



เครดิตความรู้ที่ 5

ยุทธศาสตร์



การต่อต้านการก่อการร้าย ฉบับปี 2566 (CONTEST 2023)

ต้นคิด เจียรกุล¹



เมื่อวันที่ 18 มิถุนายน 2566 กระทรวงมหาดไทย (Home Office) สหราชอาณาจักร เผยแพร่ยุทธศาสตร์การต่อต้านการก่อการร้ายฉบับปี 2566 (Counter Terrorism Strategy : CONTEST 2023) เพื่อเป็นแนวทางลดระดับความเสี่ยงและรับมือภัยคุกคามด้านการก่อการร้ายของสหราชอาณาจักรทั้งภายในประเทศและต่างประเทศ

ยุทธศาสตร์ CONTEST

ยุทธศาสตร์การต่อต้านการก่อการร้ายของสหราชอาณาจักร (The United Kingdom's Strategy for Countering Terrorism : CONTEST) เริ่มจัดทำขึ้นเมื่อปี 2546 เพื่อป้องกันและลดความเสี่ยงของสหราชอาณาจักรจากภัยคุกคามด้านการก่อการร้ายภายหลังเกิดเหตุก่อการร้ายในสหรัฐฯ เมื่อวันที่ 11 กันยายน 2544 (เหตุการณ์ 9/11) โดยเป็นความริเริ่มของเซอร์ เดวิด โอฆานด์ ซึ่งในขณะนั้นดำรงตำแหน่งปลัดสำนักงานคณะรัฐมนตรีและผู้ประสานงานด้านความมั่นคงและ

การข่าวกรองของสำนักงานคณะรัฐมนตรี ร่วมกับคณะทำงานของกระทรวงมหาดไทยแห่งสหราชอาณาจักร² โดยมีหัวใจสำคัญของยุทธศาสตร์ฯ คือหลักการ 4P ได้แก่ 1) **Prevent** : ป้องกัน การเข้าร่วมหรือสนับสนุนการก่อการร้ายของประชาชน 2) **Pursue** : ติดตาม สกัดกั้นการโจมตีที่จะเกิดขึ้นทั้งภายในและภายนอกสหราชอาณาจักร 3) **Protect** : ปกป้อง มุ่งลดความเปราะบางต่อการก่อการร้าย และ 4) **Prepare** : เตรียมพร้อม มุ่งลดผลกระทบจากการก่อการร้ายและลดโอกาสในการก่อเหตุเพิ่มเติม



¹ นักวิเคราะห์นโยบายและแผนปฏิบัติการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการ สำนักงานสภาความมั่นคงแห่งชาติ

² Home Office, Office for Security and Counter Terrorism. "Counter-terrorism strategy." Home Office. February 17, 2552. <https://web.archive.org/web/20090217221010/http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy/>.

ต่อมาสหราชอาณาจักรได้ปรับปรุงยุทธศาสตร์ฯ เพื่อให้สอดคล้องกับบริบทของการก่อการร้ายในแต่ละช่วงเวลาเรื่อยมา ซึ่งปัจจุบันมียุทธศาสตร์ฯ ทั้งหมด 5 ฉบับ ได้แก่

- 1 ฉบับปี 2003 เพื่อตอบสนองกับภัยคุกคามด้านการก่อการร้ายจากกลุ่มก่อการร้ายอิสลามภายหลังเหตุการณ์ 9/11 และสงครามต่อต้านการก่อการร้าย
- 2 ฉบับปี 2006 ที่จัดทำขึ้นเพื่อตอบสนองต่อภัยคุกคามด้านการก่อการร้ายภายหลังเหตุระเบิดในบาห์ลีเมื่อปี 2545 เหตุระเบิดที่สถานีรถไฟหลายแห่งในกรุงมาดริดปี 2547 และเหตุระเบิดต่อเนื่องในกรุงลอนดอนเมื่อวันที่ 7 กรกฎาคม 2548 ที่กลุ่มก่อการร้ายอิสลามมีพลวัตการก่อเหตุนอกพื้นที่ตะวันออกกลางและเอเชียใต้มากขึ้นอย่างต่อเนื่อง³
- 3 ฉบับปี 2001 ที่จัดทำขึ้นเพื่อให้สอดคล้องกับการอ่อนกำลังลงของกลุ่มอัลกออิดะฮ์ (Al-Qaeda : AQ) และแนวโน้มการก่อการร้ายแบบในลักษณะเป็นผู้ปฏิบัติคนเดียว (lone actor) เพิ่มขึ้นอย่างต่อเนื่อง⁴
- 4 ฉบับปี 2018 ที่ปรับปรุงเนื้อหาและแนวนโยบายให้สอดคล้องกับการผงาดของกลุ่มรัฐอิสลาม (IS หรือ Daesh) และกลุ่มก่อการร้ายอนุรักษนิยมสุดโต่ง (Extreme Right-Wing Terrorist)⁵ และ
- 5 ฉบับปี 2023 ที่จัดทำขึ้นภายหลังสถานการณ์โควิด-19 และการแยกตัวของกลุ่มก่อการร้ายเดิม แต่ถูกแทนที่ด้วยพลวัตของการก่อการร้ายในไซเบอร์สเปซและการก่อเหตุโดยปัจเจกบุคคลหรือกลุ่มขนาดเล็กนอกเครือข่ายก่อการร้ายที่สูงขึ้น⁶ โดยบทความนี้จะอธิบายรายละเอียดและเนื้อหาของยุทธศาสตร์ CONTEST 2023 ซึ่งมีการปรับปรุงเนื้อหาด้านพัฒนาการของการก่อการร้ายและการปรับปรุงแนวนโยบาย 4P และจะนำเสนอบทวิเคราะห์ของยุทธศาสตร์ดังกล่าวพร้อมข้อเสนอแนะเชิงนโยบาย ดังนี้

พัฒนาการด้านการก่อการร้ายในสหราชอาณาจักรหลังจากปี 2018

CONTEST 2023 ระบุถึงภัยคุกคามด้านการก่อการร้ายที่สำคัญที่สุด 3 อันดับ ได้แก่

- 1 กลุ่มก่อการร้ายที่มีแนวคิดมาจากศาสนาอิสลาม (Islamist terrorist)
โดยมีสัดส่วนกว่าร้อยละ 64 ของจำนวนเหตุการณ์การก่อการร้ายที่ผ่านมา ซึ่งกลุ่มที่ถูกเฝ้าระวังและติดตามอย่างต่อเนื่องยังคงเป็นกลุ่มอัลกออิดะฮ์ และกลุ่มรัฐอิสลาม (IS หรือ Daesh) ที่ถึงแม้มีศักยภาพในการปฏิบัติการที่ลดลง แต่พบการพัฒนายุทธวิธีการชักชวนผู้เข้าร่วมอย่างต่อเนื่อง
- 2 กลุ่มก่อการร้ายอนุรักษนิยมสุดโต่ง (Extreme Right-Wing Terrorist)
โดยมีสัดส่วนร้อยละ 22 ซึ่งมักจะจัดตั้งเป็นกลุ่มที่ไม่เป็นทางการผ่านแพลตฟอร์มออนไลน์และเชื่อมโยงเป็นเครือข่ายระหว่างประเทศ และ
- 3 กลุ่มก่อการร้ายฝ่ายซ้าย กลุ่มอนาธิปไตย และกลุ่มก่อการร้ายเฉพาะประเด็น ที่มีจำนวนไม่มากและในช่วงระยะหลังจะเน้นไปกิจกรรมการประท้วงต่างๆ ซึ่งมีความเสี่ยงที่จะเกิดความรุนแรง

³ HM Government, Countering International Terrorism: The United Kingdom's Strategy (The Stationery Office, London 2554), 6-7.

⁴ HM Government, CONTEST: The United Kingdom's Strategy for Countering Terrorism (The Stationery Office, London 2554), 9-10

⁵ HM Government, CONTEST: The United Kingdom's Strategy for Countering Terrorism (The Stationery Office, London 2563), 7-8.

⁶ HM Government, CONTEST: The United Kingdom's Strategy for Countering Terrorism (The Stationery Office, London 2566), 9-22.

อย่างไรก็ตาม แม้กลุ่มก่อการร้ายข้างต้นจะมีศักยภาพและขนาดที่ลดลง แต่ภัยคุกคามด้านการก่อการร้ายต่อสหราชอาณาจักรในปัจจุบันกลับมีแนวโน้มที่ผู้ก่อเหตุจะเป็นปัจเจกบุคคลหรือกลุ่มขนาดเล็กที่ปฏิบัติการนอกเครือข่ายของกลุ่มก่อการร้ายมากขึ้น ก่อปรกับการพัฒนาของเทคโนโลยีที่เป็นอีกหนึ่งปัจจัยสำคัญในการสนับสนุนการก่อการร้ายในหลายระดับตั้งแต่การโฆษณาชวนเชื่อ การปลุกฝังความรุนแรง การปกปิดของอัตลักษณ์ผู้กระทำ ตลอดจนการสนับสนุนทางการเงินแก่กลุ่มก่อการร้ายที่ได้สะดวกยิ่งขึ้น ส่งผลให้การคาดการณ์ การระบุตัวตน การสืบสวน และการยับยั้งการก่อการร้ายเป็นไปได้ยากลำบากยิ่งขึ้น

ยุทธศาสตร์ 4P ภายใต้ CONTEST 2023

พัฒนาการด้านการก่อการร้าย CONTEST 2023 เสนอแนวทางการพัฒนาตามหลัก 4P ดังนี้

1 Prevent (ป้องกัน) คือ การมุ่งหยุดยั้งการเข้าร่วมหรือสนับสนุนการก่อการร้ายของประชาชน โดยเพิ่มการฝึกอบรมและจัดทำแนวปฏิบัติที่มีความชัดเจนยิ่งขึ้นสำหรับหน่วยปฏิบัติการเพื่อสร้างความเข้าใจที่ลึกซึ้งยิ่งขึ้นต่อรูปแบบอุดมการณ์และการปลุกฝังความรุนแรงของกลุ่มก่อการร้าย และการปรับมาตรการการดูแลผู้ก่อการร้ายและผู้ที่เกี่ยวข้องในเรือนจำเพื่อให้เกิดการปรับปรุงพฤติกรรมอย่างมีประสิทธิภาพ

2 Pursue (ติดตาม) คือ การมุ่งสกัดกั้นการโจมตีที่จะเกิดทั้งภายในและภายนอกสหราชอาณาจักร ตั้งแต่การตรวจจับและทำความเข้าใจรูปแบบ ตลอดจนสืบสวนและยับยั้งการก่อการร้าย โดยการเพิ่มขีดความสามารถแก่ศูนย์ปฏิบัติการต่อต้านการก่อการร้าย (CTOC) เพิ่มการลงทุนเพื่อพัฒนาขีดความสามารถในการประเมินภัยคุกคามด้านการก่อการร้ายโดยเฉพาะกลุ่มที่ก่อเหตุโดยใช้เทคโนโลยี และสร้างการมีส่วนร่วมกับภาคเทคโนโลยีเอกชน โดยเฉพาะการประสานงานเพื่อปราบปรามการแสวงประโยชน์ที่เข้าข่ายการสนับสนุนการก่อการร้ายในอินเทอร์เน็ต

3 Protect (ปกป้อง) คือ การลดความเปราะบางต่อการก่อการร้าย อาทิ การลดความเสี่ยงพื้นที่ให้บริการขนส่งสาธารณะและโครงสร้างพื้นฐานสำคัญ การจำกัดการเข้าถึงวัสดุหรือเทคโนโลยีที่มีความเสี่ยงต่อการก่อการร้าย และการเสริมสร้างความเข้มแข็งบริเวณชายแดน โดยเพิ่มการฝึกอบรมบุคลากรและเสริมสร้างระบบรักษาความปลอดภัยให้มีขีดความสามารถในการคัดกรองบุคคลเข้าประเทศสูงขึ้น

4 Prepare (เตรียมพร้อม) คือ การมุ่งลดผลกระทบจากการก่อการร้ายและลดโอกาสในการก่อเหตุเพิ่มเติม อาทิ การมีมาตรการตอบสนองต่อเหตุที่ได้สัดส่วน การประสานงานที่มีประสิทธิภาพและความสามารถในการฟื้นตัวที่รวดเร็วโดยมุ่งพัฒนาขีดความสามารถรับมือกับภัยคุกคามที่โอกาสเกิดน้อยแต่ผลกระทบมาก และการเสริมสร้างการบูรณาการด้านการสร้างความยืดหยุ่น (resilience) กับหน่วยงานท้องถิ่น

นอกจากนี้ยุทธศาสตร์ฯ ได้เพิ่มการมีส่วนร่วมของผู้เชี่ยวชาญและหน่วยงานที่ไม่ใช่หน่วยงานบังคับใช้กฎหมายในกิจการต่อต้านการก่อการร้ายการกระชับความร่วมมือกับประเทศหุ้นส่วนด้านการต่อต้านการก่อการร้าย และการปรับปรุงมาตรการขอเข้าถึงข้อมูลที่เป็นที่ต่อการสืบสวนและขัดขวางการก่อการร้ายให้สอดคล้องกับหลักความจำเป็นและได้สัดส่วน

ข้อสังเกต CONTEST 2023

จากพัฒนาการของการก่อการร้ายและการปรับปรุงหลักการ 4Ps ของ CONTEST 2023 จะเห็นได้ว่าทิศทางด้านความมั่นคงและท่าทีของสหราชอาณาจักร โดยเฉพาะในด้านการต่อต้านการก่อการร้าย ได้เพิ่มความสำคัญด้านการป้องกันการก่อการร้ายที่เกิดจากพัฒนาการด้านเทคโนโลยีอย่างมีนัยสำคัญ จากการระบุนภัยคุกคามด้านการใช้เทคโนโลยีเพื่อวัตถุประสงค์ด้านการก่อการร้ายที่ชัดเจนขึ้น อาทิ ความเสี่ยงต่อภัยคุกคามจากแพลตฟอร์มออนไลน์ ปัญญาประดิษฐ์ และสกุลเงินดิจิทัล⁷ และการกำหนดนโยบายด้านการป้องกันการใช้พื้นที่ไซเบอร์สเปซของผู้ก่อการร้ายที่ชัดเจนมากขึ้นจากยุทธศาสตร์ฯ ฉบับเดิม (CONTEST 2018) ได้แก่ 1) การผลักดันการตรา ร่าง พ.ร.บ.ความปลอดภัยทางออนไลน์ (the Online Safety Bill) และมอบหมายให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งสหราชอาณาจักร (Office of Communications : Ofcom) เป็นหน่วยงานหลักที่มีอำนาจในการดำเนินการกำกับดูแล⁸ ซึ่งจะมีการกำหนดบทลงโทษที่ชัดเจนแก่บริษัทเอกชนผู้รับผิดชอบด้านการกำกับดูแลการเผยแพร่ข้อมูลที่ผิดกฎหมายบนแพลตฟอร์มออนไลน์ และ 2) การเพิ่มความร่วมมือกับภาคอุตสาหกรรม โดยเฉพาะผู้ผลิตเทคโนโลยีและผู้ให้บริการเครือข่ายโทรคมนาคม (Telecommunication provider) เพื่อสร้างศักยภาพในการสืบสวนและสกัดกั้นภัยคุกคามให้แก่หน่วยงานด้านการข่าวและการบังคับใช้กฎหมาย

หากพิจารณาเชิงเปรียบเทียบกับแผนปฏิบัติการด้านการต่อต้านการก่อการร้ายของไทยในกรอบนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ จะเห็นได้ว่ามีการให้ความสำคัญกับ 3 แนวทางหลัก คือ 1) การป้องกันและเสริมสร้างภูมิคุ้มกันในการรับมือภัยก่อการร้าย (Prevention) 2) การเสริมสร้างการตอบโต้วิกฤตจากการก่อการร้าย (Countering) และ 3) การเสริมสร้างการฟื้นตัวภายหลังเกิดวิกฤตก่อการร้ายให้กลับสู่สภาพปกติโดยเร็ว (Resilience) เพื่อให้เกิดการประสานงานและการบูรณาการการดำเนินงานอย่างสอดคล้องกันนั้น พบว่าแผนปฏิบัติการดังกล่าวมีศักยภาพที่จะพัฒนาเพิ่มเติมให้สอดคล้องกับพลวัตการใช้พื้นที่ไซเบอร์สเปซของผู้ก่อการร้ายที่สูงขึ้นอย่างต่อเนื่องได้ เนื่องจากแผนปฏิบัติการดังกล่าวมีแนวทางรองรับทั้งการสร้างภูมิคุ้มกันจากความคิดสุดโต่งทั้งทางกายภาพและไซเบอร์สเปซ และการสร้างการมีส่วนร่วมของบุคลากรภาครัฐและภาคเอกชนเพื่อเป็นเครือข่ายในด้านการป้องกันการก่อการร้าย

อย่างไรก็ตาม แม้จะมีการระบุแนวทางการรับมือกับการใช้พื้นที่ไซเบอร์สเปซของผู้ก่อการร้าย แต่ยังคงมีข้อจำกัดด้านรายละเอียดปลีกย่อยที่ไม่ชัดเจนถึงแนวทางการสร้างความร่วมมือกับภาคเอกชน โดยเฉพาะกลุ่มอุตสาหกรรมผู้ผลิตเทคโนโลยีและกำกับดูแลแพลตฟอร์มออนไลน์ซึ่งนับวันจะยิ่งมีบทบาทสำคัญในการร่วมรักษาความมั่นคงของไซเบอร์สเปซของไทยท่ามกลางความไม่แน่นอนในการสร้างกฎหมาย กฎระเบียบ การอำนวยความสะดวก และการกำกับดูแลให้เกิดความเป็นธรรมในพื้นที่ดังกล่าว⁹ ซึ่งในอนาคต ไทยอาจพิจารณา 1) การสร้างเครือข่ายความร่วมมือด้านการต่อต้านการใช้พื้นที่ไซเบอร์สเปซของผู้ก่อการร้ายระหว่างภาครัฐและเอกชนที่มีความชัดเจนเป็นรูปธรรมยิ่งขึ้น 2) ติดตามและศึกษาพลวัตของตัวแบบการกำกับดูแลด้านการต่อต้านการก่อการร้ายไซเบอร์จากประเทศที่มีศักยภาพและความเชี่ยวชาญ และ 3) การแสวงหาความสอดคล้องในคุณค่าด้านความมั่นคงของรัฐและคุณค่าด้านเสรีนิยมในการกำหนดหน้าที่ตามกฎหมายของผู้ให้บริการเครือข่ายไทยเพิ่มเติม¹⁰ เพื่อให้สอดคล้องกับบริบทความมั่นคงปัจจุบัน

⁷ Ibid., 21-22.

⁸ Ibid., 32.

⁹ ศรีแสงนาม, ปิติ. “Cyberspace: ภูมิรัฐศาสตร์-เศรษฐกิจใหม่ และความขัดแย้งในอนาคต.” 101World. มกราคม 25, 2566, <https://www.the101.world/cyberspace-geo-political-economy/>.

¹⁰ อารัม ตั้งนรินทร์, รายงานการวิจัยฉบับสมบูรณ์: กฎหมายความปลอดภัยทางไซเบอร์กับการกำกับดูแลเศรษฐกิจดิจิทัลของประเทศไทย ถอดบทเรียนสำหรับเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0(สำนักงานการวิจัยแห่งชาติ, 2563), 75-79.2.