การพัฒนาศักยภาพความมั่นคงทางไซเบอร์: ศึกษาบริบทสงครามลูกผสมในประเด็นความท้าทายและการรับมือของประเทศไทย

Enhancing Cybersecurity Capacity: Thailand's Challenges and Responses in the Context of Hybrid Warfare

จีระวัฒน์ ลีนะกนิษฐ์[1] และ ทัธภร ธนาวริทธิ์[2]

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

สถาบันรัชต์ภาคย์

Rajapark Institute, Thailand

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

Received July 1, 2025; **Revised** July 18, 2025; **Accepted** August 7, 2025

บทคัดย่อ

ในช่วงห้าปีที่ผ่านมา ความขัดแย้งระหว่างประเทศมีการใช้กลยุทธ์ที่ซับซ้อนมากขึ้น โดยเฉพาะการโจมตีทางไซเบอร์ซึ่งช่วยให้คู่ขัดแย้งบรรลุเป้าหมายเชิงยุทธศาสตร์โดยไม่ต้องใช้กองกำลังขนาดใหญ่ ดังปรากฏในสงครามลูกผสมระหว่างประเทศรัสเซีย–ยูเครน และสงครามกาซา งานวิจัยนี้มุ่งศึกษาศักยภาพของประเทศไทยในการรับมือกับการโจมตีทางไซเบอร์ หากเผชิญกับสถานการณ์ความขัดแย้งในลักษณะเดียวกัน และเมื่อเปรียบเทียบกับประเทศกรณีศึกษาจำเป็นต้องพัฒนาศักยภาพความมั่นคงทางไซเบอร์ในมิติใดบ้าง การศึกษานี้ใช้การรวบรวมข้อมูลทุติยภูมิที่เกี่ยวกับรูปแบบการโจมตีทางไซเบอร์ในสงครามลูกผสมระหว่างรัสเซีย–ยูเครน และสงครามกาซา และสัมภาษณ์เชิงลึกกับบริษัทความปลอดภัยทางไซเบอร์ของไทยเพิ่มเติมสำหรับบริบทในประเทศไทย โดยวิเคราะห์เปรียบเทียบใน 5 มิติ ได้แก่ 1) กฎหมาย 2) ความสามารถทางเทคนิค 3) หน่วยงานและการจัดการ 4) การพัฒนาศักยภาพ 5) ความร่วมมือ อันนำไปสู่การแนวทางการพัฒนามาตรการในการสร้างความมั่นคงทางไซเบอร์ของประเทศไทย ทั้งนี้ พบว่าประเทศไทยมีกฎหมายหลัก ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงกฎหมายสนับสนุนอื่น ๆ อย่างไรก็ตาม การพัฒนาศักยภาพด้านความสามารถทางเทคนิค ด้านการบูรณาการของหน่วยงานนั้นยังคงเป็นสิ่งสำคัญ เช่นเดียวกับการสร้างการตระหนักรู้ของประชาชน รวมถึงการวางรากฐานอธิปไตยทางไซเบอร์เพื่อสร้างความมั่นคงให้กับประเทศในระยะยาว

คำสำคัญ: สงครามลูกผสม; ภัยคุกคามทางไซเบอร์; การโจมตีทางไซเบอร์; การพัฒนาศักยภาพความมั่นคงทางไซเบอร์; ความท้าทายและการรับมือของประเทศไทย

Abstract

Over the past five years, international conflicts have increasingly adopted complex strategies, particularly cyberattacks, which enable conflicting parties to achieve strategic objectives without deploying large-scale military forces. This trend is evident in hybrid wars such as the Russia–Ukraine conflict and the Gaza conflict. This study examines Thailand's capacity to respond to cyberattacks in the event of a similar conflict scenario. It assesses which dimensions of cybersecurity capabilities require development in comparison to international case studies. The research employs secondary data on cyberattack patterns and defense mechanisms from the Russia–Ukraine and Gaza conflicts, along with in-depth interviews with Thai cybersecurity firms to reflect the national context. A comparative analysis is conducted across five dimensions: (1) legal measures, (2) technical measures, (3) organizational measures, (4) capacity building, and (5) cooperation. The study proposes strategic guidelines to enhance Thailand's cybersecurity posture. It finds that Thailand has established key legislation, including the Cybersecurity Act B.E. 2562 (2019), as well as other supporting laws. However, significant challenges remain in strengthening technical capabilities, improving institutional integration, and raising public awareness. Furthermore, laying the foundation for cyber sovereignty is deemed essential for securing Thailand's long-term national security.

Keywords: hybrid warfare; cyber threat; cyberattack; cybersecurity capacity; Thailand's challenges and responses

บทนำ

ท่ามกลางความขัดแย้งทางภูมิรัฐศาสตร์ ส่งผลให้เกิดการต่อสู้เพื่อช่วงชิงอำนาจในหลากหลายรูปแบบ เช่น สงครามลูกผสม (Hybrid warfare) ซึ่งเป็นการผสมผสานการทำสงครามในหลากหลายมิติ ใช้กลยุทธ์หลากหลายรูปแบบ ทั้งสงครามแบบดั้งเดิม สงครามไม่สมมาตร (สงครามกองโจร) สงครามไซเบอร์ การปฏิบัติการข้อมูลข่าวสาร มาตรการด้านเศรษฐกิจและพลังงาน ตั้งแต่ปี ค.ศ. 2020 เป็นต้นมา เกิดเหตุการณ์ความขัดแย้งที่ส่งผลกระทบไปทั่วโลก เช่น ในเดือนกุมภาพันธ์ ค.ศ. 2022 กองทัพรัสเซียบุกยูเครน ส่งผลให้เกิดวิกฤติการณ์ระดับนานาชาติกระทบกับเศรษฐกิจทั่วโลก เดือนตุลาคม ค.ศ. 2023 ฮามาสเปิดการโจมตีอิสราเอล ซึ่งอิสราเอลตอบโต้โดยการปฏิบัติทางทหารในเขตฉนวนกาซาเท่านั้น และพื้นที่ที่เชื่อว่าเป็นฐานที่ตั้งของกลุ่มฮามาส และพันธมิตรที่เกี่ยวข้อง ในเดือนเมษายน ค.ศ. 2024 อิหร่าน และอิสราเอลเปิดการโจมตีในหลายรูปแบบตอบโต้ระหว่างกัน และเกิดความตึงเครียดอีกครั้งในเดือนมิถุนายน ค.ศ. 2025 เมื่อกองทัพอิสราเอลเปิดปฏิบัติการ "Rising Lion" โจมตี

อิหร่านกว่า 200 จุด โดยอิหร่านสูญเสียนายทหารระดับสูงหลายนาย ในวันที่ 13 มิถุนายน และอิหร่านส่งโดรน และยิงขีปนาวุธตอบโต้โจมตีหลายพื้นที่ โดยพบว่า มีการโจมตีทางไซเบอร์ต่ออิสราเอลเพิ่มขึ้น 700% เมื่อเทียบกับช่วงก่อนวันที่ 12 มิถุนายน จากปฏิบัติการตอบโต้ของแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐบาลอิหร่านและกลุ่มที่เกี่ยวข้อง (Al Mayadeen English, 2025) นอกจากนั้น ยังมีความขัดแย้งเกิดขึ้นกระจายไปในภูมิภาคอื่น ๆ เช่น ในเดือน พฤษภาคม ค.ศ. 2025 ความขัดแย้งระหว่างอินเดียและปากีสถานปะทุขึ้นในดินแดนแคชเมียร์ โดยอินเดียเปิดปฏิบัติการ “Operation Sindoor” ซึ่งเป็นการประกาศปฏิบัติการแก้แค้นกรณีการสังหารหมู่ในแคชเมียร์–อินเดีย โดยการใช้โดรนโจมตี และมีรายงานการการโจมตีเว็บไซต์องค์กรของอินเดียโดยกลุ่มแฮกเกอร์ปากีสถาน ความขัดแย้งในทะเลจีนใต้ระหว่างจีนและไต้หวัน นอกจากการซ้อมรบ มาตรการกดดันทางเศรษฐกิจและการทูต ยังมีรายงานการโจมีตีทางไซเบอร์ต่อไต้หวันจากจีนเป็นจำนวนมาก

สำหรับประเทศไทย แม้ความขัดแย้งที่เกิดขึ้นในบริเวณช่องบก ระหว่างไทยและกัมพูชา ในเดือน พฤษภาคม พ.ศ. 2568 ยังไม่ได้ทวีความรุนแรงถึงขั้นใช้กำลังทางทหารสู้รบกัน แต่พบว่ามีรายงานการโจมตีทางไซเบอร์โจมตีเว็บไซต์ราชการและเอกชนไทย 13 แห่งในช่วงเดือนเมษายน – มิถุนายน พ.ศ. 2568 ซึ่งตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีออกหมายจับสมาชิกกลุ่มแฮกเกอร์ชาวกัมพูชาในเดือนมิถุนายน พ.ศ. 2568 รวมถึงนายภูมิธรรม เวชยชัย ได้ให้สัมภาษณ์ในวันที่ 27 มิถุนายน พ.ศ. 2568 ว่าคู่ขัดแย้งกำลังปฏิบัติการสงครามข่าวสาร และสงครามจิตวิทยา อีกทั้ง พล.อ.ณัฐพล นาคพาณิชย์ ยังกล่าวว่า ทุกคนกำลังอยู่ภายใต้สงครามข่าวสาร (IO) อย่างแท้จริงเต็มรูปแบบ เหตุการณ์ดังกล่าวสะท้อนให้เห็นว่าประเทศไทยกำลังเผชิญหน้ากับภัยคุกคามแบบผสมผสานทั้งการโจมตีทางไซเบอร์ การปฏิบัติการข้อมูล และการปฏิบัติการจิตวิทยา ทั้งนี้ การรับมือต่อการปฏิบัติการของประเทศไทยต่อเหตุการณ์ดังกล่าวส่วนใหญ่อยู่ในรูปแบบของมาตรการเชิงรับ กล่าวคือ ผู้บริหารประเทศ หรือผู้บริหารหน่วยงานที่รับผิดชอบด้านความมั่นคงให้สัมภาษณ์เพื่อให้ข้อเท็จจริงเป็นรายวันเพื่อตอบโต้แต่ละกรณีที่คู่ขัดแย้งปฏิบัติการต่อประเทศไทย หรือออกหมายจับผู้โจมตีทางไซเบอร์หลังจากเกิดความเสียหายไปแล้วระยะหนึ่ง

บทความนี้มีวัตถุประสงค์ เพื่อศึกษาแนวทางในการพัฒนาศักยภาพของประเทศไทย ในการรับมือกับการโจมตีทางไซเบอร์ หากเผชิญกับสถานการณ์สงครามลูกผสม โดยเฉพาะอย่างยิ่งภัยคุกคามจากการโจมตีทางไซเบอร์ ทั้งนี้ในการเสนอแนะแนวทางเพื่อพัฒนาศักยภาพในการรับมือกับภัยคุกคามและเสริมสร้างความมั่นคงทางไซเบอร์ของประเทศ จำเป็นจะต้องศึกษาเปรียบเทียบจากกรณีศึกษาจากประเทศที่มีพัฒนาการในการรับมือกับสงครามลูกผสมที่ทันเหตุการณ์และสามารถใช้ได้จริงในทางปฏิบัติ อาทิ ประเทศรัสเซีย ยูเครน และอิสราเอล โดยรวบรวมข้อมูลทุติยภูมิที่เกี่ยวกับรูปแบบการโจมตีทางไซเบอร์ในสงครามลูกผสมระหว่างรัสเซีย–ยูเครน และสงครามกาซา และนำมาเปรียบเทียบกับบริบทของประเทศไทย โดยสัมภาษณ์เชิงลึกกับบริษัทความปลอดภัยทางไซเบอร์ของไทยเพิ่มเติมสำหรับบริบทในประเทศไทย เพื่อค้นหาช่องโหว่และวางแนวทางในการพัฒนาศักยภาพใน

