

แนวโน้มเทคโนโลยีป้องกันประเทศปี 2020-2040

ธนรัฐ ธนะสมบูรณ์^{1*}

วันที่รับ 3 เมษายน 2563 วันที่แก้ไข 20 เมษายน 2563 วันที่ตอบรับ 21 เมษายน 2563

บทคัดย่อ

เทคโนโลยีป้องกันประเทศเป็นวิทยาการสาขาที่มีการวิจัยพัฒนาอย่างต่อเนื่องในฐานะขององค์ความรู้จำเป็นทางความมั่นคง และเครื่องมือทางยุทธศาสตร์ของทุกประเทศ รวมถึงเป็นอุตสาหกรรมที่มีมูลค่าสูงทั้งในเชิงเศรษฐกิจและการผลักดันนวัตกรรมใหม่ให้เกิดขึ้น และมีความแตกต่างจากอุตสาหกรรมภาคพลเรือนทั่วไปในเรื่องการเปิดเผยข้อมูลที่เป็นไปในวงจำกัด ยากต่อการเข้าถึงข้อมูลเนื่องจากชั้นความลับของแต่ละประเทศที่เป็นเจ้าของเทคโนโลยี ดังนั้นการศึกษาแนวโน้มเทคโนโลยีป้องกันประเทศระยะยาวในภาพรวมทั่วโลกจึงเป็นสิ่งจำเป็นในการทำความเข้าใจเจตนาของชาติที่มีศักยภาพสูงที่กำลังให้ความสนใจเทคโนโลยีประเภทใดเป็นหลัก ซึ่งจะส่งผลให้เข้าใจถึงแนวโน้มอุตสาหกรรมและยุทธวิธีการป้องกันประเทศที่จะเกิดขึ้นทั่วโลกต่อไป

โดยบทความนี้ได้ทำการศึกษารอบความน่าจะเป็นของเทคโนโลยีและอุตสาหกรรมป้องกันประเทศ 8 กลุ่มที่มีความโดดเด่น มีศักยภาพสูง และจะเปลี่ยนรูปแบบยุทธวิธีการรบในอนาคตทั่วโลกอย่างมีนัยยะสำคัญ อันจะเป็นประโยชน์ต่อการวางแผนกลยุทธ์การบริหารจัดการทรัพยากรในการวิจัยพัฒนา หรือส่งเสริมอุตสาหกรรมที่เกี่ยวข้องได้อย่างเหมาะสมต่อไป

คำสำคัญ : เทคโนโลยีทางทหาร, เทคโนโลยีป้องกันประเทศ, อุตสาหกรรมป้องกันประเทศ

¹ ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ

* ผู้แต่ง, อีเมล: thanarat.t@dti.or.th

Defence Technology Trend 2020-2040

Thanarat Thanasomboon ^{1*}

Received 3 April 2020, Revised 20 April 2020, Accepted 21 April 2020

Abstract

Defence technology is the academic field that needs continuous research and development for fundamental knowledge of strategic and national security in every country. Moreover, defence technology can push forward on high valuable industry in terms of both economic and innovation in a different approach from civilian industry because of information and knowledge restriction for each country. Therefore, studying the trend of this technology is required to understand the idea of high-caliber nations of what they plan to do in the near future all around the world.

This article attempts to give the understanding of 8 defence technology trends that stand out with high probability to have high-impact on the current defence technology and battlefield tactics in the near future. Hopefully, the discussions are beneficial to strategic management in the support of research and development policy.

Keyword : Military technology, defence Technology, defence Industry

¹ Defence Technology Analysis Department - TTA, Defence Technology Institute.

* Corresponding author, E-mail: thanarat.t@dti.or.th

1. บทนำ

ในปัจจุบัน (ค.ศ. 2020) เทคโนโลยีป้องกันประเทศมีการพัฒนาที่รวดเร็วอีกครั้ง จากการพัฒนาทางอุตสาหกรรมยุคใหม่ (Industry 4.0) รวมถึงการสิ้นสุดของยุคที่มีสหรัฐอเมริกาเป็นชาติมหาอำนาจหนึ่งเดียว จากการแผ่ขยายอิทธิพลของชาติมหาอำนาจระดับรอง เช่น รัสเซีย จีน และอินเดีย อีกทั้งนโยบายการแข่งขันอิทธิพลระดับชาติในยุคปัจจุบันได้มีการขยับจากการทำสงครามทางเศรษฐกิจ (Trade War) กลายเป็นการทำสงครามช่วงชิงเทคโนโลยี (Tech. War) รวมถึงเหตุการณ์อุบัติใหม่ เช่น โรคระบาดในปี 2020 (Covid-19) ซึ่งทำให้เกิดการเปลี่ยนแปลงในห่วงโซ่อุปทาน (Supply Chain) ในอุตสาหกรรมทุกรูปแบบ ส่งผลให้โลกมีการบีบให้เกิดการแข่งขันในด้านการวิจัยพัฒนาเทคโนโลยีที่เกี่ยวข้องกับความมั่นคงของชาติทุกด้านอย่างกว้างขวาง ทั้งในส่วนเทคโนโลยีที่เกี่ยวข้องโดยตรงกับยุทธโศปกรณ์และเทคโนโลยีสองทาง (Dual-Used)

เทคโนโลยีและอุตสาหกรรมป้องกันประเทศหากมีการเปรียบเทียบกับภาคพลเรือนแล้ว แม้ว่าจะมีความตั้งใจเหมือนกันในการยกระดับขีดความสามารถเดิมให้สูงขึ้นทั้งเชิงวิทยาการและเศรษฐกิจของแต่ละชาติ แต่มีจุดสำคัญที่แตกต่างคือเป็นส่วนงานที่ให้ความสำคัญเชิงความมั่นคงอย่างสูง เนื่องจากเป็นจุดสำคัญในเรื่องความเป็นความตายของประเทศจากการรบในสงครามทั้งตามรูปแบบปกติและสงครามนอกแบบ จนเกิดการพัฒนาให้เป็นอุตสาหกรรมป้องกันประเทศ (Defence Industry) หรืออุตสาหกรรมทางทหารขนาดใหญ่ (Military Complex) ที่มีความสัมพันธ์

อย่างเหนียวแน่นตลอดห่วงโซ่อุปทานที่ได้รับการคัดเลือกเป็นพิเศษจากความไว้วางใจระหว่างกัน อาทิ เครือข่ายอุตสาหกรรมทางทหารชาติตะวันตก กลุ่มพันธมิตร NATO หรือ อุตสาหกรรมพันธมิตร รัสเซีย-จีนแผ่นดินใหญ่ เป็นต้น ซึ่งการพัฒนาขีดความสามารถของแต่ละกลุ่มชั่วอานาจมักเป็นไปในลักษณะแสวงหาความเหนือกว่าทางเทคโนโลยี (Technology Superior) หรือต่อต้านเทคโนโลยี (Counter Technology) ต่อยุทธโศปกรณ์สำคัญของฝ่ายตรงข้าม เช่น การพัฒนาขีปนาวุธความเร็วสูงเพื่อต่อต้านเรือบรรทุกเครื่องบิน หรือ มัลแวร์โจมตีทางไซเบอร์ทำลายระบบสื่อสารของชาติ ศักยภาพสูงกว่าเพื่อชดเชยกำลังรบตามแบบ ซึ่งส่งผลให้ยุทธศาสตร์ ยุทธโศปกรณ์ และยุทธวิธีแบบเดิมถูกแก้ทางตอบโต้ไปมาอย่างไม่จบสิ้น โดยมีเทคโนโลยีอุบัติใหม่ (Emerging Technology) เป็นตัวแปรสำคัญ

บทความนี้ทางฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศได้จัดทำขึ้นเพื่อศึกษาถึงแนวโน้มของเทคโนโลยีป้องกันประเทศที่กำลังอยู่ในความสนใจของแวดวงอุตสาหกรรมทางความมั่นคงทั่วโลกว่ามีศักยภาพ มีความต้องการตลาดอย่างไร โดยสังเคราะห์จากบทวิเคราะห์หน่วยงานต่าง ๆ ผ่านเอกสารวิเคราะห์และการบรรยายในเวทีสัมมนา สรุปเป็น 8 แนวโน้มเทคโนโลยีป้องกันประเทศสำคัญในวงรอบ 20 ปีข้างหน้า ซึ่งประเทศไทยควรพิจารณาความเหมาะสมถึงการวิจัยและพัฒนาที่จะเกิดขึ้น เพื่อลดความเสี่ยงในการลงทุนที่ไม่คุ้มค่าจากการแข่งขันในตลาดหรือผลิตสินค้าที่ไม่เป็นที่ต้องการ (Out-Trend) ในอนาคต ขณะเดียวกันก็เป็นโอกาสที่จะแสวงหาความร่วมมือในการวิจัยพัฒนากับหน่วยงานอื่นเพื่อเติมเต็มเทคโนโลยีที่ยังมีช่องว่างในการเติบโตอีกด้วย

2. วิธีการศึกษา

เทคโนโลยีและอุตสาหกรรมป้องกันประเทศเป็นหนึ่งในสาขาวิชาการที่มีความเป็นพหุศาสตร์ อันมีความหลากหลายสูงต่างจากวิชาเฉพาะด้านทั่วไป เนื่องจากมีความสัมพันธ์กับหลายส่วนกิจกรรมทั้งเชิงสังคมศาสตร์ เศรษฐศาสตร์ วิศวกรรมศาสตร์ และความสัมพันธ์ระหว่างประเทศที่มีบทบาทในการกำหนดแนวทางป้องกันประเทศในด้านต่าง ๆ อยู่เสมอ โดยบทวิเคราะห์นี้ผู้เขียนได้วางแนวทางการศึกษาโดยมีเป้าหมายในการตอบคำถามหลัก 2 ประการ คือ (1) แนวโน้มและเทคโนโลยีที่จะมีบทบาทสำคัญในอนาคตคืออะไร และ (2) ช่วงระยะเวลาที่แนวโน้มและเทคโนโลยีสำคัญนั้นคือเมื่อไร ซึ่งเหล่านี้เป็นคำถามปลายเปิดและไม่มีการวัดเชิงตัวเลขอย่างแน่นอน เนื่องจากเทคโนโลยีและอุตสาหกรรมป้องกันประเทศมีหลายประเภทอย่างมากและบางกลุ่มไม่เกี่ยวเนื่องกันจนไม่อาจวัดมูลค่าเชิงตัวเลขเพื่อเปรียบเทียบได้ เช่น ไชเบอร์

