

ปฏิบัติการหลายโดเมน:
สะพานเชื่อมช่องว่างเพื่อความเหนือชั้นกว่า
MDO -Bridging the GAPS for Dominance

โดย

Kimber Nettis

สำนักงานยุทธศาสตร์และหลักนิยามกองทัพอากาศ (เพื่อพลาง)
น.อ.ยุทธศักดิ์ พูลสุวรรณ ผู้แปล

ปฏิบัติการหลายโดเมน : สะพานเชื่อมช่องว่างเพื่อความเหนือชั้นกว่า

MDO -Bridging the Gaps for Dominance

กองทัพอากาศ พร้อมกับผู้ร่วมรบ ต้องปรับความคิดและวัฒนธรรมของพวกเราให้สามารถสลับไปมาระหว่างโดเมน องค์ประกอบ และภูมิภาคต่างๆ เพื่อสร้างผลการสู้รบที่มีความเร็วสูงและแม่นยำเพื่อตอบสนองความต้องการภารกิจของผู้บัญชาการกองกำลังร่วม

—AF Multi-Domain Operations (MDO) Implementation Plan 2018

ในช่วงไม่กี่ปีที่ผ่านมากระทรวงกลาโหม (DOD) ของสหรัฐฯ ได้หันความสนใจไปที่ความต้องการที่เพิ่มขึ้นของการปฏิบัติการหลายโดเมน (Multi-Domain Operations : MDO) ยุทธศาสตร์การป้องกันประเทศระบุว่า “การแข่งขันในสภาพแวดล้อมด้านความมั่นคงที่ซับซ้อน และชิงดีชิงเด่นกันนี้ สหรัฐฯ จะต้องเตรียมพร้อมที่จะดำเนินการก้าวข้ามความขัดแย้งอย่างเต็มรูปแบบในหลายโดเมนพร้อมๆ กัน” หน่วยงานต่างๆ ของกองทัพได้ปฏิบัติตามคำแนะนำนี้ และเริ่มนำรูปแบบต่างๆ ของการปฏิบัติการหลายโดเมนเชิงบูรณาการ ไปใช้กับเหล่าทัพของตน ดังเช่น Lt Gen Norman Seip ที่ปรึกษาอาวุโสของกองทัพอากาศด้านการบัญชาการและควบคุมหลายโดเมน (Multi-Domain Command and Control) กล่าวว่า “เป้าหมายของการปฏิบัติการหลายโดเมน คือการสร้างสถานการณ์อันซับซ้อนยากลำบากที่เกิดขึ้นพร้อมๆ กันให้กับศัตรู” ในการทำเช่นนี้ เราต้องตระหนักว่าสภาพแวดล้อมปฏิบัติการในปัจจุบันของเราเปลี่ยนแปลงไปอย่างไรบ้างจากการเพิ่มขึ้นของเทคโนโลยีอวกาศ/ไซเบอร์ และการเปลี่ยนแปลงในการเข้าถึงข้อมูลของพวกเราที่กำลังเผชิญอยู่ได้ อย่างไรก็ตาม เราต้องตระหนักด้วยว่าสนามรบได้วกกลับมาอยู่ที่หน้าบ้านเราแล้ว และนี่เป็นความท้าทายใหม่ที่ต้องก้าวผ่านด้วยวิธีแก้ปัญหาแบบใหม่

บางคนแย้งว่ากระทรวงกลาโหม ได้ทำปฏิบัติการหลายโดเมนมาโดยตลอด และนี่เป็นเพียงคำศัพท์ใหม่ของเพนตากอน (Pentagon) ที่มีจุดมุ่งหมายจะดึงเงินทุนเพิ่มเติม อะไรทำให้การปฏิบัติการหลายโดเมนแตกต่างจากการปฏิบัติการแบบอื่นดังเช่น กองกำลังร่วม? (Joint Forces) บทความนี้จะบอกให้ทราบว่าสงครามมีวิวัฒนาการอย่างไร? และเหตุใดเราจึงมุ่งสู่หลักนิยมของการปฏิบัติการหลายโดเมน นอกจากนี้ บทความนี้ยังให้กรอบการทำความเข้าใจแนวคิดพื้นฐานที่สามารถนำมาใช้ในการปฏิบัติการหลายโดเมนของสงครามเชิงรุก และเชิงรับทั้งในระดับยุทธวิธีและระดับยุทธการ

วิวัฒนาการของสงคราม

แรงผลักดันหลักที่จะเปลี่ยนแปลงวิธีการทำสงครามของกองทัพนั้นขึ้นอยู่กับเทคโนโลยีและการเปลี่ยนแปลงของเทคโนโลยี และแบบแผนการรบ (scheme of maneuver) เป็นส่วนใหญ่ เมื่อมีการนำเทคโนโลยีใหม่เข้าสู่สนามรบ เราจะต้องนำแบบแผนการรบมาปรับใช้ และปรับปรุงกลยุทธ์ เทคนิค ขั้นตอน แผนงานและคำสั่งที่เกี่ยวข้อง วิวัฒนาการของการทำสงครามโดยย่อนี้จะครอบคลุมหลักนิยมที่ใช้มายาวนาน และการพัฒนาทางเทคโนโลยีที่จุดประกายการเปลี่ยนแปลงในวิธีการสู้รบของเรา

การสู้รบเริ่มแรกมีลักษณะเป็นแนวเส้นตรง (Linear) กองทัพหนึ่งจะเข้าแถวต่อต้านอีกกองทัพหนึ่งซึ่งดาบ หอก หรือปืนคาบศิลา แล้วต่อสู้จนฝ่ายใดฝ่ายหนึ่งจะชนะ เมื่อฝ่ายใดมีขนาดเล็กกว่าหรือขีดความสามารถด้อยเกินกว่าที่จะต่อสู้ในลักษณะดั้งเดิมนี้ได้ สงครามกองโจรก็จะกลายเป็นยุทธวิธีที่ช่วยให้เกิดสมดุล รวมไปถึงการชุมนุมโจมตี การก่อวินาศกรรม และการจู่โจม จากนั้นการเปลี่ยนแปลงทางเทคโนโลยีที่เรียกกันว่า “ปืนกล” ก็ได้ส่งกองทัพลงไปยังสนามเพลาะ

Nicholas Murray ผู้เขียน The Rocky

Road to the Great War กล่าวว่า “สงครามสนามเพลาะขยายวงกว้างขึ้น แต่เมื่อการพัฒนาในด้านอำนาจการยิงที่ไม่สอดคล้องกับขีดความสามารถในการเคลื่อนย้ายกำลัง ผลก็คือเป็น

เรื่องยากที่ฝ่ายตั้งรับจะเป็นฝ่ายที่ได้เปรียบ”

สงครามสนามเพลาะจึงกลายเป็นที่รู้จักกันในฐานะสัญลักษณ์ของความไร้ประโยชน์ของการ

ดำเนินการยุทธ์ การทำสงครามประเภทนี้

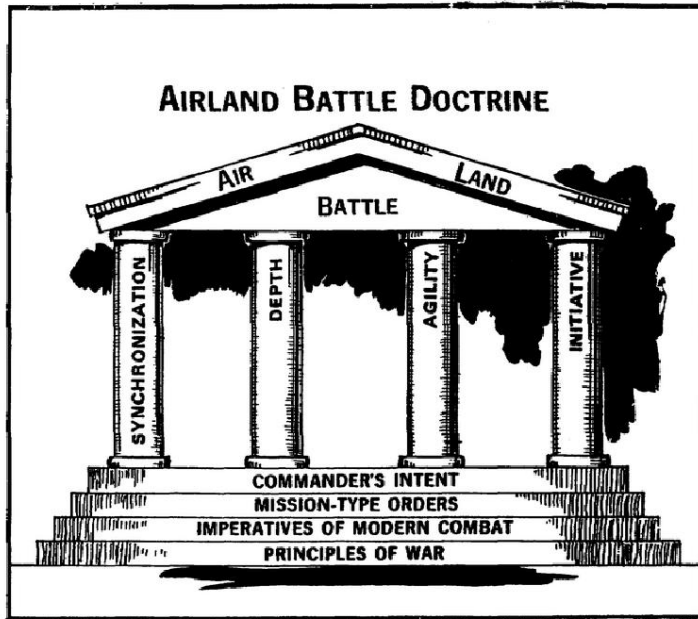
บ่อยครั้งที่เข้าจุดอับ และมีอัตราการเสียชีวิตสูง จากนั้นจึงมีการเปลี่ยนแปลงในด้านเทคโนโลยีและหลักนิยม

