สงครามยุคที่ 5: การก่อการร้ายไซเบอร์
The Fifth Dimension of Warfare: Cyber Terrorism

บทความวิชาการ

พิศาล อมรรัตนานุภาพ
Pisan Amornratananuparp
กองข่าวความมั่นคง สำนักข่าวกรอง กรมข่าวทหาร กองบัญชาการกองทัพไทย กรุงเทพฯ ประเทศไทย 10210
Security Intelligence Division, Intelligence Office, J-2,
Royal Thai Armed Forces Headquarters, Bangkok, Thailand 10210
E-mail: Pisanextra@gmail.com

บทคัดย่อ

สงครามไซเบอร์เป็นปัจจัยสำคัญในการวางยุทธศาสตร์สงครามในยุคที่ 5 ซึ่งจะครอบคลุม มิติของการคุกคามอยู่สองมิติ ได้แก่มิติที่ 1 เป็นมิติรูปแบบของสงคราม และมิติที่ 2 เป็นมิติของประเภทของเครื่องมือที่ใช้ในการสงคราม สำหรับมิติรูปแบบของสงครามหรือภัยคุกคามจะปรากฏให้เห็นในรูปแบบที่ฝ่ายคุกคามเปลี่ยนรูปแบบจากสงครามตามแบบมาสู่การใช้ความก้าวหน้าของเทคโนโลยี เป็นเครื่องมือสำคัญในการทำสงครามหรืออีกนัยหนึ่งเป็นสงครามไซเบอร์ (Cyber Warfare) และมิติของเครื่องมือทางด้านยุทธศาสตร์ที่เป็นภัยคุกคาม ในรูปแบบใหม่และเป็นสงครามนอกรูปแบบฝ่ายความมั่นคงจำเป็นจะต้องปรับแผนยุทธศาสตร์ ขีดความสามารถกำลังพล กลยุทธ์ เพราะสมรภูมิในยุคนี้ได้เปลี่ยนรูปแบบไปสู่สงครามไฮบริด (Hybrid Warfare) หรืออีกนัยหนึ่งเป็นสงครามที่มีรูปแบบ สงครามพันทาง/สงครามแบบผสมผสานที่นำสงครามตามแบบ (Conventional Warfare) ผนวกกับสงครามนอกแบบ (Irregular Warfare) ข้อแตกต่างระหว่างสงครามตามแบบกับสงครามไซเบอร์ คือ สงครามในยุคที่ 5 มิได้มุ่งหมายที่ส่งผลให้เกิดการสูญเสียชีวิต แต่หากต้องการทำการขัดขวางระบบในการปฏิบัติงาน หรือที่เรียกว่า “ยุทธการทำลายระบบ (System-disruption Operations)” ซึ่งความได้เปรียบจะขึ้นอยู่กับการพัฒนาและใช้โปรแกรมในการโจมตีที่มีหลากหลายและอาศัยความชำนาญเฉพาะบุคคล/กลุ่มเล็ก (Hackers) โดยจะปฏิบัติภารกิจสงครามกองโจร ที่มุ่งโจมตีไปที่ (ทางด้านการทหาร) ระบบการควบคุมบังคับการ (Command & Control) หรือสิ่งอุปกรณ์อิเล็กทรอนิกส์ในสนามรบ (Internet of Battlefield Things: IoBT) และ (ทางด้านความมั่นคงภายใน) ระบบสาธารณูปโภคที่สำคัญยิ่ง (Critical Infrastructure) และเป็นเป้าหมายอ่อนแอ

โดยสรุปชัยชนะของสงครามไฮบริดขึ้นอยู่กับการรวมอำนาจกำลังรบ การไม่แยกแผนยุทธการและยุทธวิธี (การรบตามแบบ การก่อการร้าย เทคโนโลยี) จากนั้น มีการวางเป้าหมายโจมตีร่วมไปที่จุดศูนย์ดุลของข้าศึก ซึ่งอาจเป็นการขัดขวางระบบการทำงานของโครงสร้างพื้นฐานที่สำคัญ

วันที่รับบทความ: 1 พ.ค.64 วันที่แก้ไขบทความ: 7 มิ.ย.64 วันที่ตอบรับบทความ: 6 ก.ค.64

คำสำคัญ: การก่อการร้ายทางไซเบอร์, โครงสร้างพื้นฐานสำคัญทางสารสนเทศ, สงครามแบบผสมผสาน

Abstract

The 5th Dimension of Warfare, Cyberterrorism

Cyberwarfare is the key factor in determining strategies for the 5th Dimension of Warfare, which includes threats in two dimensions, namely treats in warfare and threats that are the result of equipment used in warfare. As for the threats of warfare, it has been transformed from conventional warfare to the innovative use of technology as a tool to conduct warfare, in other words, Cyber Warfare. As for the strategic tools that have been used to counter non-conventional threats or non-conventional warfare, it is a necessity for security organizations to adapt their strategies, capabilities among personnel as well as tactics due to the transformation of the battlefield towards Hybrid Warfare. This new type of warfare incorporates Conventional Warfare with Irregular Warfare. The main difference between Conventional Warfare and Cyberwarfare is that the aims of operations in the 5th Dimension of Warfare do not target the loss of lives as a result, but carry out the operation through disruptive tactics, which are so-called System-disruption Operations. The advantage of the operation depends on the development and utilization of programs, as well as the various dimensions of the means of attacking through hackers. These individuals/ groups will carry out guerilla warfare that targets military assets, Command and Control, Internet of Battlefield Things: IoBT, Critical Infrastructure, and vulnerable targets.

It can be summarized that the success of Hybrid Warfare depends on the concentration of force, integrating operational and tactical plans (conventional warfare, terrorism, and technology) and joint attacks at the enemy's center of gravity, which disrupts the operation of key infrastructures.

Keywords: Cyber Terrorism, Critical Information Infrastructure, Hybrid Warfare

บทนำ

จากการศึกษาค้นคว้าเอกสารและตำราที่เกี่ยวข้องด้านความมั่นคงตั้งแต่สงครามโลกครั้งที่ 2 จนกระทั่งถึงปัจจุบัน ในเรื่องสงครามการต่อต้านการก่อการร้ายของสหรัฐอเมริกา (Global War on Terrorism) สามารถวิเคราะห์ได้ว่าไม่ว่ากำลังหรือขีดความสามารถของข้าศึกจะมีเท่าใด ในการเตรียมการวางแผนตั้งแต่ระดับยุทธศาสตร์ถึงระดับยุทธการจะต้องทำการกำหนดกรอบการยุทธ์ที่ครอบคลุมสนามรบทั้ง 4 มิติ (Domains of Warfare) ที่ประกอบด้วย พื้นดิน, ผืนฟ้า, ทะเล และอวกาศ ซึ่งการวางแผนการรบดังกล่าวเป็นไปในลักษณะของสงครามตามแบบ (Conventional Warfare) โดยใช้หลักการรบด้วยวิธีรุก รับ ร่นถอย และวางกำลังให้เหมาะสมต่อสถานการณ์นั้น ๆ โดยที่ผ่านมาเป็นที่ประจักษ์แล้วว่า ผู้ที่มีขีดความสามารถทางด้านอานุภาพและเทคโนโลยีทางทหารโดยเฉพาะอย่างยิ่งนภานุภาพ (Air Superiority) มักจะกุมความได้เปรียบในสมรภูมิซึ่งสามารถพบตัวอย่าง

จากสงครามอ่าวเปอร์เซียในปี 1991 (Gulf War 1991) ที่กองทัพภาคพื้นดินที่แข็งแกร่งของประธานาธิบดีซัดดัมได้พ่ายแพ้ต่อกลยุทธ์ การทิ้งระเบิดทางยุทธศาสตร์ (Strategic Bombing) ของสหรัฐฯ และพันธมิตร เพื่อทำลายจุดศูนย์ดุลของอำนาจกำลังรบของข้าศึกได้อย่างแม่นยำ ส่งผลให้แนวรบหน้าของสงครามอ่าวฯ ตัดสินด้วยเพียงเวลาแค่ 4 วัน และการสูญเสียทางกายภาพบนแนวรบในระดับที่ต่ำ และเป็นที่น่าสนใจว่ากองทัพอิรักที่มีประสบการณ์ในการทำสงครามมายาวนานและยากต่อความปราชัยเหตุใดจึงได้ประสบกับความพ่ายแพ้อย่างง่ายดาย ซึ่งสอดคล้องกับผลงานวิจัยหลายฉบับ พบว่า ชัยชนะที่เกิดจากกองกำลังพันธมิตรนั้นมีการพัฒนาเทคโนโลยีที่ทันสมัยกว่าคู่ต่อสู้อย่างเปรียบเทียบไม่ได้ (Cohen & Schmidt, 2014, p.109; Danahar, 2015, p.290-291; Fridman, 2018, p.20-24; Mearsheimer, 2014, p.96; Mousavian & Shaahidsaless, 2014; สุรชาติ บำรุงสุข, 2017, p.111-113)

การเขียนบทความฉบับนี้ มีวัตถุประสงค์เพื่อจะศึกษา 2 ประเด็นหลัก คือ ข้อแรก เพื่อศึกษาว่าในยุคแห่งเทคโนโลยีดิจิทัล สงครามไซเบอร์จะเป็นปัจจัยสำคัญในการวางยุทธศาสตร์สงครามในยุคที่ 5 หรือไม่ ซึ่งในที่นี้คำว่า สงครามยุคที่ 5 จะครอบคลุม มิติของการคุกคามอยู่สองมิติ ได้แก่ มิติที่ 1 เป็นมิติรูปแบบของสงคราม และมิติที่ 2 เป็นมิติของประเภทของเครื่องมือที่ใช้ในการสงคราม สำหรับมิติรูปแบบของสงครามหรือภัยคุกคามจะปรากฏให้เห็นในรูปแบบที่ฝ่ายคุกคามเปลี่ยนรูปแบบจากสงครามตามแบบมาสู่การใช้ความก้าวหน้าของเทคโนโลยีเป็นเครื่องมือสำคัญในการทำสงครามหรืออีกนัยหนึ่งเป็นสงครามไซเบอร์ (Cyber Warfare) และมิติของเครื่องมือทางด้านยุทธศาสตร์ที่เป็นภัยคุกคามในรูปแบบใหม่ และเป็นสงครามนอกรูปแบบโดยข้อสันนิษฐานดังได้กล่าวข้างต้น คือ ภัยคุกคามรูปแบบใหม่จะมาพร้อมกับความก้าวหน้าล้ำสมัยของเทคโนโลยีดิจิทัล ซึ่งฝ่ายความมั่นคงจำเป็นจะต้องทบทวนและปรับทั้งแผนยุทธศาสตร์ ขีดความสามารถกำลังพล และกลยุทธ์ เพราะสมรภูมิในยุคนี้ได้เปลี่ยนรูปแบบไปสู่สงครามไฮบริด (Hybrid Warfare) หรืออีกนัยหนึ่งเป็นสงครามที่มีรูปแบบสงครามพันทาง/สงครามแบบผสมผสาน ที่นำสงครามตามแบบ (Conventional Warfare) ผนวกกับสงครามนอกแบบ (Irregular Warfare) ข้อสอง เพื่อศึกษาเกี่ยวกับประเภทของเครื่องมือทางยุทธศาสตร์ด้านการใช้ Hard Power ซึ่งหมายถึง การใช้กำลัง/อำนาจ และ Soft Power คือ การสร้างความเชื่อ/โน้มน้าว ประเภทใดบ้างที่ภัยคุกคามรูปแบบใหม่ที่เป็นรัฐ ตัวแทนแห่งรัฐ และไม่ใช่รัฐ (State-State Proxies-Non State Actor) เลือกใช้ในการโจมตีผ่านสงครามนอกแบบแห่งยุคดิจิทัล โดยก่อนที่จะทำการค้นคว้าเอกสารฉบับนี้ผู้เขียนมีเจตนารมณ์ให้เกิดการทบทวนและความตระหนักว่าปัจจุบันเราอยู่ในยุคศตวรรษที่ 21 การดำเนินชีวิตของประชาชน การทำงานภาคเอกชน การวาง/การเตรียมกำลังและการปฏิบัติการรบของฝ่ายความมั่นคง จะต้องทำงานผ่านระบบดิจิทัลบนโลกไซเบอร์ ซึ่งผลกระทบทั้งหมดต่อ/ผ่านระบบโครงสร้างสาธารณูปโภคเครือข่าย 5G ที่เชื่อมต่อกับอุปกรณ์คอมพิวเตอร์ อินเทอร์เน็ต และสิ่งอุปกรณ์อิเล็กทรอนิกส์ที่ปัจจุบันได้กลายมาเป็นส่วนหนึ่งของการดำรงชีวิตเป็นที่เรียบร้อยแล้ว และนั่นหมายถึง ฝ่ายความมั่นคงจะต้องปรับกลยุทธ์และแผนยุทธศาสตร์ให้ทันสมัยสอดคล้องต่อกระแสการเปลี่ยนแปลงของโลกเช่นกัน

Part I: สงครามไซเบอร์ (Cyberwarfare): The Fifth Dimension of Warfare

'...Winner...combining two or more battlefield factors together-for achieving victory...'

(Qiao Liang & Wang Xiangsui, 1999: as cited in Fridman, 2018, p.12-13)

จากกรณีสงครามอ่าวเปอร์เซีย (Gulf War 1991) หากมองเพียงผิวเผิน อาจพบว่า ชัยชนะของกองกำลังร่วมสหรัฐฯ และพันธมิตรได้รับชัยชนะจากการทำสงครามตามแบบที่ทำการโจมตีด้วย จรวด/ระเบิดนำวิถี (Precision-guided Bombs) (อาวุธที่ทันสมัยในขณะนั้น) ต่ออาวุธยุทโธปกรณ์ของกองทัพอิรักส่งผลกระทบให้สูญเสียอำนาจกำลังรบไปอย่างรวดเร็ว แต่ตามความเป็นจริงจากการวิเคราะห์และสังเคราะห์ข้อมูลเป็นข้อค้นพบที่ได้จากการศึกษาแล้วจะเห็นได้ว่า นอกเหนือจากการทำลายขีดความสามารถทางทหาร ปัจจัยที่สำคัญ คือ ความก้าวหน้าทางเทคโนโลยีของสหรัฐฯ ที่ได้เริ่มใช้ ระบบบัญชาการและควบคุม (Command & Control: C2) ในการเก็บรวบรวมข้อมูล วิเคราะห์ และประเมินผลการปฏิบัติของการรบ และได้เปลี่ยนจากการยุทธ์ที่มุ่งการทำลายทางกายภาพ เป็นการยุทธ์เพื่อทำลาย/ขัดขวางระบบการบริหาร/สั่งการบังคับการและโครงสร้างพื้นฐานที่สำคัญยิ่ง (The Effect of System Disruption) หรือทางทหารเรียกว่า การทำลาย (ระบบควบคุมบังคับบัญชา) ที่เป็นจุดศูนย์ดุลย์ (Center of Gravity: CG) ซึ่งเป็นที่ประจักษ์แล้วว่าการรบตามแบบเพียงอย่างเดียวไม่สามารถนำไปสู่ชัยชนะได้ แต่จะต้องเป็นสงครามไฮบริดที่เป็นการยุทธ์ที่ผสมผสานระหว่างตัวแสดงที่หลากหลาย เทคโนโลยีที่ทันสมัย/ซับซ้อน และการใช้สงครามนอกแบบ (ประกอบด้วย สงครามกองโจร และสงครามก่อความไม่สงบ) ซึ่งทั้งหมดของการผสานสรรพกำลังหรือที่ในตำราการทหารเรียกว่า “Total War” (Fridman, 2018, p.12-13, 32-33) โดยผลลัพธ์ของการโจมตีจากรูปแบบนี้จะก่อให้เกิดผลกระทบต่อจุดยุทธศาสตร์และต่อความเป็นอยู่ของประชาชน ปัจจุบันประเทศมหาอำนาจอย่างเช่น สหรัฐอเมริกา รัสเซีย จีน ต่างตระหนักและให้ความสำคัญในการปรับเปลี่ยนแบบแผนกลยุทธ์ในการทำสงครามโดยได้มีการเพิ่มสนามรบนอกเหนือจากพื้นดิน ผืนฟ้า ทะเล อวกาศ โดยได้เพิ่มสนามรบที่ห้า คือ “ไซเบอร์สเปซ” (Cyberspace) ในการทำสงครามยุคดิจิทัล ซึ่งภัยคุกคามรูปแบบใหม่มีขีดความสามารถด้านเทคโนโลยีและเพิ่มความสลับซับซ้อนมากยิ่งขึ้น

สุรชาติ บำรุงสุข (2019) และ Fridman (2018) ได้ให้ทัศนะพ้องกันว่า ชัยชนะของสงครามไฮบริดขึ้นอยู่กับการรวมอำนาจกำลังรบ การไม่แยกแผนยุทธการและยุทธวิธี (การรบตามแบบ การก่อการร้าย เทคโนโลยี) จากนั้นมีการวางเป้าหมายโจมตีร่วมไปที่จุดศูนย์ดุลย์ของข้าศึก ซึ่งอาจเป็นการขัดขวางระบบการทำงานของโครงสร้างพื้นฐานที่สำคัญ ในสถานการณ์โลกปัจจุบันโอกาสที่รัฐจะทำสงครามสมมาตร (Symmetric Warfare) หรือสงครามตามแบบนั้นเป็นไปได้ยากเพราะต่างฝ่ายต่างไม่ต้องการที่จะเปิดเผยตัวตน เนื่องจากอาจส่งผลกระทบต่อภาพลักษณ์ในเวทีสากลจึงต้องหันมาพัฒนาวิธีโจมตีด้วยอาวุธที่ยากต่อการตรวจพบแหล่งที่มาที่แท้จริง ซึ่งนำไปสู่การสนับสนุนให้มีการสร้างนักรบไซเบอร์ (Cyber Army หรือ Cyber Warrior) ทั้งทางเปิดและทางปิด โดยหากทำการเปรียบเทียบระหว่าง นักรบในสงครามตามแบบ (Conventional/The Old Wars) กับกลุ่มนักรบไซเบอร์ในรูปแบบของสงครามแนวใหม่ (The New Wars) แล้วสามารถวิเคราะห์ได้ว่ามีหลักการ/แนวคิดในการแบ่งอำนาจการรบที่ไม่แตกต่างกัน เนื่องจากเหตุที่ว่า นักรบทั้ง 2 ยุคล้วนแล้วแต่มีเครื่องมือทางยุทธศาสตร์ในการสร้างชัยชนะที่ประกอบด้วยการใช้กำลัง/อำนาจ (Hard Power) และการสร้างความเชื่อ/โน้มน้าว (Soft Power) ทางด้าน Hard Power สิ่งที่แตกต่างที่เห็นได้ชัด 2 ประการ คือ **วัตถุประสงค์ และอาวุธ/เครื่องมือ** ส่วนแรก การวิเคราะห์วัตถุประสงค์ กล่าวคือ วัตถุประสงค์ของการโจมตีเปลี่ยนไปเนื่องจากสาเหตุที่ว่าสงครามไซเบอร์มิได้มุ่งหมายที่ส่งผลให้เกิดการสูญเสียชีวิต แต่หากต้องการทำการขัดขวางระบบในการปฏิบัติงานหรือที่เรียกว่า “ยุทธการทำลายระบบ” (System-disruption Operations) ซึ่งความได้เปรียบ

จะขึ้นอยู่กับการพัฒนาและใช้โปรแกรมในการโจมตีที่หลากหลายและอาศัยความชำนาญเฉพาะบุคคล/กลุ่มเล็ก (Hackers) โดยจะปฏิบัติภารกิจสงครามกองโจรที่มุ่งโจมตีไปที่ (ทางด้านการทหาร) ระบบการควบคุมบังคับการ (Command & Control) หรือสิ่งอุปกรณ์อิเล็กทรอนิกส์ในสนามรบ (Internet of Battlefield Things: IoBT) และ (ทางด้านความมั่นคงภายใน) ระบบสาธารณูปโภคที่สำคัญยิ่ง (Critical Infrastructure) และเป็นเป้าหมายอ่อนแอ ซึ่งหากพิจารณาถึงลักษณะหรือรูปแบบลักษณะของการปฏิบัติการแล้วเปรียบเสมือนสงครามนอกแบบที่ใช้นักรบกองโจรที่มีขีดความสามารถเฉพาะตัวเพื่อทำลายเป้าหมายจำกัด (Cohen & Schmidt, 2014, p.7, 103-112; Martin & Weinberg, 2017, p.45-46, 224; Mazanec & Whyte, 2019, p.31-32)

> "Defend forward is described as getting as close to adversaries as possible to see what they're planning as a means of informing others to prepare or take action themselves."
>
> (U.S. Cyberspace Solarium Commission, 2019 as cited in Borghard, 2020)

การวางยุทธศาสตร์ในการทำสงครามไซเบอร์ของสหรัฐฯ หน่วยงานที่รับผิดชอบโดยตรง (U.S. Cyberspace Solarium Commission) มีมุมมองเกี่ยวกับการวางยุทธศาสตร์ว่าในการทำการยุทธ์จะต้องวางกำลังและเครื่องมือให้ใกล้กับตัวหรือระบบข้าศึก/ภัยคุกคามให้มากที่สุด หรือที่เรียกว่า "Defend Forward" เพื่อช่วยในการติดตามเป้าหมายและเข้าดำเนินการระงับเหตุได้ทันท่วงที ซึ่งตามหลักของสงครามตามแบบ เรียกว่า ระบบปฏิบัติการรวบรวมข่าวกรอง (Intelligence Surveillance Reconnaissance: ISR) โดยหากจะกล่าวถึง ส่วนที่สอง ด้านการวิเคราะห์ด้านอาวุธ/เครื่องมือ จะเห็นได้ว่าในการทำสงครามไซเบอร์สามารถแบ่งออกเป็น 2 จำพวก คือ การโจมตีแบบเจาะจงอุปกรณ์กับการโจมตีต่อระบบเครือข่าย โดยการโจมตีแบบเจาะจง: มีอาวุธที่เรียกว่า การใช้มัลแวร์ (Malicious Software: MalWare) ซึ่งเป็นซอฟต์แวร์อันตรายที่ถูกออกแบบมาเพื่อทำการขัดขวางการทำงานของระบบคอมพิวเตอร์ โดยมี 3 แบบคือ Viruses, Worms, Trojan Horses รูปแบบที่พบเป็นประจำ คือ การเจาะระบบในรูปแบบม้าโทรจัน (Trojan Horses) เปรียบเสมือนหน่วยรบพิเศษในภารกิจสงครามนอกแบบที่จะทำการลักลอบและซ่อนตัวอยู่ในแนวหลังของข้าศึก โดยเป็นการโจมตีระบบเครือข่ายรูปแบบหนึ่งที่แฮกเกอร์จะเลือกเป้าหมาย เพื่อโจมตีหน่วยงานที่มีข้อมูลสำคัญ เช่น หน่วยงานทางทหารหรือหน่วยงานทางด้านความมั่นคงปลอดภัยของประเทศ หน่วยงานทางการเมือง หรือองค์กรธุรกิจขนาดใหญ่ โดยอาศัยเทคนิคการโจมตีรูปแบบต่าง ๆ ผสานกันเพื่อให้ประสบผลสำเร็จทำให้ระบบรักษาความมั่นคงปลอดภัยทั่วไปอาจจะไม่สามารถรับมือได้ ในขณะที่การโจมตีที่ระบบเครือข่าย (Distributed Denial-of-Service: DDOS) เปรียบเสมือนการรบตามแบบที่ใช้กองพลทหารราบจำนวนมากบุกโจมตีที่หมาย แต่ทางไซเบอร์จัดว่าเป็น Brute Force ซึ่งหมายถึง การใช้พลังบังคับด้วยกำลังพล Botnets ในการดำเนินกลยุทธ์ทางไซเบอร์ที่จะกระจายตัวเข้าควบคุมคอมพิวเตอร์จำนวนมาก จากนั้น จึงส่งข้อมูลเข้าสู่เป้าหมาย/ฝ่ายตรงข้ามพร้อมกันในเวลาเดียวกัน ส่งผลทำให้ แบนวิธ (Bandwidth) ปริมาณการรับ-ส่งข้อมูลมีมากจนเกินขนาดที่รองรับได้ ซึ่งเป็นการโจมตีกระทำลักษณะเพื่อปฏิเสธการให้บริการของเจ้าของระบบ/เครือข่าย (Mazanec & Whyte 2019, p.26-30, 225-226)

สรุป/ข้อเสนอ: จากข้อมูลที่ได้ผ่านการวิเคราะห์ตามหลักการทางวิชาการแล้วสรุปได้ว่าการทำสงครามในยุคทศวรรษที่ 21 ได้เดินมาสู่ยุคสงครามแบบผสมผสาน (Hybrid Warfare) เป้าหมายของการโจมตี คือ

จุดศูนย์ดุลย์ของข้าศึก (CG) เพื่อการขัดขวางระบบการควบคุมบังคับบัญชาและโครงสร้างพื้นฐานที่สำคัญยิ่ง ซึ่งแม้ว่าจะเป็นสงครามสมัยใหม่ การโจมตีจะเป็นการรวมสรรพกำลังทั้งหมด ทั้งกองกำลังสงครามตามแบบและกองกำลังสงครามนอกแบบ ดังนั้นฝ่ายความมั่นคงควรปรับเพิ่มแผนยุทธศาสตร์และแผนการรบใหม่ ตลอดจนการเพิ่มขีดความสามารถของกำลังพลโดยเฉพาะในเรื่องการเพิ่มนักรบพิเศษในสงครามไซเบอร์เพื่อให้สอดคล้องต่อสถานการณ์โลกที่เปลี่ยนไป โดยต้องตระหนักถึงตัวแสดงที่เป็นรัฐ ตัวแทนแห่งรัฐ ตัวแสดงที่ไม่ใช่รัฐ ที่ทุกฝ่ายต่างมีความเท่าเทียมในเรื่องการเข้าถึงเครื่องมือทั้ง Hard Power และ Soft Power ที่ใช้เทคโนโลยีที่ทันสมัย/ซับซ้อนในการดำเนินกลยุทธ์ด้านยุทธศาสตร์และวางแผนการทำสงครามที่สำคัญ อาจจะต้องพิจารณาไปสู่แบบการวางกำลังในทางลึกหรือแนวชายแดนของข้าศึก (Defend Forward) เพื่อทำการรวบรวมข่าวสาร/ข่าวกรอง ให้ได้มาซึ่งข้อมูล (Data) ที่เป็นทรัพยากรสำคัญในการประมวลผลในสงครามยุคดิจิทัล ให้ทันท่วงทีก่อนที่ฝ่ายตรงข้ามจะเริ่มปฏิบัติการใด ๆ จึงจะสามารถเอาชนะสงครามในยุคที่ 5 ได้อย่างแท้จริง

Part II: การก่อการร้ายทางไซเบอร์ (Cyber Terrorism)

> "The first rule of unrestricted warfare is that there are no rules, with nothing forbidden."
>
> (Qiao Liang & Wang Xiangsui, 1999 as cited in Fridman, 2018)

Mockaitis (2008, p.96-98) ระบุว่า การก่อการร้ายได้เปลี่ยนโฉมเป็นการก่อการร้ายทางไซเบอร์ (Cyber-terrorism) ที่มีขีดความสามารถในการใช้/ปล่อยมัลแวร์ (Malware): Computer Viruses, Worms, Trojan Horses โดยจะมีเป้าหมายการโจมตีไปที่โครงสร้างพื้นฐานที่สำคัญยิ่ง (Critical Infrastructure) เช่น ระบบการจ่ายไฟฟ้า โรงพยาบาล ระบบการสื่อสาร สารสนเทศ รวมถึงการเข้าถึงข้อมูลบุคคลสำคัญ ดังที่ได้กล่าวไว้ในเรื่อง The Fifth Domain of Warfare ว่า สงครามสมัยใหม่จะเป็นสงครามแบบไร้ขีดจำกัด และผู้ก่อเหตุเป็นได้ทั้งตัวแสดงที่เป็นรัฐ ตัวแทนแห่งรัฐ และไม่ใช่รัฐ ที่มีเป้าหมายการโจมตีเป็น "ยุทธการทำลายระบบ" ด้วยรูปแบบของปฏิบัติการสงครามนอกแบบ (Irregular Warfare) โดยคู่ขัดแย้ง จะเลี่ยงการเผชิญหน้ากันโดยตรง ซึ่งจากการศึกษาของ Hoffman (2017, p.210) Martin & Weinberg (2017, p.45-46, 76) และ Mazanec & Whyte (2019) พบว่า กลุ่มก่อการร้ายสมัยใหม่ (New Terrorist) ได้พัฒนาองค์กรจนสามารถเปลี่ยนโฉมกลายเป็นกลุ่มก่อการร้ายทางไซเบอร์ที่มีความสามารถด้านเทคโนโลยีแห่งยุค 5G โดยมีคุณลักษณะสำคัญ คือ ข้อแรก Hard Power เป็นพลังอำนาจเรื่องการสร้างแนวรบที่ยากต่อการตรวจพบ ซึ่งมีความสามารถในการโจมตีแบบเสรีโดยปราศจากพิกัดและเวลา กล่าวคือ สามารถทำการโจมตีจากที่ใดและเวลาใดอย่างอิสระเสรี ซึ่งเป็นการมุ่งโจมตีพื้นที่บังคับการหรือพื้นที่ส่วนหลัง เช่น ระบบโครงสร้างพื้นฐานที่สำคัญยิ่ง ข้อสอง Soft Power เป็นพลังอำนาจในการปฏิบัติการเรื่องการทำโฆษณาชวนเชื่อซึ่งในการสงครามในอดีต เรียกว่า ปฏิบัติการข่าวสาร (Information Operations: IO) โดยสื่อเกือบทั้งหมดล้วนเป็นเครื่องมือของรัฐ แต่เพียงฝ่ายเดียวแต่ปัจจุบันความทัดเทียมและโอกาสในการเข้าถึงข้อมูลข่าวสารได้ส่งผลมายังตัวแสดงที่ไม่ใช่รัฐนั้น สามารถเข้าถึงได้อย่างเท่าเทียม นับจากนี้แล้วประเด็นที่สำคัญที่ไม่อาจมองข้าม คือ ในเรื่องสงครามแบบไร้ข้อจำกัดมีส่วนที่เหมือนสงครามนอกแบบ คือ กลุ่ม/องค์กรจะหาวิธีการต่อสู้เพื่อทดแทนในสิ่งที่เป็นจุดอ่อน ซึ่งกลุ่มก่อการร้ายนั้นเข้าใจเป็นอย่างดี จึงได้ปรับเปลี่ยนองค์กรให้สอดคล้องต่อสถานการณ์โลกที่เปลี่ยนไปจนผันตนเองมาเป็นการก่อการร้ายไซเบอร์เรียบร้อยแล้ว

นอกจากนี้การวิเคราะห์ดังกล่าวข้างต้นยังสอดคล้องกับคำกล่าวของผู้บริหารบริษัทกูเกิล Cohen & Schmidt (2014, p.157-158) ซึ่งได้เขียนหนังสือ The New Digital Age

โดยได้คาดการณ์ไว้ตั้งแต่ปี ค.ศ.2014 ระบุว่า การก่อการร้ายทางไซเบอร์ (Cyber Terrorism) จะเป็นภัยคุกคามต่อความมั่นคงของโลกและจะส่งผลให้ฝ่ายความมั่นคงทั่วโลกต้องปรับกระบวนยุทธ์ในการต่อสู้และรับมือ ซึ่งนับว่าเป็นคำทำนายที่แม่นยำเนื่องจากในยุคดิจิทัลนี้ กลุ่มก่อการร้ายได้เปลี่ยนสภาพเป็นกลุ่มก่อการร้ายทางไซเบอร์เป็นที่เรียบร้อยแล้วอย่างที่ได้ปรากฏในห้วง 10 ปีที่ผ่านมา กลุ่มก่อการร้ายได้พัฒนาขีดความสามารถในการใช้เทคโนโลยีเพื่อทำสงครามโดยสามารถวางยุทธศาสตร์ทั้ง Soft Power และ Hard Power ดังจะเห็นได้จากข้อสังเกตเชิงประจักษ์กล่าวคือ ข้อแรก การใช้ Soft Power เป็นการทำสงครามทางความคิดบนพื้นที่ออนไลน์เพื่อแสวงประโยชน์จากเทคโนโลยีสารสนเทศในการเผยแพร่อุดมการณ์และแนวคิด (Ideology) ทางโลกเสมือนจริง (Virtual/Cyber Domain) ตัวอย่างที่ปรากฏในกรณีกลุ่มก่อการร้าย ISIS ที่ประสบความสำเร็จในการใช้สื่อสังคมออนไลน์ เช่น Twitter และ Facebook ในการระดมพล (Recruit) ทำให้มีนักรบ Foreign Terrorist Fighters จากทุกมุมโลกกว่า 25,000 คน เข้าร่วมปฏิบัติภารกิจในการสถาปนารัฐอิสลาม (Caliphate) อีกทั้งยังให้กลุ่มก่อการร้ายประจำถิ่นทำการสาบานตนสวามิภักดิ์ แบบ Real-time ผ่าน Social Media ข้อสอง การใช้ Hard Power ที่สนามรบทางกายภาพได้ปรับเปลี่ยนจากการก่อการร้ายชนบทมาเป็นการก่อการร้ายในเมือง และมีเป้าหมายที่จะทำลาย/ขัดขวาง (Disrupt) ระบบโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบโครงสร้างความมั่นคงทางทหาร หรือการเจาะข้อมูลเพื่อสร้างความตื่นตระหนกหวาดกลัวในหมู่ประชาชน เช่น เหตุการณ์เมื่อ 21 ก.ค.2018 กระทรวงสาธารณสุข (MOH) ของสิงคโปร์ถูกแฮ็กเจาะระบบขโมยข้อมูลประวัติคนไข้ของ SingHealth กว่า 1.5 ล้านคน หรือเมื่อ 9 ก.ค.2019 หน่วยป้องกันชายฝั่งสหรัฐฯ (U.S. Coast Guard) ถูกมัลแวร์เจาะระบบบริหารข้อมูลคลังสินค้า/ระบบสื่อสาร ซึ่งทั้ง 2 กรณีสันนิษฐานว่าเป็นการโจมตีของกลุ่มก่อการร้ายที่มีรัฐอยู่เบื้องหลัง (สุรชาติ บำรุงสุข, 2016; Cohen & Schmidt, 2014, p.151, 153-154) ซึ่งเป้าประสงค์หลักของการก่อการร้ายร่วมสมัยนี้ มิได้ต้องการที่จะก่อให้เกิดการสูญเสียขนาดใหญ่เสมือนเหตุการณ์ 9/11 แต่เพื่อแสดงให้เห็นว่า รัฐบาลไม่มีประสิทธิภาพในการปกครองหรือรักษาความสงบสุขของสาธารณชน

> “มาตรา 60 การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์...โดยมุ่งหมาย เพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือ โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ...หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้”
>
> (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562, 2562, เล่ม 136)

หากพิจารณานิยามโครงสร้างพื้นฐานที่สำคัญยิ่ง (Critical Infrastructure) ของผู้เชี่ยวชาญด้านการต่อต้านการก่อการร้าย และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ของไทยประกอบในการวิเคราะห์จะพบว่ากลุ่ม/บุคคลใดที่ทำการเข้าถึง (Hack) เพื่อหยุดหรือขัดขวางระบบโครงสร้างพื้นฐานที่สำคัญยิ่ง และสร้างความตื่นตระหนกให้แก่ประชาชน ซึ่งไม่ว่าจะเป็นการกระทำของกลุ่มเคลื่อนไหวใด ๆ หรือกลุ่มตัวแทนของรัฐ (Proxies) ล้วนนับว่าเป็นการกระทำในลักษณะความผิดของการก่อการร้ายตามกฎหมาย (Hoffman, 2017, p. 209-210; Mockaitis, 2008, p. 96-97) จากการวิเคราะห์ดังกล่าวยังพบว่ากลุ่มก่อการร้ายใหม่ในยุคดิจิทัลสามารถแสวงประโยชน์บนโลกไซเบอร์ ยุทธศาสตร์ด้าน Soft Power ในเรื่องการปฏิบัติการข่าวสาร (IO) ด้วยการผลิตโฆษณาชวนเชื่อได้อย่างมีประสิทธิภาพ แสดงให้เห็นว่าการคาดการณ์ของผู้บริหารกูเกิล Cohen & Schmidt (2014) นั้นถูกต้องแม่นยำ จึงเป็นที่น่าสนใจว่าการคาดการณ์ในเรื่อง

ต่อมา คือ “The Rise of Terrorist Hacker” ว่าการพัฒนาขีดความสามารถด้าน Hard Power ในการเจาะเพื่อควบคุมระบบ/หน่วยงานด้านความมั่นคงจะเกิดผลกระทบอย่างกว้างขวางเมื่อใด เนื่องจากที่ผ่านมาได้เกิดขึ้นจริงแล้วหลายครั้งทั้งกลุ่มตัวแทนแห่งรัฐและกลุ่มก่อการร้าย (Proxy & Non-state Actor) ดังตัวอย่างกลุ่มที่เป็นตัวแทนแห่งรัฐ (Russian Proxy) เช่น กรณีบริษัท Ukrenergo ซึ่งให้บริการจ่ายไฟฟ้าในยูเครนถูกโจมตีด้วยการฝังมัลแวร์โทรจัน (Blackenergy) นำไปสู่การก่อกวนระบบจ่ายไฟฟ้าด้วยวิธี DDOS เมื่อ 17 ธ.ค.2016 ส่งผลให้ไฟฟ้าดับครึ่งประเทศเป็นเวลาหลายชั่วโมง ซึ่งมีการสันนิษฐานว่า เป็นการโจมตีของตัวแสดงแทนแห่งรัฐ (Russian Proxy) (Fridman 2018, p.115-116) ตัวอย่างภัยจากกลุ่มที่ไม่ใช่รัฐที่มีขีดความสามารถตรงตามหลักแนวคิดของสงครามไฮบริด คือ กลุ่มก่อการร้าย เฮซบอลเลาะห์ เนื่องจากเป็นกลุ่มฯ ที่มีกองกำลังตามแบบและกองกำลังนอกแบบอยู่ในการบังคับบัญชาและเป็นที่ประจักษ์แล้วว่าในสงครามเลบานอน ครั้งที่ 2 (The 2nd Lebanon War 2006) เป็นสงครามที่กองทัพอิสราเอลไม่สามารถเอาชนะได้ นอกเหนือจากกลุ่มเฮซบอลเลาะห์มีการใช้ยุทธวิธีก่อการร้ายและเทคโนโลยีในสงคราม เช่น Unmanned Aerial Vehicle: UAV ติดอาวุธ เป็นแนวรบหน้าแทนการดำเนินกลยุทธ์ลักษณะสงครามตามแบบ แต่ยังได้ทำสิ่งที่กองทัพอิสราเอลคาดไม่ถึง คือ การพัฒนาขีดความสามารถด้านการข่าวกรองทางสัญญาณ (Signal Intelligence: SIGINT) เพื่อใช้ในการดักรับฟังความเคลื่อนไหวของผู้บังคับบัญชาของอิสราเอลอย่างต่อเนื่องทำให้สามารถหลบเลี่ยงการถูกโจมตีจุดศูนย์ดุลของฝ่ายตนเองได้ตลอดเวลา

สรุป/ข้อเสนอ: ในยุคของการเปลี่ยนอย่างฉับพลันทางดิจิทัล (Digital Disruption) ฝ่ายความมั่นคงได้ถูกความก้าวหน้าของเทคโนโลยีบังคับวิถีให้เดินเข้าสู่แนวรบที่ 5 ดังนั้น จึงควรต้องพิจารณาเพื่อทบทวนปรับแผนการยุทธ์ที่ครอบคลุมในเรื่องไซเบอร์และเทคโนโลยีเนื่องจากในคำถาม คือ สมรภูมิไซเบอร์ที่เป็นสงครามนอกแบบนั้น มีตัวแสดงรัฐ ตัวแทนแห่งรัฐ ตัวแสดงที่ไม่ใช่รัฐ (การก่อการร้ายใหม่/การก่อการร้ายไซเบอร์) ที่มีขีดความสามารถด้านเทคโนโลยีในระดับที่สูงโดยเฉพาะด้านยุทธศาสตร์ Soft Power จนสามารถจูงใจให้เกิดทัศนคติและพฤติกรรมที่ต้องการได้ ซึ่งปัจจุบันได้มีการยกระดับโดยการเพิ่มภารกิจเป็นยุทธการทำลายระบบ (Hard Power) ฝ่ายความมั่นคงมีแผนการยุทธ์สงครามไซเบอร์และแผนการจัดการสถานการณ์วิกฤต (Crisis Respond) ที่มีประสิทธิภาพและครอบคลุมทุกเป้าหมายที่เป็นโครงสร้างพื้นฐานที่สำคัญยิ่งหรือไม่ เนื่องจากระบบรักษาความมั่นคงปลอดภัยตามหลักการรบในสงครามตามแบบอาจไม่สามารถรับมือกับชุดการโจมตีที่มาจากกลุ่มก่อการร้ายไซเบอร์ที่มีอาวุธ เช่น Phishing, Advanced Malware และ Web Attacks ดังนั้น หากการปรับองค์กรช้าและไม่ทันสมัยอาจจะไม่ทันต่อภัยคุกคามรูปแบบใหม่ โดยเฉพาะอย่างยิ่งหากกลุ่มก่อการร้ายใหม่ เริ่มใช้ Soft Power เพื่อระดมสรรพกำลังให้เหล่านักรบไซเบอร์อิสระเข้าร่วมปฏิบัติการโจมตีเป้าหมายโครงสร้างพื้นฐานที่สำคัญยิ่งในเวลานี้คาดว่าฝ่ายรัฐคงยังไม่สามารถทำการแก้ไขได้ทันเวลาและด้วยเหตุนี้นโยบาย “Defend Forward” จึงเป็นกลยุทธ์ที่น่าสนใจเพื่อนำไปพัฒนาปรับใช้อย่างยิ่ง

Part III: การเตรียมการรับมือจากภัยคุกคามไซเบอร์: Cyber Warriors

“มาตรา 4: การข่าวกรอง หมายความว่า การดำเนินการเพื่อให้ทราบถึงความมุ่งหมาย กำลังความสามารถและความเคลื่อนไหว รวมทั้งวิถีทางของบุคคล กลุ่มบุคคลหรือองค์การใด ทั้งภายในประเทศ และต่างประเทศที่อาจกระทำการอันเป็นพฤติการณ์เป็นภัยคุกคาม ทั้งนี้เพื่อรักษาความมั่นคงหรือประโยชน์แห่งรัฐและให้รัฐบาลนำมาประกอบการพิจารณาในการกำหนดนโยบายแห่งชาติ” (พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562, 2562 เล่ม 136)

ผู้เชี่ยวชาญด้านยุทธศาสตร์และความมั่นคง Fridman (2018), Hoffman (2017); Martin & Weinberg (2017); Mearsheimer (2014) ล้วนมีความเห็นตรงกันว่า ชัยชนะในสงครามตั้งแต่ยุคที่ 1 ถึงยุคที่ 5 (ยุคปัจจุบัน) ล้วนอยู่บนพื้นฐานในการพัฒนาทางเทคโนโลยีที่เหนือกว่าฝ่ายตรงข้าม ปัจจุบันโลกได้เข้าสู่ยุคเทคโนโลยี 5G การทำงานแบบเดิมได้ถูกขัดขวางอย่างรุนแรงด้วยสิ่งอุปกรณ์ดิจิทัล (Digital Disruption) อย่างก้าวกระโดดและต่อเนื่อง (Exponential Growth) ซึ่งการเปลี่ยนแปลงย่อมส่งผลกระทบมาสู่งานด้านความมั่นคง เช่น ระบบบัญชาการและควบคุม (Command & Control: C2) ที่ทำการควบคุมการสื่อสารผ่านระบบเทคโนโลยีสารสนเทศ (Information and Communication Technology: ICT) อุปกรณ์ปัญญาประดิษฐ์ในสนามรบ (Battlefield Artificial Intelligence: BAI) การวิเคราะห์/ค้นหาข้อมูลสามารถใช้เทคโนโลยีการเก็บฐานข้อมูลทั้งแบบคลาวน์ (Cloud) และ Big Data ซึ่งเมื่อโลกปรับ ส่งผลให้องค์กรภาครัฐ เอกชน และประชาชน ไม่มีทางเลือกนอกจากจะต้องเปลี่ยนแปลงตนเองให้มีความพร้อมในการทำงานองค์กรดิจิทัล แต่ในความสะดวกสบายทันสมัยย่อมมาพร้อมกับความเสี่ยง โดยเฉพาะ ฝ่ายความมั่นคงที่จะต้องทบทวนแนวทาง เรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ซึ่งในวิกฤติย่อมมีโอกาสเนื่องจากการเข้าถึงเครื่องมือ/อาวุธยุทโธปกรณ์เทคโนโลยี 5G นั้น เข้าถึงและเรียนรู้ได้ง่าย เพียงแต่ผู้นำองค์กรที่มีวิสัยทัศน์ในการดำเนินการปรับไปสู่องค์กรดิจิทัล (Digital Transformation) จะต้องวางแผนให้สอดคล้องกับการยุทธ์สงครามไซเบอร์ อีกทั้งย่อมต้องตระหนักว่า การพัฒนาบุคลากรจะต้องดำเนินการให้ควบคู่ (ควรจะก่อน) กันไป โดยคุณสมบัติพื้นฐานของนักรบไซเบอร์ที่ควรมี ประกอบด้วย ความสามารถในมาตรการเชิงรับ คือ การป้องกันการรั่วไหลของข้อมูลในระบบ และมาตรการเชิงรุก คือ ความสามารถในการหา/เจาะแหล่งข้อมูลของฝ่ายตรงข้าม

การพัฒนาเทคโนโลยีทางการทหารได้มีขึ้นอย่างต่อเนื่อง โดยระบบบัญชาการและควบคุม (C2) ได้พัฒนาเป็นระบบ C4ISR (Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance) ที่มีการครอบคลุม การปฏิบัติการข่าวสาร (IO), การสื่อสารทางยุทธศาสตร์ (Strategic Communication: SC), และการปฏิบัติการห้วงไซเบอร์ (Cyber Operation: CO) ซึ่งนับว่า เป็นโครงสร้างพื้นฐานที่สำคัญยิ่งในการดำเนินกลยุทธ์ของสงครามสมัยใหม่ และเป็นเป้าหมายคุ้มค่าที่มีความเสี่ยงสูงต่อการถูกโจมตีทางไซเบอร์ เนื่องจากการปฏิบัติงานจะผ่านระบบเครือข่ายศูนย์กลาง (Network Centric Operation: NCO) ที่เป็นการเชื่อมโยงของหน่วยกำลังต่าง ๆ เข้าด้วยกันด้วยการใช้ข้อมูลร่วมกัน เพื่อเพิ่มคุณภาพของข้อมูล (Fridman, 2018, p.77-80) และการแบ่งปันการระวังป้องกันสถานการณ์แบบครอบคลุม ดังนั้น ระบบ C4ISR จึงจัดว่าเป็นยุทโธปกรณ์ที่มีคุณลักษณะเด่นนอกเหนือจากการสั่งการ/ควบคุมกำลังพลผ่านการแสดงภาพเหตุการณ์แบบ Real-time แต่ยังสามารถนำข้อมูล (Data) จำนวนมากที่ได้ถูกเก็บไว้ในฐานข้อมูล (Cloud และ Big Data) ออกมาใช้ในการวิเคราะห์และจำลองสถานการณ์ล่วงหน้าก่อนเหตุการณ์เกิดขึ้นจริง การมีข้อมูลในปริมาณที่มากย่อมสร้างความได้เปรียบในการคำนวณวางแผนการยุทธ์ ดังนั้น ข้อมูล คือ ทรัพยากรที่สำคัญยิ่ง ที่จะต้องเก็บรักษาไว้เป็นความลับ โดยการได้มาของข้อมูลเหล่านี้ฝ่ายเราอาจได้มาจากการลาดตระเวนด้านการข่าว (ISR) ที่รวมถึงการโจรกรรม ซึ่งในขณะเดียวกันฝ่ายตรงข้ามย่อมต้องการเพื่อนำไปเตรียมการวางแผนการทำการโจมตีเช่นกัน ดังนั้น ความเสี่ยงด้านการรั่วไหล ของข้อมูลบนคลาวด์คอมพิวติงจึงอยู่ในระดับที่สูงตลอดเวลา ดังนั้นการพัฒนาและเสริมสร้างนักรบไซเบอร์จึงมีความจำเป็นอย่างยิ่ง

สรุป/ข้อเสนอ จากการศึกษาของ ของ Mazanec & Whyte (2019, p.80-96, 137) สงครามยุคที่ 5 การสร้างบุคลากร/นักรบไซเบอร์ที่เป็นทรัพยากรที่สำคัญยิ่ง โดยเฉพาะสำหรับงานด้านการข่าวที่จะต้องมีคุณลักษณะของสายลับในสงครามนอกแบบ ที่ฝังตัวอยู่บนแนวหรือพื้นที่ส่วนหลังของฝ่ายตรงข้ามซึ่งสอดคล้องกับหลักการการตั้งรับบนแนวหน้า “Defend Forward” เพื่อดำรงการเกาะติด การค้นหาการวางแผนและโจรกรรมข้อมูล ซึ่งนักรบพิเศษไซเบอร์ จึงจะต้องมีความชำนาญไม่เพียงแต่ด้านมาตรการเชิงรุกเท่านั้น แต่ยังต้องเพิ่มความชำนาญในด้านมาตรการเชิงรับอีกด้วย ซึ่งมาตรการต่อต้านข่าวกรองเชิงรับนี้ รวมถึงการรักษาความลับ (Confidentiality) ไว้เพื่อป้องกันระบบสารสนเทศทางคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ต่าง ๆ จากการเข้าถึงของฝ่ายตรงข้าม ซึ่งตัวอย่างเครื่องมือเพื่อป้องกันการถูก Hack การรั่วไหล คือ การใช้เทคนิคการรหัส (Cryptographic) สามารถถูกใช้ในการป้องกันข้อมูลระหว่างการส่งข้อมูลระหว่างระบบ ลดโอกาสความเป็นไปได้ในการลักลอบเปิดเผย และแก้ไขข้อมูลระหว่างการรับ-ส่ง ด้านมาตรการเชิงรับ และยังรวมถึงการลวงทางทหาร (Military Deception) โดยใช้เทคนิค Honeypot, กิจกรรมที่ส่งผลเสียหายต่อศัตรู และ/หรือระบบที่มีส่วนเกี่ยวข้องกับการกระทำที่เป็นภัยต่อฝ่ายเรา เช่น การเปลี่ยนเส้นทาง (Redirection), การระงับการปฏิบัติ (Deactivation) หรือการย้าย (Removal) โปรแกรมประสงค์ร้าย (Malware) สำหรับทางด้านมาตรการเชิงรุกควรจะต้องมีขีดความสามารถ 2 ลักษณะ คือ ข้อแรก การโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack: CNA) ที่เปรียบเสมือนการลาดตระเวนด้วยกำลังเพื่อให้ข้าศึกเปิดเผยที่ตั้ง โดยมีวัตถุประสงค์เพื่อที่จะรบกวน สกัดกั้น และทำลาย หรือลดกิจกรรมอันตรายต่าง ๆ ที่พยายามเจาะ หรือโจมตีผ่านห้วงไซเบอร์ และ ข้อสอง การเข้าถึงข้อมูลหรือการโจรกรรมข้อมูล (Computer Network Exploitation: CNE) ซึ่งสามารถดำเนินการผ่านระบบปฏิบัติการรวบรวมข่าวกรอง (Intelligence Surveillance Reconnaissance: ISR) และจะดำเนินการก่อนการโจมตี (Cohen & Schmidt, 2014, p. 7, 103)

บทสรุป: สงครามยุคที่ 5: การก่อการร้ายไซเบอร์

ในยุคศตวรรษที่ 21 สงครามตามแบบยังคงมีความสำคัญในการวางแผนการป้องกันประเทศ แต่การกำหนดกรอบการยุทธ์ในสงครามยุคที่ 5 ซึ่งเป็นยุคการเปลี่ยนฉับพลันทางดิจิทัล (Digital Disruption) โดยไม่เพียงแต่เทคโนโลยีดิจิทัลที่เข้ามามีบทบาทในการเป็นเครื่องมือสำคัญในการคุกคามกลุ่มเป้าหมายเท่านั้น แต่ยังเพิ่มความหลากหลายของรูปแบบการรุกรานและโจมตี การเตรียมการเพื่อป้องกันและรู้เท่าทันถึงการยุทธ์ จำเป็นจะต้องเพิ่ม/ยกระดับศักยภาพทางเทคโนโลยีสนามรบดั้งเดิมทั้ง 4 มิติ-พื้นดิน, ผืนฟ้า, ทะเล และอวกาศ ด้วยการเปลี่ยนแปลงทางด้านเทคโนโลยีที่เป็นไปอย่างก้าวกระโดดและต่อเนื่อง สนามรบจึงได้ถูกขยายพื้นที่ออกไปสู่สนามรบที่ 5 สงครามบนโลกไซเบอร์ฝ่ายความมั่นคงจึงจำเป็นที่จะต้องพิจารณาปรับปรุงการเตรียมแผนการให้เป็นพื้นที่ที่มีความสำคัญเท่าเทียมกับสนามรบ ทั้ง 4 มิติ และเตรียมความพร้อมที่จะนำไปสู่การทำสงครามแบบผสมผสาน (Hybrid Warfare) ซึ่งจะเป็นการรวมสรรพกำลังทั้งหมด ทั้งกองกำลังสงครามตามแบบและกองกำลังสงครามนอกแบบที่ต้องเป็นการเตรียมความพร้อมในการรับมือจากตัวแสดงทุกฝ่ายที่ล้วนมีขีดความสามารถในการใช้เทคโนโลยีในยุค 5G เพื่อการทำลาย ขัดขวางการโจรกรรมข้อมูล และประเด็นที่บทความนี้วิเคราะห์ว่ากำลังเป็นภัยคุกคามที่ต้องทำการรับมืออย่างเร่งด่วน คือ การก่อการร้ายไซเบอร์ เนื่องจากปัจจุบันนับว่าเป็นภัยที่ใกล้ตัวและชัดเจนที่สุดทั้งการใช้ (Cyber) Hard Power หรือการใช้กำลัง/อำนาจ เพื่อการโจมตีโครงสร้างพื้นฐาน

ที่สำคัญยิ่ง ซึ่งรวมถึงระบบ Command & Control ของกองทัพเป็นการผิดกฎหมายสากล นอกจากนั้นในช่วง 5 ปี ที่ผ่านมาข้อมูลที่สำคัญ (Data) ได้ถูกจัดเก็บไว้ในระบบ Cloud ขององค์กรซึ่งย่อมจะเป็นเป้าหมายต่อการถูกโจมตี ในการใช้ Soft Power หรือการสร้างความเชื่อ/โน้มน้าว ผ่านสื่อสังคมออนไลน์ ในการระดมสรรพกำลังบนโลกไซเบอร์ โดยภาพรวมการยุทธ์บนสมรภูมิสงครามยุคที่ 5 ฝ่ายความมั่นคงจะต้องเร่งเพิ่มปริมาณนักรบในสงครามไซเบอร์ที่มีขีดความสามารถในระดับสูงและมากเพียงพอ จากนั้นจึงพัฒนาขีดความสามารถเพื่อนำไปสู่การทำสงครามในลักษณะการตั้งรบบนแนวหน้า "Defend Forward" ในเขตยุทธบริเวณหน้าของเป้าหมาย/ข้าศึก ซึ่งเป็นการเตรียมความพร้อมเพื่อรับมือภัยคุกคามแห่งโลกยุคที่ 5 ต่อไป

เอกสารอ้างอิง

"พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562" (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา.* เล่ม 136 ตอนที่ 69 ก.

"พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562" (2562, 16 เมษายน). *ราชกิจจานุเบกษา.* เล่ม 136 ตอนที่ 50 ก.

สุรชาติ บำรุงสุข. (2016). *การก่อการร้ายในเมือง: Urban Terrorism.* กรุงเทพฯ: Square Print.

_____. (2017). *สงครามอสมมาตร แบบแผนความขัดแย้งใหม่: Asymmetric Warfare.* กรุงเทพฯ: Square Print.

_____. (2019). *โฉมหน้าใหม่ของสงคราม : The New Face of War.* กรุงเทพฯ: Square Print.

Borghard, E. (2020). *Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior.* Retrieved March, 20 2021 from https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-beharior

Cohen, J. & Schmidt, E. (2014). *The New Digital Age.* London: John Murray

Danahar, P. (2015). The New Middle East: *The World After the Arab Spring*. New York: Bloomsbury.

Fishcherkeller, M. & Harknett, R. (2017). *Deterrence is Not a Credible Strategy for Cyberspace*. Retrieved March, 15 2019 from doi:10.1016/j.orbis.2017.05.003

Fridman, O. (2018). *Russian Hybrid Warfare.* London: C. Hurst & Co

Hoffman, B. (2017). *Inside Terrorism.* New York: Columbia University Press

Martin, S. & Weinberg, L. (2017). *The Role of Terrorism in Twenty-First-Century Warfare*. Manchester University Press

Mazanec, B. & Whyte, C. (2019). *Understanding Cyber Warfare: Politics*. New York : Policy and Strategy, Routledge

Mearsheimer, J. J. (2014). *The Tragedy of Great Power Politics.* New York : W.W. Norton & Co.

Mockkaitis, T. R. (2008). *The "New" Terrorism: Myths and Relaity.* California : Stanford University Press.

Mousavian, S. H. & Shaahidsaless, S. (2014). *Iran and the United States.* New York : Bloomsbury.