เพื่อจะตอบคำถามข้างต้นดังกล่าว ผู้จัดทำบทความนี้จึงได้ทำการศึกษาถึงสถานภาพเทคโนโลยีและอุตสาหกรรมป้องกันประเทศในปัจจุบันของชาติที่มีขีดความสามารถสูงเป็นหลัก เนื่องจากมีบทบาทสำคัญในการผลักดันยุทธศาสตร์และยุทธวิธีการรบในสมรภูมิต่าง ๆ ผ่านการวิจัยพัฒนายุทธโปกรณ์และกลยุทธ์ยุคอนาคตมากกว่าประเทศขนาดเล็กที่เป็นผู้ใช้งานโดยส่วนมาก โดยผู้เขียนทำการศึกษาด้านความสัมพันธ์ระหว่างประเทศ ขีดความสามารถทางอุตสาหกรรมเทคโนโลยี ปัจจัยความน่าดึงดูดทางเศรษฐกิจ ตลอดจนสถานะการณ์อุบัติใหม่ที่ส่งผลกระทบ เช่น สงครามการค้า (Trade War) สงครามทาง

เทคโนโลยี (Tech. War) และปัจจัยภายนอกกิจการป้องกันประเทศแต่มีผลกระทบกว้างอย่างโรคระบาดอุบัติใหม่ (Covid-19) ที่ส่งผลกระทบต่ออุตสาหกรรมทุกประเทศ

ในการศึกษาผู้เขียนได้เริ่มต้นขั้นตอนแรกจากการค้นหาสถานะปัจจุบันด้านยุทธศาสตร์และยุทธวิธีการรบในปัจจุบัน (ก่อน ค.ศ. 2018) ผ่านหลักนิยมหลักในการรบและการจัดวางยุทธโปกรณ์สำคัญของชาติศักยภาพสูง ที่มีพื้นฐานตามการจัดกำลังตาม 3 เหล่าทัพ (บก-เรือ-อากาศ) เป็นหลัก ซึ่งประเภทอาวุธยุทธโปกรณ์ที่มีมูลค่าสูงมากในแต่ละเหล่าทัพได้แก่ ยานรบทางบก-เรือ-อากาศ (เช่น รถถัง เรือรบ เครื่องบินรบที่มีปริมาณมาก) อาวุธนิวเคลียร์ทางยุทธศาสตร์ ยานพาหนะคุณค่ายุทธการสูง (เช่น เรือบรรทุกเครื่องบิน เรือดำน้ำพลังงานนิวเคลียร์) และระบบยานไร้คนขับ (Unmanned Vehicle) เป็นจุดเริ่มต้นของการศึกษาในเอกสารฉบับนี้

หลังจากผู้เขียนกำหนดยุทธโปกรณ์เป้าหมายขั้นต้นได้ดังกล่าว จึงเริ่มขั้นตอนที่ 2 โดยการตั้งสมมุติฐานว่าภายใต้หลักการตอบโต้ทางเทคโนโลยีปัจจุบัน (Counter-Technology) ว่ายุทธโปกรณ์ที่จะเกิดขึ้นในอนาคตอันใกล้ (ภายใน 10 ปี) จะต้องมีนัยยะสำคัญในการเอาชนะหรือชิงความได้เปรียบจากอาวุธในปัจจุบันและเป็นไปได้ที่จะนำมาใช้งานจริง เนื่องจากต้องมีการวิจัยพัฒนาอย่างต่อเนื่องมาในระดับหนึ่งแล้ว อาทิเช่น อาวุธพลังงานจลน์ อาวุธหุ่นยนต์/ระบบอัตโนมัติ และอาวุธไชเบอร์ ซึ่งมีประสิทธิภาพสูงภายใต้ราคาจำกัด (Cost-Effective) ในการใช้รับมือกับยุทธโปกรณ์ยุคปัจจุบัน

ในขั้นตอนที่ 3 ของการศึกษาเป็นการพิจารณา

ถึงอนาคตในระยะยาว (ภายใน 20 ปี) โดยผู้เขียนได้ทำการใช้สมมุติฐานเดิม (Counter-Technology) ว่ายุทธโศปกรณ์ที่อุบัติใหม่ในช่วงเวลาดังกล่าวจะต้องมีขีดความสามารถในการเอาชนะหรือชิงความได้เปรียบจากอาวุธในอนาคตระยะสั้น (ภายใน 10 ปี) เช่นกัน และมีการศึกษาในระดับพื้นฐานขั้นต้นและมีความเป็นไปได้ในความพร้อมทางเทคโนโลยี (TRL: Technology Readiness Level) ในระดับ 3 แล้วเป็นอย่างน้อยในปี ค.ศ. 2020 ซึ่งทำให้ผู้เขียนพิจารณาเลือกระบบยุทธโศปกรณ์ใหม่อย่าง อาวุธพลังงาน ปฏิบัติการภาคอวกาศ และเทคโนโลยีการคำนวณทางควอนตัมเป็นตัวเลือกสำคัญในการศึกษา

ในขั้นตอนที่ 4 อันเป็นขั้นสุดท้าย ผู้ศึกษาได้ทำการประเมินองค์ประกอบโดยรอบที่จะมีผลกับการวิจัยพัฒนาอาวุธยุทธโศปกรณ์ทั้งในอนาคตระยะสั้นและระยะยาวพร้อมกัน โดยประเมินแนวโน้มสำคัญ 2 กลุ่มคือ เทคโนโลยีและเศรษฐกิจ ซึ่งเป็นปัจจัยหลักในหลักการป้องกันประเทศ โดยในส่วนเทคโนโลยีนั้นเล็งเห็นถึงการพัฒนาปัญญาประดิษฐ์ (AI) เป็นจุดสำคัญที่สุดในฐานะเทคโนโลยีที่เปลี่ยนโลก (Disruptive Tech.) ในทุกอุตสาหกรรมอันรวมถึงการพัฒนายุทธโศปกรณ์และยุทธวิธีการรบขั้นสูง ในขณะเดียวกันส่วนทางเศรษฐกิจนั้นการเปลี่ยนแปลงของห่วงโซ่อุปทานป้องกันประเทศ (Defence Supply Chain) เนื่องจากการแข่งขันกันของมหาอำนาจและการลดความเสี่ยงจากภัยพิบัติแบบต่าง ๆ เพื่อสร้างความมั่นคงจะส่งผลกระทบให้เกิดการโยกย้าย

ฐานการผลิตระหว่างประเทศจำนวนมาก และเกิดการสูญเสียในภาคอุตสาหกรรมเดิมพร้อมทั้งเกิดเครือข่ายอุตสาหกรรมป้องกันประเทศใหม่ในหลายพื้นที่ทั่วโลก

ทั้งนี้ เมื่อได้ศึกษาทั้ง 4 ขั้นตอนแล้ว ผู้เขียนจึงได้ทำการสรุปภาพรวมต่าง ๆ เพื่อให้เห็นแนวโน้มที่มีความเป็นไปได้สูงที่จะเกิดขึ้นภายในปี ค.ศ. 2040 โดยแยกออกตามระยะเวลาโดยสังเขป ซึ่งยังเป็นไปได้ที่แต่ละชาติอาจดำเนินการในเวลาที่แตกต่างกัน แต่ยังมีแนวโน้มในการวิจัยพัฒนาเพื่อให้สอดคล้องกับ 8 แนวโน้ม ดังผลการศึกษาในหัวข้อต่อไป

3. แนวโน้มเทคโนโลยีป้องกันประเทศ 8 ด้าน

ในระหว่างปี พ.ศ. 2563-2583 (ค.ศ. 2020-2040) เทคโนโลยีป้องกันประเทศมีการพัฒนาออกมาในหลายประเภทที่ต่างจากเดิม ซึ่งเน้นไปที่การจัดเทคโนโลยีตามพื้นที่ปฏิบัติการ (Operation Domain) เช่น ยุทธโศปกรณ์ภาคพื้นดิน-ทะเล-อากาศ (Air-Land-Sea) อาทิ รถถัง เรือรบ เครื่องบินรบ แต่ในอนาคตอันใกล้เทคโนโลยีทางทหารจะเริ่มถูกจัดกลุ่มใหม่ตามคุณลักษณะเฉพาะแทน เช่น กลุ่มสารสนเทศ กลุ่มวัสดุศาสตร์ โดยเทคโนโลยีเหล่านี้อาจถูกใช้งานได้ในหลายมิติ (Multiple Domain Tech.) [1] ซึ่งผู้วิเคราะห์ฯ ได้ประเมิน 8 กลุ่มเทคโนโลยีและอุตสาหกรรมป้องกันประเทศในระดับโลก (Global Scale) ภายใน 20 ปีข้างหน้า ได้ดังนี้

ปฏิบัติการ ไซเบอร์	หุ่นยนต์/ระบบอัตโนมัติ	ปัญญาประดิษฐ์ทาง ความมั่นคง	อาวุธพลังงาน
อาวุธพลังงาน จลนขั้นสูง	ห่วงโซ่อุปทาน ทางความมั่นคง	ปฏิบัติการภาค อวกาศ	การคำนวณทาง ควอนตัม

ทั้งนี้ สามารถสังเกตได้ว่า เทคโนโลยีที่ได้รับความนิยมสูงบางประการยังไม่ถูกจัดอยู่ในลำดับกระแสช่วงต้น เนื่องจากการวิจัยพัฒนาไปมากจนอยู่ในระดับที่เสถียรและมีความพร้อมในอุตสาหกรรมแล้ว เช่น อากาศยาน ยานยนต์ทางทหาร หรือ เป็นเทคโนโลยีที่เติบโตในภาคอุตสาหกรรมพลเรือนมากกว่า เช่น การผลิตทางเลือกด้วยอุปกรณ์ 3 มิติ (3-D Printing Manufacturing) หรือเป็นเทคโนโลยีที่ทำนายสูงจนยังมีความไม่แน่นอนว่าจะเข้าสู่อุตสาหกรรมป้องกันประเทศในรูปแบบใด เช่น เทคโนโลยีพันธุวิศวกรรมทางทหาร (Military Genetic Engineering) ที่ยังขาดความชัดเจนด้านหลักเกณฑ์ทางจริยธรรมในการวิจัยเป็นต้น

จากตารางข้างต้น 8 แนวโน้มเทคโนโลยีป้องกันประเทศดังกล่าวมีระยะเวลาในการวิจัยพัฒนาจนถึงขั้นที่ใช้งานได้ ในอุตสาหกรรมที่แตกต่างกันออกไป โดยผู้วิเคราะห์ได้จัดเกณฑ์พิจารณาออกเป็น 2 ส่วนหลัก มีคะแนนแต่ละหัวข้อตั้งแต่ 1 -5 คือ ความน่าจะเป็น (Likelihood: พิจารณาจากระยะเวลาเข้าสู่ตลาด) และระดับผลกระทบ (Impact: พิจารณาจากผลกระทบในการใช้ปฏิบัติการทางยุทธวิธี/ยุทธศาสตร์) ในการนำเทคโนโลยีเหล่านี้เข้าสู่กิจการป้องกันประเทศ ซึ่งเป็นไปตามหลักการบริหารความเสี่ยงและโอกาส โดยมีรายละเอียดดังหัวข้อถัดไปนี้