ในช่วงสงครามโลกครั้งที่ 1 ฝ่ายเยอรมันมุ่งเน้นไปที่แผนการยุทธ์ที่ใช้ยุทธวิธีการแทรกซึม ในขณะที่อังกฤษและ

ฝรั่งเศสมุ่งเน้นไปที่การพัฒนารถถังไปสู่วัยชนะ



การรบทางอากาศ-พื้นดิน



Air-Land Battle เป็นหลักนิยมการรบของกองทัพสหรัฐฯ ในสงครามเวียดนาม ช่วงปีทศวรรษ 1980s และ 1990s ซึ่งตั้งตั้งแต่ปี พ.ศ. 1973 กองบัญชาการการฝึกและหลักนิยมแห่งสหรัฐอเมริกา (United States Training and Doctrine Command) ได้ถูกก่อตั้งขึ้นภายใต้การนำของ Gen William E. DePuy. จากนั้นจึงได้ส่ง Gen Donn A. Starry ไปยังอิสราเอลเพื่อทำความเข้าใจสงคราม Yom Kippur ซึ่งจังหวะความเร็ว และการแพร่กระจายของอาวุธใหม่ๆ แตกต่างจากที่เคยเห็นในสนามรบ

ใดๆ มาก่อน เขาเห็นความสำคัญของการรบด้วยกำลังทางอากาศร่วมกันกับกำลังทางบก รวมถึงจรวดนำวิถีต่อต้านรถถังสามารถเปลี่ยนสมรภูมิได้อย่างไร เขาอ้างถึงคำกล่าวที่ว่า “กองทัพที่ออกมาจากเวียดนามไม่ใช่กองทัพที่เราต้องการในอนาคต”

การเปลี่ยนแปลงหลักนิยมกลายเป็น “การปฏิวัติ DOTMLPF” ซึ่งหมายถึงกระบวนการได้มาซึ่งหลักนิยม (Doctrine) องค์กร (Organization) การฝึกอบรม (Training) ยุทโธปกรณ์ (Materiel) ความเป็นผู้นำ (Leadership) กำลังพล (Personnel) สิ่งอำนวยความสะดวก (Facilities) และนโยบาย (Policy) Starry นำบทเรียนที่เรียนรู้จากสงคราม Yom Kippur มาเริ่มต้นสิ่งที่เรียกว่าโครงการพัฒนาความทันสมัย 5 ด้าน (Big Five Modernization Project) ของกองทัพบก และเป็นแรงบันดาลใจให้กองทัพอากาศลงทุนในอาวุธปล่อยที่สามารถล่องหน และมีความแม่นยำสูง (Stealth & Precision Standoff Weapons) ระบบอาวุธใหม่ และวิธีการฝึกอบรมที่เกิดจากการเปลี่ยนแปลงหลักนิยมนำไปสู่การเปิดตัวศูนย์ฝึกอบรม และโรงเรียนผู้นำแห่งใหม่ การประเมินแนวทางการฝึกอบรม และหลักนิยมที่ต่างไปจากเดิมอย่างสิ้นเชิงนี้ออกมาในรูปแบบของปฏิบัติการพายุทะเลทราย ทั้งโลกได้เห็นสหรัฐฯ เอาชนะกองทัพที่ใหญ่เป็นอันดับสี่ของโลกในเวลาไม่ถึง 100 ชั่วโมงโดยมีผู้บาดเจ็บล้มตายเพียงเล็กน้อย มันเหมือนกับสงคราม Yom Kippur แต่เร็วกว่า และร้ายแรงกว่า

สงครามนอกแบบ (irregular Warfare)

หลักนิยมเปลี่ยนไปอีกครั้งเมื่อเราเผชิญกับภัยคุกคามใหม่ๆ เช่น องค์การนิยมความรุนแรงแบบสุดโต่ง (Violent Extremist Organizations : VEO) การทำสงครามนอกแบบกลายเป็นหนทางปกติในการสู้รบตั้งแต่



ปี 2003 เป็นต้นมา การทำสงครามนอกแบบได้รับการอธิบายว่าเป็น “การต่อสู้อย่างดุเดือดระหว่างผู้มีบทบาทของรัฐ (State) และตัวแสดงที่ไม่ใช่รัฐ (Non State) เพื่อความชอบธรรมและอิทธิพลเหนือประชาชนที่เกี่ยวข้อง” สหรัฐฯ ได้ต่อสู้กับสงครามประเภทนี้ในอิรักและอัฟกานิสถานในช่วง 2-3

ทศวรรษที่ผ่านมา ในขณะที่สหรัฐฯ เต็มไปด้วยภัยคุกคาม VEO อยู่ นั่น สงครามรูปแบบใหม่ก็เริ่มปรากฏขึ้นเมื่อภัยคุกคามเปลี่ยนไปคู่ต่อสู้ที่หัตถ์เทียมเหล่านี้นำมาซึ่งความจำเป็นต้องพิจารณาการปฏิบัติการหลายโดเมนเนื่องจากคู่ต่อสู้แตกต่างไปจาก VEO ที่สหรัฐฯ เคยเผชิญในสงครามครั้งก่อนหน้า สหรัฐฯ จะแข่งขันกันในทุกโดเมน และความเร็วของการทำสงครามก็เพิ่มขึ้นตามเทคโนโลยีใหม่ๆ ที่เกิดขึ้น เช่น ปัญญาประดิษฐ์ (AI) และไฮเปอร์โซนิก (Hypersonics) ปีบอดเวลาที่เราสามารถดำเนินการและตัดสินใจได้

การปฏิบัติการหลายโดเมน (Multi-Domains Operations)

หลักนิยมใหม่ล่าสุดที่ออกมาจากกระทรวงกลาโหม สหรัฐฯ คือการปฏิบัติการหลายโดเมน (Multi - Domain Operations : MDO) เป็นแนวคิดที่กองกำลังร่วมสามารถบรรลุความได้เปรียบในการแข่งขันเหนือคู่ต่อสู้ที่ใกล้เคียงกันโดยการแสดงภัยคุกคามหลายอย่างให้อีกฝ่ายฝ่ายจำต้องตอบสนอง ซึ่งจะเป็นการเปิดเผยช่องโหว่ของฝ่ายตรงข้ามต่อภัยคุกคามอื่นๆ มันคือการผสมผสานอย่างมีศิลปะของสถานการณ์ที่ต้องเลือกระหว่างสองทางขึ้นไป โดยเฉพาะอย่างยิ่งทางเลือกที่ไม่พึงปรารถนาอย่างเท่าเทียมกันเหล่านี้ มากกว่าที่จะเอาชนะได้อย่างชัดเจนในแง่ของความสามารถเฉพาะใดๆ ที่สร้างข้อได้เปรียบที่ต้องการ” กล่าวอีกนัยหนึ่ง MDO เป็นหนทางสร้างผลกระทบด้วยเวลา และจังหวะที่ศัตรูไม่สามารถแข่งขันได้ เสนาธิการทหารอากาศ Gen. David L. Goldfein ได้ให้ความสำคัญต่อการบัญชาการและควบคุมแบบหลายโดเมน เพื่อเป็นแนวทางในการบรรลุการปฏิบัติการหลายโดเมนในกองกำลังร่วม

ในอดีตยุทธการเน้นโดเมนเดียว โดยใช้ผลที่ได้จากการประสานงาน และกระบวนการบัญชาการและควบคุม (C2) แบบเก่า แม้ว่าปฏิบัติการในทุกวันนี้จะถูกแยกชั้น (Layered) หรือจะประสานสอดคล้อง (Synchronized) แต่ยังไม่เป็นเชิงบูรณาการที่เดียวนัก อำนาจหน้าที่ของกองกำลังด้านอวกาศ/ไซเบอร์ ยังคงอยู่ที่ระดับยุทธศาสตร์หรือระดับชาติเป็นส่วนใหญ่ ในขณะที่หน่วยงานด้านปฏิบัติการทางอากาศ (Air Operations) ยังคงอยู่ที่ระดับยุทธการ ความสามารถในการรับรู้สถานการณ์ไม่ได้ถูกออกแบบมาเพื่อให้เกิด

ความเข้าใจสมรรถุณิรบที่ครอบคลุมทุกโดเมนในเชิงบูรณาการและโครงสร้าง C2 ก็ไม่เอื้อให้เกิดความคล่องตัวเพียงพอการประสานสอดคล้องนั้น