การรับมือต่อไปในอนาคตให้ประเทศไทยสามารถปกป้องและรับมือกับภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ รวมถึงสามารถรักษาความมั่นคงทางไซเบอร์ อันส่งผลต่อการรักษาอธิปไตยของประเทศไทยได้อย่างยั่งยืน ทั้งนี้ กรอบการวิเคราะห์มุ่งเน้นเปรียบเทียบมาตรการรับมือ และนำเสนอมาตรการรับมือใน 5 มิติ ตามแนวคิดของ International Telecommunication Union ได้แก่ 1) กฎหมาย 2) ความสามารถทางเทคนิค 3) หน่วยงานและนโยบาย 4) การพัฒนาศักยภาพ 5) การบูรณาการและความสามารถในการรับมือ

สงครามลูกผสม

ในศตวรรษที่ 21 แม้รูปแบบการทำสงครามแบบดั้งเดิมยังคงมีอยู่ แต่ส่วนใหญ่อยู่ในรูปแบบสงครามลูกผสม ซึ่งเป็นรูปแบบที่ไม่จำเป็นต้องประกาศสงครามอย่างเป็นทางการ เน้นการบั่นทอนบ่อนทำลายฝ่ายตรงข้ามโดยหลีกเลี่ยงการเผชิญหน้า เพื่อการครอบงำประเทศต่าง ๆ ซึ่งไม่จำเป็นต้องครอบครองดินแดนในเชิงภูมิศาสตร์แต่ต้องการครอบงำทางการเมืองและเศรษฐกิจ ปรากฏการณ์ดังกล่าว เช่น การแทรกแซงการทางการเมือง หรือการเลือกตั้งจากประเทศมหาอำนาจในประเทศต่าง ๆ ที่จะส่งผลกระทบทางบวกให้กับตน ทั้งนี้ รูปแบบของ “สงครามลูกผสม” (Hybrid warfare) ได้รับความสนใจมากขึ้นตั้งแต่ปี ค.ศ. 2014 เมื่อรัสเซียผนวกดินแดนไครเมียเข้ามาเป็นส่วนหนึ่งของประเทศผ่านการปฏิบัติการในหลากหลายรูปแบบ ได้แก่ การใช้กองกำลังไม่ระบุตัว (Little Green Men) ของรัสเซียโดยอ้างว่าเป็น “กองกำลังติดอาวุธท้องถิ่น” เพื่อควบคุมโครงสร้างพื้นฐาน เช่น สนามบิน อาคารรัฐบาล การทำสงครามข้อมูล (Information Warfare) ปล่อยข่าวปลอมและโฆษณาชวนเชื่อทางสื่อรัสเซียและสื่อสังคม เช่น การกล่าวอ้างว่ารัฐบาลยูเครนเป็นนาซี หรือข่มเหงชาวรัสเซียในไครเมีย การปฏิบัติการจิตวิทยา (Psychological operations) ทำให้ประชาชนเกิดความสับสนและแบ่งฝ่าย ด้วยการแทรกแซงข้อมูลผ่านสื่อสังคมออนไลน์และสื่อมวลชน การสนับสนุนกลุ่มติดอาวุธท้องถิ่น (Proxy forces) รวมถึงสนับสนุนกลุ่มติดอาวุธแบ่งแยกดินแดนในไครเมียและดอนบาส เช่น การจัดหาอาวุธและเงินทุน การจัดประชามติอย่างเร่งด่วน โดยจัดประชามติเพื่ออ้างว่าชาวไครเมียต้องการแยกตัวไปรวมกับรัสเซีย และการโจมตีทางไซเบอร์ (Cyberattack) โดยมีรายงานการโจมตีโครงข่ายการสื่อสารและระบบอินเทอร์เน็ตของรัฐบาลยูเครนช่วงเวลาดังกล่าว

นิยามสงครามลูกผสม

สงครามลูกผสม (Hybrid warfare) กล่าวถึงรูปแบบความขัดแย้งที่ผสมผสานระหว่างความสามารถทางทหารตามแบบแผนแบบดั้งเดิม ยุทธวิธีที่ไม่ปกติ การก่อการร้าย และการก่ออาชญากรรมในรูปแบบต่าง ๆ เช่น สร้างความรุนแรง ปลุกปั่นสังคมให้เกิดความไม่สงบ ยุยงสร้างความแตกแยก โดยปรับใช้รูปแบบที่หลากหลายในเวลาเดียวกันทั้งการใช้เทคโนโลยีชั้นสูง การโจมตีแบบ

กองโจร (Guerrilla warfare) การโจมตีทางไซเบอร์ การปฏิบัติการทางจิตวิทยา เพื่อบรรลุเป้าหมายเชิงกลยุทธ์ที่ตั้งไว้ สงครามลูกผสมไม่มีเส้นแบ่งที่ชัดเจนระหว่าง การสู้รบที่ใช้กำลังและการไม่ใช้กำลัง สงครามและความสงบ มิติความขัดแย้งทางกายภาพและโลกเสมือน ซึ่งผู้ปฏิบัติการอาจเป็นรัฐ หรือไม่ใช่รัฐก็ได้ สิ่งเหล่านี้ทำให้รูปแบบสงครามมีความยืดหยุ่นและซับซ้อนสูง (Hajduk & Stȩpniewski, 2016) สงครามลูกผสมขยายขอบเขตไปสู่การกระทำของรัฐที่พยายามสร้างความคลุมเครือเชิงกลยุทธ์อย่างสร้างสรรค์ทำให้ไม่สามารถระบุว่าเป็นการใช้กำลังบังคับ อันเป็นผลให้กระบวนการตัดสินใจของฝ่ายตรงข้ามมีความซับซ้อนมากขึ้น หรือลดประสิทธิผลในการตัดสินใจ ทำให้เกิดพื้นที่สีเทาที่ไม่สามารถระบุขอบเขตได้อย่างชัดเจน โดยพื้นที่สีเทาที่ปราศจากการป้องกันจะถูกนำมาใช้ประโยชน์ทางการเมืองจากกลยุทธ์อื่น ๆ ที่ไม่ใช่วิธีการทางทหาร เช่น กองกำลังที่ไม่สามารถระบุฝ่าย การโจมตีทางไซเบอร์ นั่นคือ ผู้ทำสงครามใช้เครื่องแห่งอำนาจ คือ การทหาร การเมือง เศรษฐกิจ พลเรือน และข้อมูล เพื่อบั่นทอนเสถียรภาพ โจมตีจุดอ่อน หรือใช้ประโยชน์จากความเปราะบางของฝ่ายตรงข้าม ได้แก่ การเมือง การทหาร เศรษฐกิจ สังคม ข้อมูล โครงสร้างพื้นฐาน และความสัมพันธ์ระหว่างประเทศ เพื่อบรรลุเป้าหมายที่ตนต้องการ

กรณีศึกษาการโจมตีทางไซเบอร์ในสงครามลูกผสม

สงครามลูกผสมรัสเซีย–ยูเครน ในปี ค.ศ. 2022

ผู้ขัดแย้งหลักของสงคราม คือ รัสเซียกับยูเครนและกลุ่มประเทศนาโต้ (NATO) มีรายงานข่าวการทำสงครามในหลายมิติ ทั้งการใช้ทหาร และกลุ่มติดอาวุธไม่ระบุตัวตน รวมถึงการใช้ทหารรับจ้าง ตั้งแต่ช่วงต้นของสงครามตั้งแต่ ปี ค.ศ. 2022 เช่น กลุ่มแวกเนอร์ จนกระทั่งการยอมรับจากทางประเทศรัสเซียในการร่วมรบกับทหารเกาหลีเหนือในปี ค.ศ. 2025 นอกจากนี้ ยังมีการโจมตีโดยใช้เทคโนโลยีชั้นสูง และมีการใช้มาตรการตอบโต้ทั้งมาตรการคว่ำบาตรทางพลังงานและทางการเงิน และมีหลักฐานการแทรกแซงทางไซเบอร์เพื่อทำลายโครงสร้างพื้นฐาน สร้างความปั่นป่วนทางข้อมูล รบกวนการสื่อสารและควบคุมทางทหาร รวมทั้งการใช้โฆษณาชวนเชื่อที่ผ่านช่องทางสื่อดั้งเดิมและสื่อใหม่

การโจมตีทางไซเบอร์ของรัสเซียต่อยูเครน ใช้ควบคู่กับการปฏิบัติการทางทหารต่อยูเครนเพื่อเพิ่มประสิทธิภาพและผลกระทบของการโจมตี โดยมุ่งเป้าไปที่โครงสร้างพื้นฐานสำคัญ เช่น ระบบพลังงาน การคมนาคม และการสื่อสาร เพื่อสร้างความเสียหายสูงสุด โดยมีการโจมตีในหลากหลายรูปแบบ ได้แก่ เดือนมกราคม ค.ศ. 2022 เว็บไซต์รัฐบาลยูเครน กระทรวงการต่างประเทศ และหน่วยงานรัฐถูกเปลี่ยนหน้าเว็บไซต์ (Defacement) เป็นข้อความขู่ “จงกลัวและจงรอสิ่งที่เลวร้าย” พร้อมข้อความภาษารัสเซีย โปแลนด์ และยูเครน เดือนกุมภาพันธ์ ค.ศ. 2022 Wiper malware “WhisperGate” ตรวจพบมัลแวร์ (Malware) ที่ลบข้อมูลในหน่วยงานรัฐบาลและองค์กรสำคัญในยูเครน

ถูก Microsoft ตรวจสอบและเตือนล่วงหน้า นอกจากนี้ ยังโจมตีดาวเทียม Viasat ระบบดาวเทียม KA-SAT ถูกแฮก ทำให้โมเด็มดาวเทียมกว่า 30,000 เครื่องในยูเครนและยุโรปตะวันออกหยุดทำงาน มีผลกระทบกับการสื่อสารทหารยูเครน เดือนมีนาคม ค.ศ. 2022 มัลแวร์ “HermeticWiper”, “IsaacWiper”, “CaddyWiper” หลายรูปแบบของมัลแวร์ ถูกใช้เพื่อลบข้อมูลในหน่วยงานรัฐ, ธนาคาร, และบริษัทโทรคมนาคม ระหว่างปี ค.ศ. 2022–2023 การเจาะข้อมูลและ DDoS (Distributed Denial of Service) หน่วยงานรัฐ ธนาคาร (เช่น PrivatBank) และระบบขนส่งของยูเครน ถูกโจมตี DDoS เป็นระยะ ในเดือนมกราคม ค.ศ. 2024 รัสเซียได้โจมตีระบบสารสนเทศของรัฐบาลท้องถิ่นหลายแห่ง รวมถึงบริษัทพลังงานของรัฐ ทำให้บริการสาธารณะหยุดชะงัก รัฐบาลยูเครน รายงานว่า ในปี ค.ศ. 2024 ถูกโจมตีทางไซเบอร์เพิ่มขึ้น 68% มีเหตุการณ์ 4,315 ครั้ง ในปี ค.ศ. 2024 เทียบกับปี ค.ศ. 2023 ซึ่งมีเหตุการณ์ 2,541 ครั้ง ซึ่งมักโจมตีหน่วยงานรัฐบาลท้องถิ่น องค์กรของรัฐ ภาคความมั่นคงและการป้องกันประเทศ องค์กรเชิงพาณิชย์ พลังงาน โทรคมนาคม (IMI, 2025)

