อ 3 ร่วมของอนุสัญญาเจนีวาจะต้องเป็นการต่อสู้ที่มีความรุนแรง (Intensity) ไม่ใช่เพียงเหตุการณ์ความไม่สงบภายในประเทศ (Internal Disturbances) ความตึงเครียดภายในประเทศ (Internal Tensions) เช่น การจลาจล การกระทำรุนแรงเป็นครั้งคราว หรือการกระทำอย่างอื่นที่มีลักษณะเช่นเดียวกัน โดยสถานการณ์ตามข้อ 1 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2[214] ถือเป็นลักษณะของความ

---

[213] Michael Schmitt, "Classification of Cyber Conflict," Journal of Conflict & Security Law 17, no. 2 (2012). P. 258.

[214] "Protocol Additional of the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol Ii)," (8 JUNE 1977).

Article 1 (2)

ขัดแย้งที่ไม่มีความรุนแรงพอที่จะถึงระดับความรุนแรงขั้นต่ำของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ การพิจารณาระดับความรุนแรงจึงต้องพิจารณาจากปัจจัยทั้งหมดของสถานการณ์ที่เกิดขึ้นเป็นรายกรณีไป โดยการสู้รบนั้นจะต้องเป็นการสู้รบอย่าง “ยืดเยื้อ” (Protracted) ด้วย

คำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (ICTY) ในคดี Tadic ได้ให้ความหมายของการขัดกันทางอาวุธที่มิใช่ในระดับระหว่างประเทศว่าเป็นสถานการณ์ที่มีความรุนแรงในการใช้อาวุธอย่างยืดเยื้อ (Protracted Armed Violence) ระหว่างหน่วยงานของรัฐกับกลุ่มติดอาวุธหรือระหว่างกลุ่มติดอาวุธเหล่านั้นภายในรัฐ[215] โดยความรุนแรงที่มีคุณสมบัติเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศนั้นจะต้องเป็นความรุนแรงอย่าง “ยืดเยื้อ” (Protracted) ถือเป็นกุญแจสำคัญในการพิจารณาระดับความรุนแรง (A Degree of Intensity) กล่าวคือ การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะต้องเป็นการเผชิญหน้าทางทหารที่มีลักษณะยืดเยื้อ (Protracted Armed Confrontations)[216]

สำหรับปัจจัยที่เกี่ยวข้องในการพิจารณาระดับความรุนแรง (Intensity) ศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวียได้กล่าวไว้ในคำพิพากษาคดี Prosecutor V. Ramush Haradinaj ประกอบด้วย จำนวน ระยะเวลา และความรุนแรงของการปะทะของบุคคล ประเภทของอาวุธและอุปกรณ์ทางทหารอื่นๆ ที่ใช้ จำนวนและขนาดของอาวุธ จำนวนคนและประเภทของกองกำลังที่เข้าร่วมในการต่อสู้ จำนวนของผู้ประสบภัย ขนาดของสิ่งของที่ถูกทำลาย และจำนวนพลเรือนที่หลบหนีจากเขตการต่อสู้ การมีส่วนร่วมของคณะมนตรีความมั่นคงแห่งสหประชาชาติ (The UN Security Council) ก็อาจสะท้อนให้เห็นถึงความรุนแรงของการสู้รบได้[217]

“This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts.”

[215] *The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* Para. 70.

“...protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.”

[216] ICRC, "How Is the Term "Armed Conflict" Defined in International Humanitarian Law? Icrc Opinion Paper, (March 2008),"(ICRC, 2008).

[217] *The Prosecutor V. Ramush Haradinaj, Judgement (Trial Chamber), Case No. It-04-84-T*. para 49.

นอกจากนี้ ยังมีการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศภายใต้ข้อ 1 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2[218] ซึ่งพัฒนาและเพิ่มเติมตามข้อ 3 ร่วมของอนุสัญญาเจนีวา 1949 เพื่อขยายขอบเขตการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศโดยลักษณะการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศภายใต้ข้อ 1 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2 นี้จะเกี่ยวข้องกับการบังคับใช้ข้อบทตามพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 2 เท่านั้น ไม่ได้ขยายออกไปเป็นลักษณะทั่วไปของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศแต่อย่างใด[219]

การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศภายใต้ข้อ 1 ของพิธีสารเพิ่มเติมฉบับที่ 2 นี้ จะต้องเป็นการขัดกันทางอาวุธที่เกิดขึ้นในดินแดนของรัฐภาคีแห่งพิธีสารเพิ่มเติมฉบับที่ 2 เท่านั้นและจำกัดเฉพาะการขัดกันทางอาวุธที่มีกองกำลังของรัฐเข้าร่วมเป็นฝ่ายในการสู้รบ ไม่รวมถึงการขัดกันทางอาวุธที่เกิดขึ้นระหว่างกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรและจะต้องมีการควบคุมดินแดนโดยกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรด้วย

ดังนั้น เพียงแต่มีการควบคุมกิจกรรมทางไซเบอร์ไม่เพียงพอที่จะเป็นการควบคุมดินแดนภายใต้ข้อ 1 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2[220] กล่าวคือ กลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรที่จะเป็นฝ่ายในการสู้รบในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศภายใต้บังคับข้อบทตามข้อ 1 ของพิธีสารเพิ่มเติมอนุสัญญาฉบับที่ 2 จะต้องเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรซึ่งเข้าควบคุมดินแดนและดำเนินการโจมตีทางไซเบอร์ด้วย

---

[218] "Protocol Additional of the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol Ii)."

Article 1 (1)

"... which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol."

[219] ICRC Opinion paper, "How Is the Term "Armed Conflict" Defined in International Humanitarian Law? ."

[220] *Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts* Commentary on Rule 23, para 17.

ในส่วนของคู่มือทาลลินน์ (Tallinn Manual) ให้ลักษณะของการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศไว้ในกฎข้อ 23 ของคู่มือทาลลินน์ (Tallinn Manual) ความว่า การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศมีอยู่เมื่อใดก็ตามที่มีความรุนแรงในการใช้อาวุธอย่างยืดเยื้อเกิดขึ้นระหว่างกองกำลังทหารของรัฐบาลและกลุ่มกองกำลังติดอาวุธหนึ่งกลุ่มหรือมากกว่าหนึ่งกลุ่ม หรือระหว่างกองกำลังติดอาวุธ ซึ่งอาจรวมถึงหรือถูกจำกัดโดยปฏิบัติการทางไซเบอร์ การเผชิญหน้านั้นจะต้องเกินระดับความรุนแรงในขีดต่ำสุดและฝ่ายที่เกี่ยวข้องในการสู้รบจะต้องมีลักษณะเป็นองค์กร[221] โดยกฎข้อนี้เน้นย้ำกฎหมายจารีตประเพณีระหว่างประเทศของการขัดกันทางอาวุธในเรื่องการมีอยู่ของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศซึ่งมีที่มาจากข้อ 3 ร่วมของอนุสัญญาเจนีวา 1949

เมื่อพิจารณาปัจจัยในการบ่งชี้ระดับความรุนแรงของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศกับลักษณะการโจมตีทางไซเบอร์ ปัจจัยในการบ่งชี้ระดับความรุนแรงที่เกิดจากการโจมตีทางไซเบอร์ที่เป็นรูปธรรมมากที่สุดคือการก่อให้เกิดผลกระทบที่มีลักษณะรุนแรงเช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ อาทิ การโจมตีต่อระบบควบคุมการระบายน้ำของเขื่อนทำให้ประตูระบายน้ำเปิดออก การโจมตีต่อระบบควบคุมการจราจรทางอากาศเป็นเหตุให้อากาศยานตกหรือชนกันกลางอากาศ โดยการโจมตีทางไซเบอร์นั้นจะต้องไม่เป็นเพียงการกระทำเป็นครั้งคราวไปอาจพิจารณาได้ว่าเป็นการโจมตีทางไซเบอร์ที่มีระดับความรุนแรงอันเป็นเงื่อนไขของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศได้

จากการศึกษาเงื่อนไขของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศข้างต้น สรุปได้ว่า การโจมตีทางไซเบอร์ที่ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศหรือการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่ไม่ลักษณะระหว่างประเทศซึ่งสามารถนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้ได้จะต้องเป็นการโจมตีทางไซเบอร์ที่ปฏิบัติการโดย

---

[221] ibid.

Rule 23 – Characterisation as Non-International Armed Conflict

"A non-international armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organisation."

กลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร เป็นสถานการณ์ที่มีความรุนแรงอย่างยืดเยื้อที่ไม่ใช่เพียงสถานการณ์ความยุ่งยากภายในหรือความตึงเครียดภายในประเทศ เช่น การจลาจล การกระทำรุนแรงเป็นครั้งคราวหรือการกระทำอย่างอื่นที่มีลักษณะเช่นเดียวกัน นอกจากนี้ จะต้องเป็นการโจมตีทางไซเบอร์ที่เกิดขึ้นในดินแดนของรัฐภาคีระหว่างหน่วยงานรัฐบาลกับกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรหรือระหว่างกลุ่มติดอาวุธ โดยพิจารณาข้อเท็จจริงของแต่ละสถานการณ์เป็นรายกรณีไป

ยกตัวอย่าง หากกลุ่มที่ไม่ใช่รัฐที่มีแบบแผนสายการบังคับบัญชา มีกองบัญชาการที่บ่งชี้ได้ว่ามีลักษณะเป็นองค์กร A ดำเนินการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ AA ซึ่งเป็นรัฐภาคีอนุสัญญาเจนีวา 1949 โดยการโจมตีทางไซเบอร์ต่อระบบควบคุมการผลิตกระแสไฟฟ้า น้ำ พลังงาน การจราจร เป็นเหตุให้เกิดการบาดเจ็บหรือเสียชีวิตของประชาชนและทำให้เกิดความเสียหายหรือทำลายซึ่งทรัพย์สินภายในรัฐ AA ซึ่งมีระดับความรุนแรงของสถานการณ์การโจมตีทางไซเบอร์มากกว่าสถานการณ์ความยุ่งยากภายในหรือความตึงเครียดภายในประเทศ อาจพิจารณาว่าการโจมตีทางไซเบอร์ดังกล่าวเป็นจุดเริ่มต้นของสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศได้

จากการศึกษาการนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธมาทั้งหมดนี้ กล่าวสรุปได้ว่า การโจมตีทางไซเบอร์ที่ดำเนินการในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศ โดยการโจมตีทางไซเบอร์ที่เกิดขึ้นในระหว่างสถานการณ์การขัดกันทางอาวุธย่อมสามารถนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้ได้เช่นเดียวกับการโจมตีด้วยอาวุธตามแบบอย่างไม่มีข้อโต้แย้ง ดังนั้น ฝ่ายในการสู้รบจึงมีหน้าที่ตามกฎหมายมนุษยธรรมระหว่างประเทศที่จะต้องดำเนินการโจมตีทางไซเบอร์ให้สอดคล้องกับกลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ ทั้งในส่วนที่เป็นหลักการเกี่ยวกับปฏิบัติการทางทหารและการให้ความคุ้มครองแก่พลเรือนและทรัพย์สินของพลเรือน

อย่างไรก็ตาม กรณีการโจมตีทางไซเบอร์ที่เกิดขึ้นในขณะที่ยังไม่มีสถานการณ์การขัดกันทางอาวุธและไม่มีการใช้กำลังทางทหารด้วยการโจมตีด้วยอาวุธตามแบบร่วมด้วยนั้นจำเป็นจะต้องพิจารณาเงื่อนไขของการเกิดสถานการณ์การขัดกันทางอาวุธแต่ละประเภทเป็นรายกรณี กล่าวคือ การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะต้องเป็นการโจมตีทางไซเบอร์เทียบเท่ากับการใช้กำลังทางทหารของรัฐหนึ่งกระทำต่ออีกรัฐหนึ่งหรือมากกว่าหนึ่งรัฐขึ้นไป ส่วนการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะต้องเป็นการโจมตีทางไซเบอร์เทียบเท่ากับการเผชิญหน้าทางอาวุธที่ปฏิบัติการโดยกลุ่มติดอาวุธที่มี

ลักษณะเป็นองค์กรซึ่งเกิดขึ้นในดินแดนของรัฐภาคีระหว่างหน่วยงานรัฐบาลกับกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรหรือระหว่างกลุ่มติดอาวุธและเป็นสถานการณ์ที่มีความรุนแรงอย่างยืดเยื้อ ไม่ใช่เพียงสถานการณ์ความยุ่งยากภายในหรือความตึงเครียดภายในประเทศ

ทั้งนี้ การพิจารณาว่าการโจมตีทางไซเบอร์เพียงลำพัง ปราศจากการโจมตีด้วยอาวุธอื่นจะก่อให้เกิดสถานการณ์การขัดกันทางอาวุธอันเป็นเงื่อนไขในการนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้ได้หรือไม่นั้น ในขณะนี้ ยังไม่ได้บทสรุปที่ชัดเจนแต่อย่างใด จำเป็นต้องอาศัยแนวทางปฏิบัติของรัฐ (State Practice) เกี่ยวกับเรื่องนี้ในอนาคตต่อไป

ในหัวข้อถัดไปจะทำการศึกษาและวิเคราะห์หลักการเกี่ยวกับปฏิบัติการทางทหารตามกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยจะแบ่งการศึกษาเนื้อหาออกเป็น 3 ส่วน ได้แก่ หลักการการเข้าร่วมในสถานการณ์การขัดกันทางอาวุธ หลักการเกี่ยวกับการปฏิบัติต่อเป้าหมาย และหลักการทั่วไปเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบ ดังมีรายละเอียดต่อไปนี้

3.2 หลักการเกี่ยวกับปฏิบัติการทางทหาร

กฎหมายมนุษยธรรมระหว่างประเทศได้กำหนดหลักการเกี่ยวกับปฏิบัติการทางทหารที่เป็นหลักการทั่วไปบังคับใช้กับทุกสถานการณ์การขัดกันทางอาวุธ โดยในการศึกษาวิจัยเล่มนี้จะได้แบ่งการศึกษาออกเป็นหลักการเกี่ยวกับการเข้าร่วมในสถานการณ์การขัดกันทางอาวุธ หลักการเกี่ยวกับการปฏิบัติต่อเป้าหมายทางทหาร และหลักการเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบดังต่อไปนี้

3.2.1 หลักการเกี่ยวกับการเข้าร่วมในสถานการณ์การขัดกันทางอาวุธ

กฎหมายมนุษยธรรมระหว่างประเทศแบ่งแยกสถานะของบุคคลในสภาวะสงครามออกเป็นสองประเภทใหญ่ๆ ได้แก่ พลรบและพลเรือน[222] ซึ่งมีหน้าที่และความคุ้มครองแตกต่างกัน โดยพลรบ

[222] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 57.

มีสิทธิเข้าร่วมในการสู้รบและอาจตกเป็นเป้าหมายในการโจมตีได้ ในขณะที่พลเรือนได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศและไม่อาจตกเป็นเป้าหมายในการโจมตีได้ เช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจะต้องมีบุคคลเข้ามาเกี่ยวข้องไม่มากก็น้อย โดยเนื้อหาส่วนนี้จะได้ทำการศึกษาหลักการเกี่ยวกับการเข้าร่วมในสถานการณ์การขัดกันทางอาวุธที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ดังต่อไปนี้

3.2.1.1 สถานะของพลรบ

คำว่า “พลรบ” (Combatants) ปรากฏคำนิยามตามกฎหมายจารีตประเพณีระหว่างประเทศและกฎหมายสนธิสัญญา โดยในการศึกษากฎหมายจารีตประเพณีของกฎหมายมนุษยธรรมระหว่างประเทศ[223] และข้อ 43 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ได้ให้ความหมายของพลรบไว้ว่า “พลรบ คือ สมาชิกของกองกำลังทางทหารของฝ่ายในการสู้รบ (ยกเว้นบุคลากรทางการแพทย์และอนุศาสตราจารย์ตามข้อ 33 อนุสัญญาเจนีวา ค.ศ. 1949 ฉบับที่ 3) โดยพลรบมีสิทธิเข้าร่วมโดยตรงในการสู้รบ”[224]

ข้อ 43 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ยังได้ให้ลักษณะของคำว่ากองกำลังทางทหาร (Armed Forces) คือ“กองกำลังทางทหารของฝ่ายในการสู้รบประกอบด้วยกอง

---

[223] Jean-Marie Henckaerts and Louise Doswald-Beck, *Study on Customary International Humanitarian Law - Volume I: Rule*(Cambridge University Press, 2005).

Rule 3.

“All members of the armed forces of a party to the conflict are combatants, except medical and religious personnel.”

[224] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 43 (2)

“Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities.”

กำลังติดอาวุธที่มีลักษณะเป็นองค์กร กลุ่ม หน่วยรบซึ่งอยู่ภายใต้ความรับผิดชอบในการบังคับบัญชาของฝ่ายในการสู้รบสำหรับการปฏิบัติการของผู้ที่อยู่ใต้บังคับบัญชา แม้ว่าฝ่ายในการสู้รบนั้นจะมีรัฐบาลหรือเจ้าหน้าที่ที่ไม่ได้รับรองจากฝ่ายตรงข้ามในการสู้รบเป็นตัวแทน กองกำลังทางทหารดังกล่าวจะต้องอยู่ภายใต้ระบบวินัยภายใน รวมถึงจะต้องบังคับให้ปฏิบัติตามหลักการของกฎหมายระหว่างประเทศที่ใช้บังคับในการขัดกันทางอาวุธ[225]

จากการศึกษาข้อ 43 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 พอสรุปได้ว่า “พลรบ คือสมาชิกทั้งหมดของกองกำลังทางทหารของฝ่ายคู่พิพาทในการสู้รบ ไม่ว่าจะเป็นกองทหารประจำหรือกองทหารแบบไม่ประจำ รวมทั้งหน่วยกึ่งทหารหรือองค์กรที่มีหน้าที่ในการบังคับใช้กฎหมายซึ่งรวมอยู่ในกองกำลังทางทหาร ยกเว้นเพียงบุคคลกรทางการแพทย์และบุคลากรทางศาสนา”[226]

เมื่อพิจารณาตามข้อ 43 แห่งพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1 ซึ่งบังคับใช้กับสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจะเห็นได้ว่าพลรบได้รับสิทธิที่จะเข้าร่วมโดยตรงในการสู้รบ โดยที่ข้อบทดังกล่าวไม่ได้กำหนดห้ามบุคคลที่ไม่ใช่พลรบเข้าร่วมในการสู้รบแต่อย่างใด คำว่า “พลรบ” จึงสามารถใช้ในการอธิบายลักษณะของบุคคลที่มีสิทธิเข้าร่วมโดยตรงในการสู้รบ (Right to Participate Directly on Hostilities) และหมายถึงบุคคลใดก็ตามที่

---

[225] ibid.

Article 43 (1)

“The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, inter alia, shall enforce compliance with the rules of international law applicable in armed conflict.”

[226] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, ed. Second(United Kingdom: Cambridge University Press, 2010). P. 33, Para. 79.

เข้าร่วมอย่างแท้จริงในการสู้รบในสถานการณ์การขัดกันทางอาวุธในนามของฝ่ายในการสู้รบ ไม่ว่าบุคคลนั้นจะได้รับอนุญาตให้เข้าร่วมในการสู้รบหรือไม่ก็ตาม[227]

จากการศึกษาข้างต้น จะเห็นได้ว่า สถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศสามารถแบ่งพลรบออกเป็น 2 ประเภทใหญ่ๆ ได้แก่ (1) บุคคลที่เป็นสมาชิกของกองกำลังทางทหารของฝ่ายในการสู้รบ โดยไม่ต้องคำนึงถึงลักษณะงานที่ได้รับมอบหมายจะเกี่ยวข้องกับการสู้รบหรือไม่ก็ตาม (ยกเว้นบุคลากรทางการแพทย์และบุคลากรทางศาสนา) ถือเป็นพลรบที่ชอบด้วยกฎหมาย (Lawful Combatants) และ (2) บุคคลซึ่งไม่ได้เป็นสมาชิกของกองกำลังทางทหารที่เข้ามีส่วนร่วมโดยตรงในการสู้รบถือเป็นพลรบที่ไม่ชอบด้วยกฎหมาย (Unlawful Combatants) ซึ่งพลรบที่ชอบด้วยกฎหมายและพลรบที่ไม่ชอบด้วยกฎหมายจะตกอยู่ภายใต้ระบอบกฎหมายที่แตกต่างกัน[228] รวมทั้งมีสิทธิและได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศที่แตกต่างกัน

สิทธิในการเป็นพลรบที่ชอบด้วยกฎหมาย (Lawful Combatants) ได้แก่ สิทธิที่จะเข้าร่วมโดยตรงในการสู้รบ[229] สิทธิในการได้รับสถานภาพเชลยศึก (Prisoner of War) เมื่อตกอยู่ภายใต้อำนาจของฝ่ายศัตรูในการสู้รบหรือถูกจับกุมโดยฝ่ายที่เป็นปฏิปักษ์ในการสู้รบ[230] โดยสิทธิเข้า

---

[227] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012). P. 141.

[228] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 67.

[229] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 43 (2)

"Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities."

[230] "Geneva Convention (Iii) Relative to the Treatment of Prisoners of War of 12 August 1949."

Article 4 (A)

"Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:..."

ร่วมโดยตรงในการสู้รบของพลรบเป็นหลักการตามกฎหมายจารีตประเพณีระหว่างประเทศที่ยอมรับไว้ในข้อ 43 (2) แห่งพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 โดยการได้รับสถานะของพลรบยังทำให้พลรบสามารถตกเป็นเป้าหมายในการโจมตีได้โดยชอบกฎหมายมนุษยธรรมระหว่างประเทศ

ในทางตรงกันข้ามกับพลรบที่ไม่ชอบด้วยกฎหมาย (Unlawful Combatants) หรือพลรบที่ไม่ได้รับสิทธิพิเศษ (Unprivileged Combatants) จะไม่มีสิทธิได้รับสถานภาพเชลยศึก (Prisoner of War) เมื่อถูกจับกุมและยังอาจตกเป็นเป้าหมายในการโจมตีได้เช่นเดียวกับพลรบ นอกจากนี้ พลรบที่ไม่ชอบด้วยกฎหมายยังไม่ได้รับการคุ้มครองในฐานะพลเรือนอีกด้วย

ด้วยเหตุดังกล่าวข้างต้น สถานะของพลรบจึงมีความสำคัญอย่างมากสำหรับพลรบที่ชอบด้วยกฎหมายซึ่งมีสิทธิเข้าร่วมโดยตรงในการสู้รบ โดยการเข้าร่วมการสู้รบย่อมหมายถึงการทำการต่อสู้ ประหัตประหาร ทำร้ายร่างกายของพลรบฝ่ายศัตรู รวมทั้งการโจมตีทรัพย์สินอันเป็นเป้าหมายทางการทหารอีกด้วย[231] อย่างไรก็ตาม พลรบอาจจะตกเป็นเป้าหมายในการโจมตีได้โดยชอบด้วยกฎหมาย เนื่องจากสถานะของการเป็นพลรบ ไม่ได้อาศัยปฏิบัติการหรือกิจกรรมที่ทำ[232]

จากการศึกษาข้างต้น เมื่อพิจารณาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเกี่ยวกับการให้สถานะพลรบแก่บุคคลผู้ทำการโจมตีทางไซเบอร์จะต้องพิจารณาเงื่อนไขเช่นเดียวกับการให้สถานะของพลรบผู้ทำการโจมตีด้วยอาวุธตามแบบ โดยบุคคลผู้โจมตีทางไซเบอร์ที่ได้รับสถานะพลรบที่ชอบด้วยกฎหมายย่อมอาจตกเป็นเป้าหมายในการโจมตีได้ตลอดระยะเวลาในระหว่างสถานการณ์การขัดกันทางอาวุธและคงอยู่จนกว่าสถานการณ์การขัดกันทางอาวุธจะสิ้นสุดลง พลรบที่ชอบด้วยกฎหมายมีสิทธิที่จะเข้าร่วมโดยตรงในการสู้รบ สิทธิในการได้รับสถานภาพเชลยศึก (Prisoner of War) เมื่อตกอยู่ภายใต้อำนาจของฝ่ายศัตรูในการสู้รบหรือถูกจับกุมโดยฝ่ายที่เป็นปฏิปักษ์ในการสู้รบ[233] ในขณะที่ บุคคลที่ไม่ได้รับ

---

[231] ณัฐวัฒน์ กฤตยานวัช, "สถานภาพของกลุ่มพลรบตาลิบันที่ถูกควบคุมตัวโดยสหรัฐอเมริกาในกฎหมายมนุษยธรรมระหว่างประเทศ" (จุฬาลงกรณ์มหาวิทยาลัย, 2549). หน้า 43

[232] Sean Watts, "Combatant Status and Computer Network Attack," *Virginia Journal of International Law* 50, no. 2 (2010). P. 420.

[233] Vijay M. Padmanabham, "Cyber Worriors and the Jus in Bello," *International Law Studies* 89(2013). P. 292.

สถานะพลรบที่ชอบด้วยกฎหมาย หากเข้าร่วมในการโจมตีทางไซเบอร์ แม้จะกระทำในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธจะไม่มีสิทธิได้รับสถานภาพเชลยศึก (Prisoner of War) เมื่อถูกจับกุม และยังอาจตกเป็นเป้าหมายในการโจมตีได้เช่นเดียวกับพลรบและยังไม่ได้รับการคุ้มครองจากการถูกโจมตีโดยตรงในฐานะพลเรือนอีกด้วย

เมื่อพิจารณาเงื่อนไขตามข้อ 43 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 บุคคลผู้ทำการโจมตีทางไซเบอร์จะได้รับสถานะพลรบต่อเมื่อบุคคลนั้นเป็นสมาชิกของกองกำลังทางทหารของรัฐซึ่งเป็นฝ่ายในการสู้รบในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ ดังนั้น บุคคลผู้ทำการโจมตีทางไซเบอร์ที่ไม่ใช่สมาชิกของกองทัพย่อมไม่อาจได้รับสถานะพลรบตามข้อ 43 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 นี้ได้

จากลักษณะพิเศษของการโจมตีทางไซเบอร์ที่มีความซับซ้อนและจะต้องอาศัยความรู้ความเชี่ยวชาญ ทักษะเฉพาะด้านเทคโนโลยีไซเบอร์ในการดำเนินการส่งผลให้รัฐอาจว่าจ้างบริษัทเอกชนหรือผู้รับจ้าง (Contractors) ที่มีความรู้ความเชี่ยวชาญให้ทำหน้าที่เกี่ยวกับการโจมตีทางไซเบอร์ ไม่ว่าจะเป็นหน้าที่ในการรักษาความปลอดภัยทางไซเบอร์ ป้องกันเป้าหมายจากการโจมตีทางไซเบอร์ หน้าที่ในการใช้อาวุธไซเบอร์โจมตีเป้าหมายทางทหาร เมื่อพิจารณาลักษณะของกองกำลังทางทหาร (Armed Forces) ตามข้อ 43 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1 ซึ่งได้อธิบายไว้ข้างต้นแล้ว จะเห็นได้ว่า ลูกจ้างของบริษัทเอกชนที่กองทัพว่าจ้างให้เข้ามาทำหน้าที่ในการรักษาความปลอดภัยทางไซเบอร์หรือการโจมตีทางไซเบอร์ไม่อาจได้รับสถานะพลรบตามข้อ 43 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1 เนื่องจากบริษัทเอกชนไม่มีลักษณะเป็นกองกำลังทางทหารตามข้อบทดังกล่าว แม้ลูกจ้างของบริษัทเอกชนที่กองทัพว่าจ้างจะทำการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธตามที่ได้รับการว่าจ้างจากกองทัพ ลูกจ้างของบริษัทเอกชนเหล่านั้นก็ไม่ได้รับสถานะพลรบตามกฎหมายมนุษยธรรมระหว่างประเทศที่จะก่อให้เกิดสิทธิในการเข้าร่วมโดยตรงในการสู้รบตามข้อ 43 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 แต่อย่างใด

อย่างไรก็ตาม สถานะของลูกจ้างที่ทำการโจมตีทางไซเบอร์ยังคงถือเป็นพลเรือนตามข้อ 50 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[234] ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศ

---

[234] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 50 - Definition of civilians and civilian population

การที่ลูกจ้างเหล่านั้นเข้าทำการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นเหตุให้สูญเสียความคุ้มครองในฐานะพลเรือน ณ ขณะที่เข้าร่วมทำการโจมตีทางไซเบอร์เท่านั้น ซึ่งจะได้อธิบายรายละเอียดในส่วนถัดไป

นอกจากนี้ กฎหมายมนุษยธรรมระหว่างประเทศรับรองเงื่อนไขของพลรบที่ชอบด้วยกฎหมายที่ได้รับสถานภาพเชลยศึกเมื่อถูกจับกุมภายใต้ข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3[235] สรุปได้ว่า สมาชิกของกลุ่มมิลิเชีย (Militia) และสมาชิกของหน่วยอาสาสมัครอื่น รวมทั้งสมาชิกของกลุ่มเคลื่อนไหวต่อต้านที่จัดตั้งขึ้นของฝ่ายในการสู้รบและปฏิบัติการทั้งในและนอกดินแดนของตนจะต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้ จึงจะได้รับสถานะพลรบโดยชอบด้วยกฎหมาย

(ก) อยู่ภายใต้บังคับบัญชาของบุคคลผู้รับผิดชอบผู้ใต้บังคับบัญชา
(ข) มีเครื่องหมายที่กำหนดไว้อย่างเด่นชัด สามารถมองเห็นได้จากระยะไกล
(ค) ถืออาวุธอย่างเปิดเผย
(ง) ดำเนินปฏิบัติการอย่างสอดคล้องกับกฎและจารีตประเพณีของสงคราม

เมื่อพิจารณาตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 ประกอบกับข้อ 43 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 สรุปได้ว่า สมาชิกของกองกำลังทหาร มิลิเชีย หน่วย

"A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) [Link] of the Third Convention and in Article 43 [Link] of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian."

[235] "Geneva Convention (Iii) Relative to the Treatment of Prisoners of War of 12 August 1949."
Article 4 (A) (2)
"Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfil the following conditions:
(a) that of being commanded by a person responsible for his subordinates;
(b) that of having a fixed distinctive sign recognizable at a distance;
(c) that of carrying arms openly;
(d) that of conducting their operations in accordance with the laws and customs of war."

อาสาสมัครอื่นและกลุ่มเคลื่อนไหวต่อต้านจะต้องปฏิบัติตามเงื่อนไข (ก) – (ข) ข้างต้นจึงจะได้รับสถานภาพเชลยศึกหรือเป็นพลรบที่ชอบด้วยกฎหมาย

ในทางทฤษฎี หากพิจารณาตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 กับลักษณะของผู้ดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหมายความว่า บุคคลที่จะได้รับสถานะพลรบซึ่งจะมีสิทธิในการใช้เทคโนโลยีไซเบอร์ในการโจมตีทางไซเบอร์ต่อเป้าหมายได้โดยชอบด้วยกฎหมายในสภาวะสงครามจะต้องเป็นสมาชิกของกองกำลังทหาร มิลิเซีย หน่วยอาสาสมัครอื่นหรือกลุ่มเคลื่อนไหวต่อต้านจะต้องอยู่ภายใต้บังคับบัญชาของบุคคลผู้รับผิดชอบผู้ใต้บังคับบัญชา มีเครื่องหมายที่กำหนดไว้อย่างเด่นชัด สามารถมองเห็นได้จากระยะไกล ถืออาวุธอย่างเปิดเผยและดำเนินปฏิบัติการอย่างสอดคล้องกับกฎและจารีตประเพณีของสงคราม จึงจะได้รับสถานะพลรบโดยชอบด้วยกฎหมายตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3

เมื่อพิจารณาเหตุการณ์การขัดกันทางอาวุธระหว่างประเทศรัสเซียและจอร์เจียในปีค.ศ. 2008 มีการใช้กำลังทางทหารร่วมกับการโจมตีทางไซเบอร์อย่างกว้างขวางซึ่งส่วนหนึ่งของการโจมตีทางไซเบอร์มาจากกลุ่มแฮคเกอร์ออนไลน์เข้าร่วมในการโจมตีทางไซเบอร์ต่อจอร์เจียตามคำแนะนำของเว็บไซต์ที่ให้บริการบันทึกข้อมูลส่วนตัว (Blogs) หรือเว็บไซต์ของรัสเซียเกี่ยวกับการจัดเตรียมคอมพิวเตอร์ให้ทำงานอย่างอัตโนมัติในการดำเนินการโจมตีด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอสหรือเสนอให้ดาว์นโหลดโปรแกรมดีดีโอเอส[236] โดยรัสเซียปฏิเสธความเกี่ยวข้องกับการโจมตีทางไซเบอร์ทั้งหมด[237] กรณีนี้ย่อมไม่อาจพิจารณาได้ว่ากลุ่มแฮคเกอร์ที่เข้าร่วมในการโจมตีทางไซเบอร์ได้รับสถานะพลรบตามกฎหมายมนุษยธรรมระหว่างประเทศเนื่องจากไม่มีข้อบ่งชี้ว่ากลุ่มแฮคเกอร์ดังกล่าวนั้นอยู่ภายใต้บังคับบัญชาของรัฐอันเป็นเงื่อนไขหนึ่งในการได้รับสถานะพลรบที่ชอบด้วยกฎหมายตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3

---

[236] Evgeny Morozov, "An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar.," The Slate Group (August 14, 2008), http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html. [April 14, 2016]

[237] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012). P. 150.

อย่างไรก็ตาม ลักษณะการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอาจจะไม่เอื้ออำนวยกับการพิจารณาเงื่อนไขตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 ทำให้เกิดข้อท้าทายในการให้สถานะพลรบที่ชอบด้วยกฎหมายกับบุคคลผู้ทำการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธส่งผลต่อการได้รับสิทธิในการเป็นพลรบตามกฎหมายมนุษยธรรมระหว่างประเทศ ซึ่งจะทำการศึกษาในบทถัดไป

จากการศึกษาส่วนนี้ทั้งหมด สรุปได้ว่า บุคคลในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศที่จะได้รับสถานะพลรบซึ่งก่อให้เกิดสิทธิตามกฎหมายมนุษยธรรมระหว่างประเทศ ตลอดจนมีหน้าที่ต้องปฏิบัติตามหลักการเกี่ยวกับปฏิบัติการทางทหารตามกฎหมายมนุษยธรรมระหว่างประเทศจะต้องเป็นสมาชิกของกองกำลังทางทหารของฝ่ายในการสู้รบจึงจะได้รับสถานะพลรบและมีสิทธิในการใช้เทคโนโลยีไซเบอร์ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้โดยชอบด้วยกฎหมายตามข้อ 43 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1

นอกเหนือจากพลรบแล้ว พลเรือนเป็นบุคคลอีกสถานะหนึ่งในสภาวะสงครามที่อาจเกี่ยวข้องกับการเข้าร่วมในการโจมตีทางไซเบอร์สถานการณ์การขัดกันทางอาวุธส่งผลให้พลเรือนสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศได้ โดยจะศึกษาวิเคราะห์รายละเอียดในส่วนถัดไป

3.2.1.2 การเข้าร่วมโดยตรงในการสู้รบของพลเรือน

พลเรือนถือเป็นบุคคลสำคัญที่ได้รับการคุ้มครองในสถานการณ์การขัดกันทางอาวุธตามกฎหมายมนุษยธรรมระหว่างประเทศ

กฎหมายมนุษยธรรมระหว่างประเทศกำหนดให้ความคุ้มครองแก่พลเรือนตามข้อ 51 (3) แห่งพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ระบุว่า พลเรือนจักได้รับความคุ้มครองตามที่ได้บัญญัติไว้ในหมวดนี้ เว้นแต่ว่าและตราบเท่าช่วงเวลาที่พลเรือนนั้นเข้ามีส่วนร่วมโดยตรงในการสู้รบ[238]

---

[238] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 51 (3)

กล่าวคือ พลเรือนได้รับความคุ้มครอง โดยไม่อาจตกเป็นเป้าหมายในการโจมตีตลอดเวลาในการสู้รบ จนกว่าพลเรือนจะเข้ามีส่วนร่วมโดยตรงในการสู้รบ ทั้งนี้ การที่พลเรือนเข้ามีส่วนร่วมโดยตรงในการสู้รบทำให้พลเรือนสูญเสียการคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศตราบเท่าช่วงเวลา (For Such Time) ที่พลเรือนเข้ามีส่วนร่วมโดยตรงในการสู้รบเท่านั้น

จากการที่กฎหมายมนุษยธรรมระหว่างประเทศมุ่งให้ความคุ้มครองทางกฎหมายแก่พลเรือนและผู้ที่ไม่มีส่วนเกี่ยวข้องกับการสู้รบอีกต่อไป โดยพลเรือนจะได้รับการคุ้มครองจากการตกเป็นเป้าหมายในการโจมตี การเข้าร่วมโดยตรงในการสู้รบจึงเป็นข้อยกเว้นความคุ้มครองทางกฎหมายของพลเรือน

จากการศึกษาคำอธิบายพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ของคณะกรรมการกาชาดระหว่างประเทศที่มีต่อข้อ 51 (3) แห่งพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[239] ระบุว่า ความคุ้มครองที่ให้แก่ปัจเจกพลเรือนอยู่ภายใต้เงื่อนไขสำคัญคือการละเว้นจากการกระทำที่เป็นปรปักษ์ทั้งหมด (Hostile Acts) การกระทำที่เป็นปรปักษ์ควรเข้าใจว่าเป็นการกระทำที่โดยธรรมชาติและวัตถุประสงค์การกระทำตั้งใจที่จะก่อให้เกิดอันตราย (Harm) ที่แท้จริงต่อบุคคลและอุปกรณ์ของกองกำลังติดอาวุธ ดังนั้น พลเรือนที่เข้ามีส่วนร่วมในการต่อสู้ติดอาวุธทั้งรายบุคคลหรือเป็นส่วนหนึ่งของกลุ่มจึงกลายเป็นเป้าหมายโดยชอบด้วยกฎหมาย อย่างไรก็ตาม การตกเป็นเป้าหมายที่ชอบด้วยกฎหมายนั้นมีอยู่ตราบเท่าที่มีส่วนร่วมในการสู้รบเท่านั้น

แม้ว่าจะมีความเห็นของคณะกรรมการกาชาดระหว่างประเทศตามคำอธิบายความหมายของการเข้ามีส่วนร่วมโดยตรงในการสู้รบ (Direct Part in Hostilities) แต่ยังคงมีประเด็น

"Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities."

[239] Jean DE PREUX Claude PILLOUDt, Yves SANDOZ, Bruno ZIMMERMANN, Philippe Eberlin, Hans-Peter Gasser and Claude F. Wenger "Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949," ed. ICRC(Netherlands Martinus Nijhoff Publishers 1987). P. 618. Para. 1942.

"The immunity afforded individual civilians is subject to an overriding condition, namely, on their abstaining from all hostile acts. Hostile acts should be understood to be acts which by their nature and purpose are intended to cause actual harm to the personnel and equipment of the armed forces. Thus a civilian who takes part in armed combat, either individually or as part of a group, thereby becomes a legitimate target, though only for as long as he takes part in hostilities."

ข้อถกเถียงเกี่ยวกับการเข้ามีส่วนร่วมโดยตรงในการสู้รบของพลเรือนอยู่ อาทิ การกำหนดขอบเขตของการมีส่วนร่วมโดยตรง หรือขอบเขตของคำว่า “เว้นแต่ว่าและตราบเท่าช่วงเวลา (Unless and For Such Time)”

จากประเด็นความกำกวมเกี่ยวกับความหมายของการเข้ามีส่วนร่วมโดยตรงในการสู้รบของพลเรือนทำให้คณะกรรมการกาชาดระหว่างประเทศดำเนินการศึกษาเกี่ยวกับกรอบความคิดของการมีส่วนร่วมโดยตรงในการสู้รบเผยแพร่ขึ้นในปีค.ศ. 2009 ตามคำแนะนำเกี่ยวกับการตีความว่าด้วยการเข้ามีส่วนร่วมโดยตรงในการสู้รบ[240] (The Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law)

สำหรับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเกิดขึ้นในระหว่างที่มีการจัดทำคำแนะนำเกี่ยวกับการตีความว่าด้วยการเข้ามีส่วนร่วมโดยตรงในการสู้รบของคณะกรรมการกาชาดระหว่างประเทศ โดยคณะกรรมการกาชาดระหว่างประเทศประเมินเกี่ยวกับการโจมตีทางเครือข่ายคอมพิวเตอร์ว่าการแทรกแซงทางอิเล็กทรอนิกส์ด้วยเครือข่ายคอมพิวเตอร์ทางทหาร ไม่ว่าจะผ่านการโจมตีทางเครือข่ายคอมพิวเตอร์ (Computer Network Attacks) หรือการแสวงหาผลประโยชน์ทางเครือข่ายคอมพิวเตอร์ (Computer Network Exploitation) เพียงพอที่จะเป็นการเข้ามีส่วนร่วมโดยตรงในการสู้รบเช่นเดียวกับการดักฟังผู้บัญชาการระดับสูงหรือการส่งข้อมูลการกำหนดเป้าหมายทางยุทธวิธีสำหรับการโจมตี[241]

เมื่อพิจารณาข้อ 51 (3) แห่งพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 อธิบายพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ของคณะกรรมการกาชาดระหว่างประเทศและคำแนะนำเกี่ยวกับการตีความว่าด้วยการเข้ามีส่วนร่วมโดยตรงในการสู้รบประกอบกับลักษณะของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยพิจารณาประเมินขอบเขตการเข้ามีส่วนร่วมโดยตรงในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจากวิธีการตามผลกระทบ (Effect-based Approach) อาศัยการประเมินจากความตั้งใจ (Intended) หรือผลกระทบที่เป็นจริง (Actual Effect) ซึ่งเกิดจากการกระทำ ซึ่งการประเมินโดยใช้วิธีการตามผลกระทบได้รับการสนับสนุนตามแนวทาง

---

[240] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, vol. ICRC(90 IRRC 991 (2008), Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009).

[241] ibid. P. 48

ปฏิบัติของรัฐ (State Practice) และคำพิพากษาต่างๆ อาทิ คำพิพากษาของศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย คดี Strugar[242] พบว่า พลเรือนดังต่อไปนี้อาจกระทำการที่เข้าข่ายการเข้ามีส่วนร่วมโดยตรงในการสู้รบตามข้อ 51 (3) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1

(ก) พลเรือนที่ถูกว่าจ้าง โดยกองกำลังติดอาวุธหรือฝ่ายในการสู้รบอื่นเพื่อออกแบบเขียน (Malicious Code) หรือให้เข้าร่วมกองทัพในการโจมตีทางไซเบอร์อย่างอื่น โดยทำหน้าที่ภายในกองทัพหรือเคลื่อนที่ติดไปกับกองทัพ[243]

เมื่อพิจารณาตามคำแนะนำเกี่ยวกับการตีความว่าด้วยการเข้ามีส่วนร่วมโดยตรงในการสู้รบของคณะกรรมการกาชาดระหว่างประเทศเกี่ยวกับพลเรือนที่ถูกว่าจ้างและการเข้ามีส่วนร่วมโดยตรงในการสู้รบในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศระบุว่า ตราบเท่าที่ยังไม่ได้รวมอยู่ในกองกำลังติดอาวุธ พลเรือนที่ถูกว่าจ้างหรือผู้รับเหมาเอกชนยังไม่หยุดสถานะพลเรือนเพียงเพราะพวกเขาติดตามไปกับกองกำลังติดอาวุธและหรือมีหน้าที่ประจำอย่างอื่นนอกเหนือจากปฏิบัติการทางทหารที่ตามประเพณีแล้วเป็นการดำเนินการโดยบุคลากรทางทหาร ซึ่งแตกต่างกับกรณีพลเรือนที่ถูกว่าจ้างหรือผู้รับเหมาเอกชนที่มีเจตนาหรือวัตถุประสงค์ทั้งหมดเพื่อให้ได้รับการรวมเข้าไปในกองกำลังติดอาวุธของฝ่ายในการสู้รบไม่ว่าจะผ่านกระบวนการอย่างเป็นทางการภายใต้กฎหมายของรัฐหรือได้รับโดยพฤตินัยจากการทำหน้าที่ในการต่อสู้อย่างต่อเนื่อง บุคคลดังกล่าวถือเป็นสมาชิกของกองกำลังติดอาวุธที่มีลักษณะเป็นองค์กรสมาชิก กลุ่มหรือหน่วยภายใต้การรับผิดชอบบังคับบัญชาของฝ่ายในการสู้รบและไม่มีคุณสมบัติเป็นพลเรือนอีกต่อไป[244]

ดังนั้น บุคคลที่ถูกว่าจ้างให้ทำหน้าที่บำรุงรักษาเครือข่ายคอมพิวเตอร์โดยทั่วไปภายในกองทัพในฐานะผู้ให้บริการด้านไอทีทั่วไป เช่น อีเมลหรือเว็บไซต์ย่อมไม่ถูกพิจารณาว่ามีส่วนร่วมโดยตรงในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เนื่องจากการที่พวกเขาติดตามไปกับกองกำลังติดอาวุธเพื่อให้บริการด้านไอทีทั่วไปโดยไม่ได้เป็นสมาชิกของกองกำลังติดอาวุธยังไม่

---

[242] Chamber of International Criminal Tribunal for the Former Yugoslavia, *Prosecutor V. Strugar*, 2008. Paras. 176-179.

[243] Emily Crawford, "Virtual Battlegrounds: Direct Participation in Cyber Warfare " *I/S: A Journal of Law and Policy for the Information Society* 9, no. 1 (2013). P. 14.

[244] Chamber of International Criminal Tribunal for the Former Yugoslavia, Prosecutor V. Strugar, 2008. P. 39.

ถือว่าเป็นการกระทำอันเป็นการเข้ามีส่วนร่วมโดยตรงในการสู้รบ หากบุคคลเหล่านี้ถูกจับกุมในขณะที่มีการสู้รบจะได้รับสถานะเชลยศึกตามข้อ 4 เอ (4) ของอนุสัญญาเจนีวา[245] โดยไม่ถือเป็นพลรบและไม่อาจถูกโจมตีหรือตกเป็นเป้าหมายในการโจมตีโดยชอบด้วยกฎหมายได้[246]

ในขณะที่ลูกจ้างหรือผู้รับเหมาใดที่ถูกว่าจ้างให้ทำหน้าที่ดำเนินการอันเป็นปรปักษ์โจมตีทางไซเบอร์โดยเฉพาะ ในทางทฤษฎีย่อมพิจารณาได้ว่ามีส่วนร่วมโดยตรงในการสู้รบ[247] อาทิ พลเรือนที่ติดตั้งโปรแกรมบนระบบคอมพิวเตอร์และทำให้โปรแกรมดำเนินการ (ดำเนินการ หมายถึงการที่เครื่องคอมพิวเตอร์ลงมือกระทำการตามคำสั่งในโปรแกรม)

จากการวิเคราะห์ข้างต้นกล่าวได้ว่า พลเรือนที่ได้รับการว่าจ้างจากกองทัพให้ทำหน้าที่ภายในกองทัพไม่อาจถือว่าเป็นการเข้ามีส่วนร่วมโดยตรงในการสู้รบที่จะทำให้สูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศได้ทุกกรณี โดยพลเรือนที่ถูกว่าจ้างโดยกองทัพให้ทำหน้าที่ภายในกองทัพหรือเคลื่อนที่ไปกับกองกำลังของกองทัพจะต้องดำเนินการโจมตีทางไซเบอร์ที่เป็นการกระทำอันเป็นปรปักษ์ (Hostile Acts) ด้วยจึงจะเข้าข่ายการมีส่วนร่วมโดยตรงในการสู้รบ เพียงแค่การปรากฏตัวอยู่ภายในกองทัพและทำหน้าที่ทั่วไปตามที่ได้รับว่าจ้าง โดยไม่เกี่ยวข้องกับการดำเนินการโจมตีทางไซเบอร์ที่มีลักษณะเป็นการกระทำอันเป็นปรปักษ์ไม่อาจพิจารณาว่าพลเรือนเข้ามีส่วนร่วมโดยตรงในการสู้รบได้ ทั้งนี้ จะต้องพิจารณาเป็นรายกรณีไปตามความเกี่ยวข้องของหน้าที่ซึ่งได้รับมอบหมายกับการดำเนินการโจมตีทางไซเบอร์อันเป็นปรปักษ์ในสถานการณ์การขัดกันทางอาวุธ

---

[245] "Geneva Convention (Iii) Relative to the Treatment of Prisoners of War of 12 August 1949."

Article 4 (A) 4

A. Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:...

(4) Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorization from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model.

[246] David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities," *Journal of Conflict & Security Law* 17, no. 2 (2012). P. 293.

[247] Emily Crawford, "Virtual Battlegrounds: Direct Participation in Cyber Warfare " I/S: A Journal of Law and Policy for the Information Society 9, no. 1 (2013). P. 15.

