ภัยคุกคามทางข้อมูล: บทเรียนจากความขัดแย้งระหว่างรัสเซีย–ยูเครนและกาซา เพื่อเตรียมความพร้อมในการรับมือของประเทศไทย

Information Threats: Lessons from the Russia–Ukraine and Gaza Conflicts for Thailand's National Preparedness

ทัธภร ธนาวริทธิ์[1] และ จีระวัฒน์ ลีนะกนิษฐ์[2]

Tatporn Tanawarit[1], and Jeerawat Linakanit[2]

สถาบันรัชต์ภาคย์

Rajapark Institute, Thailand

E–mail: Tatporn.tanawaritt@gmail.com[1], jeerawatl1@gmail.com[2]

Received July 14, 2025; **Revised** September 27, 2025; **Accepted** September 30, 2025

Abstract

In the contemporary era, information plays a critical role in shaping advantages in warfare, particularly in cognitive warfare that extends the battlefield into cyberspace. This study investigates patterns of information threats by collecting news reports, analyses, interviews, and academic literature related to such threats—including information operations, psychological operations, and cyber operations—based on case studies from the Russia–Ukraine war and the Gaza conflict. The analysis provides insights into the application of various strategic models in information operations, as well as countermeasures between conflicting parties, and compares these findings with Thailand's current situation. The purpose is to draw lessons and propose preparedness measures for Thai government agencies to address information threats across four citizen–centered dimensions. The study finds that the Thai government should: (1) strengthen situational awareness by fostering fact–checking networks, integrating collaborative mechanisms, supporting the use of artificial intelligence to enhance the detection of cyber anomalies, and enabling real–time communication of factual information; (2) improve preventive effectiveness through cooperation with social media platforms and cybersecurity experts, as well as nationwide promotion of media and digital literacy; (3) enhance the efficiency of control and mitigation by developing proactive strategic communication capacities, alongside comprehensive regulation of information, social media platforms, and critical infrastructure in alignment with digital innovation; and (4) build resilience by safeguarding critical information

systems at Thailand's border areas. These measures collectively strengthen Thailand's capacity to respond effectively to information threats.

Keywords: information threats; information operations; cyber operations; cognitive warfare

บทคัดย่อ

ในยุคที่ข้อมูลมีบทบาทสำคัญในการกำหนดความได้เปรียบในสงคราม โดยเฉพาะสงครามทางปัญญาที่ขยายพื้นที่การต่อสู้ไปยังพื้นที่ไซเบอร์ การศึกษารูปแบบของภัยคุกคามทางข้อมูลโดยรวบรวมข้อมูลข่าวสาร บทวิเคราะห์ บทสัมภาษณ์ และเอกสารวิชาการที่เกี่ยวข้องกับภัยคุกคามทางข้อมูล เช่น การปฏิบัติการทางข้อมูล การปฏิบัติการทางจิตวิทยา การปฏิบัติการทางไซเบอร์ จากกรณีศึกษาของสงครามรัสเซีย–ยูเครน และสงครามฉนวนกาซา ช่วยให้ทราบถึงแนวทางการประยุกต์ใช้รูปแบบกลยุทธ์ต่าง ๆ ในการปฏิบัติการทางข้อมูล รวมถึงมาตรการรับมือภัยคุกคามทางข้อมูลระหว่างคู่ขัดแย้ง และนำมาเปรียบเทียบกับสถานการณ์ของประเทศไทย เพื่อสรุปบทเรียนและเสนอแนะแนวทางการเตรียมความพร้อมสำหรับการรับมือกับภัยคุกคามทางข้อมูลสำหรับหน่วยงานภาครัฐของประเทศไทย ใน 4 มิติที่มีประชาชนเป็นศูนย์กลาง จากการศึกษาพบว่า รัฐบาลไทยควร 1) เสริมสร้างศักยภาพในการรับรู้สถานการณ์ โดยการส่งเสริมเครือข่ายตรวจสอบข้อเท็จจริงทั้งการบูรณาการในการทำงานร่วมกัน การสนับสนุนการใช้ปัญญาประดิษฐ์ในการพัฒนาประสิทธิภาพการตรวจจับข้อมูลผิดปกติบนพื้นที่ไซเบอร์และการสื่อสารข้อเท็จจริงแบบทันการณ์ 2) เพิ่มประสิทธิผลการป้องกัน โดยแสวงหาความร่วมมือจากแพลตฟอร์มโซเชียลมีเดียและกลุ่มผู้เชี่ยวชาญความปลอดภัยทางไซเบอร์ รวมถึงพัฒนาทักษะการรู้เท่าทันสื่อและดิจิทัลให้กับประชาชนอย่างทั่วถึง 3) เพิ่มประสิทธิภาพการควบคุมและบรรเทาภัยคุกคาม โดยพัฒนาขีดความสามารถในการสื่อสารเชิงกลยุทธ์ในเชิงรุกไปยังประชาชน รวมถึงการควบคุมและกำกับดูแลด้านข้อมูล แพลตฟอร์มสื่อสังคมออนไลน์ โครงสร้างพื้นฐานให้ครอบคลุมหน่วยงานสำคัญอย่างทั่วถึงและเท่าทันนวัตกรรมดิจิทัล 4) พัฒนาความสามารถในการฟื้นตัว เช่น การสำรองระบบพื้นฐานสารสนเทศที่สำคัญในเขตพรมแดนประเทศไทย ซึ่งจะช่วยส่งเสริมความสามารถในการรับมือกับภัยคุกคามทางข้อมูลของประเทศไทยได้

คำสำคัญ: ภัยคุกคามทางข้อมูล; การปฏิบัติการทางข้อมูล; การปฏิบัติการทางไซเบอร์; สงครามทางปัญญา

บทนำ

ท่ามกลางความขัดแย้งทางภูมิรัฐศาสตร์ คู่ขัดแย้งต่างใช้กลยุทธ์หลากหลายรูปแบบเพื่อชิงความได้เปรียบเหนือศัตรู ทั้งการใช้กองกำลังทหาร การโจมตีทางไซเบอร์ การปฏิบัติการข้อมูลข่าวสาร การปฏิบัติการเชิงจิตวิทยา รวมทั้งมาตรการด้านเศรษฐกิจและพลังงาน ในศตวรรษที่ 21 ความพยายามของประเทศมหาอำนาจในการยึดครองพื้นที่สำคัญเชิงยุทธศาสตร์ของโลกทวีความรุนแรงขึ้น การยึดครองพื้นที่โดยกองกำลังทหารเพียงอย่างเดียวอาจไม่เพียงพอ จึงขยายขอบเขตไปยังการคุกคามทางเศรษฐกิจ การเมือง และพื้นที่ไซเบอร์ (Cyber space) ผนวกกับความก้าวหน้าทางเทคโนโลยีและการเชื่อมต่อของระบบสารสนเทศยิ่งทำให้ขอบเขตและผลกระทบของภัยคุกคามทางข้อมูลขยายวงกว้างขึ้นเป็นอย่างมาก เช่น การแพร่กระจายข้อมูลในพื้นที่ไซเบอร์ การโจมตีทางไซเบอร์ที่ซับซ้อน การประสานการปฏิบัติการแบบเรียลไทม์ทั่วโลก ล้วนเป็นปัจจัยที่ทำให้การรับมือกับภัยคุกคามเป็นเรื่องท้าทายอย่างยิ่ง

ในระยะเวลา 3 ปีที่ผ่านมา ตั้งแต่ปี 2022 เหตุการณ์ความขัดแย้งปะทุขึ้นทั่วโลก ทั้งความขัดแย้งรัสเซีย–ยูเครน ในช่วงเดือนกุมภาพันธ์ 2022 ความขัดแย้งอิสราเอลและกลุ่มฮามาส–ฮิซบอลเลาะห์–อิหร่าน ในเดือนตุลาคม 2023 ความขัดแย้งระหว่างอินเดียและปากีสถานในเดือน พฤษภาคม 2025 ความขัดแย้งในทะเลจีนใต้ รวมถึงความขัดแย้งบริเวณช่องบกระหว่างไทยและกัมพูชาในเดือน พฤษภาคม 2025 จากความขัดแย้งดังกล่าว นอกจากการใช้กองกำลังทหารในการปฏิบัติการยังพบการใช้กลยุทธ์ในรูปแบบอื่นซึ่งมีความยืดหยุ่นและซับซ้อนสูง เช่น การปฏิบัติการทางข้อมูล การปฏิบัติการทางจิตวิทยา การโจมตีทางไซเบอร์ การกดดันทางเศรษฐกิจ และการแทรกแซงทางการเมือง (Reichborn–Kjennerud & Cullen, 2022; Hoffman, 2007; Hajduk & Stępniewski, 2016) เพื่อแย่งชิงความได้เปรียบในพื้นที่สีเทา (Grey zone) ซึ่งไม่สามารถระบุขอบเขตได้อย่างชัดเจน ปราศจากการป้องกัน และมักจะถูกนำมาใช้ประโยชน์ทางการเมืองจากกลยุทธ์อื่น ๆ ที่ไม่ใช่วิธีการทางทหาร รวมถึงบั่นทอนฝ่ายตรงข้ามในด้านต่าง ๆ ได้แก่ การเมือง การทหาร เศรษฐกิจ สังคม ข้อมูล โครงสร้างพื้นฐาน และความสัมพันธ์ระหว่างประเทศ ตามเป้าหมายที่ตนต้องการ (Reichborn–Kjennerud, & Cullen, 2022)

ดังนั้น ในยุคดิจิทัลซึ่งพื้นที่การทำสงครามได้ขยายไปยังพื้นที่ไซเบอร์นั้น การทำความเข้าใจกลยุทธ์การปฏิบัติการข่าวสารจะทำให้ประชาชนเกิดการตระหนักรู้ และเท่าทันคู่ขัดแย้งที่หวังทำลายความมั่นคงของประเทศในด้านต่าง ๆ ทั้งนี้ การถอดบทเรียนมาตรการรับมือของประเทศที่เผชิญหน้ากับสงครามสมัยใหม่ สามารถนำมาใช้เป็นแนวทางให้กับรัฐบาลและหน่วยงานที่เกี่ยวข้องในการวางแผนรับมือ และเตรียมพร้อมมาตรการในการตอบโต้ได้อย่างเหมาะสมเพื่อป้องกันอันตรายและรักษาความมั่นคงของประเทศ โดยเฉพาะการใช้ประโยชน์จากข้อมูลผิดปกติ (Information Disorder) ได้แก่ 1) ข้อมูลบิดเบือน (Disinformation) คือ ข้อมูลที่สร้างขึ้นโดยไม่มีฐานความจริง หรือจริงเพียงบางส่วน มีการบิดเบือนข้อมูลโดยเจตนา เป็นการเลือกใช้ข้อมูลที่มีจุดมุ่งหมายเพื่อสร้างผลกระทบทางการเมืองที่ต้องการ 2) ข้อมูลเท็จ หรือข้อมูลที่ผิด (Mis–information) คือ ข้อมูลที่ไม่จริง ไม่สมบูรณ์ คลุมเครือ ทำให้เข้าใจผิด แต่ผู้เผยแพร่หรือผู้ส่งต่อไม่รู้หรือเชื่อว่าเป็นข้อมูลที่แท้จริง 3) ข้อมูลที่แฝงเจตนาร้าย (Mal–information) คือ ข้อมูลจริงที่ถูกออกแบบ หรือตัดแต่งเพื่อทำให้ผู้รับสารเข้าใจผิดเพื่อนำไปใช้สร้างความเสียหายแก่ผู้อื่น (Wardle & Derakhshan, 2017) เนื่องจากการปฏิบัติการข้อมูลสามารถเข้าถึงพลเรือนเป้าหมายบนพื้นที่ไซเบอร์ได้โดยตรงและส่งผลกระทบต่อการรับรู้และการตัดสินใจได้ทันที

การศึกษานี้มีวัตถุประสงค์เพื่อศึกษารูปแบบการปฏิบัติการทางข้อมูลจากกรณีศึกษาสงครามรัสเซีย–ยูเครนและสงครามฉนวนกาซา และมาตรการรับมือที่มีประสิทธิภาพทั้งในเชิงรุกและเชิงรับ รวมถึงเปรียบเทียบเหตุการณ์ความขัดแย้งระหว่างประเทศไทยและกัมพูชาที่เกิดขึ้นในเดือน พฤษภาคม 2025 เพื่อนำไปสู่ข้อเสนอแนะในการรับมือสำหรับประเทศไทยในมิติต่าง ๆ โดยการรวบรวมข้อมูลที่เกี่ยวข้องจากเอกสารวิชาการ ข่าวสารจากสื่อสำนักข่าว รวมทั้งบทสัมภาษณ์ผู้เชี่ยวชาญที่มีการเผยแพร่อย่างเป็นทางการ และวิเคราะห์เนื้อหาจากกรณีศึกษาเปรียบเทียบกับสถานการณ์ของประเทศไทยเพื่อสังเคราะห์แนวทางการรับมือภัยคุกคามทางข้อมูลที่เหมาะสมสำหรับบริบทของประเทศไทย

ภัยคุกคามทางข้อมูล

ความขัดแย้งที่เกิดขึ้นในหลายเหตุการณ์ทั่วโลกมีการเผชิญกับภัยคุกคามในรูปแบบผสมผสาน (Regan & Sari, 2024) โดยภัยคุกคามแบบผสมผสาน (Hybrid threats) หมายถึง การกระทำที่ดำเนินการโดยรัฐหรือผู้ดำเนินการที่ไม่ใช่รัฐ ซึ่งมีเป้าหมายเพื่อบ่อนทำลายเสถียรภาพ ความมั่นคง และความเชื่อมั่นของประเทศหรือองค์กรเป้าหมาย

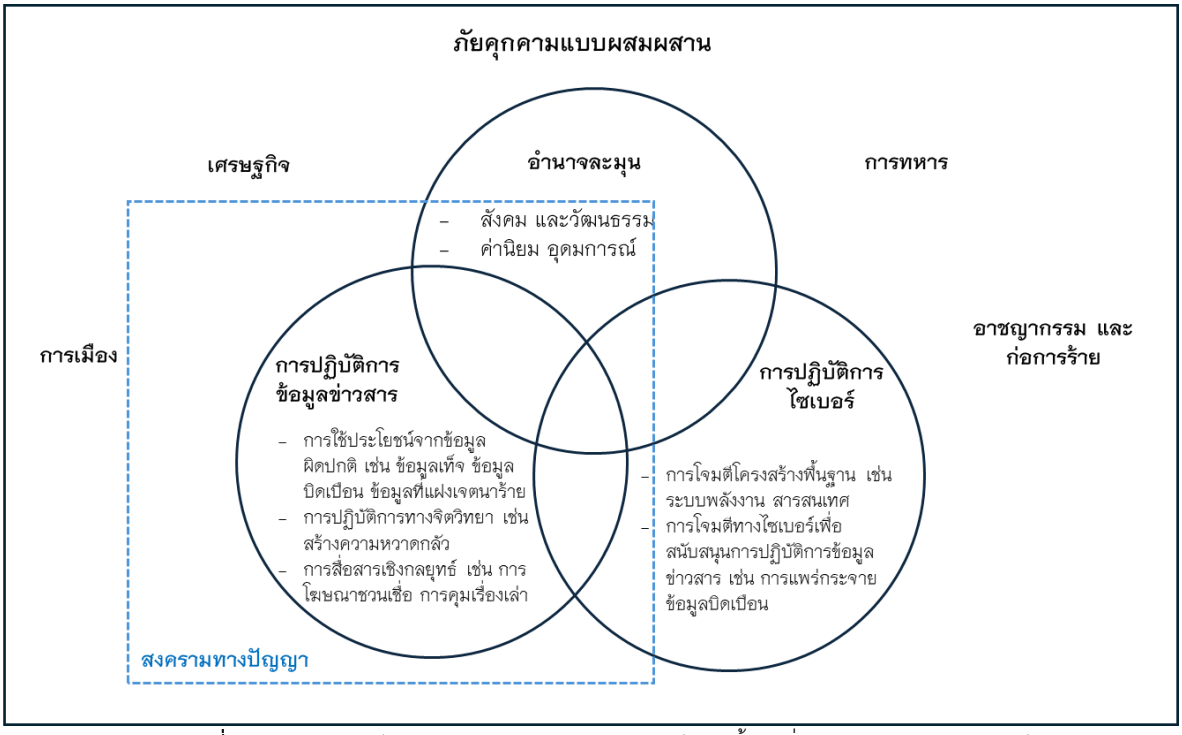
เป็นการประยุกต์กลวิธีที่หลากหลายและมีการเปลี่ยนแปลงตลอดเวลา และมีความซับซ้อนเนื่องจากความสามารถในการดำเนินการในหลายมิติพร้อมกัน ก่อให้เกิดความท้าทายหลายมิติที่ยากต่อการตรวจจับ (Borch & Heier, 2025) โดยมุ่งสร้างความเสียหายทางสังคม เศรษฐกิจ และการเมือง เช่น การบีบบังคับทางเศรษฐกิจ การปฏิบัติการลับ การปฏิบัติการทางข้อมูล การโจมตีทางไซเบอร์ รวมถึงการแทรกแซงทางการเมือง เช่น การสร้างอิทธิพลผ่านช่องทางสื่อสารออนไลน์เพื่อสร้างเรื่องราวทางการเมืองหรือเพื่อปลุกระดม ครอบงำ สั่งการผู้กระทำที่เป็นตัวแทนให้ตัดสินใจหรือดำเนินการตามเป้าหมาย (Seniutienė & Paulauskytė, 2024) ดังนั้น จึงเห็นได้ว่าภัยคุกคามที่เกี่ยวข้องกับกิจกรรมด้านข้อมูลมีบทบาทอย่างมากในการสร้างความได้เปรียบเหนือคู่ขัดแย้ง กลยุทธ์ที่เกี่ยวข้องกับกิจกรรมด้านข้อมูลเชิงรุก เช่น การโฆษณาชวนเชื่อ (Propaganda) การจัดการข้อมูล (Manipulation) การจัดการข้อมูลโดยแทรกแซงจากผู้กระทำต่างประเทศ (Foreign Information Manipulation and Interference: FIMI) และการใช้ประโยชน์จากข้อมูลที่ผิดปกติ (Information disorder) ล้วนเป็นวิธีการที่ต้นทุนต่ำ สามารถกำหนดเป้าหมายได้อย่างเจาะจง และส่งผลกระทบได้ในวงกว้างบนพื้นที่ไซเบอร์ จึงมักถูกนำมาใช้สนับสนุนการใช้กำลังทางทหาร

NATO (2025) ให้นิยามภัยคุกคามทางข้อมูล (Information threats) ว่า เป็นกิจกรรมที่ร่วมกันโดยมีเจตนาร้ายเพื่อใช้ข้อมูลสร้างอันตราย ซึ่งอาจดำเนินการโดยรัฐและองค์กรที่ไม่ใช่รัฐ เช่น กลุ่มแฮกติวิสต์ กลุ่มก่อการร้าย เพื่อทำให้เป้าหมายอ่อนแอและสร้างความแตกแยก กิจกรรมข้อมูลที่เป็นปฏิปักษ์เหล่านี้ใช้กลยุทธ์หลายประเภทเพื่อบิดเบือนความคิดเห็นของสาธารณะ โดยส่งผลอันตรายต่อข้อมูลสารสนเทศ โครงสร้างพื้นฐานสารสนเทศและพื้นที่ไซเบอร์ ซึ่งอาจรวมถึง การโจรกรรมข้อมูล การแพร่กระจายข้อมูลที่ผิดปกติ การเข้าถึง แก้ไข หรือทำลายข้อมูลที่ไม่ได้รับอนุญาติ (Jouini et al., 2014; Molander et al., 1996; Theohary, 2018; Libicki, 1995) จากวิวัฒนาการของพื้นที่ไซเบอร์ที่เกิดขึ้นอย่างรวดเร็วทำให้ผู้เจตนาร้ายเห็นโอกาสในการโจมตีช่องโหว่ใหม่ ๆ เพื่อการปฏิบัติการสร้างความได้เปรียบเหนือคู่ขัดแย้ง โดยการนำข้อมูลมาใช้ในการปฏิบัติการเพื่อสร้างความได้เปรียบบนพื้นที่สีเทา ดังนั้น การจัดการข้อมูล และระบบสารสนเทศจึงมักถูกนำมาใช้ในการสนับสนุนกลยุทธ์ทางการเมืองการทหาร (Politico–military strategies) หรือ นำมาใช้ในยามสงบโดยปราศจากการใช้กำลังทางทหาร

สงครามข้อมูล (Information warfare) คือ การปฏิบัติการข้อมูล (Information operation) เพื่อปกป้องข้อมูลและระบบสารสนเทศของฝั่งเรา และโจมตี หรือสร้างผลกระทบต่อข้อมูลและระบบสารสนเทศของศัตรู ดังนั้น สงครามข้อมูลจึงประกอบด้วย 2 มิติ ได้แก่ *การปฏิบัติการเชิงรับ* และ*การปฏิบัติการเชิงรุก* กล่าวได้ว่า สงครามข้อมูล (Information warfare) คือ การต่อสู้เพื่อควบคุมพื้นที่ข้อมูลในสังคมโดยใช้ข้อมูลและระบบสารสนเทศในการโจมตีเพื่อเอาชนะคู่ต่อสู้ โดยใช้ทุกวิถีทางในการบรรลุและปกป้องการครอบงำข้อมูล (information dominance) เพื่อสนับสนุนกลยุทธ์ทางการเมืองการทหารผ่านการจัดการข้อมูลและรบบสารสนเทศของฝั่งตรงกันข้าม ในขณะเดียวกันก็เพิ่มประสิทธิภาพการปกป้องและความปลอดภัยของข้อมูลในฝั่งตนเองอย่างต่อเนื่อง (Ventre, 2012)

ปัจจุบัน สงครามทางปัญญา (Cognitive warfare) ถูกกล่าวถึงมากขึ้น โดยเป็นแนวคิดที่ขยายขอบเขตจากสงครามข้อมูล สะท้อนถึงการเปลี่ยนแปลงของพื้นที่การต่อสู้บนพื้นที่ไซเบอร์ ในสงครามยุคใหม่ โดยการใช้เทคโนโลยีสารสนเทศ เครื่องมือ เครือข่าย และระบบที่เกี่ยวเนื่อง โดยมุ่งเป้าโจมตีสติปัญญาของปัจเจกบุคคลและกลุ่มบุคคลโดยการเปลี่ยนแปลง ชี้นำ ความคิดของผู้นำ กลุ่มคน สังคม และประชากรเป้าหมายให้เปลี่ยนแปลงการรับรู้ของแต่ละคนโดยไม่รู้ตัวว่าถูกกระทำผ่านการปฏิบัติการ ทั้งนี้เพื่อเป้าหมายที่แตกต่างกันไป เช่น ชัยชนะเหนือดินแดน การสร้างอิทธิพลทางความคิด การขโมยข้อมูล การปลุกปั่นสร้างความแตกแยก เป็นต้น (Claverie & Du Cluzel, 2022) สงครามทางปัญญา ได้ถูกนิยามว่าเป็นการกระทำที่ของรัฐหรือกลุ่มอิทธิพลที่ต้องการจะจัดการกลไก

การรับรู้ของศัตรูหรือพลเมืองของตน เพื่อให้อ่อนแอลงโดยแทรกซึม สร้างอิทธิพล ทำลายกลไกการรับรู้ โดยผสมผสานระหว่างเทคนิคทางไซเบอร์ใหม่ๆ ที่เกี่ยวข้องกับสงครามข้อมูล อำนาจละมุน (Soft power) พร้อมด้วยการปฏิบัติการทางจิตวิทยา (Psyop) ซึ่งเกี่ยวข้องกับการนำเสนอความเป็นจริงอย่างมีอคติ (Bias) และมักถูกดัดแปลงทางดิจิทัลเพื่อเอื้อต่อผลประโยชน์ของตนเองบนพื้นที่การปฏิบัติการใหม่ ซึ่งสามารถแพร่กระจายไปยังทุกพื้นที่ที่มีการใช้ข้อมูลดิจิทัล เป็นการผสมผสานระหว่างกระบวนการโจมตีศัตรูกับมาตรการตอบโต้และป้องกันพื้นที่ในฝั่งของตน (Underwood, 2017; Claverie & Du Cluzel, 2022; Backes & Swab, 2019) ซึ่งสามารถสรุปได้ดังภาพที่ 1



ภาพที่ 1 สรุปภาพรวมภัยคุกคามแบบผสมผสาน การปฏิบัติการข้อมูลข่าวสาร และสงครามทางปัญญา

Figure 1 Overview of hybrid threats, information operations, and intellectual warfare.

กรณีศึกษาการปฏิบัติการทางข้อมูลในสงครามสมัยใหม่

การปฏิบัติการทางข้อมูลมีบทบาทอย่างมากในการสร้างความได้เปรียบระหว่างคู่ขัดแย้ง โดยมีการใช้กลยุทธ์ในหลากหลายรูปแบบดังสะท้อนให้เห็นจากสงครามรัสเซีย–ยูเครน และสงครามกาซา ดังนี้

การปฏิบัติการข้อมูลโดยรัสเซีย

การปฏิบัติการข้อมูลเชิงรุก ตั้งแต่ปี 2022 พบว่า มีการสร้างและเผยแพร่ข่าวปลอมผ่านเว็บไซต์และสื่อสังคมออนไลน์ เช่น สร้างเว็บไซต์ปลอมกว่า 100 แห่งที่เลียนแบบสื่อชื่อดัง อาทิ Fox News และ The Wall Street Journal เพื่อเผยแพร่ข่าวเท็จเกี่ยวกับยูเครนและพันธมิตรตะวันตก ในปี 2022 มีรายงานเกี่ยวกับปฏิบัติการ Doppelgänger ซึ่งเป็นหนึ่งในแคมเปญที่ใช้เว็บไซต์ปลอมและบัญชีสื่อสังคมออนไลน์ เพื่อเผยแพร่ข้อมูลที่บิดเบือนเกี่ยวกับยูเครน ทั้งยังใช้เครือข่าย Troll farms ในการสร้างเนื้อหามากกว่า 1,300 ข้อความ และ 37,000 คอมเมนต์ต่อสัปดาห์ บนสื่อสังคมออนไลน์ในยูเครน รวมถึงการใช้เครือข่าย Pravda (AI chatbot) เผยแพร่เนื้อหาประมาณ 3.6 ล้านบทความต่อปี ผ่านเว็บไซต์ในหลายภาษา รวมทั้ง Wikipedia และ AI chatbots นอกจากนี้ รัสเซียใช้เทคโนโลยีปัญญาประดิษฐ์ (AI)

เพื่อสร้างวิดีโอและบทความปลอมที่ดูน่าเชื่อถือ โดย NewsGuard ได้ระบุและหักล้างข้อกล่าวหาเท็จ 302 ข้อที่เกี่ยวข้องกับสงคราม ซึ่งส่วนใหญ่มีที่มาจากการโฆษณาชวนเชื่อของรัสเซีย เช่น การกล่าวหาว่า ยูเครนสร้าง “Dirty bomb” ที่เชอร์โนบิล การกล่าวหา USAID ว่า ใช้เงินภาษีเพื่อจ้างคนดังมาเยือนยูเครน ซึ่งได้รับการชมกว่า 31 ล้านครั้ง ก่อนถูกหักล้างข้อมูลเท็จ อีกทั้ง เผยแพร่ข่าวปลอมที่อ้างว่ามีความขัดแย้งระหว่างผู้นำทางการเมืองและทหารของยูเครน เพื่อบ่อนทำลายความเป็นเอกภาพของยูเครน เช่น เผยแพร่ข้อความโจมตีเซเลนสกี้เกี่ยวกับการคอร์รัปชัน โดยใช้ TikTok มากกว่า 12,800 บัญชี ปล่อยเนื้อหามีผู้ชมหลายร้อยล้านครั้ง รวมถึงการเตรียมข้อมูลสำหรับโมเดลภาษาขนาดใหญ่ (Large Language Model: LLM) โดยเติมเต็มข้อมูลปลอมเพื่อให้ AI นำข้อมูลเหล่านี้ไปใช้ซ้ำในคำตอบ ทั้งยังพบคลิปวีดิโอสื่อลวงลึก (Deep fake) เช่น ภาพประธานาธิบดียูเครนบอกทหารให้วางอาวุธ ในเดือนมกราคม 2022 เว็บไซต์รัฐบาลยูเครนและหน่วยงานรัฐถูกโจมตีกว่า 70 แห่ง โดยเผยแพร่ข้อความขู่ “จงกลัวและจงรอสิ่งที่เลวร้าย” ภาษารัสเซีย โปแลนด์ และยูเครน อีกทั้งมีการโจมตี DDoS เว็บไซต์กระทรวงกลาโหมและธนาคารในยูเครน โดยตั้งแต่ ปี 2022 ถึง 2025 รัสเซียได้ดำเนินการปฏิบัติการข้อมูลต่อยูเครนและพันธมิตรตะวันตก อย่างต่อเนื่อง เพื่อบ่อนทำลายความเชื่อมั่น สร้างความสับสน และลดการสนับสนุนจากนานาชาติ

ในขณะเดียวกันรัสเซีย ดำเนินปฏิบัติการข้อมูลต่อพลเมืองตนเองหลายรูปแบบ เช่น *การควบคุมเรื่องเล่า* (Narrative control) เพื่อสร้างความชอบธรรมในการรุกรานยูเครน โดยปูตินอ้างว่าการรุกรานยูเครนจะเป็นการกำจัดนาซียูเครน (Denazify) และการปฏิบัติการทหารในแคว้นดอนบาสนั้นเพื่อปกป้องชะตากรรมของประชาชน 4 ล้านคน ที่เสี่ยงต่อการฆ่าล้างเผ่าพันธุ์ (Genocide) รัสเซียได้ *บิดเบือน*ประวัติศาสตร์โดยอ้างว่ายูเครน ไม่มีอัตลักษณ์หรือรัฐชาติของตนเอง (Düben, 2023) *การโฆษณาชวนเชื่อ* (Propaganda) ผ่านสื่อของรัฐอย่าง RT และ Sputnik รวมถึงเครือข่ายบัญชีปลอม (Bot networks) และ Troll farms เพื่อเผยแพร่โฆษณาชวนเชื่อที่สนับสนุนการกระทำของตนในยูเครน บิดเบือนข้อมูลที่มาจากยูเครนและตะวันตก และสร้างความชอบธรรมให้กับสงคราม

มาตรการรับมือภัยคุกคามทางข้อมูลของรัสเซีย มีความครอบคลุมในทุกมิติทั้งมีการบูรณาการร่วมกันระหว่างหน่วยงานและมีเอกภาพค่อนข้างสูง ได้แก่ รัฐบาลรัสเซียได้เพิ่มการควบคุมสื่อและสารสนเทศภายในประเทศ เช่น *กฎหมายควบคุมสื่อ ปี 2014* ให้อำนาจ Roskomnadzor ซึ่งเป็นหน่วยงานกำกับดูแลสื่อ ในการบล็อกเว็บไซต์/บัญชีโดยไม่ต้องมีคำสั่งศาล *กฎหมาย Yarovaya* กำหนดให้บริษัทโทรคมนาคมและอินเทอร์เน็ตเก็บข้อมูลการสื่อสารทั้งหมดไว้สูงสุด 6 เดือน และ metadata นาน 3 ปี รวมถึง Telegram ต้องให้หน่วยข่าวกรอง (Federal Security Service: FSB) เข้าถึงเนื้อหาการสนทนา *กฎหมายข่าวปลอม ปี* 2019 *และ 2022* ระบุบทลงโทษอย่างรุนแรงต่อการเผยแพร่ ข้อมูลเท็จเกี่ยวกับกองทัพรัสเซีย หรือการบ่อนทำลายรัฐบาล สูงสุดถึง 15 ปี เพื่อควบคุมการเล่าเรื่องภายในประเทศและป้องกันข้อมูลที่ขัดแย้งกับแนวทางของรัฐบาลไม่ให้แพร่หลาย (Sherstoboeva, 2024) *กฎหมายห้ามดูหมิ่นรัฐ ปี 2019* ห้ามเผยแพร่เนื้อหาที่ไม่เคารพต่อรัฐ โดย Roskomnadzor มีสิทธิ์บล็อกเว็บไซต์ทันที นอกจากนี้ยังกำหนดให้บริษัทเทคโนโลยีต้องให้เครื่องมือช่วยถอดรหัสข้อความ (Backdoors) ให้กับหน่วยข่าวกรอง (FSB) ซึ่งสามารถขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ตหรือโทรคมนาคมโดยไม่ต้องมีหมายศาล และใช้ระบบ System of Operative–Search Measures (SORM) ดักฟังข้อมูลที่สามารถเข้าถึงโดยตรงจากผู้ให้บริการอินเทอร์เน็ตและโทรศัพท์ (Topor & Tabachnik, 2021) การป้องกันการแทรกแซกจากต่างประเทศ เช่น *กฎหมายต่อต้านตัวแทนต่างชาติ ปี 2012 และ 2022* กำหนดให้องค์กรไม่แสวงหากำไร (NGOs), สื่อ, บุคคลธรรมดา ที่ได้รับเงินทุนจากต่างชาติและดำเนินกิจกรรมทางการเมือง รวมถึงบุคคลใด ๆ ที่อยู่ภายใต้อิทธิพลของต่างชาติต้องขึ้นทะเบียน เปิดเผยแหล่งทุน และรายงานการทำงาน อธิปไตยอินเตอร์เน็ต *กฎหมายอินเทอร์เน็ตอธิปไตย* ปี 2019 ให้อำนาจรัฐแยกโครงสร้าง

อินเทอร์เน็ตรัสเซียออกจากเครือข่ายโลกได้ ปิดกั้นสื่ออิสระและแพลตฟอร์มต่างประเทศ รวมถึงแพลตฟอร์มสื่อสังคมออนไลน์ตะวันตก เช่น Facebook, Instagram และ Twitter เพื่อควบคุมข้อมูลที่เข้าถึงพลเมืองรัสเซีย (Done, 2021) สร้างเครือข่ายพันธมิตร เช่น *กลุ่มแฮกติวิสต์ที่สนับสนุนรัสเซีย* เช่น Killnet และสร้างเครือข่ายกับกลุ่มอิทธิพลสนับสนุนรัสเซียและเบลารุส เพื่อลดการพึ่งพาและกระตุ้นความรู้สึกต่อต้านตะวันตก ทั้งมีรายงานว่ารัสเซียใช้*เทคโนโลยี Deepfake* เพื่อบิดเบือนข้อมูลและลดความน่าเชื่อถือของฝ่ายตรงข้าม รวมถึง*การบล็อกและรบกวนสัญญาณ* ในการเผยแพร่ข้อมูลตอบโต้เพื่อหักล้าง โดยบูรณาการทำงานกับหลายหน่วยงานที่เกี่ยวข้อง เช่น Federal Security Service (FSB) Internet Research Agency (IRA) สำนักข่าว RT Ministry of Digital Development, General Staff of the Armed Forces (GRU)

การปฏิบัติการข้อมูลโดยยูเครน

การปฏิบัติการข้อมูลเชิงรุก มีการดำเนินการในหลากหลายรูปแบบ เช่น การใช้แพลตฟอร์มต่าง ๆ เช่น Telegram, Twitter และ TikTok เพื่อเผยแพร่ข้อมูลเกี่ยวกับความสำเร็จของกองทัพยูเครน และการสูญเสียของรัสเซีย รวมทั้งได้ผลิตและเผยแพร่เนื้อหาที่มีอารมณ์ร่วม เช่น ในปี 2022 วิดีโอและรูปภาพของนักบินยูเครนที่ได้รับฉายาว่า “ผีแห่งเคียฟ” (Ghost of Kyiv) ยิงเครื่องบินขับไล่ของรัสเซียตก 6 ลำในช่วง 30 ชั่วโมงแรกของสงครามถูกแชร์ไปทั่วโลกออนไลน์ แต่ภายหลังได้รับการพิสูจน์ว่าเป็นเท็จ ในเดือนเมษายน 2024 กลุ่มแฮกเกอร์ ได้ดำเนินการแฮกกล้องวงจรปิด (CCTV) และระบบเฝ้าระวังในแคว้นคูร์สก์ (Kursk Oblast) ของรัสเซีย และแสดงภาพสงครามผ่านทางโทรทัศน์ของรัสเซียในพื้นที่ดังกล่าว เพื่อแสดงให้เห็นถึงความสูญเสียของรัสเซียในเมืองซุดชา (Sudzha) ซึ่งตั้งอยู่ในแคว้นคูร์สก์ ทั้งมีการใช้ซอฟท์แวร์ Clearview AI ระบุตัวตนศพของทหารรัสเซีย และเผยแพร่ข้อมูลสู่ครอบครัวเพื่อเป็นการดูหมิ่นเหยียดหยาม (Humiliation offensive) เพื่อลดขวัญกำลังใจรัสเซีย นอกจากนั้น ยูเครนใช้การโจมตีทางไซเบอร์ เช่น การแฮ็กเว็บไซต์รัสเซียเพื่อเล่นเพลงชาติยูเครนบนเว็บไซต์รัสเซีย หรือปล่อยข้อความหยุดยั้งสงคราม

ในทางตรงกันข้าม ยูเครนดำเนินการปฏิบัติการข้อมูลและจิตวิทยาต่อพลเมืองตนเองเช่นกันเพื่อสร้างความเชื่อมั่นให้กับประชาชนและพันธมิตรระหว่างประเทศ เช่น เผยแพร่ภาพของประชาชนที่ได้รับผลกระทบจากการรุกรานของรัสเซีย เพื่อสร้างความเห็นอกเห็นใจและสนับสนุนจากประชาคมโลก โดยการเผยแพร่ข้อมูลที่ถูกต้องและทันสมัยผ่านสื่อสังคมออนไลน์เพื่อเผยแพร่ข้อมูลและหักล้างข้อมูลเท็จอย่างมีประสิทธิภาพ โดยเน้นการเผยแพร่เนื้อหาที่มีอารมณ์ร่วมเพื่อสร้างความเห็นอกเห็นใจและสนับสนุนจากประชาคมโลก (Erlich & Garner, 2021) ยูเครนได้เน้นย้ำเรื่องราวของความกล้าหาญ ความเป็นเอกภาพ และความมุ่งมั่นในการปกป้องอธิปไตย รวมถึงเรื่องราวชัยชนะ ซึ่งเป็นเรื่องเล่าที่แข็งแกร่งที่ช่วยสร้างขวัญกำลังใจให้กับประชาชนยูเครน (Levin, 2025)

มาตรการรับมือภัยคุกคามทางข้อมูลของยูเครน มีการดำเนินการเปิดเผยข้อมูลเชิงรุกและรวดเร็วโดยใช้กลยุทธ์การสื่อสารที่เปิดเผยและรวดเร็ว ซึ่งมีแนวทาง “เสียงเดียว” (One Voice) เพื่อให้แน่ใจว่าข้อความจากรัฐบาลมีความสม่ำเสมอ ทันเหตุการณ์เพื่อสนับสนุนประชาธิปไตย และความกล้าหาญของชาวยูเครน โดยประธานาธิบดีเซเลนสกี้ *ใช้ช่องทางโซเชียลมีเดีย*ต่างๆ เช่น Telegram เพื่อสื่อสารโดยตรงกับประชาชนยูเครนและประชาคมโลกต่อต้านการบิดเบือนข้อมูลของรัสเซีย มี*การรวมศูนย์สื่อหลัก* เพื่อป้องกันการข้อมูลบิดเบือน โดยมีช่องข่าวหลักรวมเป็นแพลตฟอร์ม United News ที่มีกระทรวงวัฒนธรรม และสื่อหลักร่วมมือกันเสนอรายการเทเลธอน (Telethon) ข่าวสารร่วม ทั้งยัง *ใช้ AI ตรวจสอบโซเชียลมีเดีย* ผ่าน เช่น เทคโนโลยีของสตาร์ทอัพ อาทิ Osavul และ Mantis Analytics เพื่อตรวจจับข้อมูลเท็จจากรัสเซียเพื่อหักล้างข้อมูลเท็จแบบทันเหตุการณ์ หรือการวิเคราะห์ข้อมูลจากข่าวกรองแหล่งข้อมูลเปิด (Open Source Intelligence: OSINT) อาทิ Molfar และสื่อสารข้อมูลไปยังประชาชนผ่านบัญชีสื่อ

สังคมออนไลน์ต่าง ๆ เช่น @AlertBot_UA, @StopFakeBot, @UkraineWarBot ส่วนกฎหมายที่เกี่ยวข้อง เช่น *Cybersecurity law* ปี 2017, 2022 สร้างระบบการกำกับดูแลด้านความมั่นคงไซเบอร์ทั้งภาครัฐและเอกชนผ่านระบบความปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity System) Presidential Decree No. 152/2022 ซึ่งเกี่ยวกับความร่วมมือในการเสนอข้อมูลข่าวสาร (Opryshko, 2023) และสร้างเครือข่ายพันธมิตร *ตรวจสอบข้อเท็จจริง* (Fact-checking) ที่นำโดยพลเมือง (StopFake, InformNapalm, VoxCheck), ชุมชนอาสาสมัครออนไลน์ เช่น North Atlantic Fella Organization *การระดมพล "กองทัพ IT"* (IT Army of Ukraine) ยูเครนได้ก่อตั้ง "IT Army" ซึ่งเป็นการรวมตัวของอาสาสมัครด้านเทคโนโลยีและแฮกทิวิสต์ทั่วโลก โดยเปิดอาสาสมัครผ่าน Telegram เพื่อทำการโจมตีทางไซเบอร์ต่อรัสเซีย รวมถึงการช่วยเผยแพร่ข้อมูลที่ถูกต้องและต่อต้านการบิดเบือนข้อมูล (Done, 2023) *การทำงานร่วมกับแพลตฟอร์มออนไลน์* เพื่อระบุและลบเนื้อหาที่บิดเบือน และโฆษณาชวนเชื่อของรัสเซีย อีกทั้งใช้ข้อมูลจาก *หน่วยข่าวกรองของตนเองและพันธมิตร* เช่น NATO, Five eyes เพื่อเปิดเผยแผนการบิดเบือนข้อมูลของรัสเซียและให้ข้อมูลที่ถูกต้องแก่สาธารณะชน นอกจากนั้น ยังมีการจัดตั้งศูนย์ต่อต้านการบิดเบือนข้อมูล ยูเครนมีหน่วยงานที่มุ่งเน้นการต่อต้านการบิดเบือนข้อมูลโดยเฉพาะ เพื่อวิเคราะห์และตอบโต้ปฏิบัติการข้อมูลข่าวสารของรัสเซีย เช่น หน่วยงานความมั่นคงที่ต่อสู้กับปฏิบัติการข้อมูลบิดเบือน ข่าวปลอม และสงครามข้อมูลจากรัสเซีย (The Center for Countering Disinformation: CCD) หน่วยข่าวกรอง (Main Directorate of Intelligence of the Ministry of Defense of Ukraine: GUR/HUR MO) หน่วยงานกลางวางยุทธศาสตร์การสื่อสารภาครัฐและการรู้เท่าทันสื่อ (Center for Strategic Communications and Information Security: StratCom) และ Computer Emergency Response Team of Ukraine (CERT-UA) ซึ่งเป็นหน่วยงานรับมือเหตุการณ์ความมั่นคงทางไซเบอร์ระดับชาติของยูเครน (Marushchak et al., 2025) อีกทั้งสร้างความรู้เท่าทันสื่อ อาทิ โครงการ *Filter media literacy* (International Media Support, 2025) *การใช้ข่าวกรองจากแหล่งข้อมูลเปิด* Open-Source Intelligence: OSINT) เช่น Bellingcat ซึ่งเป็นองค์กรสืบสวนข่าวเชิงลึก (investigative journalism organization) นอกจากนี้ยูเครนได้สร้างระบบสำรองโครงสร้างพื้นฐานการสื่อสาร เช่น Starlink การย้ายข้อมูลของรัฐไปยังระบบคลาวด์ภายใต้โครงการ Backup Ukraine

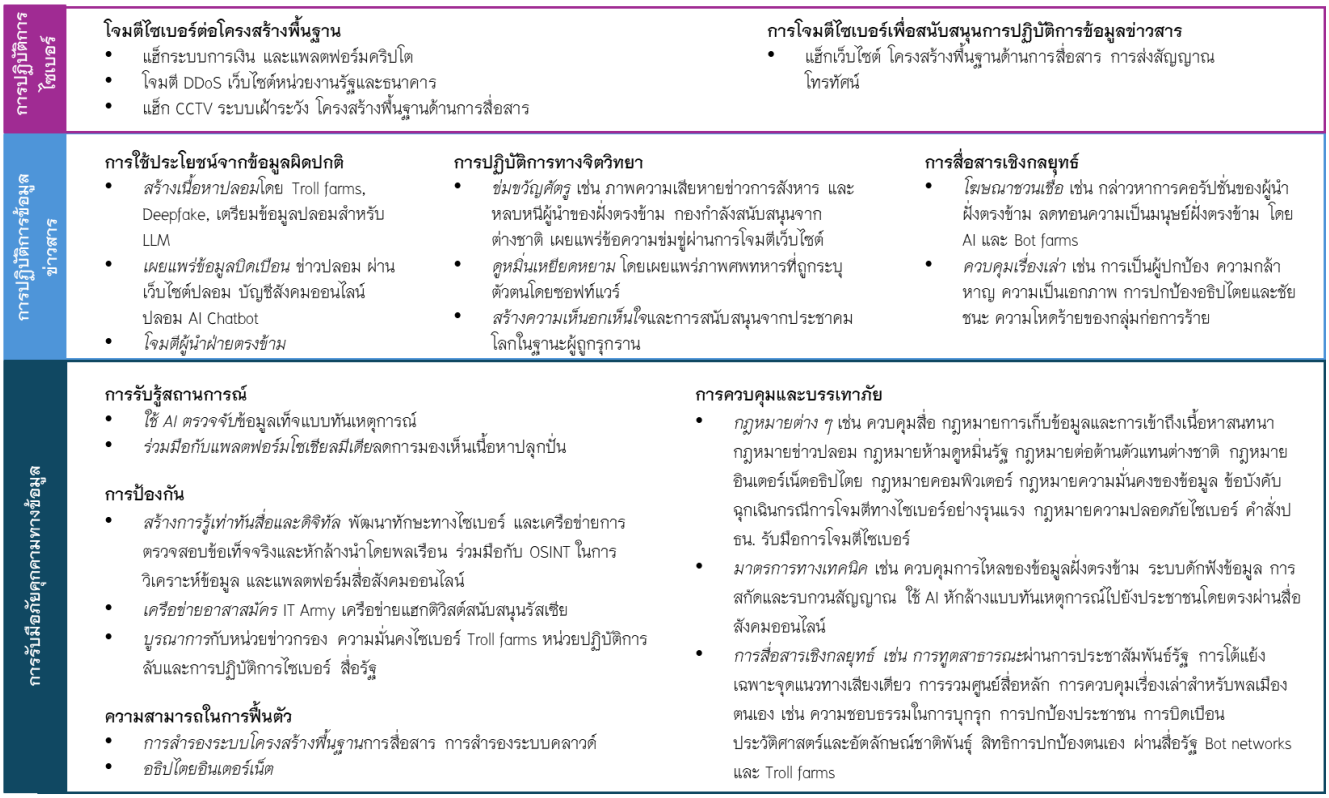
การปฏิบัติการข้อมูลโดยอิสราเอล

การปฏิบัติการข้อมูลเชิงรุก ตั้งแต่การบุกโจมตีของกลุ่มฮามาส ในวันที่ 7 ตุลาคม 2023 พบว่า ในช่องทางสื่อสังคมออนไลน์ เช่น X หรือ Twitter, TikTok, Youtube มีการเผยแพร่ข้อมูลเท็จ (Misinformation) ในหลากหลายรูปแบบทั้งภาพ คลิปวีดิโอ และข้อมูลต่าง ๆ เป็นจำนวนมาก เช่น กรณีคลิปวิดีโอที่อ้างว่าชาวปาเลสไตน์แสดงเป็นผู้ได้รับบาดเจ็บสาหัสแต่สามารถเดินออกจากโรงพยาบาลได้ในวันถัดไปแต่ความจริงคือเป็นคลิปวิดีโอของผู้ได้รับบาดเจ็บคนละราย กรณีคลิปวิดีโอแสดงให้เห็นทหารนาวิกโยธินสหรัฐ จำนวนมากเดินทางมาถึงสนามบินในอิสราเอลท่ามกลางสงครามที่ดำเนินอยู่แต่ความจริงคือเป็นวิดีโอในปี 2022 และแสดงให้เห็นทหารจากกองพลทหารอากาศที่ 101 ของกองทัพบกสหรัฐกำลังเดินทางมาถึงโรมาเนีย ทั้งยังมีรายงานการใช้ AI สร้างข่าวปลอม โดยอ้างว่ามีการประท้วงสนับสนุนอิสราเอลในอิหร่าน กรณีที่อิสราเอลลอบสังหารนักวิทยาศาสตร์นิวเคลียร์และผู้นำทหารระดับสูงของอิหร่าน แต่ Ismail Qaani ซึ่งถูกรายงานว่าเสียชีวิตจากการโจมตีโดยอิสราเอล ปรากฏตัวต่อหน้าสาธารณชนในเวลาต่อมา นอกจากนี้ มีรายงานว่า กลุ่ม “Predatory Sparrow” ที่เชื่อมโยงกับอิสราเอล เจาะระบบการเงินอิหร่าน และแพลตฟอร์มคริปโต Nobitex สูญเงินกว่า 90 ล้านดอลลาร์ ทั้งอิสราเอลแจ้งเหตุร้ายไปยังนายพลระดับสูงของอิหร่านให้หลบหนี เพื่อสร้างความหวาดกลัวกับศัตรู

ในขณะที่ อิสราเอล ได้ดำเนินการปฏิบัติการข้อมูลและจิตวิทยาต่อพลเมืองตนเองเช่นกัน โดย IDF ออกมายอมรับว่า หน่วยงานโฆษกของกองทัพอิสราเอลเปิดบัญชีสื่อสังคมออนไลน์ปลอมและใช้ประโยชน์จากบัญชีที่มีอยู่เพื่อสร้างทัศนคติเชิงบวกต่อปฏิบัติการในฉนวนกาซา ในปี 2021 โดยสร้างและควบคุมเรื่องเล่าผ่านช่องทางสื่อทั้งแบบดั้งเดิมและสื่อสังคมออนไลน์เกี่ยวกับการดำเนินการทางทหารของตน โดยเน้นย้ำถึงสิทธิในการป้องกันตนเอง และการแสดงให้เห็นถึงความรุนแรงของฮามาส ซึ่งอิสราเอลถูกบังคับใช้โจมตี แต่ก็มีการกำหนดเป้าหมายอย่างแม่นยำ โดยหลังเหตุการณ์ 7 ตุลาคม 2023 รัฐบาลอิสราเอลจ้างโฆษณาออนไลน์และเผยแพร่คลิปเหตุการณ์ความโหดร้ายของฮามาสผ่านสื่อตะวันตก โดยมีรายงานว่าใช้เงินมากกว่า 7 ล้านดอลลาร์บน YouTube, X, TikTok, เกมออนไลน์ และสื่อภาพยนตร์ เพื่อสร้างเรื่องเล่าว่าอิสราเอลปฏิบัติการเพื่อป้องกันตัว

มาตรการรับมือภัยคุกคามทางข้อมูลของอิสราเอล อิสราเอลใช้หลักการ Hasbara 2.0 คือ การอธิบายซึ่งเป็นเทคนิคทางการทูตสาธารณะ ในการประชาสัมพันธ์รัฐ และโต้ตอบภาพลักษณ์เชิงลบจากนานาชาติด้วยการโต้แย้งเฉพาะจุด (Precision rebuttals) ผ่านเรื่องเล่าในแพลตฟอร์มสื่อสังคมออนไลน์ (Aouragh, 2016; TRT World, 2024) เพื่อส่งเสริมการฟังอย่างเลือกสรร (Selective listening) ในการต่อต้านการก่อการร้าย สร้างความชอบธรรมในการป้องปรามแบบบูรณาการ ทั้งนี้ กฎหมายที่เกี่ยวข้อง ได้แก่ *Computer Law* กำหนดความผิดเกี่ยวกับการเข้าถึงข้อมูลโดยมิชอบ การรบกวนหรือทำลายข้อมูลในระบบคอมพิวเตอร์ *Classified Information Protection Laws* เป็นกฎหมายความมั่นคงของข้อมูลที่ใช้ในกองทัพ *ข้อบังคับฉุกเฉิน* เช่น Iron Swords (Temporary Law on Handling Severe Cyberattacks in the Digital and Storage Services Sector 5774–2023) ในกรณีที่การโจมตีทางไซเบอร์อย่างรุนแรง โดยมีหน่วยงานความมั่นคงทางไซเบอร์แห่งชาติอิสราเอล (Israel National Cyber Directorate – INCD) ออกแนวปฏิบัติภาคบังคับและควบคุมผ่านหน่วยงานเฉพาะในการปกป้องพื้นที่ไซเบอร์ โดยทำงานอย่างใกล้ชิดกับกองกำลังป้องกันประเทศอิสราเอล (Israel Defense Force: IDF) เช่น Unit 8200 หน่วยข่าวกรอง Shin Bet (Barucija, 2020) และหน่วยลับ Influence Unit ที่เผยแพร่ข่าวในสื่อ นอกจากนี้ อิสราเอลควบคุมการไหลของข้อมูลจากกาซา โดยจำกัดการไหลของข้อมูลออกจากฉนวนกาซา และโจมตีโครงสร้างพื้นฐานด้านการสื่อสาร เช่น อินเทอร์เน็ตและโทรศัพท์ในพื้นที่กาซา การตอบโต้ข้อมูลบิดเบือน (Counter–Disinformation) โดยมักจะใช้หลักฐานจากวิดีโอ กล้องวงจรปิด และข้อมูลข่าวกรองในการเปิดเผยข้อเท็จจริง อีกทั้งยังทำงานร่วมกับแพลตฟอร์มโซเชียลมีเดีย อิสราเอลได้ล็อบบี้แพลตฟอร์มสื่อสังคมออนไลน์ให้ลดการมองเห็นเนื้อหาที่สนับสนุนฮามาสหรือเนื้อหาที่ยุยงปลุกปั่น นอกจากนี้ อิสราเอลได้ใช้ AI และ Bot Farms ในการเผยแพร่ข้อมูลและโฆษณาชวนเชื่อ เพื่อลดทอนความเป็นมนุษย์ของชาวปาเลสไตน์ และสร้างแรงกดดันต่อฝ่ายตรงข้าม นอกจากนี้ ยังได้สร้างระบบสำรองโดยใช้แพลตฟอร์มคลาวด์ในการจัดเก็บข้อมูลของรัฐจากทั้งภายในประเทศ (Project Nimbus) และจากพันธมิตร เช่น Google/AWS สำหรับการสร้างการตระหนักรู้ให้กับประชาชน เช่น โครงการส่งเสริม OSINT ในภาคการศึกษาและประชาชน โครงการ Magshimim พัฒนาทักษะทางไซเบอร์ให้กับเยาวชน (Cordey, 2019) รวมถึงสร้างการมีส่วนร่วมกับพลเมือง เช่น โครงการ Fake news watchdogs การจัดกิจกรรม Hackathon ร่วมกับบริษัทเทคในเทลอาวีฟ เพื่อพัฒนาเครื่องมือวิเคราะห์โซเชียลมีเดีย วัดผลกระทบของข้อความ (sentiment meter) และปรับกลยุทธ์แบบเรียลไทม์

ทั้งนี้รูปแบบการปฏิบัติการทางข้อมูลและมาตรการรับมือภัยคุกคามจากกรณีศึกษาสามารถสรุปได้ ดังแสดงในภาพที่ 2



ภาพที่ 2 สรุปรูปแบบการปฏิบัติการข้อมูลข่าวสาร และการรับมือภัยคุกคามทางข้อมูลจากคู่ขัดแย้งจากกรณีศึกษา

Figure 2 Information Operations Models and Information Threat Response Models from Conflict Parties from Case Studies

มาตรการรับมือคุกคามทางข้อมูลในสงครามทางปัญญา

France 24 (2025) ได้ติดตามและระบุแคมเปญข้อมูลปลอมของรัสเซียกว่า 80 รายการระหว่างปี 2023 ถึง 2025 ดังนั้น เพื่อรับมือกับภัยคุกคามดังกล่าว NATO (2025) จึงเสนอกรอบมาตรการในการรับมือภัยคุกคามโดยเฉพาะภัยคุกคามจากข้อมูลซึ่งเกิดจากข้อมูลที่ผิดปกติ โดยเน้นแนวทางที่ประชาชนเป็นศูนย์กลาง ซึ่งไม่ได้เน้นที่การปฏิบัติการข้อมูลเชิงรุกหรือการควบคุมแบบรวมศูนย์ แต่เน้นที่การเพิ่มอำนาจให้กับพลเมืองในการประเมินข้อมูลอย่างมีวิจารณญาณ ได้แก่

การรับรู้สถานการณ์ คือ การตระหนักถึงความท้าทาย ติดตาม ตรวจสอบ และพัฒนากลยุทธ์ เช่น สร้างการตระหนักรู้เกี่ยวกับสงครามทางปัญญา รวมถึง การทำความเข้าใจสภาพแวดล้อมของข้อมูล การติดตามและวิเคราะห์ข้อมูล รวมถึงการตรวจสอบและระบุแหล่งที่มาของภัยคุกคาม เพื่อวางแผนและกำหนดรูปแบบการตอบสนองของต่อภัยคุกคามข้อมูลว่าเข้าข่ายภัยคุกคามข้อมูลจากต่างชาติหรือไม่ และสามารถประเมินประสิทธิผลของการสื่อสารสาธารณะของตนเองได้จากสภาพแวดล้อมข้อมูลผ่านการตรวจสอบและวิเคราะห์สื่อเป็นประจำ

การเพิ่มประสิทธิผลการป้องกันภัยคุกคามข้อมูล โดย*การแบ่งปันข้อมูล* ที่ถูกต้องในเชิงรุก ผ่านการสื่อสารสาธารณะที่เปิดเผย โปร่งใส และชัดเจน การ*ส่งเสริมการรู้เท่าทันสื่อ* และการฝึกอบรม เพื่อสร้างความยืดหยุ่นของสังคมต่อภัยคุกคามข้อมูล รวมถึง*สร้างพันธมิตร* สื่อมวลชน นักข่าว ให้มีส่วนร่วมกับสาธารณชนผ่านช่องทางต่างๆ รวมถึงสื่อสังคมออนไลน์ และองค์กรระหว่างประเทศ แพลตฟอร์มออนไลน์ ตลอดจนผู้มีส่วนได้ส่วนเสียอื่นๆ จากภาคประชาสังคมทั้งในและนอกประเทศ

การควบคุมและบรรเทาภัยคุกคามข้อมูล ตัวเลือกในการตอบสนองตั้งแต่ *การออกกฎหมายและควบคุมในประเทศ* เช่น การติดตาม กำกับ ดูแล ตรวจจับ ลงโทษ การตรวจสอบแหล่งข้อมูลและหักล้างข้อมูลเท็จจาก OSINT *การสื่อสารเชิงกลยุทธ์* เช่น การปฏิบัติการหลายมิติ การสื่อสารในภาวะวิกฤติ การควบคุมการเล่าเรื่อง ความโปร่งใสของรัฐบาล *มาตรการตอบโต้ทางเทคนิค* เช่น การบูรณาการไซเบอร์และข้อมูล ความปลอดภัยโครงสร้างพื้นฐานดิจิทัล *การมีส่วนร่วมทางการทูต* ตลอดจนมี*ทีมตอบสนองอย่างรวดเร็ว* (Giannopoulos et al., 2021) เช่น หน่วยงาน The Center for Countering Disinformation (CCD) การรวมศูนย์สื่อหลักผ่านรายการเทเลธอน การใช้บัญชี Chatbot ในสื่อสังคมออนไลน์ต่าง ๆ

ความสามารถในการฟื้นตัวอย่างรวดเร็ว โดยการเรียนรู้บทเรียนจากภัยคุกคามข้อมูล ประเมินกลยุทธ์ เทคนิค และขั้นตอนที่คู่ขัดแย้งใช้และช่องโหว่ที่ถูกใช้ในการโจมตี เพื่อพัฒนาวิธีตอบสนองที่มีประสิทธิภาพมากขึ้นสำหรับป้องกัน ควบคุม หรือบรรเทาเหตุการณ์ที่เกี่ยวข้องกับข้อมูลในอนาคต อันจะช่วยเสริมสร้างความตระหนักรู้เกี่ยวกับสถานการณ์ กำหนดแนวทางระยะยาวในการใช้เครื่องมือ และระบบต่างๆ รวมถึงการปรับทางเลือกในการตอบสนองที่มีอยู่เพื่อป้องกัน ควบคุม และบรรเทาผลกระทบได้อย่างเหมาะสม (NATO, 2025)

ทั้งนี้ การสื่อสารเชิงรุกถือเป็นเครื่องมือสำคัญอย่างหนึ่งในการต่อต้านภัยคุกคามข้อมูล การสื่อสารกับพลเมืองผ่านช่องทางต่างๆ อย่างทันเหตุการณ์ โดยให้ข้อมูลที่ถูกต้องช่วยให้ประชาชนรับรู้ ตระหนักและสามารถต่อต้านภัยคุกคามข้อมูลได้อย่างมีประสิทธิภาพ

ความท้าทายต่อภัยคุกคามทางข้อมูลของประเทศไทย

ประเทศไทย เผชิญหน้ากับภัยคุกคามทางข้อมูลในสถานการณ์ความขัดแย้งระหว่างไทยและกัมพูชา ซึ่งเกิดปะทะกันระหว่างทหารไทยและกัมพูชาบริเวณช่องบก ในวันที่ 28 พฤษภาคม 2025 พบว่ามีข้อมูลเท็จเกี่ยวกับความขัดแย้งสู่สาธารณชนอย่างต่อเนื่อง ดังที่ นายภูมิธรรม เวชยชัย ได้ให้สัมภาษณ์ในวันที่ 27 มิถุนายน 2025 ว่า “คู่ขัดแย้งกำลังปฏิบัติการสงครามข้อมูลข่าวสารและสงครามจิตวิทยา เพื่อจะบั่นทอนศักยภาพและความน่าเชื่อถือของรัฐบาล” ในวันที่ 4 มิถุนายน นายภูมิธรรม ได้แถลงข่าวเกี่ยวกับการวางทุ่นระเบิดในแนวปะทะนั้นอยู่คนละพื้นที่และเป็นกับระเบิดเก่า ทั้งนี้ ตั้งแต่การปะทะกัน ถึง 14 มิถุนายน ศูนย์ต่อต้านข่าวปลอม (Anti-fakenews) ได้ระบุข่าวที่เป็นเท็จซึ่งเกิดขึ้นว่ามีการแชร์ข่าวการปิดด่านชายแดน มากถึง 33 ข่าว โดยมีการตรวจสอบว่าเป็นข่าวเท็จ 9 ข่าว มีการเผยแพร่เนื้อหาข่าวว่าไทยจะยึดประเทศกัมพูชา หากกัมพูชาไม่ถอนกำลังว่าเป็นข้อมูลเท็จ ต่อจากนั้น ในวันที่ 24 มิถุนายน 2025 ผู้นำกัมพูชาระบุว่าไทยจะมีนายกรัฐมนตรีคนใหม่ภายใน 3 เดือน และรู้ล่วงหน้าว่าใครจะเป็นนายกรัฐมนตรีผ่านเฟซบุ๊ก รวมถึงการขู่จะแฉและยึดทรัพย์นักการเมืองไทย ทั้งยังมีการเผยแพร่ข้อมูลเกี่ยวกับการยื่นเรื่องพิพาทชายแดนต่อศาลยุติธรรมระหว่างประเทศ และเปรียบเทียบกรณีความขัดแย้งดังกล่าวกับฉนวนกาซา อีก 2 วันถัดมา ฮุนเซน ประกาศจะเปิดเผยข้อมูลที่ละเอียดอ่อนรวมถึงการกระทำอันเป็นการทรยศต่อชาติ และการหมิ่นสถาบันพระมหากษัตริย์ของทักษิณ ชินวัตร นอกจากนี้ ยังมีรายงานแฮกเกอร์ชาวกัมพูชาโจมตีเว็บไซต์ราชการหลายแห่งและขึ้นข้อความโจมตีประเทศไทยในช่วงเดือนเมษายน – มิถุนายน 2025 ในทางกลับกัน สื่อกัมพูชา อาทิ Khmer Times และ Phnom Penh Post ระบุว่าสื่อไทยให้ข้อมูลเท็จเกี่ยวกับกรณี–กองทัพกัมพูชา “ถอนทหารออกจากพื้นที่ช่องบก” อีกทั้ง กระทรวงไปรษณีย์และโทรคมนาคมกัมพูชาได้ออกแถลงการณ์ เมื่อวันที่ 7 กรกฎาคม 2025 ว่ากัมพูชาไม่ได้ร่วมมือกับกลุ่มแฮกเกอร์ชาวเกาหลีเหนือเพื่อโจมตีหน่วยงานต่าง ๆ ของไทย พร้อมกับอ้างว่ามี

กลุ่มแฮกเกอร์ชาวไทย ที่ชื่อว่า BlackEye–Thai ทำการโจมตีทางไซเบอร์ต่อระบบออนไลน์ของรัฐบาลกัมพูชา เกือบทั้งหมดแต่ระบบรักษาความมั่นคงทางไซเบอร์ของกัมพูชาสามารถสกัดความพยายามดังกล่าวไว้ได้

เหตุการณ์ดังกล่าวสะท้อนให้เห็นว่าประเทศไทยกำลังประสบปัญหาจากภัยคุกคามด้านข้อมูล ซึ่งส่งผลกระทบต่อเสถียรภาพทางการเมืองของไทย สืบเนื่องจากกรณีที่กัมพูชาปล่อยคลิปสนทนาระหว่าง แพทองธาร และฮุนเซน ทำให้ประชาชนไทย ที่ไม่พอใจออกมาชุมนุมเคลื่อนไหวเพื่อเรียกร้องให้นายกรัฐมนตรีลาออกในวันที่ 28 มิถุนายน 2025 และในวันที่ 1 กรกฎาคม 2025 ศาลรัฐธรรมนูญรับคำร้อง สว. ยื่นถอดถอนนายกรัฐมนตรีและสั่งหยุดปฏิบัติหน้าที่ชั่วคราว เมื่อเปรียบเทียบความพร้อมและความสามารถในการรับมือภัยคุกคามทางข้อมูลหากประเทศไทยต้องเผชิญกับสงครามทางปัญญากับการรับมือจากประเทศ กรณีตัวอย่างสามารถสรุปได้ดังแสดงในตารางที่ 1

ตารางที่ 1 เปรียบเทียบความสามารถในการรับมือภัยคุกคามทางข้อมูลของประเทศไทย

Table 1 Comparison of Thailand's Information Threat Response Capabilities

	กรณีศึกษา	**ไทย**
การรับรู้สถานการณ์	การเฝ้าระวังและตรวจสอบ การใช้ AI ในการตรวจจับข้อมูลบิดเบือน ความเป็นเอกภาพในการนำเสนอข่าว เช่น United News การมีส่วนร่วมกับพลเมืองในการตรวจสอบข้อเท็จจริง เช่น fakenews watchdogs	COFACT ร่วมตรวจสอบข้อเท็จจริง Anti–fakenews, ชัวร์ก่อนแชร์, ThaiPBS Verified
การเพิ่มประสิทธิผลการป้องกัน	พัฒนาการรู้เท่าทัน และฝึกอบรมในภาคการศึกษาเยาวชน ประชาชน เช่น การรู้เท่าทันสื่อ การรู้เท่าทันดิจิทัล อบรมการใช้ OSINT, Hackathon, Magshimim	โครงการสร้างการรู้เท่าทันสื่อและดิจิทัล (สถาบันการศึกษา กองทุนพัฒนาสื่อ)
	สร้างเครือข่ายกับหน่วยงาน/ องค์กรที่มีอิทธิพลทั้งภายในและนอกประเทศ กลุ่มแฮกติวิสต์ที่สนับสนุน	ยังไม่มีการระบุความร่วมมือระหว่างประเทศ/ แฮกติวิสต์
	บูรณาการร่วมกันระหว่างหน่วยงานรัฐ หน่วยงานความมั่นคง เอกชน สื่อสารมวลชน สื่อสังคมออนไลน์ และประชาสังคม	ประสานงานระหว่างหน่วยงานรัฐ เช่น สกมช. กระทรวงดิจิทัลฯ สตช.
การควบคุมและบรรเทาภัยคุกคาม	กฎหมาย เช่น คอมพิวเตอร์ ข้อมูลส่วนบุคคล ข่าวปลอม ความปลอดภัยทางไซเบอร์ อธิปไตยทางอินเตอร์เน็ต โครงสร้างพื้นฐานการสื่อสาร กำกับดูแลสื่อและผู้ให้บริการระบบสื่อสารโทรคมนาคม	พรบ. ไซเบอร์ พรบ. คอมพิวเตอร์ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
	การหักล้างข้อมูลเท็จ เช่น การใช้ซอฟท์แวร์ AI ในการตรวจสอบการสื่อสารผ่านบัญชี Chatbot ในแพลตฟอร์มสื่อสังคมออนไลน์	สื่อสารผ่านผู้บริหาร และช่องทางของหน่วยงานภาครัฐ สื่อมวลชน
	การสื่อสารเชิงกลยุทธ์ เช่น ควบคุมเรื่องเล่า (ความชอบธรรม การปกป้องผู้ถูกกระทำ) การประชาสัมพันธ์ การโฆษณาชวนเชื่อ การจัดการข้อมูลที่ผิดปกติ การสร้างอารมณ์ร่วมกับพลเมืองและสังคมโลก การทูตสาธารณะ การโต้แย้งเฉพาะจุด	การสื่อสารข้อเท็จจริงของแต่ละหน่วยงานไม่ตรงกัน และล่าช้า
	มาตรการทางเทคนิค เช่น การโจมตีทางไซเบอร์ (DDoS) การบล็อกหรือกวนสัญญาณ การใช้ AI (deepfakes, bot farms) Troll farms บัญชีปลอม ระบบการแจ้งเตือน การบล็อคหรือลบเนื้อหา	ยังไม่มีการระบุแน่ชัด

	กรณีศึกษา	ไทย
	หน่วยลับในการปฏิบัติการข้อมูล เช่น การสร้างเรื่องเล่า การปล่อยข่าวไปยังสื่อ	ยังไม่มีการระบุแน่ชัด
ความสามารถในการฟื้นตัว	โครงสร้างพื้นฐานการสื่อสารรองรับการโจมตีด้วยระบบสำรอง และการสนับสนุนระหว่างประเทศ เช่น การสำรองข้อมูล เครือข่ายการเชื่อมต่อ	ยังไม่มีการระบุแน่ชัด ทั้งนี้มีการกำหนดให้ระบบคลาวด์ ซึ่งบังคับใช้ในปี พ.ศ. 2569
	การควบคุมและตัดสินใจเกี่ยวกับข้อมูล โครงสร้างพื้นฐานและเทคโนโลยีดิจิทัล เช่น อธิปไตยทางอินเตอร์เน็ต	อยู่ระหว่างการอภิปรายแนวคิด
	แนวทางหลายมิติ เช่น การสื่อสารเชิงรุก ความรวดเร็วทันเหตุการณ์ เอกภาพในการสื่อสาร การบูรณาการเครือข่าย การตรวจสอบลบเนื้อหา การพัฒนา AI เพื่อปรับกลยุทธ์แบบเรียลไทม์	เอกภาพในการสื่อสารค่อนข้างน้อย ส่วนใหญ่เป็นเชิงรับ และใช้เวลานานในการลบล้าง

เมื่อเปรียบเทียบกับการรับมือจากประเทศกรณีตัวอย่าง พบว่า ประเทศไทยมีการริเริ่มดำเนินการ เพื่อเตรียมการรับมือภัยคุกคามทางข้อมูลใน 4 ขั้นตอน ทั้งด้านการรับรู้ การเพิ่มประสิทธิผลการป้องกัน การควบคุมและบรรเทาภัยคุกคามในบางส่วนแล้ว อย่างไรก็ตามจากกรณีความขัดแย้งช่องบก พบว่า รัฐบาลควรพัฒนาความสามารถในการรับมือที่มีประสิทธิภาพในมิติต่าง ๆ เพิ่มเติม ดังนี้

การตรวจสอบข้อเท็จจริง ปัจจุบันประเทศไทยมีหน่วยงาน Anti-Fakenews ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม แต่ประชาชนบางส่วนยังมีข้อกังวลเกี่ยวกับความเป็นอิสระของหน่วยงาน สำนักข่าวเองก็มีหน่วยงานตรวจสอบข้อเท็จจริง เช่น ชัวร์ก่อนแชร์ ของสำนักข่าวไทย และ Thai PBS Verified ในขณะที่เครือข่ายการตรวจสอบเท็จจริงมีเพียง COFACT ซึ่งการดำเนินการส่วนใหญ่เป็นในเชิงรับ ขาดการหักล้างตอบโต้ในเชิงรุก ทั้งนี้ ด้วยข้อจำกัดในด้านงบประมาณทำให้การใช้ปัญญาประดิษฐ์ (AI) ในการสนับสนุนการตรวจจับข้อมูลเท็จในพื้นที่สาธารณะออนไลน์ยังไม่สามารถทำได้อย่างเต็มที่ ดังนั้น 1) รัฐบาลควรสนับสนุนการใช้ปัญญาประดิษฐ์ให้กับหน่วยงานตรวจสอบข้อเท็จจริง เพื่อเพิ่มประสิทธิภาพในการตรวจจับข้อมูลเท็จ หักล้างข้อมูลเท็จ และสามารถตอบโต้ในเชิงรุกในพื้นที่ไซเบอร์ได้อย่างทันการณ์ 2) หารือร่วมกับแพลตฟอร์มโซเชียลมีเดียในการสนับสนุนการตรวจสอบเท็จจริง เช่น การแจ้งเตือน การติดแท็กเกี่ยวกับหัวข้อข่าวที่เป็นประเด็นเพื่อสร้างความตระหนักรู้ และการลดการมองเห็นข่าวปลอมในแพลตฟอร์ม เพื่อลดความสับสน และความขัดแย้งในสังคม

การเพิ่มประสิทธิผลในการป้องกัน ในการพัฒนาการรู้เท่าทันสื่อ มีหลายหน่วยงานที่เกี่ยวข้อง เช่น กองทุนพัฒนาสื่อปลอดภัยและสร้างสรรค์ กรมประชาสัมพันธ์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ แต่ยังเป็นเพียงโครงการที่ฝึกอบรมเฉพาะกลุ่ม ในระดับแกนนำ หรือผู้ที่สนใจเข้าร่วม และถึงแม้กระทรวงศึกษาธิการได้บรรจุการรู้เท่าทันสื่อในหลักสูตรการศึกษาขั้นพื้นฐานและอุดมศึกษาแต่ไม่ได้เป็นวิชาบังคับ ขึ้นอยู่กับสถานศึกษาแต่ละแห่ง ดังนั้น 1) รัฐบาลควรบรรจุวิชาการรู้เท่าทันสื่อและดิจิทัลให้เป็นวิชาพื้นฐานให้กับเด็กและเยาวชน และควรจัดอบรมให้กับกลุ่มเปราะบางอื่น ๆ ที่เข้าถึงระบบการเรียนได้ยาก เช่น กลุ่มผู้สูงอายุ รวมถึงขยายขอบเขตการศึกษาไปยังท้องถิ่นทั่วประเทศ โดยเฉพาะเจ้าหน้าที่รัฐระดับท้องถิ่น ซึ่งเป็นกลไกขับเคลื่อนในการดูแลประชาชนในชุมชนทั่วประเทศและยังสามารถเข้าถึงกลุ่มเปราะบางเพื่อให้ความรู้ด้านสื่อและดิจิทัลได้อย่างทั่วถึง 2) สร้างเครือข่ายการบูรณาการร่วมกัน นอกจากความร่วมมือกับแพลตฟอร์มสื่อสังคมออนไลน์ การสร้างเครือข่ายผู้เชี่ยวชาญ

ทางด้านความปลอดภัยไซเบอร์กับสถาบันศึกษา หน่วยงานเอกชน และกลุ่มแฮ็กเกอร์เชิงจริยธรรม (Ethical Hacker) ในการค้นหาช่องโหว่ในระบบไซเบอร์ของภาครัฐ ตรวจจับความเคลื่อนไหวที่ผิดปกติบนพื้นที่ไซเบอร์ในเขตอธิปไตยของประเทศไทยเพื่อจัดทำมาตรการป้องกันและแนวทางแก้ไขก่อนที่จะถูกโจมตีจากภายนอกก็เป็นสิ่งที่รัฐควรให้ความสำคัญ

มาตรการในการควบคุมและบรรเทาผล พบว่า ประเทศไทยมีการออกกฎหมายรองรับทั้งในส่วนภัยคุกคามทางไซเบอร์และภัยคุกคามจากข่าวปลอม ทั้งนี้ การออกกฎหมายต่าง ๆ ของประเทศไทยซึ่งสภาพสังคมมักจะอ้างเกี่ยวกับสิทธิและเสรีภาพสุดโต่ง เมื่อเปรียบเทียบกับประเทศที่มีการใช้กฎหมายอย่างเข้มข้น เช่น รัสเซีย อิสราเอล มีความคืบหน้าในการดำเนินการเป็นไปแบบค่อยเป็นค่อยไป ดังกรณีของการคัดค้านการศึกษาความเป็นไปได้ของนโยบายการใช้ช่องทางอินเตอร์เน็ตช่องทางเดียว (Single Gateway) โดยสิทธิเสรีภาพในการรับรู้ข้อมูลข่าวสาร เสรีภาพในการแสดงความคิดเห็น ความปลอดภัยของข้อมูลส่วนบุคคล ข้อมูลความลับ รวมทั้งปัญหาการละเมิดความเป็นส่วนตัวถูกหยิบยกมาเป็นประเด็นในการต่อต้าน ส่วนในเชิงปฏิบัตินั้น สืบเนื่องมาจากกฎหมายที่ยังไม่ครอบคลุมจึงไม่สามารถบังคับใช้กฎหมายหรือบทลงโทษให้ครอบคลุมภัยคุกคามทางข้อมูลทั้งหมดที่เกิดขึ้น เช่น พรบ. ไซเบอร์ที่กำหนดมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งครอบคลุมหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่เกี่ยวข้องกับความมั่นคงของรัฐ การบริการภาครัฐที่สำคัญ การเงินการธนาคาร เทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่ง พลังงานและสาธารณูปโภค สาธารณสุข แต่ยังไม่รวมถึงหน่วยงานด้านอื่น ๆ เช่น ด้านอุตสาหกรรม การบริการ การพาณิชย์ ระบบสารสนเทศที่เกี่ยวข้องกับการจัดงานในระดับประเทศ (Linakanit & Tanawarit, 2025) ดังนั้น 1) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ควรดำเนินการจารณาการขยายขอบเขตไปยังหน่วยงานอื่น ๆ นอกจากหน่วยงานที่มีความเสี่ยงต่อความมั่นคงของประเทศ เช่น หน่วยงานที่เสี่ยงจะส่งผลกระทบต่อสังคมและเศรษฐกิจของประเทศ นอกจากนี้ ในห้วงเวลาที่เกิดกระแสข่าวปลอม หน่วยงานของรัฐต่างออกมาชี้แจงข้อเท็จจริงซึ่งให้ข้อมูลไม่ตรงกัน เช่น การให้สัมภาษณ์ของผู้นำรัฐบาลและกองทัพ พบว่า รายละเอียดในบางประเด็นมีความแตกต่างกัน ประเทศไทยไม่มีช่องทางหลักในการติดตามข้อเท็จจริงจากหน่วยงานภาครัฐ ถึงแม้โฆษกประจำสำนักนายกรัฐมนตรีเป็นศูนย์ข่าวของรัฐบาลให้แก่ประชาชนและสื่อมวลชน แต่ใช้ระยะเวลาในการเตรียมการสื่อสาร จึงไม่สามารถหักล้างข้อมูลเท็จได้ทันการณ์ในยุคของสื่อสังคมออนไลน์ที่ข้อมูลบิดเบือนสามารถเผยแพร่ไปทั่วพื้นที่ไซเบอร์ในเสี้ยววินาที อันจะส่งผลให้ความคิดเห็นสาธารณะถูกชักจูงไปโดยข้อมูลบิดเบือนหรือข้อมูลเท็จ ฉะนั้น 3) รัฐบาลควรมอบหมายหน่วยงาน (ช่องทาง) ใดหน่วยงานหนึ่งให้เป็นผู้สื่อสารข้อเท็จจริง หักล้างข้อมูลเท็จอย่างทันการณ์ และสื่อสารเชิงกลยุทธ์ไปยังประชาชนและสังคมโลก โดยรัฐบาลควรประยุกต์ใช้ปัญญาประดิษฐ์ (AI) เพื่อสนับสนุนการดำเนินการ เช่น การตรวจจับกระแสข่าวปลอม ระบบแจ้งเตือนพลเรือนเกี่ยวกับภัยคุกคามและการปฏิบัติการในรูปแบบต่าง ๆ เพื่อหักล้างข้อมูลเท็จหรือข้อมูลบิดเบือนที่ส่งผลต่อความมั่นคงของประเทศ พร้อมทั้งชี้แจงข้อเท็จจริงและแนวทางการปฏิบัติสำหรับประชาชน การใช้ Chatbot จากศูนย์กลางการสื่อสารของรัฐบาลเพื่อสื่อสารข้อเท็จจริงไปยังประชาชน ซึ่งจะสามารถสร้างความเป็นเอกภาพของการสื่อสาร และลดความสับสนของพลเมืองได้ อาทิ แนวทางเสียงเดียวของยูเครน

ความสามารถในการฟื้นตัว ประเทศไทยยังอยู่ในระหว่างเตรียมดำเนินการในส่วนของการสำรองระบบ ได้แก่ การประกาศนโยบายระบบคลาวด์ภาครัฐ (Cloud First Policy) ส่วนความสามารถในการควบคุมและตัดสินใจเกี่ยวกับข้อมูล โครงสร้างพื้นฐานและเทคโนโลยีดิจิทัลในพรมแดนประเทศไทย ยังคงมีการอภิปรายถกเถียงกันจากหลายฝ่าย ดังนั้น รัฐบาลควรเร่งศึกษาความเป็นไปได้เกี่ยวกับการลดการพึ่งพิงโครงสร้างพื้นฐานการสื่อสาร

และเทคโนโลยีดิจิทัลจากต่างชาติ และแนวทางการกำกับดูแลปัญญาปัญญาประดิษฐ์ซึ่งยังอยู่ระหว่างการเปิดรับฟังความคิดเห็น

สรุป

จากความขัดแย้งทางภูมิรัฐศาสตร์ที่เกิดขึ้นในหลายภูมิภาคทั่วโลกรวมถึงความขัดแย้งระหว่างประเทศไทยและกัมพูชาในปัจจุบัน มีการใช้กลยุทธ์ที่หลากหลายในการสร้างความได้เปรียบในพื้นที่สีเทา ดังในกรณีของประเทศไทยนั้นก็แสดงให้เห็นความพยายามแทรกแซงทางการเมืองจากการปฏิบัติการข้อมูลของคู่ขัดแย้งอย่างเห็นได้ชัด หลายประเทศทั่วโลกต่างตระหนักถึงภัยคุกคามดังกล่าว และตื่นตัวต่อสงครามทางปัญญาที่เกิดขึ้น การศึกษากรณีเปรียบเทียบสงครามรัสเซีย–ยูเครน และสงครามฉนวนกาซา สามารถนำมาถอดบทเรียน เพื่อศึกษารูปแบบการปฏิบัติการทางข้อมูล และเตรียมการรับมือกับภัยคุกคามดังกล่าวหากประเทศไทยต้องเผชิญกับสงครามทางปัญญา เมื่อพิจารณาแนวทางการรับมือที่มีประชาชนเป็นศูนย์กลางใน 4 ขั้นตอน พบว่า 1) การรับรู้สถานการณ์ ยูเครน มีการตื่นตัวเกี่ยวกับการตระหนักรู้ และการมีส่วนร่วมในการตรวจสอบข้อเท็จจริงค่อนข้างสูง 2) การเพิ่มประสิทธิผลการป้องกัน ยูเครน มีการสร้างเครือข่ายกับหน่วยงานต่างประเทศและได้การสนับสนุนจากเครือข่ายต่างประเทศค่อนข้างมากรวมถึงกลุ่มแฮกติวิสต์ทั่วโลก ในขณะที่รัสเซีย มีการบูรณาการร่วมกันระหว่างหน่วยงานที่เกี่ยวข้องอย่างเป็นระบบและมีเอกภาพสูง ส่วนอิสราเอลมีการเตรียมพร้อมฝึกอบรมเยาวชนและพลเมืองในด้านทักษะทางไซเบอร์เป็นอย่างดี 3) การควบคุมและบรรเทาภัยคุกคาม เห็นได้ว่ารัสเซียมีกฎหมายที่ครอบคลุมในทุกมิติทั้งการกำกับดูแลต่างชาติ ระบบอินเตอร์เน็ต แพลตฟอร์มออนไลน์ และสื่อสารมวลชน ซึ่งกฎหมายได้ในอำนาจในการตรวจสอบและดำเนินการอย่างเต็มที่ โดยเฉพาะอย่างยิ่งการปฏิบัติการข่าวสาร ซึ่งสามารถควบคุมการเล่าเรื่องได้ตามเป้าประสงค์ และ 4) ความสามารถในการฟื้นตัว ยูเครนได้รับการสนับสนุนในการฟื้นตัวจากต่างชาติสูง ทั้งระบบสำรองข้อมูลและการสื่อสารโทรคมนาคม ในขณะที่รัสเซียสามารถลดการพึ่งพาต่างชาติได้ทั้งในส่วนของข้อมูล โครงสร้างพื้นฐานและเทคโนโลยีอินเตอร์เน็ต

เมื่อเปรียบเทียบกับการรับมือภัยคุกคามทางข้อมูลของประเทศไทย พบว่า รัฐบาลได้เริ่มดำเนินการเพื่อรับมือกับภัยคุมคามในบางส่วนไว้แล้ว แต่บางกิจกรรมยังอยู่ในขั้นตอนการเตรียมการ หรืออยู่ระหว่างการอภิปรายแนวคิด จึงนำเสนอทางเลือกเชิงนโยบายเพื่อเพิ่มประสิทธิภาพของกิจกรรมด้าน 1) การรับรู้สถานการณ์ เช่น การเพิ่มประสิทธิภาพการตรวจจับข้อมูลผิดปกติ การตรวจสอบข้อเท็จจริง และการหักล้างข้อมูลเท็จโดยการใช้ปัญญาประดิษฐ์ และร่วมมือกับแพลตฟอร์มสื่อสังคมออนไลน์ และ 2) การเพิ่มประสิทธิผลการป้องกันได้มากขึ้น เช่น เพิ่มการสร้างการเครือข่ายกับภาคพลเมือง และการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐ เอกชน และประชาสังคม และสถาบันการศึกษาในการตรวจสอบข้อเท็จจริง และพัฒนาทักษะการรู้เท่าทันสื่อและดิจิทัลสำหรับประชาชนทุกกลุ่ม สำหรับ 3) การควบคุมและบรรเทาภัยคุกคาม รัฐบาลควรให้ความสำคัญทั้งกับขอบเขตของกฎหมายที่ยังไม่ครอบคลุม การปฏิบัติงานจริงที่ยังขาดความเป็นเอกภาพและความร่วมมือกันระหว่างหน่วยงาน นอกจากนี้ ต้องปรับการสื่อสารกลยุทธ์ในเชิงรุก เพราะปัจจุบันเป็นเพียงการตั้งรับซึ่งการตอบโต้ค่อนข้างล่าช้า ดังสะท้อนจากความสับสนของประชาชนในสังคมจากข่าวปลอม และก่อให้เกิดความไม่พอใจทางการเมืองในประเทศจากการแทรกแซงของต่างชาติ ท้ายที่สุด 4) หน่วยงานรัฐที่ดูแลรับผิดชอบเกี่ยวกับความสามารถในการฟื้นตัว เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ควรให้ความสำคัญต่อดำเนินมาตรการที่รองรับการฟื้นตัวของประเทศหากเผชิญกับสงครามทางปัญญา ทั้งการเตรียมการระบบ

สำรอง ความสามารถในการควบคุมและตัดสินใจเกี่ยวกับข้อมูล โครงสร้างพื้นฐานและเทคโนโลยีดิจิทัล รวมถึงต้องปฏิบัติการเชิงรุกเพื่อสร้างความได้เปรียบให้กับประเทศไทยเหนือคู่ขัดแย้ง

References

Aouragh, M. (2016). Hasbara 2.0: Israel's public diplomacy in the digital age. *Middle East Critique, 25*(3), 271–297. https://doi.org/10.1080/19436149.2016.1179432

Backes, O., & Swab, A. (2019). *Cognitive warfare: The Russian threat to election integrity in the Baltic States*. Cambridge, MA: Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/2024-12/Cognitive%20Warfare%20%3D%20The%20Russian%20Threat%20to%20Election%20Integrity%20in%20the%20Baltic%20States.pdf

Barucija, A. (2020). The historical evolution of Israeli intelligence. *American Intelligence Journal, 37*(1), 178–182. https://www.jstor.org/stable/27087696

Borch, O. J., & Heier, T. (2025). *Preparing for hybrid threats to security: Collaborative preparedness and response*. Taylor & Francis. https://library.oapen.org/bitstream/handle/20.500.12657/93079/1/9781040153505.pdf

Claverie, B., & Du Cluzel, F. (2022). *Cognitive warfare: The advent of the concept of "Cognitics" in the field of warfare*. In *Cognitive Warfare: The Future of Cognitive Dominance*. https://hal.science/hal-03635889v1/file/NATO-CSO-CW%202022-03-01%20%28US%29%20Claverie%20DuCluzel.pdf

Cordey, S. (2019). Trend Analysis: The Israeli Unit 8200 – An OSINT-based study. Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf

Done, W. D. (2021). Russian cyber information warfare: International distribution and domestic control. *Journal of Advanced Military Studies, 12*(1), 112–127. DOI:10.21140/mcuj.20211201005

Done, W. D. (2023). The information technology army of Ukraine and cyber warfare doctrine. *Journal of Strategic Security*, *16*(4), 15–33. https://doi.org/10.5038/1944-0472.16.4.2127

Erlich, A., & Garner, C. (2021). Is pro-Kremlin disinformation effective? evidence from Ukraine. *The International Journal of Press/Politics*, *28*(1), 5–28. https://doi.org/10.1177/19401612211045221

France 24. (2025, May 7). *Russia disinformation: France, Ukraine*. https://www.france24.com/en/europe/20250507-russia-disinformation-france-ukraine

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The landscape of hybrid threats: A conceptual model (Public version)*. Publications Office of the European Union; Hybrid CoE. https://op.europa.eu/en/publication-detail/-/publication/f330dae9-6ad2-11ec-9136-01aa75ed71a1

Hajduk, J., & Stępniewski, T. (2016). Russia's Hybrid War with Ukraine: Determinants, Instruments, Accomplishments and Challenges. *Studia EUROPEJSKIE–Studies in European Affairs*, (2), 37–52. https://journalse.com/russias-hybrid-war-with-ukraine-determinants-instruments-accomplishments-and-challenges/

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies. https://www.comw.org/qdr/fulltext/0712hoffman.pdf

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Levin, J. D. (2025, March–April). *Information operations: Adapting to modern conflict*. *Military Review*. U.S. Army Combined Arms Center. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2025/Information-Operations/

Libicki, M.C. (1995). *What is information warfare?.* National Defense University Institute for National Strategic Studies, Washington DC. https://apps.dtic.mil/sti/tr/pdf/ADA367662.pdf

Linakanit, J., & Tanawarit, T. (2025). Enhancing Cybersecurity Capacity: Thailand's Challenges and Responses in the Context of Hybrid Warfare. *Arts of Management Journal, 9*(4), 1–23. https://so02.tci-thaijo.org/index.php/jam/article/download/280213/186016

Marushchak, A., Petrov, S., & Khoperiya, A. (2025). Countering AI-powered disinformation through national regulation: learning from the case of Ukraine. *Frontiers in Artificial Intelligence*, *7*, 1474034. https://doi.org/10.3389/frai.2024.1474034

NATO. (2025, February 3). *NATO's approach to counter information threats*. NATO. https://www.nato.int/cps/uk/natohq/topics_219728.htm?selectedLocale=en

Opryshko, D. (2023). *Monitoring media pluralism in the digital era: Application of the Media Pluralism Monitor in the EU, Albania, Montenegro, North Macedonia, Serbia, Turkey and Ukraine in 2022* (Research Project Report). Centre for Media Pluralism and Media Freedom (CMPF), European University Institute. https://cadmus.eui.eu/server/api/core/bitstreams/2d4d38e0-c6a7-5950-8ae7-756081d224a3/content

Reichborn–Kjennerud, E., & Cullen, P. (2022). *What is hybrid warfare?*. Norwegian Institute for International Affairs (NUPI).

Regan, M., & Sari, A. (Eds.). (2024). *Hybrid threats and grey zone conflict: The challenge to liberal democracies*. Oxford University Press.

Seniutienė, D., & Paulauskytė, L. (2024). Response to hybrid threats: Policies, concepts and strategic approaches. *Public Security and Public Order*, (36), 195–202. https://ojs.mruni.eu/ojs/vsvt/article/view/8553/6046

Sherstoboeva, E. (2024). Russian Bans on 'Fake News' about the war in Ukraine: Conditional truth and unconditional loyalty. *International Communication Gazette*, *86*(1), 36–54. https://journals.sagepub.com/doi/pdf/10.1177/17480485231220141

Theohary, C. A. (2018). Information warfare: Issues for congress. *Congressional Research Service*, *5*. https://sgp.fas.org/crs/natsec/R45142.pdf

Topor, L., & Tabachnik, A. (2021). *Russian cyber information warfare: International distribution and domestic control*. *Journal of Advanced Military Studies*, *12*(1), 112–127. https://doi.org/10.21140/mcuj.20211201005

TRT World. (2024). *The art of deception: How Israel uses Hasbara to whitewash its crimes.* https://www.trtworld.com/magazine/the–art–of–deception–how–israel–uses–hasbara–to–whitewash–its–crimes–12766404

Underwood, K. (2017). Cognitive Warfare Will Be Deciding Factor in Battle: Lt. Gen. Stewart's Rem arks at DoDIIS17. Signal, The Cyber Edge. https://www.afcea.org/content/cognitive–warfare–will–bedeciding–factor–battle; https://www.youtube.com/watch?v=Nm–lVjRjLD4.

Ventre, D. (2012). *Information warfare*. John Wiley & Sons.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe. https://rm.coe.int/information–disorder–report–november–2017/1680764666