การโจมตีทางไซเบอร์ของยูเครนรัสเซีย ใช้เพื่อเพิ่มประสิทธิภาพในการต่อสู้ โดยเลือกเป้าหมายที่มีผลกระทบสูง เช่น โครงสร้างพื้นฐานสำคัญของรัสเซีย อันได้แก่ ระบบพลังงาน การคมนาคม และการสื่อสาร เพื่อสร้างความเสียหายสูงสุด ในเดือนกุมภาพันธ์ ค.ศ. 2022 เว็บไซต์ของรัฐบาลรัสเซียถูกโจมตี เช่น กระทรวงการต่างประเทศ กระทรวงกลาโหม กระทรวงกิจการภายใน หน่วยรักษาความปลอดภัยและคณะรัฐมนตรี รวมไปถึงหน่วยงานกำกับดูแลสื่อของรัสเซีย แฮกเกอร์ยังโจมตีช่องทีวีรัสเซียเพื่อเปิดเพลงยูเครนอีกด้วย (IMI, 2025) ในเดือนเมษายน ค.ศ. 2024 กลุ่มแฮกเกอร์ได้ดำเนินการแฮกกล้องวงจรปิด (CCTV) และระบบเฝ้าระวังในแคว้นคูร์สก์ (Kursk Oblast) ของรัสเซีย อีกทั้งได้แสดงภาพสงครามผ่านทางโทรทัศน์ของรัสเซียในพื้นที่ดังกล่าว เพื่อแสดงให้เห็นถึงความสูญเสียของรัสเซียในเมืองซุดชา (Sudzha) ซึ่งตั้งอยู่ในแคว้นคูร์สก์ เดือนมิถุนายน ค.ศ. 2024 หน่วยข่าวกรองทางทหารของยูเครน (HUR) ได้ดำเนินการโจมตีเว็บไซต์กระทรวงต่าง ๆ ของรัสเซีย เช่น กระทรวงยุติธรรม กลาโหม เทคโนโลยีสารสนเทศ การคลัง นอกจากนี้ ผู้ให้บริการอินเทอร์เน็ตรายใหญ่ในไครเมียที่ถูกรัสเซียยึดครองถูกโจมตีทางไซเบอร์อย่างหนัก ส่งผลให้บริการอินเทอร์เน็ตในพื้นที่หยุดชะงัก ในวันชาติรัสเซีย ปี ค.ศ. 2024 กลุ่มแฮกเกอร์ยูเครนได้โจมตีระบบออนไลน์ของสนามบินหลายแห่งในรัสเซีย เช่น สนามบิน Domodedovo ในมอสโก และสนามบินใน Yuzhno-Sakhalinsk และ Saratov ส่งผลให้เที่ยวบินล่าช้าและบางเที่ยวบินต้องเปลี่ยนเส้นทาง รวมถึง HUR ร่วมกับกลุ่มแฮกเกอร์ BO Team โจมตีระบบดิจิทัลของการบริหารเมืองอุลยานอฟสค์ (Ulyanovsk) ทำให้ระบบไอทีเสียหายอย่างมาก รวมถึงการลบข้อมูลประมาณ 20 เทราไบต์ และการเผยแพร่คำสั่งปลอมบนเว็บไซต์ของเมือง เดือนกรกฎาคม ค.ศ. 2024 สถาบันการเงินรัสเซียระบุว่ามีส่วนเกี่ยวข้องในการระดมทุนกิจกรรมทางทหารต่อต้านยูเครนถูกโจมตี ส่งผลกระทบต่อโครงสร้างพื้นฐานการธนาคารเสมือนจริงของรัสเซียหลายด้าน รวมถึงการหยุดทำงานของระบบแอปพลิเคชั่น และพอร์ทัลของธนาคารหลายแห่ง เช่น Dom.RF, VTB Bank, Gazprombank, Sberbank เป็นต้น และยังโจมตีระบบขนส่งสาธารณะ เครือข่าย

สังคมยอดนิยมของรัสเซีย และแพลตฟอร์มอินเทอร์เน็ต ทำให้บริการของผู้ให้บริการโทรคมนาคมและอินเทอร์เน็ตรายใหญ่หลายรายของรัสเซียหยุดชะงัก เช่น MegaFon, Tele2, Beeline และ Rostelecom เดือนกุมภาพันธ์ ค.ศ. 2025 ยูเครนได้ดำเนินการโจมตีทางไซเบอร์ต่อบริษัทที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านพลังงานของรัสเซีย โดยมีรายงานว่ามีเซิร์ฟเวอร์กว่า 120 เครื่องไม่สามารถใช้งานได้ ส่งผลกระทบต่อการดำเนินงานของบริษัทเหล่านี้

สงครามลูกผสมกาซา ในปี ค.ศ. 2023

ในเดือนตุลาคมปี ค.ศ. 2023 กลุ่มติดอาวุธชาวปาเลสไตน์ (เช่น ฮามาส และฮิซบอลเลาะห์) ซึ่งนำโดยกลุ่มฮามาส โจมตีอิสราเอลโดยการยิงจรวดจากเขตฉนวนกาซาเข้าไปในดินแดนอิสราเอล และจับตัวประกัน 251 คนในดินแดนอิสราเอล คู่ขัดแย้งหลักของสงคราม คือ อิสราเอล และฮามาส อย่างไรก็ดี กลุ่มฮามาสได้ประกาศว่าสนับสนุนการทำสงครามในครั้งนี้มีอิหร่านเป็นผู้สนับสนุน ซึ่งสงครามกาซานี้ถูกมองว่าเป็นสงครามตัวแทนความขัดแย้งระหว่างอิสราเอลและอิหร่าน ซึ่งทวีความรุนแรงขึ้นในปี ค.ศ. 2024 ส่งผลให้เกิดการเผชิญหน้ากันของคู่ขัดแย้งโดยตรง สงครามกาซาในปี ค.ศ. 2023 มีการผสมผสานระหว่างการรบโดยใช้กองกำลังทหารและเทคโนโลยีชั้นสูง เช่น โดรน เครื่องร่อน ระเบิดแสวงเครื่อง การรบแบบกองโจร การใช้เครือข่ายอุโมงค์ใต้ดิน การก่อการร้าย การโจมตีทางไซเบอร์ และการปฏิบัติการข้อมูลข่าวสาร

การโจมตีทางไซเบอร์จากกลุ่มสนับสนุนปาเลสไตน์ต่ออิสราเอล อิสราเอลถูกโจมตีทางไซเบอร์เพิ่มขึ้น 3 เท่าตั้งแต่เดือนตุลาคม ค.ศ. 2023 เป็นต้นมา จากอิหร่านและกลุ่มพันธมิตร เช่น ฮิซบอลเลาะห์ โดยมีการโจมตีรวมถึงการฟิชชิ่ง (Phishing) การโจมตีแบบ DDoS และการเจาะระบบ (Hacking) ผ่านผู้ให้บริการ Managed Service Providers (MSPs) รายงานของ Atlantic Council (Handler, 2022) ระบุว่า กลุ่มฮามาสมีการเตรียมตัวโดยการเก็บข้อมูล และเรียนรู้ปฏิบัติการทางทหารของอิสราเอลจากการโจมตีทางไซเบอร์ เช่น การพัฒนาแอปพลิเคชันฟรีเผยแพร่บนระบบแอนดรอยด์ เช่น แอปพลิเคชัน Golden Cup ซึ่งเป็นโปรแกรมที่รวบรวมผลคะแนนล่าสุดในการแข่งขันบอลโลกตั้งแต่ปี ค.ศ. 2018 เพื่อแฝงมัลแวร์ และสอดแนมทหารอิสราเอล แอปพลิเคชันฟิตเนสที่ติดตามเส้นทางการวิ่งของผู้ใช้ มุ่งเป้าไปยังกลุ่มทหารอิสราเอล เพื่อรวบรวมข้อมูลสถานที่ในเขตที่มีความอ่อนไหวเป็นพิเศษ รวมถึง แอปพลิเคชันหาคู่ที่มีสปายแวร์ (Spyware) ต่างๆ เช่น Catch&See และ GrixyApp เพื่อรวบรวมข้อมูลสำหรับการทำสงคราม และยังพบว่า ฮามาสโจมตีระบบกล้องวงจรปิดในอิสราเอลล่วงหน้าถึง 7 ปี เพื่อติดตามกลุ่มเป้าหมายและระบุจุดที่เสี่ยงต่อการถูกโจมตี (English, 2024) กลุ่มแฮกเกอร์ "Dark Storm Team" ซึ่งสนับสนุนปาเลสไตน์ (Pro–Palestinian) ได้ดำเนินการโจมตี DDoS ต่อโครงสร้างพื้นฐานของอิสราเอลและพันธมิตร เดือนธันวาคม ค.ศ. 2023 รัฐบาลอิสราเอลเปิดเผยว่าอิหร่านและกลุ่มฮิซบอลเลาะห์อยู่เบื้องหลังความพยายามโจมตีทางไซเบอร์ต่อโรงพยาบาล Ziv ของอิสราเอลการโจมตีถูกสกัดกั้นก่อนที่จะสร้างความเสียหายมีเพียงข้อมูลบางส่วนถูกขโมย ทั้งนี้ กองกำลังป้องกันประเทศอิสราเอล

(Israel Defense Force: IDF) รายงานว่า ตั้งแต่วันที่ 7 ตุลาคม ค.ศ. 2023 เป็นต้นมา ระบบคลาวด์ของ IDF ถูกโจมตีทางไซเบอร์มากกว่า 3 พันล้านครั้ง แต่ไม่สามารถเจาะระบบได้สำเร็จ

การโจมตีทางไซเบอร์ของอิสราเอลต่อคู่ขัดแย้ง ในเดือนกันยายน ค.ศ. 2024 อิสราเอลได้ปฏิบัติการโจมตีทางไซเบอร์ผ่านระบบการสื่อสารเพจเจอร์ที่ใช้โดยสมาชิกฮิซบอลเลาะห์ในเลบานอน ระเบิดขึ้นพร้อมกัน เหตุการณ์นี้เชื่อว่าเป็นผลมาจากการที่อิสราเอลแทรกแซงห่วงโซ่อุปทานของอุปกรณ์เหล่านี้ โดยฝังวัตถุระเบิดขนาดเล็กไว้ในเพจเจอร์ และจุดระเบิดผ่านสัญญาณที่เข้ารหัส อย่างไรก็ตาม หน่วย 8200 ของ IDF ซึ่งเป็นหน่วยงานด้านสงครามไซเบอร์มีความเชี่ยวชาญในการสอดแนม การวิเคราะห์ข้อมูล และการโจมตีทางไซเบอร์ถูกวิพากษ์วิจารณ์ถึงความล้มเหลวในการคาดการณ์การโจมตีของฮามาสเมื่อวันที่ 7 ตุลาคม ค.ศ. 2023 เนื่องจากหน่วย 8200 ได้หยุดการสอดแนมวิทยุสื่อสารของฮามาสในปี ค.ศ. 2022 ซึ่งอาจเป็นสาเหตุหนึ่งที่ทำให้ไม่สามารถตรวจจับสัญญาณเตือนล่วงหน้าได้