(ข) พลเรือนที่เข้าร่วมในการโจมตีทางไซเบอร์ฝ่ายเดียว หรือ กลุ่มแฮคเกอร์รักชาติ (Patriotic Hackers)[248]

ตัวอย่างของพลเรือนกลุ่มนี้ ได้แก่ พลเรือนที่เข้าร่วมในการโจมตีทางไซเบอร์ต่อจอร์เจียในระหว่างสถานการณ์การขัดกันทางอาวุธระหว่างรัสเซียกับจอร์เจียในปีค.ศ. 2008 ตามคำแนะนำของเว็บไซต์ที่ให้บริการบันทึกข้อมูลส่วนตัว (Blogs) หรือเว็บไซต์ของรัสเซียเกี่ยวกับการจัดเตรียมคอมพิวเตอร์ให้ทำงานอย่างอัตโนมัติในการดำเนินการโจมตีด้วยวิธีการดีดีโอเอส หรือเสนอให้ดาว์นโหลดโปรแกรมดีดีโอเอส[249]

เมื่อพิจารณาลักษณะการกระทำของพลเรือนกลุ่มนี้ซึ่งดำเนินการด้วยความสมัครใจโดยรัฐหรือฝ่ายในการสู้รบไม่ได้บังคับหรือสั่งการให้ดำเนินการเป็นการเฉพาะแต่อย่างใด จะเห็นได้ว่าการกระทำของพลเรือนที่เข้าร่วมในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธฝ่ายเดียวโดยปราศจากการสั่งการอย่างเฉพาะเจาะจงหรือรับผิดชอบโดยฝ่ายในการสู้รบ การกระทำของกลุ่มแฮคเกอร์เหล่านี้เข้าข่ายเกณฑ์ในการเข้ามีส่วนร่วมโดยตรงในการสู้รบที่ทำให้พลเรือนสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศได้ เนื่องจากการกระทำใดๆ ทางไซเบอร์มีเจตนาหรือผลกระทบของการให้ความช่วยเหลือส่งผลให้เครือข่ายเป้าหมายในการโจมตีไร้ประโยชน์หรือไม่สามารถทำงานตามปกติได้อันมีลักษณะเป็นการกระทำอันเป็นปรปักษ์ย่อมพิจารณาว่าเป็นการเข้ามีส่วนร่วมโดยตรงในการสู้รบเช่นเดียวกับกรณีที่พลเรือนดำเนินการโจมตีด้วยอาวุธแบบดั้งเดิมที่ทำให้เกิดความเสียหายหรือการทำลายซึ่งฐานทัพทางทหารได้

[248] David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities," Journal of Conflict & Security Law 17, no. 2 (2012). P. 293.

[249] Evgeny Morozov, "An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar.," The Slate Group (August 14, 2008), http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html. [April 14, 2016]

(ค) พลเรือนที่ออกแบบหรือเขียนโปรแกรมที่ใช้สำหรับการโจมตีทางไซเบอร์ แต่ไม่ได้ดำเนินการ[250]

ในกรณีเช่นว่านี้คณะกรรมการกาชาดระหว่างประเทศชี้ให้เห็นว่า การกระทำของบุคคลที่เพียงแต่สร้างขึ้นหรือบำรุงรักษาความสามารถของฝ่ายในการสู้รบที่ก่อให้เกิดอันตรายไม่อยู่ในกรอบของการมีส่วนร่วมโดยตรงในการสู้รบ เช่น นักวิทยาศาสตร์ที่ทำการวิจัยและออกแบบเช่นเดียวกับการผลิตและการขนส่งซึ่งอาวุธและอุปกรณ์[251]

เมื่อพิจารณาลักษณะของพลเรือนที่ออกแบบหรือเขียนโปรแกรมที่ใช้สำหรับการโจมตีทางไซเบอร์เสมือนนักวิทยาศาสตร์ที่ทำการวิจัยและออกแบบอาวุธ พลเรือนดังกล่าวย่อมไม่เข้าข่ายเป็นพลเรือนที่เข้ามีส่วนร่วมโดยตรงในการสู้รบ ตราบเท่าที่พวกเขาไม่ได้มีส่วนเกี่ยวข้องโดยตรงในดำเนินการโปรแกรมที่ตนเองออกแบบหรือเขียนขึ้น

จากการศึกษาลักษณะของพลเรือนที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธข้างต้น สรุปได้ว่า พลเรือนที่เข้าร่วมในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจะต้องกระทำการอันเป็นปรปักษ์ที่มีวัตถุประสงค์หรือโดยลักษณะของการกระทำก่อให้เกิดอันตรายต่อเป้าหมาย การกระทำดังกล่าวย่อมเข้าข่ายการมีส่วนร่วมโดยตรงในการสู้รบส่งผลให้พลเรือนดังกล่าวสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศ โดยพลเรือนที่เข้าร่วมในการโจมตีทางไซเบอร์ย่อมสามารถถูกโจมตีได้โดยชอบด้วยกฎหมาย ในขณะที่เข้าร่วมในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้น

อย่างไรก็ตาม การขาดคำจำกัดความที่ชัดเจนของคำว่า “การเข้ามีส่วนโดยตรงในการสู้รบ” ตามอนุสัญญาเจนีวา นอกจากจะเป็นข้อท้าทายในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีด้วยอาวุธตามแบบแล้วยังส่งผลให้เป็นข้อท้าทายในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ด้วยเช่นกัน ซึ่งจะได้กล่าวในบทถัดไป

---

[250] Emily Crawford, "Virtual Battlegrounds: Direct Participation in Cyber Warfare " I/S: A Journal of Law and Policy for the Information Society 9, no. 1 (2013). P. 16.

[251] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, vol. ICRC(90 IRRC 991 (2008), Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009) P. 53.

3.2.2 หลักการเกี่ยวกับการปฏิบัติต่อเป้าหมาย

กฎหมายมนุษยธรรมระหว่างประเทศกำหนดหลักการเกี่ยวกับการปฏิบัติต่อเป้าหมายสำหรับฝ่ายในการสู้รบหลายประการ โดยในการศึกษาวิทยานิพนธ์เล่มนี้ จะหยิบยกเฉพาะหลักการสำคัญเกี่ยวกับการปฏิบัติต่อเป้าหมายที่ฝ่ายในการสู้รบจะต้องคำนึงระหว่างที่ดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ได้แก่ หลักการแยกแยะเป้าหมาย การปฏิบัติต่อเป้าหมายทางทหาร หลักความได้สัดส่วนในการโจมตีและหลักการใช้ความระมัดระวังในการโจมตี ก่อนที่จะได้ทำการศึกษาเกี่ยวกับหลักการพื้นฐานเกี่ยวกับการปฏิบัติต่อเป้าหมายที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจำเป็นที่ต้องทำความเข้าใจคำว่า “การโจมตี” ตามกฎหมายมนุษยธรรมระหว่างประเทศซึ่งเกี่ยวข้องกับหลักการเกี่ยวกับการปฏิบัติต่อเป้าหมายต่างๆ ดังนี้

3.2.2.1 การโจมตีทางไซเบอร์กับ “การโจมตี” ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศ

คำว่า “การโจมตี” (Attack) ปรากฏในหลักการพื้นฐานสำคัญเกี่ยวกับปฏิบัติการทางทหารตามกฎหมายมนุษยธรรมระหว่างประเทศมากมาย[252] อาทิ พลเรือนปัจเจกบุคคลตลอดจนประชากรพลเรือน จะต้องไม่ตกเป็นเป้าหมายของ “การโจมตี”[253] ทรัพย์สินของพลเรือนจะต้องไม่ตกเป็นเป้าหมายของ “การโจมตี”[254] หลักความได้สัดส่วนใน “การโจมตี”[255] ตลอดจนหลักการใช้ความ

---

[252] Nils Melzer, "Cyberwarfare and International Law," NUIDIR Resources Paper (2011). P. 25.

[253] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 51 (2)

“The civilian population as such, as well as individual civilians, shall not be the object of attack.”

[254] ibid.

Article 52 (1)

“Civilian objects shall not be the object of attack.”

[255] ibid.

Article 51 (5) (b)

“Among others, the following types of attacks are to be considered as indiscriminate:

ระมัดระวังใน “การโจมตี”[256] เป็นต้น

จะเห็นได้ว่า คำว่า “การโจมตี” (Attack) ปรากฏอยู่ในข้อบทของหลักการเกี่ยวกับการปฏิบัติต่อเป้าหมายแทบทุกหลักการ ในกรณีที่เป็นการโจมตีด้วยอาวุธตามแบบก่อให้เกิดความรุนแรงทำให้บาดเจ็บหรือเสียชีวิตของบุคคล ความเสียหายหรือการทำลายซึ่งทรัพย์สิ่งของต่างๆ ย่อมเป็นที่เข้าใจทั่วกันว่าเป็น “การโจมตี” ภายใต้ความหมายของกฎหมายมนุษยธรรมระหว่างประเทศอย่างไม่มีข้อสงสัย แต่กรณีการโจมตีทางไซเบอร์ที่มีลักษณะพิเศษแตกต่างจากการโจมตีด้วยอาวุธตามแบบ ไม่ว่าจะเป็นลักษณะการโจมตีที่เป็นการกระทำภายในห้วงไซเบอร์ที่ไม่มีลักษณะทางกายภาพ เป้าหมายการโจมตีเป็นเทคโนโลยีสารสนเทศและคอมพิวเตอร์ซึ่งมุ่งก่อให้เกิดความเสียหายต่อข้อมูล ระบบหรือเครือข่ายทางสารสนเทศและคอมพิวเตอร์มากกว่าการก่อให้เกิดการบาดเจ็บหรือเสียชีวิตของบุคคล ด้วยเหตุดังกล่าว จึงจำเป็นจะต้องพิจารณาว่าการโจมตีทางไซเบอร์เป็น “การโจมตี” ภายใต้ความหมายตามกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ อย่างไร

“การโจมตี” ภายใต้ความหมายของกฎหมายมนุษยธรรมระหว่างประเทศ ปรากฏตามข้อ 49 (1) พิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 กำหนดไว้ว่า “การโจมตี” หมายถึง การกระทำการในลักษณะรุนแรงต่อฝ่ายตรงข้าม ไม่ว่าในการรุกรานหรือการป้องกัน[257]

จากข้อ 49 (1) พิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 จะเห็นได้ว่า “การโจมตี” จะต้องเป็นการกระทำการในลักษณะรุนแรง (Acts of Violence) ถือเป็นเงื่อนไขสำคัญในการพิจารณาว่าการกระทำหรือปฏิบัติการทางทหารใดเป็น “การโจมตี” ตามกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ การกระทำการที่มีลักษณะรุนแรงจะต้องนำมาซึ่งการสูญเสียซึ่งชีวิต การบาดเจ็บ หรือ

(b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”

[256] ibid.

Article 57 (2)

“With respect to attacks, the following precautions shall be taken:

(a) those who plan or decide upon an attack shall:...”

[257] ibid.

Article 49 (1) Definition of attacks and scope of application

“Attacks”means acts of violence against the adversary, whether in offence or in defence.

ความเสียหายที่ชัดเจนต่อทรัพย์สินทางกายภาพ โดยพิจารณาลักษณะรุนแรงจากผลที่เกิดขึ้นจากการโจมตีนั้น (Effect-based Approach) ไม่ใช่ลักษณะรุนแรงจากตัวการกระทำหรืออาวุธที่ใช้ในการกระทำ การกระทำรุนแรงจึงอาจรวมถึงการโจมตีระบบเครือข่ายคอมพิวเตอร์จนถึงการทำลายล้างต่างๆ[258] หากขาดการกระทำที่มีลักษณะรุนแรง แม้จะเป็นอันตรายต่อฝ่ายตรงข้ามในการสู้รบก็ไม่ถือว่าเป็น “การโจมตี” เช่น การรวบรวมข้อมูลข่าวสารที่สำคัญทางการทหารของฝ่ายตรงข้าม หรือสงครามจิตวิทยา

อย่างไรก็ตาม “การโจมตี” ตามกฎหมายมนุษยธรรมระหว่างประเทศไม่ได้จำกัดประเภทของวิธีการหรือปัจจัยที่ใช้ในการโจมตีไว้แต่อย่างใด การโจมตีจึงไม่จำเป็นต้องเป็นการโจมตีโดยอาวุธร้ายแรงที่ทำอันตรายถึงตาย (Kinetic) เท่านั้น ปฏิบัติการทางทหารใดๆ ที่เป็นเหตุให้เกิดผลกระทบในลักษณะรุนแรงย่อมสามารถพิจารณาว่าเป็นการโจมตีตามกฎหมายมนุษยธรรมระหว่างประเทศได้ทั้งสิ้น[259]

จากการศึกษา “การโจมตี” ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศข้างต้น สามารถสรุปได้ว่า “การโจมตี” ภายใต้ความหมายของกฎหมายมนุษยธรรมระหว่างประเทศ จะต้องเป็นการกระทำที่มีลักษณะรุนแรงไม่ว่าจะเป็นการบาดเจ็บหรือเสียชีวิตของบุคคล ความเสียหายหรือการทำลายซึ่งทรัพย์สินสิ่งของพิจารณาลักษณะรุนแรงจากผลของการกระทำนั้นๆ อาทิ การโจมตีด้วยอาวุธชีวภาพ หรืออาวุธเคมีซึ่งเป็นอาวุธที่ไม่มีลักษณะรุนแรงในตัวเอง ลักษณะการใช้อาวุธชีวภาพหรืออาวุธเคมีไม่จำเป็นจะต้องใช้กำลังทางทหารหรือความรุนแรงในการโจมตี แต่สามารถก่อให้เกิดผลที่ร้ายแรง ทำให้ประชาชนเจ็บป่วย บาดเจ็บหรือเสียชีวิตจากการโจมตีด้วยอาวุธเคมีหรืออาวุธชีวภาพนั้นได้

เมื่อพิจารณาลักษณะของการโจมตีทางไซเบอร์ย่อมสามารถพิจารณาว่าเป็น “การโจมตี” ตามกฎหมายมนุษยธรรมระหว่างประเทศได้เช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ โดยมีเงื่อนไขว่าการโจมตีทางไซเบอร์นั้นจะต้องก่อให้เกิดผลที่มีลักษณะรุนแรง (Violence) กล่าวคือ การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้นจะต้องเป็นเหตุให้เกิดการบาดเจ็บหรือ

---

[258] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 85.

[259] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.," International Review of Red Cross 94(2012). P. 557.

เสียชีวิตของบุคคล หรือทำลายหรือทำให้เสียหายซึ่งทรัพย์สินสิ่งของ ตลอดจนการโจมตีทางไซเบอร์ใดที่เข้าแทรกแซงการทำงานของระบบหรือเครือข่ายที่สำคัญ แม้จะเป็นเพียงการขัดขวางการทำงานของระบบโดยไม่ได้ก่อให้เกิดความเสียหายทางกายภาพต่อระบบหรือทรัพย์สิ่งของใด แต่หากการขัดขวางการทำงานของระบบนั้นทำให้เกิดผลกระทบที่มีลักษณะรุนแรง การโจมตีทางไซเบอร์นั้นย่อมพิจารณาว่าเป็น “การโจมตี” ตามกฎหมายมนุษยธรรมระหว่างประเทศได้เช่นเดียวกัน

ยกตัวอย่าง การโจมตีทางไซเบอร์ต่อระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) เป็นเหตุให้เครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์เสียหายตามที่มีรายงานข่าว[260] เป็นการโจมตีที่ก่อให้เกิดความเสียหายทางกายภาพต่อทรัพย์สินคือเครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์เช่นนี้ย่อมเป็นการกระทำที่มีลักษณะรุนแรงถือเป็น “การโจมตี” ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศได้ หรือการโจมตีทางไซเบอร์ต่อระบบตรวจจับเรดาร์ป้องกันทางอากาศเพื่อเข้าแทรกแซงการทำงานของระบบ แม้ว่าจะไม่ก่อให้เกิดความเสียหายทางกายภาพต่อระบบ แต่การโจมตีทางไซเบอร์ดังกล่าวช่วยให้ฝ่ายที่ทำการโจมตีทางไซเบอร์สามารถใช้เครื่องบินทิ้งระเบิดต่อเป้าหมายทางทหารได้โดยไม่ถูกสกัดกั้นจากระบบป้องกันทางอากาศ เป็นเหตุให้เป้าหมายทางทหารได้รับความเสียหาย หรือถูกทำลาย พลรบได้รับบาดเจ็บหรือเสียชีวิตจากการที่เครื่องบินโจมตีทางอากาศดังกล่าว การแทรกแซงการทำงานของระบบดังกล่าว ย่อมพิจารณาว่าเป็น “การโจมตี” ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศได้ กล่าวได้ว่า การควบคุมคอมพิวเตอร์ของฝ่ายตรงข้ามเป็นเหตุให้เกิดการเสียชีวิต บาดเจ็บหรือความเสียหายต่อทรัพย์สินอาจพิจารณาว่าเป็น “การโจมตี” ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศได้

อย่างไรก็ตาม การเจาะเข้าโปรแกรมคอมพิวเตอร์ของฝ่ายตรงข้ามอย่างผิดกฎหมาย (Hacking) เพื่อรวบรวมข้อมูลข่าวสาร การเจาะความปลอดภัยในระบบคอมพิวเตอร์ (Fire Wall) การปล่อยหนอนคอมพิวเตอร์ (Worm) ในซอฟต์แวร์ การเอาข้อมูลความลับออก การได้มาซึ่งรหัสการควบคุมและการขัดขวางการติดต่อสื่อสารเหล่านี้ เมื่อพิจารณาจากผลของการกระทำที่มีลักษณะรุนแรง (Effect-based Approach) ย่อมไม่ถือเป็น “การโจมตี”ภายใต้กฎหมายมนุษยธรรมระหว่าง

[260] Yossi Melman, "Iran Pauses Uranium Enrichment at Natanz Nuclear Plant," Haaretz .COM, http://www.haaretz.com/news/world/iran-pauses-uranium-enrichment-at-natanz-nuclear-plant-1.326276.

ประเทศ เนื่องจากขาดการกระทำในลักษณะรุนแรงอันเป็นเงื่อนไขของการโจมตีภายใต้กฎหมายมนุษยธรรมระหว่างประเทศ[261]

ด้วยเหตุดังกล่าวข้างต้น การโจมตีทางไซเบอร์ใดที่สามารถพิจารณาว่าเป็น “การโจมตี” ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศจะต้องอยู่ภายใต้บังคับของหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ

3.2.2.2 หลักการพื้นฐานการแยกแยะเป้าหมาย

หลักการแยกแยะ (The Principle of Distinction) ถือเป็นหลักการพื้นฐานสำคัญตามกฎหมายมนุษยธรรมระหว่างประเทศ ทั้งการแยกแยะระหว่างพลเรือนและพลรบ[262] (Distinction between Civilians and Combatants) และการแยกแยะระหว่างทรัพย์สินพลเรือนและเป้าหมายทางทหาร[263] (Distinction between Civilian Objects and Military Objectives)

โดยหลักการแยกแยะได้รับการยอมรับปรากฏในหัวข้อ กฎเกณฑ์พื้นฐาน ตามข้อ 48 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1 ความว่า “เพื่อที่จะเป็นหลักประกันในการเคารพและคุ้มครองประชากรพลเรือนและทรัพย์สินของพลเรือน ฝ่ายต่างๆ ในการสู้รบจะต้อง

---

[261] Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," *Journal of Conflict & Security Law* 17, no. 2 (2012). P. 265.

[262] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule(Cambridge University Press, 2005)

Rule 1.

“The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians.”

[263] Jean-Marie Henckaerts and Louise Doswald-Beck, *Study on Customary International Humanitarian Law - Volume I: Rule*.

Rule 7.

“The parties to the conflict must at all times distinguish between civilian objects and military objectives. Attacks may only be directed against military objectives. Attacks must not be directed against civilian objects.”

แยกแยะระหว่างประชากรพลเรือนและพลรบและระหว่างทรัพย์สินของพลเรือนและเป้าหมายทางทหารอยู่ตลอดเวลา และต้องดำเนินปฏิบัติการเฉพาะต่อเป้าหมายทางทหารเท่านั้น”[264]

นอกจากนี้ คำพิพากษาในความเห็นเชิงปรึกษา ค.ศ. 1996 คดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์ (Advisory Opinion of Legality of The Threat or Use of Nuclear Weapons) ซึ่งศาลยุติธรรมระหว่างประเทศได้กล่าวว่า “หลักการสำคัญที่ปรากฏในตำราก่อให้เกิดเป็นโครงสร้างของกฎหมายมนุษยธรรมระหว่างประเทศ มีดังต่อไปนี้ ประการแรกคือวัตถุประสงค์ในการให้ความคุ้มครองประชากรพลเรือนและทรัพย์สินของพลเรือนและกำหนดการแยกแยะระหว่างพลรบและผู้ที่ไม่ใช่พลรบ โดยรัฐต้องไม่ทำให้พลเรือนเป็นเป้าหมายของการโจมตี และต้องไม่ใช้อาวุธที่ไม่สามารถแยกแยะระหว่างพลเรือนและเป้าหมายทางทหารได้...”[265]

ในการนี้ ศาลยุติธรรมระหว่างประเทศได้รับรองว่าหลักการแยกแยะระหว่างพลรบและพลเรือนเป็นหลักการพื้นฐานที่รัฐทุกรัฐพึงต้องปฏิบัติตาม ไม่ว่าจะได้ให้สัตยาบันอนุสัญญาที่ประกอบด้วยหลักการดังกล่าวหรือไม่ก็ตาม เนื่องจากหลักการแยกแยะระหว่างพลเรือนและพลรบก่อให้เกิดเป็นหลักการตามกฎหมายจารีตประเพณีระหว่างประเทศที่ละเมิดไม่ได้ (Intransgressible Principles of International Customary Law)[266]

---

[264] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 48 — Basic rule

“In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.”

[265] *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*. Para. 78.

“The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets...”

[266] ibid. Para. 79.

นอกจากนี้ ศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวียได้กล่าวไว้ในคดี Tadic ว่า หลักการแยกแยะในฐานะเป็นหลักการตามกฎหมายจารีตประเพณีระหว่างประเทศสามารถบังคับใช้กับการขัดกันทางอาวุธทุกประเภท[267]

จากการศึกษาข้อ 48 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1 และคำพิพากษาของศาลระหว่างประเทศข้างต้น สรุปได้ว่า หลักการพื้นฐานการแยกแยะเป้าหมายกำหนดหน้าที่ให้ฝ่ายในการสู้รบพึงต้องแยกแยะระหว่างพลเรือนและพลรบ ระหว่างทรัพย์สินของพลเรือนและเป้าหมายทางทหารตลอดเวลาที่ทำการสู้รบ เพื่อเป็นหลักประกันในการเคารพกฎหมายมนุษยธรรมระหว่างประเทศและการคุ้มครองประชากรพลเรือนและทรัพย์สินของพลเรือน

ทั้งนี้ พลเรือนและทรัพย์สินของพลเรือนต้องได้รับการคุ้มครองทางกฎหมายจากการสู้รบไม่ตกเป็นเป้าหมายของการโจมตี ในขณะที่พลรบและเป้าหมายทางทหารสามารถถูกโจมตีได้โดยชอบด้วยกฎหมายในระหว่างสถานการณ์การขัดกันทางอาวุธ โดยหลักการแยกแยะเป้าหมายบังคับใช้กับทุกสถานการณ์การขัดกันทางอาวุธ และบังคับใช้กับวิธีการและปัจจัยในการสู้รบทุกประเภท

เมื่อวิเคราะห์ลักษณะของการโจมตีทางไซเบอร์ที่เป็นไปตามหลักการแยกแยะโดยอาศัยการวิเคราะห์เช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ กล่าวได้ว่า ฝ่ายในการสู้รบที่ดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธไม่ว่าจะเป็นการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศหรือการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะต้องดำเนินการโดยเคารพหลักการแยกแยะเป้าหมายระหว่างพลเรือนและพลรบ ทรัพย์สินของพลเรือนและเป้าหมายทางทหารตลอดเวลาที่ทำการโจมตีทางไซเบอร์เช่นเดียวกับการโจมตีด้วยอาวุธที่ทำอันตรายถึงตายอื่นๆ

ดังนั้น ฝ่ายในการสู้รบจึงมีหน้าที่ในการพิจารณาแยกแยะว่าเป้าหมายในการโจมตีทางไซเบอร์นั้นว่าเป็นพลเรือนหรือพลรบ เป็นเป้าหมายทางทหารหรือทรัพย์สินของพลเรือน ฝ่ายในการสู้รบจะดำเนินการโจมตีทางไซเบอร์ต่อพลเรือนหรือทรัพย์สินของพลเรือนไม่ได้ จึงจะเป็นการโจมตีทางไซเบอร์ที่เคารพตามหลักการแยกแยะและไม่ฝ่าฝืนหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ

---

[267] *The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* Paras 112, 127.

ยกตัวอย่าง การโจมตีทางไซเบอร์ต่อระบบควบคุมการจราจรทางอากาศพลเรือนจนเป็นเหตุให้อากาศยานพลเรือนชนกันหรือการแทรกแซงฐานข้อมูลทางการแพทย์เป็นเหตุให้พลเรือนหรือพลรบซึ่งไม่มีส่วนเกี่ยวข้องกับการสู้รบได้รับการถ่ายหมู่เลือดที่ไม่ถูกต้องในการรักษาพยาบาล เช่นนี้ ย่อมเป็นการขัดต่อหลักการพื้นฐานการแยกแยะเป้าหมาย เนื่องจากพลเรือนและทรัพย์สินของพลเรือนไม่อาจตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ได้

ในส่วนถัดไปจะได้ทำการศึกษาว่า เทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่เป็นเป้าหมายทางทหารและตกเป็นเป้าหมายในการโจมตีได้โดยชอบด้วยกฎหมายประกอบด้วยเงื่อนไขในการพิจารณาอย่างไรบ้าง

3.2.2.3 เป้าหมายทางทหาร

จากการศึกษาที่ผ่านมา การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธใดๆ จะต้องดำเนินการโดยเคารพหลักการแยกแยะเป้าหมาย ดังนั้น ฝ่ายในการสู้รบจึงสามารถดำเนินการโจมตีทางไซเบอร์โดยตรงต่อเป้าหมายทางทหารเท่านั้น ด้วยเหตุดังกล่าว จำเป็นจะต้องวิเคราะห์ว่าเป้าหมายทางทหารที่สามารถดำเนินการโจมตีทางไซเบอร์ได้นั้นมีความหมายครอบคลุมสิ่งใดบ้าง ดังนี้

คำว่า เป้าหมายทางทหาร (Military Objectives) บัญญัติคำนิยามไว้ในข้อ 52 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[268] ระบุว่า “การโจมตีจะต้องจำกัดอย่างเคร่งครัดต่อเป้าหมายทางทหาร ในกรณีที่เกี่ยวกับทรัพย์สิน สิ่งของนั้น เป้าหมายทางทหารจำกัดเฉพาะทรัพย์สินสิ่งของซึ่งโดยลักษณะ สถานที่ตั้ง วัตถุประสงค์ หรือการใช้ ก่อให้เกิดประสิทธิภาพในปฏิบัติการทางทหาร และการทำลายล้างไม่ว่าทั้งหมดหรือบางส่วน การยึดหรือการทำให้หมดสมรรถภาพซึ่ง

---

[268] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 52 (2)

“Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”

ทรัพย์สิน สิ่งของ ในสภาวการณ์ขณะที่ปฏิบัติการนั้น จะก่อให้เกิดความได้เปรียบทางทหารอย่างชัดเจน”

จากข้อบทข้างต้น การพิจารณาว่าสิ่งใดเป็นเป้าหมายทางทหารประกอบด้วยเงื่อนไขสำคัญสองประการ ได้แก่ (1) ลักษณะ สถานที่ตั้ง วัตถุประสงค์หรือการใช้ และ (2) ความได้เปรียบทางทหารอย่างชัดเจน โดยมีรายละเอียดดังต่อไปนี้

3.2.2.3.1 ลักษณะ สถานที่ตั้ง วัตถุประสงค์หรือการใช้

เงื่อนไขประการแรก คือ ลักษณะ สถานที่ตั้ง วัตถุประสงค์หรือการใช้ (Nature Location Purpose or Use) ตามข้อ 52 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[269] กำหนดให้ เป้าหมายทางทหารจะต้องเป็นทรัพย์สิ่งของซึ่งโดยลักษณะ สถานที่ตั้ง วัตถุประสงค์หรือการใช้ก่อให้เกิดประสิทธิภาพในปฏิบัติการทางทหาร ดังนี้

“ลักษณะของเป้าหมายทางทหาร” จะต้องก่อให้เกิดประสิทธิภาพในปฏิบัติการทางทหาร มีคุณค่าทางทหารในตัว เช่น ฐานทัพ ระบบอาวุธ อุปกรณ์ทางทหาร โกดังและคลังอาวุธโรงงานไฟฟ้าที่ใช้ทางการทหาร เครือข่ายคมนาคมที่สำคัญทางยุทธศาสตร์ กล่าวคือ โดยลักษณะของวัตถุสิ่งของนั้นจะต้องเป็นทรัพย์สินสิ่งของต่างๆ ที่ใช้โดยกองกำลังติดอาวุธ หรือใช้สนับสนุนในการดำเนินการทางทหารต่างๆ

เมื่อพิจารณาปฏิบัติการทางทหารในปัจจุบันซึ่งพึ่งพาเทคโนโลยีสารสนเทศและคอมพิวเตอร์เพิ่มมากขึ้นในการดำเนินกิจกรรมต่างๆ ของกองทัพ ไม่ว่าจะเป็นการบริหารงานในกองทัพ หรือการทำสงครามสู้รบล้วนอาศัยเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้ใช้อำนวยความสะดวกในการดำเนินกิจกรรมต่างๆ ไม่ว่าจะเป็น การเก็บรักษาข้อมูลทางทหาร ความลับทาง

---

[269] ibid.

Article 52 (2)

“Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”

ทหาร เป้าหมายทางทหาร ตลอดจนข้อมูลส่วนตัวของสมาชิกของกองทัพต่างๆ การบัญชาการติดต่อสื่อสารต่างๆ เทคโนโลยีสารสนเทศและคอมพิวเตอร์จึงเป็นสิ่งที่ใช้สนับสนุนในปฏิบัติการทางทหารต่างๆ ได้

ดังนั้น เทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่ใช้โดยกองทัพย่อมสามารถพิจารณาว่าเป็นเป้าหมายทางทหารได้เช่นกัน ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ที่ใช้ในกองทัพ ระบบหรือเครือข่ายที่ใช้ในกิจการทางทหาร รวมทั้งศูนย์คอมพิวเตอร์ที่ใช้ในการบัญชาการติดต่อสื่อสารสิ่งต่างๆ เหล่านี้เมื่อใช้ในกิจการทางทหารย่อมเป็นเป้าหมายทางทหารได้ในตัวโดยอัตโนมัติ

“สถานที่ตั้ง” หมายถึง บริเวณที่กลุ่มเป้าหมายทางทหารตั้งอยู่ด้วยกันในขณะที่มีการสู้รบ เช่น ค่ายทหาร คลังอาวุธ กล่าวคือ ทรัพย์สิน สิ่งของซึ่งโดยลักษณะไม่มีหน้าที่หรือคุณค่าทางทหารในตัวอาจถูกพิจารณาว่าเป็นเป้าหมายทางทหารได้จาก “สถานที่ตั้ง” หากตั้งอยู่บริเวณที่กลุ่มเป้าหมายทางทหารตั้งอยู่ด้วยกันในขณะที่มีการสู้รบ

เมื่อพิจารณาจาก “สถานที่ตั้ง” หากคอมพิวเตอร์ซึ่งไม่ได้เป็นของกองทัพและไม่ได้ถูกใช้งานโดยพลรบตั้งอยู่ในบริเวณที่กลุ่มเป้าหมายทางทหารตั้งอยู่ เช่น ตั้งอยู่ภายในค่ายทหาร หรือคลังอาวุธ ย่อมทำให้คอมพิวเตอร์นั้นตกเป็นเป้าหมายทางทหารได้เช่นกัน[270]

อย่างไรก็ตาม เมื่อพิจารณาจากลักษณะของระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่ไม่มีลักษณะทางกายภาพ อีกทั้งภายในห้วงไซเบอร์ไม่มีเส้นแบ่งเขตแดนใดๆ ระบบหรือเครือข่ายทางการทหารและระบบหรือเครือข่ายของพลเรือนต่างเชื่อมต่อกันภายในห้วงไซเบอร์ ในการพิจารณาเป้าหมายทางทหารว่าระบบหรือเครือข่ายทางไซเบอร์ใดเป็นระบบหรือเครือข่ายทางการทหารอาจไม่สามารถพิจารณาจากเงื่อนไข “สถานที่ตั้ง” ได้

ในส่วนของ “วัตถุประสงค์หรือการใช้” วัตถุประสงค์จะเกี่ยวข้องกับความตั้งใจในอนาคตที่จะใช้ทรัพย์สิ่งของนั้น ในขณะที่ การใช้จะเกี่ยวข้องกับหน้าที่ในปัจจุบันของสิ่งของนั้น กล่าวคือ วัตถุประสงค์อนุมานจากความตั้งใจเริ่มต้นของการใช้ในอนาคต ซึ่งอาจเปลี่ยนแปลงไปตามลักษณะการใช้ได้ เช่น ใช้โรงเรียนเป็นค่ายทหาร ใช้รถโดยสารประจำทางในการลำเลียงพลรบ

---

[270] Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," Journal of Conflict & Security Law 17, no. 2 (2012). P. 263.

เหล่านี้ย่อมทำให้วัตถุประสงค์ทางพลเรือนเปลี่ยนเป็นวัตถุประสงค์ทางทหารได้[271] จะเห็นได้ว่าวัตถุประสงค์หรือการใช้ของทรัพย์สิ่งของนั้นเดิมทีไม่ได้ใช้เพื่อกิจการทางทหารหรือสนับสนุนในกิจการทางทหาร เมื่อถูกนำไปใช้ให้มีหน้าที่ทางทหาร ทรัพย์สิ่งของเหล่านั้นย่อมถือเป็นเป้าหมายทางทหารจากวัตถุประสงค์หรือการใช้

เมื่อพิจารณาเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่อาจเป็นเป้าหมายทางทหารได้จากวัตถุประสงค์หรือการใช้ ตัวอย่างเช่น คอมพิวเตอร์หรือเครือข่ายของพลเรือนซึ่งใช้เป็นการส่วนตัวของพลเรือน หรือใช้ในการพาณิชย์ก็ตาม หากมีการนำคอมพิวเตอร์หรือเครือข่ายของพลเรือนมาใช้ในกิจการทางทหารหรือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธย่อมทำให้เครื่องคอมพิวเตอร์หรือเครือข่ายของพลเรือนนั้นเป็นเป้าหมายทางทหารจากวัตถุประสงค์หรือการใช้งานและสามารถตกเป็นเป้าหมายในการโจมตีได้โดยชอบด้วยกฎหมาย

เป็นที่น่าสังเกตว่า ในปัจจุบันกองทัพทหารหลายประเทศได้นำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้เพิ่มประสิทธิภาพทางการทหารอย่างกว้างขวาง ไม่ว่าจะเป็นการจัดการขอบเขตทั้งหมดของการวางแผนโจมตี หรือใช้ในงานบริหารงานทางทหารทั่วไป ใช้ประมวลผลหรือใช้เป็นหน่วยเก็บข้อมูลทางทหาร และการเข้ารหัสหรือถอดรหัสคำสั่งต่างๆ คอมพิวเตอร์ของหน่วยงานทางทหารหรือคอมพิวเตอร์ของหน่วยข่าวกรองต่างๆ อุปกรณ์จัดเส้นทางข่ายงานคอมพิวเตอร์ หรือเราต์เตอร์ (Routers) เครือข่าย (Networks) เคเบิ้ล (Cables) และสินทรัพย์ไซเบอร์อื่นๆ (Cyber Assets) สิ่งต่างๆ เหล่านี้สามารถพิจารณาเป็นเป้าหมายทางทหารได้จากการใช้อำนวยความสะดวกในการติดต่อสื่อสารของทหาร[272]

จากการศึกษาข้างต้น จะเห็นได้ว่า เทคโนโลยีสารสนเทศและคอมพิวเตอร์สามารถพิจารณาว่าเป็นเป้าหมายทางทหารได้จากทั้ง “ลักษณะ” ซึ่งใช้ในกิจการทางทหารไม่ว่าจะเป็นในการบริหารหรือการสู้รบของกองทัพ “สถานที่ตั้ง” หากติดตั้งอยู่ภายในบริเวณกองบัญชาการฐานทัพทหารหรืออาคารสถานที่ของกองทัพต่างๆ รวมทั้งเมื่อถูกพาเข้าไปโดยเจ้าหน้าที่ทหาร “วัตถุประสงค์หรือการใช้” จากการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของพลเรือนมาใช้ให้มีหน้าที่ทางทหาร ไม่ว่าจะเป็นใช้ในกิจการทางทหารหรือใช้ในการโจมตีทางไซเบอร์ในสถานการณ์การ

---

[271] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 89.

[272] Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks," *Texas Law Review* 88(2010). P. 1543.

ขัดกันทางอาวุธก็ตาม เทคโนโลยีสารสนเทศและคอมพิวเตอร์ใดที่สามารถพิจารณาว่าเป็นเป้าหมายทางทหารได้ ย่อมสามารถถูกโจมตีได้โดยชอบด้วยกฎหมาย

3.3.2.3.2 ความได้เปรียบทางทหารอย่างชัดเจน

นอกเหนือจากการพิจารณาลักษณะ สถานที่ตั้ง วัตถุประสงค์หรือการใช้ของทรัพย์สิน สิ่งของนั้นๆ ตามข้อ 52 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ที่ได้ศึกษาในส่วนที่ผ่านมา คำนิยามของคำว่าเป้าหมายทางทหารตามข้อ 52 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ยังกำหนดเงื่อนไขว่า การทำลายล้างไม่ว่าทั้งหมดหรือบางส่วน การยึดหรือการทำให้หมดสมรรถภาพซึ่งทรัพย์สิน สิ่งของนั้น ในสภาวการณ์ขณะที่ปฏิบัติการนั้น จะต้องก่อให้เกิด “ความได้เปรียบทางทหารอย่างชัดเจน” อีกด้วย

การพิจารณาความได้เปรียบทางทหารที่ได้รับจากทรัพย์สินสิ่งของนั้นจะต้องเป็นความได้เปรียบทางด้านการทหารเท่านั้น มิใช่เรื่องอื่น เช่น ทางการเมือง[273] หรือทางเศรษฐกิจ ความได้เปรียบทางการเมืองที่อาจเกิดขึ้นไม่สามารถพิจารณาลักษณะของทรัพย์สินสิ่งของนั้นว่าเป็นเป้าหมายทางทหารได้ และการบังคับให้มีการเปลี่ยนแปลงท่าทีในการเจรจาต่อรองของฝ่ายตรงข้ามไม่สามารถถือว่าเป็นความได้เปรียบทางทหาร ความได้เปรียบทางทหารยังต้องพิจารณาจากความได้เปรียบที่ได้รับจากภาพรวมการโจมตี ไม่ใช่จากส่วนหนึ่งส่วนใดของการโจมตี[274]

นอกจากนี้ ในการศึกษากฎหมายจารีตประเพณีของกฎหมายมนุษยธรรมระหว่างประเทศโดยคณะกรรมการกาชาดระหว่างประเทศชี้ให้เห็นว่า ในการประเมินความได้เปรียบ

---

[273] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, ed. Second(United Kingdom: Cambridge University Press, 2010) P. 93

[274] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012). P. 191.

ทางทหารของผู้ที่รับผิดชอบในการวางแผน การตัดสินใจหรือดำเนินการโจมตีจำเป็นที่จะต้องประเมินข้อมูลจากแหล่งข้อมูลทั้งหมดที่มีอยู่ของสภาวการณ์ในขณะนั้น[275]

จากการศึกษาเงื่อนไขการพิจารณาลักษณะเป้าหมายทางทหารข้างต้น นอกจากการพิจารณาเทคโนโลยีสารสนเทศและคอมพิวเตอร์จากลักษณะ สถานที่ตั้ง วัตถุประสงค์หรือการใช้ เทคโนโลยีสารสนเทศและคอมพิวเตอร์ดังกล่าวจะต้องก่อให้เกิดความได้เปรียบทางทหารอย่างชัดเจน จึงจะสามารถพิจารณาว่าเป็นเป้าหมายทางทหารตามข้อ 52 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 และเป็นเป้าหมายในการโจมตีได้โดยชอบด้วยกฎหมาย เช่นเดียวกับทรัพย์สินสิ่งของที่เป็นเป้าหมายทางทหารในการโจมตีด้วยอาวุธตามแบบ ยกตัวอย่าง การโจมตีทางไซเบอร์ต่อระบบตรวจจับเรดาร์ป้องกันทางอากาศ ทำให้ไม่สามารถตรวจจับตำแหน่งเครื่องบินรบและทำการทิ้งระเบิดเป้าหมายได้สำเร็จ เช่นนี้ระบบหรือคอมพิวเตอร์ที่ใช้ในการแทรกซึมระบบตรวจจับเรดาร์ป้องกันอากาศยานดังกล่าว ย่อมถือเป็นทรัพย์สิ่งของที่โดยวัตถุประสงค์หรือการใช้ก่อให้เกิดความได้เปรียบทางทหารอย่างชัดเจน ในขณะที่ การใช้เครื่องคอมพิวเตอร์โจมตีระบบตลาดหลักทรัพย์ ทำให้เกิดความเสียหายทางเศรษฐกิจ แม้ว่าจะส่งผลกระทบต่อพลเรือนก่อไม่ถือว่าคอมพิวเตอร์หรือระบบที่ใช้ในการโจมตีนั้นก่อให้เกิดความได้เปรียบทางทหาร คอมพิวเตอร์หรือระบบที่ใช้โจมตีดังกล่าว ย่อมไม่สามารถพิจารณาว่าเป็นเป้าหมายทางทหารและไม่อาจถูกโจมตีได้โดยชอบด้วยกฎหมาย

เป็นที่น่าสังเกตว่า ลักษณะของเป้าหมายทางทหารที่เป็นเทคโนโลยีสารสนเทศและคอมพิวเตอร์เป็นเทคโนโลยีที่สามารถเชื่อมต่อระหว่างระบบหรือเครือข่ายทางทหารและระบบหรือเครือข่ายของพลเรือนได้ ทำให้เกิดข้อท้าทายในการปฏิบัติตามกฎหมายมนุษยธรรมระหว่างประเทศอย่างมีนัยสำคัญ ซึ่งจะได้วิเคราะห์ในบทต่อไป

นอกเหนือจากหลักการแยกแยะเป้าหมาย ฝ่ายในการสู้รบที่จะดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธพึงต้องคำนึงถึงหลักความได้สัดส่วนในการโจมตีก่อนดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธด้วย พิจารณารายละเอียดในส่วนถัดไป

---

[275] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005) P. 50.

3.2.2.4 หลักความได้สัดส่วนในการโจมตี

หลักความได้สัดส่วนในการโจมตี หรือ The Principle of Proportionality มีที่มาจากกฎหมายจารีตประเพณีระหว่างประเทศ[276] และถูกยอมรับไว้ในข้อ 51 (5) (บี)[277] ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ซึ่งเป็นข้อห้ามโจมตีโดยไม่เลือกเป้าหมาย ระบุว่า การโจมตีซึ่งอาจคาดได้ว่าจะก่อให้เกิดการสูญเสียซึ่งชีวิตของพลเรือน การบาดเจ็บของพลเรือน ความเสียหายต่อทรัพย์สินของพลเรือน หรือความเสียหายดังกล่าวรวมกัน ซึ่งมากเกินกว่าความได้เปรียบทางทหารที่มีลักษณะโดยตรงและเป็นรูปธรรมอันคาดหมายไว้

หลักความได้สัดส่วนในการโจมตีกล่าวซ้ำในข้อ 57 (2) (เอ) (III)[278] ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1 เกี่ยวกับหน้าที่ของฝ่ายในการสู้รบในการละเว้นจากการโจมตีที่คาดได้ว่าจะก่อให้เกิดความเสียหายต่อพลเรือนที่ “มากเกินกว่า” (Excessive) ความได้เปรียบทางทหารที่มีลักษณะโดยตรงและเป็นรูปธรรมอันได้คาดหมายไว้ (Concrete and Direct Military Advantage)

---

[276] Ibid.

[277] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 51 (5)

“Among others, the following types of attacks are to be considered as indiscriminate:

(b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”

[278] ibid.

Article 57 (2) (a) (iii)

“ With respect to attacks, the following precautions shall be taken:

a) those who plan or decide upon an attack shall:

iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;”

เมื่อพิจารณาข้อบทข้างต้น แม้จะไม่ปรากฏคำว่า “สัดส่วน” (Proportionality) ในพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 หลักความได้สัดส่วนในการโจมตีเป็นที่รู้จักว่าคือ ข้อห้ามการโจมตีที่ก่อให้เกิดผลกระทบข้างเคียงต่อพลเรือนหรือทรัพย์สินของพลเรือนมากเกินควร ดังถ้อยคำของผู้พิพากษา Higgins ในความเห็นแย้งคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์ ที่กล่าวว่า “แม้จะไม่ปรากฏข้อบทของหลักความได้สัดส่วนไว้เป็นการเฉพาะ หลักความได้สัดส่วนก็ปรากฏสะท้อนอยู่ในหลายข้อบทของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1949 ฉบับที่ 1 ดังนั้น แม้จะเป็นเป้าหมายที่ชอบด้วยกฎหมายก็ไม่อาจถูกโจมตีได้ หากความเสียหายข้างเคียงที่เกิดขึ้นต่อพลเรือนไม่ได้สัดส่วนกับประโยชน์ทางการทหารที่ได้รับจากการโจมตี”[279]

นอกจากนี้ การตั้งใจโจมตีโดยรู้หรือคาดหมายได้ว่าการโจมตีจะก่อให้เกิดผลกระทบต่อพลเรือนหรือทรัพย์สินของพลเรือน (Collateral Damage) ซึ่ง “มากเกินกว่าความได้เปรียบทางทหารที่มีลักษณะโดยตรงและเป็นรูปธรรมอันได้คาดหมายไว้” ยังถือเป็นอาชญากรรมสงครามภายใต้ข้อ 8 (2) (บี) (IV) ของธรรมนูญกรุงโรมว่าด้วยศาลอาญาระหว่างประเทศ (The Rome Statute of The International Criminal Court)[280] อีกด้วย

ใจความสำคัญของหลักความได้สัดส่วนคือ ผลกระทบต่อพลเรือนและทรัพย์สินของพลเรือนที่เกิดจากการโจมตีต่อเป้าหมายที่ชอบด้วยกฎหมายจะต้องคาดได้ว่าไม่มากเกินควร (Excessive) กับความได้เปรียบทางทหารที่คาดหวังไว้ ซึ่งผู้โจมตีจะต้องชั่งน้ำหนักระหว่างความได้เปรียบทางทหารกับผลกระทบต่อพลเรือน (Collateral Damage) ที่คาดได้ว่าจะเกิดขึ้นต่อพลเรือน

---

[279] *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*. at 587.

[280] "Rome Statute of the International Criminal Court."

Article 8 (2) (b) (iv),

“For the purpose of this Statute, ‘war crimes’ means:

(b) Other serious violations of the laws and customs applicable in international armed conflict, within the established framework of international law, namely, any of the following acts:

(iv) Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated;”

และทรัพย์สินของพลเรือนและยังต้องพิจารณาทางเลือกในการใช้วิธีการในการสู้รบอื่นที่จะลดผลกระทบต่อพลเรือนและทรัพย์สินของพลเรือนได้[281] โดยฝ่ายในการสู้รบจะต้องพิจารณาอย่างมีเหตุมีผล (Reasonably) ด้วยความสุจริต (Good Faith) และมีหน้าที่ในการชั่งน้ำหนักจากข้อมูลทั้งหมดที่มีอยู่ในสภาวการณ์นั้น ซึ่งศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวียได้กล่าวไว้ในคำพิพากษาคดี Galić ว่า “ในการพิจารณาว่าการโจมตีได้สัดส่วนหรือไม่นั้นจำเป็นที่จะต้องพิจารณาโดยผู้ที่มีความรู้และมีความเชี่ยวชาญในสภาวการณ์นั้น และตัดสินใจโดยใช้ข้อมูลที่มีอยู่อย่างสมเหตุสมผล ซึ่งคาดได้ว่าจะมีการบาดเจ็บเสียชีวิตของพลเรือนที่เกินควรอันเป็นผลมาจากการโจมตีนั้น”[282]

เป็นที่น่าสังเกตว่า หลักความได้สัดส่วนนี้บังคับใช้ให้ความคุ้มครองเฉพาะแก่พลเรือนและทรัพย์สินของพลเรือนเท่านั้น กฎหมายมนุษยธรรมระหว่างประเทศไม่ได้มีข้อกำหนดให้มีหลักความได้สัดส่วนระหว่างพลรบ พลรบไม่จำต้องคำนึงถึงหลักความได้สัดส่วนในการสู้รบกับพลรบฝ่ายตรงข้ามแต่อย่างใด[283]

จากการศึกษาในส่วนนี้ กล่าวได้ว่า หลักความได้สัดส่วนในการโจมตีกำหนดหน้าที่ให้ฝ่ายในการสู้รบชั่งน้ำหนักระหว่างความได้เปรียบทางทหาร (ที่มีลักษณะโดยตรงและเป็นรูปธรรมอันได้คาดหมายไว้) กับความเสียหายที่อาจเกิดขึ้นต่อพลเรือนหรือทรัพย์สินของพลเรือน (การบาดเจ็บเสียชีวิตของพลเรือน หรือความเสียหายต่อทรัพย์สินของพลเรือน) โดยความเสียหายที่อาจเกิดขึ้นต่อพลเรือนหรือทรัพย์สินของพลเรือนนั้นจะต้องไม่มากเกินกว่า (Excessive) ความได้เปรียบทางทหารที่คาดว่าจะได้รับ ทั้งนี้ หน้าที่ของฝ่ายในการสู้รบตามหลักความได้สัดส่วนจะต้องอาศัยดุลพินิจของฝ่ายในการสู้รบในการประเมินชั่งน้ำหนัก

เมื่อพิจารณาการบังคับใช้หลักความได้สัดส่วนในการโจมตีกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ จะเห็นได้ว่า ฝ่ายในการสู้รบมีหน้าที่ในการประเมินชั่งน้ำหนักระหว่างความได้เปรียบทางทหารที่คาดหมายไว้จากการโจมตีทางไซเบอร์กับผลกระทบต่อพลเรือนและทรัพย์สินของพลเรือน (Collateral Damage) ที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์นั้น

---

[281] James H. Doyle, "Computer Networks, Proportionality, and Military Operations," *International Law Studies* 76, no. 9 (2002). P. 156.

[282] *The Prosecutor V. Galic, Case No. It-98-29-T, Trial Chamber*, 5 December 2003. Para. 58.