องค์กรต่างๆ เช่น Air Force Warfighting Integrating Capability : AFWIC กำลังมองหาวิธีที่จะใช้ความรวดเร็วในการตัดสินใจ และขนาดของกองกำลังที่จำเป็นกับคู่ต่อสู้ที่เท่าเทียมกัน วิธีการปฏิบัติทั่วไปที่จะเชื่อมต่อ Sensor กับส่วนประมวลผล Processor และส่งต่อไปยัง Shooter ที่เหมาะสมแล้วนั้น พวกเขายังทำงานเพื่อให้แน่ใจว่าเขามีระบบที่เหมาะสม และมีผู้คนพร้อมสำหรับการบัญชาการและควบคุมแบบหลายโดเมน (Multi-Domain C2) และ C2 ส่วนแยก (Distributed C2)

กองทัพพบได้สร้างหน่วยงานแห่งแรกเพื่อรวมการกำหนดเป้าหมายระยะไกล (Long-range targeting) การเจาะระบบ (Hacking) การรบกวน (Jamming) และด้านอวกาศ (Space) เพื่อสนับสนุนการส่งต่อไปยังการปฏิบัติการหลายโดเมน หน่วยนี้เรียกว่า I2CEWS ซึ่งย่อมาจากความสามารถทั้งหมดที่นำมาใช้ได้แก่ ข่าวกรอง (intelligence), สารสนเทศ (information), ไซเบอร์ (cyber), สงครามอิเล็กทรอนิกส์ (electronic warfare), และอวกาศ (space) หน่วยนี้ตั้งอยู่ที่ JB Lewis-McChord กรุงวอชิงตัน สำหรับใช้ตอบโต้ภัยคุกคามของจีน

สงครามลูกผสม (Hybrid Warfare)

ก่อนที่จะเข้าสู่การพิจารณาด้านโดเมนต่างๆ มีข้อสังเกตว่าหลักนิยมในปัจจุบันที่รัสเซียยึดถือ หนึ่งในคู่แข่งชั้นนำของสหรัฐฯ รัสเซียใช้สิ่งที่เรียกว่า “สงครามลูกผสม” (Hybrid Warfare) สงครามลูกผสมเป็นเพียงการรวมคำนิยามประเภทของสงครามที่กำหนดไว้ก่อนหน้านี้ : สงครามตามแบบ, สงครามนอกแบบ, สงครามการเมืองหรือสงครามข่าวสาร ภัยคุกคามแบบ Hybrid คือข้าศึกได้ผสมผสานใช้กำลังอาวุธตามแบบ ยุทธวิธีนอกแบบ การก่อการร้าย และพฤติกรรมที่เป็นอาชญากรเข้าด้วยกันในเวลา และพื้นที่การรบเดียวกันเพื่อให้ได้มาซึ่งวัตถุประสงค์ทางการเมือง ตามข้อมูลของ Dr. Francis Hoffman นักวิจัยที่มีชื่อเสียงจาก National Defense University เห็นว่า รัสเซียใช้ยุทธวิธีสงครามข่าวสารรูปแบบใหม่ เช่น สงคราม Meme Warfare เพื่อสร้างความสับสนวุ่นวายในหมู่ประชากร เช่น สหรัฐอเมริกา ซึ่งรัสเซียยังถูกระบุว่า มีแผนแทรกแซงการเลือกตั้งหลายครั้งทั่วโลก ประกอบด้วย ยูเครน ฝรั่งเศส และสหรัฐอเมริกา รวมถึงการใช้อาวุธนิวเคลียร์ทางยุทธวิธีในมุมมองภาพรวมที่เรียกว่า “สงครามลูกผสม” แนวทางของรัฐบาลทั้งหมดพยายามที่จะจัดการการรับรู้ของฝ่ายตรงข้าม กระบวนการตัดสินใจ และมีอิทธิพลต่อพฤติกรรมเชิงกลยุทธ์ อีกทั้งลดขนาดการใช้กำลังที่รุนแรง (เมื่อเทียบกับยุคสงครามอุตสาหกรรม)"

ข้อควรพิจารณาเกี่ยวกับโดเมน (Domain Considerations)

ตอนนี้เราได้กล่าวถึงวิวัฒนาการของการทำสงครามโดยสังเขปแล้ว วิธีที่เราบรรลุถึงความ ต้องการจำเป็น (Needs) ของการปฏิบัติการหลายโดเมน เราต้องพิจารณาโดเมนต่างๆ เพื่อสร้างรากฐานสำหรับการปฏิบัติการที่เกิดขึ้น โดเมนดั้งเดิม ได้แก่ อากาศ ทะเล พื้นดิน อวกาศ และไซเบอร์ ศาสตราจารย์ Jared Donnelly และ Jon Farley แห่งวิทยาลัยเสนาธิการทหารอากาศสหรัฐฯ (ACSC) ระบุว่านิยามของโดเมน

ดังกล่าวนั้น เราเห็นแล้วว่าโดเมนที่ไม่เป็นเชิงกายภาพ (Nonphysical Domains) เหล่านี้เริ่มส่งผลกระทบอย่างแท้จริงอย่างไรต่อภารกิจของเรา พวกเขาเสนอคำนิยามของโดเมนที่กำหนดโดย Jeffrey Reilly ผู้อำนวยการของ ACSC Multi-Domain Operations Strategists ที่เน้นว่าเป็น "พื้นที่การดำเนินการยุทธศาสตร์ระดับมหภาควิกฤติ (Critical macro maneuver space) ซึ่งการเข้าถึง หรือการควบคุมมีความสำคัญอย่างยิ่งยวดต่อเสถียรภาพในการปฏิบัติการและการปกครองที่กำหนดโดยภารกิจ" มันเป็นเพียงพื้นที่ที่เราต้องเข้าถึง และสามารถสร้างผลกระทบได้ และพื้นที่นี้ไม่จำเป็นต้องมองเห็นได้ทางกายภาพ

โดเมนด้านที่หกอยู่ระหว่างการพิจารณาเมื่อเร็ว ๆ นี้เนื่องจากการปฏิบัติการข่าวสารที่เพิ่มมากขึ้น และนั่นคือโดเมนพุทธิพิสัย (Cognitive Domain) Gen Robert Brown ผู้บัญชาการทหารบกสหรัฐฯ แปซิฟิกกล่าวว่า ขอบเขตความรู้ความเข้าใจ ไม่ควรถูกพิจารณาว่าเป็นแค่โดเมนหนึ่งเท่านั้น แต่ในความเห็นของเขาแล้ว โดเมนพุทธิพิสัย (โดเมนทางความคิด) เป็นโดเมนที่สำคัญที่สุด

โดเมนพุทธิพิสัยมีความสำคัญมากขึ้นเรื่อย ๆ ด้วยความก้าวหน้าด้านอวกาศ และเทคโนโลยีไซเบอร์ โดเมนนี้ได้เปิดให้ประชาชนได้รับข้อมูลข่าวสารมากขึ้น การทำให้ผู้ดูแลระบบแบบเดิมไร้ความหมาย และการทำให้ตัวแสดงที่เป็นรัฐหรือไม่ใช่รัฐ สามารถสร้างผลกระทบต่อโดเมนต่างๆ ได้ง่ายขึ้น ผู้ดูแลระบบแบบเดิมกำลังถูกแซงหน้าในการแบ่งปันข้อมูลโดยหน่วยอื่นๆ เช่น Twitter, Facebook และสื่อสังคมออนไลน์รูปแบบต่าง ๆ

ตัวอย่างที่ดีของการที่โดเมนพุทธิพิสัยกลายเป็นโดเมนที่สำคัญยิ่งขึ้นสามารถเห็นได้ในหนังสือ War in 140 Characters : How Social Media Is Reshaping Conflict in the Twenty-First Century ผู้เขียน David Patrikarakos อธิบายว่า Twitter เป็นแหล่งข้อมูลหลักที่สำคัญ และทันเวลาในความขัดแย้งรัสเซีย-ยูเครนได้อย่างไร เขาเป็นนักข่าวที่อยู่แนวหน้าของความขัดแย้ง และรับข่าวสารล่าสุดจากผู้ใช้ผ่านทาง Twitter อย่างสม่ำเสมอ มีข้อดีและข้อเสียเมื่อพูดถึงความเร็วของข้อมูลประเภทนี้ Patrikarakos เขียนเกี่ยวกับการเห็นรายงานที่แตกต่างกันอย่างมากจากฝ่ายเข้าข้างรัสเซียและฝ่ายที่เข้าข้างยูเครน ในฐานะนักข่าว เขากังวลเกี่ยวกับการเขียนข้อเท็จจริงของสถานการณ์ แต่เขากลับเห็นข้อมูลที่เป็นเท็จ “ทวีตซ้ำนับพันครั้ง” เขากล่าวว่า “นี่ไม่ใช่โฆษณาชวนเชื่อ แต่เป็นการสร้างความเป็นจริงขึ้นใหม่ และสื่อสังคมออนไลน์คือหัวใจของมัน” Patrikarakos ยังระบุด้วยว่าเขาเห็น “แนวร่วม” ที่ประกอบด้วยทหารที่ไม่ใช่หน่วยรบ และพลเรือนสภาพแวดล้อมการปฏิบัติงานของแนวร่วมหน้าใหม่เหล่านี้สามารถส่งผลกระทบอย่างแท้จริงต่อสมรรถนะได้