4. ปฏิบัติการทางไซเบอร์ (Cyber Operation)

ผลกระทบ สูงมาก (4) ความน่าจะเป็น สูงสุด (5)

เทคโนโลยีดิจิทัลเป็นส่วนสำคัญของระบบอาวุธทางทหารยุคปัจจุบันเพิ่มขึ้นในแทบทุกส่วน ในขณะที่เดียวกันทำให้ช่องโหว่ (Vulnerability) ที่เป็นไปได้มีสูงขึ้นตามไปด้วย ซึ่งเป็นสถานการณ์ที่เกิดขึ้นทั้งในภาคกองทัพและพลเรือน [2] ที่โครงสร้างสารสนเทศขนาดใหญ่ มีความจำเป็น และคุณค่าทางยุทธการสูง

จะตกเป็นเป้าโจมตีได้ง่ายจากทั้งฝ่ายตรงข้ามและมือที่สาม ซึ่งทำให้ Cyber เกิดเป็นยุทธภูมิใหม่ที่แทบมองไม่เห็นในทางกายภาพ ซึ่งโดยปกติจะสามารถแบ่งปฏิบัติการทางไซเบอร์ได้ 3 รูปแบบหลัก คือ การโจมตี (Offense) การปกป้อง (Defence) และการฟื้นฟู (Recovery) ซึ่งมีความแตกต่างจากปฏิบัติการทางทหารทั่วไปเป็นอย่างมาก เนื่องจากการโจมตีทางไซเบอร์ไม่มีการแบ่งแยกพื้นที่เขตหน้า-หลังอย่างชัดเจน ทำให้การวางกำลังทางกายภาพเพื่อตรวจการณ์หรือป้องกันแทบไม่สามารถทำได้เลย และในขณะเดียวกันหากได้รับเสรีในการปฏิบัติการหน่วยรบทางไซเบอร์ก็สามารถบุกรุกโจมตีฝ่ายตรงข้ามให้เสียหายได้โดยการปกปิดตัวเอง

ปัจจุบันสภาวะสงครามไซเบERNั้นถือได้ว่าเกิดขึ้นไปแล้ว เนื่องจากคุณสมบัติพิเศษคือการปิดบังตนเองของผู้โจมตี และสามารถปฏิเสธความรับผิดชอบได้ง่าย ทำให้อาวุธไซเบอร์ถูกใช้เป็นเครื่องมือหลักของรัฐบาลในการบ่อนทำลายหรือแทรกแซงกิจกรรมของเป้าหมายโดยไม่เกิดผลกระทบทางกฎหมายระหว่างประเทศได้อย่างมีประสิทธิภาพ เช่น การทำลายเตาปฏิกรณ์นิวเคลียร์ของอิหร่าน การโจมตีสาธารณูปโภคของเวเนซุเอลา หรือการรบกวนการสื่อสารของเอสโตเนีย เป็นต้น ซึ่งอาวุธทางไซเบอร์เหล่านี้เป็นสิ่งที่ถูกผลิตและสร้างขึ้นมาในฐานะยุทธโธปกรณ์แบบหนึ่ง เช่น มัลแวร์ ซึ่งถูกเรียกกันว่าเป็นระเบิดตรรกะ (Logic Bomb) ที่ผู้โจมตีจะหาวิธีติดตั้งไปยังเป้าหมายล่วงหน้าก่อนและแอบแฝงตัวรอคำสั่งให้ทำงานยามที่ต้องการ และในขณะเดียวกันเทคโนโลยีเกิดใหม่ เช่น สายโซ่สารสนเทศ (Blockchain) สามารถเป็นอาวุธไซเบอร์เชิงรับที่สามารถประยุกต์ใช้ในทางทหารได้อย่างมากเช่นกัน ด้วยสถาปัตยกรรมเป็นแบบไร้ศูนย์กลางทำให้ยากต่อการโจมตี

ทั้งนี้ การใช้งานอาวุธไซเบอร์เชิงรุก มีข้อพิจารณา

สำคัญอยู่หลายประการ คือ 1) การรักษาความลับในการใช้ 2) การใช้งานครั้งเดียว (One-time Used) และ 3) อาวุธขั้นสูงไม่มีจำหน่าย เพราะเมื่อถูกเปิดเผยหรือเริ่มมีการใช้งานเมื่อไร เป้าหมายจะทำการพัฒนาการป้องกันและปิดกั้นช่องโหว่ได้อย่างรวดเร็ว (Patching) ทำให้ประสิทธิภาพในการใช้งานครั้งต่อไปลดลงอย่างมาก ทำให้ไม่มีประเทศใดจำหน่ายขีดความสามารถไซเบอร์เชิงรุกขั้นสูงแก่ประเทศอื่น

ในทางกลับกันขีดความสามารถในการป้องกันภัยคุกคามไซเบอร์อย่างเปิดเผยจะมีผู้ให้บริการเป็น

จำนวนมากทั้งภาครัฐและเอกชน แต่อย่างไรก็ดีด้วยการที่เทคโนโลยีสารสนเทศมีการพัฒนารวดเร็วมาก การสร้างขีดความสามารถทางไซเบอร์โดยแท้จริงจะอยู่ที่การสร้างทีมงานบุคลากรที่เชี่ยวชาญ แล้วนำทักษะเหล่านั้นมาออกแบบอาวุธหรือระบบป้องกันไซเบอร์ในอนาคตมากกว่าจะเป็นการจัดซื้ออุปกรณ์ (Hardware/Software) มาใช้เป็นครั้งคราว ซึ่งจะล้าสมัยในเวลาไม่นานหลังจากการเปิดเผยตัวหรือระบบไซเบอร์ของเป้าหมายได้รับการปรับปรุง (Update) ต่างจากยุทธโศปกรณ์หลักทั่วไปที่มีอายุนานตราบเท่าที่ยังได้รับการซ่อมบำรุง โดยสามารถวิเคราะห์ช่วงเวลาโดยสังเขปของเทคโนโลยีดังนี้

เวลา (ค.ศ.)	เทคโนโลยีสำคัญ	ยุทธวิธี/รูปแบบการใช้งาน
2020 - 2029	• Advance Persistent Threat (APT) • Defence Blockchain • Cyber Automation Analytic • Mobile and Cloud Security • การโจมตีผ่านพฤติกรรมผู้ใช้ (Social Engineering) และจิตวิทยา	• การฟื้นฟูไซเบอร์แบบรวดเร็ว (R3: Rapid Recovery Repair) • ระบบไซเบอร์อัตโนมัติ (Cyber-bot) • การโจมตีและปกป้องอุปกรณ์ IoT ทางทหาร เช่น Sensor หรือ Data-link • โจมตีข้อมูลของบุคลากรความมั่นคง
2030 - 2039	• บุคลากรภัยคุกคามขั้นสูง (APT) กับ ปัญญาประดิษฐ์ (AI) • มาตรฐานการทวนสอบสารสนเทศแบบใหม่ เพื่อค้นหาช่องโหว่ต้นกำเนิด (Backdoors) • Botnet ขนาดใหญ่ในโครงข่าย 5G และ IoT	• มัลแวร์ที่สามารถเรียนรู้สภาพไซเบอร์เป้าหมายและพัฒนาตัวเองได้อิสระ หรือ การบิดเบือนข้อมูล (Data Manipulation) เพื่อโจมตีเป้าหมาย • มาตรการพิสูจน์ทราบความปลอดภัยทางสารสนเทศของอุปกรณ์ไซเบอร์

ภาพรวมในอนาคตอันใกล้ของเทคโนโลยีด้านปฏิบัติการทางไซเบอร์ ตั้งแต่ระยะ 0-20 ปีข้างหน้าสามารถคาดหมายได้ว่าจะมีการใช้งานต่อเนื่อง และทวีความซับซ้อนตามแนวโน้มของเป้าหมาย

ทั้งทางทหารและพลเรือนที่มีความเป็นสารสนเทศและมีคุณลักษณะอัจฉริยะ (Smart) มากขึ้น ทำให้ช่องโหว่ (Vulnerability) ในระบบงานมีโอกาสดูกโจมตีมากขึ้นไปด้วย อีกทั้งการเข้ามาของเทคโนโลยี

แวดล้อม เช่น ปัญญาประดิษฐ์ (AI) หุ่นยนต์และระบบอัตโนมัติต่าง ๆ ตลอดเวลาทั้งในยุทธวิธีการโจมตีและป้องกัน พร้อมทั้งรักษาขีดความสามารถในการฟื้นฟูทางไซเบอร์ (Cyber Resilience) อย่างต่อเนื่อง

5. อาวุธพลังงานจลน์ขั้นสูง (Advance Kinetic Weapons)

ผลกระทบ ปกติ (2) ความน่าจะเป็น สูง (3)

ในช่วง ค.ศ. 1990-2015 อาวุธในรูปแบบจรวดอาวุธปล่อยนำวิถี หรือขีปนาวุธ ถือเป็นอาวุธทางกายภาพ (Kinetic Weapon) ที่ได้รับความนิยมในตลาดยุทธโศปกรณ์อย่างมากตั้งแต่ระดับพื้นฐาน คือ จรวดไม่นำวิถี (Unguided Rocket) จนถึงอาวุธที่มีความแม่นยำสูง (Precision Weapon) มีขีดประเภทหลากหลาย ระยะยิงไกล และติดตั้งอุปกรณ์ (Payload) ได้หลากหลายกว่าอาวุธประเภทปืนใหญ่หรือระเบิดทั่วไป จึงถือเป็นอาวุธโจมตีที่มีประสิทธิภาพสูง อาทิ ขีปนาวุธระยะกลาง-ไกล ที่ยิงขึ้นสู่ชั้นบรรยากาศบนก่อนจะโคจรถูกปล่อยเข้าโจมตีเป้าหมายด้วยความเร็วสูง หรืออาวุธปล่อยนำวิถีอัจฉริยะ (Smart) ทว่าในปัจจุบันเทคโนโลยีในการป้องกันมีการพัฒนาอย่างรวดเร็ว และมีการจัดวางเครือข่ายตั้งรับหลายชั้น (Multi-Layer Defense) เช่น โครงการโล่ขีปนาวุธ (Missile Shield) ของสหรัฐอเมริกาที่ใช้ป้องกันพื้นที่ขนาดใหญ่หรือระบบสกัดกั้นทางอากาศความแม่นยำสูงเฉพาะพื้นที่ [3] เช่น Iron Dome ของอิสราเอล จนยากที่อาวุธจรวดในรูปแบบเดิมจะรักษาอัตราความสำเร็จในการเจาะทะลวงแนวรับของเป้าหมายสำคัญได้เช่นเดิม

ตั้งแต่ช่วงปี ค.ศ. 2010 จนถึงปัจจุบัน เพื่อต่อต้านแผ่ขยายอิทธิพลของ NATO ผ่านเครือข่ายป้องกันภัยทางอากาศเพื่อปิดล้อมรัสเซียและจีนแผ่นดินใหญ่ จึงได้เริ่มการวิจัยพัฒนาอาวุธแบบใหม่ที่มีขีด

ความสามารถในการโจมตีระยะไกลและความเร็วสูงอย่างยิ่ง ซึ่งถูกจัดเป็นกลุ่มอาวุธความเร็วเหนือเสียง (Hypersonic Weapon) และปรับปรุงเป็นพาหนะร่อนความเร็วเหนือเสียง (Hypersonic Glide Vehicle: HGV) ที่เป็นอาวุธโคจรในเขตคาบสมุทรเพื่อหลบเลี่ยงเครือข่ายตรวจการณ์ พร้อมทั้งยังรักษาความเร็วสูงถึง 5 เท่าของความเร็วเสียง (หรือมากกว่า) ได้เกือบตลอดเวลาโคจร จนทำให้ฝ่ายตั้งรับมีเวลาตอบสนองน้อยมาก อีกทั้งยังคาดการณ์ทิศทางการโจมตีได้ยาก เพราะสามารถเคลื่อนที่ทางยุทธวิธีได้อย่างคล่องตัว คล้ายกับการใช้อากาศยานโจมตี ซึ่งขีดความสามารถด้านนี้มีประเทศรัสเซียและจีนเป็นผู้นำ เช่น ขีปนาวุธ Zircon และ DF-17 รวมถึงอาวุธคุณลักษณะพิเศษ เช่น ตอร์ปิโด Poseidon (รัสเซีย) ที่ขับเคลื่อนด้วยพลังงานนิวเคลียร์จนสามารถมีระยะยิงไม่จำกัดได้ เป็นต้น

ในขณะเดียวกันกลุ่มประเทศตะวันตก ก็ได้เริ่มมีการวิจัยพัฒนาอาวุธพลังงานจลน์ขั้นสูงเช่นกัน [3] เพื่อเป็นการตอบโต้ระบบป้องกันภัยทางอากาศชั้นสูงของรัสเซีย เช่น อาวุธปล่อยนำวิถีต่อสู้อากาศยานก้ำวหน้า S-400 ที่มีขีดความสามารถในการต่อตีเครื่องบินความเร็วสูง ตรวจจับได้ยาก (Anti-Stealth) ซึ่งกลุ่มประเทศตะวันตกได้มีการพัฒนาที่หลากหลายกว่า เช่น สหรัฐอเมริกาพัฒนาทั้ง HGV ความเร็วสูง รวมถึงอาวุธปืนใหญ่แม่เหล็กไฟฟ้า (Railgun) ที่มีระยะยิงไกลมากโดยใช้กระสุนราคาประหยัด ส่วนสหภาพยุโรปมีการพัฒนาอาวุธพลังงานจลน์ประเภทตรวจจับได้ยากอย่างยิ่ง (Extreme Stealth) รวมถึงประเทศมหาอำนาจระดับรอง เช่น ญี่ปุ่น และอินเดีย ก็มีแผนการพัฒนาเช่นเดียวกัน โดยสามารถคาดการณ์ว่าอาวุธพลังงานจลน์ขั้นสูงก้ำวหน้า (ประเภท HGV) จะเริ่มถูกใช้งานอย่างเป็นทางการภายใน 2023 เป็นต้นไป โดยสามารถวิเคราะห์ช่วงเวลาโดยสังเขปของเทคโนโลยีดังนี้

เวลา (ค.ศ.)	เทคโนโลยีสำคัญ	ยุทธวิธี/รูปแบบการใช้งาน
2020 - 2029	• อวูร่อนนำวิถีความเร็วสูงมาก (Hypersonic Glide Vehicle) • เครื่องยนต์ผสมผสาน (Hybrid Engine) และระบบพลังงานก้าวหน้า (Advance Power) • การบูรณาการสื่อสารและชี้เป้าระยะไกล	• พลังงานขับเคลื่อนหลายแบบ เพื่อความคล่องตัวในปฏิบัติการ • โจมตีเป้าหมายคุณค่ายุทธการสูง (HVT) ที่มีการคุ้มกันแน่นหนา
2030 - 2039	• อวูรปืนแม่เหล็กไฟฟ้า (Railgun) • เต้าปฏิกรณ์นิวเคลียร์ขนาดเล็ก • ตรวจจับได้ยากขึ้นสูง (Extreme Stealth)	• การโจมตีเป้าหมายคุณค่ายุทธการสูงจากระยะไกลมากหรือระยะอนันต์ • ป้องปรามโดยการปฏิเสธเสรีปฏิบัติการของฝ่ายตรงข้าม (A2D)

ภาพรวมของเทคโนโลยีอาวุธพลังงานจลน์ขั้นสูงในอนาคตนั้นคาดว่าจะได้เห็นการประจำการอย่างเป็นรูปธรรมภายใน 5-10 ปีข้างหน้า โดยส่วนใหญ่จะถูกใช้ในฐานะยุทธโศปกรณ์ป้องปรามเชิงยุทธศาสตร์ (Strategic Deterrence) โดยประเทศที่มีศักยภาพสูง เพื่อใช้ในการกดดันฝ่ายตรงข้ามในฐานะอาวุธที่ไม่อาจสกัดกั้นได้โดยง่ายเพื่อใช้ในการทำลายเป้าหมายคุณค่าสูงมาก เช่น กองเรือบรรทุกเครื่องบิน หรือกองบัญชาการ

6. อาวุธพลังงาน (Direct Energy Weapon)

ผลกระทบ สูง (4) ความน่าจะเป็น สูง (3)

อาวุธพลังงานเป็นหนึ่งในกระแสเทคโนโลยีใหม่ทางยุทธโศปกรณ์ที่เติบโตขึ้นพร้อมกับการพัฒนาแหล่งพลังงานคุณภาพสูงขึ้นกว่าในอดีต รวมทั้งตอบสนองทางยุทธวิธีการใช้อาวุธแบบใหม่ที่มีจุดเด่นในเรื่องค่าใช้จ่ายในการปฏิบัติการที่ต่ำมาก

(Low running-cost) และเวลาเข้าถึงเป้าหมายเป็นศูนย์ (Zero leading time) ซึ่งทำให้อาวุธพลังงานกลายเป็นทางเลือกที่มีประสิทธิภาพมากขึ้นในการใช้ตอบโต้เป้าหมายที่มีความเร็ว ความคล่องตัวสูงปริมาณมาก และควบคุมการยิงได้อย่างแม่นยำ โดยประกอบด้วยอาวุธพลังงาน 5 ประเภทหลัก [3] คือ อาวุธคลื่นไมโครเวฟ อาวุธคลื่นเสียง (Sonic) อาวุธเลเซอร์ (Laser) อาวุธลำแสงอนุภาค (Particle Beam) และอาวุธพลาสมา (Plasma) ซึ่งมีจุดเด่นการใช้งานแตกต่างกันไป

ปัจจุบันเทคโนโลยีทางการทหารได้เริ่มมีการวิจัยและพัฒนาอาวุธพลังงานอย่างเต็มรูปแบบ ซึ่งมีอาวุธเลเซอร์เป็นพื้นฐาน (Laser Based) ที่ได้รับความนิยมสูงสุด เพราะมีต้นทุนในการใช้งานน้อยและประยุกต์ได้หลากหลาย โดยในปี 2019 มีการพัฒนาระบบอาวุธต้นแบบขึ้นมาเป็นจำนวนมาก นำโดยประเทศสหรัฐอเมริกาและจีน โดยมีตัวอย่างเช่น

ระบบอัตโนมัติบนยานรบ 8x8 ซึ่งมีขีดความสามารถในการโจมตีด้วยพลังงาน 50 เมกะวัตต์ สู่เป้าหมายที่ระยะ 3-5 กม. ต่อเนื่อง 5-10 เป้าหมาย ซึ่งเหมาะสมอย่างมากในการใช้ต่อต้านระบบอาวุธขนาดเล็กราคาประหยัดที่เข้าระดมโจมตีด้วยยุทธวิธีฝูงบินขนาดใหญ่ (Swarm Attack) เนื่องจากมีค่าใช้จ่ายต่ำกว่าการใช้อาวุธปล่อยนำวิถีที่มีราคาแพง และแม่นยำกว่าปืนต่อสู้อากาศยาน และเนื่องจากมีความเร็วสูงกว่ากระสุนปืนปกติอย่างมากทำให้ระบบควบคุมการยิงลดภาระในการคำนวณวิถีกระสุนต่อเป้าหมาย ซึ่งจะเป็นมาตรการป้องกันตัวเองที่ลดทอนขีดความสามารถของอาวุธปล่อยนำวิถีหรือขีปนาวุธในปัจจุบันลงอย่างมีนัยยะสำคัญเพราะต้องสิ้นเปลืองอาวุธจำนวนมากในการโจมตี

อย่างไรก็ตาม เทคโนโลยีด้านอาวุธพลังงานนั้นยังจัดอยู่ในระดับต้นแบบการผลิต (Testing Prototype) ในช่วงปี 2020 ซึ่งยังต้องมีการปรับปรุงในอนาคตอีกหลายประการ เช่น ระบบควบคุมการยิงแบบใหม่ เช่น เซอร์การตรวจการณ์ ระบบพลังงาน (แบตเตอรี่) และชุดอุปกรณ์หล่อเย็นระบบที่จำเป็นต้องมีการศึกษาวิจัยต่อไปก่อนจะนำเข้าสู่กระบวนการผลิตกันทั้งทางอุตสาหกรรม ซึ่งคาดว่าจะเริ่มเป็นรูปธรรมภายในปี 2025 จึงจะเริ่มถูกใช้งานอย่างจริงจัง โดยสามารถประเมินเบื้องต้นได้ดังต่อไปนี้

เวลา (ค.ศ.)	เทคโนโลยีสำคัญ	ยุทธวิธี/รูปแบบการใช้งาน
2020 - 2029	• แบตเตอรี่ Li-Ion ขั้นก้าวหน้า • การบูรณาการ Sensor ตรวจการณ์กับระบบควบคุมการยิง (FCS) สำหรับอาวุธพลังงาน • เลเซอร์ปฏิกิริยาเคมี • เรดาร์ขั้นก้าวหน้า (Advance AESA)	• เลเซอร์สกัดกันเป้าหมายขนาดเล็ก เช่น UAV จรวดขนาดเล็ก • ใช้คลื่นวิทยุเพื่อสงครามอิเล็กทรอนิกส์ (EW) • อาวุธป้องกันทางจิตวิทยา เช่น การแจ้งเตือนฝ่ายตรงข้ามที่ลวงล้าพื้นที่
2030 - 2039	• แบตเตอรี่กราฟีนและ Supercapacitor • เลเซอร์กำลังสูง (High-Powered Laser) • ระบบ Pulsed Energy/Plasma	• การป้องกันทางใต้ทะเล/น่านฟ้า • สกัดกันเป้าหมายแบบต่อเนื่อง (Anti-Swarm)

ภาพรวมของอาวุธพลังงานในอนาคตอันใกล้ นั้นจะพบว่ามีความสัมพันธ์กับการพัฒนาแหล่งพลังงานใหม่ อาทิเช่น ตัวเก็บประจุประสิทธิภาพสูง (Supercapacitor) แบตเตอรี่แบบใหม่ เช่น กราฟีน แบตเตอรี่ ที่สามารถสะสมพลังงานได้จำนวนมาก และคลายพลังงานให้ไหลออกเลเซอร์ได้รวดเร็วพอ โดยบูรณาการเข้ากับเซ็นเซอร์ ระบบควบคุมการยิงในปัจจุบัน พร้อมทั้งการศึกษาเครื่องมือที่ตอบสนอง

ตัวแปรใหม่ ๆ ในการปฏิบัติการ เช่น อัลกอริทึมคำนวณสภาพแปรปรวนทางอากาศเทียบกับพลังงานเป็นต้น ซึ่งข้อจำกัดเหล่านี้สามารถอนุมานได้ว่าอาวุธพลังงานที่จะเกิดขึ้นในอนาคตอันใกล้ยังจำเป็นต้องอยู่บนฐานปฏิบัติการ (Platform Based) ขนาดใหญ่ เช่น ยานเกราะ เรือรบ หรือเครื่องบินที่ได้รับการดัดแปลงพิเศษ เป็นต้น

7. ปัญญาประดิษฐ์ทางความมั่นคง (AI in Defence)

ผลกระทบ สูงสุด (5) ความน่าจะเป็น สูง (3)

การศึกษาเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ถูกพัฒนาอย่างจริงจังพร้อมกันในทุกภาคส่วนความมั่นคงทางทหารและความต้องการภาคพลเรือน ในฐานะหัวหอกเทคโนโลยีที่ปฏิวัติอุตสาหกรรมทุกภาคส่วนในยุค 4.0 ที่มีการใช้งานฐานข้อมูลขนาดใหญ่ (Big Data) และการเชื่อมโยงอุปกรณ์ (IoT) จำนวนมหาศาล ที่ไม่สามารถใช้บุคลากรที่เป็นมนุษย์ในการพิจารณาเป็นรายกรณีได้เพียงพอและทันสถานการณ์อีกต่อไป ดังนั้น AI ที่มีขีดความสามารถในการวิเคราะห์ ตัดสินใจ จึงกลายเป็นสิ่งที่จำเป็นทั้งในการบริหารจัดการระบบภาคพลเรือนและยุทธโศปกรณ์ทางทหารที่มีการบูรณาการเป็นโครงข่าย (Network Centric) อย่างยิ่ง

ในส่วน AI ที่เกี่ยวข้องกับทางทหารโดยตรง จะถูกใช้ในกองทัพยุคใหม่ทุกมิติ ทั้งส่วนสนับสนุนการรบ เช่น การบริหารจัดการสายส่งกำลังบำรุงอัตโนมัติ (Autonomous Logistic) อาทิ การวางแผนเส้นทาง ลำดับ สำหรับการเติมเสบียงให้ยานพาหนะ การจัดช่องทางสัญญาณสื่อสาร รวมไปถึงการใช้งานในปฏิบัติการรบโดยตรง อย่างเช่นระบบปฏิบัติการสนับสนุนการรบที่ตัดสินใจแยกแยะเป้าหมาย วิเคราะห์สถานะเป้าหมายเท็จ/จริง รวมถึงการตัดสินใจรบปะทะด้วยความเร็วสูงมากเกินกว่าเจ้าหน้าที่จะสามารถตอบสนองทัน อาทิ การวางแผนสกัดกั้นขีปนาวุธและ Drone ของข้าศึกจำนวนมากที่กำลังเข้าโจมตี หรือการบินผาดแผลงเพื่อหลบหลีกอาวุธนำวิถีหลายทิศทางขณะที่เข้าต่อสู้เป้าหมายถนัดไปอย่างมีประสิทธิภาพมากที่สุด

กรณีศึกษาการใช้งาน AI เพื่อการรบเต็มรูปแบบในอนาคตอย่างจริงจัง จะส่งผลให้บุคลากรที่เป็นมนุษย์จะถูกเปลี่ยนสถานะจากผู้ปฏิบัติการ (Operator) เป็นผู้บริหารจัดการ (Manager) เนื่องจากในสถานการณ์ที่กดดันคับขัน การเฝ้าระวังต่อเนื่องเป็นระยะเวลานานมาก รวมถึงมีข้อมูลจำนวนมากโหมเข้าใส่ (Information Overload) เป็นไปได้ยากที่กำลังพลจะสามารถตัดสินใจได้อย่างรวดเร็วและถูกต้องตลอดเวลา แม้จะได้รับการฝึกมาเป็นอย่างดีแค่ไหนก็ตาม ยกตัวอย่างเช่น AI สำหรับควบคุมอากาศยานไร้คนขับในการกิจรบทางอากาศ (Fighter UAV) ที่ช่วยให้ยุทธโศปกรณ์ไม่ถูกจำกัดโดยสมรรถนะของนักบิน และสามารถตัดสินใจในยุทธวิธีการรบ (Tactical Decision) ได้เองโดยไม่ต้องพึ่งพาสัญญาณควบคุมภายนอก (Non-remote) ทำให้มีขีดความสามารถในการรบสูงขึ้นอย่างมาก ทั้งในการรบนอกระยะสายตา (BVR) และรบพัวพันระยะประชิด (Dogfight) เพราะสามารถมองเห็นทุกเป้าหมายที่เซ็นเซอร์ตรวจการณ์ได้โดยไม่พึ่งมนุษย์และตัดสินใจแบบอัตโนมัติในการต่อสู้เป้าหมายทำให้ลดระยะเวลาการตอบสนองได้เป็นอย่างมากอันนำมาซึ่งความได้เปรียบในการดำเนินกลยุทธ์ [4] สามารถวิเคราะห์ช่วงเวลาโดยสังเขปของเทคโนโลยี ดังนี้

เวลา (ค.ศ.)	เทคโนโลยีสำคัญ	ยุทธวิธี/รูปแบบการใช้งาน
2020 - 2029	- Machine/Deep Learning - Natural Language Processing (NLP) - Big Data, Cloud Computing - Human-Machine Interface	- ระบุอัตลักษณ์/คุณสมบัติของมนุษย์และวัตถุเป้าหมายผ่านยุทธโธปกรณ์ - การตอบสนองต่อภาษาธรรมชาติ - การบริหารทรัพยากรและกำลังรบ
2030 - 2039	- Quantum Computing - การตัดสินใจในการรบ (Combat Decision) - อาวุธ/อุปกรณ์อัจฉริยะ (AI-Embedded)	- สมองกลที่ควบคุมหุ่นยนต์ในการรบโดยเป็นอิสระจากมนุษย์ภายใต้เงื่อนไข - AI ฝังตัวเพื่อสนับสนุนมนุษย์ (Buddy)

ปัจจุบัน (ค.ศ. 2020) นั้น AI มีการใช้อยู่ในระดับหนึ่งแล้วในฐานะระบบสนับสนุนการรบและประเมินสถานการณ์ต่าง ๆ แต่จะมีผลมากขึ้นอย่างมีนัยยะสำคัญในอีก 10 ปีข้างหน้า สอดคล้องกับการเข้ามาของหุ่นยนต์และระบบอัตโนมัติต่าง ๆ ที่มีปัญญาประดิษฐ์คอยเสริมให้ยุทธโธปกรณ์มีความฉลาดขึ้นอย่างแท้จริง และใช้เพื่อประกอบการรบทางยุทธวิธีเพื่อคงความเหนือกว่าในการตัดสินใจในสมรภูมิ โดยปัจจัยสำคัญว่า AI จะมีบทบาทขนาดไหนในการรบคือการกำหนดมาตรฐานทางจริยธรรม (Ethical-AI) ถึงระดับที่จะให้ AI ทำงานหรือตัดสินใจแทนผู้ปฏิบัติการที่เป็นมนุษย์ เช่น สิทธิในการสั่งยิงสังหารเป้าหมาย เป็นต้น

8. หุ่นยนต์และระบบอัตโนมัติ (Robotic and Autonomous System)
ผลกระทบ สูง (3) ความน่าจะเป็น สูงมาก (4)

เทคโนโลยีหุ่นยนต์และระบบอัตโนมัตินั้นถูกวิจัยพัฒนาขึ้นอย่างต่อเนื่องในปัจจุบัน ผ่านผู้นำทั้งจากภาคอุตสาหกรรมพลเรือนและหน่วยงานความมั่นคง เพราะสามารถปรับปรุงประสิทธิภาพต่อต้นทุน (Cost-Effective) ได้อย่างมาก โดยในส่วนของเทคโนโลยี

ทางทหารนั้นจะมุ่งเน้นแนวทางใช้หุ่นยนต์และระบบอัตโนมัติใน 3 ส่วน คือ (1) การทำงานทดแทนมนุษย์ (2) การเสริมศักยภาพใหม่ของมนุษย์ และ (3) การต่อต้านหุ่นยนต์ฝ่ายตรงข้าม เป็นส่วนใหญ่ ซึ่งมักจะเริ่มจากระบบงานประเภทไร้ผู้ควบคุมบนพาหนะ (Unman Vehicle: UV) ต่างๆ เช่น UAV, UGV หรือ USV ในการปฏิบัติการกิจต่าง ๆ เป็นต้น ซึ่งมีการใช้งานมานานนับ 10 ปีแล้ว แต่ในระยะ 10 ปีข้างหน้า ก็จะมีการพัฒนาให้มีความซับซ้อน ฉลาด ประหยัด น่าเชื่อถือ และมีแหล่งพลังงานที่มีประสิทธิภาพมากขึ้น [2] เพื่อให้สอดคล้องกับยุทธวิธีการใช้งานของเหล่าทัพในอนาคต

อย่างไรก็ดี เทคโนโลยีกลุ่มนี้ก็มีการศึกษาวิจัยการใช้งานเทคโนโลยีหุ่นยนต์ร่วมกับสิ่งมีชีวิตแบบต่าง ๆ เพื่อเสริมขีดความสามารถ เช่น หุ่นยนต์กึ่งชีวภาพ (Cybernetic Organism: Cyborg) หุ่นยนต์ชีวภาพ (Bio-robotics) หุ่นยนต์จิ๋ว (Micro/Nano-bot) หรือใช้เพื่อปฏิบัติการร่วมระหว่างคน-เครื่องจักร (Human-Machine Interface) ในอนาคตที่น่าจะเห็นชัดเจนขึ้นภายใน 10 ปีข้างหน้า [6] อีกด้วย โดยอาจสรุปภาพรวมของเทคโนโลยีหุ่นยนต์และระบบอัตโนมัติที่กำลังเกิดขึ้นได้ดังต่อไปนี้