[283] Eric Talbot Jensen, "Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?," *American University International Law Review* 18, no. 5 (2003). P. 1171.

โดยผลกระทบต่อพลเรือนจะต้องไม่มาก “เกินควร” (Excessive) กับความได้เปรียบทางทหารที่คาดหมายว่าจะได้รับ

การประเมินชั่งน้ำหนักจะต้องกระทำก่อนดำเนินการโจมตีทางไซเบอร์บนพื้นฐานของข้อมูลทั้งหมดที่มีอยู่ในขณะนั้น ซึ่งฝ่ายในการสู้รบมีหน้าที่ในการรวบรวมข้อมูลเท่าที่จะเป็นไปได้[284] และประเมินชั่งน้ำหนักด้วยความสุจริตใจและความระมัดระวังตามสมควรในการคาดการณ์ผลกระทบต่อพลเรือน (Expectation of the Collateral Damage) และความได้เปรียบทางทหารที่คาดหวังไว้ (Anticipation of the Military Advantage) ที่มีลักษณะโดยตรงและเป็นรูปธรรมที่ได้จากการโจมตี

ตัวอย่างเช่น การโจมตีทางไซเบอร์โดยทำให้หยุดชะงัก ทำลาย หรือรบกวนคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ซึ่งให้บริการแก่พลเรือนเป็นหลักและสนับสนุนกิจการทางทหารด้วย จนก่อให้เกิดความเสียหายที่ไม่สามารถแก้ไขได้ต่อโครงสร้างพื้นฐานที่สำคัญของพลเรือน เช่น ระบบการจัดการน้ำ ศูนย์การวิจัย ระบบการเงินการธนาคาร ตลาดหลักทรัพย์ย่อมถือว่าเป็นผลกระทบต่อพลเรือนที่ “เกินควร” (Excessive)[285] จะเห็นได้ว่า ความเสียหายที่ไม่สามารถแก้ไขได้ต่อโครงสร้างพื้นฐานที่สำคัญของพลเรือนอันเป็นผลกระทบต่อพลเรือนนั้นมีลักษณะมากเกินควรกว่าความได้เปรียบทางทหารที่ได้รับจากการทำลายคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ที่ใช้สนับสนุนกิจการทางทหาร เนื่องจากความเสียหายที่พลเรือนได้รับนั้นเป็นความเสียหายที่ไม่สามารถแก้ไขได้

ในทำนองเดียวกัน หากฝ่ายในการสู้รบจะดำเนินการโจมตีทางไซเบอร์ต่อเป้าหมายทางทหาร เช่น ระบบการติดต่อสื่อสารทางทหาร จะต้องประเมินว่าการโจมตีนั้นเป็นการทำลายหรือลดประสิทธิภาพการติดต่อสื่อสารทางทหารอย่างแท้จริงและชั่งน้ำหนักระหว่างความได้เปรียบทางทหารที่ได้จากการทำลายการติดต่อสื่อสารทางทหารกับความเสียหายต่อพลเรือนจากการทำลายเครือข่ายและการติดต่อสื่อสารของพลเรือนโดยไม่ตั้งใจ โดยความเสียหายที่เกิดขึ้นต่อพลเรือนจะต้อง

---

[284] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005) P. 50.

[285] James H. Doyle, "Computer Networks, Proportionality, and Military Operations," International Law Studies 76, no. 9 (2002). P. 159.

ไม่มากเกินควร (Excessive) เมื่อเปรียบเทียบกับความได้เปรียบทางทหารที่จะได้รับจากการโจมตีทางไซเบอร์นั้น[286]

อย่างไรก็ตาม หลักความได้สัดส่วนในการโจมตีดังกล่าวเห็นได้ชัดว่าขึ้นอยู่กับดุลพินิจของฝ่ายในการสู้รบที่จะทำการประเมินชั่งน้ำหนัก โดยไม่มีเกณฑ์ในการกำหนดขอบเขตในการชั่งน้ำหนักที่ชัดเจน ส่งผลให้ความคุ้มครองพลเรือนตามหลักการดังกล่าวไม่อาจเกิดขึ้นได้ตามความเป็นจริง[287]

เมื่อนำหลักความได้สัดส่วนในการโจมตีบังคับใช้กับการโจมตีทางไซเบอร์ซึ่งผลกระทบที่เกิดขึ้นจากการโจมตีทางไซเบอร์ส่วนใหญ่ไม่ได้ปรากฏขึ้นในทันทีที่ถูกโจมตีต่างจากการโจมตีด้วยอาวุธตามแบบก่อให้เกิดการบาดเจ็บหรือเสียชีวิตของพลเรือน หรือความเสียหายต่อทรัพย์สินของพลเรือนขึ้นในทันทีที่โจมตีต่อเป้าหมาย เช่น การยิงปืน การทิ้งระเบิด ซึ่งฝ่ายในการสู้รบสามารถคาดการณ์ผลกระทบที่จะเกิดขึ้นต่อพลเรือนได้ตามอานุภาพในการทำลายล้างของอาวุธนั้นๆ ตลอดจนจำนวนของพลเรือนหรือทรัพย์สินของพลเรือนที่อยู่ในขอบเขตรัศมีของการโจมตีด้วยอาวุธตามแบบนั้น ด้วยเหตุที่ การโจมตีทางไซเบอร์ส่วนใหญ่ไม่ก่อให้เกิดความเสียหายหรือผลกระทบขึ้นในทันทีที่โจมตีต่อเป้าหมายจึงส่งผลกระทบต่อหน้าที่ในการประเมินชั่งน้ำหนักคาดการณ์ผลกระทบต่อพลเรือนเป็นอย่างมาก เนื่องจาก ฝ่ายในการสู้รบไม่อาจคาดการณ์ได้ว่าผลกระทบที่เกิดขึ้นจากการโจมตีทางไซเบอร์นั้นจะปรากฏขึ้นเมื่อใด ยกตัวอย่าง รูปแบบการโจมตีทางไซเบอร์โดยใช้สตักซ์เน็ต เมื่อสตักซ์เน็ตเข้าสู่ระบบของฝ่ายตรงข้ามแล้ว ผู้โจมตีไม่สามารถคาดการณ์ได้ว่าหลังจากที่สตักซ์เน็ตเข้าสู่ระบบแล้วจะใช้ระยะเวลานานเท่าใดกว่าที่สตักซ์เน็ตจะค้นพบระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ที่เป็นเป้าหมาย และเมื่อสตักซ์เน็ตพบระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) แล้วจะต้องใช้ระยะเวลาในการสร้างความเสียหายอีกนานเท่าใด

นอกจากนี้ ระดับของผลกระทบที่เกิดขึ้นจากการโจมตีทางไซเบอร์ยังส่งผลต่อหน้าที่ในการประเมินชั่งน้ำหนักของฝ่ายในการสู้รบ เนื่องจากการเชื่อมต่อของเทคโนโลยีที่ใช้ทางการทหารและพลเรือน โดยไม่มีเส้นแบ่งแยกที่ชัดเจนในห้วงไซเบอร์ทำให้ฝ่ายในการสู้รบไม่อาจคาดการณ์ได้ว่า

---

[286] Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks," Texas Law Review 88(2010). P. 1545.

[287] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 98.

ขอบเขตของผลกระทบที่พลเรือนจะได้รับจากการโจมตีทางไซเบอร์จะเกิดขึ้นมากหรือน้อยเพียงใด และระดับของผลกระทบต่อพลเรือนที่จะต้องพิจารณานั้นจะต้องพิจารณาผลกระทบในขั้นใด โดยการโจมตีทางไซเบอร์ก่อให้เกิดผลกระทบแบบ Knock-on (Knock-on Effects) หรือผลกระทบต่อเนื่องกันไปเป็นระลอกๆ อาจพิจารณาได้ดังนี้

ผลกระทบขั้นที่ 1 ที่เกิดขึ้น ได้แก่ ระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์เป้าหมายนั้นถูกรบกวน ลดค่า เปลี่ยนแปลงหรือถูกทำลาย ทำให้ระบบหรือเครือข่ายนั้นไม่สามารถใช้งานได้

ผลกระทบขั้นที่ 2 ที่อาจเกิดขึ้น หากว่าระบบหรือเครือข่ายเป้าหมายนั้น เป็นระบบที่ใช้ในโครงสร้างพื้นฐานที่สำคัญของพลเรือนด้วย (Critical Infrastructures) เมื่อระบบหรือเครือข่ายที่ใช้ในการควบคุมโครงสร้างพื้นฐานเหล่านั้นถูกทำลาย ย่อมก่อให้เกิดผลกระทบต่อการทำงานของโครงสร้างพื้นฐานสำคัญเหล่านั้น อาทิ ระบบการสื่อสารโทรคมนาคม ระบบไฟฟ้า ระบบชลประทาน ระบบหมายเลขฉุกเฉิน (911) เป็นต้น ดังนั้น ผลกระทบขั้นที่ 2 จากการโจมตีทางไซเบอร์ดังกล่าว ได้แก่ การที่พลเรือนไม่สามารถใช้งานระบบโครงสร้างพื้นฐานเหล่านั้นได้

ผลกระทบขั้นที่ 3 สืบเนื่องมาจากการเกิดผลกระทบขั้นที่ 2 เมื่อพลเรือนไม่สามารถใช้งานดังกล่าวได้ อาจทำให้เกิดการบาดเจ็บหรือสูญเสียชีวิตของพลเรือน หรือความเสียหายของทรัพย์สินของพลเรือนได้ เช่น พลเรือนไม่สามารถใช้งานระบบหมายเลขฉุกเฉินเพื่อขอความช่วยเหลือจากโรงพยาบาลได้ทันเวลา ทำให้พลเรือนเสียชีวิต หรือการโจมตีต่อระบบควบคุมการจราจร ทำให้การจราจรติดขัดหรืออุบัติเหตุบนท้องถนน

ผลกระทบขั้นที่ 4 พิจารณาไปไกลถึงผลกระทบทางเศรษฐกิจ การเงินการธนาคารที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์นั้น เช่น เมื่อพลเรือนได้รับบาดเจ็บหรือเสียชีวิตหรือความเสียหายต่อทรัพย์สินของพลเรือนตามผลกระทบขั้นที่ 3 แล้ว ทำให้พลเรือนเกิดความกังวลไม่กล้าดำเนินชีวิตตามปกติ เกิดจลาจลภายในประเทศ ทำให้เศรษฐกิจของประเทศประสบปัญหา

นอกจากนี้ ผลกระทบแบบ Knock-on อาจพิจารณาในลักษณะที่ว่า เมื่อมีการโจมตีทางไซเบอร์ต่อเป้าหมายทางทหารทำให้ระบบหรือเครือข่ายทางการทหารเสียหาย อาจทำให้ระบบหรือเครือข่ายของพลเรือนได้รับความเสียหายหรือผลกระทบจากการโจมตีต่อระบบหรือเครือข่ายที่เป็นเป้าหมายทางทหารเนื่องมาจากความเชื่อมต่อของเทคโนโลยีที่ไม่มีเส้นแบ่งที่ชัดเจนในห้วงไซเบอร์

ยกตัวอย่าง การโจมตีทางไซเบอร์ต่อระบบควบคุมการผลิตกระแสไฟฟ้าของทางการทหารทำให้ไม่สามารถผลิตกระแสไฟฟ้าใช้ภายในกองทัพได้ อาจส่งผลต่อการผลิตน้ำดื่มอุปโภคบริโภคของประชาชน เนื่องจากขาดกระแสไฟฟ้าที่ใช้ในการผลิตน้ำดื่มของพลเรือน เป็นต้น

จากลักษณะพิเศษของการโจมตีทางไซเบอร์ข้างต้น ไม่ว่าจะเป็นระยะเวลาในการปรากฏผลกระทบต่อพลเรือนหรือผลกระทบแบบ Knock-on ตามที่ได้อธิบายข้างต้นนี้ก่อให้เกิดข้อท้าทายในการบังคับใช้หลักความได้สัดส่วนในการโจมตีกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอย่างมีนัยสำคัญ ซึ่งผู้เขียนจะได้ทำการศึกษาข้อท้าทายดังกล่าวในบทถัดไป

3.2.2.5 หลักการใช้ความระมัดระวังในการโจมตี

หลักการใช้ความระมัดระวัง หรือ Precautionary Measures นี้มีลักษณะเป็นกฎหมายจารีตประเพณีระหว่างประเทศ[288] ซึ่งศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวีย (ICTY) ได้ยอมรับลักษณะจารีตประเพณีของหลักการใช้ความระมัดระวังไว้ในคดี Kupreskic และ Tadic[289] โดยในคดี Tadic ระบุว่า การใช้ความระมัดระวังเท่าที่จำเป็นเพื่อหลีกเลี่ยงความสูญเสีย การบาดเจ็บหรือการทำลายที่อาจเกิดขึ้นต่อประชากรพลเรือนมีลักษณะเป็นกฎหมายจารีตประเพณีระหว่างประเทศในการขัดกันทางอาวุธทุกประเภท[290]

---

[288] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005)

Chapter 5: Precautions in Attack and Chapter 6: Precautions Against the Effects of Attacks.

[289] *The Prosecutor V. Kupreškić, Case No. It-95-16-T, Icty*, 14 January 2000. Para. 524. *The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* Paras. 111-112.

[290] *The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* Paras. 111-112.

หลักการใช้ความระมัดระวังในการโจมตีได้รับการยืนยันตามข้อ 57 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[291] กำหนดให้ฝ่ายในการสู้รบต้องดำเนินการโดยใช้ความระมัดระวังล่วงหน้าในการโจมตี ได้แก่

---

[291] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 57 — Precautions in attack

"1. In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.

2. With respect to attacks, the following precautions shall be taken:

a) those who plan or decide upon an attack shall:

i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;

ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;

iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;

b) an attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;

c) effective advance warning shall be given of attacks which may affect the civilian population, unless circumstances do not permit.

3. When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.

4. In the conduct of military operations at sea or in the air, each Party to the conflict shall, in conformity with its rights and duties under the rules of international law applicable in armed conflict, take all reasonable precautions to avoid losses of civilian lives and damage to civilian objects.

- ในการดำเนินปฏิบัติการทางทหาร จะต้องใช้ความระมัดระวังตลอดเวลา เพื่อมิให้ประชากรพลเรือนและทรัพย์สินของพลเรือนต้องถูกกระทบกระเทือน (ข้อ 57 (1))

- ผู้วางแผนหรือผู้ตัดสินใจในการโจมตีจะต้องกระทำทุกวิถีทางเท่าที่จะเป็นไปได้เพื่อตรวจสอบว่าเป้าหมายในการโจมตี คือ เป้าหมายทางทหาร (ข้อ 57 (2) (เอ) (i))

- ผู้วางแผนหรือผู้ตัดสินใจจะต้องดำเนินการทั้งปวงเพื่อการระมัดระวังล่วงหน้าที่เป็นไปได้ ในการเลือกวิธีการและปัจจัยในการสู้รบ โดยมีวัตถุประสงค์เพื่อการหลีกเลี่ยงและอย่างน้อยเพื่อลดการสูญเสียชีวิตของพลเรือนที่อาจเกิดขึ้น การบาดเจ็บของพลเรือนและความเสียหายต่อทรัพย์สินของพลเรือน (ข้อ 57 (2) (เอ) (ii))

- ผู้วางแผนหรือผู้ตัดสินใจจะต้องละเว้นจากการตัดสินใจที่จะโจมตีซึ่งอาจคาดหมายได้ว่าจะก่อให้เกิดผลกระทบต่อพลเรือนที่มากเกินกว่าความได้เปรียบทางการทหารที่จะได้รับ (ข้อ 57 (2) (เอ) (iii))

- การโจมตีจะต้องระงับหรือเลื่อนเวลาออกไป หากปรากฏว่าเป้าหมายในการโจมตีจะก่อให้เกิดผลกระทบต่อพลเรือนที่มากเกินควรกับความได้เปรียบทางทหาร (ข้อ 57 (2) (บี))

- ผู้วางแผนหรือผู้ตัดสินใจจะต้องจัดให้มีการเตือนล่วงหน้าก่อนการโจมตีที่อาจส่งผลกระทบต่อประชากรพลเรือน เว้นแต่ว่าสภาวการณ์ไม่อนุญาตให้กระทำได้ (ข้อ 57 (2) (ซี))

หน้าที่ในการดำเนินการทุกวิถีทางในการใช้ความระมัดระวังล่วงหน้าเท่าที่กระทำได้ (All “Feasible Precautions”) ได้ตีความในการจำกัดการใช้ความระมัดระวังล่วงหน้าจากนานารัฐตามคู่มือทางทหารของรัฐ[292] และปรากฏความหมายในข้อ 3 (4) ของพิธีสารว่าด้วยการห้ามหรือจำกัดการใช้ทุ่นระเบิด กับดัก และอาวุธอื่น ๆ (พิธีสารฉบับที่ 2) แนบท้ายอนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิดที่ก่อให้เกิดการบาดเจ็บร้ายแรงเกินความจำเป็นหรือก่อให้เกิดผลโดยไม่จำกัด

---

5. No provision of this Article may be construed as authorizing any attacks against the civilian population, civilians or civilian objects.”

[292] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005) P. 54.

เป้าหมาย ปี ค.ศ. 1980[293] ว่า “การใช้ความระมัดระวังล่วงหน้าเท่าที่กระทำได้ คือการใช้ความระมัดระวังล่วงหน้าซึ่งสามารถปฏิบัติได้จริงหรือเป็นไปได้ในทางปฏิบัติ โดยคำนึงถึงทุกสถานการณ์ ณ เวลานั้น รวมทั้งการพิจารณาด้านมนุษยธรรมและการทหาร”

เมื่อพิจารณาการบังคับใช้หลักการใช้ความระมัดระวังกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้น จะต้องพิจารณาว่าการโจมตีทางไซเบอร์นั้นมีลักษณะเป็น “การโจมตี” (Attacks) ตามกฎหมายมนุษยธรรมระหว่างประเทศที่ก่อให้เกิดความเสียหายทางกายภาพต่อทรัพย์สินของพลเรือน และการบาดเจ็บหรือเสียชีวิตของพลเรือนหรือไม่ เนื่องจากหลักการให้ความระมัดระวังกำหนดหน้าที่ในการใช้ความระมัดระวังเกี่ยวกับ “การโจมตี” จึงต้องพิจารณาก่อนว่าการโจมตีทางไซเบอร์นั้นเป็น “การโจมตี” ภายใต้กรอบกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ จากนั้นจึงพิจารณาหลักการตามข้อ 57 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1

จากการศึกษาหลักการใช้ความระมัดระวังในการโจมตีข้างต้น พบว่ามีประเด็นที่น่าสนใจเกี่ยวกับการบังคับใช้หลักการใช้ความระมัดระวังในการโจมตีกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ดังนี้

(ก) การระบุเป้าหมาย (Verification of Military objectives)

จากการศึกษาตามข้อ 57 (2) (เอ) (i) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 กฎหมายมนุษยธรรมระหว่างประเทศกำหนดหน้าที่ให้กระทำทุกวิถีทางเท่าที่กระทำได้เพื่อระบุว่าเป้าหมายในการโจมตีจะต้องไม่ใช่พลเรือนหรือทรัพย์สินของพลเรือนซึ่งได้รับความคุ้มครองตาม

---

[293] "Protocol on Prohibitions or Restrictions on the Use of Mines, Booby Traps and Other Devices (Protocol Ii) Annexed to the 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) ".

Article 3 (4)

“..., Feasible precautions are those precautions which are practicable or practically possible taking into account all circumstances ruling at the time, including humanitarian and military considerations.”

กฎหมายและไม่อาจตกเป็นเป้าหมายในการโจมตี โดยเป้าหมายในการโจมตีจะต้องเป็นเป้าหมายทางทหาร (Military Objectives) เท่านั้น อาศัยพิจารณาจากข้อมูลที่มีอยู่ทั้งหมดจากทุกแหล่งที่มาที่มีอยู่ในขณะนั้นเช่นเดียวกับการพิจารณาระบุเป้าหมายในการโจมตีด้วยอาวุธตามแบบ จะเห็นได้ว่า หน้าที่ดังกล่าวนี้เป็นหน้าที่ซึ่งเกี่ยวข้องกับหลักการแยกแยะเป้าหมายโดยผู้บัญชาการในฐานะที่เป็นผู้พิจารณาการโจมตีทางไซเบอร์ จะต้องมีแผนที่เครือข่ายที่เพียงพอต่อการตรวจสอบผลกระทบของการโจมตี โดยเฉพาะผลกระทบที่อาจเกิดขึ้นต่อพลเรือนและทรัพย์สินของพลเรือนเช่นนี้ถือเป็นการใช้ความระมัดระวังล่วงหน้าเท่าที่กระทำได้แล้ว[294] ซึ่งผู้บัญชาการจะต้องตัดสินใจบนพื้นฐานของข้อมูลจากทุกแหล่งข้อมูลที่มีอยู่ในเวลานั้น[295] เพื่อให้สามารถระบุได้ว่าเป้าหมายที่จะโจมตีเป็นเป้าหมายทางทหารหรือไม่ หากเป้าหมายในการโจมตีไม่ใช่เป้าหมายทางทหารแล้ว ย่อมไม่สามารถทำการโจมตีทางไซเบอร์ต่อเป้าหมายนั้นได้

ตัวอย่างเช่น ในขั้นตอนการตระเตรียมการโจมตีทางไซเบอร์ หากผู้บัญชาการไม่สามารถตรวจสอบขอบเขตของผลกระทบที่อาจเกิดขึ้นจากการโจมตีได้ ย่อมไม่สามารถทำการโจมตีทางไซเบอร์นั้นได้ มิฉะนั้น การโจมตีดังกล่าวอาจพิจารณาว่าเป็นการโจมตีโดยไม่เลือกเป้าหมายได้ หรือถ้าผู้บัญชาการได้ใช้เทคโนโลยีที่ดีที่สุดในการกำหนดแผนที่เครือข่ายและมีการควบคุมอย่างต่อเนื่องในขั้นตอนตระเตรียมการโจมตี ย่อมไม่เป็นการฝ่าฝืนต่อหลักการใช้ความระมัดระวัง แม้ว่าในระหว่างที่ทำการโจมตี จะมีมัลแวร์แพร่กระจายโดยไม่ได้คาดคิดไปยังเครือข่ายของพลเรือน ซึ่งผู้บัญชาการไม่ได้ทราบมาก่อนว่าเครือข่ายของพลเรือนนั้นสามารถเชื่อมต่อกับระบบของทางการทหารได้ เช่นเดียวกัน หากผู้โจมตีไม่สามารถรวบรวมข้อมูลได้เพียงพอเกี่ยวกับการระบุเป้าหมายที่จะโจมตี ก็ควรที่จะจำกัดการโจมตีเฉพาะส่วนที่มีการรวบรวมข้อมูลที่เพียงพอต่อการระบุว่าเป็นเป้าหมายทางทหารเท่านั้น จึงจะเป็นการปฏิบัติตามหลักการใช้ความระมัดระวัง[296]

---

[294] Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack," *International Law Studies* 89, no. 198 (2013). P. 210.

[295] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005) P. 54.

[296] Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack," International Law Studies 89, no. 198 (2013). P. 210.

(ข) การเลือกวิธีการและปัจจัยในการโจมตี

จากการศึกษาตามข้อ 57 (2) (เอ) (ii) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ผู้วางแผน ผู้ตัดสินใจหรือผู้บังคับบัญชาจะต้องดำเนินการทั้งปวงเพื่อการระมัดระวังล่วงหน้าที่เป็นไปได้ ในการเลือกวิธีการและปัจจัยในการโจมตี เพื่อหลีกเลี่ยงและอย่างน้อยที่สุดเพื่อลดการสูญเสียชีวิต การบาดเจ็บของพลเรือน และความเสียหายต่อทรัพย์สินของพลเรือน

ดังนั้น ในการเลือกวิธีการหรือปัจจัยในการโจมตีทางไซเบอร์ ผู้วางแผนหรือผู้ตัดสินใจที่จะโจมตีพึงต้องดำเนินการทั้งปวงเพื่อการระมัดระวังล่วงหน้าเท่าที่เป็นไปได้ เพื่อหลีกเลี่ยงหรือลดความสูญเสียชีวิต การบาดเจ็บของพลเรือน และความเสียหายต่อทรัพย์สินของพลเรือน แม้ว่าด้วยเทคโนโลยีสารสนเทศและคอมพิวเตอร์ในปัจจุบัน การโจมตีทางไซเบอร์มีโอกาสก่อให้เกิดการสูญเสียชีวิต การบาดเจ็บของพลเรือนได้น้อยมาก เนื่องจากเป้าหมายของการโจมตีทางไซเบอร์เป็นระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์ ไม่ใช่พลรบหรือบุคคล อย่างไรก็ตาม ผู้วางแผนหรือผู้ตัดสินใจที่จะโจมตีทางไซเบอร์อาจติดตั้งระบบความปลอดภัยเพื่อใช้ทำลาย หากวิธีการหรือปัจจัยในการโจมตีทางไซเบอร์นั้นหลุดพ้นจากการควบคุมไป เพื่อแสดงความสุจริตใจในการหลีกเลี่ยงหรือการลดความเสียหายที่อาจเกิดขึ้นต่อพลเรือนและทรัพย์สินของพลเรือนตามหลักการใช้ความระมัดระวังในการโจมตี

จากการศึกษาหลักการใช้ความระมัดระวังในการโจมตีกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ จะเห็นได้ว่า วางแผนหรือผู้ตัดสินใจที่จะโจมตีของฝ่ายในการสู้รบมีหน้าที่ก่อนดำเนินการโจมตีทางไซเบอร์ที่จะต้องพิจารณาถึงความเสียชีวิต การบาดเจ็บของบุคคลหรือการทำลาย ความเสียหายต่อทรัพย์สินของพลเรือนอันเป็นผลกระทบต่อพลเรือนประกอบในการวางแผนหรือการตัดสินใจดำเนินการโจมตีทางไซเบอร์ โดยอาศัยการพิจารณาจากข้อมูลทั้งหมดซึ่งทำการรวบรวมมาทุกวิถีทาง

3.2.3 หลักการทั่วไปเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบ

หลักการพื้นฐานที่สำคัญของกฎหมายมนุษยธรรมระหว่างประเทศเกี่ยวกับปฏิบัติการทางทหารในการสู้รบ นอกเหนือจากหลักการเกี่ยวกับการเข้าร่วมในสถานการณ์การขัดกันทางอาวุธและการปฏิบัติต่อเป้าหมายทางทหารตามที่ได้ศึกษาก่อนหน้านี้แล้ว หลักการเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบถือเป็นหลักการสำคัญที่ฝ่ายในการสู้รบพึงปฏิบัติตามให้สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศ

ในการศึกษาหลักการเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเล่มนี้ จะทำการศึกษาเฉพาะหลักการทั่วไปตามกฎหมายจารีตประเพณีระหว่างประเทศเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบประกอบด้วยหลักการห้ามใช้วิธีการและปัจจัยในการสู้รบซึ่งก่อให้เกิดการบาดเจ็บเกินขนาดหรือการเจ็บปวดโดยไม่จำเป็นและหลักการห้ามใช้อาวุธซึ่งไม่อาจแยกแยะเป้าหมายได้[297] มีรายละเอียดดังต่อไปนี้

3.2.3.1 หลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้

หลักการห้ามใช้อาวุธซึ่งไม่อาจแยกแยะเป้าหมายได้ (Indiscriminate Weapons) เป็นหลักการสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ ยืนยันหลักการตามความเห็นของศาลยุติธรรมระหว่างประเทศในความเห็นเชิงปรึกษาคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้และการใช้อาวุธนิวเคลียร์ ค.ศ. 1996 ระบุว่า รัฐทั้งหลายจะต้องไม่ใช้อาวุธที่ไม่สามารถแยกแยะระหว่างพลเรือนและเป้าหมายทางทหารได้[298]

---

[297] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005)

Part IV: Weapons, Chapter 20. General principles on the use of weapons, "Rule 70. The use of means and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering is prohibited.

Rule 71. The use of weapons which are by nature indiscriminate is prohibited."

[298] *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*. Para. 78.

หลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้ปรากฏตามข้อ 51 (4) (บี) (ซี) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[299] สรุปได้ว่า การโจมตีโดยไม่เลือกเป้าหมายเป็นสิ่งต้องห้าม ได้แก่ การโจมตีโดยใช้วิธีการหรือปัจจัยในการสู้รบซึ่งไม่สามารถเล็งไปที่เป้าหมายทางทหารโดยเฉพาะได้ หรือการโจมตีโดยใช้วิธีการหรือปัจจัยในการสู้รบซึ่งก่อให้เกิดผลอันไม่อาจจำกัดได้ตามที่กำหนดไว้ในพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ซึ่งก่อให้เกิดผลซึ่งมีลักษณะเป็นการโจมตีเป้าหมายทหารและพลเรือนหรือทรัพย์สินของพลเรือนโดยไม่อาจแยกแยะได้

การพิจารณาหลักการห้ามใช้อาวุธที่ไม่สามารถแยกแยะเป้าหมายได้ (Indiscriminate Weapons) ตามข้อ 51 (4) (บี) (ซี) พิจารณาเฉพาะการใช้อาวุธหรือปัจจัยในการสู้รบที่ลักษณะโดยธรรมชาติของอาวุธนั้นไม่สามารถแยกแยะระหว่างเป้าหมายทางทหารกับทรัพย์สินของพลเรือนได้ ในขณะที่การพิจารณาวิธีการในการสู้รบซึ่งไม่สามารถแยกแยะเป้าหมายได้ตามข้อ 51 (4) ตามพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 เกี่ยวกับข้อห้ามโจมตีโดยไม่เลือกเป้าหมาย (Indisciminate of Attack) ซึ่งจะได้ทำการศึกษาในส่วนต่อไป

นอกจากนี้ ข้อ 51 (4) (บี) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 กำหนดห้ามการโจมตีโดยใช้วิธีการหรือปัจจัยในการสู้รบซึ่งไม่สามารถเล็งไปที่เป้าหมายทหารโดยเฉพาะได้

---

[299] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 51

Indiscriminate attacks are prohibited. Indiscriminate attacks are:

(a) ...

(b) those which employ a method or means of combat which cannot be directed at a specific military objective; or

(c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."

เช่น การโจมตีด้วยขีปนาวุธพิสัยไกล (Long-Range Missile) ด้วยระบบนำวิถีที่ไม่สามารถเล็งเป้าหมายได้อย่างแม่นยำ[300]

ในทางทฤษฎี อาวุธไซเบอร์หรือปัจจัยในการสู้รบที่ใช้ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่สามารถแยกแยะระหว่างระบบหรือเครือข่ายทางทหารกับระบบหรือเครือข่ายของพลเรือนได้ ย่อมถือเป็น อาวุธที่ไม่สามารถแยกแยะเป้าหมายได้ในตัวเอง และหากการใช้อาวุธไซเบอร์ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้นสามารถสร้างความเสียหายที่พิจารณาได้ว่าเป็น “การโจมตี” ตามกฎหมายมนุษยธรรมระหว่างประเทศ อาวุธไซเบอร์ดังกล่าวย่อมต้องห้ามตามหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้นี้

เมื่อพิจารณาการนำเทคโนโลยีไซเบอร์มาใช้เป็นปัจจัยในการสู้รบ หรือ อาวุธไซเบอร์ที่เข้าข่ายต้องห้ามตามหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้ในตามข้อ 51 (4) (บี) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 คือ การใช้มัลแวร์ต่างๆ (Malicious Code) ไม่ว่าจะเป็น ไวรัส[301] หนอนคอมพิวเตอร์[302] โทรจัน[303] นอกจากจะสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์เป้าหมายแล้ว มัลแวร์เหล่านี้ยังทำให้ระบบหรือเว็บไซต์อื่นที่เป็นของพลเรือนติดเชื้อและ

---

[300] Jean DE PREUX Claude PILLOUDt, Yves SANDOZ, Bruno ZIMMERMANN, Philippe Eberlin, Hans-Peter Gasser and Claude F. Wenger "Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949," ed. ICRC(Netherlands Martinus Nijhoff Publishers 1987). Para. 1958.

[301] ไวรัสคอมพิวเตอร์ (Computer Virus) หรือไวรัส ซึ่งเรียกชื่อเลียนแบบ ไวรัส ที่เป็นสิ่งมีชีวิต เนื่องจากมีลักษณะเช่นเดียวกับไวรัสในทางชีววิทยาที่สามารถแพร่กระจายไปในเซลล์ของสิ่งมีชีวิตเช่นเดียวกับไวรัสคอมพิวเตอรร์ที่สามารถทำสำเนาตนเองแพร่กระจายไปยังโปรแกรมหรือข้อมูลอื่นๆ โดยไวรัสเป็นชุดคำสั่งระบบปฏิบัติการที่ถูกเขียนขึ้นมาตามวัตถุประสงค์ของผู้เขียนโปรแกรมไวรัสนั้นขึ้นมา และบุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้

[302] หนอนคอมพิวเตอร์ หรือ เวิร์ม (Worms) เป็นโปรแกรมคอมพิวเตอร์อิสระ มีลักษณะเด่นคือ เมื่อคอมพิวเตอร์ติดเชื้อหนอนคอมพิวเตอร์แล้ว หนอนคอมพิวเตอร์จะทำการสำเนาตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่นที่ต่ออยู่บนเครือข่ายเดียวกัน โดยหนอนคอมพิวเตอร์สามารถสร้างความเสียหายแก่คอมพิวเตอร์ได้ โดยการใช้ทรัพยากรของเครือข่ายนั้น ทำลายข้อมูล จนทำให้คอมพิวเตอร์ช้าลง ไม่สามารถทำงานได้เป็นปกติ หากการทำสำเนาตัวเองนั้นอยู่ในระดับสูงพอจะเป็นสาเหตุทำให้ระบบเครือข่ายล่มได้

[303] โทรจัน นำมาจาก ม้าโทรจัน (Trojan horse) เป็นเครื่องมือทำลายล้างซึ่งทำงานภายใต้ลักษณะภายนอกที่ดูเป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็นโปรแกรมธรรมดาทั่วๆ ไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียกขึ้นมาทำงาน แต่เมื่อถูกใช้งานแล้ว โทรจันจะเริ่มทำลายข้อมูลหรือระบบตามที่เขียนขึ้นมา โทรจันสามารถเป็นโปรแกรมการควบคุมระยะไกล (Remote Control Program) ในการเข้าถึงเครื่องคอมพิวเตอร์ของเหยื่อและสามารถติดตั้งบนเครื่องคอมพิวเตอร์ที่เป็นพาหะ รวมถึงสามารถทำผ่านทางสิ่งที่แนบมากับอีเมลเพื่อให้ผู้ใช้งานเปิดขึ้นมา เมื่อผู้ใช้เปิดสิ่งที่แนบมากับอีเมลหรือโปรแกรมแล้ว จะติดเชื้อในทันที เมื่อโทรจันได้เริ่มติดตั้งและทำงานบนเครือข่ายแล้ว จะทำให้ผู้ที่ไม่ประสงค์ดีควบคุมเครื่องคอมพิวเตอร์ที่ติดเชื้อ (Zombies) นั้นได้

ถูกทำลายได้ด้วย กล่าวคือ โดยลักษณะในตัวเองของมัลแวร์จะแพร่กระจายไปในระบบหรือเครือข่ายที่เข้าไปอย่างไม่สามารถควบคุมทิศทางได้ ดังนั้น การใช้มัลแวร์ข้างต้นเป็นปัจจัยในการสู้รบในการโจมตีทางไซเบอร์ต่อระบบหรือเครือข่ายเป้าหมายทางทหาร เพื่อสร้างความเสียหายย่อมขัดต่อหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้นี้

อย่างไรก็ตาม อาวุธไซเบอร์บางอย่างเมื่อนำมาใช้เป็นปัจจัยในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธสามารถโจมตีต่อเป้าหมายอย่างเฉพาะเจาะจงได้ เช่น สตักซ์เน็ต (Stuxnet) ที่พัฒนาและออกแบบมาให้โจมตีเฉพาะต่อระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) เท่านั้นและสามารถสร้างความเสียหายให้แก่เครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์ที่ระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ควบคุมอยู่เป็นการเฉพาะ โดยสตักซ์เน็ตจะไม่ทำงานเพื่อสร้างความเสียหายให้แก่ระบบของพลเรือนอื่นแม้ว่าจะแพร่กระจายเข้าสู่ระบบพลเรือนด้วยก็ตาม[304] กล่าวได้ว่า สตักซ์เน็ตเป็นอาวุธไซเบอร์หรือปัจจัยในการสู้รบที่โดยลักษณะในตัวเองสามารถแยกแยะระหว่างระบบที่เป็นเป้าหมายทางทหารและระบบของพลเรือนได้อย่างเฉพาะเจาะจง การใช้สตักซ์เน็ตเป็นปัจจัยในการสู้รบจึงไม่ต้องห้ามตามหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายนี้

ข้อ 51 (4) (ซี) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 กำหนดห้ามการใช้วิธีการและปัจจัยในการสู้รบซึ่งก่อให้เกิดผลอันไม่อาจจำกัดขอบเขตได้ตามที่กำหนดไว้ในพิธีสารฉบับเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 และเป็นผลให้ให้การโจมตีนั้นมีลักษณะเป็นการทำลายเป้าหมายทางทหาร และพลเรือนหรือทรัพย์สินของพลเรือนโดยปราศจากการแยกแยะ ยกตัวอย่างการใช้ทุ่นระเบิดสังหารบุคคลเป็นอาวุธในการสู้รบซึ่งโดยลักษณะแล้วเป็นการยากมากที่จะสามารถโจมตีเฉพาะต่อเป้าหมายทางทหาร พลเรือนหรือทรัพย์สินของพลเรือนอาจได้รับความเสียหายจากทุ่นระเบิดสังหารบุคคลได้ตลอดเวลาทั้งในสถานการณ์การขัดกันทางอาวุธและภายหลังจากที่สถานการณ์การขัดกันทางอาวุธสิ้นสุดลงแล้วก็ตาม

ในทำนองเดียวกัน การพิจารณาอาวุธไซเบอร์ที่ในตัวเองไม่สามารถเพ่งเล็งต่อเป้าหมายทางทหารในลักษณะเฉพาะได้ตาม ข้อ 51 (4) (ซี) การใช้มัลแวร์ส่วนใหญ่ไม่ว่าจะเป็น ไวรัส หนอนคอมพิวเตอร์ โทรจัน เป็นปัจจัยในการโจมตีทางไซเบอร์โดยตัวมันเองไม่สามารถจำกัดขอบเขต

---

[304] Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts ed. Michael N. Schmitt(Cambridge University Press, 2013). P. 146.

ของผลกระทบในการโจมตีได้ การทำงานของมัลแวร์เหล่านี้เป็นไปอย่างไร้ทิศทาง แพร่กระจายโดยไม่สามารถควบคุมได้ ในขณะที่อาวุธไซเบอร์เช่น สตักซ์เน็ต เป็นมัลแวร์ที่พัฒนาและออกแบบมาให้มีความสามารถในการควบคุมผลกระทบ โดยสตักซ์เน็ตจะไม่ทำงานจนกว่าจะเจอระบบเป้าหมายที่ถูกต้องตามที่ออกแบบมา ผ่านการตั้งเงื่อนไขในการทำงานของสตักซ์เน็ตให้โจมตีเฉพาะต่อระบบระบบเป้าหมายทางทหารเท่านั้น[305]

จากการศึกษาจะเห็นได้ว่า อาวุธไซเบอร์หรือปัจจัยในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธมีทั้งที่สามารถโจมตีต่อเป้าหมายทางทหารได้อย่างเฉพาะเจาะจง เช่น สตักซ์เน็ต และที่ไม่สามารถโจมตีต่อเป้าหมายทางทหารเป็นการเฉพาะได้ เช่น ไวรัส โทรจัน หนอนคอมพิวเตอร์ เมื่อพิจารณาการใช้อาวุธไซเบอร์หรือปัจจัยในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธกับหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายข้างต้นจึงมีทั้งที่เป็นไปตามหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้และที่ขัดต่อหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมาย ฝ่ายในการสู้รบมีหน้าที่ในการพิจารณาว่าอาวุธไซเบอร์หรือปัจจัยในการโจมตีทางไซเบอร์ที่จะใช้ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธสามารถโจมตีต่อเป้าหมายทางทหารได้อย่างเฉพาะเจาะจง โดยอาศัยความรู้ทางด้านเทคโนโลยีประกอบในการพิจารณา เพื่อให้แน่ใจได้ว่าอาวุธไซเบอร์ที่เบือกใช้ไม่ขัดกับหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายตามกฎหมายมนุษยธรรมระหว่างประเทศ

3.2.3.2 การโจมตีทางไซเบอร์กับวิธีการและปัจจัยในการสู้รบ

กฎหมายมนุษยธรรมระหว่างประเทศจำกัดวิธีการและปัจจัยในการสู้รบ โดยฝ่ายในการสู้รบไม่สามารถใช้วิธีการและปัจจัยในการสู้รบได้อย่างไม่มีข้อจำกัดใดๆ ข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบตามกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการใช้ปัจจัยหรืออาวุธทุกประเภทและการใช้วิธีการในการสู้รบทุกรูปแบบ ในการศึกษาการบังคับใช้หลักการเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบจึงควรทำความเข้าใจเกี่ยวกับความหมายของวิธีการในการสู้รบ (Methods of Warfare) และปัจจัยในการสู้รบ (Means of Warfare) ตามกฎหมายมนุษยธรรม

---

[305] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012). P. 257.

ระหว่างประเทศว่ามีความหมายอย่างไร การโจมตีทางไซเบอร์สามารถพิจารณาว่าเป็นวิธีการและปัจจัยในการสู้รบได้หรือไม่ อย่างไร ดังต่อไปนี้

หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบปรากฏชัดเจนตามข้อ 22 ของอนุสัญญาเฮกฉบับที่ 4 ว่าด้วยกฎหมายและจารีตประเพณีในการทำสงครามภาคพื้นดิน ค.ศ. 1907 ระบุว่า “สิทธิของคู่พิพาทในการนำปัจจัยในการโจมตีฝ่ายตรงข้ามมิได้มีอย่างไม่จำกัด”[306]

แนวคิดเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบได้รับการยอมรับและยืนยันหลักการไว้ในข้อ 35 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1 ค.ศ. 1977 กำหนดว่า “สิทธิของฝ่ายในการสู้รบในการเลือกวิธีการหรือปัจจัยในการสู้รบไม่อาจกระทำได้โดยปราศจากข้อจำกัด”[307] เมื่อพิจารณาการบังคับใช้หลักการทั่วไปตามข้อ 22 ของอนุสัญญาเฮกฉบับที่ 4 ว่าด้วยกฎหมายและจารีตประเพณีในการทำสงครามภาคพื้นดิน ค.ศ. 1907 และข้อ 35 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1 ค.ศ. 1977 กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ หมายความว่า ผู้ที่มีหน้าที่รับผิดชอบในการดำเนินปฏิบัติการทางไซเบอร์ใดๆ ในระหว่างสถานการณ์การขัดกันทางอาวุธมีหน้าที่อย่างชัดเจนตามกฎหมายที่จะต้องเคารพกฎเกณฑ์ตามกฎหมายระหว่างประเทศที่ใช้บังคับในกรณีที่มีการขัดกันทางอาวุธ[308] ซึ่งหลักการนี้ต้องการแสดงให้

---

[306] "The Hague Convention (Iv) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land. (18 October 1907)."

Article 22.

“The right of belligerents to adopt means of injuring the enemy is not unlimited.”

[307] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 35 - Basic rules

“1. In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.”

[308] William H. Boothby, "Methods and Means of Cyber Warfare," *International Law Studies* 89(2013). P. 391.

เห็นถึงการกระทำที่สมดุลกันระหว่างหลักการความจำเป็นทางทหาร (Military Necessity) กับการพิจารณาทางด้านมนุษยธรรมในปฏิบัติการทางทหาร[309]

ในทำนองเดียวกัน ศาลยุติธรรมระหว่างประเทศได้ให้ข้อสังเกตเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบไว้ในความเห็นเชิงปรึกษาคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์ ค.ศ. 1996 กล่าวว่า “ลักษณะมนุษยธรรมของหลักการและกฎเกณฑ์ตามกฎหมายมนุษยธรรมซึ่งบังคับใช้ในการขัดกันทางอาวุธแทรกซึมอยู่ในกฎหมายการขัดกันทางอาวุธและบังคับใช้กับรูปแบบการสู้รบทั้งหมดและอาวุธทั้งหมด ทั้งในอดีต ปัจจุบัน และอนาคต”[310]

ดังนั้น แม้ว่าจะไม่มีข้อบทเกี่ยวกับอาวุธไซเบอร์ตามกฎหมายมนุษยธรรมระหว่างประเทศ แต่หลักการมนุษยธรรมเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบตามกฎหมายมนุษยธรรมระหว่างประเทศสามารถบังคับใช้กับการโจมตีทางไซเบอร์ซึ่งเป็นการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือที่เรียกว่า ไซเบอร์ มาใช้เป็นวิธีการหรือปัจจัยในการสู้รบ โดยมีการออกแบบ วัตถุประสงค์ หรือการใช้เพื่อก่อให้เกิดผลกระทบอย่างรุนแรง (Violent Consequences) ไม่ว่าจะเป็นการบาดเจ็บหรือเสียชีวิตของบุคคล หรือความเสียหาย การทำลายซึ่งทรัพย์สินเพื่อให้ความคุ้มครองตามกฎหมายด้านมนุษยธรรมได้

ในขณะที่ การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยลักษณะของตัวมันเองไม่มีลักษณะทางกายภาพ เกิดขึ้นในห้วงไซเบอร์ซึ่งไม่มีลักษณะทางกายภาพเช่นกัน ความเหมือนของการโจมตีด้วยอาวุธตามแบบและการโจมตีทางไซเบอร์คือ เมื่อใช้ในการสู้รบสามารถก่อให้เกิดผลกระทบอย่างรุนแรง (Violent Consequences) สร้างความเสียหายต่อชีวิตและทรัพย์สินได้เช่นเดียวกัน การพิจารณาว่าการโจมตีทางไซเบอร์เป็นวิธีการในการสู้รบ (Methods of Warfare)

---

[309] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012). P. 251.

[310] *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*. Para. 86.

หรือปัจจัยในการสู้รบ (Means of Warfare) ตามกฎหมายมนุษยธรรมระหว่างประเทศพิจารณาได้ดังนี้

ปัจจัยในการสู้รบ (Means of Warfare) หมายถึง ประเภทของอาวุธที่ใช้ในการสู้รบ[311] หรืออาวุธที่ใช้โดยฝ่ายในการขัดกันทางอาวุธในปฏิบัติการทางทหาร[312] ปัจจัยในการสู้รบประกอบด้วยอาวุธทั้งหมด แท่นรองอาวุธ (Weapons Platforms) และอุปกรณ์เครื่องมือที่เกี่ยวข้องกับอาวุธซึ่งใช้เพื่อส่งกำลังระหว่างการสู้รบ[313]

ส่วนวิธีการในการสู้รบ (Methods of Warfare) หมายถึง วิธีการที่ใช้หรือปฏิบัติการทั่วไปในการเข้าร่วมในการขัดกันทางอาวุธ[314] หรือวิธีการใช้อาวุธของฝ่ายในการขัดกันทางอาวุธปฏิบัติการทางทหาร[315] โดยวิธีการในการสู้รบหมายถึงวิธีการในการใช้อาวุธในการสู้รบด้วย[316]

เมื่อพิจารณาบริบทของการโจมตีทางไซเบอร์ซึ่งเป็นการนำเทคโนโลยีทางไซเบอร์มาใช้ในการสู้รบเปรียบเทียบกับอาวุธตามแบบซึ่งเป็นที่เข้าใจกันว่าอาวุธตามแบบมีลักษณะหลากหลาย

---

[311] International Committee of the Red Cross, "Methods and Means of Warfare," ICRC, https://www.icrc.org/eng/war-and-law/conduct-hostilities/methods-means-warfare/overview-methods-and-means-of-warfare.htm. [February 2, 2016]

[312] Geneva Academy of International Humanitarian Law and Human Rights, "Glossary," in *Weapons Law Encyclopedia*(Geneva2014).

"The term means of warfare generally describes the weapons being used by parties to an armed conflict in the conduct of hostilities."

[313] William H. Boothby, "Methods and Means of Cyber Warfare," International Law Studies 89(2013). P. 387.

[314] International Committee of the Red Cross, "Methods and Means of Warfare," ICRC, https://www.icrc.org/eng/war-and-law/conduct-hostilities/methods-means-warfare/overview-methods-and-means-of-warfare.htm. [February 2, 2016]

[315] Geneva Academy of International Humanitarian Law and Human Rights, "Glossary," in Weapons Law Encyclopedia(Geneva2014).

"The term method of warfare generally describes the way in which weapons are used by parties to an armed conflict in the conduct of hostilities."

[316] William H. Boothby, "Methods and Means of Cyber Warfare," International Law Studies 89(2013). P. 389.

