สงครามไซเบอร์กับการนิยามใหม่ของการทำสงครามในการเมืองระหว่างประเทศยุคร่วมสมัย (Cyber Warfare and the re-definition of war in International Politics of Contemporary world)"[1]

ฐิติมาศ ศรีสุข[2]

สงครามไซเบอร์คือความท้าทายรูปแบบใหม่ต่อปทัสถานที่สร้างความมั่นคงระหว่างประเทศ ที่ผ่านมาสงครามรูปแบบเดิม (Traditional War) ล้วนตั้งอยู่บนปทัสถานว่าด้วยสงครามที่เป็นธรรม (Just War) ซึ่งประกอบด้วย ปทัสถานที่ว่าด้วยการไม่ก่อสงคราม เว้นแต่จะเป็นสงครามที่มีเหตุอันชอบธรรม และวิธีการก่อสงครามที่จะต้อง ไม่สร้างความเดือดร้อนแก่พลเรือน อย่างไรก็ตาม เนื่องด้วยลักษณะอันไร้ซึ่งพรมแดนของโลกไซเบอร์ที่ทำให้ขอบเขต อำนาจรัฐไม่อาจเอื้อมถึง ทำให้รัฐไม่อาจประกันความมั่นคงให้เกิดขึ้นภายใต้พื้นที่ดังกล่าว ซึ่งในปัจจุบันที่มนุษยชาติยิ่ง พึ่งพาพื้นที่โลกไซเบอร์มากขึ้นเรื่อยๆ ก็ยิ่งทำให้

[1]บทความนี้เป็นส่วนหนึ่งของการฝึกอบรมหลักสูตรความมั่นคงศึกษา (ระดับต้น) รุ่นที่ ๓
[2]เรียบเรียงโดย นางสาวฐิติมาศ ศรีสุข นักวิเคราะห์นโยบายและแผนปฏิบัติการ กองความมั่นคงระหว่างประเทศ สำนักงานสภาความมั่นคงแห่งชาติ, รัฐศาสตร์บัณฑิต จุฬาลงกรณ์มหาวิทยาลัย

มนุษยชาติมีความเปราะบางต่อภัยคุกคามของโลกไซเบอร์มากขึ้น และด้วยข้อเท็จจริงที่ว่าผลกระทบของการไร้ซึ่งความสามารถในการสร้างความมั่นคงของรัฐในพื้นที่ดังกล่าว อีกทั้ง สงครามก็ยิ่งมีแนวโน้มที่จะขยับขยายเข้าสู่พื้นที่ดังกล่าวมากขึ้น ก็ยิ่งเป็นที่ประจักษ์ว่าปทัสถานว่าด้วยสงครามที่เป็นธรรม ซึ่งมีอิทธิพลอย่างยิ่งในโลกปัจจุบัน จะต้องได้รับการปรับปรุง เพื่อให้สอดคล้องกับบริบทของโลกที่เปลี่ยนแปลง อย่างมีนัยสำคัญต่อไป

บทนำ

หากกล่าวถึงการเมืองระหว่างประเทศ การทำสงครามถือเป็นตัวแปรสำคัญตัวแปรหนึ่งที่กำหนดกรอบของความสัมพันธ์ในการเมืองระหว่างประเทศ ตลอดระยะเวลาในประวัติศาสตร์ของมวลมนุษยชาติ ทั้งการอุบัติขึ้นของอารยธรรมอาณาจักร หรือแม้แต่รัฐชาติ สงครามล้วนเป็นตัวแปรสำคัญที่ทำให้สิ่งเหล่านี้กำเนิดขึ้นเกือบจะเสมอ แม้ว่าสงครามจะเต็มไปด้วยการประหัตประหารฆ่าฟัน ความโหดร้ายป่าเถื่อน และการสูญเสีย แต่ก็ปฏิเสธไม่ได้เลยว่าระบบการเมืองระหว่างประเทศที่สามารถสร้างสันติภาพในระดับหนึ่งได้อย่างทุกวันนี้ เกิดขึ้นจากสงคราม[3]

สงครามเกี่ยวข้องโดยตรงกับการขยายและจำกัดอำนาจของรัฐทั้งหลาย แม้ว่าในปัจจุบันการก่อสงครามจะเป็นสิ่งที่ไม่อาจยอมรับได้ในการเมืองระหว่างประเทศ แต่รัฐทั้งหลายก็ล้วนแล้วแต่พยายามจะหานวัตกรรมใหม่ๆ ในการก่อสงครามเพื่อขยายอำนาจรัฐ และจำกัดอำนาจรัฐอื่นๆ มิให้กลายเป็นภัยคุกคามแก่รัฐของตนได้ในอนาคต เพื่อการได้มาและจำกัดซึ่งอำนาจ รัฐต่างๆ ได้พยายามพัฒนาเทคโนโลยีทางการทหาร เพื่อให้ทัดเทียมหรือเหนือกว่ารัฐอื่นๆ เพื่อประกันความมั่นคงแห่งรัฐของตนทั้งในแง่การสร้างความมั่นคงผ่านการขยายอำนาจและผ่านการป้องกันโดยสะสมกำลังสรรพอาวุธ

หากกล่าวถึงยุคสมัยปัจจุบัน หลายท่านอาจกล่าวว่า ยุคแห่งสงครามระหว่างรัฐได้สิ้นสุดลงแล้ว ถึงเวลาของยุคแห่งวิวัฒนาการทางเทคโนโลยีจะเข้ามาแทนที่การประหัตประหารกันเพื่อความมั่นคงแห่งรัฐ การพัฒนาการทางเทคโนโลยีนี้จะนำไปสู่ความเจริญก้าวหน้าของมนุษยชาติ เทคโนโลยีที่พัฒนาไปอย่างไม่หยุดยั้งและควบคู่ไปกับการเชื่อมต่อกันอย่างไร้รอยต่อของโลกยุคใหม่ผ่านการร่วมมือกันทางเศรษฐกิจดูจะเป็นความหวังที่จะนำไปสู่สันติภาพ

ในยุคแห่งความหวังและความฝันนี้ คอมพิวเตอร์ถือได้ว่าเป็นเครื่องมือทางเทคโนโลยีที่สำคัญที่สุดที่ก่อให้เกิดการพัฒนาการของมนุษย์ในทุกๆ มิติ พัฒนาการของเทคโนโลยีคอมพิวเตอร์ก่อให้เกิดความก้าวหน้าทางเทคโนโลยีมากมาย เช่น ระบบคำนวณคณิตศาสตร์ที่มีประสิทธิภาพขึ้นสูง ระบบปฏิบัติการที่อำนวยความสะดวกในพัฒนาการทางวิทยาศาสตร์ ระบบปฏิบัติการที่ช่วยในการเชื่อมองค์กรต่างๆ ของรัฐบาลเข้าด้วยกัน หรือแม้แต่ระบบปฏิบัติการทางด้านการทหารในปัจจุบันก็ตาม ทั้งหมดนี้ล้วนเกิดขึ้นจากพัฒนาการของคอมพิวเตอร์ จึงไม่ผิดเลยที่จะกล่าวว่าต้นตอแห่งวิวัฒนาการทางด้านเทคโนโลยีในยุคปัจจุบัน คือ คอมพิวเตอร์

อย่างไรก็ตาม ไม่ว่าโลกจะพัฒนาไปเพียงไร แต่สาระสำคัญที่ว่า รัฐจำเป็นจะต้องอยู่รอดและปราศจากการแทรกแซงจากรัฐภายนอก ยังถือเป็นข้อเท็จจริงสำหรับการเมืองระหว่างประเทศในทุกยุคทุกสมัย[4] เกมการเมืองระหว่างรัฐไม่เคยหายไป และมีแนวโน้มที่จะรุนแรงขึ้น โดยเฉพาะอย่างยิ่งเมื่อคอมพิวเตอร์กลายเป็นปัจจัยสำคัญอย่างยิ่งในพัฒนาการทางเทคโนโลยี และช่วยอำนวยความสะดวกในเก็บข้อมูล ดำเนินกิจการต่างๆ ของรัฐ

[3]Bruce D. Porter, War and the Rise of the State (New Yrok: The Free Press, 1994), 2-5.
[4]Steven L. Lamy, Globalisation of World Politics, (New York, Oxford University Press, 2011), 116-129.

และสนับสนุนให้ปฏิบัติการของรัฐมีประสิทธิภาพสูงขึ้น ประเด็นด้านความมั่นคง ก็ย่อมเป็นความเสี่ยงที่ตามมาจากการใช้เทคโนโลยีอันแสนประเสริฐนี้ ในยุคปัจจุบัน สงครามระหว่างรัฐ การแก่งแย่งชิงดี และการต่อสู้ ได้พัฒนารูปแบบตามพัฒนาการของเทคโนโลยี และแทรกซึมเข้ามาในพื้นที่ของโลกไซเบอร์ หรือโลกเสมือนจริงในคอมพิวเตอร์ ที่เชื่อมต่ออย่างกว้างขวางและทั่วถึง หนึ่งในกรณีที่โด่งดังที่สุดของการโจมตีระหว่างรัฐกับรัฐในโลกไซเบอร์ คือ กรณีการโจมตีโปรแกรมนิวเคลียร์ของอิหร่าน โดยมัลแวร์ชนิดเวิร์มนามว่า Stuxnet[5] ซึ่งก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ของในโปรแกรมนิวเคลียร์ของอิหร่านในระดับหนึ่ง

การอุบัติขึ้นของสงครามในโลกไซเบอร์นี้ ได้นำไปสู่ปฏิกริยาที่หลากหลาย ทั้งฝ่ายที่มองว่าปฏิบัติการดังกล่าวมิได้ก่อให้เกิดความสูญเสียทางชีวิต กับบางฝ่ายที่มองว่าปฏิบัติการนี้กระทบต่อความมั่นคงของรัฐอย่างยิ่งยวด จึงทำให้เกิดคำถามที่ว่านิยามของรูปแบบการทำสงคราม และข้อจำกัดอันเกี่ยวเนื่องกับปทัสถานว่าด้วย “สงครามอันชอบธรรม” (Just War)[6] ที่มีอยู่ในปัจจุบัน เพียงพอหรือไม่ต่อการรับมือกับสถานการณ์การเมืองโลกที่ได้เปลี่ยนแปลงไปแล้วดังที่ได้กล่าว ประเด็นนี้จึงกลายเป็นจุดสนใจของงานเขียนชิ้นนี้ที่พยายามจะให้คำตอบ

ในงานเขียนชิ้นนี้ ข้าพเจ้ามีความประสงค์จะชี้ให้เห็นว่า การอุบัติขึ้นของสงครามรูปแบบใหม่หรือสงครามไซเบอร์อันเกิดจากความก้าวหน้าทางเทคโนโลยี เป็นจุดเปลี่ยนสำคัญอันหนึ่งที่จะทำให้รัฐและองค์กรที่เกี่ยวข้องต้องปรับวิสัยทัศน์ในการจัดการด้านความมั่นคง และสร้างกรอบปทัสถานบางอย่าง เพื่อให้เกิดดุลยภาพในเวทีการเมืองระหว่างประเทศ งานเขียนแบ่งออกเป็น 5 ส่วน ส่วนแรกจะกล่าวถึงแนวคิดว่าด้วยสงครามและความมั่นคงในปัจจุบัน ส่วนที่สอง อธิบายเกี่ยวกับสงครามไซเบอร์ ส่วนที่สามกล่าวถึงผลกระทบต่อความมั่นคงของระบบการเมืองระหว่างประเทศที่อาจเกิดขึ้นได้จากการอุบัติของสงครามโลกไซเบอร์ ส่วนที่สี่ จะกล่าวถึงการนิยามรูปแบบสงครามอันชอบธรรมใหม่ เพื่อตอบรับกับสงครามไซเบอร์ที่มีแนวโน้มจะเกิดขึ้น ส่วนที่ห้าจะกล่าวถึงส่วนสรุป

ว่าด้วยการสงคราม (On Warfare)

เป็นที่เข้าใจกันโดยทั่วไปว่า สงคราม[7] หมายถึงความขัดแย้งอันเกี่ยวเนื่องกับการใช้อาวุธที่เกี่ยวข้องกันระหว่างองค์กรอย่างรัฐต่อรัฐ สงครามทำให้เกิดผลกระทบเชิงลบต่อสังคมมากมายทั้งระหว่างและหลังสงคราม เช่น เกิดความเสียหายต่อชีวิตและทรัพย์สิน เกิดความชะงักชะงันของเศรษฐกิจ สภาพการเมืองอันไม่เป็นปกติ โดยทั่วไปแล้ว ภาวะสงคราม จึงเป็นสิ่งอันไม่พึงประสงค์ เพราะเป็นภัยคุกคามที่ใหญ่หลวงที่สุดต่อความมั่นคงและความอยู่รอดของประเทศ ตลอดระยะเวลาในประวัติศาสตร์มีรัฐที่ถูกลบหายออกไปจากแผนที่หลังจากการเกิดขึ้นของสงครามมากมาย เช่น หลังจากสงครามโลกครั้งที่ 1 สิ้นสุดลง อาณาจักรอันยิ่งใหญ่ที่มีอายุหลายร้อยปีต้องล่มสลายลงมากมายจากผลของสงคราม อาทิ อาณาจักรออสโตร-ฮังการี อาณาจักรรัสเซีย อาณาจักรเยอรมัน และอาณาจักรออตโตมัน และแตกเป็นรัฐย่อยๆ[8] มากมายอีกหลายรัฐ จึงจะเห็นได้ว่าผลกระทบของสงคราม มีพลังในการสั่นคลอนความมั่นคงและความอยู่รอดของรัฐได้

[5]David E. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” New York Times, Last Modified June 1, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all
[6]Alexander Mosely, “Just War Theory,” Last Modified May 12, 2018, https://www.iep.utm.edu/justwar/
[7]Oxford Dictionary, “War,” Last Modified May 12, 2018, https://en.oxforddictionaries.com/definition/war
[8]Alexander George, Gordon Craig and Paul Lauren, Force and Statecraft (New Yrok: Oxford University Press, 2007), 48.

การทำสงครามนั้นเป็นสิ่งเลวร้าย เพราะนอกจากจะเป็นภัยคุกคามที่สำคัญอย่างยิ่งต่อการคงอยู่ของรัฐแล้ว สงครามยังการทำลายชีวิตของผู้คน ละเมิดต่อศีลธรรมอันดีที่มนุษย์ควรยึดถือ ซึ่งในปัจจุบันนี้ เพื่อผดุงความสงบสุขแก่เวทีการเมืองระหว่างประเทศ องค์การสหประชาชาติ จึงได้ถูกตั้งขึ้น และได้วางหลักการอย่างชัดเจนเกี่ยวกับการไม่ยอมรับการใช้กำลังเข้าประหัตถ์ประหารรัฐฝ่ายตรงข้ามทุกกรณี โดยหลักการนี้ได้สะท้อนอยู่ในกฎบัตรสหประชาชาติ หมวดที่ 1 มาตราที่ 2 วรรค 4 ความว่า

"ในความสัมพันธ์ระหว่างประเทศ สมาชิกทั้งปวงจักต้องละเว้นการคุกคามหรือการใช้กำลังต่อบูรณภาพแห่งอาณาเขต หรือเอกราชทางการเมืองของรัฐใดๆ หรือการกระทำในลักษณะการอื่นใดที่ไม่สอดคล้องกับความมุ่งหมายของสหประชาชาติ"[9]

อย่างไรก็ตาม ในหลายๆ สถานการณ์ รัฐก็ไม่อาจหลีกเลี่ยงการก่อสงครามได้ เพราะในสภาวะอันเป็นอนาธิปไตย (anarchy) ของเวทีการเมืองระหว่างประเทศที่รัฐทุกรัฐมีสถานะเท่าเทียมกัน มีอำนาจอธิปไตยในตนเองเหมือนกันทุกรัฐ และในทางทฤษฎีไม่มีรัฐใดมีอำนาจเหนือรัฐอื่นในการบังคับใช้กฎหมายต่างๆ เพื่อบังคับให้รัฐไม่ปฏิบัติออกนอกลู่นอกทาง ภัยคุกคามอาจเกิดขึ้นจากรัฐใดรัฐหนึ่งได้ทุกเมื่อ จึงทำให้รัฐต่างๆ ร่วมกันหาทางออกเพื่อยับยั้ง และลดความรุนแรงของผลกระทบอันเกิดจากสงคราม และได้สถาปนาปทัสถานต่างๆ มากมายเพื่อเป็นกรอบในการหยุดยั้ง จำกัด และตีกรอบรูปแบบการเกิดขึ้นและการดำเนินไปของสงคราม หนึ่งในความพยายามนั้นสะท้อนให้เห็นในปทัสถานอันเป็นหลักการสำคัญอันหนึ่งขององค์การสหประชาชาติ หรือที่เรียกกันว่าหลักการ "สงครามอันชอบธรรม" (Just War)

สงครามอันชอบธรรม[10] คือ หลักการในการทำสงครามแห่งรัฐที่ถือได้ว่ามีความชอบธรรม สามารถกระทำได้อย่างไม่ผิดศีลธรรม พึงตระหนักว่าหลักสงครามอันชอบธรรมมิได้ให้ข้ออ้างในการก่อสงครามหากแต่เป็นหลักปทัสถานทางศีลธรรมที่จะชี้นำว่าการทำสงครามควรกระทำแบบไหน และกระทำอย่างไรจึงจะพอยอมรับได้ หลักการสงครามอันชอบธรรมประกอบด้วยหลักสำคัญ 2 ประการ คือ Jus ad Bellum สิทธิที่จะก่อสงคราม และ Jus in Bello วิธีการทำสงครามที่ชอบธรรม

Jus ad Bellum หรือ สิทธิในการก่อสงคราม พูดถึงสถานการณ์ที่รัฐจะสามารถทำสงครามได้อย่างชอบธรรม รัฐจะพึงมีสิทธิในการเข้าสู่สงครามได้ก็ต่อเมื่อการกระทำนั้นเป็นไปเพื่อการปกป้องอำนาจอธิปไตยและความมั่นคงแห่งรัฐจากรัฐอื่นๆ สหประชาชาติได้ใช้หลักการนี้เป็นหลักการสำคัญสำหรับการรักษาความสงบเรียบร้อยของโลก[11] โดยได้บัญญัติเอาไว้ในกฎบัตรแห่งสหประชาชาติ หมวดที่ 7 มาตราที่ 51 ว่า

"ไม่มีข้อความใดในกฎบัตรฉบับปัจจุบันอันจักรอนสิทธิประจำตัวในการป้องกันตนเองโดยลำพังตนหรือโดยร่วมกัน หากการโจมตีโดยกำลังอาวุธบังเกิดแก่สมาชิกของสหประชาชาติ..."[12]

นอกจากนี้ ในปัจจุบันยังมีกรณีหนึ่งที่จะถือได้ว่าการก่อสงครามขึ้นนั้นมีความชอบธรรม คือ เมื่อใดก็ตามที่มีการกระทำโดยรัฐใดรัฐหนึ่งได้กระทำการอันนำไปสู่ความสั่นคลอนของสันติภาพแห่งประชาคมโลก โดยได้บัญญัติเอาไว้ในหมวดที่ 7 มาตรที่ 42 ความว่า

"หากคณะมนตรีความมั่นคงพิจารณาเห็นว่ามาตรการตามที่บัญญัติไว้ในมาตรา 41 น่าจะไม่เพียงพอ

[9]องค์การสหประชาชาติ, กฎบัตรสหประชาชาติ [United Nations Charter (1945)], แปลโดย สำนักงานแถลงข่าวสหประชาชาติ, กรุงเทพ ฯ, 2488.
[10]Alexander Mosely, "Just War Theory,"
[11]International Committee of the Red Cross, "What are Jus ad Bellum and Jus in Bello?," Last Modified January 22, 2015, https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0
[12]องค์การสหประชาชาติ, กฎบัตรสหประชาชาติ.

หรือได้พิสูจน์แล้วว่าไม่เพียงพอ คณะมนตรีก็อาจดำเนินการใช้กำลังทางอากาศ ทางทะเล หรือทางพื้นดินเช่นที่เห็นจำเป็นเพื่อธำรงไว้หรือ สถาปนากลับคืนมาซึ่งสันติภาพ และความมั่นคงระหว่างประเทศ การดำเนินการเช่นว่านี้อาจรวมถึงการแสดงแสนยานุภาพ การปิดล้อม และการปฏิบัติการอย่างอื่นโดยกำลังทางอากาศ ทางทะเล หรือทางพื้นดินของบรรดาสมาชิกสหประชาชาติ"[13]

ขณะเดียวกัน Jus in Bello[14] วิธีการทำสงครามที่ชอบธรรม หรือที่เป็นรู้จักกันในปัจจุบันในชื่อ International Humanitarian Law (IHL) เป็นหลักการที่เน้นไปที่การเคารพคุณค่าของความเป็นมนุษย์ กล่าวคือ เน้นปกป้องพลเรือนหรือทหารจากการปฏิบัติอันไม่ชอบธรรมที่เกิดขึ้นในสงคราม เป็นหลักการที่ห้ามมิให้โจมตีพลเรือน ทหารบาดเจ็บ และวิธีการปฏิบัติต่อนักโทษสงครามอย่างเคารพคุณค่าความเป็นมนุษย์ หลักการที่เป็นกฎหมายระหว่างประเทศที่ใช้อยู่ในปัจจุบัน คือ อนุสัญญา Geneva Convention

ข้าพเจ้าจะขอเน้นการคิดวิเคราะห์ในประเด็นเกี่ยวกับสงครามอันชอบธรรมไปที่ Jus ad Bellum เพราะหลักการนี้เป็นหลักการเบื้องหลังของกฎหมายระหว่างประเทศอันเป็นที่เคารพของรัฐทุกรัฐ ก่อให้เกิดปทัสถานที่เป็นแนวทางในการปฏิบัติจนกลายเป็นธรรมเนียมปฏิบัติของรัฐทุกรัฐในระบบการเมืองระหว่างประเทศ จนกลายเป็นระบอบความสัมพันธ์ระหว่างประเทศ (International Regime)[15] ในฐานะธรรมเนียมปฏิบัติที่รัฐชาติทุกรัฐที่อยู่ในประชาคมโลกจะไม่ละเมิด แม้ว่าในทางปฏิบัติแล้ว กฎบัตรสหประชาชาติจะเป็นกฎหมายที่เกิดขึ้นจากความยินยอมระหว่างประเทศ ไม่มีสภาพบังคับใดๆ และไม่มีบทลงโทษใดๆ ก็ตาม แต่ในทางปฏิบัติก็มีเพียงส่วนน้อยเท่านั้นที่มีความแข็งขืนต่อปทัสถานนี้ เพราะประการแรก การละเมิดปทัสถานอาจนำไปสู่สนามการเมืองระหว่างประเทศที่รัฐไม่พึงประสงค์ เป็นที่เข้าใจกันโดยทั่วไปทั้งสำนักคิดสภาพจริงนิยมใหม่ (Neo-realism)[16] และเสรีนิยมใหม่เชิงสถาบัน (Neo-liberal Institutionalism)[17] ว่าการเมืองระหว่างประเทศอยู่ในสภาวะที่เรียกว่า"อนาธิปไตย" โดยอนาธิปไตยในที่นี้ ไม่ได้หมายถึงความยุ่งเหยิงวุ่นวายไร้ซึ่งกฎระเบียบใดๆ จนเกิดสงครามอยู่เป็นนิตย์ หากแต่หมายถึงสภาวะที่ไม่มีผู้คุมอำนาจที่คอยบังคับใช้กฎหมายให้รัฐใดรัฐหนึ่งปฏิบัติตาม เพราะรัฐทุกรัฐได้รับสิทธิอย่างเท่าเทียมในการมีอำนาจอธิปไตยเป็นของตนเองอย่างเบ็ดเสร็จโดยปราศจากการแทรกแซงจากรัฐอื่นใด เมื่อไม่มีผู้บังคับใช้อำนาจให้รัฐปฏิบัติตามกรอบปทัสถานบางอย่าง จึงทำให้รัฐใดรัฐหนึ่งอาจก่อสงครามกับรัฐอื่นได้ ซึ่งในสภาวะนี้ บีบบังคับให้การเอาตัวรอดของรัฐ หรือความมั่นคง เป็นผลประโยชน์แห่งชาติอันเป็นวาระหลักที่รัฐจะพึงรักษาไว้ เพราะไม่มีรัฐใดที่จะยอมเสียสละอำนาจอธิปไตยหรือสิทธิในการไม่ถูกรุกรานโดยรัฐอื่นไปเป็นแน่ เมื่อเป็นเช่นนี้จึงทำให้โดยธรรมชาติแล้ว รัฐต่างๆ จะไม่ไว้ใจกัน อย่างไรก็ตาม สำนักคิด Neo-liberal Institutionalism ได้เสนอเอาไว้ว่า ในสภาวะดังกล่าวก็ยังมีช่องว่างให้รัฐร่วมมือกัน เพราะในบางกรณี รัฐต่างๆ ก็ล้วนแล้วแต่มีผลประโยชน์แห่งชาติร่วมกัน แม้ว่าสภาพของโครงสร้างความสัมพันธ์ระหว่างประเทศจะบีบบังคับให้รัฐต้องแข่งกันแสวงหาอำนาจเพื่อให้มั่นใจได้ว่ารัฐของตนจะมีความมั่นคงได้อย่างแท้จริง แต่ในสภาวะของการแข่งขันก็อาจทำให้ทุกรัฐแย่ลงได้ จึงทำให้เกิดความร่วมมือกันในการปฏิบัติตามกฎหมาย หรือในที่นี้ก็คือ การปฏิบัติตามปทัสถานสงครามอันชอบธรรม

[13]Ibid.
[14]International Committee of the Red Cross, What are Jus ad and Jus in Bello?.
[15]Richard Little, Globalisation of World Politics, 294-309.
[16]Ibid, 116-129, 294-309.
[17]Ibid.

อย่างไรก็ตาม เมื่อไม่มีองค์กรใดองค์กรหนึ่งที่มีอำนาจเหนือรัฐใดรัฐหนึ่งอย่างแท้จริง ไม่มีอำนาจที่จะบังคับใช้กฎหมายอันจะเป็นการละเมิดอำนาจอธิปไตยแห่งรัฐได้ จึงทำให้เมื่อใดก็ตามรัฐหนึ่งเลิกปฏิบัติตามปทัสถานที่กำหนดร่วมกัน รัฐอื่นก็อาจกระทำเช่นเดียวกัน เมื่อสถานการณ์ดังกล่าวเกิดขึ้น ก็จะกลายเป็นว่ารัฐไม่สามารถมั่นใจได้อีกต่อไปว่ารัฐของตนจะไม่ถูกละเมิดอำนาจอธิปไตย จึงเปิดช่องทางให้การร่วมมือกันระหว่างรัฐเกิดขึ้น เพราะการละเมิด อาจนำไปสู่สถานการณ์การโต้กลับด้วยวิธีแบบเดียวกัน (tit-for-tat) ได้ ซึ่งในฐานะรัฐที่จะต้องกระทำการอย่างมีเหตุมีผลเพื่อความอยู่รอดแล้ว รัฐจึงควรจะเลือกที่จะร่วมมือกันเพื่อให้ไม่เสียผลประโยชน์ในแง่ความมั่นคงในลักษณะนี้มากกว่า

นอกจากนี้ รัฐใดที่ริเริ่มจะก่อสงคราม หรือมีทีท่าว่าจะก่อสงครามมักจะไม่ได้รับการยอมรับ ถูกเกลียดชัง และได้รับผลจากการกระทำ เช่น ในกรณีสงครามอ่าวเปอร์เซีย[18] ประเทศอิรัก นำโดยนายซัดดัม ฮุสเซน ได้ส่งทหารเข้าบุกยึดประเทศคูเวต และประกาศให้คูเวตเป็นจังหวัดที่ 19 ของอิรัก จากกรณีดังกล่าวทำให้อิรักถูกประณามในฐานะที่เป็นผู้ทำลายสันติภาพในภูมิภาค และละเมิดต่อกฎบัตรของสหประชาชาติท้ายที่สุดแล้ว จากผลของการกระทำของอิรัก ทำให้คณะมนตรีความมั่นคงแห่งสหประชาชาติ (United Nations Security Council) ลงมติประกาศโจมตีอิรักเพื่อทวงอำนาจอธิปไตยของคูเวตกลับคืนมา ฉะนั้นเพื่อหลีกเลี่ยงผลลัพธ์ที่เกิดขึ้นนี้ รัฐจึงเลือกที่จะปฏิบัติตามปทัสถานดังกล่าว

อย่างไรก็ดี พึงตระหนักข้อเท็จจริงที่ว่าการแสวงหาผลประโยชน์แห่งชาติเพื่อความมั่นคงและความอยู่รอดแห่งรัฐ ยังคงเป็นแก่นแท้ของพฤติกรรมแห่งรัฐ แม้ว่าจะมีการสถาปนาระบอบความสัมพันธ์ระหว่างประเทศ และองค์การระหว่างประเทศที่มุ่งเน้นการนำสันติภาพมาสู่มวลมนุษย์ แต่ความมั่นคงแห่งรัฐ ก็ยังมิอาจได้รับการยืนยันภายใต้ระบอบแห่งปัจจุบันได้ เพราะสภาวะแห่งความเป็นอนาธิปไตยของระบบการเมืองระหว่างประเทศยังมิได้หายไปไหน และยังคงสร้างความไม่ไว้วางใจซึ่งกันและกันระหว่างรัฐอยู่ รวมถึงแนวคิดว่าด้วยความสำคัญทางภูมิรัฐศาสตร์ต่อความมั่นคงของประเทศก็ยังคงเป็นแนวคิดที่มีอิทธิพลอยู่ จึงทำให้รัฐได้ค้นหาวิธีการใหม่ๆ ในการรับประกันความมั่นคงของตนเองอยู่เสมอมา โดยพยายามมิให้ขัดกับหลักการแห่งสงครามอันชอบธรรมที่เป็นที่ยอมรับในเวทีโลก เช่น การใช้มาตรการคว่ำบาตรประเทศที่ตนมองว่าเป็นภัยคุกคาม อย่างในกรณีที่สหรัฐอเมริกาคว่ำบาตรคิวบา[19] เพราะเกรงกลัวว่าประเทศคอมมิวนิสต์อย่างคิวบาจะสร้างอันตรายอย่างใหญ่หลวงให้แก่สหรัฐ จึงทำให้เศรษฐกิจของคิวบาไม่เจริญเติบโตอย่างที่ควรจะเป็น การทำสงครามตัวแทน (Proxy war) โดยส่งทหาร อาวุธยุทโธปกรณ์ หรือความช่วยเหลือทางด้านการเงิน ไปในประเทศที่กำลังมีสงครามกลางเมืองอยู่เพื่อเป็นการปกป้องผลประโยชน์แห่งรัฐ ไม่ว่าจะทางเศรษฐกิจ หรือในแง่ของความมั่นคงแห่งอำนาจในภูมิภาคนั้นๆ เช่น การสนับสนุนสงครามเกาหลี[20] โดยสหรัฐสนับสนุนเกาหลีใต้ และสหภาพโซเวียตสนับสนุนเกาหลีเหนือ เพื่อแย่งขอบเขตแห่งอำนาจในภูมิภาคนั้นๆ และเป็นการจำกัดภัยคุกคามที่อาจเกิดขึ้นจากการมีอำนาจของรัฐศัตรูในภูมิภาคดังกล่าว การสนับสนุนผู้ก่อการร้าย หรือทหารพลเรือนเพื่อล้มล้างกลุ่มอำนาจที่ไม่ให้การสนับสนุนรัฐของตน และอาจกลายเป็นภัยคุกคามต่อรัฐของตนในอนาคต เช่น การสนับสนุนกลุ่มคอนทราส[21] (Contras) ให้ล้มล้างรัฐบาลสังคมนิยมของนิคารากัว หรือแม้แต่ในปัจจุบัน

[18]HISTORY.com Staff, “Persian Gulf War,” Last Modified May, 13, 2018, https://www.history.com/topics/persian-gulf-war
[19]Steptoe, “Cuban Sanction,” Last Modified May 13, 2018, https://www.steptoeinternationalcomplianceblog.com/category/cubasanctions/
[20]HISTORY.com Staff, “Korean War,” Last Modified May 13, 2018, https://www.history.com/topics/korean-war
[21]HISTORY.com Staff, “Sandinistas are defeated in Nicaraguan elections,” Last Modified May 13, 2018, https://www.history.com/this-day-in-history/sandinistas-are-defeated-in-nicaraguan-elections

สงครามไซเบอร์ที่กำลังจะกล่าวถึง ก็เกิดจากความต้องการแสวงหาผลประโยชน์แห่งชาติที่ได้อธิบายไปข้างต้นนี้

สงครามไซเบอร์ (Cyber Warfare)

อย่างที่ได้กล่าวไปแล้วในตอนต้นว่าปัจจัยที่สำคัญปัจจัยหนึ่งที่ทำให้ความก้าวหน้าทางเทคโนโลยีดำเนินไปอย่างรวดเร็ว คือเทคโนโลยีที่เรียกว่า คอมพิวเตอร์[22] คอมพิวเตอร์ทำให้เกิดปรากฏการณ์การพัฒนาการทางด้านเทคโนโลยีอย่างรวดเร็วขึ้นมากมาย ทั้งเกิดขึ้นของปัญญาประดิษฐ์ที่ทำงานบางอย่างแทนมนุษย์ได้แล้ว การพัฒนาเทคโนโลยีสำรวจธรณีวิทยาและมหาสมุทรในโลก การสำรวจอวกาศ การควบคุมดูแลโรงงานนิวเคลียร์ หรือแม้แต่เทคโนโลยีการตีพิมพ์ง่ายๆ ทุกอย่างล้วนเกี่ยวข้องกับคอมพิวเตอร์ จึงกล่าวได้ว่า ในยุคปัจจุบันคอมพิวเตอร์ได้กลายเป็นเทคโนโลยีที่ขาดไม่ได้ในการทำให้สังคมดำเนินและอภิวัฒน์ได้ต่อไป

แม้แต่รัฐเองก็ยังใช้เทคโนโลยีคอมพิวเตอร์ในการบริหารจัดการทรัพยากรและอำนวยความสะดวกการดำเนินงานของรัฐมากมาย[23] ทั้งงานฝ่ายพลเรือน อย่างการเก็บข้อมูลประชากร การวิเคราะห์ข้อมูลทางด้านเศรษฐกิจ การติดต่อสื่อสาร และงานฝ่ายทหาร ที่ใช้คอมพิวเตอร์ในการวิเคราะห์ข้อมูลทางด้านยุทธศาสตร์ การควบคุมและสั่งการกองทัพจากทางไกล การยิงจรวด หรือแม้แต่การบังคับเทคโนโลยีโดรนจากทางไกลก็ล้วนแล้วแต่เป็นเทคโนโลยีอำนวยความสะดวกที่เกิดขึ้นจากคอมพิวเตอร์ทั้งสิ้น

จากเหตุผลเหล่านี้ จึงไม่แน่แปลกใจเลยว่าคอมพิวเตอร์จะตกเป็นเป้าหมายในการโจมตีของกลุ่ม หรือรัฐที่ไม่หวังผลดีต่อรัฐบาล เพราะจากการที่ข้อมูลลับ หรือข้อมูลสำคัญๆ ส่วนใหญ่ของรัฐบาลถูกเก็บเอาไว้ในคอมพิวเตอร์ ทำให้หากโจมตี หรือทำลายเครือข่ายคอมพิวเตอร์ของรัฐบาลได้ ก็จะสร้างความเสียหายให้กับรัฐบาลได้อย่างใหญ่หลวง จึงทำให้ในยุคสมัยแห่งความก้าวหน้าทางเทคโนโลยีที่มีคอมพิวเตอร์เป็นตัวแปรสำคัญอย่างยุคสมัยปัจจุบัน การโจมตีในพื้นที่ไซเบอร์หรือสงครามไซเบอร์ ไม่ใช่เรื่องไกลตัวต่อความมั่นคงของรัฐอีกต่อไป

คำว่าไซเบอร์ของสงครามไซเบอร์ (Cyber Warfare) มาจากไซเบอร์สเปซ[24] ซึ่งหมายถึงพื้นที่เสมือนจริงซึ่งถูกสร้างขึ้นโดยการเชื่อมโยงกันของคอมพิวเตอร์ อินเตอร์เน็ต เซิร์ฟเวอร์ซึ่งให้บริการเครือข่าย และส่วนประกอบโครงสร้างพื้นฐานอื่นๆ ของคอมพิวเตอร์ การเชื่อมโยงทั้งหมดนี้ก่อให้เกิดพื้นที่เสมือนจริงที่ผู้คนจะเข้ามาสนทนากัน มีปฏิสัมพันธ์ในโลกออนไลน์ และกระทำการต่างๆ เช่น เก็บข้อมูล พัฒนาซอฟต์แวร์ ค้นหาข้อมูล และอื่นๆ อีกมากมาย ฉะนั้น หากกล่าวถึงสงครามไซเบอร์[25] ก็ย่อมหมายถึงการห้ำหั่นกันใช้อาวุธหรือในที่นี้ก็คืออาวุธไซเบอร์อย่างมัลแวร์ทั้งประเภทไวรัส เวิร์ม ม้าโทรจัน การขโมยหรือทำลายข้อมูล โดยเข้าโจมตีระบบการคุ้มกันซอฟต์แวร์ชของคอมพิวเตอร์ ทั้งหมดนี้ ล้วนเป็นการกระทำที่เกิดขึ้นภายใต้กรอบสงครามไซเบอร์ เพื่อให้เกิดความเสียหายต่อผู้ถูกโจมตี โดยทั่วไปการโจมตีเหล่านี้เกิดขึ้นอยู่แล้วในชีวิตประจำวัน และเกิดขึ้นกับบุคคลทั่วไป หากแต่สงครามไซเบอร์จะมีความหมายที่ระบุไปในทิศทางที่เกี่ยวข้องกับการโจมตีที่เกิดขึ้นต่อรัฐโดยอีกรัฐหนึ่ง คล้ายกับสภาพสงครามการยุทธตามรูปแบบ (Conventional Warfare) แต่จะแตกต่างกันตรงที่มิได้ใช้คนในการประหัตประหารกัน แต่ใช้

[22]Erza Klein, “Technology is changing how we live, but it needs to change how we work,” Vox, Last Modified May 15, 2018, https://www.vox.com/a/new-economy-future/technology-productivity
[23]Ibid.
[24]John B. Sheldon, “Cyber War,” Brittanica, Last Modified May 14, 2018, https://www.britannica.com/topic/cyberwar
[25]Ibid.

โค้ดดิจิตัล ซอฟต์แวร์ มัลแวร์ DDoS (Distributed, Denial of Service) และวิถีทางอื่นๆ อันถือเป็นอาวุธไซเบอร์ในการโจมตีเพื่อเน้นให้เกิดความเสียหายต่อรัฐนั้น ๆ มากกว่าที่จะให้เกิดการรบราฆ่าฟันทหารของฝ่ายตรงข้าม

ซึ่งการก่อสงครามโดยวิธีการนี้ ยากที่จะหาหลักฐานว่าผู้ใดเป็นผู้ริเริ่มโจมตี เพราะอาวุธไซเบอร์ส่วนใหญ่ที่ใช้กันอยู่ มักจะไม่ทิ้งร่องรอยที่ใช้เป็นหลักฐานมัดตัวผู้กระทำผิดได้ จึงเป็นสถานการณ์สงครามที่ซับซ้อนอย่างยิ่ง

การโจมตีโดยรัฐต่อรัฐในโลกไซเบอร์มีให้เห็นได้ในหลายกรณี โดยจะยกตัวอย่างกรณีศึกษาดังต่อไปนี้ กรณีแรก กรณีการโจมตีโรงงานนิวเคลียร์ของอิหร่านโดยรัฐบาลสหรัฐอเมริกาและอิสราเอล ภายใต้ปฏิบัติการ Olympic Games[26] ปฏิบัติการ Olympic Games คือชื่อปฏิบัติการไซเบอร์ลับของสหรัฐฯ ที่พยายามจะยับยั้งโครงการพัฒนาอาวุธนิวเคลียร์ของประเทศอิหร่าน โดยมุ่งโจมตีโรงงานนิวเคลียร์ของอิหร่าน เพื่อมิให้แผนการพัฒนาอาวุธนิวเคลียร์ของอิหร่านประสบความสำเร็จ โดยปฏิบัติการมุ่งเป้าไปที่โรงงานเสริมสมรรถนะนิวเคลียร์ที่เมืองนาตันซ์ (Natanz) ประเทศอิหร่าน

อาวุธไซเบอร์ที่ถูกคิดค้นเพื่อบรรลุจุดประสงค์ของปฏิบัติการ Olympic Games คือ มัลแวร์ประเภทเวิร์มนามว่า Stuxnet โดยมัลแวร์ตัวนี้จะทำลายระบบควบคุมและประมวลผลคอมพิวเตอร์แบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งพัฒนาโดยบริษัท Siemens ของประเทศเยอรมัน และเป็นคอมพิวเตอร์ที่ใช้อย่างแพร่หลายในการควบคุมและดูแลกระบวนการต่างๆ ในโรงงานอุตสาหกรรม อาทิ โรงงานไฟฟ้า โรงงานประปา โรงงานผลิตสินค้าต่าง ๆ หรือแม้แต่การควบคุมสัญญาณไฟและการเดินรถของรถสาธารณะ

การเผยแพร่ของ Stuxnet จะต้องเผยแพร่ผ่านแฟลชไดร์ฟ โดยสหรัฐฯ และอิสราเอลได้ส่งสายลับเข้าไปติดตั้งมัลแวร์ไว้ในคอมพิวเตอร์หลักของโรงงาน จากนั้นมัลแวร์ก็เริ่มทำงาน โดยมัลแวร์จะเข้าไปติดตั้งโปรแกรมใหม่ในระบบ PLCs (Programmable Logic Controllers) หรือส่วนควบคุมการทำงานของระบบเครื่องจักร ภายในช่วงสัปดาห์แรกที่คอมพิวเตอร์ติดเชื้อ มัลแวร์จะยังไม่แสดงอาการ เพราะมัลแวร์ชนิดนี้จะเรียนรู้พฤติกรรมการทำงานของคอมพิวเตอร์ จนรู้แน่ชัดแล้วว่ากิจวัตรของคอมพิวเตอร์จะต้องทำอะไรบ้าง ก็จะเริ่มการทำลายล้างโปรแกรมคอมพิวเตอร์ โดยผู้ควบคุมจะไม่ทราบถึงความผิดปกติที่เกิดขึ้นกับคอมพิวเตอร์ เพราะมัลแวร์จะเลียนแบบพฤติกรรมปกติของคอมพิวเตอร์ และค่อยๆ ทำลายระบบการทำงานของเครื่องจักรจนไม่สามารถใช้งานได้

ปฏิบัติการ Olympic Games ประสบความสำเร็จอย่างมากจากการที่สามารถทำลายเครื่องหมุนเหวี่ยงแยกยูเรเนียมของอิหร่านและทำลายโปรแกรมนิวเคลียร์ของอิหร่านไปถึง 1 ใน 5 คาดเดาว่าจากการโจมตีด้วยไวรัสชนิดนี้ทำให้โครงการพัฒนานิวเคลียร์ของอิหร่านต้องล้าช้าออกไปไม่ต่ำกว่า 6 เดือน ถึง 2 ปี โดยที่รัฐบาลอิหร่านก็มิได้ตระหนักถึงการโจมตีของมัลแวร์ดังกล่าว จนกระทั่งพบว่ามัลแวร์ชนิดนี้ได้ระบาดไปทั่วโลก ทั้งอินโดนีเซีย อินเดีย อาเซอร์ไบจัน สหรัฐอเมริกา ประเทศจีน ปากีสถาน และอีกหลายประเทศ ทำให้ทั่วโลกตระหนักถึงอาวุธไซเบอร์อันร้ายแรงชนิดนี้ ซึ่งทางสหรัฐอเมริกาและอิสราเอลก็ได้ให้การปฏิเสธถึงปฏิบัติการดังกล่าว

กรณีที่ 2 ในวันที่ 24 เดือนมีนาคม 2016 กระทรวงยุติธรรมของสหรัฐได้ประกาศหมายจับแฮกเกอร์ชาวอิหร่าน 7 คน ผู้เป็นสมาชิกของกองกำลังพิทักษ์การปฏิวัติอิสลาม (Islamic Revolutionary Guard

Corp) ซึ่งเป็นหน่วยงานหนึ่งภายใต้สังกัดกองทัพอิหร่าน ด้วยข้อหาโจมตีธนาคารหลายแห่งในมหานครนิวยอร์ก ทำให้เกิดความเสียหายทางการเงินหลายล้านดอลลาร์ และข้อหายึดการควบคุมเขื่อนโบว์แมนรัฐนิวยอร์ก[27]

ในข้อหาแรก ผู้ต้องหาชาวอิหร่านได้ใช้วิธีการ DDos[28] ในการโจมตีธนาคารของสหรัฐ โดยการโจมตีดังกล่าวเกิดขึ้นได้โดยการเจาะระบบคอมพิวเตอร์ของธนาคาร และส่งระดมส่งข้อมูลขนาดใหญ่กว่า 140 กิ๊กกะบิทต่อวินาที ที่ไม่มีความหมายหรือนัยยะสำคัญเข้าไปที่เครื่องคอมพิวเตอร์หลัก เพื่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนระบบไม่สามารถทำงานได้ตามปกติ การโจมตีนี้คาดการณ์ว่าเกิดขึ้นตั้งแต่ช่วงธันวาคมปี 2011 และทำให้ผู้ใช้บริการของธนาคาร JP Morgan Chase, Wells Fargo และ American Express ไม่สามารถเข้าใช้งานได้

สำหรับข้อหาที่สอง ผู้ต้องหาชาวอิหร่านได้ทำการเจาะระบบคอมพิวเตอร์ SCADA ที่ทำการควบคุมเขื่อน Bowman Avenue ที่รัฐนิวยอร์ก โดยการเจาะระบบในครั้งนี้ทำให้ผู้ต้องหาสามารถเข้าถึงข้อมูลการปฏิบัติงานของเขื่อน ข้อมูลระดับน้ำ และยังทำให้เข้าถึงความสามารถในการเปิดปิดประตูเขื่อนอีกด้วย ซึ่งทางกระทรวงยุติธรรมได้กล่าวว่าถือว่าเป็นความโชคดีที่ในขณะนั้นประตูเขื่อนอยู่ในช่วงปรับปรุง จึงมิได้มีการควบคุมด้วยคอมพิวเตอร์ตามปกติ ไม่เช่นนั้นอาจทำให้เกิดความเสียหายต่อชีวิตและทรัพย์สินของประชาชนชาวอเมริกันได้

ผู้เชี่ยวชาญด้านความมั่นคงได้ให้ความเห็นว่าการโจมตีดังกล่าว อาจเป็นการล้างแค้นการทำลายโครงการนิวเคลียอิหร่านโดยสหรัฐและอิสราเอลด้วยการใช้มัลแวร์อย่าง Stuxnet ในการปฏิบัติการโดยการโจมตีจากอิหร่านในครั้งนี้ทำให้สหรัฐฯ ต้องตระหนักถึงภัยคุกคามของสงครามไซเบอร์ที่จะเกิดขึ้นกับรัฐของตนอย่างจริงจัง โดยเฉพาะอย่างยิ่งระบบปฏิบัติการของโครงการต่างๆ ทั้งโครงสร้างพื้นฐานและอื่นๆ ล้วนใช้คอมพิวเตอร์ จากการที่อิหร่านสามารถยึดเขื่อนของสหรัฐฯ ได้ ทำให้เป็นที่ชัดเจนว่าการโจมตีเจาะระบบเพื่อยึดโครงสร้างพื้นฐานอื่นๆ ที่มีการวางระบบรักษาความปลอดภัยไว้อย่างหละหลวมจะเป็นเป้าในการโจมตี เช่น เขื่อน โรงงานไฟฟ้า และอาจกระทบต่อชีวิตและทรัพย์สินของประชาชนชาวสหรัฐ ฯ อย่างจริงจัง

กรณีที่ 3 การโจมตีระบบเชื่อมโยงไฟฟ้าในกรุงเคียฟ (Kiev) และการโจมตีอื่นๆ ที่เกิดขึ้นในประเทศยูเครน ประเทศยูเครนเป็นประเทศที่ถูกโจมตีทางไซเบอร์หลายครั้ง[29] เช่น การโจมตีระบบการเลือกตั้งในปี 2014 โดยเชื่อว่าเป็นฝีมือของประเทศรัสเซีย แต่การโจมตีที่ถือว่าได้ว่าควรถูกบันทึกไว้ในประวัติศาสตร์ของความน่ากลัวและความรุนแรงของสงครามไซเบอร์ คือการโจมตีระบบไฟฟ้าของยูเครนทั้ง 2 ครั้งในปี 2015 และ 2016 โดยในครั้งแรก เกิดขึ้นในวันที่ 23 ธันวาคม 2015 การโจมตีในครั้งนี้ถือเป็นการโจมตีระบบไฟฟ้าด้วยวิธีการทางไซเบอร์ที่ประสบความสำเร็จครั้งแรกของโลก[30] ส่งผลให้สถานีไฟฟ้าย่อยกว่า 30 สถานีไม่สามารถทำการได้ และประชาชนกว่า 230,000 คน ไม่มีไฟฟ้าใช้นานสุดถึง 6 ชั่วโมง ท่ามกลางสภาพอากาศอันหนาวจัดของยูเครนในปลายเดือนธันวาคม โดยภายหลังได้รับการเปิดเผยว่าที่อยู่ IP ของผู้ทำการโจมตีมาจากสหพันธรัฐรัสเซีย

[26]David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran.
[27]Dustin Volz, and Jim Fickle, “U.S. indicts Iranians for hacking dozens of banks, New York dam,” Reuters, Last Modified March 24, 2016, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN-0WQ1JF
[28]Digital Attack Map, “What is DDoS Attack?,” Last Modified May 15, 2018, https://www.digitalattackmap.com/understanding-ddos/
[29]Kim Zetter, “INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE’S POWER GRID,” WIRED, Last Modified May 15, 2018, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[30]Ibid.

อันที่จริงโรงไฟฟ้าของยูเครนถือว่ามีระบบการป้องกันภัยคุกคามไซเบอร์ที่ดีในระดับหนึ่ง ถือได้ว่าดีกว่าระบบป้องกันภัยของสหรัฐฯ ในบางสถานีเสียด้วย อย่างไรก็ตาม การโจมตีดังกล่าวก็เกิดขึ้นและประสบความสำเร็จ การโจมตีในครั้งนี้ประกอบด้วยการใช้เทคนิคหลายประเภทด้วยกัน โดยเริ่มจากวิธีการ spear-phishing[31] หรือการส่งอีเมล์หลอกเพื่อล่อลวงข้อมูลสำคัญจากบุคคลเฉพาะเจาะจง จากนั้นอีเมล์ก็ได้ติดตั้งมัลแวร์ประเภทม้าโทรจันที่เรียกว่า BlackEnergy[32] ซึ่งมัลแวร์ชนิดนี้จะทำการโจมตีระบบคอมพิวเตอร์ด้วยวิธีการ DDoS จากนั้นจะส่งข้อมูลสำคัญกลับไปให้แฮกเกอร์ หลังจากแฮกเกอร์ได้ข้อมูลแล้ว แฮกเกอร์ก็ได้เข้าควบคุมคอมพิวเตอร์ SCADA ที่ควบคุมระบบโรงงานไฟฟ้าของยูเครน จากนั้นก็จะเริ่มทำลายโครงสร้างพื้นฐานที่ทำการเชื่อมโยงคำสั่งของโรงไฟฟ้าต่างๆ จากนั้น BlackEnergy จะชักนำมัลแวร์อีกประเภท ชื่อ KillDisk[33] เข้าไปทำลายเอกสารและข้อมูลต่างๆ ที่ถูกเก็บเอาไว้ในระบบ และเพื่อไม่ให้ผู้ใช้งานสามารถรายงานสถานการณ์การไฟฟ้าในปัจจุบันได้ แฮกเกอร์ได้ทำการโจมตีโดยวิธีการ DDoS ใส่ระบบทำให้ระบบคอลเซนเตอร์ไม่สามารถใช้งานได้

เหตุการณ์ทำนองเดียวกันเกิดขึ้นอีกครั้งในวันที่ 17 ธันวาคม 2016 เมื่อโรงไฟฟ้าพิฟนิชนา (Pivnichna) ของกรุงเคียฟ (Kiev) ถูกปิดระบบไฟฟ้านานกว่า 1 ชั่วโมง[34] และต้องใช้เวลาแก้ไขเพื่อให้สามารถกลับมาใช้งานได้ตามปรกติกว่า 2 เดือน โดยในครั้งนี้เป็นการโจมตีโดยมัลแวร์ที่ชื่อ Industroyer ซึ่งถือได้ว่าเป็นอาวุธไซเบอร์ศักยภาพสูงตัวที่สองที่ถูกสร้างขึ้นหลังจากการแพร่ระบาดของ Stuxnet นักวิจัยจาก ESET and Dragos Inc. ได้เปิดเผยว่ามัลแวร์ชนิดดังกล่าวมีศักยภาพในการทำลายระบบคอมพิวเตอร์ควบคุมอุตสาหกรรมขนาดใหญ่อย่างโรงไฟฟ้าได้ด้วยตนเอง เหมือน Stuxnet สามารถปรับตัวเพื่อทำการโจมตีโรงไฟฟ้าได้ไม่จำกัดเป้าหมาย มีศักยภาพในการยับยั้งระบบหยุดทำงานอัตโนมัติเมื่อเครื่องจักรผลิตไฟฟ้ามีความร้อนมากเกินไปจนอาจเกิดอันตรายต่อชีวิตได้ และสามารถนำกลับมาใช้ได้เรื่อยๆ อีกด้วย โดยวิธีการโจมตีมีลักษณะคล้ายคลึงกับ Stuxnet กล่าวคือ สามารถทำการแฝงตัวไปในระบบและทำให้ทำงานผิดปกติได้โดยที่ระบบไม่สามารถตรวจจับได้และจะไม่แสดงอาการ และทำงานได้ด้วยตนเอง ไม่จำเป็นจะต้องมีแฮกเกอร์ควบ แม้กรณีนี้จะโด่งดังน้อยกว่ากรณีเมื่อปี 2015 แต่ถือได้ว่าเป็นกรณีที่น่ากลัวกว่า เพราะการอุบัติขึ้นของมัลแวร์ชนิดนี้เท่ากับเป็นการประกาศว่าการก่อสงครามไซเบอร์สามารถสร้างความเสียหายได้จริง และสหรัฐฯ ก็ไม่ใช่ผู้เดียวที่สามารถทำได้ รัสเซียก็ทำได้เช่นกัน โดยผู้เชี่ยวชาญทางด้านความมั่นคงของยูเครนเชื่อว่ายูเครนเป็นเหมือนสนามทดลองอาวุธชนิดใหม่เพื่อนำไปใช้กับกลุ่มประเทศในยุโรปและสหรัฐอเมริกา

ผลกระทบของสงครามไซเบอร์ต่อระบบการเมืองระหว่างประเทศ (Cyber Warfare's Impact on International Politics)

จะเห็นได้ว่า สงครามไซเบอร์ เป็นสงครามที่เกิดขึ้นจริง มีความซับซ้อน และยังกระทบต่อความมั่นคงของรัฐอย่างชัดเจน นอกจากผลกระทบในเชิงความเสียหายที่เกิดขึ้นต่อรัฐแล้ว สงครามไซเบอร์ก่อให้เกิดคำถามบางประการอันอาจนำไปสู่การสร้างระบอบความสัมพันธ์ระหว่างประเทศรูปแบบใหม่

[31]Teach Target, "Spear-phishing," Last Modified May 15, 2018. https://searchsecurity.techtarget.com/definition/spear-phishing
[32]Trend Micro, "Frequently Asked Question: BlackEnergy," Last Modified February 11, 2016. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy
[33]Ibid.
[34]CBS News, "Was Russian hacking of Ukraine's power grid a test run for U.S. attack?," Last Modified June 23, 2017. https://www.cbsnews.com/news/russian-hacking-of-ukraines-power-grid-test-run-for-us-attack/

ที่ตระหนักถึงภัยคุกคามจากสงครามไซเบอร์ ดังนี้

ประการแรก ทำให้เกิดการตั้งคำถามกับขอบเขตของความเป็นรัฐชาติในโลกไซเบอร์ เป็นที่ทราบกันดีว่าโลกไซเบอร์นั้น ไร้ขอบเขต โลกไซเบอร์เป็นโลกที่จำลองพื้นที่ทุกหนทุกแห่งในโลกเอาไว้ และเชื่อมต่อพื้นที่เหล่านั้นเข้าด้วยกันภายใต้การทำงานของอินเตอร์เน็ต พื้นที่ดังกล่าว จึงลักษณะที่ค่อนข้างจะปลอดอำนาจรัฐ[35] เมื่อปลอดซึ่งอำนาจรัฐแล้ว ในแง่หนึ่งก็อาจหมายถึงเสรีภาพ และความเป็นส่วนตัวของผู้คน แต่ก็ย่อมนำภัยคุกคามจากสงครามไซเบอร์เข้ามาได้เช่นกัน สาเหตุที่การโจมตีธนาคารต่างๆ จนกระทบผู้ใช้ในสหรัฐอเมริกาจากกรณีตัวอย่างที่ 2 ที่ได้กล่าวไปก็ย่อมเกิดมาจากการเปิดกว้างของโลกไซเบอร์ หากโลกไซเบอร์มีการวางขอบเขตดูแล มีวิธีการจับตามองของรัฐที่ชัดเจน การโจมตีเหล่านี้อาจไม่เกิดขึ้นหรือต่อให้เกิดขึ้น ความเสียหายก็อาจไม่รุนแรงเท่าที่เกิดขึ้น เพราะอย่างน้อยที่สุด รัฐจะตระหนักถึงภัยคุกคามดังกล่าวก่อน และพยายามสกัดกั้นภัยคุกคามที่จะเกิดขึ้นเหล่านั้น จึงทำให้เกิดคำถามว่าแนวคิดเรื่องของอำนาจอธิปไตยแห่งรัฐ ควรจะถูกนำเข้ามาใช้ในโลกไซเบอร์หรือไม่ ซึ่งก็มีข้อกังวลที่สำคัญ คือ การนำอำนาจอธิปไตยของรัฐเข้ามาสู่พื้นที่โลกไซเบอร์ อาจขัดต่อหลักการเสรีภาพในความเป็นส่วนตัว[36] ประเด็นนี้เป็นข้อกังวลที่เกิดขึ้นต่อโลกไซเบอร์มานานแล้ว และกลายเป็นประเด็นที่ได้รับความสนใจอย่างมากตั้งแต่มีนายเอ็ดเวิร์ด สโนว์เดน อดีตเจ้าหน้าที่ของ NSA (National Security Agency) แห่งสหรัฐอเมริกา ได้ออกมาเปิดเผยถึงโปรแกรม Prism[37] หรือโปรแกรมที่ทำให้รัฐบาลสหรัฐฯ สามารถรู้ได้ถึงความเคลื่อนไหวของประชากรทั่วโลกผ่านการสะกดรอยทางโซเชียลเน็ตเวิร์กทุกประเภท การดักฟังเสียงโทรศัพท์ และการดักดูกล้องรักษาความปลอดภัย ซึ่งเมื่อมีการเปิดเผยเรื่องดังกล่าว ทำให้ผู้คนตระหนักอย่างมากเรื่องสิทธิความเป็นส่วนตัวในการปลอดจากการสอดส่องของรัฐ ซึ่งหากมีการตกลงให้อำนาจอธิปไตยเข้ามาสู่พื้นที่อิสระอย่างโลกไซเบอร์ได้อย่างเต็มที่ เสียงส่วนใหญ่ย่อมไม่เห็นด้วย เพราะอาจนำไปสู่การควบคุมการใช้อินเตอร์เน็ตของรัฐบาล เกิดการปิดหูปิดตาประชาชน อย่างเช่นที่เกิดขึ้นในประเทศจีน[38] ที่รัฐบาลได้ทำการควบคุมแบนด์วิดทั้งหมดของประเทศ เพื่อคัดกรองเนื้อหาที่จะแสดงให้สาธารณะชนเห็น ทำให้เกิดการจำกัดการแสดงออกทางความคิดเห็นได้ ซึ่งประเด็นเช่นนี้ เป็นเรื่องละเอียดอ่อนมากในประเทศโลกเสรี และเป็นสิ่งที่ไม่อาจยอมรับได้ อย่างไรก็ดี การไม่เข้าควบคุมของรัฐและสอดส่องดูแลในโลกไซเบอร์โดยรัฐบาล ก็อาจเปิดช่องโหว่ต่อความเสี่ยงในการถูกโจมตีทางโลกไซเบอร์ดังที่ได้กล่าวไปในหัวข้อสงครามไซเบอร์

อย่างไรก็ดี การสร้างมาตรการป้องกันการโจมตีทางไซเบอร์ของรัฐ ก็ยังคงมีความสำคัญอย่างยิ่ง เพราะแนวโน้มของความรุนแรงที่เกิดจากการโจมตีทางไซเบอร์ ดูจะมีสูงขึ้น เพราะพัฒนาการทางเทคโนโลยีในลักษณะที่เชื่อมโยงเครือข่ายสิ่งของเครื่องใช้ต่างๆ ผ่านคอมพิวเตอร์ (Internet of Things)[39] กลายเป็นกระแสที่กำลังจะครอบงำการใช้ชีวิตประจำวันของประชาชนในทุกมิติของชีวิต เช่น

[35]Mark Pomerleau, “Cyber needs change quickly, cyber policies have not,” Fifth Domain, Last Modified March 14, 2018, https://www.fifthdomain.com/dod/2018/03/14/cyber-needs-change-quickly-cyber-policies-have-not/

[36]Michael Grech, “DATA PROTECTION VS. THE RIGHT TO PRIVACY,” GVZH Advocates, Last Modified May 12, 2018, https://www.gvzh.com.mt/malta-law/data-protection/vs-the-right-to-privacy/

[37]Timothy B. Lee, “Here’s everything we know about PRISM to date,” the Washington Post, Last Modified June 12, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?utm_term=.d80a54455275

[38]Simon Denyer, “The walls are closing in: China finds new ways to tighten Internet controls,” the Washington Post, Last Modified September 27, 2017, https://www.washingtonpost.com/world/asia_pacific/the-walls-are-closing-in-chinafinds-new-ways-to-tighten-internet-controls/2017/09/26/2e0d3562-9ee6-11e7-b2a7-bc70b6f98089_story.html?utm_term=.d103549aa597

[39]saac Thomas, “Rise of IoT - Internet of Things,” Huffington Post, Last Modified September 10, 2017, https://www.huffingtonpost.com/entry/rise-of-iot-internet-of-things_us_59b373dee4b0bef3378ce052

ในปัจจุบัน เทคโนโลยีควบคุมรถด้วยปัญญาประดิษฐ์ผ่านการให้คำสั่งโดยระบบคอมพิวเตอร์ เพื่อสร้างรถที่ไร้คนขับ[40] เริ่มที่จะเป็นจริงขึ้นมาเรื่อยการติดต่อสื่อสารในชีวิตประจำวัน ก็กระทำการผ่านการใช้คอมพิวเตอร์ ไม่ว่าจะใช้คอมพิวเตอร์ตั้งโต๊ะหรือใช้โทรศัพท์แบบสมาร์ทโฟน หรือแม้แต่เรื่องเล็กๆ อย่างการเปิดปิดไฟ การต้มน้ำร้อน ก็สามารถทำได้จากการให้คำสั่งผ่านคอมพิวเตอร์ เพราะฉะนั้นเมื่อมีการโจมตีโดยวิธีการทางไซเบอร์เกิดขึ้น ก็อาจกระทบกับอุปกรณ์ที่ใช้ในชีวิตประจำวัน และทำให้เกิดความติดขัดในการใช้ชีวิตประจำวันของประชาชนธรรมดาจนเกิดความเดือดร้อน และอาจนำไปสู่ความหวาดวิตกของสาธารณะชนต่อศักยภาพของรัฐบาลในการรับมือแก้ไขปัญหาได้

นอกจากในระดับประชาชนแล้ว ความมั่นคงในระดับรัฐบาลก็ดูจะมีปัญหามากกว่าเก่า หากไม่มีมาตรการรับมือที่ดี เพราะ การไร้ซึ่งขอบเขตที่ชัดเจนในการดูแลโลกไซเบอร์ของรัฐ ทำให้การควบคุมสกัดกั้นการโจมตีทางไซเบอร์ไม่มีประสิทธิภาพเท่าที่ควร เพราะการโจมตีทางไซเบอร์ มักจะมีลักษณะพิเศษคือ สามารถกระจายความรุนแรงออกไปได้ไม่จำกัดพื้นที่ ดังที่ได้แสดงให้เห็นในกรณี Stuxnet แล้วที่มัลแวร์ได้แพร่กระจายไปทั่วโลก ซึ่งในอนาคตหากรัฐมหาอำนาจทุกรัฐมีอาวุธไซเบอร์ลักษณะดังกล่าว แล้วทำการโจมตีซึ่งกันและกัน ความเสียหายและความวุ่นวายที่เกิดขึ้นก็อาจยากที่จะจินตนาการและผู้จะดำเนินการรับผิดชอบในฐานะผู้กระทำก็ไม่มี เพราะลักษณะพิเศษที่ไม่สามารถหาหลักฐานจากผู้ปล่อยได้ แตกต่างจากการปล่อยขีปนาวุธซึ่งสามารถคำนวณจากพิกัดที่ขีปนาวุธตก และระยะทางความเร็ว เพื่อเสาะหาตัวการที่ปล่อยขีปนาวุธ เพราะฉะนั้น ถึงแม้ว่าการตกลงนำเรื่องอำนาจอธิปไตยของรัฐมาประยุกต์ใช้ในโลกไซเบอร์จะกระทบกับเรื่องสิทธิของประชาชน แต่รัฐชาติ และองค์กรระหว่างประเทศต่างๆ ก็จะต้องทำอะไรบางอย่างเพื่อเป็นมาตรการในการรับมือปัญหานี้ จึงอาจทำให้เกิดแนวโน้มที่รัฐและองค์กรระหว่างประเทศ สามารถหาทางออกประนีประนอมประเด็นเรื่องสิทธิกับการเข้าควบคุมโลกไซเบอร์ของรัฐเพื่อรักษาความปลอดภัย

ประการที่สอง สงครามไซเบอร์อาจนำไปสู่สภาวการณ์ที่การจัดทำยุทธศาสตร์ทางการรบมีความยุ่งยากมากยิ่งขึ้น ในการจัดทำยุทธศาสตร์รูปแบบทั่วไปของการรบ[41] โดยปกติแล้ว ฝ่ายที่ทำการโจมตี หรือถูกโจมตี จะพอมีความสามารถในการคาดการณ์ได้ว่าอะไรจะเกิดขึ้น อีกฝ่ายหนึ่งจะปฏิบัติการประมาณไหน จะทำอย่างไร โดยวิธีการนี้มักจะใช้รูปแบบการคิดของทฤษฎีเกม (Game Theory)[42] โดยจะประเมินจากทรัพยากรที่ฝ่ายตรงข้ามน่าจะมีและสิ่งที่ฝ่ายตรงข้ามน่าจะกระทำ และไม่น่าจะกระทำ เพื่อให้ปฏิบัติการ หรือยุทธศาสตร์การดำเนินนโยบายความสัมพันธ์ระหว่างประเทศเป็นไปอย่างมีประสิทธิภาพสูงสุด อย่างไรก็ตาม ลักษณะสำคัญของการโจมตีไซเบอร์ ทั้งความรวดเร็วแบบทันตาเห็น และความยากในการติดตามตัวผู้กระทำ หรือหาหลักฐานมามัดตัวผู้กระทำ ทำให้รูปแบบการคิดในลักษณะนี้ไม่สามารถใช้ได้ เพราะจากความรวดเร็ว ความซ่อนเร้นและความไร้ซึ่งผู้กระทำ ทำให้การคาดการณ์ เป็นไปได้ยาก การคิดแบบกลยุทธ์เพื่อดำเนินการอันจะไม่ทำให้เสียเปรียบจึงเป็นไปได้ยากตามไปด้วย สถานการณ์เช่นนี้จะทำให้การคิดอย่างมีเหตุมีผลของรัฐเป็นไปได้ยาก และไม่สามารถดำเนินการอย่างที่เคยทำได้ จึงถือได้ว่าเป็นอันตรายอย่างหนึ่งที่อาจเกิดขึ้นจากสงครามไซเบอร์

[40]Sean O'Kane, "HOW TESLA AND WAYMO ARE TACKLING A MAJOR PROBLEM FOR SELF-DRIVING CARS: DATA," the Verge, Last Modified Apr 19, 2018, https://www.theverge.com/transportation/2018/4/19/17204044/tesla-waymo-self-driving-car-data-simulation
[41]Andreas Haggman, "Cyber Weapons as a Game Changer: A Critical Reflection," E-International Relations, Last Modified Jun 9, 2015, https://www.e-ir.info/2015/06/09/cyber-weapons-as-a-game-changer-a-critical-reflection/
[42]Ibid.

การนิยามความหมายของสงครามอันชอบธรรมใหม่ (The re-definition of Just War)

จากผลกระทบที่อาจเกิดขึ้นจากสงครามไซเบอร์ที่ได้กล่าวไป จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการนิยามสงครามอันชอบธรรมให้ครอบคลุมถึงรูปแบบการสงครามแบบใหม่ที่กำลังจะเกิดขึ้นมานี้ ในขั้นแรก ควรมีการนิยามการจัดการความมั่นคงเสียใหม่ ให้ครอบคลุมถึงการโจมตีทางไซเบอร์ด้วย ในปัจจุบัน นิยามการโจมตีทางไซเบอร์เป็นสิ่งที่มีความเป็นสีเทา กล่าวคือ คลุมเครือระหว่างประเด็นความมั่นคงในลักษณะเดิม (Traditional Security) กล่าวคือ ความมั่นคงที่เกี่ยวข้องกับการทหารเป็นหลัก ซึ่งก็ถือว่าจริง เพราะเป็นที่ประจักษ์ว่าอาวุธไซเบอร์ถูกใช้ในปฏิบัติการที่มีลักษณะคล้ายกับปฏิบัติการทางการทหาร เพื่อรักษา หรือขยายความมั่นคงของรัฐ และยังอยู่ในขอบเขตของความมั่นคงรูปแบบใหม่ (Non-traditional Security) ซึ่งเป็นรูปแบบความมั่นคงที่เพิ่งมีการกล่าวถึงอย่างเป็นทางการในรายงานการพัฒนามนุษย์ของโครงการพัฒนาแห่งองค์การสหประชาชาติ (United Nations development programme : Human Development Report) [43] ประจำปี 1994 เป็นความมั่นคงที่นอกเหนือไปจากความมั่นคงทางการทหาร และความมั่นคงแห่งรัฐ คือ ความมั่นคงของมนุษย์ในแง่สุขภาพ สิทธิมนุษยชน สิ่งแวดล้อม ยาเสพติด การก่อการร้าย และความมั่นคงด้านต่างๆ อันไม่เกี่ยวข้องกับการทหาร ซึ่งนักวิชาการบางกลุ่มก็ได้กล่าวว่าสงครามไซเบอร์จัดอยู่ในความมั่นคงลักษณะนี้[44] เพราะเป็นภัยคุกคามอันเกิดจากการพัฒนาการของเทคโนโลยีสารสนเทศและการสื่อสาร (Information Communication technology) และเป็นปัญหาที่อยู่เหนืออำนาจของรัฐใดรัฐหนึ่งจะจัดการได้ จากการที่พื้นที่ความขัดแย้งอยู่เหนือความควบคุมของรัฐชาติ ทำให้สงครามไซเบอร์ยังมิได้รับคำนิยามที่ชัดเจนในเวทีโลก ซึ่งจากความก้ำกึ่งของสงครามไซเบอร์นี้ ก่อได้ทำให้เกิดข้อถกเถียงทางวิชาการว่าสงครามไซเบอร์จะถูกจัดไปอยู่ในความมั่นคงรูปแบบใด และควรมีวิธีการใดในการแก้ไขปัญหา

แต่อย่างที่ได้กล่าวไปหลายครั้งหลายหนแล้วว่า สงครามไซเบอร์ถือเป็นภัยคุกคามต่อความมั่นคงทั้งของรัฐและระบอบการเมืองระหว่างประเทศที่มีอยู่จริง จึงทำให้มีความจำเป็นอย่างยิ่งที่ในอนาคตจะต้องมีการนิยามคำศัพท์ดังกล่าว รวมถึงรูปแบบสงครามอันชอบธรรมเสียใหม่ ว่าการก่อสงครามเช่นนี้ จะถือได้ว่าขัดต่อหลักการสงครามอันชอบธรรมหรือไม่ เพราะหากวิเคราะห์ตามหลัก Jus ad Bellum แล้ว สงครามไซเบอร์อาจเป็นสิ่งที่ถูกต้องด้วยหลายมุมมอง เช่น เพราะเป็นการทำเพื่อปกป้องผลประโยชน์และความมั่นคงของรัฐจากภัยคุกคามที่อาจเกิดขึ้น หรือเพราะสงครามไซเบอร์มิใช่สงครามรูปแบบทั่วไปที่มีการประกาศสงครามกันอย่างชัดเจน หรือมีการฆ่าฟันกัน และหากวิเคราะห์ตามหลักการ Jus in Bello แล้ว การทำสงครามไซเบอร์ก็มิวิธีการที่ผิด เพราะมิมุ่งทำร้ายพลเรือน ทหารที่บาดเจ็บ หรือเชลยศึกแต่อย่างใด หากแต่มุ่งสร้างความเสียหายให้แก่รัฐ ซึ่งในมุมหนึ่งสงครามในลักษณะนี้อาจเป็นสิ่งที่ดีกว่าสงครามที่มีการรบกันซึ่งหน้า เพราะความเสียหายต่อชีวิตมีจำกัดกว่ามาก

แต่หากจะวิเคราะห์ให้รูปแบบของสงครามไซเบอร์ขัดกับหลักการสงครามอันชอบธรรมแล้ว ก็ถือได้ว่าในการตีความบางรูปแบบก็เปิดช่องให้เป็นไปได้ เป็นต้นว่า ผลกระทบที่เกิดขึ้นจากสงคราม ละเมิดทั้งหลักการ Jus ad Bellum และ Jus in Bello เพราะเป็นการละเมิดอธิปไตยของรัฐอย่างชัดเจน และมีความเสียหายเชิงประจักษ์ที่เกิดขึ้น ซึ่งความ

[43]UNDP, Human Development Report 1994, (New York, Oxford University Press, 1994), 22.
[44]Ibid.

เสียหายที่เกิดขึ้นนั้น กระทบกับชีวิตและทรัพย์สินของพลเรือน และหากการพัฒนาการของมัลแวร์มีสูงขึ้นไปจนสามารถทำอันตรายต่อชีวิตและทรัพย์สินของประชาชนได้ ตัวอย่างเช่น ในอนาคต ผู้สร้างมัลแวร์ Industroyer ต้องการให้เกิดระเบิดในโรงไฟฟ้าโดยทำให้ระบบเกิดการมีความร้อนสูงเกินไป (overheat) และทำให้ระบบหยุดการทำงานอัตโนมัติไม่ทำงาน ความอันตรายของอาวุธไซเบอร์ก็ย่อมผิดต่อหลักการที่จะไม่ทำความเสียหายแก่ผู้เกี่ยวข้อง ฉะนั้น จึงจำเป็นอย่างยิ่งที่จะต้องมีการสร้างปทัสถานที่ชัดเจน เพื่อครอบคลุมรูปแบบการโจมตีไซเบอร์ที่มีแนวโน้มจะเกิดขึ้นในอนาคต และเป็นการสร้างปทัสถานในระบอบความมั่นคง (Security Regime) ในการเมืองระหว่างประเทศ ที่รัฐทุกรัฐจะยอมร่วมมือกันปฏิบัติตาม

นอกจากความยากในการพิจารณาการนิยามสงครามไซเบอร์แล้ว การแยกสงครามไซเบอร์ออกจากอาชญากรรมไซเบอร์ก็เป็นสิ่งที่ทำได้ยากเช่นกัน[45] เพราะในบางสถานการณ์ การแฮกข้อมูลก็อาจเป็นเพียงอาชญากรรมข้อมูลที่กระทบบุคคลเท่านั้น มิได้กระทบกับรัฐ เช่น การขโมยข้อมูลธุรกรรมการเงินที่เกิดขึ้นบ่อยครั้งในปัจจุบัน แต่หากการขโมยข้อมูลนั้นทำโดยบุคคลคนเดียว มิได้ทำโดยรัฐ แต่ส่งผลกระทบเป็นวงกว้าง เช่น หากเกิดเหตุการณ์ที่แฮกเกอร์ชาวรัสเซียได้ทำการจารกรรมข้อมูลอันเกี่ยวข้องกับความมั่นคงของสหรัฐ นั่นอาจทำให้พิจารณาว่าเป็นความตั้งใจในการบ่อนทำลายความมั่นคงของประเทศ ซึ่งหลังจากการกระทำดังกล่าว รัฐบาลรัสเซียอาจรู้เห็นเป็นใจอย่างลับๆ โดยการไม่ได้ลงโทษผู้กระทำผิด และปล่อยให้ความผิดลอยนวลไป เช่นนี้ ก็อาจพิจารณาได้เช่นกันว่าการจารกรรมข้อมูลดังกล่าว มิใช่อาชญากรรมไซเบอร์ แต่เป็นการก่อสงครามไซเบอร์

อันที่จริงรัฐและองค์กรระหว่างประเทศได้พยายามกำหนดคำจำกัดความของสงครามไซเบอร์แล้ว โดยเริ่มมีการพูดคุย และจัดให้เป็นวาระการประชุมครั้งแรกในสภายุโรป (Council of Europe) ในปี 2001 ซึ่งกลายเป็นอนุสัญญาบุดาเปสต์ว่าด้วยอาชญากรรมสงคราม[46] นี่ถือเป็นความพยายามโดยรัฐชาติและองค์กรระหว่างประเทศครั้งแรกที่พยายามจะจัดการกับปัญหาภัยคุกคามจากโลกไซเบอร์ ถึงแม้ว่าจะไม่ได้เป็นประเด็นที่เกี่ยวข้องกับสงครามไซเบอร์โดยตรงก็ตาม ขณะเดียวกันสหประชาชาติได้ออกมติ 57/239[47] ให้นานาชาติตระหนักถึงภัยคุกคามจากโลกไซเบอร์ และในปี 2016 ได้มีการจัดประชุมสมัชชาสหประชาชาติที่มหานครนิวยอร์ก[48] ครั้งที่ 71 ว่าด้วยภัยคุกคามจากโลกไซเบอร์ และสงครามไซเบอร์ แม้ว่าสุดท้ายแล้วการประชุมจะไม่ได้ข้อสรุปในวาระดังกล่าวก็ตาม แต่การตระหนักถึงภัยจากโลกไซเบอร์ และความจำเป็นที่จะนิยามคำจำกัดความของสงครามอันชอบธรรมให้ครอบคลุมกรอบของสงครามไซเบอร์ ก็ดูเหมือนจะมีมากขึ้น ซึ่งในช่วงเดือนมีนาคม ปี 2018 ที่ผ่านมา นายแอนโตนิโอ กูเตอร์เรส เลขาธิการสหประชาชาติ ได้เรียกร้องให้มีการปกป้องสิทธิพลเรือนจากการโจมตีทางไซเบอร์ และ ได้กล่าวว่า “there is no regulatory scheme for that type of warfare... It is not clear how the Geneva Convention or International Humanitarian Law applies to it.” [49]

[45]Martin Roesler, “When Do We Call a Cyber Attack an Act of Cyber War?,” Last Modified March 15, 2013, https://blog.trendmicro.com/trendlabs-security-intelligence/when-do-we-call-a-cyber-attack-an-act-of-cyber-war/

[46]Council of Europe, “Budapest Convention on Cybercrime,” Last Modified May 17, 2018, https://www.coe.int/en/web/cybercrime/the-budapest-convention

[47]UN General Assembly, “Resolution adopted by the General Assembly [on the report of the Second Committee (A/57/529/Add.3)] 57/239. Creation of a global culture of cybersecurity,” the United Nations, Last Modified January 31, 2003, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

[48]Michael Beaver, “THE UNITED NATIONS AND CYBERWARFARE,” Global Risk Advisor, Last Modified Sep 28, 2016, https://global-riskadvisors.com/blog/united-nations-cyber-warfare/

[49]Joseph S. Nye, “Billions of devices will soon be vulnerable to cyberattack. But we're not ready,” World Economic Forum, Last Modified, March 13, 2018, https://www.weforum.org/agenda/2018/03/how-will-new-cybersecurity-norms-develop

สรุป

ในปัจจุบัน พื้นที่ของสงครามมิได้จำกัดอยู่แค่การรบทางบก ทางน้ำ หรืออากาศอีกต่อไป แม้แต่พื้นที่โลกไซเบอร์ อันเป็นโลกเสมือนจริงที่ผู้คนใช้ติดต่อสื่อสารกันผ่านคอมพิวเตอร์ ได้พัฒนามาเป็นสนามรบรูปแบบใหม่รัฐชาติ การโจมตีในโลกไซเบอร์นี้ ได้นำพาความไม่มั่นคงรูปแบบใหม่มาสู่รัฐชาติ และระบบการเมืองระหว่างประเทศ ยิ่งพัฒนาการทางเทคโนโลยีที่ดำเนินไปอย่างรวดเร็วมากเท่าไร การพัฒนาการและความรุนแรงของการโจมตีในโลกไซเบอร์ก็ยิ่งทวีความรุนแรงมากขึ้นเท่านั้น และที่น่าเป็นห่วงก็คือยังไม่มีปทัสถานชุดใด ที่จะนำมาใช้รองรับภัยคุกคามรูปแบบใหม่ที่กำลังเกิดขึ้น ปทัสถานทางการเมืองระหว่างประเทศที่ใช้ในการจำกัดภัยคุกคามที่เกิดขึ้นต่อเสรีภาพของโลกในปัจจุบันอย่างหลักการสงครามอันชอบธรรม ก็ยังไม่สามารถที่จะใช้เป็นระบอบในการควบคุมและจำกัดความรุนแรงรูปแบบใหม่ที่เกิดขึ้นมาได้ การโจมตีอันรุนแรงและกระทบต่อความมั่นคงของรัฐอย่างกรณีการทำลายโรงงานนิวเคลียร์ของอิหร่านโดยมัลแวร์ Stuxnet การเจาะข้อมูลและป่วนระบบการเงินของสหรัฐ ฯ หรือแม้แต่การทำลายระบบควบคุมโรงไฟฟ้าของยูเครน ยังเป็นแค่จุดเริ่มต้นความรุนแรงของสถานการณ์การโจมตีที่เกิดขึ้นในโลกไซเบอร์และลามมาสู่โลกแห่งความเป็นจริงเช่นนี้จะยังคงเกิดขึ้น และรุนแรงมากขึ้นเรื่อยๆ หากปราศจากปทัสถานที่ทั่วโลกสามารถใช้ร่วมกันได้ รัฐชาติและสหประชาชาติจึงควรที่จะคิดพิจารณาหลักการที่จะสามารถนำมาตอบสนองต่อสถานการณ์ที่เกิดขึ้นนี้ เพื่อปกป้องคุ้มครองประชาชนธรรมดาทั่วไป และคงไว้ซึ่งสันติภาพของโลก

จริงอยู่ที่การสถาปนาปทัสถานใหม่ หรือนิยามปทัสถานที่จะครอบคลุมการโจมตีทางโลกไซเบอร์นี้จะมิได้แก้ปัญหาภัยคุกคามจากโลกไซเบอร์ได้อย่างเด็ดขาด แต่การสร้างปทัสถานบางอย่างเพื่อควบคุมและกำกับ ก็ยังช่วยบรรเทาความรุนแรงของสถานการณ์ และเป็นกลไกที่สามารถระงับการโจมตีโดยรัฐชาติได้ในระดับหนึ่ง ความพยายามของผู้เชี่ยวชาญด้านความมั่นคง นักวิจัย ผู้นำประเทศหรือผู้นำองค์กรระหว่างประเทศ ในแต่ละยุคแต่ละสมัยที่ได้ผ่านมา ได้พิสูจน์แล้วว่า แม้ว่าระบบความสัมพันธ์ระหว่างประเทศจะมีความเป็นอนาธิปไตย รัฐทุกรัฐมีอำนาจของตนเอง และความวุ่นวายในโลกก็ยังคงดำเนินต่อไป แต่การเริ่มทำอะไรบางอย่าง ก็ยังดีกว่าไม่ทำอะไรเลย แม้เป้าหมายอันหอมหวานและชวนเพ้อฝันอย่างสันติภาพจะยังคงเป็นเป้าหมายที่ยังดูไกลเกินกว่าจะเอื้อมจนดูเหมือนว่าจะไม่มีวันเป็นจริง แต่อย่างน้อยที่สุดโลกที่มีระเบียบกฎเกณฑ์ มีศีลธรรมกำกับมิให้รัฐใดรัฐหนึ่งกระทำการอันไร้ซึ่งความชอบธรรมต่ออีกรัฐหนึ่ง ก็ถือได้ว่าเป็นก้าวสำคัญในการจะทำให้โลกเป็นที่ที่น่าอยู่ขึ้นสำหรับมนุษยชาติ