เวลา (ค.ศ.)	เทคโนโลยีสำคัญ	ยุทธวิธี/รูปแบบการใช้งาน
2010 - 2019	• UAV (Unmanned Aerial Vehicle) • UGV (Unmanned Ground Vehicle) • USV (Unmanned Surface Vehicle) • ระบบตรวจการณ์ (Surveillance Sys.)	• ISR (Intelligence, Surveillance and Reconnaissance) • สายส่งกำลังบำรุง (Logistic Support) • เก็บกู้/ตรวจสอบวัตถุระเบิด (EOD) • ติตอาวุธ (Combat Support)
2020 - 2029	• UUV (Unmanned Underwater Vehicle) • Micro-bot (หุ่นเล็ก)/ Swarm (ฝูงหุ่นยนต์) • แหล่งพลังงานขั้นสูง เช่น กราฟีนแบตเตอรี่ • AI เพื่อการตัดสินใจและสนับสนุนการรบ • การต่อต้านระบบ Unmanned	• คลื่นโจมตีขนาดใหญ่ (Swarm Attack) • หน่วยสนับสนุนทางไกล เช่น UAV เต็มเชื้อเพลิงกลางอากาศ • สงครามอิเล็กทรอนิกส์เพื่อต่อต้าน/ยับยั้งการต่อต้านการใช้หุ่นยนต์ เช่น Radio, GNSS Jammer
2030 - 2039	• Advance/Hybrid Propulsion • Exoskeleton (ชุดโครงเสริมกายภาพ) • Human-Machine interface • Cybernetic Organ • NeuraLink (ระบบประสาทจักรกล)	• การป้องกันทางใต้ทะเล/น่านฟ้า • หุ่นรบภักดี (Loyalty Robot) • ชุดรบก้าวหน้า (Advance Suit) • ระบบสื่อสารระหว่างกำลังพล-หุ่นยนต์ • อวัยวะ/ระบบประสาทเทียมทางทหาร

ในช่วงปัจจุบันถึงอนาคตอันใกล้ เทคโนโลยีหุ่นยนต์และระบบอัตโนมัติในกิจการความมั่นคง/ป้องกันประเทศนี้มักถูกใช้ในภารกิจพื้นฐาน 3D (Danger-Dirty-Dull คือ กิจกรรมที่อันตราย สกปรก และซ้ำซาก) เป็นหลัก ผนวกกับการกิจเชิงปริมาณและซับซ้อน หรือต้องการการตอบสนองที่รวดเร็วกว่าปกติ โดยระบบดังกล่าวสามารถแบ่งเบาภาระด้านทรัพยากรบุคคลได้เป็นอย่างมาก ทำให้มีข้อดี เช่น การเฝ้าระวังตรวจการณ์ การสนับสนุนการรบ เป็นต้น ก่อนจะยกระดับขึ้นด้วยเทคโนโลยีประสานคน-เครื่องจักรเข้าหากันในอนาคต [7]

9. ปฏิบัติการภาคอวกาศ (Space Operation)

ผลกระทบ สูง (4) ความน่าจะเป็น ปกติ (2)

อวกาศถือเป็นหนึ่งในพื้นที่ปฏิบัติการใหม่ที่ได้ได้รับความสนใจในฐานะเทคโนโลยีป้องกันประเทศ ซึ่งเริ่มขยายวงกว้างจากกิจกรรมทางเศรษฐกิจและการใช้งานเชิงพาณิชย์เป็นจำนวนมากในช่วง 10 ปีที่ผ่านมา จากการเติบโตของอุตสาหกรรมอวกาศที่เริ่มขยายตัวออกจากชาติมหาอำนาจหลัก [5] เช่น สหรัฐฯ รัสเซีย และสาธารณรัฐประชาชนจีน ไปยังชาติอุตสาหกรรมศักยภาพสูง เช่น ญี่ปุ่น อินเดีย สหภาพยุโรป รวมไปถึงภาคเอกชนที่มีขีดความสามารถ เช่น

SpaceX ทำให้ต้นทุนการปฏิบัติการในอวกาศต่ำลงอย่างต่อเนื่องจนแม้แต่ชาติกำลังพัฒนาก็สามารถใช้ประโยชน์จากห้วงอวกาศสากลได้อย่างต่อเนื่อง อาทิเช่น ดาวเทียมขนาดเล็ก (CubeSat) ที่สามารถติดตั้งอุปกรณ์ (Payload) หลากหลาย และสามารถส่งขึ้นอวกาศครั้งละมาก ๆ ผ่านบริการภาคเอกชนได้ในราคาประหยัด รวมไปถึงความพยายามของภาคเอกชนขนาดใหญ่ เช่น SpaceX และ Amazon ที่ผลักดันให้ห้วงอวกาศเป็นเครือข่ายโทรคมนาคมแห่งใหม่ด้วยดาวเทียมขนาดเล็กจำนวนมากขึ้นลง เพื่อทดแทนการวางโครงข่ายใยแก้วนำแสงข้ามทวีปแบบเดิม

อย่างไรก็ดี การใช้งานห้วงอวกาศในความมั่นคงยังคงมีความสำคัญอย่างยิ่ง เนื่องจากเป็นส่วนสำคัญ

ในการบูรณาการการสื่อสาร การนำร่องทิศทาง และบริหารจัดการระบบภูมิสารสนเทศของยุโรปกรณีขั้นสูง อย่างเช่นการใช้งานโครงข่ายข้อมูล (Data Link) การระบุพิกัดภูมิประเทศ (GNSS) และการเฝ้าตรวจการณ์ภัยคุกคามจากอวกาศ (Space Early Warning) โดยชาติมหาอำนาจทั้งสหรัฐฯ รัสเซีย และจีน ต่างได้มีการจัดตั้งกองทัพอวกาศ (Space Force) หรือหน่วยงานความมั่นคงที่รับผิดชอบห้วงอวกาศแล้วทั้งสิ้น เพื่อรักษาขีดความสามารถในห้วงอวกาศของตน ส่วนหลายประเทศที่แม้จะไม่มีศักยภาพในการใช้ประโยชน์จากอวกาศอย่างเต็มที่ก็มีการเสริมขีดความสามารถในการป้องกันทางอวกาศเช่นกัน อาทิ การพัฒนาอาวุธต่อต้านดาวเทียม (Anti-Satellite system) ของอินเดีย โดยสามารถวิเคราะห์ช่วงเวลาโดยสังเขปของเทคโนโลยีดังนี้

เวลา (ค.ศ.)	เทคโนโลยีสำคัญ	ยุทธวิธี/รูปแบบการใช้งาน
2020 - 2029	- เทคโนโลยีการเฝ้าตรวจการณ์ห้วงอวกาศ - อาวุธปล่อยนำวิถีต่อต้านดาวเทียม (ASAT) - การผลิต/นำส่งดาวเทียมราคาประหยัด - การบูรณาการเซ็นเซอร์หลายประเภท	- ติดตั้งอาวุธ ASAT ให้กับฐานปฏิบัติการอวกาศยาน/เรือรบ - จัดตั้งฐานปฏิบัติการส่งดาวเทียมหลัก/สำรองในหลายพื้นที่
2030 - 2039	- อาวุธต่อต้านดาวเทียมในบริเวณกว้าง - ฐานปฏิบัติการอวกาศ (Space Platform) - ฐานปฏิบัติการบนเทหวัตถุ (Space Object)	- อาวุธแม่เหล็กไฟฟ้า (EMP) ห้วงอวกาศ - ต้นแบบยานอวกาศ (Spaceship) และสถานีอวกาศทางทหารบนดวงดาว

ในปัจจุบันรูปแบบสงครามในห้วงอวกาศยังไม่ได้มีการกำหนดหลักนิยามอย่างแน่ชัด ด้วยข้อจำกัดทางเทคโนโลยีและต้นทุนการปฏิบัติการที่ยังสูงอยู่

มาก และสงครามตามแบบ (Convention Warfare) ของแต่ละประเทศยังมีพื้นฐานอยู่บนดาวเคราะห์โลกเป็นหลัก ดังนั้นในช่วงระยะ 10 ปีข้างหน้า

หลักนิยามการรบในอวกาศจึงจำกัดอยู่ที่การปกป้องทรัพย์สินของฝ่ายเดียวกันในห้วงอวกาศ หรือสกัดกั้นฝ่ายตรงข้ามในการใช้อวกาศโดยเสรีเป็นสำคัญ รวมถึงภัยคุกคามทางธรรมชาติและสิ่งแวดล้อม เช่น การรบกวนของอุกกาบาตหรือเศษซากชิ้นส่วนจากอวกาศ โดยมีตัวอย่างเช่นในประเทศสหรัฐฯ นับตั้งแต่ปี ค.ศ. 2017 ได้เริ่มพัฒนาการฝึกประจำปีที่เรียกว่า “Space Flag” ขึ้นเพื่อจำลองการที่ดาวเทียมฝ่ายตนถูกโจมตี

10. การคำนวณควอนตัม
(Quantum Computing)

ผลกระทบ สูงมาก (5) ความน่าจะเป็น น้อย (1)

รากฐานการประมวลผลทางคอมพิวเตอร์ในปัจจุบันมีพื้นฐานจากการกำหนดเลข 0 และ 1 เพื่อใช้ในการคำนวณต่าง ๆ นำลงมาบรรจุลงแผงวงจรทรานซิสเตอร์ แล้วนำวงจรเหล่านั้นจำนวนมากมาประกอบกันเป็นหน่วยประมวลผล (CPU) ในอุตสาหกรรมหลายรูปแบบ โดยตามทฤษฎีของมัวร์ (Moore’s Law) ระบุว่าจำนวนทรานซิสเตอร์ดังกล่าวจะเพิ่มขึ้นเท่าตัวในทุก 2 ปี บริษัทผู้ผลิตวงจรเหล่านี้

เช่น Intel, AMD มักใช้วิธีการสร้างสถาปัตยกรรมวงจรที่เล็กลงอย่างมาก (ระดับนาโนเมตร) เพื่อให้สามารถนำวงจรเหล่านี้ลงไปในหน่วยประมวลผลให้ได้มากที่สุด ซึ่งในปัจจุบันบริษัทดังกล่าวเริ่มเผชิญกับความท้าทายเชิงโครงสร้างทางเทคโนโลยีมากขึ้นเรื่อย ๆ เพราะความพยายามย่อส่วนวงจรจนเล็กมากจนส่งผลกระทบต่อความอ่อนไหวในการเคลื่อนไหวของอิเล็กตรอนในวัสดุจนเริ่มจะเสียประสิทธิภาพการทำงานไปแล้ว อุตสาหกรรมสารสนเทศจึงเริ่มมองหาเลือกเทคโนโลยีอื่นด้านการคำนวณตั้งแต่ขั้นพื้นฐาน ซึ่งควอนตัมเป็นหนึ่งในทางเลือกที่ได้รับความสนใจอย่างยิ่ง ในฐานะเครื่องมือในการคำนวณ (Quantum Computing) ที่แตกต่างจากหลักการของหน่วยประมวลผลแบบเดิม (ที่มีสถานะ 0 หรือ 1) แต่ควอนตัมจะใช้สิ่งที่เรียกว่า ‘คิวบิต’ (Qubit) ซึ่งเป็นหน่วยประมวลผลที่สามารถแสดงสถานะได้ทั้ง 0 และ 1 ในเวลาเดียวกันโดยอาศัยปรากฏการณ์ทางธรรมชาติของอะตอมที่เหนือสามัญสำนึกทั่วไป และสามารถนำมาประยุกต์ใช้กับเทคโนโลยีอื่นทั้งภาคพลเรือนและทหารได้ ยกตัวอย่างเช่น

รูปแบบ	คุณลักษณะควอนตัม	เทคโนโลยีอนาคต
Quantum Superposition (หลักการซ้อนทับควอนตัม)	อะตอมหนึ่งตัวสามารถมีตัวตนอยู่หลายตำแหน่งได้เวลาเดียวกัน	• ประมวลผลปริมาณมาก • การถอดรหัสจำนวนอนันต์
Quantum Tunneling (อุโมงค์ควอนตัม)	อะตอมสามารถทะลุผ่านกำแพงได้โดยไม่ต้องอ้อมหรือกระโดดข้าม	• เคลื่อนย้ายฉับพลันทางไกล (Teleport/Warp)
Quantum Entanglement (การพัวพันเชิงควอนตัม)	อะตอมหลายตัวสามารถสื่อสารกันโดยไม่ต้องมีการส่งสัญญาณหรือสื่อกลาง	• ระบบที่ไร้การดักฟังและไม่สามารถถูกเจาะ (Hack) ได้ • ควอนตัมเรดาร์

ซึ่งกฎเกณฑ์ทางธรรมชาติเหล่านี้ได้รับการพิสูจน์ผ่านทฤษฎีควอนตัมฟิสิกส์อย่างต่อเนื่อง และบริษัทด้าน ICT ขนาดใหญ่จำนวนมาก เช่น Google, IBM ก็เริ่มนำกฎเกณฑ์เหล่านี้มาศึกษาในการสร้างคอมพิวเตอร์แบบใหม่เพื่อตอบสนองเป้าหมายของตนเอง อาทิ เป้าหมายว่าต้องการพัฒนา AI ที่มีประสิทธิภาพสูงจนฮาร์ดแวร์พื้นฐานในปัจจุบันตอบสนองได้ยาก หรือถึงตอบสนองได้ก็ต้องใช้ทรัพยากรมากเกินไปจนจะบรรจุลงไปในอุปกรณ์ได้โดยสะดวก ตัวอย่างเช่น Google ได้ประเมินว่า Supercomputer ที่ใช้ในการพยากรณ์สภาพอากาศที่สามารถลดขนาดลงได้นับร้อยเท่าเมื่อเปลี่ยนวิธีการคำนวณมาใช้ Quantum-AI [5]

ปัจจุบันภาพรวมในอนาคตของคอมพิวเตอร์ควอนตัมนั้นยังไม่ชัดเจนมากกว่าผู้วิจัยแต่ละหน่วยงานจะเลือกใช้ไปประยุกต์กับเทคโนโลยีแบบใดเป็นหลัก และยากต่อการคำนวณว่าเทคโนโลยีควอนตัมใดจะประสบความสำเร็จในตลาดก่อนหรือหลังจึงไม่อาจทำตารางประเมินระยะเวลาได้ในขณะนี้ อีกทั้งยังมีคู่แข่งของเทคโนโลยีในอุตสาหกรรมเดิมทั้งส่วนฮาร์ดแวร์ (เซมิคอนดักเตอร์) และซอฟต์แวร์ (ระบบปฏิบัติการ: OS และโปรแกรมประยุกต์: Application) อีกทั้งการวิจัยควอนตัมคอมพิวเตอร์ในปัจจุบันยังมีข้อจำกัดหลายประการ เช่น มาตรฐานทางภาษาของโปรแกรมคอมพิวเตอร์ และอุปกรณ์ทดสอบจำเป็นต้องอยู่ในอุณหภูมิเย็นจัดมาก เพื่อลดความแปรปรวน จนหน่วยงานวิจัยขนาดเล็กไม่สามารถดำเนินการได้ง่าย โดยคาดหมายได้ว่าจะเริ่มเห็นทิศทางของควอนตัมได้ชัดเจนในอีก 10 ปีข้างหน้า เป็นต้นไป อย่างไรก็ตาม บางสาขาเทคโนโลยีทางการป้องกันประเทศสามารถได้รับประโยชน์โดยตรงได้รวดเร็ว เช่น กระบวนการเข้ารหัสทางควอนตัม

(ยากต่อการเจาะระบบ/ดักฟัง) และกระบวนการใช้ควอนตัมเจาะระบบ/ถอดรหัสลับสารสนเทศแบบเดิม (Quantum Hacking) เป็นต้น และควอนตัมเรดาร์ที่ใช้หลักการของอะตอมแทนคลื่นวิทยุทำให้สามารถตรวจจับอากาศยานล่องหน (Stealth) ได้ โดยไม่สามารถหลบเลี่ยง

11. ห่วงโซ่อุปทานทางความมั่นคง (Defense Supply chain)

ผลกระทบ ปกติ (2) ความน่าจะเป็น สูงมาก (4)

เนื่องจากในช่วงระยะเวลาปัจจุบันจนถึงอนาคตอันใกล้ มีการเปลี่ยนแปลงเชิงยุทธศาสตร์ภาพใหญ่ (Grand Strategy) ของชาติมหาอำนาจในปัจจุบัน โดยเฉพาะสหรัฐอเมริกากับชาติพันธมิตร เช่น กลุ่ม NATO พันธมิตรเอเชียตะวันออกเฉียงไกล (เกาหลีใต้/ญี่ปุ่น/ไต้หวัน) และภูมิภาคตะวันออกกลาง รวมถึงอิทธิพลของจีนแผ่นดินใหญ่ที่เพิ่มสูงขึ้น ทำให้เกิดความขัดแย้งต่าง ๆ ทางเศรษฐกิจ เช่น สงครามการค้า (Trade War) และขยายผลเป็นสงครามชิงความได้เปรียบทางเทคโนโลยี (Technology War) ซึ่งยุทธศาสตร์ดังกล่าวนี้จะส่งผลกระทบยาวให้แต่ละประเทศเริ่มมีนโยบายแยกตัวทางเศรษฐกิจและความมั่นคงให้เป็นอิสระต่อกันมากขึ้น อันจะส่งผลต่อห่วงโซ่อุปทานทางอุตสาหกรรม (Industry Supply Chain) ทุกประเภททั่วโลก

การเปลี่ยนแปลงเชิงยุทธศาสตร์เหล่านี้จะส่งผลกระทบต่ออุตสาหกรรมทุกประเภท รวมถึงอุตสาหกรรมป้องกันประเทศในกลุ่มชาติตะวันตก ที่ปัจจุบันมักดำเนินธุรกิจตามรูปแบบโลกาภิวัตน์สุดขีด ที่กระจายสายการผลิต แหล่งวัตถุดิบ แรงงาน และตลาดไปยังส่วนต่าง ๆ ของโลกที่มีขีดความสามารถสูง เพื่อให้สามารถทำต้นทุนการผลิตได้ต่ำและผล

กำไรสูงสุดเท่าที่จะเป็นไปได้ พร้อมทั้งยังสร้างหุ้นส่วนธุรกิจจำนวนมากที่ค้าขายกันเองสร้างเม็ดเงินในระบบเศรษฐกิจตลอดห่วงโซ่อุปทานระยะยาวดังกล่าว (Long Distance Supply Chain) เช่น สายการผลิตเครื่องบินขับไล่ F35 และ Eurofighter ที่มีการกระจายชิ้นส่วนไปยังชาติพันธมิตรหลายสิบประเทศเพื่อสร้างเครือข่ายอุตสาหกรรมร่วมกัน แต่ในทางกลับกันหากเกิดข้อขัดแย้งระหว่างชาติสมาชิกก็จะส่งผลกระทบต่อสายการผลิตยุโรปกรณีนั้นโดยตรง เช่น กรณีที่สหรัฐฯ ขับไล่ตุรกีออกจากโครงการ F35 หรือ สาธารณรัฐประชาชนจีนตอบโต้สหรัฐฯ โดยการระงับการส่งออกสินแร่หายาก (Rare Earth) จนส่งผลกระทบต่อการจัดทำวัตถุดิบสำหรับการทำเชื้อเพลิงของอาวุธปล่อยนำวิถีหลายรุ่นของสหรัฐฯ หรือความเสี่ยงจากการที่พันธมิตรอาจไม่สามารถจัดส่งชิ้นส่วนจำเป็นได้ ตัวอย่างเช่น กรณีได้หวัน ซึ่งเป็นผู้ผลิตชิป (Chip) ที่ก้าวหน้าที่สุดในปัจจุบันและจำหน่ายให้กับยุทธโปกรณ์ชั้นสูงของสหรัฐฯ เป็นจำนวนมาก แต่มีความเสี่ยงในการถูกจีนแผ่นดินใหญ่

กดดันหรือครอบครอง อันจะทำให้ห่วงโซ่อุปทานด้านอิเล็กทรอนิกส์ทั่วโลกเสียหายอย่างร้ายแรงได้

ข้อแตกต่างประการสำคัญในการกีดกันทางการค้าระหว่างอุตสาหกรรมภาคพลเรือนกับทหารมักอยู่ในกระบวนการบังคับใช้ที่จับต้องได้และจับต้องไม่ได้ เช่น ในภาคพลเรือนมักถูกบังคับทางธุรกิจผ่านกระบวนการกฎหมายทรัพย์สินทางปัญญา ซึ่งมีหน่วยงานกลางระหว่างประเทศควบคุม อาทิ องค์การทรัพย์สินทางปัญญาโลก (WIPO) ขณะที่องค์ความรู้ชั้นสูงในอุตสาหกรรมทางทหารมักไม่มีการขึ้นทะเบียนอย่างเปิดเผยเพื่อหลีกเลี่ยงการทำวิศวกรรมย้อนกลับ (Reverse Engineering) จากผู้อื่น จึงมักใช้การควบคุมทางวัตถุดิบตั้งต้น หรือผลิตภัณฑ์มูลฐานที่ระบบย่อยสำคัญแทน อาทิ เหล็กเกรดสูง วัตถุดิบมันตรังสี หรือชิปนำร่อง ความแม่นยำสูงที่ใช้ในชิปนาวูเป็นต้น โดยสามารถวิเคราะห์ช่วงเวลาโดยสังเขปของเทคโนโลยีดังนี้

เวลา (ค.ศ.)	การเปลี่ยนแปลงทางอุตสาหกรรมสำคัญ	ผลกระทบในการเปลี่ยนแปลง
2020 - 2029	- การวิจัยออกแบบบนพื้นฐานของการใช้อุปกรณ์หลายแหล่ง (Multi-Sourcing) - การจัดทำมาตรฐานสากลทางวัตถุดิบ - สายการผลิต OEM ที่สามารถทดแทนกัน (Redundancy Source/Manufacturing)	- เทคโนโลยีร่วมภาคพลเรือนและความมั่นคง (Dual-Used) จะขยายตัวตามความอ่อนปรนของภาครัฐ - การส่งเสริม Defense OEM ในประเทศเกิดใหม่และเป็นกลาง
2030 - 2039	- การรวมศูนย์การผลิตสมบูรณ์ภายในประเทศ - การพัฒนาอุตสาหกรรมวัตถุดิบต้นน้ำ - มาตรฐานการบังคับใช้ทรัพย์สินทางปัญญา	- หลักความน่าเชื่อถือในสายการผลิตเริ่มสำคัญกว่ากำไร - การควบคุมอุตสาหกรรมเพื่อความสามารถในการแข่งขัน

อย่างไรก็ดี อุตสาหกรรมป้องกันประเทศเป็นสิ่งที่ผูกพันระหว่างประเทศกันอย่างเหนียวแน่นเป็นเวลานาน จึงไม่สามารถถอนตัวจากกันอย่างกะทันหันได้โดยง่าย เนื่องจากมีผลกระทบทางเศรษฐกิจและความมั่นคงของแต่ละประเทศเป็นอย่างสูง ดังนั้น ภาพรวมที่จะเกิดขึ้นในอนาคตอีก 10-15 ปีข้างหน้า คือ โครงการที่มีข้อผูกมัดในระยะสั้นจะยังคงดำเนินการต่อไป แต่ละชาติจะพยายามพึ่งพาทรัพยากรและศักยภาพของตนเองให้มากขึ้น โดยเพิ่มความมั่นคงในห่วงโซ่อุปทานให้มีความหลากหลายอย่างค่อยเป็นค่อยไป แม้จะสูญเสียกำไรหรือต้องลงทุนวิจัยเพิ่มเติมก็มักจะยินดี เช่น ความพยายามในการพัฒนาเครื่องบินรบยุคที่ 6 ด้วยตัวเองของสหราชอาณาจักร และการลงทุนพัฒนาเครื่องบินรบยุคที่ 5 ของญี่ปุ่นและเกาหลีใต้ แม้จะเป็นพันธมิตรที่เหนียวแน่นกับสหรัฐฯ อยู่แล้วเพื่อให้เป็นอิสระในการดำเนินการจากอิทธิพลต่างประเทศมากขึ้น รวมถึงประเทศขนาดเล็กจะมีการลงทุนเรื่องวัตถุดิบและยุทธโศปกรณ์อย่างจริงจัง โดยเฉพาะอาวุธพื้นฐานหรืออาวุธเชิงป้องกันที่มีต้นทุนต่ำ เช่น ยุทธโศปกรณ์เบาสำหรับทหารและอาวุธไซเบอร์ เป็นต้น

จาก 8 แนวโน้มอุตสาหกรรมภาพรวมข้างต้น จะเห็นได้ว่าในระยะสั้นช่วง 10 ปีแรกนั้น มักอยู่ในรูปของอุตสาหกรรมหรือตัวอย่างผลิตภัณฑ์ต้นแบบ (Prototype) เป็นหลัก เนื่องจากยุทธโศปกรณ์ตามรูปการจกกำลังรบในรูปแบบเดิมยังมีอยู่ในเหล่าทัพต่างๆ ทั่วโลกเป็นจำนวนมาก เช่น ยานรบทางบก - ทะเล - อากาศ ซึ่งด้วยงบประมาณกลาโหมที่ค่อนข้างจำกัดทั่วโลก โดยเฉพาะหลังภาวะวิกฤติทางเศรษฐกิจในหลายประเทศหลังสงครามการค้าและภาวะโรคระบาด จึงจำเป็นต้องใช้เวลาในการทยอยปลดประจำการ

และทดแทนด้วยยุทธโศปกรณ์เทคโนโลยีใหม่ดังกล่าว ยกเว้นแต่จะเกิดสถานการณ์สงครามหรือความขัดแย้งระหว่างประเทศศักยภาพสูงด้วยกันอย่างกะทันหัน จึงอาจจะทำให้กระบวนการเปลี่ยนผ่านเทคโนโลยีดังกล่าวเร็วขึ้นได้

12. บทสรุป

การจัดกลุ่มเทคโนโลยีและอุตสาหกรรมป้องกันประเทศ 8 ชนิด ช่วงปี 2020-2040 ตามหัวข้อข้างต้นได้ประเมินจากระดับผลกระทบที่เกิดขึ้นทางยุทธศาสตร์การป้องกันประเทศ และระยะเวลาในการเข้าสู่ตลาดหรืออุตสาหกรรมในระดับโลกเป็นสำคัญ โดยผู้จัดทำบทความจัดลำดับความสำคัญเบื้องต้นได้ดังตารางในหน้า 60

จากตารางจะเห็นได้ว่าในลำดับคะแนนรวมกลุ่มเทคโนโลยีสารสนเทศ (ICT) อย่างปฏิบัติการไซเบอร์และปัญญาประดิษฐ์มีผลกระทบอย่างสูงในปัจจุบัน เนื่องจากได้รับการส่งเสริมอย่างมากทั้งจากภาคพลเรือนและฝ่ายความมั่นคงในแทบทุกประเภท มีการใช้งานเต็มรูปแบบในปัจจุบันและยังมีแนวโน้มใช้งานอย่างต่อเนื่องในอนาคต ในขณะที่กลุ่มลำดับรอง อาทิ หุ่นยนต์และระบบอัตโนมัติ รวมถึงอาวุธพลังงานนั้นเป็นสาขาวิชาที่ได้รับการวิจัยพัฒนาอย่างเต็มที่ แต่เนื่องจากยังไม่ได้มีการนำยุทธโศปกรณ์เหล่านี้เข้าประจำการเป็นจำนวนมาก จึงคาดหมายได้ว่าจะถูกส่งเสริมให้มีบทบาทในกองกำลังทั่วโลกต่อไป ส่วนกลุ่มคะแนนระดับท้ายมักเป็นสาขาวิชาที่ยังต้องได้รับการพิสูจน์อีกระยะหนึ่ง (ควอนตัม) หรือเป็นอาวุธสำคัญเชิงยุทธศาสตร์ที่อาจมีผลกระทบมาก แต่การใช้งานจริงเชิงปริมาณยังมีข้อจำกัดกว่า จึงถูก

ประเภทเทคโนโลยี	ระดับผลกระทบ (A)	เวลาในการเข้าสู่ตลาด (B)	คะแนนรวม (AxB)
ปฏิบัติการทางไซเบอร์	4	5	20
ปัญญาประดิษฐ์	5	3	15
หุ่นยนต์และระบบอัตโนมัติ	3	4	12
อาวุธพลังงาน	4	3	12
ห่วงโซ่อุปทานทางทหาร	2	4	8
ปฏิบัติการภาคอวกาศ	4	2	8
อาวุธพลังงานจลน์ขั้นสูง	2	3	6
เทคโนโลยีควอนตัม	5	1	5

ประเมินว่ามีความสำคัญในภาพรวมเป็นลำดับรอง

ทั้งนี้ สำหรับประเทศไทย ซึ่งมีสถานะในปัจจุบันเป็นชาติเป็นกลางขนาดเล็ก และมีขีดความสามารถในเทคโนโลยีป้องกันประเทศอยู่ในวงจำกัด เมื่อเทียบกับชาติมหาอำนาจที่กำลังวิจัยพัฒนาเทคโนโลยีสำคัญทั้ง 8 ด้านขั้นต้น จึงเป็นไปได้ยากที่จะแข่งขันกันในเชิงผลิตภัณฑ์/บริการยุทธโศปกรณ์โดยตรงในตลาดสากล แต่เนื่องจากเทคโนโลยีกลุ่มนี้ยังเป็นเรื่องที่ค่อนข้างใหม่มากแม้ในกลุ่มวิจัยพัฒนาของชาติมหาอำนาจ จึงยังมีโอกาสบางส่วนของประเทศไทยจะสร้างขีดความสามารถแท้จริงของเทคโนโลยีเหล่านี้ โดยเล็งผลที่ระบบ/เทคโนโลยี/บริการ ที่เป็นส่วนประกอบต่าง ๆ เช่น การพัฒนา

ขีดความสามารถสารสนเทศเพื่อสนับสนุน AI ด้านภาษาธรรมชาติของประเทศไทยหรือภูมิภาค หรือการพัฒนาขีดความสามารถอุตสาหกรรมด้านเครื่องยนต์ พลังงานทางเลือก หรือระบบอิเล็กทรอนิกส์ที่เป็นการต่อยอดอุตสาหกรรมเดิมในประเทศ โดยอาศัยคุณลักษณะเฉพาะทางภูมิศาสตร์และรัฐศาสตร์ในการเข้าสู่ตลาดยุทธโศปกรณ์โลกได้ทั้งค่ายตะวันตกและตะวันออก ซึ่งเป็นการสอดคล้องกับนโยบายระดับชาติ เช่น Thailand 4.0 หรือการส่งเสริมทางเศรษฐกิจ เช่น EEC ต่อไปในอนาคตกับชาติมหาอำนาจที่กำลังวิจัยพัฒนาเทคโนโลยีสำคัญ

8. เอกสารอ้างอิง

[1] Michael O'Hanlon, Forecasting Change in Military Technology 2020-2040.

[2] Frost&Sullivan, Global Defense Outlook, 2019.

[3] Frost&Sullivan, ADEC Exhibition - Milsim 2018, Singapore.

[4] M.L.Cummings, Artificial Intelligence and the Future of Warfare, International Security Department and US and the Americas Program 2017.

[5] Siva Banda, Aerospace System Directorate Overview, Air Force Research Laboratory (AFRL) 2019.

[6] CCDC CBC-TR-1599, Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DOD.

[7] Strategic Plan FY19-23, DoD Digital Modernization Strategy, 2019.