รูปแบบ เช่น ระเบิด จรวด กระสุนปืน กระสุนปืนใหญ่ก่อให้เกิดผลกระทบในการทำลายล้างโดยการใช้แรงทางกายภาพ (Kinetic Force) ในขณะที่อาวุธบางประเภท เช่น แก๊สพิษ อาวุธเคมี อาวุธชีวภาพ บรรลุผลในการก่อให้เกิดการบาดเจ็บหรือเสียชีวิตตามวัตถุประสงค์ได้โดยไม่จำเป็นต้องอาศัยแรงทางกายภาพในการดำเนินการ ดังนั้น เงื่อนไขที่สำคัญของอาวุธทุกประเภทคือ จะต้องเป็นผลให้เกิดอันตรายหรือก่อให้เกิดความเสียหายต่อบุคคลหรือทรัพย์สินของฝ่ายตรงข้ามในการสู้รบ[317] โดยไม่ต้องคำนึงว่าจะมีการใช้แรงทางกายภาพหรือไม่ก้ตาม

จากการศึกษาข้างต้นสรุปได้ว่า ในการพิจารณาว่าเทคโนโลยีไซเบอร์ใดมีลักษณะเป็นอาวุธไซเบอร์หรือไม่ จะต้องพิจารณาว่าความสามารถของเทคโนโลยีไซเบอร์ จากการออกแบบตั้งใจ หรือการใช้สามารถก่อให้เกิดผลกระทบอย่างรุนแรง (Violent Consequences) เป็นเหตุให้เกิดการบาดเจ็บหรือเสียชีวิตของบุคคล หรือสร้างความเสียหายหรือทำลายซึ่งทรัพย์สินได้หรือไม่

ยกตัวอย่าง การโจมตีทางไซเบอร์ต่อระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ที่ใช้ควบคุมสาธารณูปโภคสำคัญทางการทหาร เช่น โรงงานผลิตกระแสไฟฟ้า พลังงานเชื้อเพลิง จนเป็นเป็นเหตุให้เครื่องมือที่ใช้ในการผลิตกระแสไฟฟ้าหรือพลังงานเชื้อเพลิงนั้นเสียหาย เช่นเหตุการณ์การโจมตีด้วยสตักซ์เน็ตต่อโรงงานนิวเคลียร์ของอิหร่าน ทำให้เครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์ถูกทำลายกว่า 1,000 เครื่อง เห็นได้ชัดเจนว่าความเสียหายของกรณีดังกล่าวเกิดขึ้นจากการโจมตีทางไซเบอร์จึงสามารถพิจารณาได้ว่า สตักซ์เน็ตที่ใช้ในการโจมตีดังกล่าวเป็นอาวุธไซเบอร์ หรือปัจจัยในการโจมตีทางไซเบอร์ ในขณะที่ การทำให้ระบบหยุดทำงานลงเพียงชั่วคราวทำให้ได้รับความไม่สะดวก สร้างความรำคาญ โดยไม่ก่อให้เกิดการบาดเจ็บ เสียชีวิตของบุคคลหรือความเสียหายต่อทรัพย์สิน การใช้เทคโนโลยีไซเบอร์นั้น ย่อมไม่สามารถพิจารณาได้ว่าอาวุธไซเบอร์หรือปัจจัยที่ใช้ในการโจมตีทางไซเบอร์นั้นเป็นปัจจัยในการสู้รบ

คู่มือทาลลินน์ได้ให้ความหมายเกี่ยวกับวิธีการและปัจจัยในสงครามไซเบอร์ไว้ว่า ปัจจัยในสงครามไซเบอร์ หมายถึง อาวุธไซเบอร์ (Cyber Weapons) และระบบที่เกี่ยวข้อง[318] โดย

---

[317] Ibid.

[318] Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts ed. Michael N. Schmitt(Cambridge University Press, 2013).

Rule 41.

“(a) ‘means of cyber warfare’ are cyber weapons and their associated cyber systems; and

อธิบายว่า อาวุธไซเบอร์คือปัจจัยทางไซเบอร์ในการสู้รบที่โดยการออกแบบ การใช้ หรือวัตถุประสงค์ในการใช้สามารถทำให้เกิด (1) การบาดเจ็บ เสียชีวิตของบุคคล หรือ (2) สร้างความเสียหายหรือทำลายซึ่งทรัพย์สินตามเงื่อนไขของการโจมตีทางไซเบอร์ ปัจจัยในการโจมตีทางไซเบอร์จึงประกอบด้วยอาวุธไซเบอร์และระบบอาวุธไซเบอร์ ไม่ว่าจะเป็นอุปกรณ์ไซเบอร์ เครื่องมือ วัสดุอุปกรณ์ กลไกหรือซอฟต์แวร์ที่ใช้ ออกแบบหรือตั้งใจใช้ในการดำเนินการโจมตีทางไซเบอร์

ส่วนวิธีการในสงครามไซเบอร์ หมายถึง กลยุทธ์ทางไซเบอร์ เทคนิค และวิธีการในการดำเนินการสู้รบ[319] กล่าวคือ วิธีการในการดำเนินการทางไซเบอร์ ยกตัวอย่าง ปฏิบัติการทางไซเบอร์โดยใช้บอตเน็ต (Botnet) เพื่อให้เกิดการโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการ (Distributed Denial of Service หรือ DDOS) โดยบอตเน็ต (Botnet) ถือเป็นปัจจัยในการสู้รบทางไซเบอร์ ในขณะที่ การทำให้ระบบปฏิเสธการให้บริการ (Distributed Denial of Service: DDOS) คือวิธีการในการสู้รบทางไซเบอร์

จากการศึกษาข้างต้น สรุปได้ว่า การใช้เทคโนโลยีไซเบอร์ในการสู้รบอาจเป็นได้ทั้งวิธีการในการสู้รบหรือปัจจัยในการสู้รบ โดยการใช้เทคโนโลยีไซเบอร์ไม่ว่าจะใช้เป็นวิธีการหรือปัจจัยในการสู้รบนั้น จะต้องมีลักษณะการออกแบบ วัตถุประสงค์ หรือการใช้เพื่อก่อให้เกิดผลกระทบอย่างรุนแรง (Violent Consequences) ไม่ว่าจะเป็นการบาดเจ็บหรือเสียชีวิตของบุคคล หรือความเสียหาย การทำลายซึ่งทรัพย์สิน การนำเทคโนโลยีไซเบอร์มาใช้เป็นปัจจัยในการสู้รบ อาทิ คอมพิวเตอร์ทั้งฮาร์ดแวร์และซอฟต์แวร์ ระบบโปรแกรม ข้อมูลที่บรรจุในคอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ที่เกี่ยวข้องกับคอมพิวเตอร์และสารสนเทศ ตลอดจนมัลแวร์ต่างๆ[320] ในขณะที่ การนำเทคโนโลยีไซเบอร์มาใช้เป็นวิธีการในการสู้รบ คือ การนำปัจจัยในการสู้รบหรืออาวุธไซเบอร์ต่างๆ มาใช้ในการสู้รบเพื่อทำให้เกิดผลกระทบอย่างรุนแรง

(b) 'methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conducted."

[319] *Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts* P. 142.

[320]มัลแวร์ (Malware) ย่อมาจาก Malicious Software หมายถึง โปรแกรมคอมพิวเตอร์ใดๆ ที่เป็นอันตรายต่อคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ อาทิ ไวรัส (Virus) หนอนคอมพิวเตอร์ (Worm) โทรจัน (Trojan Horse) สตักซ์เน็ต (Stuxnet) สปายแวร์ (Spyware)

อย่างไรก็ตาม ส่วนใหญ่แล้ว อาวุธไซเบอร์ต่างๆ โดยลักษณะในตัวเองไม่สามารถก่อให้เกิดผลกระทบอย่างรุนแรง ไม่ว่าจะเป็นคอมพิวเตอร์ อุปกรณ์เครื่องมือสารสนเทศและคอมพิวเตอร์ อินเทอร์เน็ต แต่ก็มีบ้างที่สามารถก่อให้เกิดผลกระทบอย่างรุนแรง คือ สร้างความเสียหายทางกายภาพต่ออุปกรณ์ที่พึ่งพาระบบเป้าหมาย เช่น สตักซ์เน็ต ซึ่งถูกออกแบบมาให้ทำลายระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ส่งผลให้เครื่องหมุนเหวี่ยงวัสดุนิวเคลียร์ของโรงงานอิหร่านทำงานผิดพลาดจนเป็นเหตุให้เครื่องเสียหายกว่า 1,000 เครื่องตามรายงานข่าวที่ได้ศึกษาในบทที่ 2 อย่างไรก็ตาม การพัฒนาทางเทคโนโลยีอย่างต่อเนื่องอาจทำให้มีอาวุธไซเบอร์ที่สามารถสร้างความเสียหายต่อร่างกายและชีวิตได้ในอนาคต

จากการศึกษาในส่วนนี้ สรุปได้ว่า โดยการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบหรืออาวุธไซเบอร์สามารถพิจารณาเป็นได้ทั้งอาวุธ วิธีการและปัจจัยในการสู้รบจึงต้องพิจารณาหลักการเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบตามกฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกับอาวุธทุกประเภท ไม่ว่าจะเป็นอาวุธธรรมดาหรืออาวุธที่มีอานุภาพในการทำลายล้างสูงแม้ว่าจะไม่มีข้อบทเฉพาะเกี่ยวกับการโจมตีทางไซเบอร์ก็ตาม

3.2.3.3 หลักการห้ามใช้วิธีการและปัจจัยในการสู้รบซึ่งก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็น

กฎหมายมนุษยธรรมระหว่างประเทศกำหนดห้ามใช้วิธีการและปัจจัยในการสู้รบซึ่งโดยลักษณะของวิธีการและปัจจัยในการสู้รบนั้นก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็น ดังที่ได้กล่าวมาแล้วว่าหลักการห้ามใช้วิธีการและปัจจัยในการสู้รบก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็น (Superfluous Injury and Unnecessary Suffering) ถือเป็นกฎหมายจารีตประเพณีระหว่างประเทศ[321]

[321] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005) P. 237.

ศาลยุติธรรมระหว่างประเทศได้ยืนยันหลักการห้ามใช้วิธีการและปัจจัยในการสู้รบซึ่งโดยลักษณะก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นว่าเป็นหนึ่งในหลักการสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ[322] ในการบังคับใช้หลักการนี้ รัฐไม่มีเสรีภาพที่ปราศจากข้อจำกัดในการเลือกวิธีการเกี่ยวกับอาวุธที่ใช้[323]

หลักการห้ามก่อให้เกิดเกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นปรากฏตามข้อ 35 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ความว่า “ห้ามมิให้อาวุธ กระสุนและวัตถุ และวิธีการในการสู้รบในลักษณะที่จะก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็น”[324]

อย่างไรก็ดี ศาลอาญาระหว่างประเทศสำหรับอดีตยูโกสลาเวียให้ความเห็นไว้ในคดี Tadic ว่า สิ่งที่ไร้มนุษยธรรมตามที่กำหนดไว้ในการสู้รบที่มีลักษณะระหว่างประเทศไม่สามารถกระทำอย่างไร้มนุษยธรรมและไม่สามารถยอมรับได้ในความขัดแย้งภายใน[325] ดังนั้น หลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นบังคับใช้กับการขัดกันทางอาวุธที่ไม่ลักษณะระหว่างประเทศด้วยเช่นกัน

---

[322] *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*. Para. 238.

“harm greater than that inavoidable to achieve legitimate military objectives”

[323] ibid. Para. 78.

[324] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article. 35 (2)

“It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or necessary suffering”

[325]*The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty)* Para. 119. Jean-Marie Henckaerts and Louise Doswald-Beck, *Study on Customary International Humanitarian Law - Volume I: Rule*. P. 240.

“What is inhumane, and consequently proscribed, in international wars cannot but be inhumane and inadmissible in civil strife.”

จากหลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นตามข้อ 35 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 สามารถแบ่งการพิจารณาออกเป็นข้อห้ามปัจจัยในการสู้รบ (Means of Warfare) ซึ่งโดยลักษณะจะก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็น และข้อห้ามวิธีการในการสู้รบ (Methods of Warfare) ซึ่งโดยลักษณะจะก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็น

จากการศึกษากฎหมายจารีตประเพณีของกฎหมายมนุษยธรรมระหว่างประเทศโดยคณะกรรมการกาชาดระหว่างประเทศระบุว่าข้อห้ามปัจจัยในการสู้รบ (Means of Warfare) ที่โดยลักษณะจะก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็น หมายถึง ผลกระทบของอาวุธที่มีต่อพลรบ จะต้องไม่ก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็น[326] โดยศาลยุติธรรมระหว่างประเทศให้คำนิยามของคำว่า “ความทุกข์ทรมานโดยไม่จำเป็น” (Unnecessary Suffering) ไว้ในความเห็นเชิงปรึกษาคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้หรือการใช้อาวุธนิวเคลียร์ ค.ศ. 1996 ว่า ความทุกข์ทรมานโดยไม่จำเป็น หมายถึง กรณีที่ส่งผลร้ายอย่างหลีกเลี่ยงไม่ได้มากกว่าการบรรลุผลในการโจมตีเป้าหมายทางทหาร[327] ดังนั้น กฎหมายมนุษยธรรมระหว่างประเทศห้ามอาวุธหรือการใช้อาวุธที่ทำให้เกิดความทุกข์ทรมานเพิ่มมากขึ้นโดยไม่ทำให้เกิดความได้เปรียบทางทหารเพิ่มขึ้นแต่อย่างใด[328] ฝ่ายในการสู้รบมีหน้าที่ในการประเมินว่าอาวุธที่ใช้ในการสู้รบฝ่าฝืนหลักการห้ามก่อให้เกิดความทุกข์ทรมานเกินความจำเป็นหรือไม่ โดยพิจารณาว่าความเจ็บปวดหรือความทุกข์ทรมานนั้นสามารถหลีกเลี่ยงได้หรือไม่จากการ

---

[326] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005) P. 241.

[327] *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*. Para. 78.

[328] Burrus M. Carnahan, "Unnecessary Suffering, the Red Cross and Tactical Laser Weapons," *Loyola of Los Angeles International and Comparative Law Review* 18(1996). P. 713.

เปรียบเทียบระหว่างอาวุธที่ใช้กับทางเลือกในการใช้อาวุธอื่นว่าก่อให้เกิดความเจ็บปวดหรือทุกข์ทรมานน้อยกว่าหรือไม่[329]

เมื่อพิจารณาการโจมตีทางไซเบอร์ในลักษณะเป็นอาวุธหรือปัจจัยในการสู้รบ โดยลักษณะของเทคโนโลยีต่างๆ ที่ใช้ในการสู้รบ ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ เครือข่ายและระบบโปรแกรมสารสนเทศต่างๆ ไม่สามารถสังหารบุคคลหรือส่งผลกระทบต่อบุคคลได้โดยตรง เทคโนโลยีในปัจจุบันสามารถสร้างความเสียหายทางกายภาพต่อเทคโนโลยีที่มนุษย์พึ่งพาอยู่เท่านั้น การโจมตีทางไซเบอร์ซึ่งนำเทคโนโลยีไซเบอร์มาใช้เป็นปัจจัยในการสู้รบ โดยลักษณะในตัวเองจึงไม่สามารถก่อให้เกิดผลกระทบต่อบุคคลในลักษณะที่จะก่อให้เกิดการบาดเจ็บหรือความทุกข์ทรมานต่อบุคคลได้

อย่างไรก็ตาม ดังที่ได้กล่าวมาแล้วว่า การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธมีทั้งที่เป็นปัจจัยในการสู้รบและวิธีการในการสู้รบขึ้นอยู่กับลักษณะการใช้ จึงจำเป็นจะต้องพิจารณาข้อห้ามวิธีการในการสู้รบซึ่งโดยลักษณะจะก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็นเกี่ยวกับการนำเทคโนโลยีไซเบอร์มาใช้เป็นวิธีการในการสู้รบ (Methods of Warfare) ด้วยเช่นกัน

ในการบังคับใช้หลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นจะต้องประเมินชั่งน้ำหนักเปรียบเทียบความเหมาะสมระหว่างความได้เปรียบทางทหารกับผลกระทบที่เกิดจากการใช้อาวุธ โดยรัฐและนักวิชาการบางส่วนเห็นว่าการเปรียบเทียบที่ถูกต้องคือการเปรียบเทียบระหว่างความได้เปรียบทางทหารที่เกิดจากการใช้อาวุธตามความตั้งใจในการใช้ปกติกับระดับการบาดเจ็บหรือความทุกข์ทรมานที่จะเกิดจากการใช้อาวุธนั้น[330] ซึ่งถูกโต้แย้งโดยนักวิชาการบางส่วนเห็นว่า ในการพิจารณาว่าการใช้อาวุธใดขัดต่อหลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นหรือไม่นั้นจำเป็นจะต้องชั่งน้ำหนักระหว่างความได้เปรียบ

---

[329] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, ed. Second(United Kingdom: Cambridge University Press, 2010) P .65.

[330] William H. Boothby, *Weapons and the Law of Armed Conflict*(OUP Oxford, 2009). P. 62.

ทางทหารกับสิ่งที่มนุษย์จะได้รับผลกระทบจากการใช้อาวุธนั้นในอนาคต[331] ยิ่งไปกว่านั้น การพิจารณาการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็นนั้นจะต้องพิจารณาว่าการบาดเจ็บหรือความทุกข์ทรมานนั้นเป็นสิ่งที่หลีกเลี่ยงได้หรือไม่ได้[332]

ดังนั้น เมื่อพิจารณาการบังคับใช้หลักการห้ามวิธีการในการสู้รบที่ก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็นกับการโจมตีทางไซเบอร์ที่เป็นวิธีการในการสู้รบตามความเห็นแรก จึงจำต้องประเมินโดยเปรียบเทียบลักษณะและขนาดของความได้เปรียบทางทหารโดยทั่วไปซึ่งคาดการณ์จากอาวุธที่จะใช้กับรูปแบบความเจ็บปวดหรือความทุกข์ทรมานที่จะเกิดจากการใช้อาวุธไซเบอร์นั้น[333]

ในขณะที่ การพิจารณาบังคับใช้หลักการห้ามวิธีการในการสู้รบที่ก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็นกับการโจมตีทางไซเบอร์ที่เป็นวิธีการในการสู้รบตามความเห็นโต้แย้งจำเป็นจะต้องชั่งน้ำหนักระหว่างความได้เปรียบทางทหารที่คาดว่าจะได้จากการใช้วิธีการโจมตีทางไซเบอร์เปรียบเทียบกับผลกระทบที่ก่อให้เกิดการบาดเจ็บหรือความทุกข์ทรมานและทางเลือกในการใช้วิธีการโจมตีทางไซเบอร์ในการสู้รบนั้น[334]

จากการศึกษาหลักการห้ามใช้วิธีการในการสู้รบในลักษณะที่ก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็นข้างต้น ผู้เขียนเห็นว่า จำเป็นที่จะต้องเปรียบเทียบระหว่างความได้เปรียบทางทหารที่คาดว่าจะได้รับจากการใช้วิธีการโจมตีทางไซเบอร์นั้นกับผลกระทบที่เกิดจากการใช้วิธีการโจมตีทางไซเบอร์ที่ก่อให้เกิดการบาดเจ็บหรือความทุกข์ทรมานต่อพลรบว่า

---

[331] Christopher Greenwood, "The Law of Weaponry at the Start of the New Millennium," *International Law Studies* 71(1998). P. 199.

[332] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, ed. Second(United Kingdom: Cambridge University Press, 2010) P. 65.

[333] William H. Boothby, "Methods and Means of Cyber Warfare," International Law Studies 89(2013). P. 392.

[334] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012). P. 255.

สามารถหลีกเลี่ยงได้หรือไม่ โดยการบังคับใช้หลักการห้ามใช้วิธีการและปัจจัยในการสู้รบซึ่งก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจะต้องแยกการพิจารณาออกเป็นการนำเทคโนโลยีไซเบอร์มาใช้เป็นปัจจัยในการสู้รบ (Means of Warfare) และการนำเทคโนโลยีไซเบอร์มาใช้เป็นวิธีการในการสู้รบ (Methods of Warfare) ด้วยเทคโนโลยี ณ ปัจจุบันขณะที่ทำการศึกษาวิจัยเล่มนี้ ยังไม่พบว่า การนำเทคโนโลยีมาใช้เป็นปัจจัยในการสู้รบหรืออาวุธโดยลักษณะในตัวเองสามารถก่อให้เกิดผลกระทบทางกายภาพต่อบุคคลหรือสังหารบุคคลได้เหมือนเช่นอาวุธอื่น โดยโอกาสที่การนำเทคโนโลยีมาใช้เป็นปัจจัยในการสู้รบที่ทำให้เกิดการบาดเจ็บหรือความทุกข์ทรมานเกินขนาดเป็นไปได้น้อยมาก

ส่วนการนำเทคโนโลยีไซเบอร์มาใช้เป็นวิธีการในการสู้รบจะต้องทำการประเมินโดยชั่งน้ำหนักเปรียบเทียบระหว่างความได้เปรียบทางทหารที่คาดว่าจะได้รับจากการเลือกใช้วิธีการโจมตีทางไซเบอร์ใดกับผลกระทบจากการใช้วิธีการทางไซเบอร์นั้นที่ก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็นต่อพลรบว่าสามารถหลีกเลี่ยงวิธีการโจมตีทางไซเบอร์ดังกล่าวได้หรือไม่ ด้วยเทคโนโลยีไซเบอร์ในปัจจุบันมีโอกาสก่อให้เกิดการบาดเจ็บและการทำลายทางกายภาพจากการใช้น้อยมาก อย่างไรก็ตาม การใช้เทคโนโลยีไซเบอร์ในฐานะวิธีการในการสู้รบ (Methods of Warfare) อาจก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นได้ เช่น การโจมตีทางไซเบอร์โดยควบคุมระบบการช็อตด้วยไฟฟ้ากระตุ้นการเต้นของหัวใจ (Defibrillation) ต่อพลรบฝ่ายตรงข้ามที่มีอุปกรณ์กระตุ้นหัวใจภายในร่างกาย เพื่อทำให้หัวใจหยุดเต้นจากนั้นจึงกระตุ้นไฟฟ้าหลายๆ ครั้งจนทำให้พลรบนั้นเสียชีวิตลงในที่สุด[335] ถือเป็นการใช้วิธีการโจมตีทางไซเบอร์โดยตั้งใจที่จะทำให้เกิดความเจ็บปวดและความทุกข์ทรมานต่อพลรบเพิ่มมากขึ้น การกระทำดังกล่าวย่อมพิจารณาได้ว่าเป็นการนำเทคโนโลยีไซเบอร์มาใช้วิธีการในการสู้รบซึ่งขัดต่อหลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็นตามกฎหมายมนุษยธรรมระหว่างประเทศได้

นอกจากหลักการเกี่ยวกับการปฏิบัติการทางทหารตามที่ได้ศึกษามาแล้วข้างต้นนี้ หลักการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนถือเป็นหลักการที่สำคัญตามกฎหมาย

---

[335] Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts ed. Michael N. Schmitt(Cambridge University Press, 2013). P.144.

มนุษยธรรมระหว่างประเทศอีกส่วนหนึ่งที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ซึ่งจะได้ทำการศึกษาในส่วนต่อไป

3.3 การให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือน

นอกเหนือจากหลักการเกี่ยวกับปฏิบัติการทางทหารสำหรับฝ่ายในการสู้รบที่ใช้ในทุกสถานการณ์การขัดกันทางอาวุธ กฎหมายมนุษยธรรมระหว่างประเทศยังกำหนดหลักการเพื่อให้ความคุ้มครองทางกฎหมายแก่พลเรือนและผู้ที่ไม่ส่วนเกี่ยวข้องในการสู้รบอีกต่อไป ตลอดจนหลักการให้ความคุ้มครองแก่ทรัพย์สินของพลเรือน โดยก่อนที่จะทำการศึกษาหลักการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือน จำเป็นต้องศึกษาว่าพลเรือนและทรัพย์สินของพลเรือนที่ได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศครอบคลุมถึงบุคคลและทรัพย์สิ่งของใดบ้าง ดังนี้

3.3.1 พลเรือนและทรัพย์สินของพลเรือน

กฎหมายมนุษยธรรมระหว่างประเทศกำหนดให้พลเรือนหรือบุคคลที่ไม่ได้เป็นพลรบเป็นผู้ได้รับความคุ้มครองทางกฎหมายตามกฎหมายมนุษยธรรมระหว่างประเทศ โดยฝ่ายในการสู้รบมีหน้าที่ทั่วไปในการให้ความคุ้มครองและปฏิบัติต่อพลเรือนอย่างมีมนุษยธรรม[336]

ในการศึกษาข้อ 50 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ได้ให้นิยามของคำว่าพลเรือนไว้ว่า “พลเรือน ได้แก่ บุคคลใดๆ ซึ่งไม่ได้จัดอยู่ในประเภทของบุคคลตามที่อ้างถึงในข้อ 4 เอ (1), (2), (3) และ (6) แห่งอนุสัญญา ฉบับที่ 3 (อนุสัญญาเจนีวา ค.ศ. 1949) และในข้อ 43 แห่งพิธีสารนี้ (พิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977)”[337]

---

[336] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 119.

[337] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 50 (1)– Definition of civilians and civilian population

“A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2),(3) and (6) of the Third Convention and in Article 43 of this Protocol.”

จากการให้คำนิยามตามข้อ 50 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ข้างต้น เป็นการให้คำนิยามเชิงลบเพื่อหลีกเลี่ยงช่องโหว่ทางกฎหมายที่อาจเป็นไปได้ ในกรณีที่บุคคลอาจถูกมองว่าไม่ใช่ทั้งพลเรือนและพลรบและอาจถูกกั้นออกจากความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศ[338] จากคำนิยามตามข้อ 50 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 สามารถแบ่งประเภทบุคคลในสถานการณ์การขัดกันทางอาวุธได้ออกเป็นสองประเภทใหญ่ๆ คือพลรบ (Combatants) และพลเรือน (Civilians or Non-Combatants)

นอกจากนี้ ข้อ 50 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ให้คำนิยามประชากรพลเรือนว่าประกอบด้วยบุคคลทุกคนที่เป็นพลเรือน[339] โดยข้อ 50 (3)ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ยังกำหนดว่า การปรากฏของปัจเจกชนที่ไม่ได้อยู่ภายใต้คำนิยามของพลเรือนท่ามกลางประชากรพลเรือน ไม่ทำให้ประชากรนั้นต้องสูญเสียลักษณะการเป็นพลเรือนไปแต่อย่างใด[340]

ทั้งนี้ ในกรณีเป็นที่สงสัยว่าบุคคลใดมีสถานะเป็นพลเรือนหรือไม่ ให้สันนิษฐานไว้ก่อนว่าบุคคลนั้นเป็นพลเรือนตามข้อ 50 (1) พิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1[341]

เมื่อพิจารณาข้อ 50 (1) พิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1 ประกอบกับการศึกษาความหมายของพลรบตามหัวข้อ 3.2.1.1 สถานะของพลรบที่สรุปได้ว่า “พลรบ หมายถึง

[338] Robert Kolb and Richard Hyde, An Introduction to the International Law of Armed Conflicts(USA: Hart Publishing, 2008). P. 127.

[339] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 50 (2)

“The civilian population comprises all persons who are civilians.”

[340] Ibid.

Article 50 (3)

“The presence within the civilian population of individuals who do not come within the definition of civilians does not deprive the population of its civilian character.”

[341] ibid.

Article 50 (1)

“... In case of doubt whether a person is a civilian, that person shall be considered to be a civilian.”

สมาชิกทั้งหมดของกองกำลังทางทหารของฝ่ายคู่พิพาทในการสู้รบ” กล่าวได้ว่า พลเรือนคือบุคคลที่ไม่ได้เป็นสมาชิกของกองกำลังทหาร (Armed Force) ของฝ่ายในการสู้รบหรือไม่ใช่พลรบ (Combatants) นั่นเอง โดยลักษณะของพลเรือนจะต้องไม่เป็นสมาชิกของกองกำลังทหารหรือไม่มีส่วนร่วมโดยตรงในการสู้รบ[342]

ส่วนการให้คำนิยามคำว่า ทรัพย์สินของพลเรือน (Civilian Objectives) ปรากฏคำนิยามตามข้อ 52 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[343] สรุปได้ว่า “ทรัพย์สินของพลเรือน ได้แก่ บรรดาทรัพย์สิน สิ่งของพลเรือนซึ่งไม่ใช่เป้าหมายทางทหาร” เป็นการให้คำนิยามเชิงลบเช่นเดียวกับการให้คำนิยามคำว่า “พลเรือน” จึงจำต้องพิจารณาโดยอ้างอิงถึงคำนิยามของเป้าหมายทางทหารประกอบ

ทั้งนี้ ในกรณีที่มีข้อสงสัยว่าทรัพย์สิ่งของซึ่งโดยปกติแล้วใช้เพื่อวัตถุประสงค์ทางพลเรือนถูกนำมาใช้เพื่อช่วยก่อให้เกิดประสิทธิผลในปฏิบัติการทางทหารหรือไม่นั้น ให้สันนิษฐานไว้ก่อนว่ามิได้นำมาใช้เพื่อวัตถุประสงค์ทางทหารปรากฏข้อสันนิษฐานกฎหมายตามข้อ 52 (3) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[344]

เมื่อพิจารณาข้อ 52 (1) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ประกอบด้วยคำนิยามของเป้าหมายทางทหารตามที่ได้ศึกษาในข้อ 3.2.2.3 เป้าหมายทางทหารก่อนหน้านี้ สรุปได้ว่า ทรัพย์สินของพลเรือนคือทรัพย์สินสิ่งของที่โดยลักษณะ สถานที่ตั้ง วัตถุประสงค์หรือการใช้ไม่ก่อให้เกิดประสิทธิภาพในปฏิบัติการทางทหาร และการยึดหรือการทำให้หมดสมรรถภาพซึ่งทรัพย์สินสิ่งของในสภาวการณ์ขณะที่ปฏิบัติการนั้น ไม่ก่อให้เกิดความได้เปรียบทางทหารอย่างชัดเจน

---

[342] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, ed. Second(United Kingdom: Cambridge University Press, 2010) P. 121.

[343] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 52 (1)

“...Civilian objects are all objects which are not military objectives as defined in paragraph 2.”

[344] ibid.

Article 52 (3)

“In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.”

สรุปสั้นๆ ได้ว่า ทรัพย์สินของพลเรือนจะต้องเป็นทรัพย์สิ่งของที่ใช้เพื่อวัตถุประสงค์ทางพลเรือนเท่านั้น โดยไม่ได้นำมาใช้เพื่อก่อให้เกิดประสิทธิผลในปฏิบัติการทางทหารแต่อย่างใด

กฎมหายมนุษยธรรมระหว่างประเทศให้ความคุ้มครองแก่ทรัพย์สินของพลเรือนเช่นเดียวกับการให้ความคุ้มครองพลเรือน กล่าวคือฝ่ายในการสู้รบมีหน้าที่ในการให้ความคุ้มครองแก่ทรัพย์สินของพลเรือนโดยห้ามโจมตีโดยตรงต่อทรัพย์สินของพลเรือนและห้ามโจมตีโดยไม่เลือกเป้าหมาย

เมื่อพิจารณาความหมายของทรัพย์สินของพลเรือนที่ได้รับความคุ้มครองทางกฎหมายข้างต้น เทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่ไม่ได้ใช้เพื่อก่อให้เกิดประสิทธิผลในทางการทหารหรือใช้เพื่อวัตถุประสงค์ทางการทหารย่อมไม่ใช่เป้าหมายทางทหาร และได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศที่จะไม่ตกเป็นเป้าหมายในการโจมตี อาทิ เครื่องคอมพิวเตอร์ส่วนตัวของพลเรือน ระบบหรือเครือข่ายที่ใช้ในโครงสร้างพื้นฐานที่สำคัญของรัฐต่างๆ การพาณิชย์ การเงินการธนาคาร ไม่ว่าจะเป็น ระบบผลิตกระแสไฟฟ้า ระบบควบคุมการจราจรทางอากาศของเครื่องบินพาณิชย์ ระบบจ่ายน้ำ ดังนั้น การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธต่อทรัพย์สิ่งของพลเรือนย่อมเป็นการฝ่าฝืนกฎหมายมนุษยธรรมระหว่างประเทศ ฝ่ายในการสู้รบมีหน้าที่ในการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเช่นเดียวกับการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนจากการโจมตีด้วยอาวุธตามแบบ (Conventional Attack)

3.3.2 การให้ความคุ้มครองแก่พลเรือนและทรัพย์สินของพลเรือนจากการโจมตี

เป็นที่ยอมรับโดยทั่วไปว่า ฝ่ายในการสู้รบสามารถโจมตีโดยตรงต่อพลรบและเป้าหมายทางทหารได้โดยชอบด้วยกฎหมายในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธ ในขณะที่พลเรือนและทรัพย์สินของพลเรือนไม่อาจตกเป็นเป้าหมายในการโจมตีได้ตามกฎหมายมนุษยธรรมระหว่างประเทศ ซึ่งกำหนดให้ฝ่ายในการสู้รบมีหน้าที่ในการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนจากการโจมตีในสถานการณ์การขัดกันทางอาวุธตามหลักการห้ามมิให้โจมตีโดยตรงต่อพลเรือนและทรัพย์สินของพลเรือน และหลักการห้ามโจมตีโดยไม่เลือกเป้าหมาย ซึ่งจะศึกษาต่อไปดังนี้

3.3.2.1 หลักการห้ามโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือน

จากหลักการพื้นฐานการแยกแยะเป้าหมายตามข้อ 48 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[345] กำหนดหน้าที่ให้ฝ่ายในการสู้รบจะต้องแยกแยะตลอดเวลาระหว่างพลเรือนและพลรบ รวมถึงเป้าหมายทางทหารและทรัพย์สินของพลเรือนอันเป็นหลักการพื้นฐานสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ โดยศาลยุติธรรมระหว่างประเทศยืนยันหลักการนี้ไว้ในความเห็นเชิงปรึกษาคดีความชอบด้วยกฎหมายของการคุกคามที่จะใช้และการใช้อาวุธนิวเคลียร์ ค.ศ. 1996 กล่าวว่า รัฐจะต้องไม่ใช้พลเรือนเป็นเป้าหมายในการโจมตี[346]

หลักการข้างต้นได้รับการยืนยันข้อห้ามโจมตีพลเรือนและทรัพย์สินของพลเรือนตามข้อ 51 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ระบุว่า ประชากรพลเรือน ตลอดจนพลเรือนต้องไม่ตกเป็นเป้าหมายของการโจมตี การคุกคามหรือใช้ความรุนแรง โดยมีวัตถุประสงค์หลักในการสร้างความหวาดกลัวให้แพร่หลายไปในหมู่ประชากรพลเรือนเป็นสิ่งต้องห้าม[347] ฝ่ายในการสู้รบจึงมีหน้าที่ห้ามโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือน (Direct Attacks Against Civilians or Civilian Objects)

นอกจากนี้ การเจตนาหรือจงใจโจมตีโดยตรงต่อพลเรือนที่ไม่มีส่วนร่วมโดยตรงในการสู้รบ หรือทรัพย์สินของพลเรือนที่ไม่ได้ใช้เพื่อก่อให้เกิดประสิทธิผลในปฏิบัติการทางทหารถือเป็นการกระทำอันเป็นอาชญากรรมสงคราม (War Crime) ตามข้อ 8 ข้อ (2) (บี) (I) – (II) ของธรรมนูญกรุงโรมว่าด้วยศาลอาญาระหว่างประเทศ (The Rome Statute Of The International Criminal

---

[345] ibid.

Article 48 - Basic rule

"In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."

[346] *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*. Para. 78.

[347] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 51 (2)

"The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."

Court)[348] ในทางตรงกันข้าม หากความเสียหายเกิดจากการดำเนินการที่ปราศจากเจตนา เช่น เป็นผลข้างเคียงจากการโจมตีเป้าหมายทางทหารหรือเกิดจากความผิดพลาดในการดำเนินการโจมตี ผู้ดำเนินการโจมตีก็ย่อมหลุดพ้นจากความรับผิดตามข้อบทนี้ แต่หากการโจมตีที่มุ่งโจมตีต่อพลเรือนแต่ไม่บรรลุเป้าหมาย การโจมตีดังกล่าวก็ยังคงเข้าข่ายอาชญากรรมสงครามตามธรรมนูญกรุงโรมฯ[349]

การบังคับใช้หลักการโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือนไม่ได้ขึ้นอยู่กับขนาดของปฏิบัติการทางทหาร ฝ่ายในการสู้รบต้องนำไปบังคับใช้ทั้งการโจมตีขนาดใหญ่ เช่น การโจมตีโดยการใช้ระเบิดหรืออาวุธที่มีอานุภาพร้ายแรงในพื้นที่ที่มีผู้คนอาศัยอยู่อย่างหนาแน่นไปจนถึงการโจมตีขนาดเล็ก เช่น การลอบยิงพลเรือนเป็นรายบุคคล[350] แม้ว่าผู้โจมตีจะมีเหตุผลที่เชื่อได้ว่าการโจมตีโดยสร้างความหวาดกลัวแก่ประชากรพลเรือนของฝ่ายตรงข้ามจะประสบความสำเร็จทำลายขวัญกำลังใจของประชากรพลเรือน เพื่อกัดกร่อนความมุ่งมั่นของฝ่ายตรงข้ามในการสู้รบในสถานการณ์การขัดกันทางอาวุธและทำให้การสู้รบนั้นเข้าสู่บทสรุปยุติการสู้รบอย่างรวดเร็วซึ่งอาจจะเป็นผลให้รักษาชีวิตพลรบและพลเรือนของทั้งสองฝ่ายเป็นจำนวนนับไม่ถ้วนก็ตาม

หลักการห้ามโจมตีโดยตรงต่อพลเรือนและทรัพย์สินของพลเรือนดังกล่าวนี้บังคับใช้เมื่อพลเรือนหรือทรัพย์สินของพลเรือนคือเป้าหมายในการโจมตีในการสร้างความหวาดกลัวโดยไม่ห้ามการโจมตีต่อพลรบหรือเป้าหมายทางทหารขนาดใหญ่ แม้ว่าผลลัพธ์จากการโจมตีนั้นจะทำลายขวัญกำลังใจของพลเรือน ทำให้พลเรือนเกิดความหวาดกลัวและสะเทือนใจ เพราะเป้าหมาย

---

[348] "Rome Statute of the International Criminal Court."
Article 8 (2) (b) (i) – (ii) War crimes
" For the purpose of this Statute, "war crimes" means:
(b) Other serious violations of the laws and customs applicable in international armed conflict, within the established framework of international law, namely, any of the following acts:
(i) Intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities;
(ii) Intentionally directing attacks against civilian objects, that is, objects which are not military objectives;"

[349] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 120.

[350] Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," Journal of Conflict & Security Law 17, no. 2 (2012). P. 265.

ของการโจมตีไม่ใช่พลเรือนหรือทรัพย์สินของพลเรือนซึ่งต้องห้ามโจมตีตามกฎหมายมนุษยธรรมระหว่างประเทศแต่อย่างใด

จากการศึกษาหลักการห้ามโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือนข้างต้นที่บังคับใช้กับปฏิบัติการทางทหารทุกขนาดไม่ว่าจะเป็นการโจมตีขนาดเล็ก หรือการโจมตีขนาดใหญ่ก็ตาม ดังนั้น การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจึงอยู่ภายใต้บังคับหลักการดังกล่าวเช่นเดียวกับการโจมตีด้วยอาวุธตามแบบ โดยหลักการห้ามโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือนนำมาบังคับใช้กับการโจมตีทางไซเบอร์มากที่สุดเท่าที่บังคับใช้กับปฏิบัติการร้ายแรงที่ทำอันตรายถึงตาย (Kinetic Operations) โดยมีเงื่อนไขว่าการโจมตีทางไซเบอร์นั้นจะต้องมีความรุนแรง (Violence)

ยกตัวอย่าง การโจมตีทางไซเบอร์เพื่อเข้าควบคุมระบบคอมพิวเตอร์ของสายการบินของพลเรือน หรือหอควบคุมการจราจรทางอากาศของสายการบินของพลเรือน เพื่อให้เครื่องบินที่เต็มไปด้วยพลเรือนผู้โดยสารบนเครื่องบินชนกัน การโจมตีทางไซเบอร์ดังกล่าวย่อมก่อให้เกิดเป็นการโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือนต้องห้ามตามกฎหมายมนุษยธรรมระหว่างประเทศ

นอกจากนี้ เมื่อพิจารณาวัตถุประสงค์หลักของกฎหมายมนุษยธรรมระหว่างประเทศในการให้ความคุ้มครองแก่พลเรือนและทรัพย์สินของพลเรือนในระหว่างสถานการณ์การขัดกันทางอาวุธ ฝ่ายในการสู้รบจะดำเนินการโจมตีทางไซเบอร์โดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือนเพื่อให้เกิดการบาดเจ็บหรือเสียชีวิตของพลเรือนหรือการทำลายหรือความเสียหายซึ่งทรัพย์สินของพลเรือนอันเป็นการกระทำที่มีลักษณะรุนแรงไม่ได้

อย่างไรก็ตาม ด้วยลักษณะของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เป็นการกระทำภายในห้วงไซเบอร์ต่อระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ไม่ว่าจะเพื่อปรับเปลี่ยน รบกวน หลอกลวง ลดค่า หรือทำลายล้วนเป็นการโจมตีที่มุ่งโจมตีต่อระบบหรือเครือข่าย ข้อมูลสารสนเทศและคอมพิวเตอร์เป็นหลัก การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจึงอาจฝ่าฝืนต่อหลักการห้ามโจมตีโดยตรงต่อทรัพย์สินของพลเรือนเท่านั้น เนื่องจากเทคโนโลยีในปัจจุบันยังไม่สามารถดำเนินการโจมตีทางไซเบอร์โดยมุ่งโจมตีต่อพลเรือนโดยตรงได้ ฝ่ายในการสู้รบจึงมีหน้าที่ในการพิจารณาแยกแยะระหว่างทรัพย์สินของพลเรือนและเป้าหมายทางทหารว่าระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่มุ่งโจมตีนั้น

มีลักษณะเป็นเป้าหมายทางทหารอย่างแท้จริงหรือไม่ หากกรณีเป็นที่สงสัยว่าระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ซึ่งโดยปกติแล้วใช้เพื่อวัตถุประสงค์ทางพลเรือนถูกนำมาใช้เพื่อช่วยก่อให้เกิดประสิทธิผลในปฏิบัติการทางทหารหรือไม่นั้น ให้สันนิษฐานไว้ก่อนว่ามิได้นำมาใช้เพื่อวัตถุประสงค์ทางทหารอันเป็นข้อสันนิษฐานทางกฎหมายตามข้อ 52 (3) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[351]

ดังนั้น ฝ่ายในการสู้รบจะต้องไม่ดำเนินการโจมตีทางไซเบอร์ต่อระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์อันเป็นทรัพย์สินของพลเรือนหรือหากกรณีเป็นที่สงสัยว่าเป็นระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของพลเรือนใดถูกใช้ในปฏิบัติการทางทหารให้สันนิษฐานไว้ก่อนว่าเป็นทรัพย์สินของพลเรือนซึ่งไม่สามารถตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ได้โดยชอบด้วยกฎหมายและไม่อาจโจมตีทางไซเบอร์โดยตรงต่อระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ซึ่งเป็นที่สงสัยนั้นด้วยเช่นกัน

อย่างไรก็ดี ด้วยพัฒนาการของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่มีอยู่ในปัจจุบัน การโจมตีทางไซเบอร์ยังไม่สามารถก่อให้เกิดความเสียหายหรือมุ่งโจมตีต่อพลเรือนโดยตรงได้ กล่าวได้ว่า การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นปฏิบัติการทางทหารที่สอดคล้องกับหลักการห้ามโจมตีโดยตรงต่อพลเรือน ซึ่งฝ่ายในการสู้รบอาจใช้การโจมตีทางไซเบอร์เป็นทางเลือกในการสู้รบเพื่อหลีกเลี่ยงการฝ่าฝืนต่อหลักการห้ามโจมตีโดยตรงต่อพลเรือนตามกฎหมายมนุษยธรรมระหว่างประเทศนี้ได้

3.3.2.2 หลักการห้ามโจมตีโดยไม่เลือกเป้าหมาย

นอกจากข้อห้ามโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือนแล้ว กฎหมายมนุษยธรรมระหว่างประเทศยังให้ความคุ้มครองแก่พลเรือนและทรัพย์สินของพลเรือนตามหลักการห้ามการโจมตีโดยไม่เลือกเป้าหมาย (Indiscriminate Attacks) ซึ่งเป็นกฎหมายจารีตประเพณี

---

[351] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 52 (3)

"In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used."

ระหว่างประเทศ ยืนยันหลักการดังกล่าวตามข้อ 51 (4) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1977 ฉบับที่ 1[352] ระบุว่า

ข้อ 51 (4) การโจมตีโดยไม่เลือกเป้าหมายเป็นสิ่งต้องห้าม การโจมตีโดยไม่เลือกเป้าหมาย ได้แก่

(เอ) การโจมตีโดยไม่ได้กระทำโดยตรงต่อเป้าหมายทหารโดยเฉพาะ

(บี) การโจมตีโดยใช้วิธีการหรือปัจจัยในการสู้รบ ซึ่งไม่สามารถเล็งไปที่เป้าหมายทหารโดยเฉพาะได้ หรือ

(ซี) การโจมตีโดยใช้วิธีการหรือปัจจัยในการสู้รบซึ่งก่อให้เกิดผลอันไม่อาจจำกัดได้ตามที่กำหนดไว้ในพิธีสารฉบับนี้ (พิธีสารฉบับที่ 1)

และในแต่ละกรณีนั้น ก่อให้เกิดผลซึ่งมีลักษณะเป็นการโจมตีเป้าหมายทหารและพลเรือนหรือทรัพย์สินของพลเรือนโดยไม่อาจแยกแยะได้

การโจมตีโดยไม่เลือกเป้าหมาย (Indiscriminate Attacks) แตกต่างจากการโจมตีโดยตรงต่อพลเรือน (Direct Attacks Against Civilians) ในแง่ที่ว่า ผู้โจมตีไม่ได้เจตนาหรือพยายามที่จะทำให้เกิดอันตรายโดยตรงต่อประชากรพลเรือนอันเป็นการโจมตีโดยตรงต่อพลเรือนหรือทรัพย์สินของพลเรือน หากแต่การบาดเจ็บหรือความเสียหายที่เกิดขึ้นต่อพลเรือนเป็นเพียงสิ่งที่เกิดขึ้นจากการที่ผู้โจมตีไม่ได้คำนึงว่าการโจมตีจะส่งผลกระทบต่อประชากรพลเรือนหรือไม่อย่างไร[353]

---

[352] ibid.

Article. 51 (4)

"Indiscriminate attacks are prohibited. Indiscriminate attacks are:

(a) those which are not directed at a specific military objective;

(b) those which employ a method or means of combat which cannot be directed at a specific military objective; or

(c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;

and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

[353] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, ed. Second(United Kingdom: Cambridge University Press, 2010) P. 127.

ข้อ 51 (5) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[354] ระบุตัวอย่างของการโจมตีโดยไม่เลือกเป้าหมายไว้ดังนี้

“(เอ) การโจมตีโดยการทิ้งระเบิดไม่ว่าด้วยวิธีการหรือปัจจัยใดๆ ซึ่งปฏิบัติต่อเป้าหมายทางทหารที่ถูกโจมตีรวม เป็นหน่วยเดียวกัน แม้ว่าเป้าหมายเหล่านั้นได้มีการแยกแยะอย่างชัดเจนว่าเป็นเป้าหมายทางทหาร ซึ่งตั้งอยู่ในเมือง เขตชุมชน หมู่บ้าน หรือบริเวณอื่นซึ่งมีพลเรือนหรือทรัพย์สินของพลเรือนรวมกันอยู่ และ

(บี) การโจมตีซึ่งอาจคาดได้ว่าจะก่อให้เกิดการสูญเสียซึ่งชีวิตของพลเรือน การบาดเจ็บของพลเรือน ความเสียหายต่อทรัพย์สินของพลเรือน หรือความเสียหายดังกล่าวรวมกันโดยหลีกเลี่ยงไม่ได้ ซึ่งมากเกินกว่าความได้เปรียบทางทหารที่มีลักษณะโดยตรงและเป็นรูปธรรมอันคาดหมายไว้”

จากการศึกษาการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนจะเห็นได้ว่ากฎหมายมนุษยธรรมระหว่างประเทศมุ่งให้ความคุ้มครองแก่พลเรือนและทรัพย์สินของพลเรือน ทั้งการถูกโจมตีโดยตรง (Direct Attacks) และการโจมตีโดยไม่เลือกเป้าหมาย (Indiscriminate Attacks) ซึ่งแม้จะไม่ได้มุ่งโจมตีต่อพลเรือนหรือทรัพย์สินของพลเรือนโดยตรง แต่หากการโจมตีนั้นอาจก่อให้เกิดอันตรายแก่พลเรือนหรือทรัพย์สินของพลเรือนได้ การโจมตีดังกล่าวย่อมต้องห้ามตามกฎหมายมนุษยธรรมระหว่างประเทศเช่นกัน

เมื่อพิจารณาหลักการห้ามโจมตีโดยไม่เลือกเป้าหมาย (Indiscriminate Attacks) ในการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนนี้ จะพิจารณาเฉพาะส่วนของการโดยใช้วิธีการในการสู้รบ (Methods of Warfare) โดยไม่เลือกเป้าหมาย สำหรับการโจมตีโดยไม่เลือก

---

[354] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 51 (5)

“Among others, the following types of attacks are to be considered as indiscriminate:

(a) an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects; and

(b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”

เป้าหมายโดยใช้ปัจจัยในการสู้รบ (Means of Warfare) สามารถพิจารณาได้ตามหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมาย (Indiscriminate Weapons) ที่ได้ศึกษามาแล้วก่อนหน้านี้ (หัวข้อ 3.2.3.1 หลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้)

ในทำนองเดียวกับหลักการห้ามใช้อาวุธที่ไม่สามารถแยกแยะเป้าหมายได้ การพิจารณาหลักการห้ามโจมตีโดยไม่เลือกเป้าหมายตามวิธีการในการสู้รบ (Methods of Warfare) ซึ่งโดยลักษณะของวิธีการนั้นไม่สามารถแยกแยะเป้าหมายระหว่างพลเรือนกับพลรบ หรือทรัพย์สินของพลเรือนกับเป้าหมายทางทหารได้ย่อมเป็นการต้องห้ามตามกฎหมายมนุษยธรรมระหว่างประเทศ

ในทางทฤษฎี การโจมตีทางไซเบอร์อาจมีลักษณะเป็นการโจมตีโดยไม่เลือกเป้าหมายได้ หากฝ่ายในการสู้รบดำเนินการโจมตีต่อคอมพิวเตอร์ของฝ่ายตรงข้ามทั้งหมด โดยไม่มีความพยายามใดๆ ในการสร้างขึ้นเพื่อแยกความแตกต่างระหว่างเป้าหมายทางทหารและทรัพย์สินของพลเรือนตามลักษณะ การใช้ วัตถุประสงค์หรือสถานที่ตั้ง หากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้นทำอันตรายหรือทำให้พลเรือนได้รับบาดเจ็บ หรือมากกว่าความเสียหายเล็กน้อยทางกายภาพต่อทรัพย์สินของพลเรือน การโจมตีทางไซเบอร์ดังกล่าวถือเป็นการกระทำที่ฝ่าฝืนกฎหมายมนุษยธรรมระหว่างประเทศ[355]

แม้ว่าการโจมตีทางไซเบอร์ส่วนใหญ่เป็นการกระทำที่มุ่งต่อระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์ และมีโอกาสก่อให้เกิดการบาดเจ็บหรือเสียชีวิตของบุคคลน้อยมาก การโจมตีทางไซเบอร์อาจเป็นการโจมตีโดยไม่เลือกเป้าหมายได้ หากการโจมตีทางไซเบอร์นั้นไม่สามารถควบคุมหรือจำกัดผลเฉพาะต่อพลรบหรือเป้าหมายทางทหารได้ ตัวอย่างเช่น การโจมตีทางไซเบอร์ต่อระบบที่ใช้ในทางการทหารซึ่งใช้ในทางพลเรือนด้วย อย่างเช่น ระบบกำหนดตำแหน่งบนโลกหรือระบบจีพีเอส แม้จะเป็นการโจมตีต่อเป้าหมายทางทหารแต่ด้วยลักษณะความเชื่อมต่อกันของเทคโนโลยีทางทหารและพลเรือน ทำให้เป้าหมายทางทหารดังกล่าวเป็นเป้าหมายทางทหารที่มีทรัพย์สินของพลเรือนรวมกันอยู่ได้ การโจมตีทางไซเบอร์ต่อระบบจีพีเอสดังกล่าวอาจทำให้เกิดผลกระทบต่อการใช้งานทรัพย์สินของพลเรือนด้วยเช่นกันจึงเป็นการโจมตีโดยไม่เลือกเป้าหมายได้ เช่นเดียวกับตัวอย่างการโจมตีโดยไม่เลือกเป้าหมายโดยการทิ้งระเบิดตามข้อ 51 (5) (เอ) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1

---

[355] Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," Journal of Conflict & Security Law 17, no. 2 (2012). P. 267.

เมื่อพิจารณาจากตัวอย่างเหตุการณ์โจมตีทางไซเบอร์ที่เคยเกิดขึ้น ได้แก่ การโจมตีโดยการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอสต่อประเทศจอร์เจียถือเป็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ฝ่าฝืนหลักการห้ามโจมตีโดยไม่เลือกเป้าหมาย เนื่องจากลักษณะวิธีการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอสนั้นไม่สามารถเล็งไปที่เป้าหมายทางทหารโดยเฉพาะและไม่สามารถควบคุมผลของการโจมตีให้จำกัดเฉพาะต่อเป้าหมายทางทหารได้ เห็นได้ชัดจากรายงานข่าวที่ระบุว่า ระบบการสื่อสารและพาณิชย์ทั่วประเทศ เว็บไซต์ที่รองรับการทำงานของเครือข่ายโทรศัพท์หรือหนังสือพิมพ์ซึ่งถือเป็นทรัพย์สินของพลเรือนที่ไม่เกี่ยวข้องกับปฏิบัติการทางทหารใดๆ ล้วนได้รับความเสียหายจากการโจมตีทางไซเบอร์ดังกล่าว ฉะนั้น การโจมตีทางไซเบอร์โดยวิธีการทำให้ระบบปฏิเสธการให้บริการ หรือ ดีดีโอเอส จึงสามารถพิจารณาว่าเป็นวิธีการในการสู้รบที่ขัดต่อหลักการห้ามโจมตีโดยไม่เลือกเป้าหมายได้

อย่างไรก็ตาม การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่ต้องห้ามตามหลักการห้ามโจมตีโดยไม่เลือกเป้าหมายสามารถกระทำได้ ตัวอย่าง การโจมตีทางไซเบอร์โดยวิธีการฝังข้อมูลที่ไม่ถูกต้องที่สามารถเล็งเป้าหมายทางทหารคือระบบป้องกันทางอากาศของซีเรียโดยเฉพาะได้ ลักษณะการโจมตีดังกล่าวที่ก่อให้เกิดผลต่อเป้าหมายทางทหารได้โดยเฉพาะจึงมีลักษณะเป็นการโจมตีที่สามารถแยกแยะเป้าหมายทางทหารกับทรัพย์สินของพลเรือนได้และไม่ต้องห้ามตามหลักการห้ามโจมตีโดยไม่เลือกเป้าหมายนี้ กล่าวได้ว่า การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธใดที่สามารถหาตำแหน่งของเป้าหมายทางทหารที่แน่นอน แม่นยำได้ย่อมเป็นการโจมตีที่สอดคล้องกับหลักการห้ามโจมตีโดยไม่เลือกเป้าหมายตามกฎหมายมนุษยธรรมระหว่างประเทศ

3.3.3 การให้ความคุ้มครองพิเศษ

นอกเหนือจากการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนตามที่ได้ศึกษามาแล้วข้างต้น กฎหมายมนุษยธรรมระหว่างประเทศยังได้กำหนดให้ความคุ้มครองพิเศษแก่ทรัพย์สินในบางบริเวณและทรัพย์สินบางประเภทซึ่งมีความสำคัญต่อประชาคมระหว่างประเทศและมนุษยชาติ เพื่อเหตุผลทางด้านมนุษยธรรมและให้ความคุ้มครองแก่พลเรือนและทรัพย์สินของพลเรือนอันเป็นวัตถุประสงค์หลักของกฎหมายมนุษยธรรมระหว่างประเทศ อาทิ สถานที่ซึ่งไม่ได้รับการป้องกันและเขตปลอดทหาร สิ่งแวดล้อมทางธรรมชาติ ทรัพย์สินทางวัฒนธรรม สิ่งติดตั้งที่บรรจุพลังงานอันตรายวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน โรงพยาบาลและหน่วยแพทย์อื่นๆ ซึ่งใน

การศึกษาวิทยานิพนธ์เล่มนี้ ผู้เขียนจะหยิบยกเฉพาะกรณีการให้ความคุ้มครองพิเศษแก่ทรัพย์สินที่อาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ได้แก่ สิ่งติดตั้งที่บรรจุพลังงานอันตราย วัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน โรงพยาบาลและหน่วยแพทย์อื่นๆ ดังมีรายละเอียดดังนี้

3.3.3.1 สิ่งติดตั้งที่บรรจุพลังงานอันตราย

สิ่งติดตั้งที่บรรจุพลังงานอันตราย (Installations Containing Dangerous Forces) ได้รับความคุ้มครองตามข้อ 56 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[356] และข้อ 15 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2[357] กำหนดให้งานและสิ่งติดตั้งที่บรรจุพลังงานอันตรายกล่าวคือ เขื่อน ฝาย โรงไฟฟ้าพลังงานนิวเคลียร์จะต้องไม่ตกเป็นเป้าหมายในการโจมตี แม้ว่าสิ่งก่อสร้างเหล่านี้จะเป็นเป้าหมายทางทหารก็ตาม หากการโจมตีดังกล่าวอาจก่อให้เกิดการปลดปล่อยพลังงานอันตรายและเป็นผลให้เกิดความเสียหายร้ายแรงต่อประชากรพลเรือน โดยข้อ 56 ของพิธีสาร

---

[356] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 56 Protection of works and installations containing dangerous forces

"Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population. Other military objectives located at or in the vicinity of these works or installations shall not be made the object of attack if such attack may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population."

[357] "Protocol Additional of the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol Ii)."

Article 15 Protection of works and installations containing dangerous forces

"Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."

เพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ให้ความคุ้มครองรวมถึงเป้าหมายทางทหารที่ตั้งอยู่หรืออยู่ในบริเวณใกล้เคียงกันกับงานหรือสิ่งติดตั้งเหล่านี้จะต้องไม่ตกเป็นเป้าหมายในการโจมตี หากการโจมตีดังกล่าวอาจก่อให้เกิดการปลดปล่อยพลังงานอันตรายจากงานหรือสิ่งติดตั้งและเป็นผลให้เกิดความเสียหายร้ายแรงต่อประชากรพลเรือน

การกำหนดให้ความคุ้มครองแก่เขื่อน ฝายและโรงไฟฟ้าพลังงานนิวเคลียร์ เนื่องจากสิ่งติดตั้งที่บรรจุพลังงานอันตรายเหล่านี้ หากถูกโจมตีอาจก่อให้เกิดความเสียหายอย่างร้ายแรงต่อประชากรพลเรือนจากการปลดปล่อยพลังงานที่ไม่สามารถควบคุมได้ เช่น การโจมตีเขื่อน ฝายอาจทำให้เกิดภัยพิบัติน้ำท่วมบริเวณที่ประชากรอาศัยอยู่

หลักการห้ามโจมตีสิ่งติดตั้งที่บรรจุพลังงานอันตรายสะท้อนให้เห็นความพยายามในการจำกัดขอบเขตของผลกระทบต่อพลเรือน (Collateral Damage) ที่อาจเกิดขึ้นได้ซึ่งแม้สิ่งติดตั้งที่บรรจุพลังงานอันตรายนั้นจะเป็นเป้าหมายทางทหารก็ไม่สามารถทำการโจมตีได้ ข้อบทของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาทั้งสองฉบับ (พิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 และพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2) กำหนดรายการสิ่งติดตั้งที่บรรจุพลังงานอันตรายที่ได้รับความคุ้มครองไว้เป็นการเฉพาะ ได้แก่ เขื่อน ฝาย และโรงไฟฟ้าพลังงานนิวเคลียร์จึงไม่บังคับใช้หลักการนี้กับงานหรือสิ่งติดตั้งที่บรรจุพลังงานอันตรายอื่น เช่น โรงงานเคมี โรงกลั่นน้ำมัน

สิ่งติดตั้งที่บรรจุพลังงานอันตรายอาจสูญเสียความคุ้มครองพิเศษตามหลักการนี้ไป หากสิ่งก่อสร้างเหล่านั้นถูกใช้นอกเหนือจากหน้าที่ตามปกติ และใช้ในการสนับสนุนในลักษณะประจำสำคัญโดยตรงต่อปฏิบัติการทางทหารและการโจมตีเป็นเพียงวิธีการเดียวที่จะยุติการสนับสนุนนั้น[358] นอกจากนี้ ฝ่ายในการสู้รบยังมีหน้าที่ในการใช้ความพยายามในการหลีกเลี่ยงการจัดตั้งเป้าหมายทางทหารในสถานที่ใกล้เคียงกับงานหรือสิ่งติดตั้งที่บรรจุพลังงานอันตรายด้วย[359]

---

[358] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 56 (2)

The special protection against attack provided by paragraph 1 shall cease:

(a) for a dam or a dyke only if it is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;..."

[359] ibid.

อย่างไรก็ตาม หลักการดังกล่าวนี้ยังไม่ถือเป็นกฎหมายจารีตประเพณีระหว่างประเทศ ยกเว้นกรณีที่การโจมตีต่อสิ่งติดตั้งที่บรรจุพลังงานอันตรายนั้นเป็นเหตุให้เกิดผลกระทบต่อพลเรือนอย่างร้ายแรงซึ่งเป็นข้อห้ามที่ได้รับการยอมรับเป็นการทั่วไปแล้ว[360]

เมื่อพิจารณาจากข้อ 56 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 กำหนดให้ความคุ้มครองครอบคลุมไปถึงเป้าหมายทางการทหารอื่นที่ตั้งอยู่ หรืออยู่ในบริเวณใกล้เคียงกันกับงานหรือสิ่งติดตั้งที่บรรจุพลังงานอันตราย การให้ความคุ้มครองแก่สิ่งติดตั้งที่บรรจุพลังงานอันตรายนี้ย่อมหมายความรวมถึงคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งเป็นส่วนหนึ่งและสนับสนุนการทำงานของงานหรือสิ่งติดตั้งเช่นกัน[361]

ในปัจจุบัน เทคโนโลยีสารสนเทศและคอมพิวเตอร์ได้นำมาใช้ในการควบคุมการปฏิบัติงานของสิ่งติดตั้งที่บรรจุพลังงานอันตรายต่างๆ ไม่ว่าจะเป็น เขื่อน ฝาย หรือโรงงานไฟฟ้านิวเคลียร์เหล่านี้ต่างล้วนอาศัยระบบหรือโปรแกรมในการควบคุมหน้าที่ต่างๆ เช่น ระบบควบคุมการปล่อยน้ำของเขื่อนหรือฝาย ระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ของโรงงานไฟฟ้านิวเคลียร์ทำให้สิ่งติดตั้งที่บรรจุพลังงานอาจตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้

จากการศึกาการให้ความคุ้มครองพิเศษแก่สิ่งติดตั้งที่บรรจุพลังงานอันตรายข้างต้น สรุปได้ว่า การโจมตีทางไซเบอร์ต่อเครือข่ายหรือระบบการทำงานของสิ่งติดตั้งที่บรรจุพลังงาน

Article 56 (5)

"The Parties to the conflict shall endeavour to avoid locating any military objectives in the vicinity of the works or installations mentioned in paragraph 1. Nevertheless, installations erected for the sole purpose of defending the protected works or installations from attack are permissible and shall not themselves be made the object of attack, provided that they are not used in hostilities except for defensive actions necessary to respond to attacks against the protected works or installations and that their armament is limited to weapons capable only of repelling hostile action against the protected works or installations."

[360]จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 203.

[361] Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts ed. Michael N. Schmitt(Cambridge University Press, 2013). P. 224.

อันตรายที่อาจก่อให้เกิดการปลดปล่อยพลังงานอันตรายและเป็นผลให้เกิดความเสียหายอย่างร้ายแรงต่อประชากรพลเรือนย่อมเป็นการต้องห้ามตามหลักการนี้ เช่น การโจมตีระบบควบคุมการทำงานของเขื่อนที่ควบคุมการทำงานประตูระบายน้ำของเขื่อนซึ่งบรรจุน้ำหลายล้านแกลลอน (Gallons) จนเป็นเหตุให้น้ำจากเขื่อนถูกปลดปล่อยไหลลงสู่แม่น้ำและท่วมเมืองที่ประชากรพลเรือนอาศัยอยู่ การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธดังกล่าวย่อมไม่ชอบด้วยกฎหมายมนุษยธรรมระหว่างประเทศ

3.3.3.2 วัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน

วัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน (Objects Indispensable to the Survival of the Civilian Population) ได้รับความคุ้มครองพิเศษตามกฎหมายมนุษยธรรมระหว่างประเทศสะท้อนมาจากกฎหมายจารีตประเพณีระหว่างประเทศ กำหนดห้ามฝ่ายในการสู้รบโจมตีวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน ปรากฏตามข้อ 54 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[362] และข้อ 14 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2[363] โดยข้อ 54 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 กำหนดว่า “ห้ามโจมตี ทำลาย เคลื่อนย้าย หรือทำให้ไร้ประโยชน์ซึ่งวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน เช่น เสบียงอาหาร พื้นที่

---

[362] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

Article 54 (2) Protection of objects indispensable to the survival of the civilian population

“1. ...

2. It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive.”

[363] "Protocol Additional of the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol Ii)."

Article 14 Protection of objects indispensable to the survival of the civilian population

“... It is therefore prohibited to attack, destroy, remove or render useless, for that purpose, objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works.”

เกษตรกรรมสำหรับการผลิตเสบียงอาหาร พืชผล ปศุสัตว์ สถานที่เก็บและจ่ายน้ำดื่ม และงานชลประทาน โดยมีวัตถุประสงค์เฉพาะเพื่อกันมิให้ประชากรพลเรือนหรือฝ่ายตรงข้ามได้รับประโยชน์ในการดำรงชีวิต ทั้งนี้ ไม่ว่าจะด้วยมูลเหตุจูงใจใด ไม่ว่าเพื่อทำให้พลเรือนอดอยากหรือทำให้ต้องอพยพย้ายถิ่นออกไป หรือเพื่อมูลเหตุจูงใจอื่นใด”

หลักการห้ามโจมตีวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือนมีเป้าหมายในการห้ามใช้วิธีการที่ขาดมนุษยธรรมเพราะการโจมตีวัตถุอันจำเป็นในการดำรงชีวิต นอกจากจะทำให้ฝ่ายตรงข้ามขาดแคลนอาหารยังส่งผลกระทบต่อประชากรพลเรือนที่อาศัยอยู่ในบริเวณที่ถูกโจมตีต้องประสบกับภาวะขาดแคลนอาหารด้วยเช่นเดียวกัน หลักการดังกล่าวนี้กำหนดห้ามเฉพาะการใช้วิธีการในการสู้รบที่มีวัตถุประสงค์เพื่อให้ประชากรพลเรือนต้องขาดอาหาร อดอยากและย้ายที่อยู่อาศัยเท่านั้น การกระทำที่มีวัตถุประสงค์อื่นซึ่งมิได้กันประชากรพลเรือนจากการรับประโยชน์ในการดำรงชีพ ไม่ต้องห้ามตามหลักการนี้ เช่น สิ่งติดตั้งเพื่อผลิตน้ำดื่มที่ตั้งอยู่ในฐานทัพของฝ่ายศัตรู หรือคลองชลประทานที่ใช้เป็นแนวป้องกันอาจถูกโจมตีได้ หากทำเพื่อป้องกันการรุกรานของฝ่ายศัตรู[364]

ทั้งนี้ เมื่อพิจารณาตามข้อ 54 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 จะเห็นได้ว่าการโจมตีต่อวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือนจะต้องกระทำไปโดยมีวัตถุประสงค์เฉพาะ เพื่อกันมิให้ประชากรพลเรือนหรือฝ่ายตรงข้ามได้รับประโยชน์ในการดำรงชีวิตด้วย

เมื่อพิจารณาลักษณะของวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน อาทิ สถานที่เก็บและจ่ายน้ำดื่มและการชลประทาน จะเห็นได้ว่าเทคโนโลยีสารสนเทศและคอมพิวเตอร์ได้นำมาใช้ในการควบคุมการทำงานของวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือนข้างต้นอย่างแพร่หลาย อาทิ การใช้ระบบควบคุมการผลิตอาหาร การผลิตกระแสไฟฟ้า หรือระบบควบคุมและประเมินผลแบบศูนย์รวม (SCADA) ในการควบคุมระบบการจ่ายน้ำดื่มหรือชลประทาน การนำเทคโนโลยีเข้ามาใช้ควบคุมวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือนดังกล่าวจึงทำให้วัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือนมีความเสี่ยงที่จะถูกโจมตีทางไซเบอร์ได้จากการเชื่อมต่อของระบบหรือเครือข่ายเทคโนโลยี ดังนั้น การโจมตีทางไซเบอร์ในสถานการณ์การ

---

[364] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 198.

ขัดกันทางอาวุธต่อระบบหรือเครือข่ายที่ใช้ควบคุมวัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือนทำให้วัตถุเหล่านั้นใช้การไม่ได้ โดยมีวัตถุประสงค์เฉพาะเพื่อกันมิให้ประชากรพลเรือนหรือฝ่ายตรงข้ามได้รับประโยชน์ในการดำรงชีวิตย่อมเป็นการฝ่าฝืนกฎหมายมนุษยธรรมระหว่างประเทศ ยกตัวอย่าง การโจมตีต่อระบบควบคุมการจ่ายน้ำของชลประทาน โดยมีวัตถุประสงค์เฉพาะเพื่อกันมิให้กองกำลังฝ่ายตรงข้ามใช้ในการดำรงชีวิตและคาดได้ว่าประชากรพลเรือนจะต้องประสบปัญหาการขาดแคลนน้ำอุปโภคบริโภคเช่นเดียวกันมีลักษณะเป็นการกระทำที่มีวัตถุประสงค์เพื่อกันมิให้ประชากรพลเรือนหรือฝ่ายตรงข้ามได้รับประโยชน์ในการดำรงชีวิตเป็นการต้องห้ามตามกฎหมายมนุษยธรรมระหว่างประเทศ

3.3.3.3 โรงพยาบาล และหน่วยแพทย์อื่นๆ

โรงพยาบาล หน่วยแพทย์และยานพาหนะทางการแพทย์รวมทั้งเรือโรงพยาบาล อากาศยานโรงพยาบาลล้วนได้รับความคุ้มครองพิเศษทั้งในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศในฐานะเป็นกฎหมายจารีตประเพณีระหว่างประเทศ[365] โดยฝ่ายในการสู้รบต้องให้ความเคารพและให้ความคุ้มครองตลอดเวลา โดยเฉพาะอย่างยิ่ง โรงพยาบาลและหน่วยแพทย์อื่นๆ จะต้องไม่ถูกใช้เพื่อเป็นเป้าหมายทางทหารจากการโจมตี ยืนยันหลักการดังกล่าวตามข้อ 19 24 25 35 และ 36 ของอนุสัญญากรุงเจนีวา ฉบับที่ 1[366] ข้อ 22 24 25 27 36-39 ของอนุสัญญาเจนีวาฉบับที่ 2[367] ข้อ 18-

[365] Jean-Marie Henckaerts and Louise Doswald-Beck, Study on Customary International Humanitarian Law - Volume I: Rule (Cambridge University Press, 2005)

[366] "Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949."

[367] "Geneva Convention (Ii) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949."

22 ของอนุสัญญาเจนีวา ฉบับที่ 4[368] ข้อ 12 15 21-24 และ 26 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1[369] และข้อ 9 ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 2[370]

จากการศึกษาข้อบทข้างต้น จะเห็นได้ว่า ฝ่ายในการสู้รบมีหน้าที่ให้ความเคารพที่จะไม่ขัดขวางหรือกีดกั้นโรงพยาบาล หน่วยแพทย์และยานพาหนะทางการแพทย์จากการปฏิบัติหน้าที่ทางการแพทย์ ดูแลรักษาผู้บาดเจ็บหรือเจ็บป่วย หรือการปฏิบัติหน้าที่ทางมนุษยธรรม

นอกจากนี้ ฝ่ายในการสู้รบจะต้องให้ความคุ้มครองแก่โรงพยาบาล หน่วยแพทย์และยานพาหนะทางการแพทย์จากการถูกโจมตีและต้องดูแลมิให้มีการใช้สำหรับปฏิบัติการทางทหารที่เป็นปฏิปักษ์ใดๆ[371]

อย่างไรก็ตาม การคุ้มครองพิเศษนี้จะสิ้นสุดลง เมื่อโรงพยาบาล หน่วยแพทย์และยานพาหนะทางการแพทย์ใดถูกใช้ไปนอกเหนือจากการปฏิบัติหน้าที่ทางมนุษยธรรม และเป็นอันตรายต่อฝ่ายศัตรูในการสู้รบ

การบังคับใช้หลักการห้ามโจมตีโรงพยาบาล หน่วยแพทย์อื่นๆ สำหรับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้น ฝ่ายในการสู้รบจะต้องให้ความคุ้มครองพิเศษแก่โรงพยาบาล หน่วยแพทย์และยานพาหนะทางการแพทย์ซึ่งจะต้องได้รับความเคารพและความคุ้มครองตลอดเวลาที่ทำการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธซึ่งเมื่อพิจารณาการทำงานของโรงพยาบาล หน่วยแพทย์อื่นๆ ในปัจจุบันมีการนำเทคโนโลยีเข้ามาใช้ในทางการแพทย์

---

[368] "Geneva Convention (Iv) Relative to the Protection of Civilian Persons in Time of War of 12 August 1949."

[369] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)."

[370] "Protocol Additional of the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol Ii)."

[371] จตุรนต์ ถิระวัฒน์, กฎหมายมนุษยธรรมระหว่างประเทศ(กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550). หน้า 186.

อย่างมีนัยสำคัญ ไม่ว่าจะเป็นเครื่องมืออุปกรณ์ที่ใช้ในการรักษาพยาบาลในโรงพยาบาลซึ่งใช้เทคโนโลยีในการควบคุมการทำงาน ฐานข้อมูลทางการแพทย์และระบบข้อมูลสารสนเทศทางการแพทย์ล้วนแต่ใช้ระบบหรือเครือข่ายเทคโนโลยีสารสนเทศในการเก็บรักษาข้อมูลสารสนเทศทางการแพทย์ทั้งสิ้น โดยเครื่องมืออุปกรณ์ คอมพิวเตอร์พกพาและฐานข้อมูลที่บรรจุระบบหรือเครือข่ายสารสนเทศเหล่านั้นสามารถพิจารณาว่าเป็นส่วนหนึ่งของชิ้นส่วนวัสดุอุปกรณ์ทางการแพทย์ที่ได้รับความคุ้มครองตามข้อบทแห่งอนุสัญญาเจนีวา ฉบับที่ 1 ได้ การใช้เทคโนโลยีในการควบคุมการทำงานของวัสดุอุปกรณ์ทางการแพทย์ตลอดจนฐานข้อมูลทางการแพทย์เหล่านี้ทำให้วัสดุอุปกรณ์ทางการแพทย์ตลอดจนฐานข้อมูลทางการแพทย์ดังกล่าวมีความเสี่ยงที่จะตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้

จากที่ได้ศึกษาข้างต้น ครื่องมืออุปกรณ์ คอมพิวเตอร์พกพาและฐานข้อมูลที่บรรจุระบบหรือเครือข่ายสารสนเทศในทางการแพทย์ย่อมได้รับความคุ้มครองพิเศษตามข้อ 19 ของอนุสัญญาเจนีวา ฉบับที่ 1[372] ทั้งนี้ ทรัพย์สินข้างต้นจะต้องไม่ถูกใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากการปฏิบัติหน้าที่ทางมนุษยธรรม โดยความคุ้มครองจะคงอยู่ตลอดเวลาที่ระบบถูกใช้เพื่อการดูแลรักษาผู้บาดเจ็บหรือผู้เจ็บป่วยและการป้องกันโรคภัยไข้เจ็บโดยเฉพาะ ยกตัวอย่าง การเข้าสู่บันทึกทางการแพทย์เพื่อใช้ในการดูแลรักษาพยาบาล เช่น การเข้าสู่ระบบข้อมูลสารสนเทศเพื่อประเมินความต้องการวัคซีนเป็นการใช้ระบบข้อมูลสารสนเทศเพื่อการป้องกันการเกิดโรคภัยไข้เจ็บเช่นนี้ ระบบข้อมูลสารสนเทศดังกล่าวย่อมได้รับความคุ้มครองพิเศษตามกฎหมายมนุษยธรรมระหว่างประเทศ ในขณะที่การใช้ระบบหรือฐานข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากการปฏิบัติหน้าที่ทางการแพทย์และหน้าที่ทางมนุษยธรรม เช่น การใช้ฐานข้อมูลเพื่อทำการวิจัยผลกระทบของระบบอาวุธใหม่ซึ่งเป็นส่วนหนึ่งในการศึกษาวิจัยพัฒนาอาวุธย่อมทำให้ระบบสิ้นสุดการได้รับความคุ้มครอง

---

[372] "Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949."

Article 19

"Fixed establishments and mobile medical units of the Medical Service may in no circumstances be attacked, but shall at all times be respected and protected by the Parties to the conflict."

ตามกฎหมายมนุษยธรรมระหว่างประเทศและทำให้ฐานข้อมูลนั้นกลายเป็นเป้าหมายทางทหารในการโจมตีทางไซเบอร์ได้[373]

จากการศึกษาทั้งหมดในบทนี้ จะพบว่า การพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์ในปัจจุบันได้เข้ามามีบทบาทสำคัญต่อทั้งการดำเนินชีวิตของพลเรือนและปฏิบัติการทางทหารและการสู้รบของพลรบ การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจึงเป็นวิธีการและปัจจัยในการสู้รบการนำเทคโนโลยีไซเบอร์ที่เกิดจากการนำความก้าวหน้าทางเทคโนโลยีมาใช้ประโยชน์ในทางการทหาร อย่างไรก็ดี ลักษณะพิเศษของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ในปัจจุบันที่มีความเชื่อมต่อของระบบหรือเครือข่ายเทคโนโลยีที่ใช้ในกิจการของพลเรือนและระบบหรือเครือข่ายเทคโนโลยีที่ใช้ในทางทหารส่งผลให้พลเรือนอาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้

เมื่อพิจารณากฎหมายมนุษยธรรมระหว่างประเทศอันเป็นกฎหมายระหว่างประเทศที่บังคับใช้ในสถานการณ์การขัดกันทางอาวุธมีบทบาทสำคัญในการให้ความคุ้มครองทางกฎหมายแก่พลเรือน จะเห็นได้ว่า ในกรณีที่มีสถานการณ์การขัดกันทางอาวุธที่มีการใช้กำลังทางทหารเกิดขึ้นแล้ว การโจมตีทางไซเบอร์ในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธจะต้องอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศอย่างไม่มีข้อสงสัย แม้ว่ากฎหมายมนุษยธรรมระหว่างประเทศจะมีอยู่ก่อนการนำเทคโนโลยีมาใช้เป็นวิธีการและปัจจัยในการสู้รบและไม่มีข้อบทตามกฎหมายมนุษยธรรมระหว่างประเทศระบุถึงการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธไว้ก็ตาม

อย่างไรก็ดี ในกรณีที่ยังไม่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น การพิจารณาว่ากฎหมายมนุษยธรรมระหว่างประเทศจะบังคับใช้กับการโจมตีทางไซเบอร์ได้หรือไม่นั้น มีเงื่อนไขสำคัญคือต้องมีการขัดกันทางอาวุธ (Armed Conflict) เกิดขึ้น โดยพิจารณาว่าการโจมตีทางไซเบอร์เพียงลำพังจะเป็นชนวนเริ่มต้นให้มีการขัดกันทางอาวุธเกิดขึ้นหรือไม่ จากการการเทียบเคียงว่าการเริ่มต้นโจมตีทาง

[373] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012). P. 243.

ไซเบอร์เทียบเท่าได้กับการโจมตีโดยใช้อาวุธตามแบบอันเป็นการใช้กำลังทางทหาร (Armed Attack) สำหรับกรณีนี้ ยังไม่ได้ข้อสรุปที่ชัดเจนว่าการโจมตีทางไซเบอร์เพียงลำพังจะเป็นชนวนเริ่มต้นของการเกิดสถานการณ์การขัดกันทางอาวุธได้หรือไม่ โดยมีเงื่อนไขในพิจารณาการเกิดสถานการณ์การขัดกันทางอาวุธหลายประการที่ยังมีข้อท้าทายจำเป็นจะต้องอาศัยแนวทางปฏิบัติของรัฐในการให้ความชัดเจนในกรณีดังกล่าวต่อไป

จากการศึกษาการใช้หลักการเกี่ยวกับปฏิบัติการทางทหารและการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือนทั้งหมดในบทนี้ จะเห็นได้ว่าหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศสามารถนำมาบังคับใช้กับการโจมตีทางไซเบอร์อันเกิดจากการนำเทคโนโลยีเข้ามาใช้เป็นวิธีการและปัจจัยในการสู้รบใหม่นี้ได้ทั้งสิ้น จึงกล่าวสรุปได้ว่ากฎหมายมนุษยธรรมระหว่างประเทศมีความยืดหยุ่นครอบคลุมกับการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้เป็นวิธีการและปัจจัยในการสู้รบ เพื่อให้ความคุ้มครองแก่พลเรือนได้ แม้ว่าจะไม่มีข้อบทเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธไว้เป็นการเฉพาะ

อย่างไรก็ตาม ด้วยลักษณะพิเศษของการโจมตีทางไซเบอร์บางประการก่อให้เกิดข้อท้าทายในทางปฏิบัติและทางกฎหมายเกี่ยวกับการบังคับใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธซึ่งจะได้ทำการศึกษาในบทถัดไป

บทที่ 4
ข้อท้าทายในการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศและการพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

จากเนื้อหาบทที่แล้ว จะเห็นได้ว่า ลักษณะพิเศษของการนำเทคโนโลยีทางไซเบอร์มาใช้เป็นวิธีการและปัจจัยในการสู้รบอาจก่อให้เกิดปัญหาในทางปฏิบัติอันเป็นข้อท้าทายในการใช้หลักการบางประการตามกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อให้ความคุ้มครองแก่พลเรือนและผู้ที่ไม่มีส่วนเกี่ยวข้องกับการสู้รบอีกต่อไปอันเป็นวัตถุประสงค์หลักของกฎหมายมนุษยธรรมระหว่างประเทศนั้น

ในบทนี้ จะได้ทำการวิเคราะห์ถึงข้อท้าทายในการบังคับใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ตลอดจนแนวทางในการแก้ไขข้อท้าทายที่เกิดจากการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยมีรายละเอียดดังต่อไปนี้

4.1 การขาดคำนิยามคำว่า “การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ”

ดังที่ได้กล่าวไว้แล้วว่า คำว่า “การโจมตีทางไซเบอร์” ถูกนำไปใช้ในหลากหลายบริบท ทั้งในสถานการณ์ปกติและสถานการณ์ที่มีความขัดแย้ง การขาดคำนิยามของคำว่า “การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ” ส่งผลให้เกิดข้อท้าทายในการพิจารณาว่าเหตุการณ์การโจมตีทางไซเบอร์ใดเป็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศ

หากเป็นการโจมตีทางไซเบอร์ที่เกิดขึ้นในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นและยังไม่สิ้นสุด กรณีการโจมตีทางไซเบอร์ดังกล่าวย่อมสามารถพิจารณาได้ว่าอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกับการโจมตีด้วยอาวุธอย่างอื่นอย่างไม่มีข้อสงสัยตามที่ได้อธิบายรายละเอียดไปแล้ว

ในขณะที่ หากยังไม่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น การจะพิจารณาว่าการโจมตีทางไซเบอร์ใดเป็นจุดเริ่มต้นของการเกิดสถานการณ์การขัดกันทางอาวุธจะต้องพิจารณาจากลักษณะของ

การโจมตีทางไซเบอร์นั้นว่ามีปัจจัยบ่งชี้อันเป็นเงื่อนไขของการเกิดสถานการณ์การขัดกันทางอาวุธตามแต่ละประเภท (การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศหรือการขัดกันทางอาวุธที่ไม่ลักษณะระหว่างประเทศ) ตามที่ได้ศึกษามาแล้ว อย่างไรก็ดี ประเด็นที่ว่า การโจมตีทางไซเบอร์สามารถพิจารณาเทียบเท่าการใช้กำลังทางทหารได้หรือไม่ ยังคงเป็นที่ถกเถียงกันในทางวิชาการ อาจจะเนื่องมาจากการที่ยังไม่มีเหตุการณ์โจมตีทางไซเบอร์ใดที่ปราศจากการใช้กำลังทางทหารหรือการโจมตีด้วยอาวุธตามแบบอย่างอื่นร่วมด้วยที่เข้าข่ายเกณฑ์ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธเกิดขึ้นจริง การมองภาพการเกิดสถานการณ์การขัดกันทางอาวุธจากการโจมตีทางไซเบอร์อาจจะยังไม่ชัดเจนมากนัก

กรณีที่ยังไม่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น การกำหนดคำนิยามที่เฉพาะเจาะจงของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธซึ่งเป็นที่ยอมรับของประชาคมระหว่างประเทศ จะช่วยให้ฝ่ายในการสู้รบสามารถทำการประเมินเบื้องต้นได้ว่า การโจมตีทางไซเบอร์ที่ฝ่ายในการสู้รบจะดำเนินการ หรือเหตุการณ์การโจมตีทางไซเบอร์ที่เผชิญอยู่เป็นการโจมตีทางไซเบอร์ภายใต้บังคับกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ จะต้องปฏิบัติการโจมตีทางไซเบอร์ให้สอดคล้องกับหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ อย่างไร กล่าวคือ หากการโจมตีทางไซเบอร์นั้นเข้าข่ายตามคำนิยามที่เฉพาะเจาะจงของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ฝ่ายในการสู้รบที่เลือกใช้การโจมตีทางไซเบอร์มีหน้าที่ในการประเมินหรือชั่งน้ำหนักเกี่ยวกับระดับความรุนแรง ผลกระทบของการโจมตีทางไซเบอร์ให้เหมาะสมสอดคล้องกับหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ

ยกตัวอย่าง ปฏิบัติการทางไซเบอร์ที่ทำการเก็บรวบรวมข้อมูลที่อยู่ในห้วงไซเบอร์หรือเครือข่ายทางไซเบอร์อาจพิจารณาว่าเป็นการจารกรรมข้อมูลไซเบอร์ได้ แต่หากการเก็บรวบรวมข้อมูลนั้นมีวัตถุประสงค์เพื่อความได้เปรียบทางการทหาร อาจจะถูกพิจารณาให้เป็นมากกว่าการจารกรรมข้อมูลไซเบอร์หรือยกระดับเป็นการใช้กำลังหรือการโจมตีทางไซเบอร์ได้ การกำหนดคำนิยามที่เฉพาะเจาะจงของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธย่อมทำให้เกิดความชัดเจนในการพิจารณาว่าการรวบรวมข้อมูลทางไซเบอร์ลักษณะใดเป็นการโจมตีทางไซเบอร์ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศได้

4.2 ความไม่ชัดเจนของการบ่งชี้การเกิดสถานการณ์การขัดกันทางอาวุธจากการโจมตีทางไซเบอร์บางประการ

จากการศึกษาวิเคราะห์การนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ที่ก่อให้เกิดสถานการณ์การขัดกันทางอาวุธทั้งการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ พบว่ามีข้อท้าทายเกี่ยวกับเงื่อนไขการเกิดสถานการณ์การขัดกันทางอาวุธจากการโจมตีทางไซเบอร์ ดังต่อไปนี้

4.2.1 การขาดความสามารถในการพิสูจน์ว่าเป็นการกระทำของรัฐ

ลักษณะพิเศษของการโจมตีทางไซเบอร์ก่อให้เกิดข้อท้าทายในทางปฏิบัติเกี่ยวกับการพิสูจน์ว่าเป็นการกระทำของรัฐ (Attributable to a State) ซึ่งเป็นเงื่อนไขสำคัญในการพิจารณาว่าเป็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ เนื่องจากวิทยาการความก้าวหน้าของเทคโนโลยีซึ่งสามารถปกปิดร่องรอยที่มาของการโจมตีทางไซเบอร์ ความซับซ้อนของเทคโนโลยีที่ใช้ในการโจมตีทางไซเบอร์ ทำให้ไม่สามารถพิสูจน์ได้ว่าการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้นมีจุดเริ่มต้นมาจากที่ใด

เมื่อพิจารณาลักษณะของการโจมตีทางไซเบอร์ที่สามารถดำเนินการโจมตีทางไซเบอร์จากสถานที่ใดก็ได้ทั่วโลก ไม่จำเป็นจะต้องดำเนินการโจมตีทางไซเบอร์จากดินแดนของรัฐซึ่งเป็นฝ่ายในการสู้รบเท่านั้น นอกจากนี้ การโจมตีทางไซเบอร์บางรูปแบบ เช่น การโจมตีด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอสที่อาศัยการใช้คอมพิวเตอร์จำนวนมากในการโจมตีซึ่งคอมพิวเตอร์ที่ติดเชื้อ (Zombies) อาจมาจากคอมพิวเตอร์หลายๆ ประเทศรวมกันหรือจากประเทศเดียวทั้งหมดก็ได้ โดยที่ผู้ใช้งานอาจไม่ทราบมาก่อนว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่นั้นกลายเป็นอาวุธที่ใช้ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธแล้ว ความซับซ้อนของเทคโนโลยีดังกล่าวข้างต้นทำให้ยากในการพิสูจน์ว่าการโจมตีทางไซเบอร์ที่เกิดขึ้นเป็นการกระทำของรัฐใด

นอกจากนี้ แม้จะสามารถตามรอยเส้นทางการโจมตีทางไซเบอร์จนถึงแหล่งที่มาได้ แต่การเชื่อมโยงการโจมตีทางไซเบอร์ให้เป็นการกระทำของรัฐหรือพิสูจน์ว่ารัฐอยู่เบื้องหลังการโจมตีอันเป็นความรับผิดของรัฐนั้น ในขณะนี้ยังไม่มีเครื่องมือในการพิสูจน์ว่าเป็นการกระทำของรัฐที่แม่นยำและเชื่อถือได้ ยกตัวอย่าง แม้จะสืบสวนจนทำให้ทราบแน่ชัดว่าการโจมตีทางไซเบอร์ต่อรัฐ A

มีจุดเริ่มต้นมาจากคอมพิวเตอร์เครื่องหนึ่งในรัฐ B แต่การพิสูจน์ชี้ชัดว่าการกระทำของผู้โจมตีนั้นเป็นการกระทำของรัฐ B หรือเป็นเพียงการกระทำส่วนตัวของนักแฮคเกอร์นั้นทำได้ยาก หรือกรณีที่รัฐ X ว่าจ้างกลุ่มแฮคเกอร์ (Hackers) กระทำการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ Y โดยให้กลุ่มแฮคเกอร์ (Hackers) ดำเนินการจากคอมพิวเตอร์ภายในรัฐ Z ยิ่งทำให้การพิสูจน์ความเกี่ยวข้องระหว่างรัฐ X กับกลุ่มแฮคเกอร์มีความยุ่งยากและซับซ้อนขึ้นไปอีก การพิสูจน์ว่าการโจมตีทางไซเบอร์ทั้งสองกรณีเป็นการกระทำของรัฐหรือว่ามีรัฐอยู่เบื้องหลังการโจมตีทางไซเบอร์ด้วยเทคโนโลยีปัจจุบันยังไม่มีเครื่องมือหรือวิธีการที่สามารถทำการพิสูจน์ระบุให้ชี้ชัดได้ หากไม่มีรัฐใดออกมาแสดงความรับผิดชอบต่อเหตุการณ์โจมตีทางไซเบอร์ที่เกิดขึ้น เงื่อนไขของการเกิดการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศย่อมจะไม่เกิดขึ้น ดังเช่นกรณีการโจมตีทางไซเบอร์ด้วยสตักซ์เน็ตต่อโรงงานนิวเคลียร์ของอิหร่านที่ไม่สามารถปรับความรับผิดให้แก่รัฐใดได้ แม้ว่าทางการอิหร่านจะเชื่อว่าประเทศอิสราเอลและประเทศทางตะวันตกอยู่เบื้องหลังการโจมตีทางไซเบอร์ก็ตาม[374]

จะเห็นได้ว่า ความซับซ้อนของเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์ที่เพิ่มมากขึ้นตามกาลเวลาทำให้การสอบสวนหาที่มาของการโจมตีทางไซเบอร์ การระบุตัวตนของผู้โจมตีจึงทำได้ยากจากการปกปิดร่องรอยที่มาของการกระทำและการปกปิดตัวตนของผู้กระทำ ตลอดจนกระบวนการในการสอบสวนหาหลักฐานแสดงความเชื่อมโยงของรัฐที่มีในการโจมตีทางไซเบอร์

จากข้อท้าทายในทางปฏิบัติเกี่ยวกับการขาดความสามารถในการพิสูจน์ว่าเป็นการกระทำของรัฐนี้ทำให้การพิจารณาว่าการเกิดสถานการณ์การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศซึ่งเริ่มต้นมาจากการโจมตีทางไซเบอร์ โดยปราศจากการโจมตีด้วยอาวุธตามแบบนั้นเป็นเพียงความเห็นทางวิชาการในทางทฤษฎีที่ทำได้ยากยิ่งในทางปฏิบัติ

ทั้งนี้ ผู้เขียนเห็นว่า แนวทางในการแก้ไขข้อท้าทายดังกล่าวขึ้นอยู่กับการพัฒนาขีดความสามารถทางเทคโนโลยีในการตามรอยสืบสวนหาที่มาย้อนหลังไปยังต้นกำเนิดของการโจมตีทางไซเบอร์ให้ทันกับเทคโนโลยีในการปกปิดร่องรอยที่มาการโจมตี การกำหนดกฎเกณฑ์ของกฎหมายระหว่างประเทศเรื่องความรับผิดของรัฐจากการโจมตีทางไซเบอร์ ตลอดจนการแสดงความรับผิดชอบต่อการโจมตีทางไซเบอร์ของฝ่ายที่ดำเนินการโจมตีทางไซเบอร์เองเท่านั้น

---

[374] Reuters, "Iran Says Cyber Foes Caused Centrifuge Problems," http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129. [April 8, 2016]

4.2.2 อุปสรรคในการบ่งชี้ว่าเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร

ดังที่ได้ศึกษามาแล้วว่าเงื่อนไขที่สำคัญของลักษณะการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศคือฝ่ายในการสู้รบจะต้องเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร โดยการให้ลักษณะการเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรสามารถพิจารณาจากปัจจัยบ่งชี้ซึ่งแสดงระดับของการจัดตั้งองค์กรหลายประการ

อย่างไรก็ตาม ด้วยลักษณะของการโจมตีทางไซเบอร์ที่แตกต่างกับการโจมตีด้วยอาวุธตามแบบ อาทิ การโจมตีทางไซเบอร์สามารถกระทำได้แม้ว่าจะทรัพยากรบุคคลน้อย ไม่จำต้องอาศัยบุคลากรจำนวนมากในการโจมตีเหมือนเช่นการโจมตีด้วยอาวุธตามแบบ นักรบไซเบอร์ (Cyber Warrior) ที่ดำเนินการโจมตีทางไซเบอร์จึงอาจประกอบไปด้วยสมาชิกที่มีจำนวนไม่มากพอที่จะต้องจัดตั้งกองบัญชาการหรือแบบแผนสายการบังคับบัญชา เนื่องจากการทำงานของนักรบไซเบอร์ส่วนใหญ่ไม่มีแบบแผนสายการบังคับบัญชา กฎระเบียบวินัย หรือการจัดตั้งกองบัญชาการที่ชัดเจน นักรบไซเบอร์สามารถปฏิบัติการโจมตีทางไซเบอร์จากประเทศหรือสถานที่แตกต่างกัน เป็นกลุ่มที่มีลักษณะเป็นองค์กรเสมือนจริงซึ่งสมาชิกของกลุ่มส่วนใหญ่จะไม่มีการติดต่อกันทางกายภาพแต่อย่างใด[375] ส่งผลให้การบ่งชี้ว่าเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรโดยใช้ปัจจัยเช่นเดียวกับการโจมตีด้วยอาวุธตามแบบทำให้การบ่งชี้ว่าเป็นกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กรอันเป็นเงื่อนไขหนึ่งในการพิจารณาการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศไม่สอดคล้องกับลักษณะของกลุ่มนักรบไซเบอร์

4.3 ข้อท้าทายเกี่ยวกับหลักการปฏิบัติการทางทหารและการให้ความคุ้มครองพลเรือนและทรัพย์สินของพลเรือน

จากการศึกษา พบว่าแม้กฎหมายมนุษยธรรมระหว่างประเทศจะยืดหยุ่นครอบคลุมในการบังคับใช้กับการโจมตีทางไซเบอร์ซึ่งเป็นวิธีการและปัจจัยในการสู้รบใหม่ แต่การใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศยังมีข้อท้าทายที่ส่งผลต่อประสิทธิภาพของการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศหลายประการ ดังนี้

---

[375] Michael Schmitt, "Classification of Cyber Conflict," Journal of Conflict & Security Law 17, no. 2 (2012). P. 256.