ศัตรูตระหนักภูมิานานแล้วว่าพวกเขาไม่สามารถเอาชนะในการสู้รบระหว่างทหารกับกองทัพสหรัฐฯ ได้ ดังนั้นวิถีทางแข่งขันรูปแบบอื่นจึงกลายเป็นหนทางที่จะเอาชนะขีดความสามารถยุทธโศภกรณ์ และอำนาจการรบได้ Patrikarakos กล่าวว่า “ฉันเริ่มเข้าใจว่าฉันติดกับอยู่ในสองสงคราม: หนึ่งต่อสู้บนพื้นดินด้วยรถถังปืนใหญ่ และสงครามข่าวสารที่ขยายใหญ่ขึ้นเรื่อย ๆ ไม่ใช่แค่เฉพาะที่ผ่านสื่อสังคม (Social Media) และบางทีอาจจะขัดกับสามัญสำนึกที่ว่า “ผู้ชนะสงครามเป็นคนที่ใช้ถ้อยคำและเล่าเรื่องเก่งมากกว่าคนที่มีความรู้ที่ทรงพลังที่สุด”

ตัวอย่างของวิธีที่สื่อสังคมออนไลน์สามารถเปลี่ยนสมรรถนะสามารถพบได้ในบทความเรื่อง “With Just \$60 and Internet Access, Researchers Found and Tracked NATO Troops and Even Tricked

Them into Disobeying Orders.” บทความนี้แสดงให้เห็นถึงความสำคัญของผู้บังคับบัญชาที่ตระหนักถึงภาพปฏิบัติการทั้งหมด นักวิจัยของ NATO’s Strategic Communications Center of Excellence ใช้ข้อมูล Open-Source - สื่อสังคมเป็นหลัก—เพื่อพิสูจน์ทราบทหาร 150 นาย ระบุที่ตั้งกองพันหลายหน่วย ติดตามการเคลื่อนไหวของกองทหาร และแม้กระทั่งชักชวนให้ละทิ้งงาน และเข้าร่วมใน ‘พฤติกรรมที่ไม่พึงประสงค์’ อื่นๆ ในระหว่างการซ้อมรบทางทหาร” คำแถลงระบุว่านักวิจัยเป็นสมาชิกทีมสีแดง แต่เข้าถึงสามารถเป็นใครก็ได้ที่มีการเข้าถึงอินเทอร์เน็ต และเป้าหมาย

เพื่อตอบสนองต่อสภาพแวดล้อมที่เปลี่ยนแปลงตลอดเวลาดังกล่าว เมื่อเร็วๆ นี้กองทัพอากาศสหรัฐฯ ได้จัดตั้งกองกำลังทางอากาศที่ 16 รองรับการสงครามสารสนเทศจำนวนมาก คำสั่งใหม่จะ “รวมข่าวกรองจากหลายแหล่ง การเฝ้าระวัง และการลาดตระเวน สงครามไซเบอร์ สงครามอิเล็กทรอนิกส์ และความสามารถในการปฏิบัติการด้านข้อมูลครอบคลุมทั่วทุกความขัดแย้ง เพื่อให้แน่ใจว่ากองทัพอากาศจะยังมีความรวดเร็ว รุนแรง และการบูรณาการอย่างเต็มที่ทั้งในการแข่งขันประชันและสงคราม

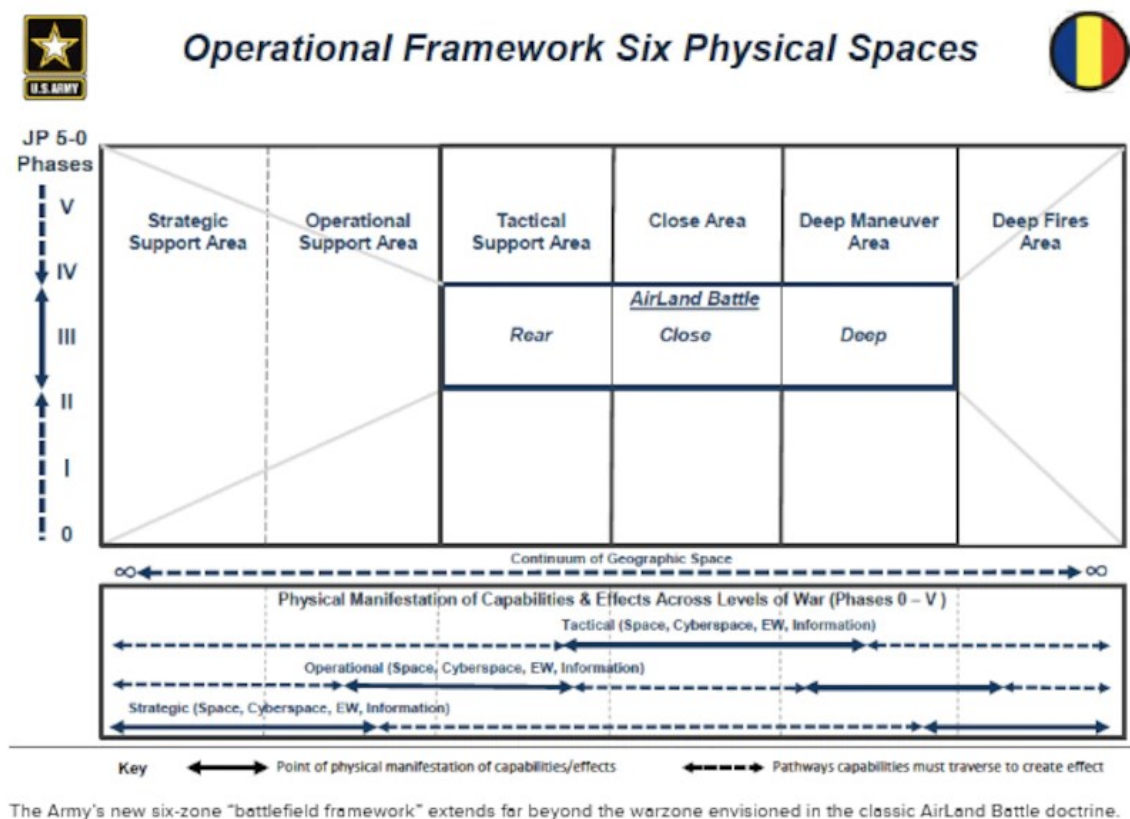
การขยายตัวของโดเมนไซเบอร์ยังได้รับการกล่าวถึงในเวทีหลายแห่งเพื่อเปลี่ยนเป็นโดเมนด้านแม่เหล็กไฟฟ้า (Electromagnetic Spectrum : EMS) Gen James M. Holmes ผู้บัญชาการกองบัญชาการรบทางอากาศ (Air Combat Command : ACC) กล่าวในการประชุมเทคโนโลยีสารสนเทศและไซเบอร์สเปซของกองทัพอากาศ (AFITC) ปี 2019 ว่าอยู่ระหว่างการพิจารณาให้เปลี่ยนคำว่า Cyberspace เป็น EMS เมื่อพูดถึงโดเมนที่ ACC ครอบครอง การเปลี่ยนแปลงนี้เกิดจากการที่ไซเบอร์เป็นส่วนย่อยของสิ่งที่ใหญ่กว่าซึ่งใช้สร้างผลกระทบต่างๆ

สมรภูมิที่กำลังขยายตัว (Expanding Battlefield)

แนวคิดต่อไปที่จะถูกถกเถียงคือการขยายสนามรบ เนื่องจากเทคโนโลยีใหม่ ๆ ที่สหรัฐฯ มีในปัจจุบัน ผู้มีบทบาทของรัฐ และที่ไม่ใช่รัฐสามารถส่งผลกระทบอย่างมากต่อเทคโนโลยี และการปฏิบัติการทางทหารจากทุกที่ในโลก เทคโนโลยีที่มีราคาถูก และพร้อมใช้งานสำหรับทุกคน ไม่เพียงแต่เข้าถึงจะส่งผลกระทบต่อการปฏิบัติการภายในยุทธบริเวณเท่านั้น แต่ตอนนี้เข้าถึงสามารถโจมตีฐานที่ตั้งหลักของเรา และส่งผลกระทบลุกล้ำต่อพื้นที่รับผิดชอบ (Area Of Responsibility : AOR) Patrikarakos อธิบายสนามรบที่ถูกขยายว่า :

กองกำลังนอกแบบอาจโจมตีในพื้นที่สีเทาที่กองทหารทั่วไปจะทำสงครามอย่างเป็นทางการ หากการโจมตีระลอกแรกอาจเกิดจากตัวแทน เช่น กบฏยูเครนที่ได้รับการสนับสนุนจากรัสเซีย กองกำลังไม่ทราบฝ่าย เช่น Little Green Men ในแหลมไครเมีย หรือเรือประมงรัฐของจีนในทะเลจีนใต้ หน่วยงานเสริมที่ไม่ใช่ทหาร เช่น หน่วยยามฝั่งจีน หรือ หน่วย 'Lone Wolf' ที่ได้รับแรงบันดาลใจจากไซเชยลมีเดียแต่ไม่มีความเกี่ยวข้องอันใดกับฝ่ายตรงข้าม การโจมตีทางไซเบอร์อาจมีสาเหตุที่ยากจะเข้าใจ และอาจมีการเตรียมการอย่างรอบคอบเป็นเวลาหลายเดือนหรือหลายปี เพื่อส่งผลกระทบในไม่กีวินาที

วิทัศน์ “การพัฒนาของภัยคุกคามต่อการปรับปรุงกองทัพในโลกที่ซับซ้อน” ผลิตโดยกองทัพบกสหรัฐฯ อธิบายอย่างละเอียดว่าศัตรูสามารถส่งผลกระทบต่อการใช้งานได้อย่างไร แม้กระทั่งก่อนออกจากฐานที่ตั้ง หากศัตรูสามารถหยุดกองทหาร หรือทำให้ขวัญเสียตั้งแต่ก่อนที่กองทัพจะออกจากสหรัฐฯ พวกเขาคงจะไม่มีทางเข้าสู่ยุทธบริเวณทั่วโลก หรือหากเข้าไปได้ก็จะเสียเปรียบอย่างใหญ่หลวง



ภาพที่ 1 Army's Operational Framework Six Physical Spaces.

ที่มา : David G.Perkins, "Multi-Domain Battle: Driving Change to Win in the Future," Military Review (July–August 2017), 10.

ภาพที่ 1 นำมาจาก "กรอบปฏิบัติการเชิงกายภาพ" ของกองทัพบกสหรัฐฯ มันแสดงให้เห็นแนวคิดดั้งเดิมของความเข้าใจในพื้นที่รบจากฝ่ายกองกำลังสีน้ำเงินเริ่มจาก "พื้นที่สนับสนุนยุทธศาสตร์" ถึง "พื้นที่สนับสนุนยุทธวิธี" ในขณะที่พื้นที่จาก "พื้นที่ระยะใกล้" ถึง "พื้นที่การยิงแนวลึก" เป็นฝ่ายกองกำลังสีแดง สิ่งที่ต้องตระหนักคือเทคโนโลยีใหม่ๆ "ที่หลบภัย" ของค่ายทหาร หรือเพียงแค่การอาศัยอยู่ในสหรัฐอเมริกา ก็จะไม่ "ปลอดภัย" อีกต่อไป ไม่ว่าจะเป็นผู้กระทำโดยรัฐหรือไม่ใช่รัฐ ทั้งสองมีหนทางที่จะบรรลุผลที่จะทำให้เราเสียหายได้ ตัวอย่างบางส่วนเช่น :

- หน่วยงานของรัฐโจมตีโครงสร้างพื้นฐานที่สำคัญจากทั่วโลก

- ตัวแสดงที่ไม่ใช่รัฐโจมตีระบบอวกาศของเรา หรือก่อวินาศกรรม GPS
- ทีม Lone Wolf บินโดรนพาณิชย์ติดระเบิดเหนือฐานทัพทหาร และระเบิดพื้นที่/อาวุธยุทโธปกรณ์ขนาดใหญ่ เช่นที่เห็นในยูเครนในปี 2560
- กลุ่มโฆเซียลิสต์กลุ่มรัฐอิสลามในอิรักและซีเรีย (ISIS) โจมตีระบบประปาในสหรัฐอเมริกา

กองทัพต้องเริ่มมองว่าสถานที่ปฏิบัติงานไม่ใช่แค่เพียง "พื้นที่สนับสนุนยุทธศาสตร์" เท่านั้น แต่รวมถึง "พื้นที่ระยะใกล้" ที่ต้องได้รับการปกป้องอย่างใกล้ชิดด้วย ยิ่งไปกว่านั้นพวกเขายังต้องมองว่าชุมชนมีความสำคัญในการร่วมกันป้องกันภัยด้วย เพราะการโจมตีจากศัตรูไปยังเป้าหมายเหล่านั้น สามารถส่งผลกระทบต่อการทำงานของทางทหารได้เช่นกัน

ตัวอย่างเช่น ศัตรูสามารถกำหนดเป้าหมายโจมตีระบบประปาภายในชุมชนของเรา หรือทำลายโครงข่ายระบบไฟฟ้า จึงเป็นความสำคัญอย่างยิ่งในการรักษาความปลอดภัยโครงสร้างพื้นฐาน และทรัพยากรที่สำคัญผ่านกระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) อย่างไรก็ตาม แนวความคิดในการมองที่ตั้งมาตุภูมิของเราจะกลายเป็นส่วนหนึ่งของยุทธวิธีใหม่ ๆ โดยเฉพาะอย่างยิ่งสำหรับกองทัพอากาศ

การปฏิบัติการหลายโดเมนเชิงรับ

ฐานบิน Wright Patterson AFB (WPAFB) รัฐโอไฮโอ มุ่งเน้นไปที่ MDC2 ในเชิงรับ ในขณะที่หน่วยในกองทัพอากาศส่วนใหญ่มุ่งเน้นไปที่การบัญชาการและควบคุม MDO เชิงรุกในระดับปฏิบัติการ (MDC2)

กองบินที่ 88 ภายใต้การบังคับบัญชาของ Col Thomas P. Sherman กำลังปรับเปลี่ยนโครงสร้างของกองบินที่อาจดูเหมือนว่ารองรับ MDC2 เชิงรับที่ระดับกองบัญชาการ เช่นเดียวกับศูนย์ปฏิบัติการทางอากาศที่อาศัยโครงสร้าง C2 เพื่อรองรับการปฏิบัติการสงครามทางอากาศ การรักษาความปลอดภัยของกองบัญชาการต้องอาศัยระบบ C2 ที่เป็นที่ยอมรับซึ่งมีเอกภาพในการบัญชาการภายใต้ผู้บังคับบัญชาคนเดียว Col Winn ในฐานะผู้บัญชาการกลุ่มปฏิบัติการภารกิจที่ 88 (เฉพาะกาล) กล่าวว่า "กองทัพอากาศต้องมองเห็นว่ากองบัญชาการหน่วยมีคุณลักษณะเช่นเดียวกับเรือบรรทุกเครื่องบินที่มีความสามารถที่สามารถปล่อยเครื่องบินออกไปปฏิบัติการได้ ประเทศของเรากำลังอยู่ในสถานะที่ข้อมูลองค์ความรู้ที่รวดเร็ว และกองบัญชาการเป็นสิ่งสำคัญยิ่งยวดเมื่อมันปรับใช้ในลำเลียงกำลังพล และยุทธโธปกรณ์ไปยังพื้นที่ปฏิบัติการ"

ความพยายามที่ WPAFB เป็นทวีคูณ: มันเกี่ยวข้องกับโครงสร้างองค์กรใหม่ที่เราเรียกว่า Mission Operations Group เช่นเดียวกับการหลอมรวมหน้าที่ใหม่สำหรับ C2 ที่เรียกว่า Installation Command and Control Cell

ปัจจุบัน WPAFB กำลังดำเนินการ "90 day sprint" กลุ่มงานการสื่อสารที่มีอยู่ได้เปลี่ยนชื่อใหม่เป็นกลุ่มปฏิบัติการภารกิจ (เฉพาะกาล) โดยมีฝูงบิน 2 ฝูงบินที่ได้รับมอบหมาย (ฝูงบินสนับสนุนการปฏิบัติการที่ 88 และฝูงบินสื่อสารที่ 88) ฝูงบินเพิ่มเติมอีก 2 ฝูง (กองทหารรักษาการณ์ที่ 88 และกองวิศวกรรมโยธาที่ 788) และเจ้าหน้าที่ฝ่ายอำนวยการอีก 1 หน่วย (งานการป้องกันข่าวสารของกองบิน) การจัดตำแหน่งองค์กรนี้

จะสร้างกลุ่มที่มีหลายโดเมนหนึ่งกลุ่ม (โดเมนทางอากาศ โดเมนทางบก และโดเมนไซเบอร์) โดยมุ่งเน้นที่การคุ้มครอง และป้องกันกองบัญชาการ เพื่อให้มั่นใจว่าหน่วยที่ตั้งทางทหารจะปลอดภัย มั่นคง และยืดหยุ่น คล่องตัวพอที่จะปกป้องผู้คน โครงสร้างพื้นฐานที่สำคัญ และข่าวสารสารสนเทศ หลังจากเร่ร่อนนี้ กองบินจะประเมินผล และพิจารณาหนทางปฏิบัติต่อไป

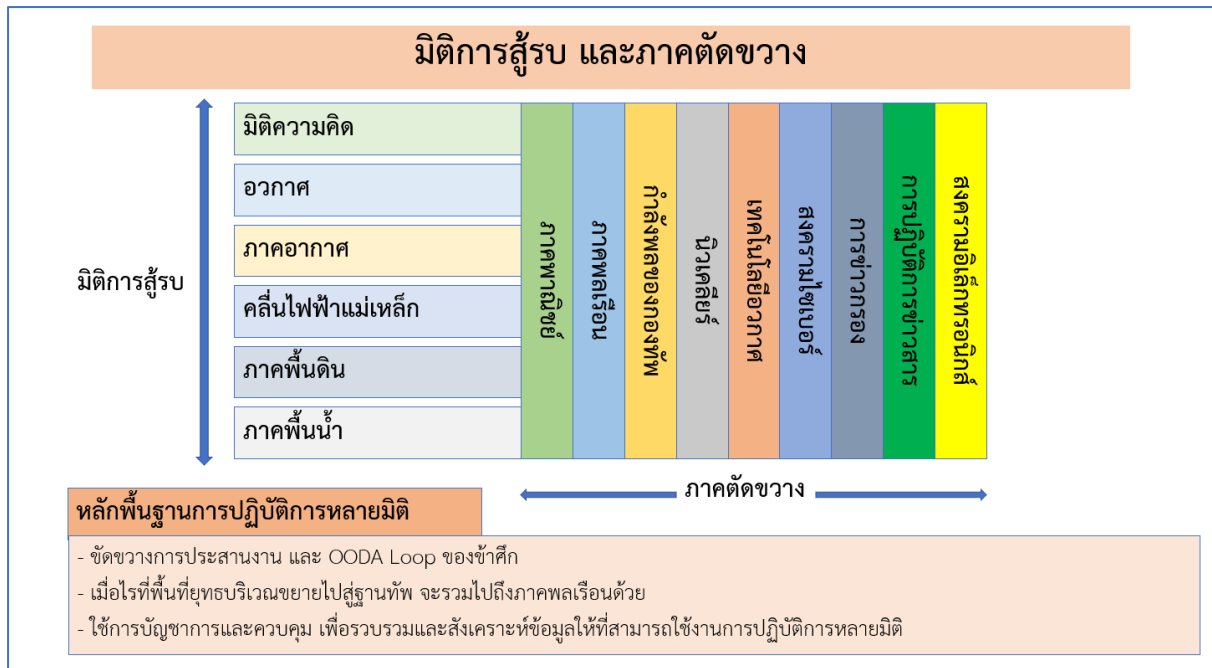
WPAFB ทำการทดลองต่อมาคือการหลอมรวมศูนย์ปฏิบัติการของฐานทัพทั้งหมด เช่น ศูนย์ปฏิบัติการป้องกันฐานบิน, หน่วยปฏิบัติงานการจัดการสนามบิน, หน่วยดับเพลิง และ ศูนย์ปฏิบัติการข่าวกรองไซเบอร์ เพื่อสร้างการรับรู้สถานการณ์ทั้งหมดของหน่วยจัดตั้ง ผู้บังคับการกองบินต้องการข้อมูลที่ถูกต้อง และทันท่วงทีเกี่ยวกับสิ่งที่เกิดขึ้นในฐานทัพต่างๆ ตามที่ปรากฏ WPAFB เป็นสถานที่ที่สมบูรณ์แบบในการฝึกวิธีการโครงสร้าง C2 ใหม่ เนื่องจากพวกเขาจัดกิจกรรมระดับสูง เช่น Air Force Marathon และ Corona Conference ในแต่ละปี ซึ่งต้องมีการรักษาความปลอดภัย และการประสานงานแบบบูรณาการองค์ประกอบ C2 นี้มาจากการประชุม Air Force Installation Management และการประชุม Installation Weapons and Tactics Conference 2019 ของศูนย์สนับสนุน นอกจากนี้ WPAFB ยังเป็นหนึ่งในห้าฐานทัพที่นำร่องแนวคิด Command and Control Cell ซึ่งได้รับการบรรยายสรุปต่อหัวหน้าฝ่ายเสนาธิการของกองทัพอากาศมาแล้ว

ความคิดริเริ่มเหล่านี้ที่ WPAFB กำลังผลักดันให้เกิด MDC2 เชิงรับสำหรับกองทัพอากาศ ในโลกอันซับซ้อนที่มีวิวัฒนาการของภัยคุกคามแบบหลายโดเมน ผลลัพธ์ของการทดลองเหล่านี้จะช่วยปรับแต่งอนาคตของการป้องกันฐานทัพต่อไป

กรอบการปฏิบัติการหลายโดเมน

กรอบงานต่อไปนี้จะถูกสร้างขึ้นเพื่อช่วยระบุภาคตัดขวางใดที่ส่งผลต่อโดเมนทั้งหมด นับตั้งแต่มีการสร้าง ได้มีการนำไปประยุกต์ใช้งานหลากหลายที่ได้รับการพิสูจน์แล้วว่าเป็นประโยชน์ต่อการทำความเข้าใจแนวคิด MDO ที่อาจเป็นประโยชน์สำหรับผู้บังคับบัญชา และนักวางแผนในระดับต่างๆ ของการบังคับบัญชา นอกจากนี้ยังได้ดัดแปลงเป็นแผนภูมิที่ใช้เพื่อช่วยให้ความรู้แก่นักศึกษาหลักสูตรป้องกันประเทศ ซึ่งสอดคล้องกับความคิดของ Gen Goldfein ที่กล่าวไว้ว่า MDO เป็นการป้องกันรูปแบบใหม่

ในภาพที่ 2 โดเมนต่างๆ เป็นแถบแนวนอน และรวมถึงโดเมนความรู้ความนึกคิดด้วย ในขณะที่โดเมนไซเบอร์จะแสดงเป็นสเปกตรัมแม่เหล็กไฟฟ้าที่ใหญ่กว่า ภาคตัดขวางเป็นการรวมกันของหน่วยงานทางทหาร รัฐบาล และภาคเอกชนในระดับท้องถิ่น ระดับรัฐ และระดับรัฐบาลกลาง ภาคส่วนเหล่านี้เกินขอบเขตหรือโดเมนทางการทหารแต่ดั้งเดิมอย่างสิ้นเชิง ภาคตัดขวางเหล่านี้รวมถึงภาคพาณิชย์ ภาคพลเรือน บุคลากรทางทหาร เทคโนโลยีอวกาศ ไซเบอร์ นิวเคลียร์ ข้าราชการ ปฏิบัติการข่าวสาร และสงครามอิเล็กทรอนิกส์ โดยที่แต่ละโดเมนตัดกับภาคตัดขวางทุกจุด



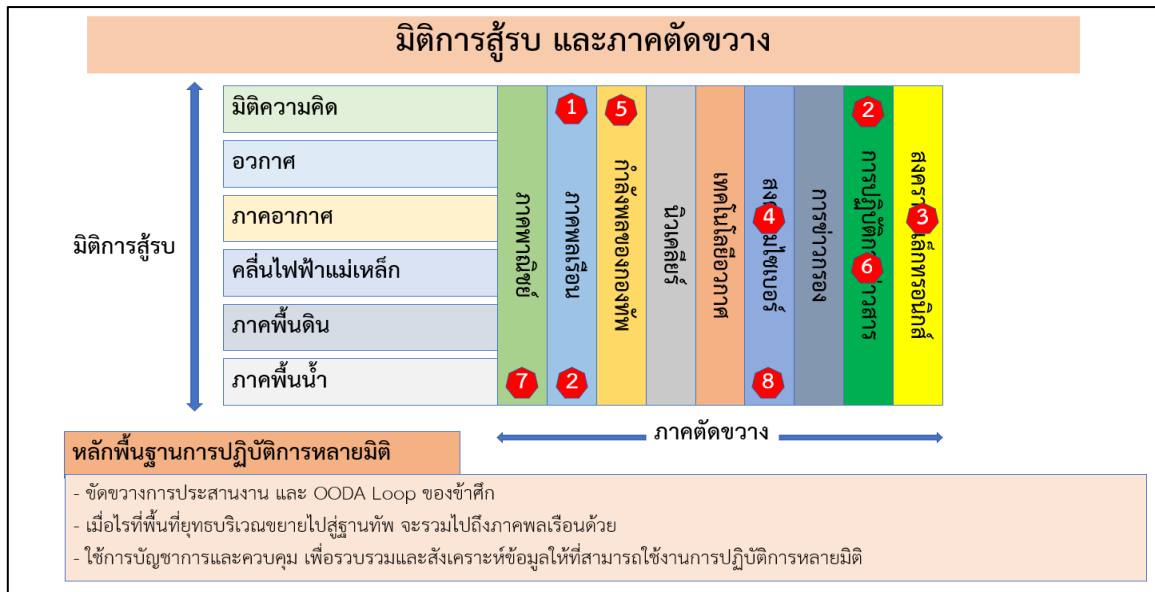
ภาพที่ 2 MDO Framework ที่แสดงภาพโดเมนการสู้รบและการตัดขวางภาคส่วนที่มีผลกระทบต่อพวกเขา

ผู้บังคับบัญชาหรือผู้วางแผนสามารถดูรอบการทำงานนี้ด้วยความคิดที่เป็นเชิงรุก และถามว่าเราจะสร้างผลกระทบในจุดตัดต่างๆ ได้อย่างไร ในลักษณะนี้ เราสามารถสร้างความยุ่งยากให้กับข้าศึกในโดเมนต่างๆ ส่งผลให้กระบวนการตัดสินใจของศัตรูช้าลง การใช้รอบการทำงานที่เรียบง่าย เช่น รูปที่ 2 สามารถช่วยให้นักวางแผนหลุดออกจากกรอบเดิม และพิจารณาเป้าหมายที่เป็นไปได้ทั้งหมดด้วยวิธีการโจมตีที่หลากหลาย การเติบโตมาจากวิชาชีพหรือเหล่าทัพบางอย่างมีแนวโน้มที่จะติดอยู่ในกรอบความคิดดั้งเดิมนั้น แต่หากผ่านกรอบความคิดนี้ไปได้จะเป็นการเปิดโอกาสสร้างทางเลือกอื่นๆ ให้กับผู้บังคับบัญชาและนักวางแผน

ในทำนองเดียวกัน เมื่อมองในเชิงรับ เราอาจพิจารณาว่าเราอ่อนแอในจุดใดบ้าง ตัวอย่างเช่น ที่ WPAFB กำลังฝึกการปฏิบัติการหลายโดเมนเชิงรับ มีวัตถุประสงค์ที่จะยกเลิกการฝึก Active Shooter แบบดั้งเดิม และสร้างบางสิ่งที่เตรียมรองรับการเปลี่ยนแปลงทั้งหมดที่ได้พบเห็นในสภาพแวดล้อมปฏิบัติการ รวมทั้งสงครามที่ยังเป็นโซน "สีเทา" ประเด็นทั่วไปประการหนึ่งที่เกิดขึ้นขณะดำเนินการตามกระบวนการนี้คือหลายคนที่เกี่ยวข้องไม่เข้าใจการปฏิบัติการหลายโดเมน หรือการเปลี่ยนแปลงในสภาพแวดล้อมการปฏิบัติการ การศึกษาต้องเป็นก้าวแรกที่จะดำเนินการเพื่อทะลุมะลวงปัญหานี้

กรอบการทำงานนี้สามารถนำไปใช้ในระดับยุทธวิธี หรือระดับกองบัญชาการได้เช่นที่กล่าวไว้ข้างต้น และยังสามารถนำไปใช้ในระดับยุทธการได้อีกด้วย นักวางแผนสามารถใช้กรอบการทำงานในการพิจารณาวัตถุประสงค์ของการฝึกปฏิบัติในทุกโดเมน และในทุกภาคส่วน

ตัวอย่างต่อไปแสดงให้เห็นว่าโมเดลนี้ได้รับการดัดแปลงอย่างไรสำหรับ 13O Initial Skills Training ที่ Hurlburt Field รัฐฟลอริดา ตัวอย่างนี้ให้ไว้สำหรับผู้ที่จะวางแผนใช้พิจารณาทางเลือกในเชิงรุกและเชิงรับ



นักวางแผนจำเป็นต้องคิดทั้งเชิงรุก และเชิงรับ	
1	อิทธิพลของความคิดเห็นของประชาชนเกี่ยวกับความชอบธรรมของการเลือกตั้ง เราถูกโจมตีระหว่างการเลือกตั้งประธานาธิบดีครั้งล่าสุดหรือไม่? เราคาดหวังรับดีกว่าไหม? เราสามารถโน้มน้าวการเลือกตั้งต่างประเทศเพื่อขับไล่พรรคฝ่ายค้านได้หรือไม่? นี่เป็นการใช้โดเมนที่ดีหรือไม่? ประเด็นทางกฎหมายและจริยธรรมอื่นใดที่มีการอภิปรายในเรื่องนี้?
2	อากาศยานใดสามารถรบกวาดเรดาร์ข้าศึก ส่งผลทำให้ปฏิบัติการอื่น ๆ เกิดขึ้นได้โดยไม่มีใครสังเกต เราจะเตรียมและป้องกันการโจมตีทางสงครามอิเล็กทรอนิกส์ได้อย่างไร?
3	การปรับเนื้อหาเว็บไซต์ข่าวออนไลน์เพื่อเบี่ยงเบนความสนใจของผู้อ่านจากปัจจัยพื้นฐานของกลุ่ม มีเว็บไซต์ของเราที่ถูก "เจาะระบบ" หรือไม่? เราเคยทำสิ่งนี้กับศัตรูหรือไม่? เราสามารถส่งผลกระทบต่อโดเมนคลื่นแม่เหล็กไฟฟ้า และโดเมนทางความคิดผ่านการปฏิบัติการข่าวสารหรือไม่?
4	การเคลื่อนย้ายกองเรือ Carrier Strike Group (CSG). ประชาชนชาวอเมริกันมีปฏิกิริยาอย่างไรกับการเคลื่อนไหวกองเรือบรรทุกเครื่องบินจีน เราหวังว่าจะมีอิทธิพลต่อความคิดของประชากรศัตรูได้อย่างไร ถ้าเราย้าย CSG ใกล้ชายฝั่งของใครบางคน?
5	เราจะใช้ Social media ให้มีผลต่อกำลังพลทหารอย่างไร? ข่าวสารอะไรสามารถให้เราเรียนรู้จากการโพสต์หรือการโต้ตอบของพวกเขา? เราสามารถสร้างผลกระทบต่อสนามรบผ่านสื่อสังคมออนไลน์ซึ่งมีเป้าหมายอยู่ที่ตัวกำลังพล
6	จะเกิดอะไรขึ้นถ้าเราไม่มีเวลาพอที่จะเคลื่อนย้ายกองเรือ Carrier Strike Group เราสามารถยับยั้งจากไหนได้บ้าง? เราจะอุดช่องโหว่ในระบบเราได้หรือไม่?
7	อะไรเกี่ยวกับอากาศยาน? เราสามารถขโมย ลดระดับ หรือทำลายเครื่องบินข้าศึกผ่านไซเบอร์ได้หรือไม่?
การนำแต่ละประเด็นมาใช้โดยลำพังสามารถสร้างผลลัพธ์ได้ แต่จะไม่ผสมผสาน ผลลัพธ์เหล่านั้นจะไม่หลอมรวมเป็นหนึ่งเดียวกัน	

ภาพที่ 3 กรอบการทำงาน MDO ในตัวอย่างที่เป็นแถบจุดตัดสีแดง

สุดท้ายนี้ เราอาจดูตัวอย่างว่าภาคพาณิชย์มีผลกระทบต่อโดเมนอื่นๆ และความพร้อมทางทหารของเราอย่างไร? โดยการตรวจสอบเหตุการณ์การโจมตีทางอินเทอร์เน็ตของ NotPetya ต่อกลุ่มบริษัทเดินเรือที่ใหญ่ที่สุดในโลก “A.P. Moller-Maersk” บริษัทยักษ์ใหญ่ที่มีพนักงาน 80,000 คนทั่วโลก ในปี 2560 บริษัทได้รับผลกระทบจาก “Ransomware” ที่เป็นสาเหตุให้ท่าเรือ 76 แห่งทั่วโลก และเรือเดินทะเลเกือบ 800 ลำ รวมถึงเรือคอนเทนเนอร์ที่บรรทุกสินค้าหลายสิบล้านตัน ซึ่งคิดเป็นเกือบหนึ่งในห้าของความสามารถในการขนส่งทั่วโลกเป็นอัมพาตอยู่ในน้ำ” กระทรวงกลาโหมควรกังวลอย่างมากเกี่ยวกับการโจมตีครั้งนี้ ในขณะที่เรามักใช้บริษัทพลเรือนเช่น Maersk ทั้งในยามสงบ และในยามสงครามเพื่อส่งเสบียงของเราไปทั่วโลก มีบทเรียนมากมายให้เรียนรู้จากการโจมตีครั้งนี้เพื่อการเตรียมไม่เพียงแต่ระบบทหารของเราเท่านั้น แต่ยังเตรียมบริษัทสำคัญเหล่านั้นที่จะนำไปใช้เมื่อยามสงครามเริ่มต้นขึ้น



(US Air Force photo by Eric Dietrich)

ภาพที่ 4 การอภิปราย MDO. Maj Gen Chance Saltzman (คนที่สองจากด้านซ้าย) รองผู้บัญชาการของศูนย์บัญชาการกองกำลังทางอากาศสหรัฐฯ อภิปรายการบูรณาการขีดความสามารถการปฏิบัติการหลายโดเมนและอวกาศในการสมมนาการสงครามทางอากาศของสมาคมกองทัพอากาศ (The Air Force Association’s Air Warfare Symposium) Orlando, Florida. 27 ก.พ. 2020

บทสรุป

กองทัพสหรัฐมักกล่าวถึง "การเอาชนะทั้งหัวใจและจิตใจ" (winning hearts and minds) แต่มีแนวโน้มที่จะเอนเอียงไปทางวิธีการทำสงครามแบบ "เอาจรวดไปจ่อหัว" (warheads on foreheads) เหตุผลนี้อยู่ในกระบวนการที่ดำเนินการยุทธโดยการปล่อยระเบิดลงไปถึงเป้าหมายง่ายกว่าการประสานงานอย่างดีเยี่ยมของการปฏิบัติการข่าวสาร ผลที่เกิดขึ้นล้วนเป็นชัยชนะครั้งยิ่งใหญ่ด้วยเช่นกัน อย่างไรก็ตามผู้เชี่ยวชาญการต้องตระหนักถึงศักยภาพของตัวเลือกที่ไม่ใช่กำลังทหารเช่นเดียวกับตัวเลือกที่ใช้กำลังทหาร ปัญหาคือไม่มีกระบวนการหรือเทคโนโลยีเพียงพอสำหรับการบูรณาการเรื่องนี้ จำเป็นต้องมีการทบทวนและปรับปรุงวงจรการกำหนดเป้าหมายร่วม และสกัดการโจมตีเพื่อรวมการบูรณาการอย่างราบรื่นของโดเมนใหม่ๆ เพื่อรองรับความขัดแย้ง MDO ในอนาคต เราจำเป็นอย่างยิ่งที่จะ "ปฏิวัติ DOTMLPFP" อีกเพื่อทำให้การริเริ่มในเรื่อง MDC2 ในการสนับสนุน MDO ของ Gen Goldfein บรรลุผลอย่างแท้จริง

การทำความเข้าใจกับสภาพแวดล้อมในปัจจุบัน และวิธีการแผ่ขยายโดเมนต่างๆ จะช่วยให้เราตัดสินใจได้ดีขึ้น และนำเราไปสู่เทคโนโลยีที่เหมาะสมในการหลอมรวมเศษชิ้นส่วนที่แตกต่างกันเหล่านี้เข้าด้วยกัน แต่ละโดเมนสามารถมีผลอย่างมหาศาลต่อความยอดเยี่ยมของโดเมนอื่นๆ แต่ขั้นตอนแรกคือการคำนึงถึงโดเมนที่เพิ่มเติมขึ้นมาในเกมนี้ การมองที่กรอบงานใหม่ๆ เพื่อให้เห็นว่าโดเมนต่างๆ และภาคตัดขวางมีปฏิสัมพันธ์กันอย่างไร จะช่วยระบุวัตถุประสงค์ของ MDO ในการฝึกสำหรับสงครามครั้งต่อไป MDO ต้องการความเข้าใจในขอบเขตของโดเมนแต่ละโดเมน และความต้องการที่จะเชื่อมต่อช่องว่างกับโดเมนอื่นเพื่อให้ได้มาซึ่งขีดความสามารถเหนือกว่าข้าศึกที่จะกระทำเช่นเดียวกัน มันไม่จำเป็นต้องมีการปรับโครงสร้างองค์กรครั้งใหญ่ แต่ต้องทบทวนการศึกษาของกองทัพ นายทหารแต่ละคนโดยเฉพาะนักวางแผน จำเป็นต้องขยายมุมมองของตนให้กว้างขวางครอบคลุมโดเมนของพวกเขา นอกจากนี้ยุทธวิธีและการปฏิบัติการที่ยึดโยงความต้องการของภาคส่วนต่างๆ ที่ดีกว่าเดิม เพื่อการตอบสนองต่อเหตุการณ์อย่างรวดเร็วและไม่หยุดนิ่ง

กระบวนการที่ผ่านมาของการศึกษาร่วมมุ่งเน้นไปที่การบูรณาการทางบก ทะเล อากาศ และอวกาศ กระบวนทัศน์ใหม่ต้องพิจารณาการเข้าถึงแต่ละโดเมน และใช้ขีดความสามารถที่เกิดผลครอบคลุมโดเมนอื่นๆ พร้อมเพียงกัน กองทัพต้องสร้างปัญหาที่ซับซ้อนให้กับข้าศึก ในขณะที่ต้องรับมือกับกลยุทธ์ใหม่ๆ ที่แสดงให้เห็นในสถานการณ์ความขัดแย้งทั่วโลกในทุกวันนี้

เราต้องสำรวจต่อไปว่าฐานที่ตั้งมีความเสี่ยงและมีคุณค่าเพียงใด? และจะสนับสนุนชุมชน และหน่วยในพื้นที่รับผิดชอบในสนามรบที่กว้างขวางขึ้นอย่างไร? MDO ต้องการความเข้าใจในขอบเขตของโดเมนแต่ละโดเมน และความต้องการที่จะเชื่อมต่อช่องว่างกับโดเมนอื่นเพื่อให้ได้มาซึ่งขีดความสามารถเหนือกว่าข้าศึกที่จะกระทำเช่นเดียวกัน สหรัฐฯ สามารถรักษาความได้เปรียบในสนามรบด้วยการขยายพื้นที่การรบของข้าศึกและส่งผลกระทบต่อนักสู้ในแต่ละโดเมน อย่างไรก็ตามทางทหารยังต้องรักษาท่าทีการป้องกันที่ครอบคลุม MDC2 และปกป้องฐานที่ตั้ง และชุมชนของเรา การปฏิบัติการนี้อาจต้องมีการปรับโครงสร้างหรือคิดใหม่ แต่ท้ายที่สุดผู้ใดก็ตามที่ปรับตัวได้ คือผู้ที่มีชัยในสงคราม

เกี่ยวกับผู้เขียน

Maj Kimber Nettis, USAF ตำแหน่งรองผู้อำนวยการโครงการ Cyber Professional Continuing Education Program ใน School of Strategic Force Studies ที่ Wright-Patterson AFB รัฐโอไฮโอ เธอสำเร็จการศึกษาศิลปศาสตรมหาบัณฑิตสาขาความมั่นคงแห่งมาตุภูมิ และศิลปศาสตรมหาบัณฑิตสาขาพันธกิจคริสเตียน (MA, American Military University; MA, Liberty University)

อ้างอิง

Maj Kimber Nettis. (2020). **Multi-Domain Operations: Bridging the Gaps for Dominance**, สืบค้นเมื่อ 25 ตุลาคม 2564. จาก. <https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2109784/multi-domain-operations-bridging-the-gaps-for-dominance/>