กรณีศึกษามาตรการรับมือภัยคุกคามทางไซเบอร์

การตอบโต้ของประเทศคู่ความขัดแย้งมีมาตรการแตกต่างกันในหลายระดับ โดยระดับความสามารถในการรับขึ้นอยู่กับการบังคับใช้กฎหมาย การให้อำนาจหน่วยงานในการควบคุม การบูรณาการความร่วมมือ รวมถึงศักยภาพของบุคลากรของรัฐ

การรับมือภัยคุกคามทางไซเบอร์ของรัสเซีย

ถึงแม้ว่ารัสเซียถูกระบุว่าเป็นหนึ่งในประเทศต้นทางการโจมตีไซเบอร์สูงสุดในปี ค.ศ. 2024 และติดอันดับ 1 ใน 3 ของประเทศที่มีขีดความสามารถทางไซเบอร์ (Cyber capabilities) สูงสุดในโลก ปี ค.ศ. 2024 (Lowy Institute, n.d.; Voo, Hemani & Cassidy, 2022) อย่างไรก็ตาม ในสงครามรัสเซีย–ยูเครน รัสเซียก็เผชิญกับการโจมตีทางไซเบอร์จากยูเครนและกลุ่มแฮกติวิสต์ (Hacktivist) ทั่วโลกที่สนับสนุนยูเครนเช่นกัน รัสเซียจึงมีมาตรการป้องกันที่หลากหลาย ทั้งด้านกฎหมาย เทคนิค และการควบคุมข้อมูล เพื่อเสริมสร้างความมั่นคงทางไซเบอร์ภายในประเทศ

ด้านกฎหมาย รัสเซียมีกฎหมายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์หลายฉบับ เช่น Federal Law On the Security of Critical Information Infrastructure of the Russian Federation" No. 187–FZ, 2017 หรือ CII Law กำหนดมาตรการด้านความปลอดภัยของโครงสร้างพื้นฐานสำคัญทางข้อมูล ซึ่งผู้ดำเนินการต้องจดทะเบียนกับรัฐและปฏิบัติตามข้อกำหนดความปลอดภัย Sovereign Internet Law (Federal Law No. 90–FZ) ให้อำนาจรัฐควบคุมและแยกการดำเนินงานอินเทอร์เน็ตในประเทศ (Runet) จากเครือข่ายโลก Federal Law No. 152–FZ หรือ Personal Data Law กำหนดให้ข้อมูลส่วนบุคคลของพลเมืองรัสเซียต้องถูกจัดเก็บในเซิร์ฟเวอร์ภายในประเทศ รวมถึง Yarovaya Law

บังคับให้ผู้ให้บริการโทรคมนาคมเก็บข้อมูลการสื่อสาร (Metadata และเนื้อหา) และให้ข้อมูลแก่รัฐตามคำขอภายใต้การควบคุมความมั่นคง

ด้านความสามารถทางเทคนิค มีการลงทุนในโครงสร้างพื้นฐานสำคัญ เช่น เครือข่ายพลังงาน การเงิน และโทรคมนาคม โดยเน้นการใช้เทคโนโลยีและซอฟต์แวร์ที่พัฒนาขึ้นภายในประเทศเพื่อลดการพึ่งพาเทคโนโลยีจากต่างประเทศ นอกจากนี้ ยังมีระบบตรวจสอบและป้องกันภัยคุกคาม ที่เป็นระบบการตรวจสอบภัยคุกคามทางไซเบอร์แบบรวมศูนย์ (Centralized threat intelligence) และมีการพัฒนาเครื่องมือและเทคนิคในการตรวจจับการบุกรุกและการโจมตี จะเห็นได้ว่า การป้องกันทางไซเบอร์ของรัสเซีย มีการดำเนินการอย่างเข้มงวดทั้งควบคุมโครงสร้างพื้นฐานดิจิทัลภายในประเทศ จำกัดการเข้าถึงอินเทอร์เน็ตจากต่างประเทศ ใช้ซอฟต์แวร์และฮาร์ดแวร์ภายในประเทศ เพื่อลดความเสี่ยงจากการแทรกซึมของมัลแวร์หรือการโจมตีจากภายนอก อธิปไตยทางอินเทอร์เน็ตที่มีระบบอินเทอร์เน็ตที่สามารถแยกตัวออกจากอินเทอร์เน็ตสากลได้ รองรับภัยคุกคามไซเบอร์จากต่างประเทศ ซึ่งสามารถบล็อกเว็บไซต์ แอปพลิเคชัน และข้อมูลที่รัฐมองว่าเป็นภัยต่อความมั่นคง เช่น Google, Facebook, Twitter เพื่อให้สามารถควบคุมการไหลของข้อมูลและป้องกันการโจมตีจากภายนอกได้ง่ายขึ้น (Freedom House, 2023)

ด้านหน่วยงานและการจัดการ หน่วยงานหลัก คือ Federal Security Service (FSB) ดูแลด้านข่าวกรองและความมั่นคงไซเบอร์ภายใน ซึ่งมีศูนย์เฉพาะทางด้านไซเบอร์ เช่น Center 16 รับผิดชอบการดักจับข้อมูลและการโจมตีทางไซเบอร์เพื่อรวบรวมข่าวกรอง และ Center 18 รับผิดชอบด้านความมั่นคงทางไซเบอร์เชิงรับ การต่อต้านข่าวกรอง และการปกป้องโครงสร้างพื้นฐานที่สำคัญ ทำงานใกล้ชิดกับหน่วยข่าวกรอง เช่น Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), Foreign Intelligence Service (SVR) และหน่วยงานที่เกี่ยวข้อง เช่น Ministry of Digital Development, Communications and Mass Media, Federal Protective Service (FSO), Roskomnadzor, Federal Technical and Export Control Service (FSTEC) (Bowen, 2022)

การพัฒนาศักยภาพ สำหรับหน่วยงานและบุคลากรทั้งในภาครัฐและเอกชนที่ทำงานร่วมกันเพื่อป้องกัน ตรวจจับ และตอบสนองต่อการโจมตี ซึ่งมีการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ (ForumSPB, 2023) รวมถึงเสริมสร้างความมั่นคงทางไซเบอร์ของหน่วยงานรัฐ ทั้งการอัปเดตซอฟต์แวร์ ปรับปรุงระบบป้องกัน และฝึกอบรมเจ้าหน้าที่ให้มีความรู้ด้านความปลอดภัยทางไซเบอร์ เพื่อป้องกันการโจมตีจากกลุ่มแฮกเกอร์

ด้านความร่วมมือ หน่วยงานที่เกี่ยวข้องทำงานร่วมกันอย่างมีเอกภาพ นอกจากนี้ยังมีความร่วมมือระหว่างภาคเอกชน และกลุ่มแฮกติวิสต์ที่สนับสนุนรัสเซีย เช่น Killnet รวมถึงกลุ่มอิทธิพลสนับสนุนรัสเซียและเบาลรุส เพื่อลดการพึ่งพาตะวันตก (Voo, 2025)

การรับมือภัยคุกคามทางไซเบอร์ของยูเครน

การรับมือกับภัยคุคามทางไซเบอร์ของยูเครนได้รับการสนับสนุนจากชาติพันธมิตร เช่น สหรัฐอเมริกาและสหภาพยุโรป รวมถึงองค์การต่างชาติ เช่น NATO ในหลายมิติ

ด้านกฎหมาย รัสเซียมีกฎหมายที่เกี่ยวข้อง เช่น Law on the Basic Principles of Cybersecurity of Ukraine เสริมสร้างความสามารถในการป้องกันทางไซเบอร์ของประเทศและปกป้องทรัพยากรข้อมูลของรัฐให้สอดคล้องกับแนวทางของสหภาพยุโรป (NIS2 Directive) ซึ่งเป็นกฎหมายไซเบอร์ฉบับหลักของยูเครน วางกรอบการดำเนินงาน ความร่วมมือ และการป้องกันไซเบอร์ระดับชาติ โดยความผิดหลักเกี่ยวกับความปลอดภัยไซเบอร์ถูกกำหนดไว้ในมาตรา 360–363 ของประมวลกฎหมายอาญาของยูเครน และกฎหมายอื่นที่เกี่ยวข้อง เช่น Law of Ukraine on Information Protection in Information and Telecommunication Systems ซึ่งเป็นหลักการด้านการป้องกันข้อมูลในระบบสารสนเทศและการสื่อสาร ใช้ควบคู่กับกฎหมายไซเบอร์ฉบับหลัก Law on Personal Data Protection ควบคุมการเก็บ ใช้ และปกป้องข้อมูลส่วนบุคคล รวมถึง Law on Critical Infrastructure Protection กำหนดให้หน่วยงานรัฐและเอกชนที่ดูแลโครงสร้างพื้นฐานสำคัญ ต้องมีมาตรการป้องกันภัยไซเบอร์และรายงานเหตุการณ์ รวมทั้งประธานาธิบดีได้ออกคำสั่ง Decrees by the President on Cybersecurity Emergency Response เกี่ยวกับการป้องกันและรับมือเหตุการณ์ไซเบอร์ในช่วงสงคราม เช่น การตอบโต้ APT และการร่วมมือกับพันธมิตรตะวันตก

ความสามารถทางเทคนิค ยูเครนย้ายข้อมูลภาครัฐและระบบสำคัญไปยังแพลตฟอร์มคลาวด์ทั้งในและนอกประเทศ (Amazon Web Services, 2022) เพื่อเพิ่มความปลอดภัยและความยืดหยุ่น ลดความเสี่ยงจากการโจมตีทางไซเบอร์โดยตรงต่อเซิร์ฟเวอร์ในประเทศ และมีระบบสำรองโครงสร้างพื้นฐานระบบสารสนเทศ เช่น Starlink

ด้านหน่วยงานและการจัดการ สำหรับยูเครนเอง ได้มีการพัฒนาและบังคับใช้ยุทธศาสตร์ความมั่นคงทางไซเบอร์ ได้แก่ Cybersecurity Strategy for 2021–2025 เพื่อเสริมสร้างความยืดหยุ่นทางไซเบอร์ของประเทศ มุ่งเน้นการเพิ่มความสามารถในการป้องกันภัยไซเบอร์ของประเทศ กิจกรรมข่าวกรอง การปราบปรามอาชญากรรมทางไซเบอร์ และการพัฒนาเครื่องมือป้องกันภัย โดยมีหน่วยงานหลัก ได้แก่ State Service of Special Communications and Information Protection (SSSCIP) กำหนดและดำเนินการนโยบายด้านความมั่นคงทางไซเบอร์แห่งชาติ การปกป้องทรัพยากรข้อมูลของรัฐ และโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญ (CII) บริหารจัดการและประสานงานด้านความมั่นคงทางไซเบอร์โดยรวมของประเทศ และหน่วยงานความมั่นคง เช่น National Coordination Center for Cybersecurity (NCCC), Security Service of Ukraine (SBU), Main Directorate of Intelligence of the Ministry of Defense of Ukraine (GUR/HUR MO) และสร้างหน่วยงานเฉพาะทางสำหรับการตอบสนองต่อเหตุการณ์ไซเบอร์ (CERT–UA) นอกจากนี้ยังมีหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เช่น Ministry of Digital Transformation (MOD) (Semenchenko, Pleskach, Zaiarnyi & Pleskach, 2020)

การพัฒนาศักยภาพ ยูเครนร่วมมือกับพันธมิตร เช่น สหรัฐอเมริกา สหราชอาณาจักร สหภาพยุโรป และนาโต้ ในการแลกเปลี่ยนข้อมูลภัยคุกคาม การฝึกอบรมผู้เชี่ยวชาญ การจัดหาอุปกรณ์ และการให้คำปรึกษาทางเทคนิค ยูเครนลงทุนพัฒนาบุคลากรด้านความมั่นคงทางไซเบอร์ของตนเองอย่างต่อเนื่อง (Bandouil, 2025)

ความร่วมมือ ยูเครนได้รับการสนับสนุนและความร่วมมือจากชาติพันธมิตรตะวันตก เช่น สหภาพยุโรป ในการแลกเปลี่ยนข้อมูลและความร่วมมือ และสหรัฐอเมริกา ซึ่งให้ความช่วยเหลือทั้งทางด้านเทคนิคและเงินสนับสนุน นอกจากนี้ ยังมีการระดมอาสาสมัครกลุ่มแฮกติวิสต์ IT Army ที่สนับสนุนยูเครนเพื่อโจมตีและต่อต้านการโจมตีทางไซเบอร์จากรัสเซีย (Done, 2023)

การรับมือภัยคุกคามทางไซเบอร์ของประเทศอิสราเอล

อิสราเอล ดำเนินมาตรการการป้องกันทางไซเบอร์เชิงรุกและเชิงรับ โดยมีการดำเนินการในด้านต่าง ๆ ดังนี้

ด้านกฎหมาย กฎหมายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ได้แก่ Protection of Privacy Law (PPL) คุ้มครองข้อมูลส่วนบุคคลของประชาชน กำหนดการเก็บ การใช้ และการโอนข้อมูล รวมถึงความมั่นคงของระบบสารสนเทศที่จัดเก็บข้อมูลส่วนตัว Computer Law กำหนดความผิดเกี่ยวกับการเข้าถึงข้อมูลโดยมิชอบ การรบกวนหรือทำลายข้อมูลในระบบคอมพิวเตอร์ มีผลต่อการดำเนินคดีด้านอาชญากรรมทางไซเบอร์ The Regulation of Security in Public Bodies Law ควบคุมการคุ้มครองหน่วยงานของรัฐและหน่วยงานสาธารณะที่ให้บริการสาธารณะที่จำเป็นและโครงสร้างพื้นฐานที่สำคัญ ในเรื่องที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์ Classified Information Protection Laws ครอบคลุมกฎหมายความมั่นคงของข้อมูลที่ใช้ในกองทัพ เช่น หน่วย Unit 8200 และหน่วยงานข่าวกรองภายในประเทศ นอกจากนี้ อิสราเอลยังมีการออกข้อบังคับฉุกเฉิน (Iron Swords) หรือผ่านกฎหมายชั่วคราว เช่น A "Temporary Law on Handling Severe Cyberattacks in the Digital and Storage Services Sector (Iron Swords) 5774–2023 เฉพาะในห้วงเวลาที่การโจมตีทางไซเบอร์ที่รุนแรงอีกด้วย โดยกฎหมายและมาตรการฉุกเฉิน ที่ออกในเดือนพฤศจิกายน ค.ศ. 2023 ให้อำนาจแก่ INCD และหน่วยงานอื่นๆ ในการตรวจจับ ป้องกัน และควบคุมการโจมตีทางไซเบอร์ที่รุนแรงในภาคบริการดิจิทัลและบริการจัดเก็บข้อมูล

ด้านความสามารถทางเทคนิค มีการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ในปฏิบัติการทางไซเบอร์ในการตรวจจับภัยคุกคามและการตอบสนองต่อการโจมตีแบบเรียลไทม์ อิสราเอล ปกป้องโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) เช่น ระบบพลังงาน น้ำ การเงิน และโทรคมนาคม โดยใช้เทคโนโลยีตรวจจับภัยคุกคามขั้นสูงและการประเมินช่องโหว่อย่างต่อเนื่อง เช่น การประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ในปฏิบัติการทางไซเบอร์ เพื่อเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามแบบเรียลไทม์ การวิเคราะห์ข้อมูล และการตอบสนองต่อการโจมตี รวมถึงใช้แพลตฟอร์มคลาวด์ในการ

จัดเก็บของมูลของรัฐจากทั้งภายในประเทศ (Project Nimbus) จากพันธมิตร เช่น Google/AWS (Haskins, 2024)

ด้านหน่วยงานและนโยบาย อิสราเอลไม่ได้ใช้กฎหมายเดียวครอบคลุมความปลอดภัยทางไซเบอร์หลัก แต่ให้อำนาจแก่หน่วยงานความมั่นคงทางไซเบอร์แห่งชาติอิสราเอล (Israel National Cyber Directorate – INCD) ออกแนวปฏิบัติภาคบังคับและควบคุมผ่านหน่วยงานเฉพาะ ซึ่งเป็นหน่วยงานหลักที่รับผิดชอบในการปกป้องพื้นที่ไซเบอร์ของพลเรือนในอิสราเอล โดยทำงานอย่างใกล้ชิดกับหน่วยข่าวกรองทหาร เช่น Unit 8200, Shin Bet (Barucija, 2020) เพื่อประสานงานการป้องกัน การตรวจจับ และการตอบสนองต่อภัยคุกคาม (Israel National Cyber Directorate, 2025)

การพัฒนาศักยภาพ รัฐบาลเสริมสร้างความตระหนักรู้ของประชาชน ว่าเป็นส่วนสำคัญของการป้องกันภัยทางไซเบอร์ จึงมีการรณรงค์ให้ความรู้เพื่อเพิ่มความตระหนักรู้เกี่ยวกับพิชชิ่งและการโจมตีอื่นๆ (Israel National Cyber Directorate, 2025)

ความร่วมมือ อิสราเอลพัฒนาความร่วมมือด้านความมั่นคงทางไซเบอร์กับสหรัฐอเมริกาหลายโครงการ เช่น การสนับสนุนจาก Cybersecurity and Infrastructure Security Agency (Foundation for defense of democracies, 2023) ความร่วมมือพัฒนาเครื่องมือไซเบอร์ขั้นสูงในโครงการ “Olympic Games” ความร่วมมือพัฒนาเทคโนโลยีด้านความมั่นคงไซเบอร์ภายใต้ United States–Israel Advanced Research Partnership Act (2016) และยังได้รับการสนับสนุนคลาวด์และ AI อีกด้วย

จากการศึกษาสงครามลูกผสมระหว่างรัสเซีย–ยูเครน และสงครามกาซา สามารถสรุปรูปแบบการปฏิบัติการ การโจมตีทางไซเบอร์ และมาตรการรับมือได้ดังแสดงในภาพที่ 1

ภาพที่ 1 สรุปภาพรวมการปฏิบัติการสงครามลูกผสมและการรับมือการปฏิบัติการทางไซเบอร์จากกรณีศึกษา

ความพร้อมต่อการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย

ภัยคุกคามทางไซเบอร์ข้ามแดนสามารถโจมตีประเทศเป้าหมายข้ามพรมแดน จากกรณีศึกษาข้างต้นพบว่าการโจมตีทางไซเบอร์เป็นส่วนหนึ่งของกลยุทธ์ในการทำสงครามเพื่อใช้ประโยชน์จากพื้นที่สีเทา ทำลายความมั่นคงทางเศรษฐกิจ สังคมและการเมืองของประเทศคู่ขัดแย้ง ซึ่งส่วนใหญ่ไม่ได้โจมตีเพื่อเงิน ซึ่งทั้งหน่วยงานรัฐบาลและภาคเอกชนต่างก็มีความเสี่ยงสูงเช่นเดียวกัน (Keepnet Labs, 2024) ทั้งนี้ รัฐบาลไทยมีการดำเนินการต่าง ๆ เพื่อป้องกันและรับมือกับการคุกคามทางไซบอร์ โดยมีการออกนโยบายและกฎหมายที่เกี่ยวข้อง รวมถึงการจัดตั้งหน่วยงานต่าง ๆ เพื่อกำกับดูแล ตรวจสอบ รวมถึงดูแลข้อมูลส่วนบุคคล รวมถึงประสานความร่วมมือกับภาคเอกชนในการป้องกันภัยคุกคามทางไซเบอร์ ดังนี้

ด้านกฎหมาย ประเทศไทยมีกฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มุ่งเน้นการปกป้องโครงสร้างพื้นฐานของประเทศจากภัยคุกคามทางไซเบอร์ เน้นมาตรการป้องกัน กำหนดบทบาทหน้าที่หน่วยงานที่อยู่ภายใต้บังคับ โดยจัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เพื่อกำหนดนโยบาย มาตรการ และแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) เพื่อป้องกัน รับมือ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และยังกำหนดมาตรการรับมือภัยคุกคามทางไซเบอร์ในหลายระดับ โดยกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีกลไกเฝ้าระวังภัยคุกคามทางไซเบอร์ ต้องรายงานเมื่อเกิดเหตุภัยคุกคามและรับมือตามแนวทางที่กำหนด รวมทั้งสามารถเข้าตรวจสอบหน่วยงาน เข้าร่วมในการป้องกัน เสนอแนะหรือสั่งการให้ใช้ระบบในการแก้ปัญหา อีกทั้งวิเคราะห์ข้อมูล แจ้งเตือนภัยคุกคาม และมีการกำหนดบทลงโทษสำหรับผู้ไม่ปฏิบัติตาม หรือฝ่าฝืนคำสั่ง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เน้นการปราบปรามอาชญากรรมคอมพิวเตอร์ กำหนดความผิดและบทลงโทษสำหรับการกระทำผิดทางไซเบอร์ เช่น การเข้าถึงข้อมูลโดยมิชอบ การทำให้ระบบเสียหาย การเผยแพร่ข้อมูลอันเป็นเท็จ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกันการรั่วไหลหรือการนำข้อมูลไปใช้โดยมิชอบ ซึ่งเป็นส่วนสำคัญของความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ส่งเสริมการพัฒนารัฐบาลดิจิทัล พร้อมกับกำหนดให้หน่วยงานรัฐต้องมีมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึง พระราชบัญญัติมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 คุ้มครองประชาชนผู้ถูกหลอกลวงผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์

ด้านหน่วยงานและการจัดการ มีการกำหนด นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570) จัดทำขึ้นโดยคณะกรรมการการรักษาความมั่นคง

ปลอดภัยไซเบอร์แห่งชาติ (กมช.) เพื่อเป็นแนวทางในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยมียุทธศาสตร์หลัก 4 ด้าน ได้แก่ 1) สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ในส่วน บุคลากร องค์ความรู้ และเทคโนโลยี 2) สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ 3) การบูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ 4) สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน เพื่อเป็นกรอบแนวทางในการดำเนินงานด้านความปลอดภัยทางไซเบอร์ของประเทศเช่นกัน (Secretariat of the National Cybersecurity Committee, 2023) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ในสังกัดสำนักนายกรัฐมนตรี ยังได้ประกาศนโยบายระบบคลาวด์ภาครัฐ (Cloud First Policy) โดยได้จัดทำประกาศมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ซึ่งจะมีผลบังคับใช้ในปี พ.ศ. 2569 ทั้งนี้ หน่วยงานหลักที่เกี่ยวข้อง คือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทำหน้าที่จัดทำนโยบาย แผน และมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของชาติ ดูแลและกำกับหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศ รวมถึงตรวจสอบเฝ้าระวัง และประสานงานในการรับมือกับภัยคุกคามทางไซเบอร์ระดับต่าง ๆ ส่งเสริมและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศ ทั้งยังมีบทบาทสำคัญในการรวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ วิเคราะห์ข้อมูลเพื่อหาสัญญาณบ่งชี้การโจมตี และให้ความช่วยเหลือในการกู้คืนระบบหรือข้อมูล มาตรา 67 ของ พระราชบัญญัติไซเบอร์ฯ ระบุว่า "ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง" และ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) ภายใต้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งดำเนินมาตรการเชิงรุก เพื่อป้องกันและเฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น ตรวจสอบและติดตามข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ทั้งในและต่างประเทศอย่างต่อเนื่อง รวบรวม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับรูปแบบภัยคุกคาม ช่องโหว่ และวิธีการโจมตีใหม่ๆ รวมถึงเผยแพร่ความรู้ เช่น พัฒนาและเผยแพร่แนวปฏิบัติ (Best practices) มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ และแจ้งเตือนภัยคุกคามกับหน่วยงานที่เกี่ยวข้องและประชาชนทั่วไปได้รับทราบ และมาตรการเชิงรับ เช่น ดำเนินการรับแจ้งเหตุภัยคุกคาม ตรวจสอบ วิเคราะห์ และประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้น ให้คำแนะนำ ให้ความช่วยเหลือทางเทคนิคแก่หน่วยงานที่ได้รับผลกระทบ รวมถึงรวบรวมหลักฐานทางดิจิทัลที่เกี่ยวข้องกับเหตุการณ์เพื่อใช้ในการสืบสวนและดำเนินคดีตามกฎหมาย ส่วน พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2560 ระบุว่าหากเกิดการโจมตีทางไซเบอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ สำนักงานตำรวจแห่งชาติมีอำนาจตรวจสอบและปราบปรามอาชญากรรมไซเบอร์ สำหรับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เป็นหน่วยงาน

หลักในการกำกับดูแลและส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลของประชาชน โดยมีหน้าที่ วางหลักเกณฑ์ มาตรฐาน และแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ส่งเสริมความตระหนักรู้ รับเรื่องร้องเรียน ตรวจสอบ ให้คำแนะนำแก่หน่วยงานภาครัฐและเอกชนในการปฏิบัติตามกฎหมาย และทำงานร่วมกับหน่วยงานอื่นๆ ทั้งในและต่างประเทศในเรื่องที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

การพัฒนาศักยภาพ พบว่าประเทศไทยจะได้รับการจัดอันดับดัชนีความมั่นคงปลอดภัยไซเบอร์โลก Global Cybersecurity Index 2024 อยู่ในอับดับที่ 7 ของโลก (International Telecommunication Union (ITU), 2024) สะท้อนถึงความมุ่งมั่นและศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ที่แข็งแกร่งทั้งในด้านกฎหมาย มาตรการทางเทคนิค หน่วยงานและนโยบาย การพัฒนาศักยภาพ และความร่วมมือ แต่ ITU ยังคงเสนอแนะให้พัฒนามาตรการในด้านหน่วยงาน/นโยบาย (Organizational measures) ที่เกี่ยวกับโครงสร้างองค์กรและนโยบายระดับชาติที่รองรับความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเมื่อพิจารณาความพร้อมของประเทศไทยในการรับมือภัยคุกคามจากไซเบอร์พบว่า ประเทศไทยจำเป็นต้องพัฒนาความสามารถการรับมืออย่างต่อเนื่อง เนื่องจากดัชนีชี้วัดความเสี่ยงของประเทศต่ออาชญากรรมทางไซเบอร์ Cybersecurity Exposure Index (CEI) 2020 ระบุว่า ประเทศไทยมีความเสี่ยงอยู่ในอันดับที่ 38 ของโลก อีกทั้ง Cybersecurity Country Rankings 2025 จัดประเทศไทยให้ติดอันดับ 7 ของประเทศที่มีความเสี่ยงจากการก่ออาชญากรรมทางไซเบอร์สูงสุด (Salgado, 2024) ถึงแม้ประเทศไทยมีระดับความมุ่งมั่นและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับที่สูง ในทางกลับกัน ประเทศไทยมีความเสี่ยงต่อภัยคุกคามทางไซเบอร์สูงติดอันดับ 1 ใน 10 ประเทศของโลกเช่นกัน จากรายงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พบว่า สถิติภัยคุกคามทางไซเบอร์ตั้งแต่ มกราคม – พฤษภาคม พ.ศ. 2568 พบเหตุการณ์ภัยคุกคามทั้งสิ้น 1,002 เหตุการณ์ โดยหน่วยงานที่ถูกโจมตีสูงสุด 3 อันดับแรก ได้แก่ หน่วยงานด้านการศึกษา 265 เหตุการณ์ หน่วยงานภาครัฐด้านอื่น ๆ 192 เหตุการณ์ และหน่วยงานด้านการเงินและการธนาคาร 177 เหตุการณ์ เมื่อเปรียบเทียบจำนวนเหตุการณ์พบว่าสถิติที่ประกาศจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต่างจากสถิติที่รายงานโดยบริษัทด้านความปลอดภัยไซเบอร์อย่างมีนัยสำคัญ เช่น ไตรมาสแรกของปี พ.ศ. 2567 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรายงานเหตุการณ์ภัยคุมคามทางไซเบอร์รวม 483 เหตุการณ์ ในขณะที่ Kaspersky ระบุว่า ในไตรมาสแรกของปี พ.ศ. 2567 ตรวจพบและสกัดการโจมตี 157,935 รายการ สูงขึ้นจากปีก่อนหน้า สถิติจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในปี พ.ศ. 2568 มีค่าเฉลี่ยเหตุการณ์ที่เกิดขึ้นตั้งแต่เดือน มกราคม – พฤษภาคม ประมาณ 200 เหตุการณ์ต่อเดือน ในขณะที่ Check Point Software Technologies รายงานว่า ประเทศไทยเผชิญกับการโจมตีโดยเฉลี่ย 3,180 ครั้งต่อสัปดาห์ต่อองค์กร ในช่วง 6 เดือนที่ผ่านมา (สิงหาคม พ.ศ. 2567–มกราคม พ.ศ. 2568) ซึ่งสูงกว่าค่าเฉลี่ยทั่วโลกที่ 1,843 ครั้งต่อสัปดาห์ต่อองค์กร ซึ่งมากกว่าค่าเฉลี่ย

ทั้งโลกถึง 70% (Bangkok Post, 2024) อย่างไรก็ตาม ประเทศไทยให้ความสำคัญกับการพัฒนาศักยภาพบุคลากรอย่างต่อเนื่องโดยมีความร่วมมือกับนานาชาติ เช่น ญี่ปุ่น เกาหลีใต้และอาเซียน ในการอบรมแบ่งปันความรู้ และการซ้อมรับมืออย่างต่อเนื่อง (Thailand National Cyber Academy, 2024)

อีกทั้ง พบว่าการสร้างการตระหนักรู้แก่พลเมือง เช่น การแจ้งเตือนรูปแบบภัยคุกคามต่าง ๆ ส่วนใหญ่เป็นการแจ้งเตือนของบริษัทความปลอดภัยไซเบอร์ผ่านช่องทางการสื่อสารเฉพาะและสร้างการรู้ได้ในวงจำกัด ในขณะที่ การตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับสาธารณชนยังอยู่ในวงแคบ ดังแสดงให้เห็นได้จากจำนวนข่าวสารที่เผยแพร่ในช่องทางออนไลน์เกี่ยวกับการโจมตีทางไซเบอร์ที่เกิดขึ้นในประเทศไทย เช่น ข่าวปฏิบัติการ OpThailand ในเดือนมิถุนายน พ.ศ. 2566 ซึ่งเป็นเหตุการณ์ที่ประเทศไทยถูกโจมตีโดยกลุ่มแฮกติวิสต์กัมพูชาที่เรียกตนเองว่า Anonymous Cambodia โจมตี DDoS เว็บไซต์ภาครัฐและเอกชนไทยหลายแห่งส่งผลให้ต้องหยุดให้บริการ ซึ่งมีการขโมยข้อมูลองค์กรบางแห่งด้วย SQLmap และนำไปเผยแพร่ ในเดือนมีนาคม พ.ศ. 2568 เว็บไซต์ของรัฐบาลไทยถูกโจมตีโดยกลุ่ม AnonSecKh เป็นกลุ่มที่มีความเกี่ยวข้องกับกัมพูชา (Pro–Cambodian) โจมตี DDOS มุ่งเป้าไปที่เว็บไซต์ของรัฐบาล หน่วยงานทางทหาร ภาคการผลิต และสถาบันการเงิน เช่น กระทรวงกลาโหม, กระทรวงการต่างประเทศ และกรุงเทพมหานคร การตระหนักรู้ และความสนใจสำหรับพลเมืองไทยในกรณีการถูกโจมตีทางไซเบอร์ทั้ง 2 เหตุการณ์ยังน้อยมากสะท้อนจากจำนวนการค้นหาจาก Google Search ด้วยคำค้นหา “การโจมตีทางไซเบอร์” และ“cyber attack” เพียง 101 ครั้ง ในเดือนมิถุนายน พ.ศ. 2566 และเพียง 95 ครั้ง ในเดือนมีนาคม พ.ศ. 2568 นอกจากนี้ กรณีการแจ้งเตือนภัยคุกคามทางไซเบอร์ข้ามพรมแดนจาก Cyfirma (2024) ที่ระบุว่า ผู้ก่ออาชญากรรมทางไซเบอร์อาจใช้ประโยชน์จากโครงสร้างพื้นฐานด้านความปลอดภัยทางไซเบอร์ที่อ่อนแอของกัมพูชาเพื่อโจมตีข้ามพรมแดน รวมถึงการตระหนักรู้เกี่ยวกับกลุ่มแฮกติวิสต์ที่มีต้นทางอยู่ในกลุ่มประเทศเพื่อนบ้านซึ่งมีการประกาศเตือนการโจมตีข้ามพรมแดน เช่น OceanLotus (หรือ APT32) อันมีสายสัมพันธ์กับรัฐบาลเวียดนามว่า มีส่วนร่วมในการจารกรรมทางไซเบอร์ (Cyber espionage) ต่อรัฐบาลและหน่วยงานทหารของประเทศเพื่อนบ้านในอาเซียน ทว่าข่าวดังกล่าวกลับไม่มีการเผยแพร่ผ่านสำนักข่าวใหญ่ ๆ ที่สามารถเผยแพร่สู่ประชาชนในวงกว้าง

ความสามารถทางเทคนิค ประเทศไทยมีการพัฒนาซอฟท์แวร์ที่พัฒนาเองในประเทศ เช่น TCTA (ThaiCERT Threat Analysis) ซึ่งเป็นระบบเฝ้าระวังภัยไซเบอร์ อย่างไรก็ตาม หน่วยงานส่วนใหญ่ยังคงใช้เทคโนโลยีและซอฟท์แวร์ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์จากต่างประเทศ

ความร่วมมือ ในทางปฏิบัติ การกำกับดูแลของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไม่ครอบคลุมการโจมตีทางไซเบอร์ที่เกิดขึ้นทั้งหมดในประเทศไทย ซึ่งมีความหลากหลายกว่ากลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่กำหนดตาม พ.ร.บ. ไซเบอร์ ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่ง ด้านพลังงานและสาธารณูปโภค ด้าน

สาธารณสุข ทั้งนี้ ประเด็นที่เกี่ยวข้องกับการขยายขอบเขตหน่วยงานไปยังกลุ่มอื่นๆ เช่น ภาคอุตสาหกรรม บริการ พาณิชย์ เครือข่ายโครงสร้างพื้นฐานสารสนเทศ หรือระบบสารสนเทศที่เกี่ยวข้องกับการจัดงานต่าง ๆ ในระดับประเทศ เช่น การเลือกตั้ง การจัดงานระดับนานาชาติ อยู่ในระหว่างการพิจารณาขอบเขตเพิ่มเติมของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ปัจจุบันยังไม่มีหน่วยงานใดที่ตรวจสอบและป้องกันภัยคุกคามในภาพรวมของประเทศ ซึ่งยังขาดการบูรณาการกับหน่วยงานที่เกี่ยวข้อง อย่างไรก็ดี สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีความร่วมมือเฉพาะในบางองค์กร เช่น สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ธนาคารแห่งประเทศไทย ส่งผลให้การวิเคราะห์รูปแบบภัยคุกคามจากไซเบอร์ไม่ครอบคลุมเหตุการณ์จริงที่เกิดขึ้น การวางนโยบาย และแผนการปฏิบัติการต่าง ๆ จึงไม่ครบถ้วนตามสภาพความเป็นจริง การทำงานของหลายหน่วยงานยังคงเป็นในเชิงรับ เช่น พ.ร.บ.ไซเบอร์ ที่มีการกำหนดให้มีการรายงานเมื่อเกิดภัยคุกคาม ยังไม่มีความชัดเจนในส่วนของระยะเวลาในการแจ้งเตือน ลักษณะของภัยคุกคามที่เข้าข่าย และเนื้อหาที่จะต้องระบุในรายงาน บางครั้งหน่วยงานยังไม่ทราบถึงการโจมตีทางไซเบอร์แต่อย่างใด ภาคเอกชนยังมองว่าการรายงานการถูกโจมตีทางไซเบอร์ส่งผลกระทบต่อภาพลักษณ์ขององค์กร ซึ่งส่งผลต่อความเชื่อมั่นและรายได้ขององค์กร นอกจากนั้น หน่วยงานส่วนใหญ่ยังคงไม่มีผู้เชี่ยวชาญทางความปลอดภัยทางไซเบอร์ประจำ และมักจะใช้หน่วยงานที่ปรึกษา หรือทีมภายนอกในการดูแลความปลอดภัยทางไซเบอร์ขององค์กร ดังนั้น เมื่อพบเหตุการณ์โจมตีทางไซเบอร์ บริษัทที่ปรึกษาด้านความปลอดภัยทางไซเบอร์นั้นจะรายงานโดยตรงต่อหน่วยงานเท่านั้น หากการโจมตีไม่เกี่ยวข้องกับอาชญากรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ถือว่าไม่เข้าข่ายความคุ้มครองของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บทลงโทษไม่สามารถบังคับใช้ได้ อีกทั้งระหว่างบริษัทด้านความปลอดภัยไซเบอร์ และระหว่างหน่วยงานกำกับดูแลของรัฐที่เกี่ยวข้องไม่มีการแบ่งปันข้อมูลการโจมตีทางไซเบอร์ ระหว่างกันไทยเป็นสมาชิกในกรอบ ASEAN Cybersecurity Cooperation Strategy เพื่อพัฒนาบุคลากรและซ้อมแผนตอบโต้

การพัฒนาศักยภาพความมั่นคงทางไซเบอร์ของประเทศไทย

จากการเปรียบเทียบกรณีศึกษากับประเทศไทยในการรับมือภัยคุกคามทางไซเบอร์ในด้านต่าง ๆ อ้างอิงจากความพร้อมใน 5 ด้านจากกรอบแนวคิดของ ITU สามารถสรุปตารางเปรียบเทียบได้ดังนี้

ตารางที่ 1 เปรียบเทียบการรับมือภัยคุกคามทางไซเบอร์ระหว่างประเทศกรณีศึกษาและประเทศไทย

ประเทศ	รัสเซีย	ยูเครน	อิสราเอล	ไทย
กฎหมาย และระเบียบข้อบังคับ	กฎหมายอธิปไตยอินเตอร์เน็ต และกฎหมายที่เกี่ยวข้อง	กฎหมายหลัก และกฎหมายที่เกี่ยวข้อง	ไม่มีกฎหมายหลัก แต่ใช้กฎหมายที่เกี่ยวข้องประกอบ	กฎหมายหลัก และกฎหมายที่เกี่ยวข้อง
ความสามารถทางเทคนิค และโครงสร้างพื้นฐาน	มีเทคโนโลยีและโปรแกรมป้องกันความปลอดภัยทางไซเบอร์ที่พัฒนาในประเทศ	ได้รับการสนับสนุนจากสหภาพยุโรป ใช้แพลตฟอร์มคลาวด์	มีเทคโนโลยีและโปรแกรมความปลอดภัยทางไซเบอร์ที่พัฒนาในประเทศ	เริ่มพัฒนาโปรแกรมความปลอดภัยทางไซเบอร์ที่ในประเทศ แต่ยังพึ่งพาภายนอก
หน่วยงานและการจัดการ	มีหน่วยงานหลักความมั่นคงทางไซเบอร์ (ความมั่นคง)	มีหน่วยงานหลักความมั่นคงทางไซเบอร์ (ความมั่นคง)	มีหน่วยงานหลักความมั่นคงทางไซเบอร์ (ความมั่นคง)	มีหน่วยงานหลักความมั่นคงทางไซเบอร์ (สำนักนายกรัฐมนตรี)
การพัฒนาศักยภาพ และการตระหนักรู้	มีการพัฒนาศักยภาพ การปฏิบัติจริงของเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้อง	มีการพัฒนาศักยภาพ การปฏิบัติจริง ประชาชนตระหนักรู้สูง (สงคราม)	มีการพัฒนาศักยภาพ การปฏิบัติจริง ประชาชนตระหนักรู้สูง (สงคราม)	มีการพัฒนาศักยภาพซ้อมรับมือและตอบโต้แต่การสร้างการรับรู้ให้กับประชาชนค่อนข้างน้อย
ความร่วมมือ	ทำงานร่วมกับหน่วยงานความมั่นคง และภาคเอกชน สื่อมวลชน ผู้ให้บริการโทรคมนาคม รวมถึงกลุ่มแฮกติวิสต์	การทำงานร่วมกับหน่วยงานความมั่นคง และได้รับการสนับสนุนจากสหภาพยุโรป สหรัฐ รวมถึงแฮกติวิสต์	การทำงานร่วมกับสถาบันการศึกษาและหน่วยงานความมั่นคง มีความร่วมมือกับสหรัฐ	การทำงานร่วมกับและหน่วยงานความมั่นคง ความร่วมมือกับเอกชนเฉพาะมีความร่วมมือกับอาเซียน สหรัฐ ญี่ปุ่น เกาหลีใต้

จากการวิเคราะห์พบว่า ประเทศไทยมีโอกาสในการสามารถพัฒนาขีดความสามารถในการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น เช่น การพัฒนาด้านการป้องกันภัยทางไซเบอร์ในแง่มุมของรัฐบาล ทั้งการบูรณาการทำงานระหว่างหน่วยงานที่เกี่ยวข้องทั้งในภาครัฐ หน่วยงานความมั่นคง และสถาบันการศึกษาและวิจัย รวมถึงภาคเอกชน เช่น บริษัทความปลอดภัยทางไซเบอร์ การพัฒนาระบบการป้องกันภัยทางไซเบอร์ของประเทศไทยเอง การวางแผน

ป้องกันรวมถึงการฝึกซ้อมการป้องกันภัยทางไซเบอร์ร่วมกันระหว่างหน่วยงานโครงสร้างพื้นฐานของประเทศทั้งหมด การขยายขอบเขตการป้องกันภัยคุกคามและการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทยไปยังหน่วยงานภาครัฐที่ไม่ได้ระบุใน CII ไม่เฉพาะเพียงหน่วยงานที่กำหนด เนื่องจากการโจมตีทางไซเบอร์ในภาคเอกชนก็ส่งผลทางเศรษฐกิจและสังคมเช่นกัน อย่างไรก็ดี การสร้างความตระหนักรู้เกี่ยวกับการป้องกันภัยทางไซเบอร์ให้กับประชาชนเป็นอีกปัจจัยในการขับเคลื่อน ทั้งการร่วมมือกับสถาบันการศึกษา และสื่อมวลชนในการเผยแพร่ข่าวสารอันเป็นภัยคุกคามที่ส่งผลกระทบรุนแรง ถือเป็นมาตรการเชิงรุกและช่วยเพิ่มประสิทธิผลในการป้องกันภัยคุกคามทางไซเบอร์

ประเด็นสำคัญคือ อธิปไตยทางไซเบอร์ ซึ่งรัฐบาลควรให้ความสำคัญเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางดิจิทัล แพลตฟอร์มรวมถึงระบบข้อมูลออนไลน์ เพื่อให้ผู้ใช้ประโยชน์และผู้ให้บริการข้ามพรมแดนอยู่ภายใต้กฎหมายการควบคุมของรัฐไทยโดยปราศจากการแทรกแซงจากภายนอก อธิปไตยทางไซเบอร์ (Cyber sovereignty) เป็นปัจจัยที่บ่งชี้ได้ว่าประเทศมีความมั่นคงและสามารถจัดการรับมือจากภัยคุกคามไซเบอร์ โครงสร้างพื้นฐานสำคัญทางดิจิทัล แพลตฟอร์มรวมถึงระบบข้อมูลออนไลน์ เฉพาะอย่างยิ่งบริบทบริการไร้พรมแดน เช่น แพลตฟอร์มคลาวด์ แพลตฟอร์มออนไลน์ ภายใต้อธิปไตยทางไซเบอร์เมื่อพิจารณาในแง่อธิปไตยทางอินเตอร์เน็ต (Internet sovereignty) ซึ่งเป็นองค์ประกอบหนึ่งของอธิปไตยทางไซเบอร์ รัฐบาลไทยยังไม่มีอำนาจจัดการได้ เทียบกับประเทศรัสเซียที่สามารถแยกระบบอินเทอร์เน็ตออกจากอินเทอร์เน็ตสากลทำให้สามารถควบคุมแพลตฟอร์ม ข้อมูล และการใช้งานอินเตอร์เน็ตภายในพรมแดนของประเทศตนเองได้ (Hong & Goodnight, 2022) อย่างไรก็ตาม การตีความเกี่ยวกับอธิปไตยทางอินเตอร์เน็ตขัดแย้งกับแนวคิดของฝั่งตะวันตก เช่น สหภาพยุโรปที่ประกาศนโยบายอธิปไตยทางดิจิทัล (Digital sovereignty) เน้นที่โครงสร้างพื้นฐาน เทคโนโลยี และแพลตฟอร์มมากกว่าการควบคุมเนื้อหาหรือการไหลของข้อมูลเพื่อสร้างอธิปไตยทางอินเตอร์เน็ต ซึ่งมักเกี่ยวข้องกับระบอบเผด็จการ (Litvinenko, 2021; Glasze, et al., 2023; Chander & Sun, 2022) ปัจจุบันประเทศไทยยังไม่มีกฎหมายครอบคลุมการให้บริการจากต่างประเทศ ทั้งนี้ หากมีการกำหนดให้ผู้บริการต่างชาติที่ส่งผลต่อโครงสร้างพื้นฐานที่สำคัญของประเทศว่าจะต้องมีหน่วยงานหรือผู้แทนในไทย และอยู่ภายใต้กฎหมายการควบคุมของรัฐไทย เช่น การกำหนดว่าข้อมูลของพลเมืองให้ถูกเก็บ ประมวลผล และใช้งานภายในประเทศ การควบคุมเครือข่ายอินเทอร์เน็ต ระบบโทรคมนาคม และศูนย์ข้อมูลที่สำคัญภายในประเทศ การกำหนดว่าเนื้อหาใดที่เหมาะสมหรือไม่เหมาะสมสำหรับพลเมืองของตน จะช่วยให้รัฐสามารถจัดการภัยคุกคามทางไซเบอร์และปกครองพื้นที่ไซเบอร์ (Cyberspace) ภายในประเทศได้อย่างอิสระ อย่างไรก็ตาม ประเด็นดังกล่าวเป็นประเด็นที่ละเอียดอ่อน โดยจำเป็นต้องศึกษาความสมดุลระหว่างอธิปไตยทางไซเบอร์ของประเทศ และสิทธิเสรีภาพในการแสดงออกของประชาชน รวมถึงการละเมิดความเป็นส่วนตัว ดังนั้น การดำเนินการที่เกี่ยวข้องกับ

อธิปไตยทางไซเบอร์สำหรับประเทศไทยต้องพิจารณาอย่างรอบคอบ โดยจำเป็นต้องศึกษาวิจัยต่อยอดในอนาคตเกี่ยวกับรูปแบบของอธิปไตยทางไซเบอร์ที่เหมาะสมและผลกระทบที่เกิดกับประชาชน

สรุป

ท่ามกลางความขัดแย้งในยุคดิจิทัล มีการใช้การโจมตีทางไซเบอร์เพื่อสร้างความได้เปรียบในสงคราม จากกรณีศึกษาสงครามรัสเซีย–ยูเครน และสงครามฮามาส พบว่า การโจมตีทางไซเบอร์เป็นส่วนหนึ่งของกลยุทธ์ในการโจมตีศัตรู และเมื่อมีการโจมตีทางไซเบอร์ในรูปแบบใหม่ๆ รูปแบบการตอบสนองต่อการโจมตีจะต้องมีการปรับเปลี่ยนอย่างต่อเนื่อง ดังนั้น กรณีศึกษาของประเทศที่เผชิญหน้ากับภัยคุกคามทางไซเบอร์ที่รุนแรง มีรูปแบบการโจมตีที่หลากหลาย สามารถนำมาใช้เป็นแนวทางในการกำหนดกรอบการรับมือการโจมตีทางไซเบอร์ในระดับประเทศทั้งเชิงรุกและเชิงรับ

การเปรียบเทียบจากกรณีศึกษาใน 5 มิติ พบว่าประเทศไทย มีกฎหมายหลักและกฎหมายอื่น ๆ ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ รวมถึงหน่วยงานหลักที่รับผิดชอบเกี่ยวกับความมั่นคงทางไซเบอร์ เช่นเดียวกับรัสเซีย ยูเครน ในขณะที่อิสราเอลไม่มีกฎหมายหลัก แต่มีการใช้กฎหมายที่เกี่ยวข้องหลายฉบับในการรับมือกับภัยคุกคามทางไซเบอร์ ส่วนความสามารถทางเทคนิค พบว่ารัสเซียและอิสราเอลมีการพัฒนาระบบที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ในประเทศ ในขณะที่ยูเครนได้รับการสนับสนุนจากสหภาพยุโรป ในขณะที่ระบบที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ของประเทศไทยล้วนมาจากต่างประเทศ ในด้านหน่วยงานและการจัดการที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์นั้น ทั้งรัสเซีย ยูเครน และอิสราเอล ล้วนมีการกำหนดนโยบายและกลยุทธ์ด้านความมั่นคงทางไซเบอร์ในระดับประเทศเช่นเดียวกับประเทศไทย อย่างไรก็ตาม ในทางปฏิบัติการดำเนินงานของหน่วยงานยังอยู่ในลักษณะการกำกับดูแล และการดำเนินงานส่วนใหญ่ยังจำกัดอยู่ในกลุ่ม CII ส่วนการพัฒนาศักยภาพ การตระหนักรู้ของประชาชนในประเทศไทยค่อนข้างน้อย ดังแสดงได้จากการนำเสนอข่าวสารเกี่ยวกับการโจมตีทางไซเบอร์ที่เกิดขึ้นในประเทศไทย หรือความเสี่ยงในการถูกโจมตีทางไซเบอร์ จากการค้นหาข้อมูลออนไลน์พบว่าการนำเสนอข่าวที่เกี่ยวข้องอยู่ในวงจำกัดเฉพาะด้านเทคโนโลยีและความปลอดภัยทางไซเบอร์ ถึงแม้จะมีการพัฒนาศักยภาพบุคลากรด้านความปลอดภัยทางไซเบอร์อย่างต่อเนื่องแต่ก็ยังคงมีจำนวนจำกัด เนื่องจากหน่วยงานส่วนใหญ่ใช้บริการที่ปรึกษาจากภายนอก ยิ่งไปกว่านั้น ความร่วมมือ ประเทศไทยสามารถพัฒนาการบูรณาการร่วมกันเพิ่มเติมเมื่อเปรียบเทียบกับกรณีศึกษาซึ่งมีความร่วมมือกันระหว่างหน่วยงานภายในที่เกี่ยวข้องทั้งภาครัฐและเอกชนอย่างใกล้ชิด รวมถึงความร่วมมือกันระหว่างประเทศ เช่น ยูเครนที่มีความร่วมมือกับสหภาพยุโรปและนาโต้ รัสเซียมีการฝึกซ้อมเตรียมรับมือการโจมตีทางไซเบอร์ร่วมกันเป็นประจำ อิสราเอลจัดตั้ง CyberSpark ซึ่งเชื่อมโยงบริษัทสตาร์ทอัพ บริษัทระดับโลก สถาบันการศึกษา และศูนย์ความปลอดภัยทางไซเบอร์ทั้งของพลเรือนและทหารไว้ด้วยกัน ประเทศไทยควรให้ความสำคัญในการบูรณาการเพื่อพัฒนาขีดความสามารถในหลายมิติ เช่น การขยายความร่วมมือไปยังหน่วยงานอื่น ๆ

ทั้งภาครัฐ เอกชน และสถาบันการศึกษา รวมถึงการสร้างความตระหนักรู้เกี่ยวกับการป้องกันภัยทางไซเบอร์ให้กับประชาชนใน นอกจากนี้ รัฐบาลจำเป็นต้องสร้างอธิปไตยทางไซเบอร์เหนือโครงสร้างพื้นฐานสำคัญทางดิจิทัล แพลตฟอร์มรวมถึงระบบข้อมูลออนไลน์ เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม และสามารถลดการพึ่งพาจากต่างประเทศได้

References

Amazon Web Services. (2022, June 9). *Safeguarding Ukraine's data to preserve its present and build its future*. https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

Al Mayadeen English. (2025, June 15). *Cyber attacks on 'Israel' surge 700% after strikes on Iran*. https://english.almayadeen.net/news/politics/cyber-attacks-on--israel--surge-700--after-strikes-on-iran

Bandouil, S. (2025, March 28). *Parliament passes bill enhancing Ukraine's cybersecurity defense strategy*. The Kyiv Independent. https://kyivindependent.com/parliament-passes-bill-enhancing-ukraines-cybersecurity-defense-strategy/?utm_source=chatgpt.com

Bangkok Post. (2024, June 1). *Cyber attack surge plunges Thailand into security crisis*. https://www.bangkokpost.com/business/general/2963743/cyber-attack-surge-plunges-thailand-into-security-crisis

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

Bowen, A. S. (2022, February 2). *In focus: Russian cyber units (CRS Report No. IF11718).* Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11718

Chander, A., & Sun, H. (2022). Sovereignty 2.0. *Vand. J. Transnat'l L., 55*, 283. https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=2748&context=vjtl

Cyfirma. (2024, February 15). *The changing cyber threat landscape in Southeast Asia*. https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-southeast-asia-2/

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

English, G. (2024, December 31). *Hamas spied on Israel for seven years using security cameras & even a kindergarten, before Oct 7 massacre, seized docs show*. The Sun. https://www.thesun.co.uk/news/32546190/hamas-spied-israel-years-security-cameras-october-7/

ForumSPB. (2023). *International cyber championship to test defense against state-scale cyberattacks on National Cyber Range platform*. https://forumspb.com/en/news/news/na-mezhdunarodnom-kiberchempionate-v-ramkah-pmef-2023-na-platforme-natsionalnogo-kiberpoligona-otrabotajut-otrazhenie-kiberatak-gosudarstvennogo-masshtaba/

Foundation for Defense of Democracies. (2023, October 11). *Washington Provides Cyber Support to Israel.* https://www.fdd.org/analysis/2023/10/11/washington-provides-cyber-support-to-israel/

Freedom House. (2023). *Freedom on the Net 2023: Russia*. https://freedomhouse.org/country/russia/freedom-net/2023

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

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://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-2ac92738-4d5a-40b3-a48d-d3175455bc0b/c/2-2016_hajduk.pdf

Handler, S. (2022, November 7). *The cyber strategy and operations of Hamas: Green flags and green hats*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats

Hong, Y., & Goodnight, G. T. (2022). How to think about cyber sovereignty: The case of China. In *China's Globalizing Internet* (pp. 7–25). Routledge. https://doi.org/10.1080/17544750.2019.1687536

Israel National Cyber Directorate. (2025, February). *Israel national cybersecurity strategy 2025.* https://www.gov.il/BlobFolder/news/cyber_strategy_2025/he/israel_national_cybersecurity_strategy_feb2025.pdf

IMI. (2025, January 9). *Cyber attacks on Ukraine spiked by 70% in 2024*. https://imi.org.ua/en/news/cyber-attacks-on-ukraine-spiked-by-70-in-2024-i65939

International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index (GCI) 2024*. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Keepnet Labs. (2024, September 11). *171+ cyber security statistics: 2024's updated trends and data.* https://keepnetlabs.com/blog/171-cyber-security-statistics-2024-s-updated-trends-and-data

Litvinenko, A. (2021). Re-defining borders online: Russia's strategic narrative on internet sovereignty. *Media and Communication*, *9*, 5–15. https://www.cogitatiopress.com/mediaandcommunication/article/view/4292/2326

Lowy Institute. (n.d.). *Cyber capabilities*. *Asia Power Index*. https://power.lowyinstitute.org/data/military-capability/signature-capabilities/cyber-capabilities/

Othman, S. N., Jawad, A. M., Hameed, R., Kawad, R. T., & Khlaponin, D. (2025). The impact of cybersecurity law in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, (23), 392-420. https://doi.org/10.5281/zenodo.1429128

Salgado, K. (2024, December 2). *Global cybercrime report 2025: Countries most affected by cybercrime*. Proxyrack. https://www.proxyrack.com/blog/global-cybercrime-report-2025/

Secretariat of the National Cybersecurity Committee (SEC-NIA). (2023, January). *New national cybersecurity operational plan 2023-2027*. https://www.secnia.go.th

Semenchenko, A., Pleskach, V., Zaiarnyi O., & Pleskach, M. (2020). *Cybersecurity of critical infrastructure of Ukraine: Regulatory support and practical aspects [Conference paper].* In Pleskach, V. L. (Ed.), CEUR Workshop Proceedings, 2866, 276–283. http://ceur-ws.org/Vol-2866/ceur_276_283_pleskach.pdf

Thailand National Cyber Academy. (2024, October 18). *NCSA announces Thailand's Cybersecurity achievements, showing leaps and bounds of potential at ASEAN and Japan conferences*. https://www.thnca.or.th/the17th-asean-japan-cybersecurity-policy-meeting/

Voo, Julia. (2025, June 16). *Russia's information confrontation doctrine in practice (2014–Present): Intent, evolution, and implications* (Research Paper). International Institute for Strategic Studies. https://www.iiss.org/research-paper/2025/06/russias-information-confrontation-doctrine-in-practice-2014present-intent-evolution-and-implications/

Voo, J., Hemani, I. & Cassidy, D. (2022). *National Cyber Power Index 2022*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf