ประเด็น ยุทธวิธีทางทหารฉบับที่ T26	8 มิ.ย. 68	วิทยาลัยการทัพบก
ประเด็น สงครามรัสเซีย - ยูเครน	ปฏิบัติการใยแมงมุม “Operation Spider’s Web”	
ประเด็นสำคัญ	- สถานการณ์การรบรัสเซีย – ยูเครนในปัจจุบัน - Scenario การปฏิบัติการ “Operation Spider’s Web” - ผลกระทบในด้านขีดความสามารถการป้องกันและจิตวิทยา - การปฏิบัติทางยุทธวิธีส่งผลต่อยุทธศาสตร์ได้โดยตรงในทุกพื้นที่ - บทเรียนที่สามารถนำมาประยุกต์ใช้กับประเทศไทยในการป้องกันการก่อวินาศกรรม	

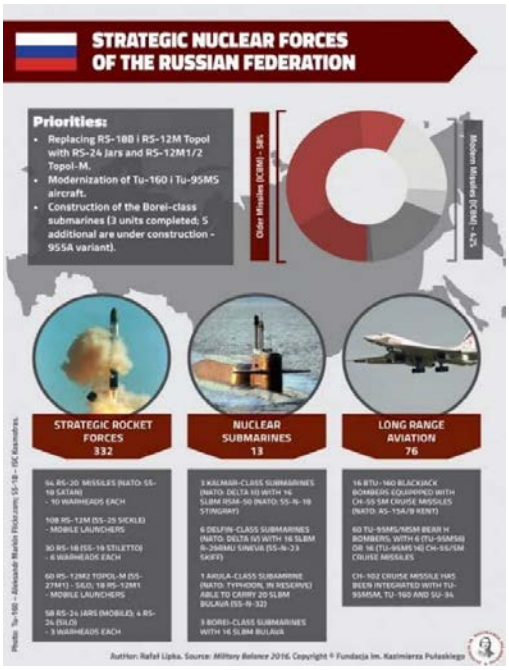
สถานการณ์การรบรัสเซีย – ยูเครนในปัจจุบัน

หลังผ่านพ้นระยะเวลากว่า 3 ปีของความขัดแย้งอย่างต่อเนื่อง สงครามระหว่างรัสเซียกับยูเครนได้พัฒนาเข้าสู่รูปแบบที่ซับซ้อนและไร้รูปทรงของสงครามในอดีตโดยสิ้นเชิง เมื่อปี 2022 ความพยายามของรัสเซียในการใช้ปฏิบัติการพิเศษทางทหารเพื่อกวาดล้างกองกำลังก่อการร้ายในยูเครนที่ต้องการให้จบภายในไม่กี่สัปดาห์ ซึ่งกลับกลายเป็นจุดเริ่มต้นของสงครามยืดเยื้อที่ผันตัวเป็นการประลองเชิงระบบอำนาจ และเทคโนโลยีที่ครอบคลุมทุกมิติของปฏิบัติการทางทหารในศตวรรษที่ 21

ในเชิงภูมิรัฐศาสตร์ สงครามครั้งนี้มิใช่เพียงข้อพิพาทเรื่องดินแดนระหว่างสองประเทศเท่านั้น แต่เป็นการวัดขีดความสามารถในการป้องกัน การโจมตีระยะไกล และการควบคุมโครงสร้างพื้นฐานทางทหาร โดยเฉพาะอย่างยิ่งการบั่นทอนศูนย์กลางการตัดสินใจและการสื่อสารผ่านการปฏิบัติการแบบอสมมาตร ยูเครนซึ่งขาด ความเหนือกว่าทางยุทโธปกรณ์แบบดั้งเดิม ได้เลือกตอบโต้ด้วยกลยุทธ์ที่ผสมผสานเทคโนโลยีสมัยใหม่ ข่าวกรอง และการโจมตีเชิงลึกด้วยระบบควบคุมระยะไกล ส่งผลให้รัสเซียต้องปรับยุทธศาสตร์หลายครั้งตลอด 3 ปีที่ผ่านมา ซึ่งเราได้เห็นสงครามสนามเพลาะ สงครามอสมมาตร ไปจนถึงสงครามที่ใช้ปฏิบัติการหลายมิติผสมผสานกัน

สิ่งที่น่าตะลึง คือเข้าสู่กลางปี 2025 รูปแบบของสงครามได้เปลี่ยนสภาพสู่การโจมตีที่ไม่จำเป็นต้องมีแนวรบการรุกลึกเข้าสู่ดินแดนรัสเซียด้วยอาวุธพิสัยไกล โดรน FPV ขนาดเล็กและขีปนาวุธระยะกลางที่ชาติตะวันตก สนับสนุนได้กลายเป็นหัวใจของกลยุทธ์ของยูเครน ขณะที่รัสเซียแม้จะมีขีดความสามารถในการโจมตีเมืองยูเครนอย่างต่อเนื่อง แต่กลับเริ่มเผชิญกับข้อจำกัดเชิงระบบมากขึ้น ไม่ว่าจะเป็นความสามารถของระบบป้องกันภัยทางอากาศที่ไม่ทั่วถึง การขาดข้อมูลแบบ real-time จากพื้นที่ปฏิบัติการ หรือแม้แต่การเผชิญกับการโจมตีทางลึกกว่า 7,000 กม. จากขอบหน้าพื้นที่การรบที่ไม่สามารถคาดการณ์ได้

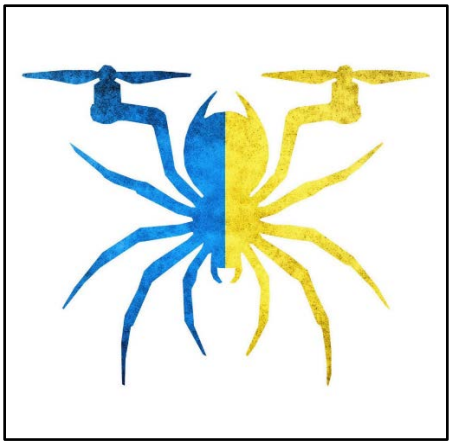
หนึ่งในเหตุการณ์สำคัญที่สุดที่สะท้อนความเปลี่ยนแปลงของสถานการณ์คือเหตุการณ์วันที่ 1 มิถุนายน 2025 ซึ่งตรงกับวันครบรอบ 29 ปีที่ยูเครนส่งคืนหัวรบนิวเคลียร์ให้กับรัสเซียตามข้อตกลงบูดาเปสต์ ในวันเดียวกันนั้น ยูเครนได้ปล่อยปฏิบัติการลับที่สามารถเจาะทะลุถึงสนามบินทางทหารในดินแดนลึกของรัสเซีย และทำลายเครื่องบินทิ้งระเบิด Tu-95MS ซึ่งเป็นหนึ่งใน 3 เสาหลักของยุทธศาสตร์นิวเคลียร์ (NUCLEAR TRIAD : อากาศยานทิ้งระเบิดระยะไกล , เรือดำน้ำ, จรวดภาคพื้น) ได้หลายลำ ซึ่งจะส่งผลทางยุทธศาสตร์อย่างยิ่งต่อรัสเซีย ความเสียหายไม่ได้จำกัดอยู่ที่อุปกรณ์แต่นำไปสู่**การตั้งคำถามครั้งใหญ่เกี่ยวกับความมั่นคงของระบบยุทธศาสตร์ภายในประเทศรัสเซียเอง**



สงครามในปีที่ 3 นี้ จึงไม่ได้เป็นการเผชิญหน้าระหว่างสองกองทัพเท่านั้น แต่เป็นการรบระหว่างระบบ ระบบข้อมูล ระบบควบคุม ระบบยิง และระบบป้องกันในโลกที่ไม่มีใครสามารถมั่นใจได้ว่า “แนวหลัง” จะปลอดภัยอีกต่อไป

Scenario การปฏิบัติการ “Operation Spider’s Web”