4.3.1 ข้อท้าทายเกี่ยวกับสถานะของบุคคลที่เข้าร่วมโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

จากการศึกษาในบทที่ 3 สถานะของบุคคลในสถานการณ์การขัดกันทางอาวุธเป็นสิ่งสำคัญอย่างยิ่งต่อการกำหนดสิทธิและหน้าที่ตามกฎหมายมนุษยธรรมระหว่างประเทศ โดยบุคคลที่ได้รับสถานะพลรบมีสิทธิเข้าร่วมในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธและอาจตกเป็นเป้าหมายในการโจมตีได้ รวมทั้งอาจได้รับสถานะเป็นเชลยศึกเมื่อถูกจับกุมในสถานการณ์การขัดกันทางอาวุธ ในขณะที่พลเรือนเป็นบุคคลที่กฎหมายมนุษยธรรมระหว่างประเทศมุ่งให้ความคุ้มครองตามกฎหมาย โดยพลเรือนไม่อาจตกเป็นเป้าหมายในการโจมตีทางไซเบอร์ได้ อย่างไรก็ตาม หากพลเรือนเข้าร่วมโดยตรงในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธย่อมทำให้พลเรือนสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศในฐานะพลเรือน และอาจตกเป็นเป้าหมายในการโจมตีได้เช่นเดียวกับพลรบ

จากการศึกษาลักษณะของการโจมตีทางไซเบอร์จะเห็นได้ว่าการโจมตีทางไซเบอร์มีลักษณะพิเศษแตกต่างจากการโจมตีด้วยอาวุธตามแบบหลายประการ ไม่ว่าจะเป็นวิธีการในการโจมตีที่ไม่อาจมองเห็นเป้าหมายในการโจมตีในระยะที่มองเห็น เป้าหมายในการโจมตีทางไซเบอร์ที่ไม่มีลักษณะทางกายภาพเช่น ระบบหรือเครือข่ายสารสนเทศ อาวุธไซเบอร์ที่ใช้ในการโจมตีซึ่งไม่ใช่อาวุธโดยสภาพในตัวเอง เป็นต้น ลักษณะพิเศษเหล่านี้ส่งผลให้เกิดข้อท้าทายเกี่ยวกับสถานะของบุคคลที่เข้าร่วมในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอย่างมีนัยสำคัญ ดังนี้

4.3.1.1 ข้อจำกัดเกี่ยวกับความจำเป็นของเงื่อนไขบางประการในการได้รับสถานะพลรบ

ด้วยลักษณะพิเศษของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่สามารถทำการโจมตีทางไซเบอร์จากสถานที่ใดก็ได้ ผู้โจมตีและเป้าหมายที่ถูกโจมตีไม่อยู่ในระยะที่สามารถมองเห็นกันได้ สามารถปฏิบัติการโจมตีโดยลำพัง ขนาดและจำนวนของกองทัพทหารไม่เป็นสิ่งที่ก่อให้เกิดความได้เปรียบในการสู้รบ บุคคลใดก็ตามที่มีความรู้ความสามารถทางเทคโนโลยีสามารถทำการโจมตีทางไซเบอร์ได้ทั้งสิ้น ไม่ว่าจะเป็นเด็ก ผู้ใหญ่ คนชรา หรือแม้แต่คนพิการที่ยังพอสามารถช่วยเหลือตนเองและใช้คอมพิวเตอร์ได้ก็สามารถทำการโจมตีทางไซเบอร์ได้ โดยที่ระยะทางหรือสภาพภูมิประเทศไม่เป็นอุปสรรคหรือตัวแปรสำคัญในการโจมตี นอกจากนี้ การโจมตีทางไซเบอร์เป็นการกระทำที่ดำเนินการภายในห้วงไซเบอร์ซึ่งเป็นสมรภูมิการรบที่ไม่มีลักษณะทางกายภาพ

ด้วยลักษณะพิเศษเหล่านี้ที่แตกต่างจากการโจมตีด้วยอาวุธตามแบบส่งผลให้เกิดข้อท้าทายเกี่ยวกับเงื่อนไขในการได้รับสถานะพลรบตามกฎหมายมนุษยธรรมระหว่างประเทศ

เนื่องจากเป็นการยากที่จะพิจารณาเงื่อนไขของการได้รับสถานะพลรบที่ชอบด้วยกฎหมายที่ได้รับสถานภาพเชลยศึกเมื่อถูกจับกุมภายใต้ข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3[376] กับพลรบที่ดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่จะต้องปฏิบัติตามเงื่อนไขข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 ในการมีเครื่องหมายที่กำหนดไว้อย่างเด่นชัด สามารถมองเห็นได้จากระยะไกล หรือถืออาวุธอย่างเปิดเผย เนื่องจากอาวุธไซเบอร์ ไม่ว่าจะเป็นมัลแวร์ ซอฟต์แวร์ ระบบโปรแกรมหรือเครือข่ายสารสนเทศไม่มีลักษณะทางกายภาพ แม้จะอยู่ในระยะที่สามารถมองเห็นได้ก็ไม่สามารถมองเห็นได้ว่าถืออาวุธไซเบอร์หรือมีเครื่องหมายที่กำหนดไว้ชัดเจนได้ ก่อให้เกิดข้อท้าทายในการพิจารณาเงื่อนไขการได้รับสถานะพลรบที่ชอบด้วยกฎหมายตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 ว่าเงื่อนไขดังกล่าวจำเป็นในการบังคับใช้กับการโจมตีทางไซเบอร์หรือไม่ พลรบที่ดำเนินการโจมตีทางไซเบอร์ หากไม่ทำการติดเครื่องหมายหรือสัญลักษณ์ที่กำหนดไว้อย่างชัดเจน มองเห็นได้จากระยะไกล หรือพลรบที่ไม่ถืออาวุธอย่างเปิดเผยขณะดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจะยังได้รับสถานะพลรบที่ชอบด้วยกฎหมายตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 หรือไม่

แนวทางในการแก้ไขข้อท้าทายข้างต้น เพื่อให้พลรบได้รับสถานภาพเชลยศึกเมื่อถูกจับกุมอาจทำได้โดยกำหนดให้พลรบดำเนินการโจมตีทางไซเบอร์ใดๆ กระทำผ่านระบบหรือ

---

[376] "Geneva Convention (Iii) Relative to the Treatment of Prisoners of War of 12 August 1949." Article 4 (A) (2)

"Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfil the following conditions:

(a) that of being commanded by a person responsible for his subordinates;

(b) that of having a fixed distinctive sign recognizable at a distance;

(c) that of carrying arms openly;

(d) that of conducting their operations in accordance with the laws and customs of war."

คอมพิวเตอร์ทางทหารโดยเฉพาะที่สามารถระบุและแสดงไอพี แอดเดรส (IP Address)[377] เท่านั้น โดยสมาชิกของกองกำลังทางทหารไม่ใช้เครื่องคอมพิวเตอร์ส่วนตัวในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อให้ทราบว่าการโจมตีทางไซเบอร์นั้นเป็นการกระทำที่มาจากกองกำลังทางทหาร โดยพิจารณาการแสดง IP Address เสมือนเป็นการถืออาวุธอย่างติดตัวซึ่งพลรบที่โจมตีทางไซเบอร์จาก IP Address ทางทหารอาจพิจารณาว่าได้ปฏิบัติตามเงื่อนไขการถืออาวุธอย่างติดตัวตามมข้อ4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 แล้ว

เนื่องจากวัตถุประสงค์ของเงื่อนไขดังกล่าวกำหนดขึ้นเพื่อขจัดความสับสนในการแยกแยะระหว่างพลรบและพลเรือน รวมทั้งป้องกันการหลอกลวง[378] จึงกำหนดให้พลรบติดเครื่องหมายหรือสัญลักษณ์แยกแยะที่อาจสังเกตเห็นได้และการพกอาวุธอย่างเปิดเผย เมื่อพิจารณาจากวัตถุประสงค์ของเงื่อนไขดังกล่าวแล้ว พลรบที่ดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธผ่านทาง IP Address หรือเซิร์ฟเวอร์ (Server) ทางการทหารโดยเฉพาะน่าจะถือได้ว่าเป็นการกระทำที่ขาดเจตนาที่จะหลอกลวงหรือขาดเจตนาที่จะก่อให้เกิดความสับสนว่าเป็นพลเรือนอาจถือว่าได้ปฏิบัติตามเงื่อนไขในการมีเครื่องหมายที่กำหนดไว้อย่างเด่นชัด สามารถมองเห็นได้จากระยะไกล หรือถืออาวุธอย่างเปิดเผยตามข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 แล้วและอาจได้รับสถานภาพเชลยศึกเมื่อถูกจับกุมขณะดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ นอกจากนี้ เมื่อเปรียบเทียบกับการโจมตีด้วยอาวุธตามแบบ กรณีสมาชิกของกองกำลังทางทหารบนเรือรบหรืออากาศยานรบที่ไม่ได้สวมเครื่องแบบ หรือติดเครื่องหมายที่กำหนดไว้และเข้ามีส่วนร่วมในการสู้รบสมาชิกของกองกำลังทหารเหล่านั้นยังคงได้รับสถานะพลรบอยู่แม้จะไม่ได้สวมเครื่องแบบหรือติดเครื่องหมายที่ถูกต้องก็ตาม[379] ดังนั้น พลรบที่ทำการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่ได้สวมเครื่องแบบหรือมีเครื่องหมายที่กำหนดไว้อย่างเด่นชัดสามารถมองเห็นได้จากระยะไกลย่อมยังคงได้รับสถานะพลรบเช่นเดียวกัน

---

[377] IP Address ย่อมาจากคำเต็มว่า Internet Protocal Address คือหมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP

[378] Sean Watts, "Combatant Status and Computer Network Attack," Virginia Journal of International Law 50, no. 2 (2010). P. 432.

[379] Knut Ipsen, "Combatants and Non-Combatants," in *The Handbook of Humanitarian Law in Armed Conflicts*, ed. Dieter Fleck(Oxford University Press, 1999). P. 101.

4.3.1.2 การตีความคำว่า "มีส่วนร่วมโดยตรงในการสู้รบ" ที่ส่งผลให้สูญเสียสถานะพลเรือน

การเข้ามีส่วนร่วมโดยตรงในการสู้รบของพลเรือน (Direct Participation by Civilians) ส่งผลให้พลเรือนสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศไปทันทีและตราบเท่าที่พลเรือนเข้ามีส่วนร่วมโดยในการสู้รบ ซึ่งขอบเขตของการเข้ามีส่วนร่วมโดยตรงในการสู้รบตามข้อ 51 (3) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ยังไม่มีคำจำกัดความ[380] หรือการกำหนดขอบเขตของการกระทำหรือระยะเวลาที่ชัดเจนขึ้นอยู่กับการตีความการเข้ามีส่วนร่วมโดยตรงในการสู้รบเป็นรายกรณีไป แม้ว่าจะมีคำอธิบายพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ของคณะกรรมการกาชาดระหว่างประเทศ[381] และคำแนะนำเกี่ยวกับการตีความว่าด้วยการเข้ามีส่วนร่วมโดยตรงในการสู้รบของคณะกรรมการกาชาดระหว่างประเทศ[382] การให้ความชัดเจนในกรณีดังกล่าวก็ไม่ได้ข้อสรุปที่ชัดเจน โดยคณะกรรมการกาชาดระหว่างประเทศระบุว่าการพิจารณาเกี่ยวกับการเข้ามีส่วนร่วมโดยตรงในการสู้รบของพลเรือนขึ้นอยู่กับความหลากหลายของปัจจัยในแต่ละสถานการณ์ซึ่งไม่สามารถอธิบายได้อย่างครอบคลุมเป็นรูปธรรมได้ตามคำแนะนำเกี่ยวกับการตีความว่าด้วยการเข้ามีส่วนร่วมโดยตรงในการสู้รบ[383] ด้วยเหตุดังกล่าว การพิจารณาลักษณะการกระทำของพลเรือนที่เข้ามีส่วนร่วมโดยตรงในการโจมตีทางไซเบอร์ซึ่งส่งผลให้สูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศยังไม่มีความชัดเจนขึ้นอยู่กับการตีความแต่ละรายกรณีไปเช่นเดียวกัน

ความเชื่อมต่อระหว่างเทคโนโลยีที่ใช้ในทางทหารกับทางพลเรือนส่งผลให้พลเรือนอาจมีส่วนร่วมในการโจมตีทางไซเบอร์ได้อย่างง่ายดาย ไม่ว่าจะเป็นผู้ให้บริการ ผู้พัฒนาระบบหรือโปรแกรม แม้กระทั่งพลเรือนที่ใช้ระบบหรือเครือข่ายอินเทอร์เน็ตซึ่งติดตั้งอยู่ภายในที่พักอาศัยของตนเองอาจเข้ามีส่วนร่วมในการโจมตีทางไซเบอร์ได้โดยไม่รู้ตัว หากคอมพิวเตอร์ที่ใช้งานอยู่ติดเชื้อ

---

[380] Teerapat Asavasungsidhi (Thai Translation), "กฎหมายจารีตประเพณี Customary Law," International Review of the Red Cross 87, no. 857 (2005). หน้า 17.

[381] Jean DE PREUX Claude PILLOUDt, Yves SANDOZ, Bruno ZIMMERMANN, Philippe Eberlin, Hans-Peter Gasser and Claude F. Wenger "Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949," ed. ICRC(Netherlands Martinus Nijhoff Publishers 1987). P. 618.

[382] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, vol. ICRC(90 IRRC 991 (2008), Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009) P. 65.

[383] Ibid.

(Zombies) และเป็นส่วนหนึ่งในอีกคอมพิวเตอร์อีกหลายๆ เครื่องที่ใช้ในการโจมตีทางไซเบอร์ด้วยวิธีการทำให้ระบบปฏิเสธการให้บริการหรือดีดีโอเอส เป็นต้น

ประเด็นดังกล่าวนี้ ผู้เขียนเห็นว่า รัฐอาจหลีกเลี่ยงข้อท้าทายดังกล่าวได้ โดยการพัฒนาขีดความสามารถทางด้านเทคโนโลยีไซเบอร์ของกองทัพให้แก่สมาชิกของกองทัพและกำหนดให้สมาชิกของกองทัพที่มีความรู้ความสามารถ มีทักษะและความเชี่ยวชาญเกี่ยวกับการโจมตีทางไซเบอร์ให้มีหน้าที่เป็นผู้กระทำการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธโดยเฉพาะแทนการว่าจ้างพลเรือนในการทำหน้าที่เกี่ยวกับการดำเนินการโจมตีทางไซเบอร์ในสถานการณ์ในการขัดกันทางอาวุธซึ่งอาจทำให้พลเรือนสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศจากการเข้าร่วมโดยตรงในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้ รวมทั้งการเลือกใช้วิธีการและปัจจัยในการโจมตีทางไซเบอร์ที่สามารถโจมตีต่อเป้าหมายได้อย่างเฉพาะเจาะจง ไม่แพร่กระจายเข้าสู่ระบบหรือเครือข่ายของพลเรือน

ตลอดจนการส่งเสริมให้พลเรือนมีความรู้ความเข้าใจเกี่ยวกับหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศเพื่อมิให้พลเรือนเข้าไปมีส่วนร่วมโดยตรงในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ทำให้พลเรือนสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศและอาจตกเป็นเป้าหมายในการโจมตีได้โดยชอบด้วยกฎหมาย

อย่างไรก็ดี พลเรือนควรตระหนักรู้ถึงโอกาสและความเสี่ยงที่ตนเองจะเข้าไปมีส่วนร่วมโดยตรงในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยพลเรือนสามารถป้องกันตนเองไม่ให้เป็นส่วนหนึ่งในการโจมตีทางไซเบอร์ได้ จากการหมั่นศึกษาหาความรู้ทางด้านไซเบอร์ ไม่ใช้ระบบหรือโปรแกรมซอฟต์แวร์เถื่อนที่ทำให้เครื่องคอมพิวเตอร์มีโอกาสติดเชื้อได้ง่าย ใช้ซอฟต์แวร์ของแท้ และหมั่นทำการอัพเดทความปลอดภัยของคอมพิวเตอร์ เพื่อป้องกันมิให้คอมพิวเตอร์ของตนเองกลายเป็นคอมพิวเตอร์ติดเชื้อและแพร่กระจายต่อไป

4.3.2 ปัญหาเนื่องมาจากเทคโนโลยีที่ใช้ได้สองทาง

จากการพัฒนาทางเทคโนโลยีทางไซเบอร์ที่นำไปใช้งานทั้งในกิจการพลเรือนและทางทหาร ความเชื่อมต่อกันระหว่างระบบหรือเครือข่ายที่ใช้ในทางทหารและทางพลเรือน ทำให้เกิดข้อท้าทายที่สำคัญในการดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธให้สอดคล้องกับหลักการเกี่ยวกับปฏิบัติการทางทหารโดยเฉพาะหลักการพื้นฐานการแยกแยะเป้าหมาย ดังนี้

คำว่า เป้าหมายที่ใช้ได้สองทาง (Dual-use Target) ไม่ใช่คำนิยามในทางกฎหมายมนุษยธรรมระหว่างประเทศ เป็นคำที่นิยมใช้อย่างหลากหลายเพื่ออ้างถึงทรัพย์สินหรือวัตถุสิ่งของที่พลเรือนและทหารใช้ร่วมกัน[384] จากการศึกษาวิเคราะห์เกี่ยวกับการนำหลักการปฏิบัติการทางทหารบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ฝ่ายในการสู้รบมีหน้าที่ในการแยกแยะระหว่างพลเรือนและพลรบ เป้าหมายทางทหารและทรัพย์สินของพลเรือนตลอดเวลาที่ดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธตามหลักการพื้นฐานการแยกแยะเป้าหมายซึ่งเมื่อพิจารณาจากลักษณะเป้าหมายในการโจมตีทางไซเบอร์ได้แก่ ระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์อันมีลักษณะเป็นเป้าหมายที่ใช้ได้สองทาง (Dual-use Target) จากการมีวัตถุประสงค์เพื่อใช้ในกิจการของพลเรือน ในขณะเดียวกันก็มีลักษณะเป็นเป้าหมายทางทหารซึ่งสามารถถูกโจมตีโดยชอบด้วยกฎหมายได้ด้วยเช่นกัน

เทคโนโลยีทางคอมพิวเตอร์ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ส่วนใหญ่มีลักษณะการใช้ได้สองทาง (Dual-use) ระบบหรือเครือข่ายบางอย่าง ถูกออกแบบมาเพื่อใช้ในกิจการทหาร ต่อมาถูกผสมผสานให้ใช้ในกิจการของพลเรือน ระบบหรือเครือข่ายดังกล่าวเมื่อถูกรบกวนหรือขัดขวางการใช้งานโดยการโจมตีทางไซเบอร์อาจก่อให้เกิดผลกระทบรุนแรงต่อพลเรือนได้ เช่น ระบบกำหนดตำแหน่งบนโลก หรือระบบจีพีเอส (Global Positioning Systems-GPS) เริ่มแรกเป็นระบบที่พัฒนาขึ้นเพื่อใช้ในทางการทหารของสหรัฐอเมริกากลายเป็นถูกผสมผสานเข้าสู่การประยุกต์ใช้ในทางทางพลเรือนอย่างหลากหลายจากการควบคุมการจราจรทางอากาศไปถึงโทรศัพท์เคลื่อนที่และคอมพิวเตอร์แบบพกพาหรือแล็ปท็อป (Laptops) แม้แต่ในเครือข่ายอินเตอร์เน็ตก็ตาม การขัดขวางการให้บริการระบบกำหนดตำแหน่งบนโลก หรือระบบจีพีเอส โดยการก่อกวน (Jamming) การปิดกั้น (Blocking) หรือการปลอมแปลง (Spoofing) สัญญาณจีพีเอสผ่านทางการโจมตีทางไซเบอร์อาจก่อให้เกิดการหยุดชะงักขนาดใหญ่ของระบบและอาจเกิดอันตรายขึ้นต่อชีวิตของพลเรือนได้[385]

ประเด็นเป้าหมายที่ใช้ได้สองทาง (Dual-use Targets) กลายเป็นข้อท้าทายที่สำคัญเกี่ยวกับการบังคับใช้หลักความได้สัดส่วนในการโจมตี เนื่องจากเป้าหมายที่ใช้ได้สองทางซึ่งมีความเกี่ยวพันกันของทรัพย์สินของพลเรือนและเป้าหมายทางทหาร การโจมตีต่อระบบหรือเครือข่ายที่มีลักษณะเป็น

---

[384] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (the United States of America: Cambridge University Press, 2012).P. 193.

[385] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*. P. 194.

เป้าหมายที่ใช้ได้สองทาง อาจทำให้ได้รับความได้เปรียบทางทหารจากการทำลายคุณค่าของเป้าหมายทางทหาร ในขณะเดียวกัน การโจมตีดังกล่าวก็ส่งผลกระทบต่อพลเรือนได้ด้วยเช่นกัน[386]

ลักษณะความเชื่อมต่อระหว่างระบบหรือเครือข่ายของพลเรือนกับระบบหรือเครือข่ายที่ในทางทหารทำให้เกิดข้อท้าทายเกี่ยวกับหลักปฏิบัติการทางทหารมากมาย อาทิ ความยากลำบากของฝ่ายในการสู้รบที่ดำเนินการโจมตีทางไซเบอร์ในการแยกแยะเป้าหมายระหว่างเป้าหมายทางทหารกับทรัพย์สินของพลเรือน การประเมินผลกระทบทางอ้อมที่เกิดขึ้นต่อเครือข่ายของพลเรือนจากการโจมตีเครือข่ายทางทหาร เป็นต้น[387]

จะเห็นได้ว่า ลักษณะเทคโนโลยีที่ใช้ได้สองทางส่งผลกระทบอย่างมากต่อหลักการแยกแยะเป้าหมายซึ่งกำหนดให้ฝ่ายในการสู้รบมีหน้าที่ในการแยกแยะระหว่างเป้าหมายทางทหารและทรัพย์สินของพลเรือนตลอดเวลาในสถานการณ์การขัดกันทางอาวุธ โดยทรัพย์สินของพลเรือนจะต้องได้รับความคุ้มครองตามกฎหมายไม่ตกเป็นเป้าหมายในการโจมตีด้วยอาวุธตามแบบรวมทั้งการโจมตีทางไซเบอร์ด้วย การโจมตีทางไซเบอร์ต่อเป้าหมายที่ใช้ได้สองทางอาจพิจารณาได้ว่าเป็นการฝ่าฝืนหลักการแยกแยะเป้าหมายตามกฎหมายมนุษยธรรมระหว่างประเทศได้ ฝ่ายในการสู้รบจึงจำเป็นที่จะต้องพิจารณาผลกระทบที่อาจเกิดขึ้นต่อพลเรือน (Collateral Damage) ไม่ว่าจะเป็นการบาดเจ็บหรือเสียชีวิตหรือความเสียหายต่อทรัพย์สินของพลเรือนที่เกิดขึ้นโดยไม่ตั้งใจประกอบในการกำหนดเป้าหมายทางทหาร

ทั้งนี้ ผู้เขียนเห็นว่า แม้ว่าเป้าหมายในการโจมตีทางไซเบอร์นั้นจะมีลักษณะเป็นเป้าหมายทางทหารอย่างแท้จริง การโจมตีทางไซเบอร์ต่อเป้าหมายดังกล่าว ฝ่ายในการสู้รบควรประเมินผลกระทบต่อพลเรือนที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธประกอบ หากประเมินได้ว่าผลกระทบต่อพลเรือนจากการโจมตีทางไซเบอร์นั้นจะมีมากเกินกว่าความได้เปรียบทางทหาร ฝ่ายในการสู้รบควรหลีกเลี่ยงการโจมตีทางไซเบอร์ต่อเป้าหมายทางทหารดังกล่าวหรือ

---

[386] Michael N. Schmitt, "Targeting and Humanitarian Law: Current Issues," *International Law Studies* 80, no. International Law and Military Operations (2004). P. 155.

[387] "Weapons: ICRC Statement to the United Nations, 2013," https://www.icrc.org/eng/resources/documents/statement/2013/united-nations-weapons-statement-2013-10-16.htm. [December 12, 2015]

หากจำเป็นที่จะต้องโจมตีทางไซเบอร์ต่อเป้าหมายทางทหารนั้น ฝ่ายในการสู้รบควรที่จะเลือกใช้วิธีการหรือปัจจัยในการโจมตีทางไซเบอร์ที่สามารถควบคุมและจำกัดผลกระทบให้ได้มากที่สุด

4.3.3 การพิจารณาผลกระทบแบบ Knock-on

ในการบังคับใช้หลักความได้สัดส่วนในการโจมตีตามกฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธกำหนดให้ฝ่ายในการสู้รบมีหน้าที่ในการประเมินชั่งน้ำหนักระหว่างความได้เปรียบทางทหารที่คาดว่าจะได้รับจากการโจมตีทางไซเบอร์กับผลกระทบต่อพลเรือนที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ซึ่งเมื่อพิจารณาจากลักษณะของการโจมตีทางไซเบอร์ที่ไม่ปรากฏความเสียหายของเป้าหมายในทันทีหรือเวลาไล่เลี่ยกับที่มีการโจมตีทางไซเบอร์ อีกทั้งลักษณะความเชื่อมต่อของเทคโนโลยีที่ใช้ในทางการทหารและเทคโนโลยีของพลเรือน โดยไม่สามารถแบ่งแยกได้ชัดเจนภายในห้วงไซเบอร์ก่อให้เกิดข้อท้าทายเกี่ยวกับผลกระทบแบบ Knock-on หรือ Knock-on Effects อันเป็นผลกระทบที่ไม่ได้เกิดขึ้นจากการโจมตีโดยตรงและไม่ได้เกิดขึ้นทันที เป็นผลกระทบที่เกิดขึ้นชั้นที่ 2 หรือชั้นที่ 3 ของการโจมตี เป็นปัญหาในทางปฏิบัติเกี่ยวกับการคาดการณ์ล่วงหน้าถึงผลกระทบที่ตามมาภายหลัง หรือผลกระทบที่สะท้อนกลับ (Reverberating Consequences)

ตัวอย่าง ผลกระทบแบบ Knock-on ที่สำคัญคือเหตุการณ์ The Gulf War ในปี ค.ศ. 1990-1991[388] เป็นตัวอย่างเหตุการณ์สำคัญที่ผลกระทบแบบ Knock-on ของการโจมตีก่อให้เกิดอันตรายต่อพลเรือนมากกว่าผลกระทบโดยตรงของการโจมตีเอง[389] จากการที่พันธมิตรบุกโจมตีทางอากาศและทางเรือต่อเป้าหมายทางทหาร ซึ่งแม้การโจมตีนั้นจะประสบความสำเร็จในการรบกวนการทำงานของศูนย์สั่งการและควบคุมของอิรัก แต่ก็เป็นการตัดไฟฟ้าของพลเรือนทั่วไปด้วย ซึ่งส่งผลกระทบต่อการทำงานของโรงพยาบาล ระบบรักษาความปลอดภัย เป็นต้น เช่นเดียวกับการทิ้งระเบิดโจมตีต่อหม้อแปลงจ่ายกระแสไฟฟ้าของยูโกสลาเวียในปฏิบัติการ Allied Force ของ

---

[388] Yoram Dinstein, "Discussion," in *Legal and Ethical Lessons of Nato's Kosovo Campaign*, ed. Andru E. Wall(Newport: Naval War College, 2002). P. 219.

การโจมตีต่อโครงข่ายไฟฟ้า (Electrical Grid) ของอิรักโดยกองกำลังพันธมิตรในปีค.ศ. 1990-1991 ไม่เพียงแต่ก่อให้เกิดความได้เปรียบทางทหารจากการปิดสถานีเรดาร์ทางทหาร คอมพิวเตอร์ทางทหาร แต่ยังสร้างความเสียหายเป็นบริเวณกว้างต่อพลเรือนจากการที่โรงพยาบาลไม่สามารถปฏิบัติงานได้ ระบบสูบน้ำหยุดทำงาน

[389] Christopher Greenwood, "The Law of Weaponry at the Start of the New Millennium," International Law Studies 71(1998). P. 202.

องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ โดยองค์การสนธิสัญญาป้องกันแอตแลนติกเหนืออ้างว่ากำหนดเป้าหมายไปที่หม้อแปลงจ่ายกระแสไฟฟ้า แต่การโจมตีดังกล่าวส่งผลให้สถานีสูบน้ำดื่มบริโภคของยูโกสลาเวียปิดตัวลง[390]

จากความใกล้ชิดและเชื่อมต่อกันของระบบและเครือข่ายทางทหารและพลเรือน ทำให้การเกิดผลกระทบแบบ Knock-on เป็นปัญหาในการพิจารณาหลักความได้สัดส่วนและหลักการใช้ความระมัดระวังในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่อาจก่อให้เกิดผลกระทบแบบ Knock-on ได้ด้วยเช่นกันด้วย โดยผลกระทบแบบ Knock-on ของการโจมตีต่อระบบเครือข่ายคอมพิวเตอร์เกิดขึ้นย่อมส่งผลกระทบในวงกว้างได้มากกว่าการโจมตีโดยอาวุธโดยทั่วไป

ผลกระทบแบบ Knock- on นี้ก่อให้เกิดข้อท้าทายเกี่ยวกับหน้าที่ในการปฏิบัติตามหลักความได้สัดส่วนในการโจมตีและการใช้ความระมัดระวังล่วงหน้าซึ่งฝ่ายในการสู้รบจะต้องพิจารณาถึงผลกระทบต่อพลเรือนจากการโจมตีทางไซเบอร์ โดยยังไม่มีความชัดเจนถึงระดับของผลกระทบที่ผู้วางแผนโจมตีจะต้องพิจารณาคาดการณ์ล่วงหน้าถึงผลกระทบในระดับใด การพิจารณาผลกระทบแบบ Knock-on ชั้นที่ 2 หรือ 3 จะถือว่าฝ่ายในการสู้รบได้คาดการณ์ล่วงหน้าถึงผลกระทบที่ตามมาอย่างเพียงพอหรือไม่

กล่าวคือ หน้าที่ในการใช้ความระมัดระวังในการโจมตีซึ่งกำหนดให้ผู้บัญชาการ ผู้วางแผนหรือผู้ตัดสินใจในการโจมตีของฝ่ายในการสู้รบจะต้องพิจารณาระบุเป้าหมายในการโจมตี โดยเป้าหมายในการโจมตีนั้นจะต้องเป็นเป้าหมายทางทหารเท่านั้น ประชากรพลเรือนและทรัพย์สินของพลเรือนจะเป็นเป้าหมายในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้นไม่ได้ตามข้อ 57 (2) (เอ) (i)) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ก่อให้เกิดข้อท้าทายเกี่ยวกับการรวบรวมข้อมูลประกอบการระบุเป้าหมายของผู้วางแผนหรือผู้ตัดสินใจ ซึ่งจะต้องอาศัยข้อมูลจากทุกแหล่งที่มาในการระบุเป้าหมาย และจะต้องเป็นข้อมูลที่ได้จากการประเมินของผู้ที่มีความรู้ความสามารถทางด้านไซเบอร์โดยเฉพาะ ฝ่ายในการสู้รบอาจจะต้องจัดตั้งหน่วยรวบรวมข้อมูล

[390] BBC, "Nato Denies Targeting Water Supplies " http://news.bbc.co.uk/2/hi/europe/351780.stm. Available at http://news.bbc.co.uk/2/hi/europe/351780.stm [May 15, 2016]

ทางด้านไซเบอร์โดยเฉพาะ เพื่อให้การระบุเป้าหมายตามหลักการใช้ความระมัดระวังในการโจมตีเป็นไปตามกฎหมายมนุษยธรรมระหว่างประเทศมากที่สุด

นอกจากนี้ กฎหมายมนุษยธรรมระหว่างประเทศยังกำหนดหน้าที่เกี่ยวกับการใช้ความระมัดระวังล่วงหน้าเท่าที่เป็นไปได้ในการเลือกวิธีการและปัจจัยในการโจมตี เพื่อหลีกเลี่ยงและอย่างน้อยเพื่อลดความสูญเสีย บาดเจ็บของพลเรือนและความเสียหายต่อทรัพย์สินของพลเรือนตามข้อ 57 (2) (เอ) (ii) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ฉบับที่ 1 ส่งผลให้ผู้วางแผนหรือผู้ตัดสินใจจะโจมตีทางไซเบอร์จะต้องอาศัยความรู้ความเชี่ยวชาญทางด้านไซเบอร์ หรือผู้ที่มีความรู้ความเชี่ยวชาญทางด้านไซเบอร์ในการพิจารณาเลือกวิธีการหรือปัจจัยในการโจมตีทางไซเบอร์แต่ละครั้งด้วยเช่นกัน

สำหรับการบังคับใช้หลักการทั่วไปเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธนั้น จะเห็นได้ว่า การโจมตีทางไซเบอร์เป็นวิธีการและปัจจัยในการสู้รบที่สอดคล้องกับหลักการข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบยิ่งไปกว่ากว่าการโจมตีด้วยอาวุธตามแบบเสียอีก จากการที่ลักษณะของการโจมตีทางไซเบอร์ซึ่งเป็นการกระทำโดยใช้เทคโนโลยีไซเบอร์มุ่งโจมตีต่อระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์ของเป้าหมายเพื่อให้ปรับเปลี่ยน ขัดข้อง ถูกรบกวน ทำให้ใช้การไม่ได้หรือทำลายซึ่งระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์ของฝ่ายตรงข้าม ลักษณะของการโจมตีทางไซเบอร์ไม่ได้เป็นวิธีการหรือปัจจัยในการสู้รบที่มุ่งทำให้เกิดการบาดเจ็บหรือเสียชีวิตของบุคคลแต่อย่างใด

กรณีการใช้เทคโนโลยีไซเบอร์ในฐานะปัจจัยในการสู้รบ (Means of Warfare) ในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่อาจฝ่าฝืนต่อหลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานเกินความจำเป็นในปัจจุบันมีโอกาสเกิดขึ้นได้น้อยมาก เนื่องจากลักษณะอาวุธไซเบอร์ที่ใช้ในการทำลายเป้าหมายนั้น โดยตัวของอาวุธไซเบอร์เองไม่ก่อให้เกิดการบาดเจ็บหรือเสียชีวิตของบุคคล ไม่ว่าจะเป็นมัลแวร์ ระบบโปรแกรมหรือเครือข่ายทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์ กล่าวได้ว่า การโจมตีทางไซเบอร์เป็นทางเลือกที่น่าสนใจของฝ่ายในการสู้รบ ในการเลือกใช้อาวุธในการสู้รบ (Means of Warfare) เช่น หากต้องการที่จะขจัดความสามารถของฝ่ายตรงข้าม โดยการระเบิดโรงงานผลิตกระแสไฟฟ้าที่ใช้ทางทหาร ฝ่ายในการสู้รบอาจเลือกใช้อาวุธไซเบอร์ในการโจมตีทางไซเบอร์เพื่อปิดระบบการผลิตกระแสไฟฟ้าแทนการทิ้งระเบิดโรงงานผลิตกระแสไฟฟ้าที่อาจก่อให้เกิดการบาดเจ็บหรือความทุกข์ทรมานโดยไม่จำเป็นได้

อย่างไรก็ตาม การใช้เทคโนโลยีไซเบอร์ในฐานะวิธีการในการสู้รบ (Methods of Warfare) ในการโจมตีทางไซเบอร์อาจก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็นได้ เช่น การโจมตีทางไซเบอร์โดยควบคุมระบบการช็อตด้วยไฟฟ้ากระตุ้นการเต้นของหัวใจ (Defibrillation) เพื่อทำให้หัวใจหยุดเต้น โดยตั้งใจที่จะทำให้เกิดความเจ็บปวดและความทุกข์ทรมานเพิ่มมากขึ้นเพื่อวัตถุประสงค์ของตนเองที่ไม่เกี่ยวข้องหรือมากเกินไปกว่าเพื่อให้บรรลุผลในการโจมตีเป้าหมายทางทหาร[391] หรือหากในอนาคต มีการนำเครื่องมือหรืออุปกรณ์ซึ่งควบคุมจากระยะไกลด้วยระบบหรือเครือข่ายสารสนเทศที่มีลักษณะในการใช้งานจะต้องใช้งานอย่างติดตัวพลรบคล้ายการใช้เทคโนโลยีบลูทูธ (Bluetooth Technology) หากฝ่ายในการสู้รบเลือกใช้วิธีการโจมตีทางไซเบอร์ต่อเทคโนโลยีที่ติดตัวพลรบอยู่ เพื่อทำให้อุปกรณ์ทำงานขัดข้องทำลายตัวเองหรือระเบิดออกในขณะที่ติดตัวพบรบ โดยมีเจตนาให้พลรบได้รับการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็น ทั้งที่สามารถเลือกใช้วิธีการโจมตีทางไซเบอร์อื่นที่ทำให้เทคโนโลยีติดตัวพลรบไม่สามารถใช้งานได้หรือไม่สามารถติดต่อกับกองบัญชาการได้ การเลือกใช้วิธีการโจมตีทางไซเบอร์ดังกล่าวย่อมเป็นการขัดต่อหลักการห้ามใช้วิธีการและปัจจัยในการสู้รบก่อให้เกิดการบาดเจ็บเกินขนาดหรือความทุกข์ทรมานโดยไม่จำเป็น

ในส่วนข้อท้าทายทางกฎหมายของหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะได้ (Incriminate Weapons) เมื่อพิจารณาลักษณะของอาวุธไซเบอร์ต่างๆ แล้ว ในปัจจุบันยังไม่พบข้อท้าทายในการบังคับใช้หลักการดังกล่าวกับการโจมตีทางไซเบอร์แต่อย่างใด โดยข้อท้าทายเกี่ยวกับการบังคับใช้หลักการนี้เป็นข้อท้าทายในทางปฏิบัติ กล่าวคือ ความรู้ความสามารถ ทักษะความเชี่ยวชาญทางด้านไซเบอร์ของฝ่ายในการสู้รบ ทั้งผู้บัญชาการที่มีอำนาจในการตัดสินใจดำเนินการโจมตีทางไซเบอร์ พลรบผู้ดำเนินการโจมตีทางไซเบอร์ ในการเลือกใช้เทคโนโลยีไซเบอร์ในการโจมตีที่สามารถแยกแยะเป้าหมายได้ เช่น สตักซ์เน็ต (Stuxnet) ที่ออกแบบมาให้สามารถกำหนดเงื่อนไขในการจู่โจมเพื่อให้มั่นใจว่าระบบหรือส่วนของซอฟต์แวร์หรือข้อมูลของระบบที่ถูกโจมตีนั้น เป็นระบบทางทหารที่ต้องการโจมตี ตลอดจนการพัฒนาเทคโนโลยีไซเบอร์ของกองทัพในอนาคตที่สามารถโจมตีต่อเป้าหมายได้อย่างเฉพาะเจาะจงหรือก่อให้เกิดผลที่สามารถควบคุมได้เช่นเดียวกับสตักซ์เน็ต

[391] Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts ed. Michael N. Schmitt(Cambridge University Press, 2013). P.144.

กล่าวได้ว่า การโจมตีทางไซเบอร์เป็นวิธีการและปัจจัยในการสู้รบที่เป็นทางเลือกที่ดีของฝ่ายในการสู้รบในการเลือกใช้อาวุธ วิธีการหรือปัจจัยในการสู้รบที่สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศ เพื่อหลีกเลี่ยงปฏิบัติการทางทหารที่อาจฝ่าฝืนกับหลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็น หรือหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้ ข้อท้าทายอย่างเดียวสำหรับการใช้หลักการเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบกับการโจมตีทางไซเบอร์คงอยู่ที่ความรู้ความสามารถเฉพาะทางด้านเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของฝ่ายในการสู้รบที่จะเลือกใช้วิธีการหรือปัจจัยในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธว่ามีทักษะ ความรู้ความสามารถ ความเชี่ยวชาญเพียงพอที่จะเลือกอาวุธไซเบอร์หรือดำเนินการโจมตีทางไซเบอร์ที่ไม่ขัดต่อหลักการทั่วไปเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบตามกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่

4.3.4 ความรู้ความสามารถทางด้านเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์ของฝ่ายในการสู้รบ

โดยทั่วไป กองกำลังทางทหารของประเทศที่เจริญแล้ว มีแนวโน้มที่จะไม่ทำการโจมตีต่อเป้าหมายพลเรือนโดยตั้งใจ อย่างไรก็ตาม โอกาสของเหตุการณ์การโจมตีโดยไม่เลือกเป้าหมายก็เกิดขึ้นได้ แม้จะเป็นกองกำลังทางทหารที่มีความก้าวหน้าทางเทคโนโลยีแล้วก็ตาม ยกตัวอย่างเช่น การปล่อยในที่ลับตาเหนือดินแดนของฝ่ายตรงข้ามในการสู้รบของการทิ้งระเบิดโดยเครื่องบินทหารซึ่งพลาดหรือไม่สามารถถึงเป้าหมายทางทหาร หากการห้ามโจมตีโดยไม่เลือกเป้าหมายจะสำเร็จได้อย่างสมบูรณ์นั้นต้องอาศัยการฝึกอบรมทางการทหารอย่างเข้มงวด และวินัยที่เคร่งครัดเป็นอย่างมาก เช่นเดียวกันกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

เพื่อหลีกเลี่ยงการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ฝ่าฝืนหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ ผู้วางแผนหรือผู้ตัดสินใจที่จะโจมตี จะต้องอาศัยข้อมูลผลกระทบจากการโจมตีทางไซเบอร์ที่เพียงพอประกอบการพิจารณาการเลือกใช้วิธีการและปัจจัยในการโจมตีทางไซเบอร์ ตลอดจนพลรบที่ทำการโจมตีทางไซเบอร์จะต้องอาศัยความรู้ความเชี่ยวชาญทางด้านเทคโนโลยีเพิ่มเติมจากการฝึกอบรมทางทหารอย่างเข้มงวดและวินัยที่เคร่งครัด เพื่อให้สามารถเลือกใช้วิธีการหรือปัจจัยในการโจมตีทางไซเบอร์ที่สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศและเกิดผลกระทบต่อพลเรือนผู้บริสุทธิ์ในทางที่น้อยที่สุด

ในส่วนของการให้ความคุ้มครองพิเศษแก่ทรัพย์สินบางประเภทตามการศึกษาวิจัยในเล่มนี้ ล้วนเป็นทรัพย์สินที่ได้รับความคุ้มครองพิเศษตามกฎหมายมนุษยธรรมระหว่างประเทศและเป็นทรัพย์สินที่มีการพึ่งพาเทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการควบคุมดูแลการทำงานของทรัพย์สินเหล่านั้นเพิ่มมากขึ้น ไม่ว่าจะเป็นสิ่งติดตั้งที่บรรจุพลังงานอันตราย ได้แก่ เขื่อน ฝาย โรงไฟฟ้าพลังงานนิวเคลียร์ที่มีการนำเทคโนโลยีไซเบอร์ไปใช้ในการควบคุม วัตถุอันจำเป็นในการดำรงชีวิตของประชากรพลเรือน อาทิ สถานที่เก็บและจ่ายน้ำดื่ม งานชลประทาน และโรงพยาบาลหรือหน่วยแพทย์อื่นๆ ซึ่งระบบที่ใช้ในการควบคุมดูแลการทำงานเหล่านั้น เป็นระบบที่สามารถเชื่อมต่อกับระบบที่ใช้ทางการทหารได้ ส่งผลให้ทรัพย์สินที่ได้รับความคุ้มครองพิเศษเหล่านั้นตกอยู่ในความเสี่ยงที่จะถูกโจมตีทางไซเบอร์ได้ และหากทรัพย์สินที่ได้รับความคุ้มครองพิเศษเหล่านี้ถูกโจมตีทางไซเบอร์อาจก่อให้เกิดความเสียหายอย่างใหญ่หลวงต่อประชากรพลเรือนได้เช่นเดียวกับการโจมตีด้วยอาวุธตามแบบก่อให้เกิดข้อท้าทายในการให้ความคุ้มครองแก่ทรัพย์สินเหล่านี้ในทางปฏิบัติ

แนวทางในการให้ความคุ้มครองพิเศษแก่ทรัพย์สินเหล่านี้ขึ้นอยู่กับความสามารถของฝ่ายในการสู้รบในการควบคุมจำกัดผลกระทบที่จะเกิดขึ้นจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธตลอดจนการเลือกใช้วิธีการและปัจจัยในการโจมตีทางไซเบอร์ที่สามารถโจมตีต่อเป้าหมายทางหทารได้อย่างเฉพาะเจาะจงและสามารถควบคุมผลกระทบตามหลักการให้ความคุ้มครองพลเรือนและทรัพย์สินพลเรือน นอกจากนี้ ฝ่ายในการสู้รบจะต้องไม่โจมตีทางไซเบอร์ต่อทรัพย์สินที่ได้รับความคุ้มครองพิเศษนี้อย่างเด็ดขาด ไม่ว่าจะด้วยวิธีการหรือปัจจัยในการสู้รบใดๆ มีความรุนแรงมากหรือน้อยเพียงใด แม้ว่าจะก่อให้เกิดความได้เปรียบทางทหารหรือทำให้การสู้รบยุติลงอย่างรวดเร็วก็ตาม

จากการศึกษาในส่วนของข้อท้าทายเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ จะเห็นได้ว่า ข้อท้าทายส่วนใหญ่สืบเนื่องมาจากลักษณะพิเศษของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่มีความเชื่อมต่อกันระหว่างระบบหรือเครือข่ายทางการทหารและพลเรือนอย่างใกล้ชิด ทำให้เกิดความยากลำบากในทางปฏิบัติแก่ฝ่ายในการสู้รบเกี่ยวกับการปฏิบัติตามกฎหมายมนุษยธรรมระหว่างประเทศ ความเชื่อมต่อกันทางเทคโนโลยีระหว่างพลเรือนและทางทหารนี้ยังส่งผลให้ประชากรพลเรือนมีความเสี่ยงที่จะได้รับผลกระทบจากการโจมตีทางไซเบอร์นี้เพิ่มมากขึ้น อย่างไรก็ตาม นอกเหนือจากการให้ความคุ้มครองพลเรือนจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธผ่านข้อบทตามกฎหมายมนุษยธรรมระหว่างประเทศ การพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การ

ขัดกันทางอาวุธผ่านภาคประชาสังคม ภาครัฐและองค์การระหว่างประเทศต่างๆ เป็นอีกกลไกที่สำคัญในการให้ความคุ้มครองพลเรือนจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้ ดังนี้

4.4 การพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

ความเชื่อมต่อของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ในปัจจุบันทำให้การดำเนินกิจกรรมทางการทหารและกิจกรรมของพลเรือนมีความใกล้ชิดกันมากยิ่งขึ้น ซึ่งการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบยังทำให้พลเรือนผู้ที่ไม่มีส่วนเกี่ยวข้องอาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเพิ่มมากยิ่งขึ้น จำเป็นอย่างยิ่งที่ผู้มีส่วนเกี่ยวข้องทุกภาคส่วนจะต้องหาแนวทางในการรับมือกับการโจมตีทางไซเบอร์ที่จะเกิดขึ้น ไม่ว่าจะเป็นการตั้งรับทางด้านเทคโนโลยีที่จะได้รับความเสียหายจากการโจมตี การตั้งรับทางด้านกฎหมายที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ เป็นต้น

4.4.1 ภาคประชาสังคม

ภาคประชาสังคม (Civil Society) เป็นหน่วยที่สามของสังคม นอกเหนือจากภาครัฐ (Government) และภาคธุรกิจ (Business) ประกอบด้วยองค์กรภาคประชาสังคม (Civil Society Organizations) และองค์กรที่ไม่ใช่ภาครัฐ (Non-Governmental Organizations)[392] จากความเชื่อมต่อของเทคโนโลยีที่ใช้ในทางการทหารและทางพลเรือนทำให้ภาคประชาสังคมเป็นส่วนหนึ่งที่อาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธและสามารถเข้ามามีมีบทบาทในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้

ที่ผ่านมา ภาคประชาสังคมถือเป็นส่วนหนึ่งที่มีบทบาทสำคัญในทำงานร่วมกับรัฐที่มีแนวความคิดเดียวกัน (Like-mimded States) และองค์การระหว่างประเทศเพื่อพัฒนามาตรการทางกฎหมายในการควบคุมอาวุธบางประเภท ได้แก่ การพัฒนาอนุสัญญาว่าด้วยการห้ามใช้ สะสม ผลิต และโอน และการทำลายทุ่นระเบิดสังหารบุคคล หรืออนุสัญญาห้ามทุ่นระเบิดสังหารบุคคล (Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-personnel Mines and on Their Destruction, 18 September 1977) และอนุสัญญาว่าด้วย

---

[392] United Nations, "Civil Society," http://www.un.org/en/sections/resources/civil-society/index.html. [July 16, 2016]

ระเบิดพวง (Convention on Cluster Munitions, 30 May 2008[393] ซึ่งความสำเร็จของการพัฒนาดังกล่าวส่วนหนึ่งมาจากการทำงานอย่างต่อเนื่องของภาคประชาสังคมที่เกี่ยวข้องซึ่งมีลักษณะการมีส่วนร่วมในการทำงานร่วมกันของกลุ่มพันธมิตรองค์กรที่ไม่ใช่ภาครัฐ (NGO) จากหลากหลายประเทศ

การพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของภาคประชาสังคมอาจทำได้โดยการรวบรวมข้อมูลความเสียหายหรือผลกระทบที่เกิดจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ไม่ว่าจะเป็นผลกระทบในทางตรงหรือทางอ้อม หากโครงสร้างพื้นฐานสาธารณะถูกโจมตี ทำการแลกเปลี่ยนข้อมูลข่าวสาร กำหนดกรอบการพิจารณาตามประเภทของเป้าหมายในการโจมตีทางไซเบอร์และความเสียหายในระยะยาวที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ต่อเป้าหมายแต่ละประเภท (โดยเฉพาะโครงสร้างพื้นฐานที่สำคัญต่างๆ ของรัฐ) ถกเถียงแลกเปลี่ยนความคิด โดยนำข้อมูลที่ได้จากการรวบรวมมาวิเคราะห์และประเมินเกี่ยวกับระดับความรุนแรงและลักษณะปัญหาที่เกิดขึ้นจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อกระตุ้นให้เกิดความตระหนักเกี่ยวกับภัยคุกคามของการโจมตีทางไซเบอร์ซึ่งส่งผลกระทบต่อการดำเนินชีวิตของประชาชนและอาจลุกลามไปสู่การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหรือสงครามไซเบอร์อย่างเต็มรูปแบบในอนาคตได้

ภาคเอกชน ในฐานะผู้ให้บริการรักษาความปลอดภัยทางไซเบอร์ หรือผู้พัฒนาอาวุธไซเบอร์ระบบโปรแกรมไม่ว่าจะในการป้องกันหรือการโจมตีจำเป็นที่จะต้องมีความรู้ความเข้าใจเกี่ยวกับหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ เนื่องจากการทำงานให้กับกองทัพในขณะที่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น ภาคเอกชนย่อมมีความเสี่ยง เพื่อหลีกเลี่ยงการกระทำที่เป็นการฝ่าฝืนตามกฎหมายมนุษยธรรมระหว่างประเทศ ซึ่งส่งผลให้เกิดการสูญเสียความคุ้มครองตามกฎหมาย

จากที่กล่าวมาข้างต้น จะเห็นได้ว่า บทบาทของภาคประชาสังคมในการพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นบทบาทอย่างไม่เป็นทางการของภาคประชาสังคม เพื่อสร้างความตระหนักทางด้านมนุษยธรรมของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันเป็นการนำเทคโนโลยีใหม่มาใช้ในการสู้รบและอาจนำไปสู่

---

[393] Richard Moyes Brian Rappert, Anna Crowe, and Thomas Nash,, "The Roles of Civil Society in the Development of Standards around New Weapons and Other Technologies of Warfare," *International Review of the Red Cross* 94, no. 886 (2012). P. 768.