ปฏิบัติการที่ยูเครนใช้โจมตีสนามบินเชิงยุทธศาสตร์ของรัสเซียในวันที่ 1 มิถุนายน 2025 ภายใต้รหัส **“Operation Spider’s Web”** มิใช่เพียงการส่งโดรนพลีชีพเข้าโจมตีเป้าหมายห่างไกล แต่คือการแสดงให้เห็นถึงระบบการรบรูปแบบใหม่ที่เชื่อมต่อระหว่างเทคโนโลยีพลเรือน ข่าวกรองพิเศษ และการควบคุมที่ไม่มีทหารปรากฏตัวในสนามรบ การวางแผนปฏิบัติการครั้งนี้อาศัยการบูรณาการแบบเต็มรูปจากเครือข่าย ISR และระบบบัญชาการ C2 ที่กระจายตัว ผ่านเครือข่าย LTE และการแฝงตัวของหน่วยควบคุมโดรน ในดินแดนของรัสเซียเอง



หัวใจของปฏิบัติการ Spider Web อยู่ที่การซ่อน UAV ไว้ภายใน “Modified House” หรือกล่องไม้เคลื่อนที่ที่ดูเป็นโครงสร้างพลเรือนธรรมดา ติดตั้งบนรถบรรทุกที่ไม่มีเครื่องหมายทางทหารและแม้แต่พลขับรถก็ยังไม่ล่วงรู้ ตู้บรรทุกเหล่านี้ถูกลักลอบนำเข้ามายังพื้นที่ชานเมืองของไซบีเรียและบางแห่งใน Murmansk ซึ่งมีเส้นเขตเวลาต่างกันมาก ผ่านช่องโหว่ของระบบการตรวจสอบภายในของรัสเซีย ภายในตู้บรรทุกมีระบบ UAV ที่ใช้กลไกหลังคาเปิดอัตโนมัติ พร้อมแบตเตอรี่พลังงานภายใน ระบบส่งสัญญาณ LTE หรือ E-sim (ซึ่งยังไม่แน่ชัด) และกล้อง IR สำหรับยืนยันเป้าหมายก่อนปล่อย UAV

UAV ที่ใช้ใน Spider Web เป็น FPV drone รุ่นปรับแต่งพิเศษ มีระบบควบคุมผ่าน Raspberry Pi ที่เชื่อมต่อกับระบบ autopilot แบบทั่วไป ซึ่งประสานการทำงานกับดาวเทียม **ICEYE SAR (Synthetic Aperture Radar)** เป็นเรดาร์แบบสังเคราะห์ ซึ่งใช้เทคโนโลยีดาวเทียมขนาดเล็ก (microsatellite) เพื่อถ่ายภาพพื้นผิวโลกแบบทะลุเมฆหรือแม้แต่ในเวลากลางคืนได้โดยแบ่งปันจากกลุ่มข่าวกรองพันธมิตร ข้อมูลทั้งหมดจะเข้าสู่ระบบกลางในประเทศที่สาม แล้วจึงส่งคำสั่งกลับสู่จุดปล่อยผ่านโครงข่ายสื่อสารพลเรือนด้วยเทคโนโลยีนี้ ยูเครนสามารถดำเนินปฏิบัติการ “ลึกเข้าไปทั่วในเขตแดนรัสเซีย” โดยไม่ต้องมีทหารหรืออากาศยานใดล้ำข้ามพรมแดนเลยแม้แต่น้อย

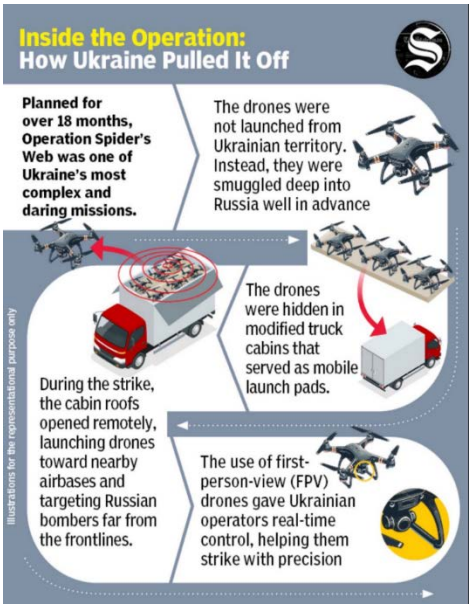
เมื่อได้รับคำสั่ง UAV ทั้งหมดจะถูกปล่อยพร้อมกันในรูปแบบ web จำนวน 114 ลำ ลำแรกมีหน้าที่สังเกตการณ์และล่อเป้า ลำหลังตามด้วย payload สำหรับทำลายเป้าหมายคือ**เครื่องบิน Tu-95MS** ที่จอดในสนามบิน เช่น Belaya และ Olenya โดยที่ระบบป้องกันภัยทางอากาศในพื้นที่ไม่สามารถตอบสนองได้ทัน และไม่สามารถตรวจจับต้นทางของการปล่อย UAV ได้เนื่องจากถูกฝังอยู่ในพื้นที่ที่ไม่มีใครคาดคิด

ความสำเร็จของ Spider Web ไม่ได้อยู่ที่จำนวน UAV ที่พุ่งชนเป้าหมาย แต่อยู่ที่การ **“ท้าทายศูนย์กลางความมั่นคง”** ของฝ่ายตรงข้ามและแสดงให้เห็นว่าระบบ C4ISR ของรัสเซีย มีช่องว่างที่สามารถถูกใช้เป็นจุดอ่อนในระดับโครงสร้างไม่ใช่เพียง tactical error แต่คือ strategic vulnerability ที่ยากจะป้องกันทันในภาวะสงคราม

ปฏิบัติการนี้จึงกลายเป็นต้นแบบของการโจมตีแบบไร้ข้อจำกัดด้านระยะปฏิบัติการ ที่ศัตรูไม่รู้ว่าความเสียหายเกิดขึ้นได้อย่างไร เพราะทั้งกระบวนการตรวจหา ยืนยัน เริ่มและทำลายเป้าหมาย ล้วนเกิดขึ้นภายใต้ระบบพลเรือนที่ได้รับการปรับแต่งให้ทำงานได้ในระดับเทียบเท่าการทหาร โดยไม่ต้องใช้กำลังพลแม้แต่คนเดียวในพื้นที่จริง

ผลกระทบในด้านขีดความสามารถการป้องกันและจิตวิทยา

ผลกระทบของปฏิบัติการ Spider Web ไม่ได้จำกัดอยู่แค่ความเสียหายทางกายภาพ ที่ถูกทำลายเท่านั้น แต่เป็นแรงสะเทือนที่เข้าไปกระทบโดยตรงต่อแนวคิดพื้นฐานของระบบป้องกันเชิงยุทธศาสตร์ของสหพันธรัฐรัสเซีย ในมุมของขีดความสามารถทางเทคนิค รัสเซียถือเป็นประเทศที่มีระบบป้องกันภัยทางอากาศหลายชั้นมากที่สุดในโลก ตั้งแต่ S-300,S-400, ไปจนถึงระบบที่ยังอยู่ระหว่างการพัฒนาอย่าง S-500 และระบบต่อต้านอากาศยานระยะประชิดอย่าง Pantsir-S1 แต่ปฏิบัติการในลักษณะ spider web ซึ่งไม่ได้ใช้วิธีบุกโจมตีจากภายนอก หากแต่แฝงตัวเข้ามาจากภายในแสดงให้เห็นถึงช่องโหว่เชิงโครงสร้างที่ระบบป้องกันเหล่านั้นต้องมีการประเมินและจัดระบบใหม่



การโจมตีจากระยะโดยไม่มีสัญญาณเตือนล่วงหน้า บั่นทอนความเชื่อมั่นต่อขีดความสามารถของระบบป้องกันภัยทางอากาศระดับประเทศ UAV ที่บินต่ำด้วยความเร็วสูงใช้การนำทางด้วยระบบ GLONASS และควบคุมจากระยะไกลผ่าน LTE ที่ไม่มีคลื่น RF ในทางทหาร ทำให้ไม่สามารถใช้เรดาร์ทางทหารมาตรฐานในการตรวจจับได้ทันท่วงที ยิ่งไปกว่านั้น รูปแบบของ **“ตู้บรรทุกปล่อยฝูงโดรน”** ยังไม่เคยถูกนำมาพิจารณาเป็นภัยคุกคามในมาตรฐานป้องกันดินแดนของรัสเซียมาก่อน ส่งผลให้พื้นที่ไซบีเรีย และภาคเหนือที่เคยเชื่อว่าเป็น **“แนวหลังที่ปลอดภัย”** ต้องถูกจัดโซนใหม่ในเชิงยุทธศาสตร์ และจำเป็นต้องลงทุนในระบบเฝ้าระวังพื้นฐานที่แตกต่างไปจากเดิมอย่างเร่งด่วน

ในด้านจิตวิทยาการทหาร ปฏิบัติการครั้งนี้ได้เปลี่ยน perception หรือการรับรู้ของกำลังพลรัสเซียในระดับปฏิบัติการและยุทธศาสตร์ จากเดิมที่เชื่อว่าฐานทัพภายในประเทศคือพื้นที่ปลอดภัย ปราศจากการรุกล้ำโดยตรง กลับต้องเข้าสู่สถานะเฝ้าระวังสูงสุด 24 ชั่วโมงอย่างไม่จำกัดเวลา ความตึงเครียดในการปฏิบัติการเพิ่มสูงขึ้น สร้างภาระต่อทั้งผู้ควบคุมสนามบิน ผู้ดูแลความปลอดภัยของเมืองในการตรวจยานพาหนะทุกคัน และหน่วยซ่อมบำรุงเครื่องบินที่ไม่เคยถูกฝึกให้ปฏิบัติการในภาวะคุกคามโดยตรงในพื้นที่ตัวเองมาก่อน

นอกจากนี้ ภาพข่าวกรองที่แสดงการระเบิดและไฟไหม้ของเครื่องบิน Tu-95MS ซึ่งถูกปล่อยผ่านสื่ออย่างจงใจโดยฝั่งยูเครน ทำหน้าที่เป็นอาวุธทางจิตวิทยาในตัวของมันเอง ภาพการโจมตีซ้ำในเวลาใกล้กันหลายจุด แสดงความแม่นยำที่ไม่ใช่เรื่องบังเอิญ แต่คือความสามารถในการประสานงานข้ามมิติ ทั้งภาพถ่ายดาวเทียม การสั่งการควบคุม UAV และระบบเผยแพร่ข้อมูลผลการโจมตีแบบพร้อมกันในหลายช่องทาง สิ่งเหล่านี้มีผลโดยตรงต่อ morale ของทั้งกำลังพลและประชาชนรัสเซีย และขณะเดียวกันก็สร้างแรงหนุนด้านจิตวิทยาให้กับฝ่ายยูเครนอย่างมหาศาลในเชิง **"ชัยชนะเชิงสัญลักษณ์"** แม้ในพื้นที่การรบระยะใกล้จะยังถูกเจาะอย่างต่อเนื่อง

การปฏิบัติทางยุทธวิธีส่งผลต่อยุทธศาสตร์ได้โดยตรงในทุกพื้นที่

หนึ่งในบทเรียนสำคัญจากปฏิบัติการ Spider Web คือการตอกย้ำว่า "การปฏิบัติทางยุทธวิธี" แม้จะเกิดขึ้นในระดับหน่วยขนาดเล็กหรือในพื้นที่เฉพาะจุด ก็สามารถส่งผลกระทบในระดับ "ยุทธศาสตร์" ได้โดยตรงและชัดเจนในโลกยุคใหม่ ที่เทคโนโลยีทำให้ระยะทางและขนาดของกำลังพลไม่ใช่ตัวชี้วัดผลของปฏิบัติการอีกต่อไป ตัวอย่างที่เห็นได้ชัดคือ การโจมตีเป้าหมายทางอากาศระดับยุทธศาสตร์ของรัสเซีย ซึ่งไม่เพียงแต่เป็นการลดขีดความสามารถเชิงระบบ แต่ยังสร้างแรงสั่นสะเทือนในมิติจิตวิทยาและการรับรู้ (perception) อย่างลึกซึ้ง อย่างไรก็ตาม ด้วยขีดความสามารถเชิงเทคนิคของยูเครนที่ยังมีข้อจำกัด จึงเป็นไปได้อย่างยิ่งว่าปฏิบัติการครั้งนี้ไม่ได้ดำเนินการโดยลำพัง หากแต่มีการสนับสนุนจากชาติตะวันตกในหลากหลายมิติ ทั้งด้านข่าวกรอง ดาวเทียม เทคโนโลยีควบคุม UAV หรือแม้แต่การกำหนดเป้าหมายระดับยุทธศาสตร์ร่วมกัน

ขณะที่รัสเซียเองก็ได้ปรับตัวตอบสนองต่อภัยคุกคามดังกล่าว ด้วยการพัฒนาและย้ายระบบปล่อยอาวุธนิวเคลียร์ไปสู่ขีปนาวุธภาคพื้นดินในสัดส่วนที่เพิ่มขึ้น แม้จะช่วยลดความเปราะบางของระบบเดิม แต่ก็แลกมากับต้นทุนที่สูงขึ้นทั้งในด้านเทคนิค ความปลอดภัย และการซ่อมบำรุงลักษณะการปฏิบัติการของยูเครนยังสะท้อนถึงแนวทางที่ผสมผสานระหว่างผลทางกายภาพและผลทางจิตวิทยาอย่างชาญฉลาด การโจมตีสนามบินที่มีเครื่องบินทิ้งระเบิด Tu-95MS ส่งผลชัดเจนต่อขีดความสามารถทางยุทธศาสตร์ แต่ในเวลาเดียวกัน ความคลุมเครือของข้อมูลความเสียหาย และการตอบโต้ข่าวสารระหว่างทั้งสองฝ่าย ก็ถูกใช้เป็นเครื่องมือในการขยายผลทางจิตวิทยาอย่างได้ผล

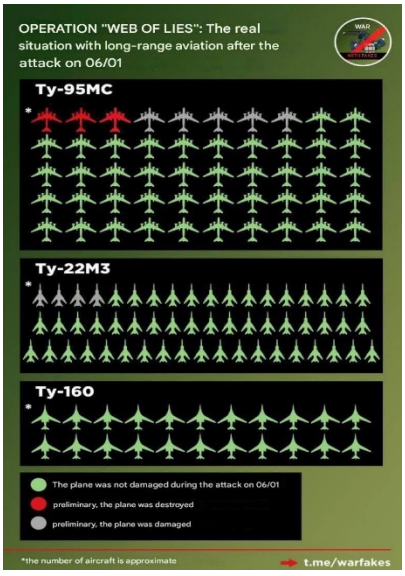
ยูเครนยังเดินหน้าการรบในลักษณะอสมมาตร (Asymmetric Warfare) โดยมุ่งเป้าไปที่จุดสำคัญที่ให้ผลตอบแทนเชิงยุทธศาสตร์สูง เช่น การลอบสังหาร การระเบิดสะพานไครเมีย หรือการส่งโดรนโจมตีในเชิงลึก ทุกปฏิบัติการเหล่านี้สามารถส่งผลกระทบทั้งต่อระบบบัญชาการ คลังยุทโธปกรณ์ ไปจนถึงขวัญกำลังใจของฝ่ายตรงข้ามได้ในวงกว้าง ในภาพรวมปฏิบัติการครั้งนี้ยังท้าทายแนวคิดดั้งเดิมเรื่อง “พื้นที่ส่วนหลัง” (Rear Area) อย่างชัดเจน สหรัฐฯ เองได้ปรับแนวทางการจัดการพื้นที่ส่วนหลังไปสู่แนวคิด “Consolidation Area” ซึ่งหมายถึงการรักษาความมั่นคงและความพร้อมในทุกพื้นที่ ไม่ว่าจะอยู่ใกล้หรือไกลจากแนวหน้า เนื่องจากภัยคุกคามสามารถแทรกซึมได้จากทุกทิศทาง

สำหรับประเทศไทย บทเรียนนี้มีความสำคัญอย่างยิ่ง เพราะโครงสร้างพื้นฐานหลัก เช่น สนามบินทหาร สถานีเรดาร์ หรือระบบสื่อสารเชิงยุทธศาสตร์จำนวนมาก ยังขาดการป้องกันเชิงลึกที่เพียงพอ โดยเฉพาะต่อภัยคุกคามจากโดรน ซึ่งสามารถขึ้นบินได้จากทุกที่ บรรทุกอาวุธหรืออุปกรณ์จารกรรมได้หลากหลาย แม้ระบบตรวจจับและตอบโต้จะพัฒนาแล้วในระดับหนึ่ง แต่หากโดรนถูกปล่อยในระยะประชิด เวลาสำหรับการตอบสนองก็จะจำกัด และหากเป็นการโจมตีในรูปแบบ “ฝูง” (Swarm Attack) การป้องกันจะยิ่งท้าทายมากขึ้น ดังนั้นประเทศไทยจึงต้องเร่งเสริมสร้างระบบการป้องกันที่ไม่ใช่แค่รอรับ แต่ต้องสามารถตรวจจับล่วงหน้า ตอบสนองแบบบูรณาการ และปรับตัวในเชิงระบบได้อย่างทันท่วงที โดยเฉพาะในพื้นที่ยุทธศาสตร์หรือพื้นที่เสี่ยงสูง เช่น สามจังหวัดชายแดนภาคใต้ หรือโครงสร้างพื้นฐานที่เกี่ยวข้องกับความมั่นคงระดับชาติ

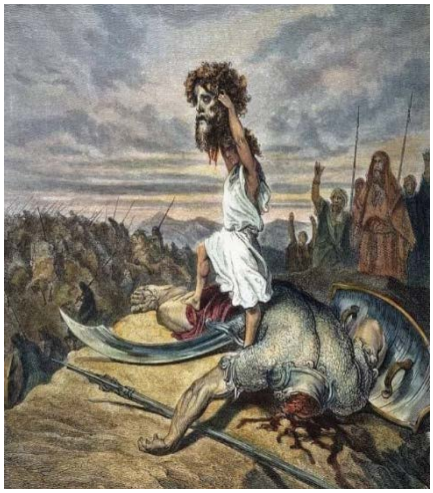
บทเรียนที่สามารถนำมาประยุกต์ใช้กับประเทศไทยในการป้องกันการก่อวินาศกรรม

ปฏิบัติการ Spider Web ของยูเครนในเดือนมิถุนายน 2025 ไม่ได้เป็นเพียงแค่การส่งโดรนขนาดเล็กเข้าไปโจมตีสนามบินทหารลึกในไซบีเรียเท่านั้น หากแต่คือการสะท้อนถึงศักยภาพของการทำสงครามยุคใหม่ ซึ่งให้ความสำคัญกับการเจาะจุดอ่อนเชิงระบบ มากกว่าการรุกด้วยกำลังพลหรืออาวุธหนัก

ยูเครนสามารถระบุ **EEFI (Essential Elements of Friendly Information) เครื่องมือสำคัญที่ต้องปกปิดรักษาของฝ่ายรัสเซียได้อย่างแม่นยำ เพราะเป็น DP (decisive Point)** ซึ่งในกรณีนี้หมายถึง **การกระแทรกต่อจุดเปราะบาง (critical Vulnerability)** ของระบบยุทธศาสตร์รัสเซีย คือ การเก็บรักษาเครื่องบิน Tu-95MS Strategic Bombers ในที่โล่ง เมื่อวิเคราะห์อย่างเป็นระบบ สิ่งที่ยูเครนโจมตีนั้นคือ **CC (Critical Capabilities) หรือ ขีดความสามารถสำคัญของศัตรูที่อาจไม่ถึงกับทำให้รัสเซียพ่ายแพ้โดยตรง** แต่ก็เพียงพอจะสร้างการ **Disruption หรือ “ความชะงักงัน”** ต่อการใช้กำลังทางอากาศของฝ่ายรัสเซีย ซึ่งประเทศไทยสามารถนำบทเรียนนี้มาประยุกต์ใช้โดยไม่จำกัดเพียงการพัฒนาเทคโนโลยี แต่ต้องเริ่มจาก**การสร้างภาพรวม (situational picture)** ที่ชัดเจนของตนเอง ว่า EEFI ของฝ่ายไทยคืออะไร และขีดความสามารถอะไรบ้างที่อาจตกเป็นเป้าของการก่อวินาศกรรมยุคใหม่ เช่น สนามบินทหารที่มีระบบควบคุมพลเรือน, สถานีเรดาร์ที่ไม่มีการป้องกันทางไซเบอร์ ระบบสื่อสารที่เชื่อมต่อผ่านโครงข่าย 5G แบบเปิดโล่ง หรือแม้แต่การเก็บยุทโธปกรณ์สำคัญที่อาจจะถูกก่อวินาศกรรมได้จากระบบ รปภ. ที่ไม่แน่นหนารัดกุม



การวางระบบเฝ้าระวังแบบ Proactive Surveillance เช่น การตรวจจับสัญญาณ RF จากอุปกรณ์พกพา การฝึกเจ้าหน้าที่ให้วิเคราะห์พฤติกรรมแปลกปลอมในพื้นที่ยุทธศาสตร์ และการฝึกซ้อมสถานการณ์จำลองใน**รูปแบบ Multi-Domain Operations (MDO)** คือแนวทางที่ควรเร่งพัฒนา เพื่อเชื่อมโยงข้อมูลข่าวกรอง การตอบสนองทางยุทธ์วิธี และการจัดการทรัพยากรแบบบูรณาการ โดยเฉพาะพื้นที่เปราะบางทางยุทธศาสตร์ เช่น สามจังหวัดชายแดนภาคใต้ ซึ่งมีลักษณะภูมิประเทศเปิด การเคลื่อนย้ายประชากรอย่างเสรี และสภาพความมั่นคงที่มีความละเอียดอ่อน หน่วยความมั่นคงไทยต้องเตรียมพร้อมรับมือกับการก่อวินาศกรรมในลักษณะเดียวกับ Spider Web ที่อาจอาศัยอุปกรณ์เชิงพาณิชย์อย่าง UAV, โทรศัพท์มือถือ หรือแม้แต่ระบบขนส่งพื้นฐานเป็นเครื่องมือแฝงในการลอบโจมตี การประสานงานระดับนโยบายจึงควรพิจารณาสร้าง Joint Intelligence Center ระหว่างฝ่ายทหาร ตำรวจ และพลเรือน เพื่อให้เกิด **Shared Situational Awareness** และการตอบสนองในแบบที่ต่างคนต่างทำแต่ทำงานในแบบเครือข่าย (network-centric defense)



การปฏิบัติทางยุทธวิธีส่งผลต่อยุทธศาสตร์ได้โดยตรงในทุกๆที่

ในท้ายที่สุด บทเรียนที่สำคัญที่สุดคือ ไม่ว่าเราจะมีเครื่องบินรบ รถถัง หรือขีปนาวุธมากเพียงใด หากละเลยจุดอ่อนเล็ก ๆ ที่ซ่อนอยู่ในระบบ จุดนั้นอาจเป็นบาดแผลเดียวที่ทำให้ทั้งระบบพังครืนลงได้ ดังคำกล่าวที่ว่า

“David no longer stands with just a sling - he commands systems, networks, and the will of a nation. And Goliath, though armored, bleeds when struck where he never looked.”

“ดาวิดในวันนี้ไม่ได้มีแค่หนังสติ๊ก แต่เขาบัญชาระบบ เครือข่าย และเจตจำนงแห่งชาติ ส่วนโกไลแอท แม้หุ้มเกราะหนา ก็ยังเลือดไหลเมื่อถูกโจมตีตรงจุดที่เขาไม่ทันระวัง” และในทุกวันนี้ไม่มีที่ใดที่จะปลอดภัย 100% อีกต่อไป

พ.อ.อรรถพร ประชานุกูล

อจ.สยผ.วทบ.

อ้างอิง :

- สำนักข่าวรอยเตอร์. (1 มิถุนายน 2025). ยูเครนเปิดปฏิบัติการโจมตีฐานทัพอากาศรัสเซียด้วยโดรนกว่า 100 ลำ. สืบค้นจาก: https://www.reuters.com/business/aerospace-defense/ukraine-stages-major-attack-russian-aircraft-with-drones-security-official-says-2025-06-01/
- สำนักข่าวบิสิเนสอินไซเดอร์. (2 มิถุนายน 2025). ปฏิบัติการ Spiderweb ของยูเครนสะท้อนภัยคุกคามเชิงระบบใหม่ที่ทั่วโลกต้องจับตา. สืบค้นจาก: https://www.businessinsider.com/ukraines-spiderweb-drone-attack-warning-for-all-militaries-2025-06
- สำนักข่าวแอกซิออส. (4 มิถุนายน 2025). Spiderweb: ปฏิบัติการโดรนที่เปลี่ยนวิธีการสงครามสมัยใหม่. สืบค้นจาก: https://www.axios.com/2025/06/04/ukraine-spiderweb-drone-attack-shipping