การพัฒนามาตรฐานในการควบคุมเทคโนโลยีที่ใช้ในการสู้รบในอานคตต่อไป ทั้งนี้ ด้วยข้อจำกัดเกี่ยวกับขีดความสามารถ จำนวนบุคลากรและเงินทุนของภาคประชาสังคมที่มีอย่างจำกัด การพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของภาคประชาสังคมที่มีประสิทธิภาพจำเป็นจะต้องอาศัยความร่วมมือของผู้มีส่วนได้เสีย (Stakeholders) ทุกฝ่ายที่เกี่ยวข้อง ไม่ว่าจะเป็นภาครัฐ องค์การระหว่างประเทศ ภาคเอกชน สถาบันการศึกษาต่างๆ ในการทำงานร่วมกับภาคประชาสังคม

4.4.2 ภาครัฐ

จากการศึกษาแนวทางของรัฐในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในบทที่ 2 ที่ผ่านมา จะเห็นได้ว่า การตั้งรับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของภาครัฐส่วนใหญ่มุ่งเน้นไปที่การพัฒนาขีดความสามารถด้านไซเบอร์ทางการทหารของรัฐว่าจะเป็นการกำหนดแผนพัฒนาขีดความสามารถ การกำหนดหลักนิยมยุทธศาสตร์ทางการทหาร หรือการจัดตั้งหน่วยบัญชาการทางไซเบอร์ขึ้นโดยเฉพาะ

แนวโน้มการพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของภาครัฐเป็นการตั้งรับทางด้านเทคโนโลยี โดยการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของรัฐ โดยเฉพาะการป้องกันโครงสร้างพื้นฐานที่สำคัญของรัฐ (Critical Infrastructures) ซึ่งมีความเสี่ยงที่จะถูกโจมตีทางไซเบอร์ทั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธ และหากโครงสร้างพื้นฐานที่สำคัญของรัฐถูกโจมตีทางไซเบอร์จนทำให้ไม่สามารถใช้งานได้เป็นปกติจะทำให้ประชากรพลเรือนได้รับผลกระทบและสร้างความเสียหายต่อทั้งเศรษฐกิจ สังคม และความมั่นคงของรัฐได้

นอกจากการพัฒนาแนวทางในการตั้งรับทางเทคโนโลยีแล้ว การพัฒนากฎหมายภายในของรัฐเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์เป็นอีกสิ่งหนึ่งในการรับมือกับการโจมตีทางไซเบอร์ได้ เพื่อแสดงจุดยืนต่อประชาคมระหว่างประเทศว่ารัฐตนไม่ได้เพิกเฉยกับการใช้ดินแดนของรัฐเป็นต้นตอหรือที่มาในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธต่อรัฐอื่นโดยพัฒนากฎหมายภายในของรัฐเพื่อดำเนินคดีหรือลงโทษกลุ่มแฮคเกอร์หรือผู้โจมตีทางไซเบอร์ รวมทั้งให้ความร่วมมือกับรัฐอื่นในการสืบหาต้นตอของผู้โจมตีไม่ว่าจะเป็นการแลกเปลี่ยนข้อมูลข่าวสาร หรืออำนวยความสะดวกให้ความช่วยเหลือในการตรวจสอบที่มาของการโจมตี การพิสูจน์ตัวตนของผู้โจมตีที่เกิดขึ้นในดินแดนของรัฐ ตลอดจนการพัฒนาความร่วมมือระหว่างประเทศในการปรึกษาหารือเพื่อหาความ

ชัดเจนของหลักการตามกฎหมายระหว่างประเทศ เพื่อที่จะได้นำมายึดถือเป็นแนวทางปฏิบัติของรัฐต่อไปตลอดจนการกำหนดนโยบายหรือแนวทางปฏิบัติของรัฐเกี่ยวกับการใช้เทคโนโลยีไซเบอร์ที่สอดคล้องกับหลักการตามกฎหมายระหว่างประเทศ

ยิ่งไปกว่านั้น รัฐควรส่งเสริมให้มีการทำงานร่วมกันระหว่างภาครัฐ ภาคเอกชนและภาคประชาสังคมในการพัฒนาความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์อันเกิดการการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธภายในรัฐ เพื่อสร้างความเข้มแข็งและศักยภาพในการรับมือกับการโจมตีทางไซเบอร์ให้ครอบคลุมกับทุกภาคส่วนที่มีความเกี่ยวข้องและอาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

4.4.3 ความร่วมมือระดับระหว่างประเทศ

องค์การระหว่างประเทศถือเป็นส่วนที่สำคัญในการกำหนดแนวทางในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ผ่านมาตรการต่างๆ ทั้งที่มีสภาพบังคับและไม่มีสภาพบังคับ อาทิ การสร้างมาตรฐานทางกฎหมาย การให้ความช่วยเหลือรัฐสมาชิกเมื่อเกิดการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เป็นเวทีในการแลกเปลี่ยนข้อมูลความรู้ ความคิดเห็นเกี่ยวกับการนำเทคโนโลยีไซเบอร์มาใช้ในการสู้รบระหว่างรัฐสมาชิก การกำหนดขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เป็นต้น

4.4.3.1 กรอบของคณะกรรมการกาชาดระหว่างประเทศ

บทบาทของคณะกรรมการกาชาดระหว่างประเทศในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นการพัฒนาแนวทางด้านกฎหมายในการส่งเสริมการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธรวมทั้งการปรับปรุงประสิทธิภาพของกฎหมายมนุษยธรรมระหว่างประเทศให้มีความชัดเจนเป็นรูปธรรม เพื่อเป็นแนวทางปฏิบัติให้รัฐต่อไป

คณะกรรมการกาชาดระหว่างประเทศแสดงจุดยืนเกี่ยวกับสงครามไซเบอร์และกฎหมายมนุษยธรรมระหว่างประเทศในฐานะที่สงครามไซเบอร์เป็นวิธีการและปัจจัยในการสู้รบประกอบด้วยการโจมตีทางไซเบอร์ที่ดำเนินการในบริบทของการขัดกันทางอาวุธภายในความหมาย

ตามกรอบกฎหมายมนุษยธรรมระหว่างประเทศ โดยแสดงความกังวลเกี่ยวกับสงครามไซเบอร์ เนื่องจากช่องโหว่ของระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์และผลกระทบทางด้านมนุษยธรรมที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เมื่อระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์ของรัฐถูกโจมตี แทรกแซงหรือปิดกั้นก่อให้เกิดความเสี่ยงต่อพลเรือนในการถูกตัดขาดจากโครงสร้างพื้นฐานที่จำเป็น เช่น น้ำดื่มบริโภค การรักษาทางการแพทย์ กระแสไฟฟ้า[394]

คณะกรรมการกาชาดระหว่างประเทศแสดงจุดยืนเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ โดยเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ยืดหยุ่นครอบคลุมกับการนำเทคโนโลยีไซเบอร์มาใช้เป็นวิธีการและปัจจัยในการสู้รบได้ แม้ว่าเทคโนโลยีไซเบอร์จะไม่ใช่อาวุธในตัวเองก็ตาม หากการโจมตีทางไซเบอร์ก่อให้เกิดผลกระทบต่อพลเรือนในสถานการณ์การขัดกันทางอาวุธย่อมอยู่ภายใต้บังคับของหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ[395]

นอกจากนี้ คณะกรรมการกาชาดระหว่างประเทศยังกำหนดภารกิจในการตั้งรับทางด้านกฎหมายเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอย่างต่อเนื่อง เพื่อให้มั่นใจว่ากฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ครอบคลุมกับการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้ในการสู้รบได้ ไม่ว่าจะเป็น การสนับสนุนเผยแพร่บทความทางวิชาการของที่ปรึกษากฎหมายของคณะกรรมการกาชาดระหว่างประเทศที่เกี่ยวข้องกับการโจมตีทางไซเบอร์และกฎหมายมนุษยธรรมระหว่างประเทศ[396] การเรียกร้องให้ประชาคมระหว่างประเทศตระหนักเกี่ยวกับภัยคุกคามของการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้ในการสู้รบผ่านแถลงการณ์ในเวที

---

[394] ICRC, "Cyber Warfare and International Humanitarian Law: The Icrc's Position," https://www.icrc.org/eng/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf."

[395] Ibid.

[396] Cordula Droege, "No Legal Vacuum in Cyber Space," ICRC International Committee of the Red Cross, https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm. Knut Dörmann, "Computer Network Attack and International Humanitarian Law," *The Cambridge Review of International Affairs* Internet and State Security Forum(2001). Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks," (2004), https://www.icrc.org/eng/resources/documents/misc/68lg92.htm. Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello," International Review of the Red Cross 84(2002).

ระหว่างประเทศต่างๆ[397] การเป็นเวทีระหว่างประเทศในการจัดให้ผู้เชี่ยวชาญทางด้านกฎหมายประชุมปรึกษาหารือเกี่ยวกับกฎหมายมนุษยธรรมระหว่างประเทศและข้อท้าทายเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหรือสงครามไซเบอร์ในการประชุมองค์กรกาชาดและเสี้ยววงเดือนแดงระหว่างประเทศ[398] นอกจากนี้ คณะกรรมการกาชาดระหว่างประเทศยังเรียกร้องให้รัฐภาคีอนุสัญญาเจนีวาตรวจสอบความชอบด้วยกฎหมายของอาวุธ วิธีการและปัจจัยในการสู้รบใหม่อย่างเข้มงวดและหลากหลายแง่มุม ตลอดจนการเตือนให้ฝ่ายในการสู้รบใช้ความระมัดระวังในการแยกแยะพลเรือน และบังคับใช้กฎหมายมนุษยธรรมระหว่างกับการใช้ไซเบอร์ในการสู้รบเช่นเดียวกับการใช้ปืนไรเฟิล ปืนใหญ่หรือขีปนาวุธ[399]

จากการพัฒนาแนวทางการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธข้างต้น จะเห็นได้ว่า การตั้งรับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของคณะกรรมการกาชาดระหว่างประเทศเป็นการตั้งรับทางด้านกฎหมายผ่านการรวบรวมการศึกษาค้นคว้าข้อมูลจากทั้งภายในประเทศ ระหว่างประเทศ โดยที่ปรึกษากฎหมายของคณะกรรมการกาชาดระหว่างประเทศและผู้เชี่ยวชาญทางด้านกฎหมายต่างๆ เพื่อปรับปรุงกฎหมายมนุษยธรรมระหว่างประเทศให้มีความชัดเจนมากยิ่งขึ้น การส่งเสริมและผลักดันให้ฝ่ายในการสู้รบบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธ ตลอดจนการปรับปรุงกฎหมายมนุษยธรรมระหว่างประเทศให้มีความชัดเจนเกี่ยวกับแนวปฏิบัติที่สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศมากขึ้น เพื่อที่ฝ่ายในการสู้รบจะได้ยึดถือนำไปเป็นแนวทางปฏิบัติของรัฐเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธต่อไป ทั้งนี้ เพื่อให้มั่นใจว่าพลเรือนผู้บริสุทธิ์จะได้รับความคุ้มครองทางกฎหมายจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันเป็นจุดมุ่งหมายสำคัญของคณะกรรมการกาชาดระหว่างประเทศ

---

[397] ICRC, "International Humanitarian Law and New Weapon Technologies (34th Round Table on Current Issues of International Humanitarian Law)," in *San Remo, 8-10 September 2011.*(2011). "Weapons – Icrc Statement to the United Nations, 2011," https://www.icrc.org/eng/resources/documents/statement/united-nations-weapons-statement-2011-10-11.htm.

[398] ICRC, "International Humanitarian Law and the Challenges of Contemporary Armed Conflict " in 31st International Conference of the Red Cross and Red Crescent(Geneva, Switzerland2011). "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts " in 32nd International Conference of the Red Cross and Red Crescent(Geneva, Switzerland2015).

[399] ICRC, "Cyber Warfare and International Humanitarian Law: The ICRC's Position," https://www.icrc.org/eng/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf."

4.4.3.2 กรอบความร่วมมือระหว่างประเทศ

จากการศึกษาความร่วมมือระหว่างประเทศในการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธทั้งในระดับทวิภาคและพหุภาคีในบทที่ 2 พบว่า แนวทางการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่มีอยู่ในปัจจุบันอยู่ภายใต้บริบทของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ซึ่งมุ่งเน้นไปที่การรักษาความปลอดภัยของระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์ทั้งในสถานการณ์ปกติ และสถานการณ์การขัดกันทางอาวุธ โดยไม่ได้แบ่งแยกเป็นการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นการเฉพาะเจาะจงแต่อย่างใด

อย่างไรก็ตาม ความพยายามในทางระหว่างประเทศภายใต้บริบทของการรักษาความปลอดภัยทางไซเบอร์บางอย่างสะท้อนมุมมองเกี่ยวกับการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของประชาคมระหว่างประเทศที่น่าสนใจและมีนัยสำคัญ ดังนี้

(ก) สมัชชาสหประชาชาติกำหนดกระบวนการภายใต้กรอบสหประชาชาติเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ในประเด็นทางการเมืองและการทหาร (Politico-military) โดยแสดงความกังวลเกี่ยวกับเทคโนโลยีและปัจจัยซึ่งอาจจะใช้เพื่อวัตถุประสงค์ที่ไม่สอดคล้องกับวัตถุประสงค์ในการรักษาเสถียรภาพและความมั่นคงระหว่างประเทศและอาจส่งผลกระทบต่อความมั่นคงของรัฐตามมติของสมัชชาสหประชาชาติที่ A/RES/53/70[400]

ภารกิจการพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธของสมัชชาสหประชาชาติกำหนดไว้ภายใต้การทำงานของคณะกรรมาธิการที่หนึ่งว่าด้วยลดอาวุธและประเด็นเกี่ยวกับความมั่นคงระหว่างประเทศ (First Committee) รวมถึงการจัดตั้งกลุ่มผู้เชี่ยวชาญภาครัฐ (Group of Governmental Experts - GGEs) เพื่อเจรจาหารือและตรวจสอบภัยคุกคามที่มีอยู่และอาจเกิดขึ้นจากขอบเขตทางไซเบอร์และมาตรการที่เป็นไปได้ในการจัดการกับภัยคุกคามเหล่านั้น[401] โดยนำเสนอรายงานต่อที่ประชุมสมัชชาสหประชาชาติอย่าง

---

[400] UNGA, "Resolution Adopted by the General Assembly: 53/70. Developments in the Field of Information and Telecommunications in the Context of International Security (a/Res/53/70),"(1999).

[401] UNODA, "Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security,"(2015).

ต่อเนื่องล่าสุดในวันที่ 23 ธันวาคม 2015 ภายใต้ที่ประชุมสมัชชาสหประชาชาติยอมรับมติที่ 70/237 รายงานของกลุ่มผู้เชี่ยวชาญภาครัฐประจำปี 2014/2015 และให้จัดตั้งกลุ่มผู้เชี่ยวชาญภาครัฐกลุ่มใหม่ เพื่อทำรายงานเสนอต่อที่ประชุมสมัชชาสหประชาชาติในปีค.ศ. 2017 ต่อไป[402]

จะเห็นได้ว่า การพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธภายใต้กรอบสหประชาชาติเป็นการตั้งรับทางด้านกฎหมายด้วยความริเริ่มในการตรวจสอบและสำรวจความเข้าใจของรัฐที่มีต่อภัยคุกคามทางไซเบอร์ซึ่งรวมถึงการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเพื่อส่งเสริมความร่วมมือระหว่างประเทศในการระดมความคิดเกี่ยวกับมาตรการที่เป็นไปได้ในการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ ทั้งนี้ การทำงานภายใต้หัวข้อการพัฒนาด้านข้อมูลสารสนเทศและการสื่อสารโทรคมนาคมในบริบทของความมั่นคงระหว่างประเทศของกลุ่มผู้เชี่ยวชาญภาครัฐ (GGEs) มีแนวโน้มการทำงานอย่างต่อเนื่องซึ่งอาจจะนำไปสู่ความตกลงระหว่างประเทศในอนาคต

(ข) สถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติ (United Nations Institute for Disarmament Research - UNIDIR) กับโครงการศึกษาวิจัยเกี่ยวกับไซเบอร์(Cyber) ภายในหัวข้อภัยคุกคามต่อความมั่นคงปลอดภัยที่เกิดขึ้นใหม่ (Emerging Security Threats)[403] โดยมีโครงการศึกษาวิจัยที่ยังคงดำเนินการอยู่อย่างต่อเนื่องและเผยแพร่สิ่งตีพิมพ์ออกเป็นวาระ ได้แก่

- การประชุมเชิงปฏิบัติการประเด็นความมั่นคงปลอดภัยทางไซเบอร์ระหว่างประเทศ (International Security Cyber Issues Workshop Series) เพื่อระบุพื้นที่ความเข้าใจร่วมกันและความแตกต่างของประเด็นเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการพัฒนาบรรทัดฐานมาตรการทางกฎหมายและวิธีการที่เป็นไปได้ในการใช้งานเครื่องมือไซเบอร์[404]

- การสัมมนาว่าด้วยเสถียรภาพทางไซเบอร์ (Cyber Stability Conference Series) เพื่อนำเสนอโอกาสสำหรับรัฐและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในการเจรจาหารือเกี่ยวกับวิธีการ

---

[402] UNGA, "Resolution Adopted by the General Assembly on 23 December 2015 (a/Res/70/237),"(2015).

[403] UNIDIR, "Emerging Security Threats," http://www.unidir.org/programmes/emerging-security-threats. [July 20, 2016]

[404] "International Security Cyber Issues Workshop Series," http://www.unidir.org/programmes/emerging-security-threats/international-security-cyber-issues-workshop-series. [July 20, 2016]

ขั้นตอนในทางปฏิบัติที่จะทำให้สภาพแวดล้อมในห้วงไซเบอร์มีเสถียรภาพมากขึ้น โดยให้ความสำคัญกับความเสี่ยงที่เพิ่มขึ้นของความขัดแย้งทางไซเบอร์ (Cyber Conflict) ความจำเป็นในการพัฒนากลไกการเจรจาหารือ การศึกษา และการมีส่วนร่วมอย่างสร้างสรรค์เกี่ยวกับวิธีการปรับปรุงเสถียรภาพในห้วงไซเบอร์ในระดับพหุภาคี[405]

- การสนับสนุนกลุ่มผู้เชี่ยวชาญภาครัฐแห่งสหประชาชาติ (Support to the UN GGEs (Space and Cyber)) ในฐานะที่ปรึกษาผู้เชี่ยวชาญของกลุ่มผู้เชี่ยวชาญภาครัฐ (Group pf Governmental Experts - GGEs) ในการประชุมว่าด้วยการพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสารโทรคมนาคมในบริบทของการรักษาความปลอดภัยระหว่างประเทศ (Developments in the Field of Information and Telecommunications in the Context of International Security)[406] และ

- การประชุมในหัวข้อพฤติกรรมของรัฐและกฎหมายระหว่างประเทศในห้วงไซเบอร์ (International Law and State Behaviour in Cyberspace Meeting Series) เพื่อสำรวจปัญหาและกระตุ้นให้เกิดการตรวจสอบข้อเท็จจริงของปัญหาที่เกี่ยวข้องให้มากที่สุดของรัฐในแต่ละภูมิภาค โดยแบ่งการประชุมออกเป็นภูมิภาคเอเชีย-แปซิฟิก (Asia–Pacific) แอฟริกา (Africa) และยุโรป-เอเชีย (Eurasia) ครอบคลุมประเด็นของความร่วมมือในระดับภูมิภาคและการบังคับใช้ของกฎหมายระหว่างประเทศที่เกี่ยวกับห้วงไซเบอร์[407]

จะเห็นได้ว่า การพัฒนาแนวทางในการรับมือของสถาบันวิจัยเพื่อการลดอาวุธแห่งสหประชาชาติเป็นการตั้งรับโดยการศึกษาวิจัยและวิเคราะห์เกี่ยวกับภัยคุกคามทางไซเบอร์ซึ่งรวมถึงการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันส่งผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ของประชาคมระหว่างประเทศ เพื่อสร้างความตระหนักในการริเริ่มความร่วมมือระหว่าง

---

[405] "Cyber Stability Conference Series," http://www.unidir.org/programmes/emerging-security-threats/cyber-stability-conference-series. [July 20, 2016]

[406] "Support to the Un Gges (Space and Cyber)," http://www.unidir.org/programmes/emerging-security-threats/support-to-the-un-gges-space-and-cyber. [July 20, 2016]

[407] "International Law and State Behaviour in Cyberspace Meeting Series," http://www.unidir.org/programmes/emerging-security-threats/international-law-and-state-behaviour-in-cyberspace-meeting-series. [July 20, 2016]

ประเทศ องค์การระหว่างประเทศและผู้มีส่วนได้เสียอื่นๆ เพื่อรับมือกับผลกระทบด้านต่างๆ ที่เกิดจากภัยคุกคามทางไซเบอร์

(ค) องค์การความร่วมมือเซียงไฮ้ (Shanghai Cooperation Organisation) หรือ SCO กับแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (International Code of Conduct for Information Security)[408] จากการริเริ่มผลักดันแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศต่อที่ประชุมสมัชชาแห่งสหประชาชาติ (United Nations General Assembly) ในปีค.ศ. 2011 ภายใต้การผลักดันและความร่วมมือของประเทศจีน รัสเซีย ทาจิกิสถานและอุซเบกิสถาน โดยเรียกร้องให้มีการปรึกษาหารือระหว่างประเทศภายใต้กรอบองค์การสหประชาชาติ ตลอดจนการไม่ใช้เครือข่ายและเทคโนโลยีสารสนเทศและการสื่อสารในการดำเนินกิจกรรมอันเป็นปรปักษ์ (Hostile Activities) หรือการกระทำอันเป็นการรุกราน (Acts of Aggression) ที่ก่อให้เกิดภัยคุกคามต่อสันติภาพและความมั่นคงหรือการขยายอาวุธข้อมูลข่าวสาร (Information Weapons) หรือเทคโนโลยีที่เกี่ยวข้อง (ข้อ บี)[409]

ต่อมาในปีค.ศ. 2015 องค์การความร่วมมือเซียงไฮ้ (Shanghai Cooperation Organisation) หรือ SCO ภายใต้การผลักดันของประเทศจีน คาซัคสถาน คีร์กีซสถาน รัสเซีย ทาจิกิสถานและอุซเบกิซสถาน เนื้อหาของแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับล่าสุดมีการแก้ไขเปลี่ยนแปลงเล็กน้อย ในส่วนของแนวความคิดทั่วไปและลักษณะรูปแบบของเอกสารยังคงเดิม การเปลี่ยนแปลงเนื้อหาในแนวทางปฏิบัติระหว่างประเทศสำหรับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฉบับล่าสุดที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธปรากฏตาม ส่วนที่ 2 แนวทางปฏิบัติ

---

[408] UN, "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary (International Code of Conduct for Information Security)." ดูรายละเอียดได้ในภาคผนวก 2

[409] General Assembly, "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General ", ed. United Nations(2011). (A/66/359)

(Code of Conduct) ข้อ บี โดยละเว้นคำว่า อาวุธข้อมูลสารสนเทศ (Information Weapons)[410] ในข้อบีเดิม และเปลี่ยนแปลงเป็นการไม่ใช้เครือข่ายและเทคโนโลยีสารสนเทศและการสื่อสารในการดำเนินกิจกรรมที่สวนทางกับภารกิจในการรักษาสันติภาพและความมั่นคงระหว่างประเทศ

จะเห็นได้ว่า องค์การความร่วมมือเซี่ยงไฮ้กำหนดภารกิจในการพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธโดยเรียกร้องให้รัฐต่างๆ ดำเนินการตามแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศโดยสมัครใจ เพื่อให้มีการระบุถึงสิทธิหน้าที่และความรับผิดของรัฐในห้วงข้อมูลสารสนเทศ (Information Space) การเสริมสร้างความร่วมมือในการแก้ไขจัดการภัยคุกคามและข้อท้าทายในห้วงข้อมูลสารสนเทศร่วมกัน เพื่อให้มั่นใจว่าการใช้เทคโนโลยีสารสนเทศและการสื่อสาร เครือข่ายสารสนเทศและการสื่อสารเป็นไปเพื่อการพัฒนาทางเศรษฐกิจ สังคมและความเป็นอยู่ที่ดีของประชาชนและไม่สวนทางกับวัตถุประสงค์ของการสร้างความเชื่อมั่นในสันติภาพและความมั่นคงระหว่างประเทศ โดยปรับเปลี่ยนแก้ไขเนื้อหาของแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยบางส่วน เพื่อหลีกเลี่ยงประเด็นที่ถูกโต้แย้งจากกลุ่มประเทศตะวันตกและสหรัฐอเมริกาว่าแนวทางปฏิบัติดังกล่าวเป็นการกำหนดให้รัฐมีอำนาจในการควบคุมเนื้อหาข้อมูลสารสนเทศซึ่งขัดต่อสิทธิมนุษยชนขั้นพื้นฐานเกี่ยวกับเสรีภาพในการแสดงออกและการเคลื่อนย้ายเสรีของข้อมูลสารสนเทศภายในห้วงไซเบอร์ ทั้งนี้ เพื่อให้ประชาคมระหว่างประเทศยอมรับในแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

(ง) ศูนย์ความร่วมมือป้องกันไซเบอร์แห่งองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (Cooperative Cyber Defence Centre of Excellence - CCDCOE) ภายใต้องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (NATO) สนับสนุนการจัดทำคู่มือว่าด้วยการบังคับใช้กฎหมายระหว่างประเทศกับสงครามไซเบอร์ หรือ คู่มือทาลลินน์ 2.0 (Tallinn 2.0) คาดว่าจะแล้วเสร็จและตีพิมพ์เผยแพร่ในปีค.ศ. 2016 โดยสำนักพิมพ์มหาวิทยาลัยเคมบริดจ์ (Cambridge University Press)[411]

---

[410] Henry Rõigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?," https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html. [March 15, 2016]

[411] CCDCOE, "Tallinn Manual 2.0 to Be Completed in 2016," https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html.

ในเนื้อหาของคู่มือทาลลินน์ 2.0 กลุ่มผู้เชี่ยวชาญอิสระขยายขอบเขตจากการศึกษาตามคู่มือทาลลินน์เดิม เพื่อนำเสนอเครื่องมือที่จะเป็นคำแนะนำให้แก่รัฐต่างๆ ผ่านการตีความกฎหมายระหว่างประเทศ สนธิสัญญาและบรรทัดฐานทางกฎหมายที่มีอยู่ซึ่งเกี่ยวข้องกับการดำเนินกิจกรรมในห้วงไซเบอร์ เนื้อหาของคู่มือทาลลินน์ 2.0 จะกล่าวถึงกฎเกณฑ์เกี่ยวกับความรับผิดของรัฐ (State Responsibility) และความรับผิดขององค์การระหว่างประเทศ (Responsibility of International Organizations) กฎหมายโทรคมนาคมระหว่างประเทศ (International Telecommunications Law) กฎหมายสิทธิมนุษยชน (Human Rights Law) และปฏิบัติการเพื่อสันติภาพ (Peace Operations)[412] โดยร่างคู่มือทาลลินน์ 2.0 ประกอบด้วยกฎและความคิดเห็นที่มีต่อกฎแต่ละข้อซึ่งสะท้อนเฉพาะมุมมองของกลุ่มผู้เชี่ยวชาญอิสระเท่านั้น ไม่รวมถึงองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (NATO) ศูนย์ความร่วมมือป้องกันไซเบอร์แห่งองค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (Cooperative Cyber Defence Centre of Excellence - CCDCOE) หรือรัฐผู้สนับสนุนใดๆ

เป็นที่น่าสังเกตว่า ร่างคู่มือทาลลินน์ 2.0 ขยายขอบเขตในการศึกษาของคู่มือทาลลินน์เดิมไปสู่การพิจารณากฎหมายระหว่างประเทศในสถานการณ์ปกติเพื่อจัดการกับเหตุการณ์ทางไซเบอร์ที่รัฐจะต้องเผชิญ โดยไม่ได้เปลี่ยนแปลงหรือทำการศึกษาเพิ่มเติมกฎหมายระหว่างประเทศที่เกี่ยวข้องกับสงครามไซเบอร์แต่อย่างใด

จากที่ได้กล่าวมาทั้งหมดนี้ จะเห็นได้ว่า ประเด็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหรือสงครามไซเบอร์เป็นประเด็นที่หลายฝ่ายได้ให้ความสนใจและตื่นตัวกับการตั้งรับภัยจากการใช้เทคโนโลยีในการสู้รบเพิ่มมากขึ้น จากความเชื่อมต่อของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ซึ่งทำให้ทุกฝ่ายมีความใกล้ชิดกันทางด้านเทคโนโลยีและอาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธได้ทุกฝ่าย

อย่างไรก็ดี การพัฒนาแนวทางการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธปรากฏอยู่ภายในบริบทของความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เป็นส่วนใหญ่ โดยถือว่าการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นภัยคุกคามทางไซเบอร์อย่างหนึ่งและให้ความสำคัญในการป้องกันโครงสร้างพื้นฐานที่สำคัญของรัฐผ่านมาตรการ

---

[412] ibid.

ป้องกันทางไซเบอร์ในการรับมือทั้งในสถานการณ์ปกติและสถานการณ์การขัดกันทางอาวุธโดยมิได้ให้น้ำหนักกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นการเฉพาะแต่อย่างใด

แม้ว่าเทคโนโลยีสารสนเทศและคอมพิวเตอร์จะได้ใช้กันอย่างแพร่หลายทั่วโลก (Worldwide) ทุกภูมิภาคต่างอาศัยเทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการพัฒนาภายในรัฐและการดำเนินความสัมพันธ์ในทางระหว่างประเทศต่างๆ เกี่ยวข้องกับหลายภาคส่วนทั้งภาครัฐ ภาคเอกชน ภาคประชาสังคมและความร่วมมือระหว่างประเทศต่างๆ มากมาย กระนั้นก็ตาม กลับพบความพยายามในการพัฒนาแนวทางในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่เป็นรูปธรรมไม่มากนัก เมื่อเปรียบเทียบกับการรับมือการโจมตีด้วยอาวุธอื่นๆ ในสถานการณ์การขัดกันทางอาวุธที่เป็นเช่นนี้ เนื่องมาจากในปัจจุบันมีข้อเท็จจริงที่ชัดเจน เป็นรูปธรรมเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธไม่มากนัก เห็นได้จากเหตุการณ์โจมตีทางไซเบอร์ต่างๆ ที่เกิดขึ้นแสดงให้เห็นเพียงความเสียหายเกิดขึ้นจริง โดยไม่มีหลักฐานเกี่ยวกับผู้ดำเนินการโจมตีทางไซเบอร์ที่แน่ชัดหรือข้อเท็จจริงอื่นๆ ส่งผลให้การตระหนักในรายละเอียดทางด้านเทคนิคของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธยังไม่เพียงพอที่จะกำหนดมาตรการหรือแนวทาง ไม่ว่าจะเป็นการป้องกัน หรือการผลักดันแนวคิดหรือแนวทางเพื่อหาความชัดเจนเกี่ยวกับการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธหรือการใช้ห้วงไซเบอร์ต่างๆ

จากที่ได้ทำการศึกษามาทั้งหมดนี้ จะเห็นได้ว่า การนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้เป็นวิธีการและปัจจัยในการสู้รบอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศเมื่อมีสถานการณ์การขัดกันทางอาวุธเกิดขึ้น ฝ่ายในการสู้รบจึงมีหน้าที่ในการพิจารณาความชอบด้วยกฎหมายและดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธให้สอดคล้องกับหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ โดยเฉพาะหลักการแยกแยะเป้าหมาย หลักความได้สัดส่วนและการใช้ความระมัดระวังในการโจมตี รวมทั้งข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบต่างๆ

อย่างไรก็ตาม ด้วยลักษณะพิเศษของการโจมตีทางไซเบอร์และเทคโนโลยีสารสนเทศและคอมพิวเตอร์ซึ่งไม่ได้มีลักษณะเป็นอาวุธโดยสภาพ ไม่ได้มุ่งโจมตีต่อร่างกายหรือชีวิตโดยตรง เป็นการกระทำภายในห้วงไซเบอร์ซึ่งแตกต่างจากสมรภูมิการรบอื่น ก่อให้เกิดข้อท้าทายในทางปฏิบัติเกี่ยวกับการบังคับใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศที่ต้องคำนึงหลายประการ

ดังนั้น จำเป็นอย่างยิ่งที่ประชาคมระหว่างประเทศจะต้องร่วมมือกำหนดแนวทางปฏิบัติของรัฐในการใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศที่ชัดเจน และพัฒนาความร่วมมือในการรับมือและแก้ไขข้อท้าทายอันเกิดจากการใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ เพื่อให้ความคุ้มครองทางกฎหมายแก่พลเรือนและผู้ที่ไม่มีส่วนเกี่ยวข้องกับการสู้รบผู้บริสุทธิ์เหล่านั้นจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเป็นไปอย่างมีประสิทธิภาพถือเป็นหัวใจสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

จากการศึกษาวิทยานิพนธ์ฉบับนี้ จะเห็นได้ว่า ปฏิบัติการทางทหารและการสู้รบในปัจจุบันนำเอาเทคโนโลยีทางไซเบอร์เข้ามาใช้เป็นวิธีการและปัจจัยในการสู้รบใหม่ซึ่งมีลักษณะพิเศษแตกต่างไปจากการโจมตีด้วยอาวุธตามแบบ (Conventional Weapons) หลายประการ ไม่ว่าจะเป็นลักษณะที่ไม่เป็นรูปธรรม ความเสียหายเกิดขึ้นอย่างรวดเร็ว กว้างขวางและใช้ระยะเวลาต่อเนื่อง ความซับซ้อนของวิธีการที่ต้องอาศัยความรู้ความเชี่ยวชาญด้านเทคโนโลยีทางไซเบอร์ ความสามารถในการโจมตีทางไซเบอร์ที่ไม่จำกัดเขตแดนและระยะทาง และความยากลำบากในการพิสูจน์ความเกี่ยวข้องของผู้โจมตีกับฝ่ายในการสู้รบ เป็นต้น ลักษณะพิเศษดังกล่าวส่งผลกระทบให้รัฐต่างๆ ต้องปรับหลักนิยม ยุทธศาสตร์ทางทหาร พัฒนาบุคลากรที่มีความรู้ความเชี่ยวชาญด้านเทคโนโลยีทางไซเบอร์ ตลอดจนจัดตั้งหน่วยงานหรือกองกำลังทหารทางไซเบอร์เพื่อรับมือการโจมตีทางไซเบอร์เป็นการเฉพาะ

ทั้งนี้ เมื่อมีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นย่อมส่งผลกระทบต่อพลเรือนและผู้ที่ไม่มีส่วนเกี่ยวข้องกับการสู้รบอย่างหลีกเลี่ยงไม่ได้ ไม่ว่าจะเกิดจากการโจมตีด้วยอาวุธตามแบบการโจมตีทางไซเบอร์จึงจำเป็นที่จะต้องนำกฎหมายมนุษยธรรมระหว่างประเทศซึ่งเป็นกฎหมายที่มีที่มาจากทั้งสนธิสัญญาระหว่างประเทศและจารีตประเพณีระหว่างประเทศประกอบด้วยหลักการเกี่ยวกับปฏิบัติการทางทหารสำหรับฝ่ายในการสู้รบ รวมทั้งหลักการเกี่ยวกับข้อจำกัดทางด้านวิธีการและปัจจัยในการสู้รบ มาบังคับใช้เมื่อเกิดการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเพื่อคุ้มครองพลเรือนและบุคคลที่ไม่ได้มีส่วนเกี่ยวข้องกับการสู้รบ

แม้กฎหมายมนุษยธรรมระหว่างประเทศจะเป็นกฎหมายที่ใช้บังคับเมื่อเกิดสถานการณ์การขัดกันทางอาวุธ อีกทั้งข้อบทของกฎหมายมนุษยธรรมระหว่างประเทศเป็นกฎหมายที่มีอยู่แล้วก่อนที่จะมีการนำเทคโนโลยีทางไซเบอร์มาใช้ในการสู้รบจึงไม่มีข้อบทใดตามกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวข้องกับการโจมตีทางไซเบอร์เป็นการเฉพาะ อย่างไรก็ตาม การโจมตีทาง

ไซเบอร์ในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธเกิดขึ้นย่อมอยู่ภายใต้บังคับของกฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกับการโจมตีด้วยอาวุธประเภทอื่นๆ ในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธอย่างไม่มีข้อโต้แย้ง แสดงให้เห็นว่า กฎหมายมนุษยธรรมระหว่างประเทศมีความยืดหยุ่นครอบคลุมในการรองรับวิธีการและปัจจัยในการสู้รบใหม่ที่จะเกิดขึ้นต่อไปในอนาคตได้ เนื่องจากกฎหมายมนุษยธรรมระหว่างประเทศมีข้อกำหนดและข้อบทกฎหมายที่ใช้วิธีการตีความและการเปรียบเทียบ เพื่อหลีกเลี่ยงช่องว่างของกฎหมายซึ่งยืนยันหลักการตามคำพิพากษาของศาลระหว่างประเทศซึ่งถือเป็นแหล่งที่มาของกฎหมายระหว่างประเทศในลำดับรอง

อย่างไรก็ตาม การบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศยังมีข้อท้าทายเกี่ยวกับการใช้หลักการตามกฎหมายมนุษยธรรมระหว่างประเทศทั้งที่เป็นข้อท้าทายที่มาจากลักษณะพิเศษของการโจมตีทางไซเบอร์ที่มีความแตกต่างกับการโจมตีด้วยอาวุธตามแบบ และข้อท้าทายในทางปฏิบัติ เกี่ยวกับการตีความและพิจารณาเงื่อนไขหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศบางประการ โดยข้อท้าทายที่เกิดขึ้นจากการนำเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์มาใช้เป็นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอาจสรุปได้ ดังนี้

- การพิจารณาว่าการโจมตีทางไซเบอร์เพียงลำพังจะเป็นชนวนเริ่มต้นให้เกิดการขัดกันทางอาวุธอันเป็นเงื่อนไขในการนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้ได้หรือไม่นั้น ความเห็นของนักวิชาการทางด้านกฎหมายส่วนใหญ่เห็นว่าการโจมตีทางไซเบอร์เทียบเท่ากับการโจมตีด้วยอาวุธตามแบบที่เป็นชนวนเริ่มต้นให้เกิดสถานการณ์การขัดกันทางอาวุธได้ โดยประเด็นดังกล่าวนี้จำเป็นต้องอาศัยแนวทางปฏิบัติของรัฐ (State Practice) ที่ชัดเจนในอนาคตต่อไป

- หลักเกี่ยวกับการเข้าร่วมโจมตีในสถานการณ์การขัดกันทางอาวุธ จะพบว่า เงื่อนไขของการได้รับสถานะพลรบบางประการ เช่น การติดเครื่องหมายหรือสัญลักษณ์ และพกอาวุธอย่างเปิดเผยถูกลดความสำคัญเนื่องมาจากลักษณะพิเศษของการโจมตีทางไซเบอร์ที่ไม่ได้ถูกจำกัดด้วยเขตแดนหรือระยะทางในการโจมตี อีกทั้งการตีความลักษณะการมีส่วนร่วมโดยตรงในการสู้รบของพลเรือนที่ทำให้พลเรือนสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศ กรณีดังกล่าวยังเป็นที่สงสัยว่าควรกำหนดสถานะของบุคคลเหล่านั้นอย่างไร

- ในส่วนของหลักการเกี่ยวกับการปฏิบัติการทางทหาร ลักษณะของเทคโนโลยีที่ใช้ได้สองทาง (Dual-use Technology) ส่งผลให้ทรัพย์สิ่งของมีลักษณะเป็นเป้าหมายทางทหารที่สามารถโจมตีได้

โดยชอบด้วยกฎหมายและเป็นทรัพย์สินพลเรือนซึ่งต้องห้ามโจมตีตามกฎหมายมนุษยธรรมระหว่างประเทศได้เช่นกันก่อให้เกิดข้อท้าทายในการเคารพและปฏิบัติตามหลักการพื้นฐานการแยกแยะเป้าหมาย หลักความได้สัดส่วนในการโจมตีและหลักการใช้ความระมัดระวัง

นอกจากนี้ หลักความได้สัดส่วนในการโจมตียังไม่มีการกำหนดขอบเขตที่แน่นอนตามกฎหมายมนุษยธรรมระหว่างประเทศในการชั่งน้ำหนักความสมดุลระหว่างความได้เปรียบทางการทหารและผลกระทบต่อพลเรือน รวมทั้งการพิจารณาประเมินผลกระทบต่อพลเรือนอันเกิดจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ฝ่ายในการสู้รบจะต้องพิจารณาชั่งน้ำหนักกับความได้เปรียบทางทหารที่ได้รับจากการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ นอกจากนี้ การพิจารณาผลกระทบแบบ Knock-on ที่เกิดจากการโจมตีทางไซเบอร์ยังไม่มีความชัดเจนถึงระดับของผลกระทบที่ผู้วางแผนโจมตีจะต้องพิจารณาตามหลักความได้สัดส่วนในการโจมตีและการใช้ความระมัดระวังในการโจมตี

อย่างไรก็ตาม การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธถือเป็นวิธีการและปัจจัยในการสู้รบที่เคารพและสอดคล้องกับหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศ อย่างเช่นหลักการห้ามใช้วิธีการและปัจจัยในการสู้รบซึ่งก่อให้เกิดการบาดเจ็บเกินขนาดและความทุกข์ทรมานโดยไม่จำเป็น เนื่องจากเป้าหมายในการโจมตีทางไซเบอร์คือระบบหรือเครือข่ายสารสนเทศและคอมพิวเตอร์ไม่ใช่เนื้อตัวร่างกายของพลรบโอกาสของการบาดเจ็บเกินขนาดและความทุกข์ทรมานโดยไม่จำเป็นจากการโจมตีทางไซเบอร์ที่ไม่เป็นไปตามหลักกฎหมายมนุษยธรรมระหว่างประเทศจึงเป็นไปได้น้อยมาก กล่าวได้ว่า การโจมตีทางไซเบอร์เป็นทางเลือกที่ดีของฝ่ายในการสู้รบในการเลือกใช้อาวุธ วิธีการหรือปัจจัยในการสู้รบที่สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศ เพื่อหลีกเลี่ยงปฏิบัติการทางทหารที่อาจฝ่าฝืนกับหลักการห้ามก่อให้เกิดการบาดเจ็บเกินขนาดหรือการทุกข์ทรมานโดยไม่จำเป็น หรือหลักการห้ามใช้อาวุธซึ่งไม่สามารถแยกแยะเป้าหมายได้ ข้อท้าทายที่สำคัญของการโจมตีทางไซเบอร์ในสถานการณ์การณ์การขัดกันทางอาวุธขึ้นอยู่กับความรู้ความสามารถเฉพาะทางด้านเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของฝ่ายในการสู้รบที่จะเลือกใช้วิธีการหรือปัจจัยในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธว่ามีทักษะ ความรู้ความสามารถ ความเชี่ยวชาญเพียงพอที่จะเลือกอาวุธไซเบอร์หรือดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่ไม่ขัดต่อหลักการทั่วไปเกี่ยวกับข้อจำกัดด้านวิธีการและปัจจัยในการสู้รบตามกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่

จากที่ได้ศึกษามาทั้งหมดสรุปได้ว่า กฎหมายมนุษยธรรมระหว่างประเทศสามารถบังคับใช้กับการโจมตีทางไซเบอร์ที่เกิดขึ้นในระหว่างที่มีสถานการณ์การขัดกันทางอาวุธ โดยหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศมีความยืดหยุ่นสามารถที่จะบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ แต่ยังมีข้อท้าทายในการบังคับใช้หลักการกฎหมายมนุษยธรรมระหว่างประเทศหลายประการซึ่งจำเป็นจะต้องมาตรการและความร่วมมือจากทุกฝ่ายที่เกี่ยวข้องทั้งภาคประชาสังคม ภาครัฐและความร่วมมือระหว่างประเทศในการสร้างบรรทัดฐานการเคารพและปฏิบัติตามกฎหมายมนุษยธรรมระหว่างประเทศ

ในการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจำเป็นจะต้องอาศัยกลไกความร่วมมือระหว่างประเทศในการพัฒนาแนวทางในการรับมือทางด้านกฎหมาย โดยเฉพาะคณะกรรมการกาชาดระหว่างประเทศควรเข้ามามีบทบาทในส่งเสริมกฎหมายมนุษยธรรมระหว่างประเทศเพิ่มมากขึ้น สร้างความตระหนักเกี่ยวกับความร้ายแรงของการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ เพื่อให้มั่นใจว่าฝ่ายในการสู้รบจะดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธโดยยึดถือและปฏิบัติตามกฎหมายมนุษยธรรมระหว่างประเทศ

อย่างไรก็ดี การพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์เห็นได้ชัดว่าก่อให้เกิดคุณประโยชน์มากมาย ไม่ว่าจะเป็นการอำนวยความสะดวกในการดำเนินชีวิตและโครงสร้างพื้นฐานที่สำคัญต่างๆ การพัฒนาและเปลี่ยนแปลงทางเศรษฐกิจ การเงิน การธนาคาร สังคม การเมือง การติดต่อสื่อสารถือได้ว่าเป็นยุคสมัยของเทคโนโลยีสารสนเทศและคอมพิวเตอร์อย่างแท้จริง ความจำเป็นของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่มีต่อทางการทหารและทางพลเรือนนำไปสู่ความเสี่ยงที่เทคโนโลยีสารสนเทศและคอมพิวเตอร์จะตกเป็นเป้าหมายในการโจมตีและนำไปใช้ในการดำเนินกิจกรรมอันเป็นปรปักษ์ในการสู้รบเพิ่มมากขึ้น กล่าวได้ว่า เทคโนโลยีสารสนเทศและคอมพิวเตอร์มีทั้งประโยชน์และโทษได้ในคราวเดียวกัน และเช่นเดียวกันในทุกยุคทุกสมัยเมื่อมีสถานการณ์การขัดกันทางอาวุธหรือการสู้รบเกิดขึ้นไม่ว่าจะด้วยวิธีการและปัจจัยในการสู้รบใดประชากรพลเรือนย่อมได้รับผลกระทบจากการสู้รบอย่างหลีกเลี่ยงไม่ได้

ในการนี้ กฎหมายมนุษยธรรมระหว่างประเทศมีบทบาทสำคัญในการให้ความคุ้มครองทางกฎหมายแก่พลเรือนผู้บริสุทธิ์ที่ไม่มีส่วนเกี่ยวข้องกับการสู้รบซึ่งแม้จะไม่มีข้อบทกฎหมายเกี่ยวกับการใช้เทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการสู้รบ แต่สามารถนำกฎหมายมนุษยธรรมระหว่างประเทศบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเพื่อให้ความคุ้มครองแก่พลเรือนเหล่านั้นได้ ผู้เขียนเห็นว่า การไม่มีข้อบทเกี่ยวกับการโจมตีทางไซเบอร์ในสถานการณ์

การขัดกันทางอาวุธอาจเป็นผลดีต่อการตีความกฎหมายโดยคำนึงถึงวัตถุประสงค์ของกฎหมายในการให้ความคุ้มครองพลเรือนจากการสู้รบ เนื่องจากพลวัตทางกฎหมายที่ไม่หยุดนิ่งเช่นเดียวกับการพัฒนาทางเทคโนโลยีสารสนเทศและคอมพิวเตอร์อาจนำไปสู่การเปลี่ยนแปลงเนื้อหาของกฎหมายในอนาคต กฎหมายมนุษยธรรมระหว่างประเทศที่ดีจึงควรเป็นกฎหมายที่มีความยืดหยุ่นโดยการตีความกฎหมายมนุษยธรรมระหว่างประเทศให้ครอบคลุมกับการใช้เทคโนโลยีสารสนเทศและคอมพิวเตอร์ในการสู้รบใดๆ จะต้องคำนึงทั้งบริบททางด้านมนุษยธรรมและปฏิบัติการทางทหารควบคู่กันไป การตีความโดยพิจารณาเฉพาะด้านมนุษยธรรมเพียงประการเดียวอาจทำให้ฝ่ายในการสู้รบไม่ยอมรับและไม่นำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้กับการโจมตีทางไซเบอร์ทำให้พลเรือนไม่ได้รับความคุ้มครองทางกฎหมายใดๆ จากการสู้รบเช่นเดียวกับการตีความโดยคำนึงเฉพาะด้านปฏิบัติการทางทหาร แม้จะทำให้ฝ่ายในการสู้รบสามารถนำกฎหมายมนุษยธรรมระหว่างประเทศไปบังคับใช้ได้จริงแต่ก็อาจทำให้พลเรือนได้รับผลกระทบจากการโจมตีทางไซเบอร์มากเกินไป

เมื่อพิจารณาลักษณะความเชื่อมต่อของระบบหรือเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่ใช้ทางการทหารและพลเรือนยังทำให้พลเรือนเข้ามาเกี่ยวข้องกับการสู้รบที่นำเอาเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาใช้เป็นวิธีการและปัจจัยในการสู้รบเพิ่มมากขึ้นทั้งที่ตั้งใจและไม่ตั้งใจและไม่จำกัดเฉพาะแต่พลเรือนที่อาศัยอยู่ในดินแดนที่มีการสู้รบเหมือนดังเช่นการสู้รบตามแบบ หากแต่ครอบคลุมประชากรพลเรือนทั่วโลกภายในห้วงไซเบอร์ที่พึ่งพาเทคโนโลยีสารสนเทศและคอมพิวเตอร์ การสู้รบในยุคไซเบอร์จึงไม่ได้เป็นเรื่องของรัฐและทางทหารเท่านั้น ทั้งนี้ การบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศให้มีประสิทธิภาพไม่ได้ขึ้นอยู่กับข้อบทกฎหมายมนุษยธรรมระหว่างประเทศแต่เพียงประการเดียว หากจะต้องอาศัยการผลักดันโดยความร่วมมือระหว่างประเทศ เพื่อให้ฝ่ายในการสู้รบยึดถือและคำนึงถึงหลักการตามกฎหมายมนุษยธรรมระหว่างประเทศในการดำเนินการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธและความร่วมมือของผู้มีส่วนได้เสียที่เกี่ยวข้องทุกภาคส่วน ทั้งภาครัฐ ความร่วมมือระหว่างประเทศ ภาคเอกชน ภาคประชาสังคมตลอดจนพลเรือนในการพัฒนาแนวทางการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธซึ่งเป็นที่ยอมรับและเป็นรูปธรรมต่อไป

5.2 ข้อเสนอแนะ

1. กลไกความร่วมมือระหว่างประเทศควรยึดถือกฎหมายมนุษยธรรมระหว่างประเทศในการพัฒนาแนวทางการรับมือกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ผลักดันและเป็นเวทีให้ประชาคมระหว่างประเทศเจรจาปรึกษาหารือและพัฒนาความร่วมมือ ในการสร้างบรรทัดฐานและจัดทำคำแนะนำเกี่ยวกับการดำเนินการโจมตีทางไซเบอร์ที่เคารพหลักการต่างๆ ตามกฎหมายมนุษยธรรมระหว่างประเทศ

2. รัฐจะต้องมีความจริงใจในการปฏิบัติตามหลักการของกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ เพื่อให้เกิดเป็นแนวทางปฏิบัติของรัฐและก่อให้เกิดเป็นจารีตประเพณีระหว่างประเทศต่อไป

รัฐจะต้องสนับสนุนและให้ความร่วมมือกับองค์กรระหว่างประเทศในการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการโจมตีทางไซเบอร์ให้สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศให้แก่กองทัพและพลรบของตน

รัฐควรส่งเสริมให้ภาคเอกชนและภาคประชาสังคมเข้ามามีบทบาทที่เหมาะสมในการรักษาความปลอดภัยและการใช้เทคโนโลยีสารสนเทศและคอมพิวเตอร์ที่เหมาะสม ตลอดจนทำงานร่วมกับองคการระหว่างประเทศ ภาคเอกชนและภาคประชาสังคมที่เกี่ยวข้อง เพื่อเสริมสร้างความแข็งแกร่งในการตั้งรับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ

นอกจากนี้ หากมีการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธเกิดขึ้นในดินแดนของรัฐ รัฐจะต้องให้ความร่วมมือในการสืบสวนสอบสวน เมื่อมีการร้องขอ ตลอดจนรัฐจะต้องไม่ยินยอมให้ใช้ดินแดนของรัฐเป็นสถานที่ในการโจมตีทางไซเบอร์ต่อรัฐอื่น และไม่เพิกเฉย เมื่อทราบว่ามีการโจมตีทางไซเบอร์ต่อรัฐอื่นเกิดขึ้นภายในดินแดนของตน

3. ฝ่ายในการสู้รบที่มิใช่รัฐในการโจมตีทางไซเบอร์ที่ไม่มีลักษณะระหว่างประเทศจะต้องเคารพและปฏิบัติตามพันธกรณีในการให้ความคุ้มครองแก่พลเรือนและผู้ที่ไม่ส่วนเกี่ยวข้องกับการสู้รบ รวมทั้งพัฒนา ฝึกอบรม ความรู้ความเชี่ยวชาญทางด้านเทคโนโลยีทางไซเบอร์ของผู้โจมตี ตลอดจนควรจะมีการกำหนดกฎระเบียบภายในองค์กรเกี่ยวกับหลักกฎหมายมนุษยธรรมระหว่าง

ประเทศและบังคับให้สมาชิกปฏิบัติตามอย่างเคร่งครัด เพื่อแสดงเจตจำนงในการเคารพกฎหมายมนุษยธรรมระหว่างประเทศ

4. กองทัพทหารหรือกองกำลังติดอาวุธของรัฐจะต้องเคารพและปฏิบัติตามหลักกฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ ตลอดจนกำหนดหลักนิยม ยุทธศาสตร์ แนวทางและวิธีปฏิบัติเกี่ยวกับการโจมตีทางไซเบอร์ที่สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศไว้ในคู่มือทหาร และพึงแยกแยะพลเรือนและพลรบ ทรัพย์สินพลเรือนและเป้าหมายทางทหารตลอดเวลาที่ทำการโจมตีทางไซเบอร์

นอกจากนี้ กองทัพทหารควรหลีกเลี่ยงการโจมตีทางไซเบอร์ที่ไม่สามารถแยกแยะเป้าหมายเพื่อหลีกเลี่ยงความเสียหายที่เป็นผลกระทบต่อพลเรือน

5. พลเรือนจะต้องตระหนักรู้ และไม่เข้าร่วมโดยตรงในการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ไม่ว่าในทางใดๆ เพื่อป้องกันการสูญเสียความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศ ไม่ใช้ระบบหรือโปรแกรมซอฟต์แวร์เถื่อนที่ทำให้เครื่องคอมพิวเตอร์มีโอกาสติดเชื้อได้ง่าย ใช้ซอฟต์แวร์ของแท้ และหมั่นทำการอัพเดทความปลอดภัยของคอมพิวเตอร์ เพื่อป้องกันมิให้คอมพิวเตอร์ของตนเองกลายเป็นคอมพิวเตอร์ติดเชื้อและแพร่กระจายต่อไป หมั่นศึกษาหาความรู้ทางด้านการรักษาความปลอดภัยทางไซเบอร์และกฎหมายระหว่างประเทศที่เกี่ยวข้องกับการใช้เทคโนโลยี เพื่อให้มั่นใจว่าการใช้เทคโนโลยีของตนเป็นไปอย่างเหมาะสมไม่ขัดหรือฝ่าฝืนต่อข้อบทกฎหมายทั้งกฎหมายภายในและกฎหมายระหว่างประเทศ

รายการอ้างอิง

ภาษาไทย

เดลินิวส์. "กองทัพเน้นปกป้องสถาบัน ตั้ง"กองสงครามไซเบอร์"สู้ " http://www.dailynews.co.th/politics/355320.

กรมอาเซียน กระทรวงการต่างประเทศ. "คำศัพท์ - คำย่อ." In หนังสือคำศัพท์-คำย่อทางการทูต สถาบันการต่างประเทศ กต. (ฉบับปรับปรุงครั้งที่ 2).

กองการเมืองและความมั่นคง กรมอาเซียน. "การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก (Asean Regional Forum - Arf)." 2557.

จตุชัย แพงจันทร์. "Cyber Warfare." ข่าวทหารอากาศ 72, no. 4 (2555).

จตุรนต์ ถิระวัฒน์. กฎหมายมนุษยธรรมระหว่างประเทศ. กรุงเทพมหานคร: คณะกรรมการกาชาดระหว่างประเทศ (ICRC), 2550.

ณัฐวัฒน์ กฤตยานวัช. "สถานภาพของกลุ่มพลรบตาลิบันที่ถูกควบคุมตัวโดยสหรัฐอเมริกาในกฎหมายมนุษยธรรมระหว่างประเทศ." จุฬาลงกรณ์มหาวิทยาลัย, 2549.

ตะวัน พึ่งพุทธารักษ์. "ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์." จุฬาลงกรณ์มหาวิทยาลัย, 2546.

นันทชัย เพียรสนอง. "การใช้เทคโนโลยีสารสนเทศกับผลกระทบทางกฎหมาย." งานวิจัยในการอบรมหลักสูตรผู้บริหารกระบวนการยุติธรรมระดับสูง (บ.ย.ส.), 2539.

นิวัติ เนียมพลอย. "ไซเบอร์ กับการรักษาความปลอดภัยและการปฏิบัติการ (Cyber with Security and Operations)." https://nniwat.wordpress.com/2013/11/08/%E0%B9%84%E0%B8%8B%E0%B9%80%E0%B8%9A%E0%B8%AD%E0%B8%A3%E0%B9%8C-%E0%B8%81%E0%B8%B1%E0%B8%9A%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A3%E0%B8%B1%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/.

ปิยชาต เจริญผล. คู่มือกฎการใช้กำลัง สถาบันกฎหมายมนุษยธรรมระหว่างประเทศ, 2554.

รุ่งธรรม บัวแตง. "ความหมายของ ไซเบอร์ (Cyber) " http://www.dstd.mi.th/board/index.php?topic=887.0.

วราภรณ์ เหลืองทอง. "ปัญหาในการนิยามคำว่า "การขัดกันทางอาวุธ" อันเป็นเงื่อนไขสำหรับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ." มหาวิทยาลัยธรรมศาสตร์, 2553.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. "เกี่ยวกับไทยเซิร์ต." สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), https://www.thaicert.or.th/about.html.

สหพงษ์ เครือเพ็ชร. "ระบบอาวุธเลเซอร์." วารสารหลักเมือง, มกราคม 2558, 18.

ภาษาอังกฤษ

Aaron Mehta and Paul Kallender-Umezu. "Us, Japan Strike New Military Agreement." DefenseNews, http://www.defensenews.com/story/breaking-news/2015/04/27/us-japan-new-military-agreement/26443297/.

ICJ. *Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons*, 1996.

"Annex1 to the Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (Unofficial Translation)." edited by SCO, 2 Dec 2008.

ARF. "Asean Regional Forum Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space." http://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html.

———. "Co-Chairs' Summary Report of the Arf Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects." 2013.

———. "Co-Chairs' Summary Report Arf Workshop on Proxy Actors in Cyberspace." Hoi An City, Viet Nam, 2012.

"Asean Regional Forum Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security." 2012.

Associated Press. "North Korea Launched Cyber Attacks, Says South " *The guardian*, 11 July 2009.

———. "South Korea Blames North Korea for Cyberattack on Media, Government Sites." *Fox News*, 16 July 2013

Barack Obama. "Taking the Cyberattack Threat Seriously." *the Wall Street Journal* (2012).

BBC. "Nato Denies Targeting Water Supplies " http://news.bbc.co.uk/2/hi/europe/351780.stm.

———. "Russia 'Ends Georgia Operation' " http://news.bbc.co.uk/2/hi/europe/7555858.stm.

Belarus News. "Belarusian Army to Combat Cyber Threats." Belarusian Telegraph Agency, http://eng.belta.by/society/view/belarusian-army-to-combat-cyber-threats-24388-2011.

Brazilian Ministry of Defence. "National Strategy of Defense: Peace and Security for Brazil.": Ministry of Defense, 2008.

Brian McCartan. "Myanmar on the Cyber-Offensive." AsiaTimes, http://www.atimes.com/atimes/Southeast_Asia/JJ01Ae01.html.

Brian Rappert, Richard Moyes, Anna Crowe, and Thomas Nash,. "The Roles of Civil Society in the Development of Standards around New Weapons and Other Technologies of Warfare." *International Review of the Red Cross* 94, no. 886 (2012).

Burrus M. Carnahan. "Unnecessary Suffering, the Red Cross and Tactical Laser Weapons." *Loyola of Los Angeles International and Comparative Law Review* 18 (1996).

Carmen-Cristina Cirlig. "Cyber Defence in the Eu: Preparing for Cyber Warfare?": European Parliament, European Union, October 2014.

CCDCOE. "About Cyber Defence Centre." https://ccdcoe.org/about-us.html.

———. "Tallinn Manual 2.0 to Be Completed in 2016." https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html.

Center for Strategic and International Studies. "Preliminary Assessment of National Doctrine and Organization: Cybersecurity and Cyberwarfare." UNIDIR Resources Paper, 2011.

The Charter of the United Nations. A Commentary. edited by Daniel-Erasmus Khan Bruno Simma, Georg Nolte, and Andreas Paulus, Third Edition Oxford: Oxford University Press, 1995.

Chief of Defence of the Republic of Lithuania. "Lithuanian Military Doctrine." 2010.

CHOE SANG-HUN. "Computer Networks in South Korea Are Paralyzed in Cyberattacks." *The New York Times*, 20 March 2013.

Christopher Greenwood. "The Law of Weaponry at the Start of the New Millennium." *International Law Studies* 71 (1998): 186.

Claude PILLOUDt, Jean DE PREUX, Yves SANDOZ, Bruno ZIMMERMANN, Philippe Eberlin, Hans-Peter Gasser and Claude F. Wenger, . "Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949." edited by ICRC. Netherlands Martinus Nijhoff Publishers 1987.

Compiled by Al Rees, CCIPS. "Computer Crime and Intellectual Property Section." edited by U.S. Department of Justice, 2006.

Cordula Droege. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.". *International Review of Red Cross* 94 (2012): 533-78.

———. "No Legal Vacuum in Cyber Space." ICRC International Committee of the Red Cross, https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm.

Council of Europe Parliamentary Assembly. "Resolution 1633 (2008):The Consequences of the War between Georgia and Russia ", 2008.

Council of the European Union. "Eu Cyber Defence Policy Framework." Brussels, 2014.

CyberSecurity Malaysia. "Malaysia and Morocco Are Now Partners in Cyber Security." 2010.

David Albright, Paul Brannan, and Christina Walrond,. "Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?". Preliminary Assessment (2010).

David E. Sanger. "Obama Order Sped up Wave of Cyberattacks against Iran." The New Yoek Times, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.

David Turns. "Cyber Warfare and the Notion of Direct Participation in Hostilities." *Journal of Conflict & Security Law* 17, no. 2 (2012).

David Weissbrodt. "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage." *Minnesota Journal of International Law* 22 (2013).

Davis Brown. "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict ". *Harvard International Law Journal* 17, no. 1 (2006).

"Dmitry Medvedev Made a Statement on the Situation in South Ossetia (2008)." http://en.kremlin.ru/events/president/news/1043.

Douglas Perry. "Austria Hires 1600 Soldiers for 'Cyber' Security." Tom's Guide, http://www.tomsguide.com/us/austria-cyber-crime-cyber-defense-secret-service,news-11077.html.

Duncan B. Hollis. "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" In *CYBERWAR: LAW &ETHICS FOR VIRTUAL CONFLICTS,* edited by Claire Findkelstein and Kevin Govern Jens David OhlinOxford University Press, 2014.

Elisabeth Bumiller and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

Elizabeth Wilmshurst. *International Law and the Classification of Conflicts*. United Kingdom: Oxford University Press, 2012.

Elizabeth Winkel. "Benelux Sign Memorandum of Understanding on Cyber Security." European Urban Knowledge Network, http://www.eukn.eu/e-library/project/bericht/eventDetail/benelux-sign-memorandum-of-understanding-on-cyber-security/.

Emily Crawford. "Virtual Battlegrounds: Direct Participation in Cyber Warfare ". *I/S: A Journal of Law and Policy for the Information Society* 9, no. 1 (2013).

Eneken Tikk, Kadri Kaska, Liis Vihul,. "International Cyber Incidents: Legal Considerations." *Cooperative Cyber Defence Centre of Excellence (CCD COE)* (2010).

Eric Talbot Jensen. "Cyber Attacks: Proportionality and Precautions in Attack." *International Law Studies* 89, no. 198 (2013).

———. "Cyber Warfare and Precautions against the Effects of Attacks." *Texas Law Review* 88 (2010): 1533.

———. "Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?". *American University International Law Review* 18, no. 5 (2003).

Erki Kodar. "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocal I." *ENDC Proceedings* 15 (2012): 107-32.

European Parliament, Directorate-General for External Policies of the Union. "Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the Eu." 2011.

European Union. "Council Framework Decision 2005/222/Jha of 24 February 2005 on Attacks against Information Systems." 16.3.2005.

———. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." European Commission, 2013.

———. "Directive on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/Jha." 2013.

———. "Eu and Nato Cyber Defence Cooperation." http://eeas.europa.eu/top_stories/2016/100216_eu-nato-cyber-defence-cooperation_en.htm.

Evgeny Morozov. "An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar." The Slate Group (August 14, 2008), http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.

ExecutiveBiz. "Iranian Cyber Army Second-Largest in the World, Claims Iranian Commander." http://blog.executivebiz.com/2010/05/iranian-cyber-army-second-largest-in-the-world-claims-iranian-commander/.

General Assembly. "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General ", edited by United Nations, 2011.

Geneva Academy of International Humanitarian Law and Human Rights. "Glossary." In *Weapons Law Encyclopedia*. Geneva, 2014.

———. "Qualification of Armed Conflicts." (2012). http://www.geneva-academy.ch/RULAC/qualification_of_armed_conflict.php.

"Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949."

"Geneva Convention (Ii) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949."

"Geneva Convention (Iii) Relative to the Treatment of Prisoners of War of 12 August 1949."

"Geneva Convention (Iv) Relative to the Protection of Civilian Persons in Time of War of 12 August 1949."

"The Geneva Conventions of 12 August 1949."

"The Hague Convention (Iv) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land. (18 October 1907)."

Hamadoun I. Touré. *The Quest for Cyber Peace*. International Telecommunication Union, 2011.

Heather Harrison Dinniss. *Cyber Warfare and the Laws of War*. the United States of America: Cambridge University Press, 2012.

Henry Rõigas. "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?" https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html.

ICRC. "Cyber Warfare." https://www.icrc.org/eng/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm.

———. "Cyber Warfare and International Humanitarian Law: The Icrc's Position." https://www.icrc.org/eng/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf.

———. "The Icrc's Mandate and Mission." https://www.icrc.org/en/mandate-and-mission.

———. "International Humanitarian Law and New Weapon Technologies (34th Round Table on Current Issues of International Humanitarian Law)." In *San Remo,* 8-10 *September* 2011., 2011.

———. "International Humanitarian Law and the Challenges of Contemporary Armed Conflict " In 31*st International Conference of the Red Cross and Red Crescent*. Geneva, Switzerland, 2011.

———. "Weapons – Icrc Statement to the United Nations, 2011." https://www.icrc.org/eng/resources/documents/statement/united-nations-weapons-statement-2011-10-11.htm.

———. "Weapons: Icrc Statement to the United Nations, 2013." https://www.icrc.org/eng/resources/documents/statement/2013/united-nations-weapons-statement-2013-10-16.htm.

———. "Weapons: Icrc Statement to the United Nations, 2014." https://www.icrc.org/en/document/weapons-icrc-statement-united-nations-2014.

———. "Weapons: Icrc Statement to the United Nations, 2015." https://www.icrc.org/en/document/weapons-icrc-statement-united-nations-2015.

ICRC Opinion paper. "How Is the Term "Armed Conflict" Defined in International Humanitarian Law? ." ICRC, 2008.

ILC. "Responsibility of States for Internationally Wrongful Acts." In *Yearbook of the International Law Commission,* 2001*, vol. II (Part Two)* UN, 2005.

International Committee of the Red Cross. "Methods and Means of Warfare." ICRC, https://www.icrc.org/eng/war-and-law/conduct-hostilities/methods-means-warfare/overview-methods-and-means-of-warfare.htm.

James H. Doyle. "Computer Networks, Proportionality, and Military Operations." *International Law Studies* 76, no. 9 (2002).

Japanese Ministry of Defence. "Defense of Japan 2010." edited by Ministry of Defence, 2010.

Javier Ulises Ortiz. "Argentina: The Challenge of Information Operations." *IOSphere* Special Edition (2008).

Jean-Marie Henckaerts and Louise Doswald-Beck. *Study on Customary International Humanitarian Law - Volume I: Rule*. Cambridge University Press, 2005.

Jean S. Pictet. *Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva,* 12 *August* 1949. Switzerland: ICRC, 1952.

John Markoff and Andrew E. Kramer. "U.S. And Russia Differ on a Treaty for Cyberspace." *The New York Times*, 2009.

John Richardson. "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield." *John Marshall Journal Of Computer & Information Law* 29, no. 1 (2011).

Joint Chiefs Of Staff Dod. "Department of Defense Dictionary of Military and Associated Terms." CreateSpace Independent Publishing Platform, 2009.

Jr., Charles J. Dunlap. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* (2011).

Kevin G. Coleman. "Cyber Espionage Targets Sensitive Data." (2008). Published electronically December 29, 2008. See more at: http://sip-trunking.tmcnet.com/topics/security/articles/47927-cyber-espionage-targets-sensitive-data.htm#sthash.6TTlz9qg.dpuf.

Knut Dörmann. "Applicability of the Additional Protocols to Computer Network Attacks." (2004). Published electronically 17-19.11.2004. https://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

———. "Computer Network Attack and International Humanitarian Law." *The Cambridge Review of International Affairs* Internet and State Security Forum (2001).

Knut Ipsen. "Combatants and Non-Combatants." In *The Handbook of Humanitarian Law in Armed Conflicts*, edited by Dieter Fleck: Oxford University Press, 1999.

Laurent Gisel. "The Law of War Imposes Limits on Cyber Attacks Too." ICRC, https://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm.

Lesly Swanson. "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict." *Loyola of Los Angeles International and Comparative Law Review* 32, no. 2/5 (2010).

Louise Arimatsu. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations." In 4*th International Conferrence on Cyber Conflict*, edited by R. Ottis C. Czosseck, K. Ziolkowski: NATO CCD COE Publications, 2012.

Marco Sassòli, Antoine A. Bouvier and Anne Quintin. *How Does Law Protect in War?* edited by Third. Vol. I, Geneva: ICRC, 2011.

Mark Clayton. "Stuxnet Malware Is 'Weapon' out to Destroy ... Iran's Bushehr Nuclear Plant? ." http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

Martin C. Libicki. *What Is Information Warfare?* : National Defense University, 1995.

Michael N. Schmitt. "Classification of Cyber Conflict." *Journal of Conflict & Security Law* 17, no. 2 (2012): 256.

———. "Targeting and Humanitarian Law: Current Issues." *International Law Studies* 80, no. International Law and Military Operations (2004).

———. "Wired Warfare: Computer Network Attack and Jus in Bello." *International Review of the Red Cross* 84 (2002): 365-99.

Ministry of Foreign Affairs. "Cyber Attacks Disable Georgian Websites." http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html.

NATO. "Nato Member Countries " http://www.nato.int/cps/en/natohq/nato_countries.htm.

———. "Nato Opens New Centre of Excellence on Cyber Defence." http://www.nato.int/docu/update/2008/05-may/e0514a.html.

———. "The North Atlantic Treaty." North Atlantic Treaty Organization, 1949.

———. "What Is Nato?" http://www.nato.int/nato-welcome/index.html.

NATO Parliamentary Assembly. "Nato and Cyber Defence." NATO, 2009.

NATO Standardization Agency. "Nato Glossary of Terms and Definitions." North Atlantic Treaty Organization, 2008.

Nils Melzer. "Cyber Operations and Jus in Bello." In *Confronting Cyberconflict in Disarmament Forum*, edited by Kerstin Vignard. Geneva: UNIDIR, 2011.

———. "Cyberwarfare and International Law." *NUIDIR Resources Paper* (2011).

———. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*. Vol. ICRC: 90 IRRC 991 (2008), Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009.

Olivia Solon. "Do We Need a Geneva Convention for Cyber Warfare?" wired.com, www.wired.co.uk/news/archive/2010-10/15/cyber-warfare-ethics.

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel,. "The Law of Cyber-Attack." *California Law Review* 100 (2012).

OSCE. "40 Years of Osce." http://www.osce.org/whatistheosce.

———. "Decision No. 1106 Initial Set of Osce Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies." 2013.

Prosecutor V . Tadic, (Appeal Judgment), Case It-94-1-*A*, 15 July 1999 15 July 1999.

The Prosecutor V. Bemba Gombo (Decision on Confirmation of Charges) Icc-01/05-01/08 15 June 2006.

The Prosecutor V. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeals Chamber (Icty) 2 October 1995.

Prosecutor V. Fatmir Limaj, Haradin Bala and Isak Musliu, Judgement (Trial Chamber Ii), Case No. It-03-66-*T*, 30 November 2005.

Prosecutor V. Fofana (Decision on Appeal against Decision on Prosecutor's Motion for Judicial Notice and Admission of Evidence) Scsl-04-14-*T*-398*, Separate Opinion of Judge Robertson*, 16 May 2005.

The Prosecutor V. Galic, Case No. It-98-29-*T, Trial Chamber*, 5 December 2003.

The Prosecutor V. Jean-Paul Akayesu, Ictr-96-4-*T, Trial Chamber I*, 2 September 1998.

The Prosecutor V. Kupreškić, Case No. It-95-16-*T, Icty*, 14 January 2000.

The Prosecutor V. Lubanga (Decision on Confirmation of Charges) Icc-01/04-01/06 29 January 2007.

The Prosecutor V. Ramush Haradinaj, Judgement (Trial Chamber), Case No. It-04-84-*T*, 3 April 2008 3 April 2008.

The Prosecutor V. Rutaganda, Ictr-96-3-*T, Judgment*, 6 December 1999.

Chamber of International Criminal Tribunal for the Former Yugoslavia. *Prosecutor V. Strugar*, 2008.

"Protocol Additional of the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol Ii)." 8 JUNE 1977.

"Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)." 8 June 1977.

"Protocol on Prohibitions or Restrictions on the Use of Mines, Booby Traps and Other Devices (Protocol Ii) Annexed to the 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) ".

Reuters. "Factbox: What Is Stuxnet?" http://www.reuters.com/article/us-security-cyber-iran-fb-idUSTRE68N3PT20100924.

———. "Iran Says Cyber Foes Caused Centrifuge Problems." http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129.

Rex Hughes. "A Treaty for Cyberspace." *International Affairs* 86, no. 2 (2010): 523-41.

RIA Novosti. "Russia Considering Establishing Cyber-Security Command " Atlantic Council, http://www.atlanticcouncil.org/blogs/natosource/russia-considering-establishing-cybersecurity-command.

Richard A Clarke and Robert K Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins, 2010.

Robert Kolb and Richard Hyde. *An Introduction to the International Law of Armed Conflicts*. USA: Hart Publishing, 2008.

"Rome Statute of the International Criminal Court." opened for signature 17 July 1998, entered into force 1 July 2002.

SCO. "Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (Unofficial Translation)." 2008.

———. "Brief Introduction to the Shanghai Cooperation Organisation " http://www.sectsco.org/EN123/brief.asp.

Sean Watts. "Combatant Status and Computer Network Attack." *Virginia Journal of International Law* 50, no. 2 (2010).

SecurityWeek News. "Cyberwarfare Brazilian Army to Get Cyberwarfare Training and Security Support from Panda Security."

http://www.securityweek.com/brazilian-army-get-cyberwarfare-training-and-security-support-panda-security.

Shanghai Cooperation Organisation. "Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation." 16 June 2009.

Stacy Combest. "Building a Cyber Secure Plant." Siemens totally integrated automation, http://www.totallyintegratedautomation.com/2010/09/building-a-cyber-secure-plant/.

Stephanie Pepi. "Usaid Launches the Albanian Cyber-Security Program." https://www.usaid.gov/news-information/press-releases/usaid-launches-albanian-cyber-security-program.

Steven Adair. "Georgian Websites under Attack - Ddos and Defacement." https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080811.

Stuart S. Malawer. "Cyber Warfare: Law and Policy Proposals for U.S. And Global Governance." *Virginia Lawyer* 58 (2010).

Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts edited by Michael N. Schmitt: Cambridge University Press, 2013.

Teerapat Asavasungsidhi. "Customary Law." *International Review of the Red Cross* 87, no. 857 (2005).

The Chosunilbo. "Cyber Security Is Vital for National Defense." http://english.chosun.com/site/data/html_dir/2009/11/02/2009110200788.html.

The Hindu. "India, Pakistan Become Full Sco Members." http://www.thehindu.com/news/international/india-gets-full-membership-of-the-shanghai-cooperation-organisation-along-with-pakistan/article7407873.ece.

The News Desk. "Brazilian Army Prepares Its Cdciber, the 'Cyber Defense Center'." Linha Defensiva, http://www.linhadefensiva.com/2012/05/brazilian-army-prepares-its-cdciber-the-cyber-defense-center/.

Tim Maurer. *Cyber Norm Emergence at the United Nations – an Analysis of the Un's Activities Regarding Cyber-Security*. Discussion Paper 2011-11. Cambridge: Belfer Center for Science and International Affairs, 2011.

UN. "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary (International Code of Conduct for Information Security)." 2015.

UNGA. "Developments in the Field of Information and Telecommunications in the Context of International Security " In *A/*64/386, 2009.

———. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." In *A/*65/201, 2010.

———. "Resolution Adopted by the General Assembly on 23 December 2015 (a/Res/70/237)." 2015.

———. "Resolution Adopted by the General Assembly: 53/70. Developments in the Field of Information and Telecommunications in the Context of International Security (a/Res/53/70)." 1999.

UNIDIR. "The Cyber Index: International Security Trends and Realities." Geneva, Switzerland: United Nations, 2013.

———. "Cyber Stability Conference Series." http://www.unidir.org/programmes/emerging-security-threats/cyber-stability-conference-series.

———. "Emerging Security Threats." http://www.unidir.org/programmes/emerging-security-threats.

———. "The Institute." http://www.unidir.org/about/the-institute.

———. "International Law and State Behaviour in Cyberspace Meeting Series." http://www.unidir.org/programmes/emerging-security-threats/international-law-and-state-behaviour-in-cyberspace-meeting-series.

———. "International Security Cyber Issues Workshop Series." http://www.unidir.org/programmes/emerging-security-threats/international-security-cyber-issues-workshop-series.

———. "Mandate." http://www.unidir.org/about/the-institute/mandate.

———. "Support to the Un Gges (Space and Cyber)." http://www.unidir.org/programmes/emerging-security-threats/support-to-the-un-gges-space-and-cyber.

United Nations. "Charter of the United Nations."

———. "Civil Society." http://www.un.org/en/sections/resources/civil-society/index.html.

———. "What We Do." https://www.un.org/en/sections/what-we-do/index.html.

United Nations General Assembly Resolution 3314, (XXIX). "Resolution 3314 (Xxix), Definition of Aggression." 1970.

UNODA. "Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security." 2015.

Vijay M. Padmanabham. "Cyber Worriors and the Jus in Bello." *International Law Studies* 89 (2013).

"What Is Ihl? (International Humanitarian Law: Answers to Your Questions)." (18 September 2015). https://www.icrc.org/en/document/what-ihl.

William C. Ashmore. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defence Review* 11 (2009).

William H. Boothby. "Methods and Means of Cyber Warfare." *International Law Studies* 89 (2013).

———. *Weapons and the Law of Armed Conflict*. OUP Oxford, 2009.

William J. Broad and David E. Sanger. "Worm Was Perfect for Sabotaging Centrifuges." The New York Times, http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?_r=0.

William J. Lynn III. "Defending a New Domain." the Council on Foreign Relations, Foreign Affairs, 2010.

William M. Arkin. "The Cyber Bomb in Yugoslavia." washingtonpost.com, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

Xinhua. "Iran's Armed Forces to Launch 'Cyber Command'." China Daily, http://www.chinadaily.com.cn/world/2011-06/16/content_12707489.htm.

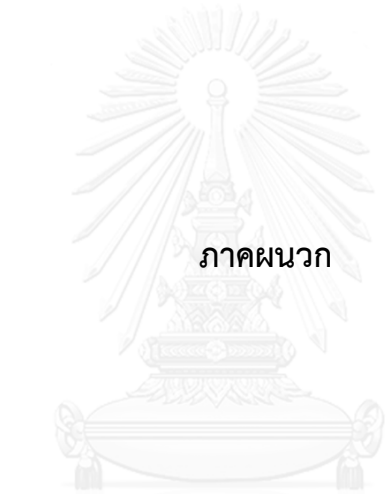
Yoram Dinstein. *The Conduct of Hostilities under the Law of International Armed Conflict*. edited by Second United Kingdom: Cambridge University Press, 2010.

———. "Discussion." Chap. PART III: Targeting In *Legal and Ethical Lessons of Nato's Kosovo Campaign*, edited by Andru E. Wall. Newport: Naval War College, 2002.

———. "The Principle of Distinction and Cyber War in International Armed Conflicts." *Journal of Conflict & Security Law* 17, no. 2 (2012): 261-77.

Yossi Melman. "Iran Pauses Uranium Enrichment at Natanz Nuclear Plant." Haaretz .COM, http://www.haaretz.com/news/world/iran-pauses-uranium-enrichment-at-natanz-nuclear-plant-1.326276.

ภาคผนวก



ภาคผนวก 1

REPORT OF THE GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Summary

Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. Threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.

The growing use of information and communications technologies (ICTs) in critical infrastructure creates new vulnerabilities and opportunities for disruption. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Since ICTs are inherently dual-use in nature, the same technologies that support robust e-commerce can also be used to threaten international peace and national security.

The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence, and they can act from virtually anywhere. These attributes facilitate the use of ICTs for disruptive activities. Uncertainty regarding attribution and the absence of a common understanding creates the risk of instability and misperception.

There is increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. The growing sophistication and scale of criminal activity increases the potential for harmful action. While there are few indications of terrorist use of ICTs to execute disruptive operations, it may intensify in the future.

Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. The report of the Group of Governmental Experts offers recommendations for further dialogue among States to reduce risk and protect critical national and international infrastructure.

Foreword by the Secretary-General

A decade ago we could not have foreseen how deeply information technologies and telecommunications would be integrated into our daily lives, or how much we would come to rely on them. These technologies have created a globally linked international community and, while this linkage brings immense benefits, it also brings vulnerability and risk.

Considerable progress has been made in addressing the implications of the new technologies. But the task is arduous and we have only begun to develop the norms, laws and modes of cooperation needed for this new information environment.

With that in mind, I appointed a group of governmental experts from 15 States to study existing and potential threats in this sphere, and to recommend ways to address them. I thank the Chair of the Group and the experts for their diligent and careful work, which has produced this report, a concise statement of the problem and of possible next steps.

The General Assembly has an important role to play in the process of making information technology and telecommunications more secure, both nationally and internationally. Dialogue among Member States will be essential for developing common perspectives. Practical cooperation is also vital, to share best practices, exchange information and build capacity in developing countries, and to reduce the risk of misperception, which could hinder the international community's ability to manage major incidents in cyberspace.

This is a rich agenda for future work. The present report is meant to serve as an initial step towards building the international framework for security and stability that these new technologies require. I commend its analysis and recommendations to Member States and to a wide global audience.

Letter of transmittal

16 July 2010

I have the honour to submit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established in 2009 pursuant to paragraph 4 of General Assembly resolution 60/45. As Chair of the Group, I am pleased to inform you that consensus was reached on the report.

In that resolution, entitled "Developments in the field of information and telecommunications in the context of international security", the General Assembly requested that a group of governmental experts be established in 2009, on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as concepts aimed at strengthening the security of global information and telecommunications systems. The Secretary-General was requested to submit a report on the results of that study to the General Assembly at its sixtyfifth session.

In accordance with the terms of the resolution, experts were appointed from 15 States: Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland and the United States of America. The list of experts is contained in the annex.

The Group of Governmental Experts met in four sessions: the first from 24 to 26 November 2009 in Geneva; the second from 11 to 15 January 2010 at United Nations Headquarters; the third from 21 to 25 June 2010 in Geneva; and the fourth from 12 to 16 July at United Nations Headquarters.

The Group had a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international security. Furthermore, the Group took into account the views expressed in the replies received from Member States in response to General Assembly resolutions 60/45, 61/54, 62/17 and 63/37, respectively entitled "Developments in the field of information and telecommunications in the context of international security", as well as contributions and background papers made available by individual members of the Group. The Group wishes to express its appreciation for the contribution of the United Nations Institute for Disarmament Research, which served as consultant to the Group and which was represented by James Lewis and Kerstin Vignard.

The Group also wishes to express its appreciation to Ewen Buchanan, Information Officer of the Information and Outreach Branch of the Office for Disarmament Affairs of the Secretariat, who served as Secretary of the Group, and to other Secretariat officials who assisted the Group.

(Signed) Andrey V. Krutskikh
Chairman of the Group

I. Introduction

1. Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. These threats may cause substantial damage to economies and national and international security. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.

2. Information and communication technologies (ICTs) have unique attributes that make it difficult to address threats that States and other users may face. ICTs are ubiquitous and widely available. They are neither inherently civil nor military in nature, and the purpose to which they are put depends mainly on the motives of the user. Networks in many cases are owned and operated by the private sector or individuals. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Malicious use of ICTs can easily be concealed. The origin of a disruption, the identity of the perpetrator or the motivation can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence. Threat actors can operate with substantial impunity from virtually anywhere. These attributes facilitate the use of ICTs for disruptive activities.

3. Considering the implications of these developments for international security, the United Nations General Assembly asked the Secretary-General, with the assistance of governmental experts, to study both threats in the sphere of information security and relevant international concepts and to suggest possible cooperative measures that could strengthen the security of global information and communication systems.

II. Threats, risks and vulnerabilities

4. The global network of ICTs has become an arena for disruptive activity. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of State conflict. The source of these threats includes non-State actors such as criminals and, potentially, terrorists, as well as States themselves. ICTs can be used to damage information resources and infrastructures. Because they are inherently dual-use in nature, the same ICTs that support robust e-commerce can also be used to threaten international peace and national security.

5. Many malicious tools and methodologies originate in the efforts of criminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions.

. 6. Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future. At the present time terrorists mostly rely on these technologies

to communicate, collect information, recruit, organize, promote their ideas and actions, and solicit funding, but could eventually adopt the use of ICTs for attack.

7. There is increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes. Uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception.

8. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. Such proxies, whether motivated by financial gain or other reasons, can offer an array of malicious services to State and non-State actors.

9. The growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services.

10. States are also concerned that the ICT supply chain could be influenced or subverted in ways that would affect the normal, secure and reliable use of ICTs. The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security.

11. The varying degrees of ICT capacity and security among different States increases the vulnerability of the global network. Differences in national laws and practices may create challenges to achieving a secure and resilient digital environment.
III. Cooperative measures

12. The risks associated with globally interconnected networks require concerted responses. Member States over the past decade have repeatedly affirmed the need for international cooperation against threats in the sphere of ICT security in order to combat the criminal misuse of information technology, to create a global culture of cybersecurity and to promote other essential measures that can reduce risk.

13. Over the past decade, efforts to combat the threat of cybercrime have been conducted internationally, in particular, within the Shanghai Cooperation Organization, the Organization of American States, the Asia-Pacific Economic Cooperation Forum, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Economic Community of West African States, the African Union, the European Union, the Organization for Security and Cooperation in Europe and the Council of Europe, as well as through bilateral efforts between States.

14. Non-criminal areas of transnational concern should receive appropriate attention. These include the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to State use of ICTs, which could affect crisis management in the event of major incidents. This argues for the elaboration of measures designed to enhance cooperation where possible. Such

measures could also be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability.

15. As disruptive activities using information and communications technologies grow more complex and dangerous, it is obvious that no State is able to address these threats alone. Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. Therefore, the international community should examine the need for cooperative actions and mechanisms.

16. Existing agreements include norms relevant to the use of ICTs by States. Given the unique attributes of ICTs, additional norms could be developed over time.

17. Capacity-building is of vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security. Close international cooperation will be needed to build capacity in States that may require assistance in addressing the security of their ICTs.

IV. Recommendations

18. Taking into account the existing and potential threats, risks and vulnerabilities in the field of information security, the Group of Governmental Experts considers it useful to recommend further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions:

(i) Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure;

(ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;

(iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;

(iv) Identification of measures to support capacity-building in less developed

(v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.

Annex

List of members of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Mr. Vladimir N. Gerasimovich
Head of the Department of International Security and Arms Control
Ministry of Foreign Affairs
Belarus

Mr. Aleksandr Ponomarev (third session)
Counsellor of the Permanent Mission of the Republic of Belarus to the United Nations Office at Geneva

Mr. Alexandre Mariano Feitosa
Commander
Brazilian Marine Corps, Brazilian Navy
Policy, Strategy and International Affairs Secretariat
Ministry of Defence
Brazil

Mr. Li Song (first and second sessions)
Deputy Director General
Department of Arms Control and Disarmament
Ministry of Foreign Affairs
China

Mr. Kang Yong (third and fourth sessions)
Deputy Director General
Department of Arms Control and Disarmament
Ministry of Foreign Affairs
China

Mr. Linnar Viik
Associate Professor
Estonian IT College
Estonia

Mr. Aymeric Simon
Relations internationales
Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
France

Mr. Gregor Koebel
Head of the Division for Conventional Arms Control
Federal Foreign Office
Germany

Mr. B. J. Srinath
Senior Director
Indian Computer Emergency Response Team
Department of Information Technology
India

Ms. Rodica Radian-Gordon
Director
Arms Control Department
Ministry of Foreign Affairs
Israel

Mr. Vincenzo Della Corte (first and third sessions)
Director of Communication Security Sector
Presidency of the Council of Ministers
Italy

Mr. Walter Mecchia (second and fourth sessions)
Communication Security Sector
Presidency of the Council of Ministers
Italy

Mr. Rashid A. Al-Mohannadi (first session)
Commander of the Land Forces Signal Company
Amiri Signal Corps
Qatar

Mr. Saad M. R. Al-Kaabi
Lieutenant Colonel (Engineer)
Ministry of Defence
Qatar

Mr. Lew Kwang-chul
Ambassador
Ministry of Foreign Affairs and Trade
Republic of Korea

Mr. Andrey V. Krutskikh
Deputy Director
Department of New Challenges and Threats
Ministry of Foreign Affairs
Russian Federation

Ms. Palesa Banda (first session)
Deputy Director, Internet Governance
Department of Communication
South Africa

Maj. Gen. Mario Silvino Brazzoli
Government Information Technology Officer
Department of Defence
South Africa

Mr. Gavin Willis
International Relations Team
National Technical Authority for Information Assurance (CESG)
United Kingdom of Great Britain and Northern Ireland

Ms. Michele G. Markoff
Senior Policy Adviser
Office of Cyber Affairs
US Department of State
United States of America

ภาคผนวก 2

INTERNATIONAL CODE OF CONDUCT FOR INFORMATION SECURITY

Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General

[Original: Chinese and Russian]

International code of conduct for information security

The General Assembly,

Recalling its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012 and 68/243 of 27 December 2013, on developments in the field of information and telecommunications in the context of international security,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Recognizing the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies and, in that context, stressing the role that can be played by the United Nations and other international and regional organizations,

Highlighting the importance of the security, continuity and stability of the Internet and the need to protect the Internet and other information and communication technology networks from threats and vulnerabilities, and reaffirming the need for a common understanding of the issues of Internet security and for further cooperation at the national and international levels,

Reaffirming that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues,

Bearing in mind the assessments and recommendations contained in the report of the Group of Governmental Experts established in 2012 on the basis of equitable geographical distribution, in fulfilment of resolution 66/24, and which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them,

including norms, rules or principles of responsible behaviour of States and confidence-building measures in the information space, and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Stressing the need to develop a common understanding of how norms derived from existing international law relevant to the use of information and communication technologies by States, a measure essential to reduce risks to international peace, security and stability, will apply to State behaviour and the use of information and communication technologies by States, in accordance with paragraph 16 of the report of the Group of Governmental Experts (A/68/98 of 24 June 2013),

Noting that, given the unique attributes of information and communication technologies, additional norms could be developed over time, in accordance with paragraph 16 of the report of the Group of Governmental Experts,

Recognizing that confidence and security in the use of information and communications technologies are among the main pillars of the information society and that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented, pursuant to General Assembly resolution 64/211, entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures",

Stressing the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries in the areas of cybersecurity best practices and training, pursuant to that General Assembly resolution,

Adopts the following international code of conduct for information security:

1.Purpose and scope

The purpose of the present code of conduct is to identify the rights and responsibilities of States in the information space, promote constructive and responsible behaviour on their part and enhance their cooperation in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open and founded on cooperation, and to ensure that the use of information and communications technologies and information and communications networks facilitates the comprehensive economic and social development and well-being of peoples, and does not run counter to the objective of ensuring international peace and security.

Adherence to the code is voluntary and open to all States.

2.Code of conduct

Each State voluntarily subscribing to this Code of Conduct pledges:

(1) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries;

(2) Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security;

(3) Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability;

(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds;

(5) To endeavour to ensure the supply chain security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and communications networks to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security;

(6) To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage;

(7) To recognize that the rights of an individual in the offline environment must also be protected in the online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information, taking into account the fact that the International Covenant on Civil and Political Rights (article 19) attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) for respect of the rights or reputations of others;

(b) for the protection of national security or of public order (ordre public), or of public health or morals;

(8) All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet;

(9) All States must cooperate fully with other interested parties in encouraging a deeper understanding by all elements in society, including the private sector and civil-society institutions, of their responsibility to ensure information security, by means including the creation of a culture of information security and the provision of support for efforts to protect critical information infrastructure;

(10) To develop confidence-building measures aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict. Such measures will include, inter alia, voluntary exchange of information regarding national strategies and organizational structures for ensuring a State's information security, the publication of white papers and exchanges of best practice, wherever practical and advisable;

(11) To assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide;

(12) To bolster bilateral, regional and international cooperation, promote a prominent role for the United Nations in areas such as encouraging the development of international legal norms for information security, peaceful settlement of international disputes, qualitative improvements in international cooperation in the field of information security; and to enhance coordination among relevant international organizations;

(13) To settle any dispute resulting from the application of this code of conduct through peaceful means, and to refrain from the threat or use of force.

ภาคผนวก 3

ASEAN REGIONAL FORUM STATEMENT ON COOPERATION IN FIGHTING CYBER ATTACK AND TERRORIST MISUSE OF CYBER SPACE

ASEAN REGIONAL FORUM
STATEMENT ON COOPERATION IN FIGHTING CYBER ATTACK AND TERRORIST MISUSE OF CYBER SPACE

The Chairman of the ASEAN Regional Forum (ARF), on behalf of the participating states and organization, issues the following statement:

Strongly condemning all acts of terrorism regardless of their motivations, whenever and by whomsoever committed, as one of the most serious threats to international peace and security;

Reaffirming the imperative to combat terrorism in all its forms and manifestations;

Rejecting any attempt to associate terrorism with any religion, nationality, race, or culture;

Ensuring that all measures to combat terrorism are in accordance with the United Nations Charter and other applicable principles of international law, including humanitarian and human rights law;

Acknowledging that terrorist misuse of cyber space is a destructive and devastating form and manifestation of global terrorism whose magnitude and rapid spread would be exacerbated by the increasing cyber interconnectivity of countries in the region;

Recognizing the serious ramifications of an attack via cyber space to critical infrastructure on the security of the people and on the economic and physical well-being of countries in the region;

Recognizing the detrimental impact of fear which can be enhanced by the terrorists in conjunction with attacks in physical space;

Further recognizing that terrorist misuse of cyber space is a form of cyber crime and a criminal misuse of information technologies;

Acknowledging that the proceeds from cyber crime may be laundered and/or used to fund terrorist activities;

Emphasizing the importance of ARF countries acting cooperatively to prevent the exploitation of technology, communications, and resources, including Internet, to

incite support for and/or commit criminal or terrorist acts, including the use by terrorists of the internet for recruitment and training purposes.

Recalling the ARF Statement on Strengthening Transport Security against International Terrorism of 2 July 2004, which mentions, in particular, that ARF countries will endeavor to cooperate to ensure that terrorists are prevented from using information technology and its applications to disrupt and sabotage the operation of transportation systems;

Stressing the need for cooperation between governments and the private sector in identifying, preventing, and mitigating cyber-attacks and terrorist misuse of cyber-space;

Believing that an effective fight against cyber-attacks and terrorist misuse of cyber space requires increased, rapid and well-functioning legal and other forms of cooperation.

1. ARF participating states and organization endeavor to enact, if they have not yet done so, and implement cyber crime and cyber security laws in accordance with their national conditions and by referring to relevant international instruments and recommendations/guidelines for the prevention, detection, reduction, and mitigation of attacks to which they are party, including the ten recommendations in the UN General Assembly Resolution 55/63 on Combating the Criminal Misuse of Information Technologies.

2. ARF participating countries and organization acknowledge the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework that may include the following proposed courses of action:

   - Identify national cyber security units and increase coordination among national agencies;
   - Develop national watch, warning, and incident response capabilities;
   - Collaborate/cooperate with international and regional agencies for cyber investigation and collection and sharing of cyber evidence and, effective management of resources for mutually beneficial partnerships that foster international cooperation, interoperability, and coordination in fighting criminal and terrorist misuse of cyber space;
   - Conduct training/ technology transfer and counter-measures, especially digital forensics;
   - Reinforce capabilities to protect and recover critical infrastructure, minimize loss, track and trace the sabotage activities on such infrastructure;

- Encourage private sector partnership with the government in the field of information security and fighting cyber crime, including the protection of critical infrastructure;
- Increase public awareness on cyber security and cyber ethics with emphasis on safety and security, best practices, the responsibilities of using information networks and negative consequences from misuse of networks.

3. ARF participating states and organization agree to work together to improve their capabilities to adequately address cyber crime, including the terrorist misuse of cyber space by:

- Endeavoring to identify national cyber security units and joining and participating in established networks of cooperation;
- Endeavoring to establish an ARF-wide network of Computer Security Incident Response Teams (CSIRT) concerning cybercrime to facilitate the real time exchange of threat and vulnerability assessment and issuance of required warnings and patches and which would join existing cyber and incident warning and response networks;
- Leveraging on existing cooperation among different CSIRT networks and collaborating with other international and regional organizations with similar concerns;
- Providing, where and when possible, technical assistance and capacity-building programs to countries that request help in developing laws, extending training (in forensics, law enforcement, legal and technical matters), and when and where possible, providing hardware and software;
- Within the framework of applicable data protection regulation, information and intelligence sharing between law enforcement, partners, and regional agencies, and community;
- Enhancing efforts towards training and awareness among the masses to bring about a culture of cyber security.

4. The ARF participating countries and organization also commit to continue working together in the fight against cyber crime, including terrorist misuse of cyber space, through activities aimed at enhancing confidence among different national CSIRTs, as well as formulating advocacy and public awareness programs.

5. ARF participating countries and organization commit themselves to adopting such measures as may be appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts, including through computer networks.

6. The ARF participating countries and organization decide to annually review the progress of these and other efforts to combat cyber attack and the terrorist misuse of cyber space at subsequent ARF Ministerial Meetings.

28 July 2006
Kuala Lumpur

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวอุบลวรรณ ภีระเป็ง สำเร็จการศึกษาระดับมัธยมศึกษาจากโรงเรียนยุพราชวิทยาลัย จังหวัดเชียงใหม่ เมื่อปี พ.ศ. 2548 และเข้าศึกษาต่อระดับอุดมศึกษาที่คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่ สำเร็จการศึกษาเมื่อปี พ.ศ. 2552 และเข้าศึกษาต่อที่สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภาในปีเดียวกันจนสำเร็จการศึกษาขั้นเนติบัณฑิต สมัยที่ 63 ปี พ.ศ. 2553 ก่อนเข้าศึกษาต่อในหลักสูตรนิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย