การเตรียมความพร้อมของกองทัพไทยต่อภัยคุกคามที่เปลี่ยนแปลง เพื่อต่อสู้กับสงครามไซเบอร์

จาก ยุคอนาล็อก (Analog Age) ที่เป็นจุดเริ่มต้นผลิตภัณฑ์อุปกรณ์อิเล็กทรอนิกส์ เช่น ตัวต้านทาน (Resister) ตัวเก็บประจุ (Capacitor)[1] ที่มีการวิวัฒนาการผลิตภัณฑ์จากหลอดสุญญากาศ (Vacuum Tube) กลายเป็นอุปกรณ์สารกึ่งตัวนำ (Semiconductor) เช่น ไดโอด (Diode) ทรานซิสเตอร์ (Transistor)[2] พลิกโฉมรูปแบบนวัตกรรมเทคโนโลยีสมัยใหม่ที่เรียกว่า วงจรรวม (Integrated Circuit, IC)[3] เข้าสู่ ยุคดิจิทัล (Digital Age) ที่มีการพัฒนาต่อยอดการประยุกต์ใช้งานอุปกรณ์อิเล็กทรอนิกส์ให้มีขนาดเล็กลง และซับซ้อนมากยิ่งขึ้น สามารถจัดเก็บข้อมูลซึ่งมีมากมายมหาศาล[4] เข้าสู่ ยุคสารสนเทศ (Information Age) ที่ช่วยให้มนุษย์มีความสะดวกสบายในการใช้ชีวิตประจำวัน มีการนำเอาระบบอินเทอร์เน็ต (Internet)[5] มาใช้งานในระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information Technology and Communication, ICT) เครือข่ายโทรคมนาคมและการขนส่ง (Telecommunication and Transportation) กลายเป็นส่วนหนึ่งในการดำรงชีวิตและการทำงาน[6] ก้าวเข้าสู่ ยุคโลกาภิวัตน์ (Globalization Age) ที่เป็นโครงข่ายไร้พรมแดน (Borderless Network) เปลี่ยนให้โลกกลายเป็น หมู่บ้านโลก (Global Village)[7] เมื่อประเทศไทยเข้าสู่ ยุคเศรษฐกิจดิจิทัล (Digital Economy Age) มีการใช้งานอินเทอร์เน็ตอย่างแพร่หลาย[8] ระบบเศรษฐกิจและสังคมสามารถติดต่อสื่อสาร โดยอาศัยโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร[9] การทำงานขึ้นอยู่กับเทคโนโลยีหลัก 2 ด้าน คือ (1) เทคโนโลยี SMIC (Social, Mobile, Information และ Cloud) เช่น การใช้งานเว็บไซต์ (Web Site) การรับส่งจดหมายอิเล็กทรอนิกส์ (Electronic Mail, E-Mail) การซื้อขายผ่านทางอินเทอร์เน็ต (Electronic Commerce, E-Commerce) ไปจนถึงการทำธุรกรรมอิเล็กทรอนิกส์ (Electronic Business, E-Business) เป็นต้น[10] และ (2) เทคโนโลยีที่ทุกอุปกรณ์เชื่อมต่อกับอินเทอร์เน็ต (Internet of Thing, IoT) ตั้งแต่อุปกรณ์พื้นฐาน เช่น เครื่องคอมพิวเตอร์, คอมพิวเตอร์พกพา (Notebook), โทรศัพท์เคลื่อนที่อัจฉริยะ (Smart Phone), โทรทัศน์อัจฉริยะ (Smart TV), ตู้เย็นอัจฉริยะ (Smart Fridge) รวมถึงอุปกรณ์ที่สวมใส่ (Wearable Device) เช่น แว่นตาอัจฉริยะ (Google Glass), นาฬิกาอัจฉริยะ (Smart Watch), หรือแม้แต่รองเท้าอัจฉริยะ (Smart Shoe) ก็สามารถเชื่อมต่อ

กับเครือข่ายอินเทอร์เน็ต[11, 12] เมื่อมีการพัฒนาการเชื่อมต่อกล้องวงจรปิดอัจฉริยะ (Smart Closed Circuit TeleVision, CCTV) เข้ากับทุกระบบที่หลากหลายประสานการทำงานเข้าด้วยกัน สามารถบริหารจัดการผ่านคอมพิวเตอร์ หรือ มือถือได้ง่าย ทำให้เข้าสู่วิถีชีวิตสมัยใหม่ (Smart Life) โดยที่พักอาศัยมีความปลอดภัยกลายเป็นบ้านอัจฉริยะ (Smart Home) เชื่อมโยงที่พักอาศัยเป็นเมืองอัจฉริยะ (Smart City)[13] สอดประสานกับอุตสาหกรรมแห่งอนาคตใน ยุคอุตสาหกรรม 4.0 (Industry 4.0) ที่พัฒนาอย่างต่อเนื่องในรูปแบบการทำงานอย่างชาญฉลาด โดยนำเอาเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ความเป็นจริงเสมือน (Virtual Reality, VR) มาผสมผสานเชื่อมโยงเข้ากับระบบอุตสาหกรรมที่หลากหลาย เช่น เครื่องจักรกล และชิ้นส่วนอุปกรณ์ที่ใช้ในงานอุตสาหกรรม[14] เรียกระบบนี้ว่า ระบบงานที่รวมการทำงานในโลกไซเบอร์ (Cyber-Physical-System, CPS)[15] ประกอบด้วย (1) ระบบงานบนอุปกรณ์ที่ทำงานในโลกไซเบอร์ (Cyber on Devices) เช่น ระบบเทคโนโลยีที่ทุกอุปกรณ์เชื่อมต่อกับอินเทอร์เน็ต ตัวอย่างเช่น อุปกรณ์การระบุเอกลักษณ์ด้วยคลื่นวิทยุ (Radio Frequency Identification, RFID), รหัสคิวอาร์ (Quick Response, QR code), การส่งข้อมูลระยะสั้น (Beacon), อุปกรณ์ตรวจจับสัญญาณ (Sensors) และ (2) ระบบงานบนกลุ่มเมฆที่ทำงานในโลกไซเบอร์ (Cyber in Cloud) เช่น ระบบการประมวลผลเป็นกลุ่มเมฆ (Cloud Computing) สำหรับการจัดการกับข้อมูลขนาดใหญ่ (Big Data) เพื่อให้ตัดสินใจในการทำงานได้อย่างรวดเร็ว ถูกต้อง แม่นยำ และทันเวลา ในรูปแบบการจัดการด้วยมนุษย์ (Human) และปัญญาประดิษฐ์ (Artificial Intelligence, AI) แบบระบบหุ่นยนต์อัตโนมัติ (Autonomous Robots) ตลอดจนนำห่วงโซ่คุณค่า (Value Chain) เข้ามาใช้ในสายการผลิต มีแหล่งพลังงานที่หลากหลายหล่อเลี้ยงทั้งระบบที่เรียกว่า โครงข่ายไฟฟ้าอัจฉริยะ (Smart Grid)[16] การดำเนินการทั้งปวงขึ้นอยู่กับระบบโครงสร้างพื้นฐานสารสนเทศสำคัญ (Critical Information Infrastructure, CII)[17] ที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ซึ่งจะเป็นกลไกหลักในการสนับสนุนการทำงานระบบโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure, CI) เช่น ระบบไฟฟ้า ระบบน้ำประปา ระบบการชลประทาน ระบบขนส่งมวลชน ระบบบริการสาธารณสุข ระบบบริการการเงิน และระบบสื่อสารโทรคมนาคม[18] ทั้งนี้มุ่งประสงค์เพื่อส่งเสริมความสัมพันธ์ทางด้านพลังอำนาจแห่งชาติ (National Power) ด้านความมั่นคงที่เรียกว่า ปัจจัยสภาพแวดล้อมในการปฏิบัติการ (PMESII-PT) ประกอบด้วย การเมือง (Political) การทหาร (Military) เศรษฐกิจ (Economic) สังคมที่อยู่ในสภาพแวดล้อม (Sociology)

โครงสร้างพื้นฐาน (Infrastructure) สารสนเทศ (Information) สภาวะแวดล้อมทางกายภาพ (Physical Environment) และ เวลา (Time) ให้ทำงานประสานสอดคล้องเชื่อมโยงระหว่างปัจเจกบุคคล ชุมชน ภาคเอกชน และภาครัฐ[19] ซึ่งรัฐบาลภายใต้การนำของ พลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) เล็งเห็นความสำคัญจึงขับเคลื่อนการปฏิรูปประเทศทั้งระบบเข้าสู่ ยุคไทยแลนด์ 4.0 (Thailand 4.0) เพื่อปรับแก้จัดระบบ ปรับทิศทาง และสร้างหนทางพัฒนาประเทศให้เจริญตาม ยุทธศาสตร์ชาติ 20 ปี พ.ศ.2560-2579 ที่เน้นการผนึกกำลังของทุกภาคส่วน ภายใต้แนวคิด “ประชารัฐ (Civil State)” เพื่อให้สามารถรับมือภัยคุกคาม (Threat) รูปแบบใหม่ที่เปลี่ยนแปลงอย่างรวดเร็วในศตวรรษที่ 21 ได้ ตามวิสัยทัศน์ของรัฐบาลที่กล่าวว่า “มั่นคง มั่งคั่ง และยั่งยืน”[20]

ไซเบอร์ ใช้นำหน้าคำอื่นเพื่อสื่อความหมายที่เกี่ยวข้องกับคอมพิวเตอร์ หรืออิเล็กทรอนิกส์[21] โดยมี มิติไซเบอร์ (Cyberspace) เป็นที่ว่าง หรือห้วงอวกาศที่สร้างขึ้นด้วยระบบอิเล็กทรอนิกส์เพื่อใช้สื่อสารติดต่อกัน[22] อาจกล่าวได้ว่าเป็นการกระทำทุกอย่างบนแถบความถี่แม่เหล็กไฟฟ้า (Electromagnetic Spectrum, EMS) ครอบคลุมขอบเขตการทำงานของระบบเครือข่ายคอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์ระยะไกล เพื่อให้สามารถติอต่อกันได้ทั่วโลก[23]

ข้อมูลหรือสารสนเทศขององค์กรเป็นข้อมูลที่มีความสำคัญ (Sensitive Data) จัดเก็บในลักษณะข้อมูลขนาดใหญ่ในเครื่องผู้ให้บริการ (Server) หรือบนกลุ่มเมฆที่เชื่อมต่อกับอินเทอร์เน็ต สามารถเข้าถึงข้อมูลได้ง่าย สะดวก รวดเร็ว ในแบบทุกที่ทุกเวลาและทุกอุปกรณ์ (Anytime Anywhere and Any device) ทำให้มีความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Threat) ต่อองค์กร ทั้งจากภัยคุกคามภายใน (Insider Threat) และภัยคุกคามภายนอก (Outsider Threat)[24] ที่มีการโจมตีทางไซเบอร์ (Cyber Attack) ต่อเป้าหมายที่หลากหลายและซับซ้อนตามโครงสร้างพื้นฐานสำคัญที่เปลี่ยนแปลง จากการก่ออาชญากรรมทางไซเบอร์ (Cyber Crime) พัฒนาเป็นการจารกรรมทางไซเบอร์ (Cyber Espionage) การก่อวินาศกรรมทางไซเบอร์ (Cyber Sabotage) ท้ายสุดกลายเป็นการโจมตีในแบบรัฐต่อรัฐ (State-to-State Attack) โดยหาช่องโหว่ (Vulnerability) ของระบบ เพื่อโจมตีโครงสร้างพื้นฐานสำคัญให้หยุดการทำงานหรือทำงานผิดพลาด ก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศในวงกว้าง[25]

ภัยคุกคามทางไซเบอร์ เป็นภัยคุกคามผสมที่ซับซ้อนในเศรษฐกิจ สังคม การเมือง และการทหาร มาจากที่ใดก็ได้ในโลก ผ่านวงจรการสื่อสารที่เชื่อมต่ออินเทอร์เน็ต แบบมีสาย (Wire) และไร้สาย (Wireless) มุ่งโจมตีระบบคอมพิวเตอร์ที่ควบคุมโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union, ITU) จัดอันดับประเทศเสี่ยงต่อภัยคุกคามทางไซเบอร์ของโลก พบว่าประเทศไทยมีความเสี่ยงสูงอยู่ในลำดับที่ 15 จาก 165 ประเทศทั่วโลก (สำรวจเมื่อ 4 ส.ค.2560)[26]

การโจมตีทางไซเบอร์ที่กระทำผ่านช่องโหว่ ของ ระบบปฏิบัติการ (Operating System, OS) โปรแกรมสืบค้น (Browser) และโปรแกรมประยุกต์ (Application) ต่าง ๆ หรือการใช้โปรแกรมประสงค์ร้าย (Malicious Software, Malware) ที่พัฒนาการโจมตีตลอดเวลา การโจมตีที่พบมากมี 3 รูปแบบ คือ การจารกรรมข้อมูล โดยนักเจาะระบบ (Hacker) อาศัยช่องโหว่ของระบบรักษาความปลอดภัยเพื่อเข้าถึงข้อมูลของเป้าหมาย[27] การทำลายชื่อเสียง (Destroy Reputation) หรือการปล่อยข้อมูลลวง (Propaganda) จากการเจาะระบบฐานข้อมูลในศูนย์ข้อมูล เพื่อเข้าถึงหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลหรือองค์กร เพื่อนำไปใช้ทำลายภาพลักษณ์ ชื่อเสียง ความน่าเชื่อถือของหน่วยงาน หรือสร้างความแตกแยกในสังคม[28] และการก่อวินาศกรรมทางไซเบอร์ ที่ในอดีตระบบควบคุมโครงสร้างพื้นฐานสำคัญเป็นแบบสวิตซ์และเครื่องจักรกล สามารถป้องกันการโจมตีทางไซเบอร์ได้ แต่ปัจจุบันระบบควบคุมฯ สามารถออนไลน์ (Online) ผ่านอินเทอร์เน็ต เกิดช่องโหว่ในการป้องกัน ผู้โจมตีสามารถส่งรหัสคอมพิวเตอร์ในแบบของไวรัสหรือโปรแกรมประสงค์ร้าย เช่น Stuxnet เพื่อควบคุมโครงข่ายไฟฟ้ากำลัง (Electrical Power Grid) ที่เชื่อมกับระบบควบคุมอุตสาหกรรม (Industrial Control System, ICS) โดยหยุดการทำงานของเครื่องกำเนิดไฟฟ้าที่เชื่อมกับโครงข่ายไฟฟ้ากำลังได้ในเวลาไม่ถึงนาที[29, 30]

การโจมตีทางไซเบอร์ที่กระทำผ่านทุกอุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ต เพื่อควบคุมอุปกรณ์และทำให้อุปกรณ์นั้นระเบิด คล้ายกับการโจมตีด้วยแรงระเบิด และอาวุธทางกายภาพที่เคลื่อนที่ได้ เช่น ยานยนต์สมัยใหม่ที่มีคอมพิวเตอร์เป็นส่วนประกอบเชื่อมต่อกับอินเทอร์เน็ต สามารถถูกโจมตีโดยโปรแกรมประสงค์ร้าย ส่งรหัสควบคุมไปยังระบบเบรค คันเร่ง ถุงลมนิรภัย การล็อคประตู และระบบไฟ ซึ่งรถยนต์รุ่นเดียวกันสามารถเชื่อมต่อผ่านอินเทอร์เน็ต

ถึงกัน เพิ่มโอกาสโจมตีมากขึ้น[31] อุปกรณ์อำนวยความสะดวกในที่พักอาศัย หรือภาคอุตสาหกรรม มีระบบสมองกลฝังตัว (Embedded System) ควบคุมติดตั้งอยู่ภายใน โดยเชื่อมต่อผ่านอินเทอร์เน็ตไร้สาย สามารถควบคุมจากระยะไกล สุ่มเสี่ยงต่อการถูกใช้โจมตี[32]

การโจมตีทางไซเบอร์ต่อความมั่นคงของประเทศที่พบมาก คือ โปรแกรมประสงค์ร้ายแฝงตัวมาในรูปแบบต่าง ๆ ผ่านทางอินเตอร์เน็ต[33] การปลอมทางอิเล็กทรอนิกส์ (Phishing) เพื่อหลอกให้เป้าหมายกดปุ่มติดตั้งโปรแกรมประสงค์ร้าย[34] การส่งคำสั่ง SQL (Sequential Query Language) ผ่านทาง Web Application เพื่อเข้าถึงฐานข้อมูล (SQL Injection Attack) เน้นที่เว็บไซต์และเครื่องให้บริการ[35] การส่งคำสั่งสคริปข้ามเว็บไซต์ (Cross-Site Scripting, XSS) โดยใส่รหัสคำสั่งอันตรายลงในช่องที่ผู้ใช้งานเว็บไซต์จะต้องเปิด[36] การโจมตีโดยปฏิเสธการให้บริการ (Denial of Service, DoS) ทำให้เครื่องหรือทรัพยากรเครือข่ายของเป้าหมายใช้บริการไม่ได้อย่างชั่วคราวหรือถาวร[37] การใช้รหัสผ่านซ้ำ ๆ (Credential Reuse) ผู้ใช้ที่ใช้รหัสผ่านซ้ำกันสำหรับการเข้าระบบทั้งหมด เมื่อผู้โจมตีได้รหัสผ่านจะสามารถเข้าถึงระบบทั้งหมดได้[38] และภัยคุกคามแบบต่อเนื่องขั้นสูงโดยโจมตีแบบเจาะจงเป้าหมาย (Advanced Persistent Threat, APT) เจาะระบบความปลอดภัย และซ่อนตัวอยู่นาน คอยนำข้อมูลที่มีค่าทยอยออกมา หรือการสร้างความเสียหาย โดยหน่วยงานที่ทำธุรกรรมด้วยจะเป็นกลุ่มที่เป็นเป้าหมาย[39]

การนำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security, InfoSec) มาใช้ในการป้องกันระบบสารสนเทศจากการเข้าถึง การใช้ การเปิดเผยสู่สาธารณะ การขัดขวาง การปรับเปลี่ยน การอ่าน การตรวจสอบการบันทึก หรือการทำลายที่ไม่ได้รับอนุญาต เพื่อให้ข้อมูลมีการรักษาความลับ (Confidentiality) อยู่ในสภาพพร้อมใช้งาน (Availability) มีบูรณภาพ (Integrity) ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)[40, 41] เพื่อปกป้องระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทรัพย์สิน รวมถึงผลประโยชน์ขององค์กร[42]

ปัญหาการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย เกิดจากหน่วยงานไม่ให้ความสำคัญกับภัยคุกคามไซเบอร์ ขาดการรวมกลุ่มจัดตั้งทีมเฝ้าระวัง ไม่มีการระบุโครงสร้างพื้นฐานสำคัญของชาติอย่างชัดเจน เมื่อเกิดการโจมตีทางไซเบอร์ องค์กรเอกชนมักจะปกปิด เนื่องจากกลัวเสียชื่อเสียง ยังไม่มีกฎหมายสนับสนุนการดำเนินงานด้านภัยคุกคามไซเบอร์ที่ครอบคลุม เกิดการทับซ้อนการดำเนินการรักษาความปลอดภัยไซเบอร์ที่ต่างฝ่ายต่างทำงาน ขาดการสนับสนุนการวิจัยและพัฒนาเทคโนโลยีการรักษาความปลอดภัยไซเบอร์จากภาครัฐ ขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์ ที่สำคัญ หน่วยงานภาครัฐ เอกชน และประชาชน ขาดความตระหนักรู้ด้านภัยคุกคามไซเบอร์[43]

การเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย ภาครัฐควรกำหนดโครงสร้างพื้นฐานสำคัญและนโยบายคุ้มครองโครงสร้างพื้นฐานสำคัญของชาติ ในกรอบการดำเนินการที่ชัดเจน กระตุ้นองค์กรภาครัฐและเอกชนนำมาตรฐาน ISO/IEC 27001: 2005 เพื่อการป้องกันโครงสร้างสารสนเทศพื้นฐานของประเทศ (Critical Information Infrastructure Protection, CIIP)[44] มาใช้ให้มากขึ้น นำระดับความปลอดภัยทางไซเบอร์ของ สหภาพโทรคมนาคมระหว่างประเทศ มาเป็นแนวทางปฏิบัติ ครอบคลุมหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทั้งภาครัฐและเอกชน เน้นความไว้วางใจเป็นหัวใจของการประสานและดำเนินการร่วม โดยรัฐสร้างบรรยากาศความไว้วางใจให้แก่หน่วยงานในประเทศและต่างประเทศ เพิ่มบุคลากรด้านความปลอดภัยไซเบอร์ให้เพียงพอกับความต้องการภายในประเทศ สุดท้ายการสร้างความตระหนักรู้ให้กับทุกภาคส่วน[45]

นโยบายของรัฐบาลที่ต้องการเปลี่ยนเศรษฐกิจแบบเดิมเพื่อไปสู่การใช้นวัตกรรมเพื่อขับเคลื่อนเศรษฐกิจภายใต้ ยุทธศาสตร์ไทยแลนด์ 4.0 พบว่าการเข้าสู่ยุคดิจิทัลเป็นการเพิ่มสาเหตุของอาชญากรรมไซเบอร์ที่พัฒนาไปสู่สงครามไซเบอร์ (Cyber Warfare, CW)

วัตถุประสงค์ในการทำวิจัย เพื่อเตรียมกำลังพล (People) กระบวนการทำงาน (Process) เทคโนโลยียุทโธปกรณ์ทางไซเบอร์ (Technology) สำหรับเตรียมความพร้อมรับมือภัยคุกคามในมิติต่าง ๆ ของกองทัพไทย (ทท.) ต่อภัยคุกคามที่เปลี่ยนแปลงเพื่อต่อสู้กับสงครามไซเบอร์

สงครามไซเบอร์ นิยามโดย ริชาร์ด เอ. คลาร์ก (Richard A. Clarke) ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยของรัฐบาลสหรัฐอเมริกา หมายถึง การที่รัฐหรือชาติใดก็ตาม ได้ทำการแทรกซึมเข้าไปยังเครือข่าย หรือระบบคอมพิวเตอร์ของเป้าหมาย เพื่อหวังทำลายหรือสร้างความแตกแยกโดยใช้อาวุธทางอิเล็กทรอนิกส์เป็นเครื่องมือทำลาย หรือขโมยข้อมูลอีกฝ่าย ถือว่าอันตรายอย่างยิ่งต่อปฏิบัติการทางทหาร ทั้งทางภาคพื้นดิน อากาศ และทะเล[46]

สงครามไซเบอร์ เป็นภัยคุกคามนอกแบบ (Non-Traditional Threats) และสงครามอสมมาตร (Asymmetric Warfare, AW) ผู้ก่อการร้ายอาจเป็นเพียงคนคนเดียวแต่มีความสามารถในการเข้าถึงอินเทอร์เน็ต เข้าโจมตีผ่านทางมิติไซเบอร์ได้[47] ในปี พ.ศ.2552 บารัค โอบามา ประธานาธิบดีสหรัฐอเมริกา ประกาศว่า ระบบพื้นฐานดิจิทัลของสหรัฐฯ เป็น “สินทรัพย์ทางยุทธศาสตร์ของชาติ” ในปีถัดมา กระทรวงกลาโหมของสหรัฐอเมริกา ได้จัดตั้ง กองบัญชาการไซเบอร์ (United States CYBER COMmand, USCYBERCOM) เพื่อใช้ป้องกันเครือข่ายทางทหารของสหรัฐ และจู่โจมตอบกลับต่อระบบของประเทศคู่กรณี ภายใต้การควบคุมของผู้บริหารสภาความมั่นคงแห่งชาติสหรัฐ มุ่งป้องกันการโจรกรรมข้อมูลทางเศรษฐกิจและจับกุมผู้เข้าร่วมกระบวนการของนักเจาะระบบ โดยแบ่งเป็นหน่วยระดับชาติ หน่วยโจมตี และหน่วยป้องกัน[48]

การเตรียมความพร้อมของประเทศไทยต่อภัยคุกคามทางไซเบอร์ จากที่ไทยถูกจัดเป็นประเทศที่ถูกโจมตีทางไซเบอร์อันดับที่ 15 ของโลก เป็นสวรรค์ของนักเจาะระบบทั่วโลกเข้ามาทดสอบฝีมือ โดยใช้ช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เพื่อเข้ามาทำลาย หรือขัดขวางการทำงาน โดยโจมตีระบบเครือข่ายคอมพิวเตอร์โครงสร้างพื้นฐานสำคัญ ที่ใช้เป็นเครื่องมือในการขับเคลื่อนการปฏิบัติงานภาครัฐ ภาคเอกชน ตลอดจนคุกคามบุคคลและองค์กร มีผลกระทบต่อความมั่นคงของประเทศ ซึ่งรัฐบาลไทยมีพระราชบัญญัติ (พรบ.) สอบสวนคดีพิเศษ พ.ศ.2547[49] และ พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 และ พ.ศ.2551 ใช้รับรองกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการทำธุรกรรมหรือสัญญาให้มีผลเช่นเดียวกับการทำสัญญาตามหลักเกณฑ์ที่กฎหมายปัจจุบันกำหนดไว้[50] และปรับปรุง พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เป็น พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 (ฉบับใหม่) มีผลบังคับใช้เมื่อวันที่ 23 พฤษภาคม 2560 ครอบคลุมการกระทำความผิดที่มีมากขึ้น[51] นอกจากนี้ นโยบายความมั่นคงแห่งชาติ

พ.ศ.2558-2564 ในส่วนที่ 2 นโยบายความมั่นคงแห่งชาติทั่วไป กล่าวถึงเรื่อง นโยบายที่ 10 การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ และนโยบายที่ 12 การเสริมสร้างความมั่นคงทางพลังงาน[52] และ นโยบายการเตรียมความพร้อมแห่งชาติ ได้กล่าวถึงเรื่อง การบริหารจัดการในการเตรียมความพร้อมด้าน ทรัพยากร การมีส่วนร่วมของทุกภาคส่วน การจัดทำแผนทั้งระบบ อย่างมีเอกภาพ ประสิทธิภาพและทันท่วงทีในทุกสถานการณ์ที่เกิดขึ้น[53]

การเตรียมความพร้อมของกองทัพไทยต่อภัยคุกคามที่เปลี่ยนแปลงเพื่อต่อสู้กับสงครามไซเบอร์ กระทรวงกลาโหม (กห.) ในฐานะหน่วยบังคับบัญชาโดยตรงของ ทท. ประกอบด้วย กองบัญชาการกองทัพไทย (บก.ทท.) และเหล่าทัพ มี กองทัพบก (ทบ.) กองทัพเรือ (ทร.) และ กองทัพอากาศ (ทอ.) ตาม พรบ.การจัดการระเบียบราชการ กห. พ.ศ.2551 กำหนดอำนาจหน้าที่ของ กห. ที่เกี่ยวข้อง คือ พิทักษ์รักษาเอกราชและความมั่นคงแห่งราชอาณาจักรจากภัยคุกคามทั้งภายนอกและภายในราชอาณาจักร ปกป้องสถาบันพระมหากษัตริย์ พิทักษ์รักษาผลประโยชน์แห่งชาติ สนับสนุนภารกิจของรัฐในการพัฒนาประเทศ ศึกษา วิจัย พัฒนาและดำเนินการด้านอุตสาหกรรมป้องกันประเทศและพลังงานทหาร วิทยาศาสตร์และเทคโนโลยีป้องกันประเทศ และกิจการอวกาศ เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อสนับสนุนภารกิจของ กห. และความมั่นคงของประเทศ[54]

ทท. กำหนดอำนาจหน้าที่ของ ทท. ใน พรบ.จัดระเบียบราชการ กห. พ.ศ.2551[55] ประกอบด้วย การเตรียมกำลังของ ทท. เพื่อการป้องกันราชอาณาจักร และการใช้กำลังทหารตามอำนาจหน้าที่ของ กห. โดยมีผู้บัญชาการทหารสูงสุด (ผบ.ทสส.) เป็นผู้บังคับบัญชาสูงสุด ซึ่ง ทท. อาจตั้งคณะกรรมการ อนุกรรมการ หรือบุคคลใด พิจารณาเรื่องที่เกี่ยวกับแผนเพื่อรักษาเอกราชและผลประโยชน์แห่งชาติ รวมทั้งการปฏิบัติการทางทหารของ บก.ทท. เหล่าทัพ และส่วนราชการ ตามที่กำหนดโดยพระราชกฤษฎีกา มี ผบ.ทสส. เป็นผู้บังคับบัญชาให้ บก.ทท. รับผิดชอบการฝึกและศึกษาในระดับยุทธศาสตร์ การปฏิบัติการร่วมของ ทท. และให้เหล่าทัพรับผิดชอบในระดับปฏิบัติการและระดับยุทธวิธี ที่สำคัญให้ บก.ทท. รับผิดชอบการวางแผน พัฒนาและดำเนินการเกี่ยวกับระบบควบคุมบังคับบัญชาของ ทท. ให้เชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในระดับรัฐบาล ระดับกระทรวง และ กห. ได้ สุดท้ายให้ ทท. จัดตั้งศูนย์บัญชาการทางทหาร (ศบท.) ในแต่ละระดับ เพื่อใช้ติดตามสถานการณ์ และ

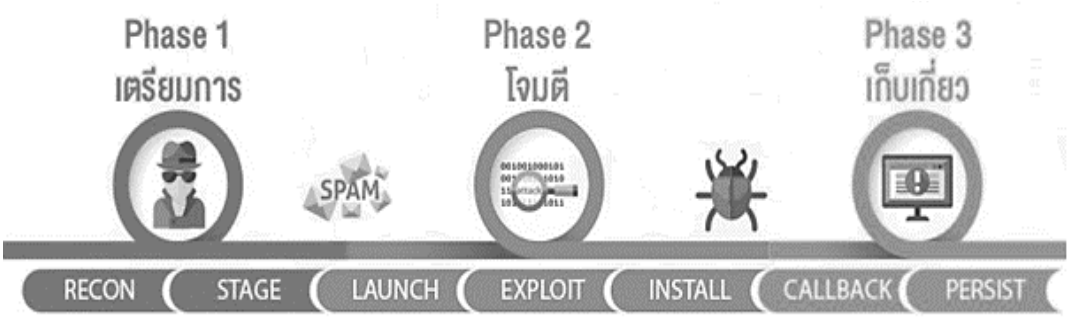
เป็นศูนย์ควบคุม อำนวยการและสั่งการ ให้ ศบท. (บก.ทท.) มีหน้าที่ควบคุม อำนวยการและสั่งการ ศบท. ในแต่ละระดับ (ศบท.เหล่าทัพ) หรือกองกำลังเฉพาะกิจร่วมที่จัดตั้งขึ้นตามแผนป้องกันประเทศ แล้วแต่กรณี

ทท. เป็นหน่วยงานหนึ่งในโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ.2559 ตามประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์[56] ซึ่ง ทท. เป็นหน่วยงานหลักในการป้องกันประเทศ เมื่อการโจมตีทางไซเบอร์ถูกยกระดับเป็นสงครามไซเบอร์แล้ว ทท. ต้องพร้อมรับมือต่อภัยคุกคามทางไซเบอร์ที่พัฒนาวิธีการโจมตีรูปแบบใหม่ที่ซับซ้อน โดยพัฒนา 3 เสาหลัก ที่ประกอบด้วย กำลังพล กระบวนการทำงาน และเทคโนโลยีให้ทันสมัย ทั้ง ไซเบอร์เชิงรับ (Cyber Defensive) และเชิงรุก (Cyber Offensive) ตามมาตรฐานสากล

การปฏิบัติการในมิติไซเบอร์ (Cyber Operation) ของ ทท. ตาม พรบ.จัดระเบียบราชการ กห. พ.ศ.2551 กล่าวว่า การปฏิบัติการในมิติไซเบอร์ของ ทท. เป็นการปฏิบัติการทางทหารอย่างหนึ่ง เพื่อรับมือต่อภัยคุกคามรูปแบบเดิม และรูปแบบใหม่ ที่สอดคล้องกับหน้าที่ของ ทท. ในการเตรียมกำลัง การป้องกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังทหาร ซึ่ง ทท. ต้องใช้พลังอำนาจทางไซเบอร์ตามอำนาจหน้าที่ที่ได้กำหนดไว้ใน พรบ. นี้

การปฏิบัติการในมิติไซเบอร์ สำหรับการทำสงครามไซเบอร์ เพื่อให้สามารถเอาชนะฝ่ายตรงข้ามได้ โดยไม่ต้องสู้รบกันแบบเผชิญหน้าเหมือนในอดีต สนามรบไซเบอร์ (Cyber Battlefield) ในปัจจุบัน ยุทธบริเวณ (Theater of Operations) ของการรบเปลี่ยนไปเป็น สนามรบที่ไร้พรหมแดน (Borderless Battlefield) ที่เรียกว่า มิติไซเบอร์ ที่ซึ่งนักรบไซเบอร์ (Cyber Warrior) สามารถปฏิบัติการได้อิสระทุกที่ที่มีการเชื่อมต่อการสื่อสารเกิดขึ้น เพียงแค่หาวิธีโจมตีต่อเป้าหมายหลัก เช่น ระบบคอมพิวเตอร์และเครือข่าย เครื่องผู้ให้บริการ หรือระบบปฏิบัติการที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งแก่คอมพิวเตอร์ จนเครื่องผู้ให้บริการทำงานหนักมากใช้การไม่ได้ ต้องปิดระบบตัวเองของศูนย์บัญชาการ[57] นักรบไซเบอร์มีทักษะการนำกระบวนการ Cyber Kill Chain ที่นักเจาะระบบนิยมใช้เพื่อโจมตีต่อเป้าหมายมี 3 ขั้นตอนหลัก ขั้นตอนที่ 1 การเตรียมการ ประกอบด้วย การลาดตระเวน (Recon) เก็บรวบรวมข้อมูลของเป้าหมาย

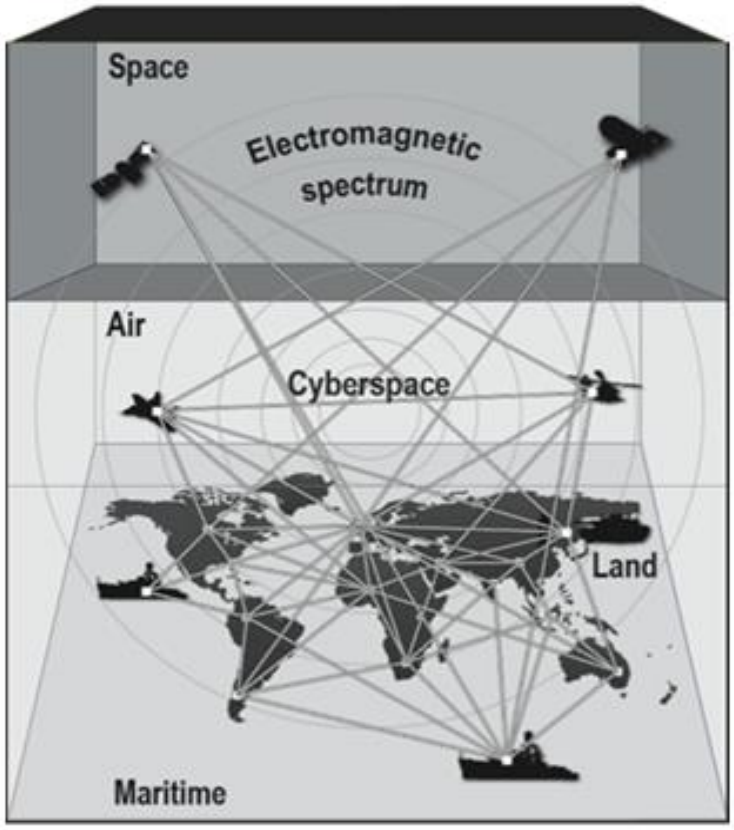
และเตรียมอาวุธสำหรับโจมตี (Stage) โดยหาวิธีเจาะระบบและเตรียมคำสั่งโปรแกรมประสงค์ร้าย (Malicious Payload) เพื่อส่งไปยังเป้าหมาย จากนั้นเข้าสู่ขั้นตอนที่ 2 การโจมตี ประกอบด้วย การส่งคำสั่งโปรแกรมประสงค์ร้าย (Launch) ไปยังเป้าหมายผ่านทางจดหมายอิเล็กทรอนิกส์ เว็บไซต์ หรือ USB (Universal Serial Bus) ที่บรรจุคำสั่ง (Payload) วิธีการโจมตีอยู่ภายใน จากนั้นทำการเจาะระบบ (Exploit) ของเป้าหมายด้วยวิธีต่าง ๆ ตามบรรจุคำสั่งที่ส่งมา และติดตั้งโปรแกรมประสงค์ร้าย (Install) บนเครื่องเป้าหมาย เพื่อคอยรับคำสั่งและกระทำการบางอย่างตามที่ผู้โจมตีต้องการ สุดท้ายขั้นตอนที่ 3 การเก็บเกี่ยว ประกอบด้วย การสร้างช่องทางในการรับส่งคำสั่งกับโปรแกรมประสงค์ร้าย (Callback) เพื่อควบคุมโปรแกรมประสงค์ร้ายให้ทำงานตามความต้องการ และเก็บเกี่ยวผลประโยชน์ตามที่ผู้โจมตีต้องการ (Persist) จากระบบเครือข่ายของเป้าหมาย[58] ปัจจุบันนักเจาะระบบเน้นโจมตีต่อการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operation, NCO) ที่เป็นหัวใจการติดต่อสื่อสารประสานการปฏิบัติของ บก.ทท. และเหล่าทัพ



ภาพที่ 1 ขั้นตอนการเจาะระบบเพื่อโจมตีทางไซเบอร์ (Cyber Kill Chain)[59]

ไซเบอร์ เป็นส่วนหนึ่งของการรบในมิติที่ 5 (Fifth Domain) ถัดจากการรบ ภาคพื้นดิน (Land) ทะเล (Maritime) อากาศ (Air) และ อวกาศ (Space)[60] เป็นการปฏิบัติการของตัวแทนที่เป็นรัฐ (State Actor) ต่อระบบคอมพิวเตอร์ หรือเครือข่ายของอีกชาติหนึ่ง โดยมีวัตถุประสงค์เพื่อทำลายหรือก่อกวนให้ระบบหยุดชะงักไม่สามารถทำงานได้ตามปกติ (Disruption) [61] ซึ่งจะรวมถึงผู้ที่กระทำไม่ใช่รัฐ (Non State Actor) เช่น กลุ่มผู้ก่อการร้าย (Terrorist Group) กลุ่มอุดมการณ์หัวรุนแรง (Ideological Extremist Group), นักเจาะระบบ และองค์กรอาชญากรรมข้ามชาติ (Transnational Crime Organization) ซึ่งหลายประเทศ รวมถึง ทท.

ได้กำหนดให้สงครามไซเบอร์บูรณาการเข้าเป็นส่วนหนึ่งของยุทธศาสตร์ทางทหาร[62] โดย สงครามไซเบอร์ จะเกี่ยวข้องกับ สงครามข่าวสาร (Information Warfare, IW) และสงครามอิเล็กทรอนิกส์ (Electronic Warfare, EW) ที่เป็นส่วนสนับสนุนให้การรบดำเนินกลยุทธ์ฝ่ายเราเหนือกว่าฝ่ายตรงข้าม



ภาพที่ 2 ความสัมพันธ์ระหว่างการปฏิบัติการทางทหารในสนามรบหลายมิติ (Multi-Domain Battle) บนแถบความถี่คลื่นแม่เหล็กไฟฟ้า[63, 64]

สงครามข่าวสาร เน้นการปฏิบัติการข่าวสาร (Information Operation, IO) ในด้าน “ความสามารถในการรวบรวม ดำเนินกรรมวิธี ใช้และกระจายข้อมูลข่าวสารให้สามารถไหลไปได้อย่างต่อเนื่องไม่ติดขัด ช่วงชิงความได้เปรียบ และปิดกั้นไม่ให้ฝ่ายตรงข้ามมีขีดความสามารถดังกล่าวทัดเทียมกับฝ่ายเราได้”[65] การปฏิบัติการข่าวสารเป็นขีดความสามารถที่สนับสนุนการสื่อสารทางยุทธศาสตร์ (Strategic Communication : SC) ของ ทท.[66] บก.ทท. มีส่วนปฏิบัติการข่าวสาร ศูนย์บัญชาการทางทหาร (สปข.ศบท.) ทำหน้าที่วางแผน

และจัดทำแผ่นภาพข้อมูล (Information Graphic, InfoGraphic) เผยแพร่ในสื่อต่าง ๆ เพื่อสร้างภาพพจน์ที่ดี เรียกความเชื่อมั่นศรัทธาของประชาชนที่มีต่อกองทัพและรัฐบาล[67] ในอดีตที่ผ่านมาพบว่าการปฏิบัติการข่าวสารจากการใช้สื่อสังคมออนไลน์ (Social Media) สามารถทำให้หลายประเทศเกิดการเปลี่ยนแปลง เช่น กรณี อาหรับสปริง (Arab Spring) เป็นต้น

สงครามอิเล็กทรอนิกส์ เป็น “การปฏิบัติทางทหารที่เกี่ยวกับการใช้พลังงานคลื่นแม่เหล็กไฟฟ้าเพื่อกำหนดขยายผล ลด หรือ ป้องกันการใช้ย่านความถี่คลื่นแม่เหล็กไฟฟ้าของฝ่ายตรงข้าม และปฏิบัติการซึ่งมุ่งดำรงรักษาการใช้ย่านความถี่คลื่นแม่เหล็กไฟฟ้าของฝ่ายเรา”[68] สามารถแบ่งการทำงานได้ 3 ส่วนหลัก คือ การโจมตีทางอิเล็กทรอนิกส์ (Electronic Attack, EA), การป้องกันทางอิเล็กทรอนิกส์ (Electronic Protection, EP) และการสนับสนุนการสงครามอิเล็กทรอนิกส์ (Electronic Support, ES) โดยจะกระทำการที่เกี่ยวกับการใช้งานแถบคลื่นแม่เหล็กไฟฟ้า ซึ่งเป็นพลังงานที่มีอยู่ทั่วไป แม้ไม่มีตัวตน แต่สามารถรับรู้ผลของงานในรูปของ ความร้อน แสง และเสียง เป็นต้น[69] ฝ่ายใดที่ครองสมรภูมิสงครามอิเล็กทรอนิกส์ได้ อาจกล่าวได้ว่าฝ่ายนั้นเป็นผู้ชนะ เพราะการทำสงครามยุคปัจจุบัน การเชื่อมต่อการสื่อสารทางทหารจะกระทำผ่านระบบอิเล็กทรอนิกส์เป็นหลัก

การปฏิบัติการทางทหารของฝ่ายเรา จะมุ่งโจมตีที่ระบบอิเล็กทรอนิกส์ของฝ่ายตรงข้าม เพื่อไม่ให้ใช้การได้เต็มประสิทธิภาพ และไม่สามารถตรวจจับฝ่ายเราได้ โดยการดักฟังสัญญาณ (Tampering) การก่อกวน (Jamming) การลวง (Deception) รวมไปถึง การทำลายเป้าหมาย (Destructive)[70] เช่น ระบบเรดาร์ (Radio Detection And Ranging, RADAR) ระบบสื่อสาร (Communication) ระบบวิทยุ (Radio) และระบบตรวจจับ (Sensor) ต่าง ๆ[71]

กลับกัน ถ้าฝ่ายตรงข้ามโจมตีทางอิเล็กทรอนิกส์ต่อฝ่ายเรา โดยการเจาะ (Hack) ระบบเรดาร์เพื่อเข้าถึงและควบคุมระบบอาวุธป้องกันภัยทางอากาศ (Air Defense Weapon) แบบพื้นสู่อากาศ (Surface to Air) หรืออาวุธจรวดสกัดกั้นทางอากาศ (Intercepting Missile) แบบอากาศสู่อากาศ (Air to Air), อุปกรณ์เลเซอร์ (Laser) ที่ติดตั้งบนอากาศยาน และยานรบ

ภาคพื้น เป็นต้น ซึ่งอุปกรณ์ควบคุมอาวุธเหล่านี้เป็นอุปกรณ์อิเล็กทรอนิกส์ที่มีอิเล็กทรอน (Electron) วิ่งทำงานอยู่ ดังนั้นการรับมือของฝ่ายเราต้องมีความสามารถในการป้องกันทางอิเล็กทรอนิกส์ที่มีประสิทธิภาพ

ในส่วนของ บก.ทท. นั้น การประสานการปฏิบัติทางการรบกับเหล่าทัพ จะขึ้นอยู่กับการสื่อสารทางทหารเป็นหลัก ทางพลเรือนเป็นรอง กองพันทหารสื่อสาร (พัน ส.) กับ กองพันปฏิบัติการสงครามอิเล็กทรอนิกส์ (พัน ปสอ.) สังกัดภายใต้ กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย (สส.ทหาร บก.ทท.) ได้ปฏิบัติตาม พรบ.ประกอบกิจการกระจายเสียงและกิจการโทรทัศน์ พ.ศ.2551[72] และ พรบ. ประกอบกิจการโทรคมนาคม พ.ศ.255[73] ที่เกี่ยวข้องกับการปฏิบัติการในมิติไซเบอร์ของ ทท. มีความสัมพันธ์กับโครงข่ายโทรคมนาคม เจ้าของโครงข่าย การเชื่อมต่อ และคลื่นความถี่ ในส่วนของอิเล็กทรอนิกส์ และแถบคลื่นแม่เหล็กไฟฟ้า พบว่า ทท. มีความพร้อมต่อการทำสงครามอิเล็กทรอนิกส์อยู่ในระดับหนึ่ง

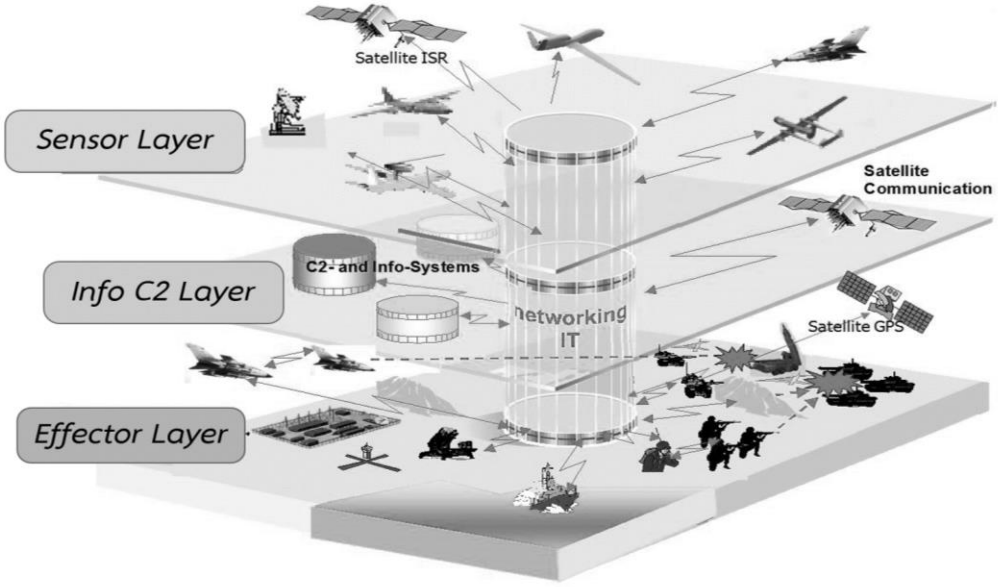
ปัจจุบันหลายประเทศพัฒนาอาวุธเพื่อให้ทำลายอุปกรณ์อิเล็กทรอนิกส์ทุกประเภท เช่น EMP (Electromagnetic Pulse) อาวุธที่มีขนาดประมาณกระเป๋าเอกสาร จาก สถาบันลอสอาลามอส (Los Alamos) รัฐนิวเม็กซิโก ประเทศสหรัฐ โดยนำกระเป๋าที่บรรจุ EMP ตั้งเวลาให้เครื่องทำงาน ไปวางไว้แถวอาคารเป้าหมาย เมื่อเกิดการระเบิดคลื่นแม่เหล็กไฟฟ้าเหมือนฟ้าผ่า ส่วนประกอบที่เป็นตัวนำไฟฟ้าในอาคาร หรือที่เกี่ยวข้องด้วยระบบอิเล็กทรอนิกส์จะหมดสภาพการใช้งาน[74] จัดเป็น สงครามโฟตอน (Photonic Warfare) ที่ทำให้อุปกรณ์ที่มีชิ้นส่วนอิเล็กทรอนิกส์และข้อมูลภายในถูกทำลาย ไม่สามารถทำงานได้อีก การป้องกันในระดับนี้ ทท. ยังไม่สามารถดำเนินการได้[75]

การสร้างความได้เปรียบในการครองมิติไซเบอร์ (Cyber Superiority) เพื่อดำเนินกลยุทธ์ เมื่อเข้าใจสงครามทั้ง 3 รูปแบบ คือ สงครามไซเบอร์ สงครามข่าวสาร และสงครามอิเล็กทรอนิกส์ ที่มักเกิดขึ้นพร้อม ๆ กัน ในการปฏิบัติการทางทหารเพื่อให้ผู้บังคับบัญชารับรู้สถานการณ์ (Situation Awareness, SA) ร่วมกันแบบทันทีทันใด (Real Time) สามารถใช้การสื่อสารด้วยระบบดิจิทัล เช่น การประชุมผ่านระบบสื่อสารที่มีทั้งภาพและเสียง (Video Tele Conference, VTC) โดยไม่ต้องมาอยู่ ณ ที่เดียวกัน ช่วยให้ผู้บังคับหน่วยสามารถอยู่ ณ ที่

ตำบล ที่นำหน่วยได้ดีที่สุด[76] ผู้บังคับหน่วย บก.ทท. และเหล่าทัพ สามารถเข้าใจในสถานการณ์ (Situational Understanding, SU) อย่างถ่องแท้ ในสถานการณ์ของพันธมิตร สถานการณ์ของข้าศึก และสถานการณ์ด้านการดำรงสภาพที่เป็นปัจจุบัน ด้วยระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารทหารที่ บก.ทท. ให้การสนับสนุน เช่น (1) ระบบแผ่นภาพสถานการณ์ร่วม (Common Operation Picture, COP) ที่เป็นปัจจุบัน โดยความเข้าใจในภาพรวมนี้ จะทำให้ผู้บังคับบัญชาและฝ่ายอำนวยการของหน่วยที่เกี่ยวข้อง ได้เห็นและใช้ข้อมูลการรบชุดเดียวกัน ในเวลาที่ใกล้เคียงกับเวลาจริง มีความเข้าใจในสถานการณ์ตรงกัน เกิดเอกภาพในการบังคับบัญชา (Unity of Command) และเอกภาพในการพยายาม (Unity of Effort) (2) ระบบข้อมูลข่าวสารร่วมกัน (Message Text Format, MTF) ทำให้มองเห็นการเคลื่อนไหวของข้อมูล ทั้งการยุทธ์และส่งกำลัง ความต้องการของหน่วย และแผ่นภาพสถานการณ์ร่วมที่เป็นปัจจุบันร่วมกัน ด้วยโครงสร้างพื้นฐานระบบคอมพิวเตอร์และเครือข่ายที่เหมาะสมของเหล่าทัพ ทำให้สามารถแบ่งปันและแลกเปลี่ยนข้อมูลที่มีขนาดใหญ่ได้พร้อมกัน (3) ระบบกำหนดตำแหน่งบนพื้นโลก (Global Positioning System, GPS) ติดตั้งพร้อมกล้องบนยานพาหนะและบุคคล สามารถติดตามการเคลื่อนที่และการปฏิบัติของกำลังพลและสิ่งอุปกรณ์ ก่อน ระหว่าง และหลัง ในพื้นที่ปฏิบัติการ ด้วยระบบข้อมูลข่าวสารและการสื่อสารที่ทันสมัย

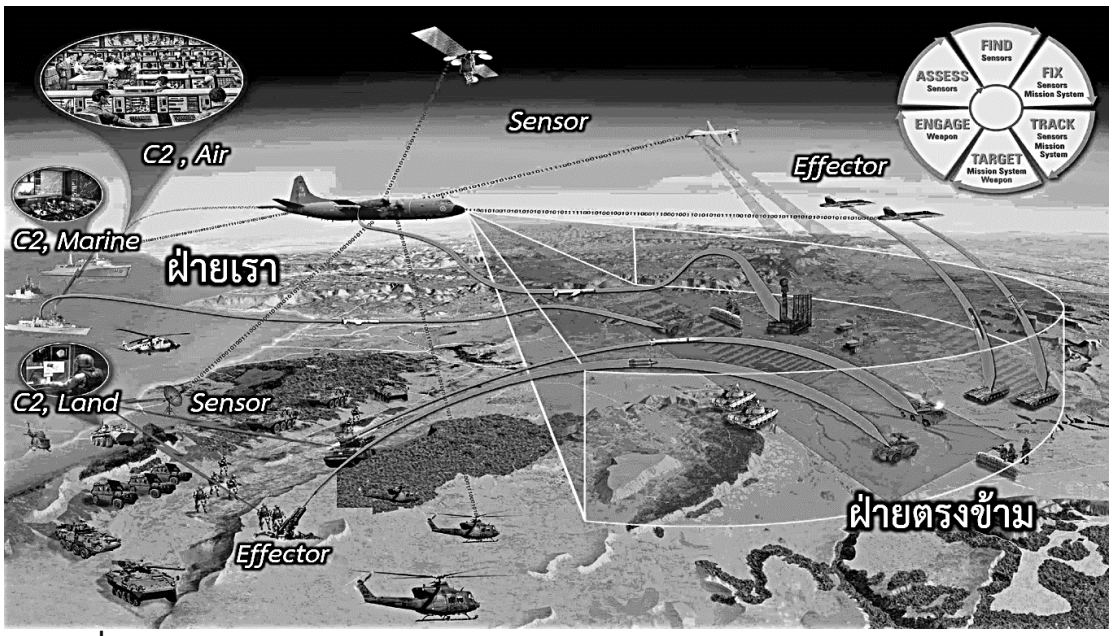
การก้าวสู่สงครามไซเบอร์ที่เน้นการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง เป็นปฏิบัติการทางทหารที่ตอบสนองทฤษฎีการสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare : NCW) เชื่อมโยงกำลังทหารเข้าเป็นระบบเครือข่าย ก่อให้เกิดความร่วมมือด้านข้อมูลข่าวสาร[77] โดยใช้เทคโนโลยีสารสนเทศและการสื่อสารทางทหาร ก่อให้เกิดอานุภาพในการรบ สนับสนุนการแลกเปลี่ยนข้อมูลระหว่างระบบตรวจจับและค้นหา (Sensor Layer), ระบบผู้บังคับบัญชาที่มีอำนาจตัดสินใจ (Command Control (C2) Layer) และผู้ปฏิบัติในพื้นที่การรบ (Effector Layer) โดยใช้เครือข่ายเป็นศูนย์กลาง ทั้งภายในและระหว่างหน่วยทหาร ทั้งระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ เพื่อให้ข้อมูลสารสนเทศ ภาพสถานการณ์ และคำสั่ง ผ่านการสื่อสารเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link, TDL) ระหว่างผู้บังคับบัญชาที่มีอำนาจตัดสินใจ และผู้ปฏิบัติในพื้นที่การรบ เพื่อรับรู้สถานการณ์ร่วมกัน เกิดความรวดเร็วและถูกต้องในการตัดสินใจที่แม่นยำและทั่วถึง นำไปสู่การปฏิบัติที่ถูกจังหวะเวลา มีอานุภาพทำลายล้างสูง ลดการสูญเสียของกำลังพลและอาวุธยุทโธปกรณ์ของฝ่ายเรา สร้าง

ความเป็นหนึ่งเดียวในการปฏิบัติ ทันต่อสถานการณ์ ก่อให้เกิดความได้เปรียบในการทำสงคราม[78] หลายประเทศรวมถึง ทท. ได้นำแนวคิดนี้มาเป็นหลักในการพัฒนาระบบควบคุมบังคับบัญชา ระบบตรวจจับ ระบบอาวุธ และระบบการสื่อสารของกองทัพ[79]



ภาพที่ 3 การสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare : NCW) [80]

การทวีกำลังรบ (Force Multiplier) บนสนามรบหลายมิติ (Multi-Domain Battle) จากการสร้างภาพสถานการณ์การรบโดยระบบแผ่นภาพสถานการณ์ร่วม เพื่อให้กำลังภาคพื้นดิน เรือรบ และอากาศยานทุกลำ ของเหล่าทัพ สามารถเชื่อมต่อและปฏิบัติการร่วมกันได้โดยตรง มองเห็นข้อมูลทั้งหมดเหมือนกันผ่าน ศูนย์ปฏิบัติการ กองทัพบก (ศปก.ทบ.) ระบบอำนวยการรบ (Combat Management System, CMS) ของ ทร. และระบบบัญชาการควบคุมทางอากาศ (Air Command and Control : ACCS) ของ ทอ. โดยส่งภาพและเสียงมายังระบบควบคุมบังคับบัญชาและสั่งการ (Command, Control, Communication, Computer, Intelligence, C^4I) ของ ศบท. (บก.ทท.)



ภาพที่ 4 การครองความได้เปรียบในมิติไซเบอร์ในการทวีกำลังรบบนสนามรบหลายมิติโดยใช้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง[81]

แผนผังแสดงองค์ประกอบหลักของยุทธศาสตร์ทหารด้านสงครามไซเบอร์ของ ทท. พ.ศ.2558[82]

<table>
<tr><td>End</td><td colspan="3">กองทัพไทยมีอำนาจทางไซเบอร์
เพื่อนำไปสู่ความได้เปรียบในมิติไซเบอร์ ทท.</td><td colspan="3">กองทัพไทยเกิดความเข้าใจร่วมกันเกี่ยวกับ
การปฏิบัติการในมิติไซเบอร์ ทท.</td></tr>
<tr><td>Strategic Theme</td><td colspan="2">การป้องกันเชิงรุก
สำหรับการปฏิบัติการในมิติไซเบอร์</td><td colspan="2">การผนึกกำลังป้องกันประเทศ
สำหรับการปฏิบัติการในมิติไซเบอร์</td><td>การสร้างความร่วมมือด้านความมั่นคง
สำหรับการปฏิบัติการในมิติไซเบอร์</td></tr>
<tr><td>Ways</td><td colspan="2">RTARF Cyber Power
เสริมสร้างพลังอำนาจทางไซเบอร์ ทท.
ใช้การปฏิบัติการในมิติไซเบอร์ ทท. ในลักษณะป้องกันเชิงรุก
บูรณาการการปฏิบัติการในมิติไซเบอร์ ทท. เข้ากับการปฏิบัติอื่นๆ
พัฒนาการปฏิบัติการในมิติไซเบอร์ ทท. ในลักษณะป้องกันเชิงรุก
พัฒนาการฝึกร่วมผสมทางไซเบอร์ ทท.</td><td>ปกป้องสถาบันโดยใช้พลังอำนาจทางไซเบอร์
สนับสนุนรัฐบาลแก้ไขปัญหาจากภัยคุกคามรูปแบบใหม่
ร่วมมือกับภาครัฐและเอกชน ในการรับมือภัยคุกคาม
ร่วมกับ กห. ในการกำหนดแนวทางพัฒนา
บูรณาการร่วมกันในการปฏิบัติงานร่วมกันระหว่างหน่วยงานด้านไซเบอร์ ทท.
สนับสนุนรัฐบาลแก้ไขปัญหาความสงบเรียบร้อยภายในประเทศ</td><td>สร้างความสัมพันธ์ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับมิตรประเทศและประเทศมหาอำนาจ
สร้างความร่วมมือทางทหารเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ในภูมิภาค</td></tr>
<tr><td>Means</td><td colspan="2">โครงสร้างกำลังรบทางไซเบอร์ ทท. ที่ต้องการ
(ภาวะปกติ)</td><td colspan="2">โครงสร้างกำลังรบทางไซเบอร์ ทท. ที่ต้องการ
(ภาวะฉุกเฉิน)</td></tr>
</table>

จากการเปลี่ยนแปลงภัยคุกคามทางไซเบอร์ ที่มาจากเทคโนโลยีและนวัตกรรมที่ล้ำสมัย ทท. ต้องเตรียมความพร้อมปฏิบัติภารกิจด้านไซเบอร์ ในการพัฒนากำลังพล กระบวนการทำงาน และเทคโนโลยีไซเบอร์ทางการทหาร เพื่อการปฏิบัติการด้านไซเบอร์ทั้งเชิงรับ และเชิงรุก

การปฏิบัติการด้านไซเบอร์เชิงรับ บก.ทท. ต้องมีความทนทานต่อการถูกโจมตีทางไซเบอร์ (Cyber Resilience) อยู่ในระดับการทำงานที่ยังรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Service Level Agreement, SLA) ได้ โดย

1) **การพัฒนากำลังพล** กำลังพลที่บรรจุใน ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด (ศซบ.สน.ทสส.) ต้องจบสาขาที่เกี่ยวกับคอมพิวเตอร์ เทคโนโลยีสารสนเทศ หรือได้รับใบรับรองสำหรับผู้ที่ผ่านการทดสอบตามมาตรฐานของ สมาคมเทคโนโลยีคอมพิวเตอร์และอุตสาหกรรม (The Computing Technology Industry Association, CompTIA), สมาคมไม่แสวงหาผลกำไรนานาชาติที่มุ่งหวังในการสร้างโลกไซเบอร์ที่มั่นคงและปลอดภัย (The International Information System Security Certification Consortium, ISC2), สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (Information Systems Audit and Control Association, ISACA) และ สถาบันผู้บริหารระบบเครือข่ายและความมั่นคง (System Administration Network and Security Institute, SANS) เป็นต้น การจัดกำลังพลจากหน่วยขึ้นตรง (นขต.) บก.ทท. เข้าร่วมการฝึกไซเบอร์ ทท. ประจำปี เพื่อประสานความร่วมมือทางไซเบอร์ของ นขต.บก.ทท. และเหล่าทัพ รวมถึงหน่วยงานความมั่นคงอื่น ๆ ภายในประเทศ และการฝึกไซเบอร์ร่วมกับมิตรประเทศ เช่น การประชุมคณะกรรมการควบคุมและสั่งการร่วมไทย-สหรัฐ (Command and Control Interoperability Board, CCIB), การประชุมคณะทำงานป้องกันไซเบอร์ร่วม (Cyber Defense Working Group, CDWG), การฝึกสนธิการสื่อสารนานาชาติ (Multinational Communications Interoperability Program, MCIP) ภายใต้รหัส PE (Pacific Endeavor), คอบร้าโกลด์ (Cobra Gold, CG) และ การประชุมแลกเปลี่ยนผู้เชี่ยวชาญด้านไซเบอร์ ไทย–สหรัฐ (Cyber Security Subject Master Expert Exchange, SMEE) เป็นต้น ในด้านการสร้างและฝึกทักษะของกำลังพลเพื่อพัฒนาเป็นนักรบไซเบอร์ โดยทำการฝึกในระบบงานจำลองยุทธ์ทางไซเบอร์ (Cyber Range) และการซ้อมรับการโจมตีทางไซเบอร์ (Cyber Drill) เพื่อให้สามารถปฏิบัติงานได้ทั้งเชิงรับ และเชิงรุก สุดท้ายเป็นการอบรมกำลังพล บก.ทท. ประจำปี เพื่อสร้างความตระหนักรู้ทางไซเบอร์ (Cyber Awareness) ให้กับกำลังพล

2) **กระบวนการทำงาน** โดยวางกลยุทธ์ด้านความมั่นคงปลอดภัยสำหรับการปฏิบัติการไซเบอร์เชิงรับ เพื่อเพิ่มประสิทธิภาพของระบบรักษาความปลอดภัยทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ ตาม สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity) เพื่อบริหารความเสี่ยงด้านไซเบอร์ โดยทำการฝึกซ้อมเพิ่มทักษะและประสบการณ์ในการรับมือกับภัยคุกคามตลอดเวลา เพื่อให้ผู้ใช้ทุกระดับได้ตระหนักถึงความสำคัญ เพราะจุดอ่อนขององค์กรมักอยู่ที่ "คน" ในด้านการต่อต้านการข่าวทางไซเบอร์ เช่น การจัดการต่อเว็บหมิ่นต่อสถาบันพระมหากษัตริย์ และความมั่นคงของรัฐทางสื่อสังคมออนไลน์ เป็นหน้าที่การปฏิบัติการข่าวสารเชิงรับ โดย สปข.ศบท. และ การปฏิบัติการข่าวสารทางไซเบอร์เชิงรับของ กรมข่าวทหาร (ขว.ทหาร) และ ศูนย์รักษาความปลอดภัย (ศรภ.) บก.ทท. ในด้านการสร้างความร่วมมือการผนึกกำลังทางไซเบอร์ (Cyber Unity) ได้ทำการระดมสรรพกำลังทางไซเบอร์ (Cyber Mobilization) โดยการจัดการประชุมประชาคมไซเบอร์ (Cyber Community) ทท. กับเหล่าทัพ และหน่วยงานความมั่นคง เช่น กห. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดท.) กรมสอบสวนคดีพิเศษ (กสพ.) สถาบันเทคโนโลยีป้องกันประเทศ (สทป.) และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)[83] สุดท้ายนำ นโยบายการรักษาความปลอดภัยสารสนเทศ บก.ทท. พ.ศ.2559 ที่ผ่านการประเมินโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ปัจจุบัน คือ ดท.) อ้างอิงตามมาตรฐาน ISO/IEC 27001: 2005 มาบังคับใช้

3) **เทคโนโลยีการปฏิบัติการไซเบอร์เชิงรับ** หน่วยงานที่เกี่ยวข้องในการจัดหาอุปกรณ์เพื่อการป้องกันไซเบอร์เชิงรับ ประกอบด้วย ศูนย์คอมพิวเตอร์ บก.ทท. (Data Center) จัดเก็บและประมวลผลข้อมูลที่สำคัญของ นขต.บก.ทท. ศูนย์ปฏิบัติการเครือข่ายทางไซเบอร์ (Network Operation Center, NOC) ที่มีกำลังพลเฝ้าระวังและติดตามภัยคุกคามทางเครือข่ายตลอด 24 ชั่วโมงทุกวัน (24x7) และ ศซบ.สน.ทสส. ประกอบด้วย 2 ศูนย์ย่อย คือ ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center, SOC) ทำหน้าที่เฝ้าระวังติดตามภัยคุกคาม และป้องกันการบุกรุกระบบของ บก.ทท. ตลอด 24 ชั่วโมง และ ศูนย์ปฏิบัติการไซเบอร์ร่วม (Joint Cyber Operation Center, JCOC) ทำหน้าที่ประสานงานด้านไซเบอร์

ระหว่าง บก.ทท. กับเหล่าทัพ และหน่วยงานด้านความมั่นคงของประเทศ มีการนำมาตรการการรักษาความปลอดภัยในการยืนยันตัวตนมาใช้ วิธีพื้นฐานใช้บัตรและรหัสผ่าน (Password) วิธีที่ปลอดภัยที่สุดเป็นการนำเทคโนโลยีการตรวจวัดทางชีวภาพ (Biometric) โดยใช้ข้อมูลทางกายภาพส่วนบุคคล เช่น ลายนิ้วมือ (Finger) เส้นเลือดดำบนฝ่ามือ (Vain) เสียง (Voice) ม่านตา (Retina) ใบหน้า (Face) และ หู (Ear) หรือ การนำพฤติกรรม (Behavior) เช่น ลายเซ็น (Signature) และท่าเดิน (Walking) มาใช้ในการยืนยันสิทธิการเข้าถึงระบบต่าง ๆ

การปฏิบัติการด้านไซเบอร์เชิงรุก ผู้บังคับบัญชาต้องมีความตระหนักรู้เกี่ยวกับ “ART” ที่ประกอบด้วย ความสามารถพิสูจน์ทราบคุณลักษณะการโจมตีทางไซเบอร์ (Attribution) ความสามารถเข้าตอบโต้การโจมตีอย่างเหมาะสม (Rule Of Engagement, ROE) และประเมินความเสี่ยงของฝ่ายตรงข้าม (Trust Relationship)[84] การดำเนินการด้านการทำสงครามไซเบอร์ในปัจจุบันยังไม่มีกฎหมายรองรับ ดังนั้น ทท. ต้องเตรียมความพร้อมในการปฏิบัติการเชิงรุก โดย

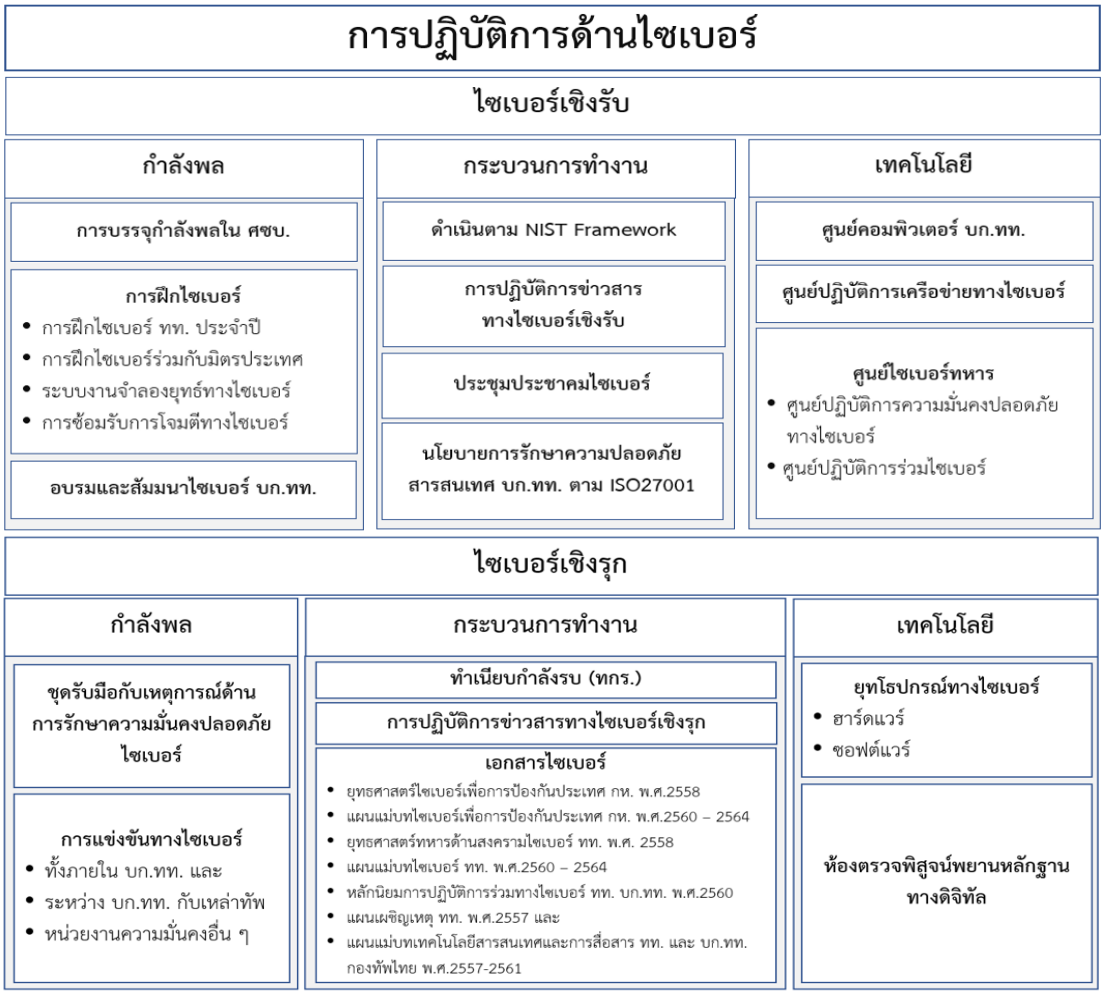
1) **การพัฒนากำลังพล** จัดให้มีชุดรับมือกับเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Response Team, CSIRT) ทำหน้าที่เก็บข้อมูลหลักฐาน และประสานผู้เกี่ยวข้องทราบถึงความเสียหายจากการถูกโจมตีทางไซเบอร์ เช่น เจ้าของระบบ (System Owner) และการแข่งขันทางไซเบอร์ (Cyber Exercise) ของ ทท. ทั้งภายใน บก.ทท. และระหว่าง บก.ทท. กับเหล่าทัพ รวมถึงหน่วยงานความมั่นคงอื่น ๆ

2) **กระบวนการทำงาน** ในสงครามไซเบอร์ที่ไม่รู้ว่าเป็นใคร การจัดการข่าวกรองทางไซเบอร์ (Cyber Intelligence) ได้นำหลักพิชัยสงคราม (Art of War) “รู้เขา รู้เรา รบร้อยครั้ง ชนะร้อยครั้ง” ของ ซุนวู มาปรับใช้ เพื่อจัดทำทำเนียบกำลังรบ (ทกร.) ที่เป็นบัญชีเป้าหมายทางไซเบอร์ โดยเฉพาะระบบโครงสร้างพื้นฐานสำคัญของรัฐและไซเบอร์ทางทหาร เป้าหมายที่มีความอ่อนไหวสำคัญทางยุทธศาสตร์ของฝ่ายเราและฝ่ายตรงข้าม และการจัดทำแผ่นภาพข้อมูลเชิงรุกด้านการตระหนักรู้ให้กับกำลังพลของ ทท. เผยแพร่ในสื่อที่เหมาะสม โดยการปฏิบัติการข่าวสารเชิงรุก ของ สปข. ศบท. และ การปฏิบัติการข่าวสารทางไซเบอร์เชิงรุก ของ ขว.ทหาร และ ศรภ. สุดท้าย กห. กับ ทท. จัดทำ ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กห. พ.ศ.2558 แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กห. พ.ศ.2560–2564 ยุทธศาสตร์ทหารด้านสงครามไซเบอร์ ทท. พ.ศ. 2558 แผนแม่บทไซเบอร์ ทท. พ.ศ.2560–2564 หลักนิยมการปฏิบัติการร่วม

ทางไซเบอร์ ทท. บก.ทท. พ.ศ.2560 แผนเผชิญเหตุ ทท. พ.ศ.2557 และ แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ทท. และ บก.ทท. กองทัพไทย พ.ศ.2557-2561 เพื่อมาเป็นแนวทางการปฏิบัติทางไซเบอร์ให้กับเหล่าทัพ

3) **เทคโนโลยีการปฏิบัติการไซเบอร์เชิงรุก** จัดหายุทโธปกรณ์ทางไซเบอร์ (Cyber Weapon) ทั้งฮาร์ดแวร์และซอฟต์แวร์ เมื่อ ทท. ถูกโจมตีทางไซเบอร์ ต้องสามารถเก็บข้อมูลหลักฐานที่เกี่ยวข้องโดยผ่านกระบวนการตามมาตรฐานของ ห้องตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensic Lab) ของ ทท. เพื่อส่งหลักฐานให้กับหน่วยงานที่เกี่ยวข้องดำเนินการตามกฎหมายต่อไป

แผนผังสรุปการปฏิบัติการไซเบอร์เชิงรุกและเชิงรับ ของ กองบัญชาการกองทัพไทย



ผลการวิจัย พบว่า บก.ทท. สามารถเป็นต้นแบบระบบงานด้านไซเบอร์ทั้งเชิงรับ และเชิงรุก ในภาวะปกติ และฉุกเฉิน มีความพร้อมในการเตรียมกำลัง และ การปฏิบัติการร่วมในมิติไซเบอร์ของ ทท. เป็นไปในทิศทางเดียวกัน โดยมี ทท. เป็นองค์กรหลัก เมื่อผนึกกำลังทางไซเบอร์แล้วจะสามารถพิทักษ์ผลประโยชน์แห่งชาติได้

บทสรุป

ปัจจุบันภัยคุกคามทางไซเบอร์ภาครัฐและเอกชน เริ่มจากอาชญากรรมทางไซเบอร์ และมีแนวโน้มการโจมตีทางไซเบอร์ระหว่างรัฐต่อรัฐ โดยมีเป้าหมายต่อโครงสร้างพื้นฐานสำคัญของชาติ เมื่อเหตุการณ์ลุกลามเป็นการปฏิบัติการทางทหารที่ใช้กำลังกระทำการรบแบบหลายมิติ โดย ทท. ทำการบูรณาการขีดความสามารถของ บก.ทท. และเหล่าทัพ ให้มีประสิทธิภาพทั่วทั้งมิติ ทางบก ทะเล อากาศ อวกาศ และพื้นที่ไซเบอร์ เพื่อยับยั้งและเอาชนะฝ่ายตรงข้ามที่มีขีดความสามารถสูงจากภัยคุกคามในสงครามไซเบอร์ สงครามข่าวสาร และสงครามอิเล็กทรอนิกส์ สร้างความได้เปรียบในการครองมิติไซเบอร์ให้ฝ่ายเรา มีอิสระในการปฏิบัติการในมิติไซเบอร์ได้อย่างปลอดภัย เชื่อถือได้ ในช่วงเวลาและสถานที่ที่ต้องการ ปราศจากการขัดขวางจากฝ่ายตรงข้าม โดยปฏิบัติตามยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กห. พ.ศ.2558 เรื่อง การมีเสรีในการใช้ไซเบอร์ของฝ่ายเรา จำกัดเสรีในการใช้ไซเบอร์ของฝ่ายตรงข้าม และ ยุทธศาสตร์ทหารด้านสงครามไซเบอร์ ทท. พ.ศ.2558 ประเด็น การป้องกันเชิงรุก การผนึกกำลังป้องกันประเทศ และการสร้างความร่วมมือด้านความมั่นคงสำหรับการปฏิบัติการในมิติไซเบอร์ของ ทท. เพื่อให้การปฏิบัติการในการทวีกำลังรบของ ทท. ที่ใช้เครือข่ายเป็นศูนย์กลางร่วมกันระหว่าง บก.ทท. และเหล่าทัพ เป็นไปอย่างมีประสิทธิภาพ

ณ วันนี้ สงครามไซเบอร์ ไม่มีผู้ใดตอบได้ว่าจะลงเอยอย่างไร ทท. ต้องรู้เท่าทันการโจมตีทางไซเบอร์ ซึ่งในส่วนของไซเบอร์เชิงรุก ปัจจุบันยังไม่มีกฎหมายรองรับการดำเนินการในการทำสงครามไซเบอร์ ในส่วนของไซเบอร์เชิงรับ ระบบเทคโนโลยีสารสนเทศและการสื่อสารของฝ่ายเราต้องมีความทนทานต่อการถูกโจมตีทางไซเบอร์ อยู่ในระดับการทำงานที่ยังรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ ทท. ได้ ซึ่ง **บก.ทท. สามารถเป็นต้นแบบในการพัฒนาไซเบอร์เชิงรุกและเชิงรับให้กับเหล่าทัพ** และหน่วยงานความมั่นคง โดย**มีมาตรการเตรียมความพร้อมด้าน**

กำลังพล กระบวนการ และเทคโนโลยีทางไซเบอร์ ที่พัฒนาในระดับมาตรฐานสากล มียุทธศาสตร์ แผนแม่บท หลักนิยม และแผนเผชิญเหตุที่ครอบคลุมสงครามไซเบอร์ มีการประชุมประชาคมไซเบอร์ของ ทท. เพื่อ**การระดมสรรพกำลังทางไซเบอร์** สร้างความร่วมมือด้านความมั่นคงทางไซเบอร์กับหน่วยงานความมั่นคงทั้งในและต่างประเทศ พัฒนาเป็นประชาคมไซเบอร์ระดับชาติ แสวงหาความร่วมมือกับมิตรประเทศ เพื่อพัฒนากำลังพลให้มีองค์ความรู้ ความสามารถในระดับที่เท่าเทียม หรือเหนือกว่านักเจาะระบบมืออาชีพ **เพื่อเป็นส่วนหนึ่งในการผนึกกำลังทางไซเบอร์** ป้องกันโครงสร้างสารสนเทศพื้นฐานของประเทศ เสริมสร้างพลังอำนาจแห่งชาติในการรับมือการโจมตีทางไซเบอร์ โดยมุ่งเน้นพิทักษ์ผลประโยชน์แห่งชาติเป็นสำคัญ.

เอกสารอ้างอิง

[1] อิเล็กทรอนิกส์ [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 ตุลาคม 2560]. เข้าถึงได้จาก : https://th.wikipedia.org/wiki/อิเล็กทรอนิกส์.

[2] สารกึ่งตัวนำ [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 ตุลาคม 2560]. เข้าถึงได้จาก : http:// www.scimath.org/ lesson-physics/item/7237-2017-06-11-14-15-33.

[3] วงจรรวม [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 23 ตุลาคม 2560]. เข้าถึงได้จาก : https://th.wikipedia.org/wiki/วงจรรวม.

[4] หลักเมือง ข่าวสารของสำนักงานปลัดกระทรวงกลาโหม. เทคโนโลยีดิจิตอล (Digital Technology) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 2 มกราคม 2561, แก้ไขล่าสุดเมื่อวันที่ 5 มกราคม 2561 เวลา 09:50 น.]. เข้าถึงได้จาก : http://lakmuangonline.com/\?p=4207.

[5] ยุคสารสนเทศ (Information) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 26 ตุลาคม 2560]. เข้าถึงได้จาก : https://th.wikipedia.org/wiki/ยุคสารสนเทศ.

[6] เทคโนโลยีสารสนเทศและการสื่อสาร [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 28 ตุลาคม 2560]. เข้าถึงได้จาก : https:// th.wikipedia.org/wiki/เทคโนโลยีสารสนเทศและการสื่อสาร.

[7] รศ.ดร.สมนึก เอื้อจิระพงษ์พันธ์ และจาตุรนต์ ชุติธรพงษ์. บทบาทของการจัดการความรู้กับการพัฒนาการหยั่งรู้เชิงกลยุทธ์ (The Role of Knowledge Management in Developing Strategic Intuition), วารสารราชภัฏสุราษฎร์ธานี ปีที่ 4 ฉบับที่ 2 (กรกฎาคม – ธันวาคม 2560). หน้า 21.

[8] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจสังคม (Digital Thailand), 1 พฤษภาคม พ.ศ. 2559. หน้า 3.

[9] พระราชบัญญัติ การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560. ราชกิจจานุเบกษา เล่ม 134 ตอนที่ 10 ก 24 ม.ค. 2560. หน้า 1-2.

[10] คณะทำงานพัฒนาหลักสูตรอบรมด้านการตรวจสอบภายใน และคณะอนุกรรมการด้านการพัฒนาวิชาชีพบัญชี. สรุปสาระสำคัญจากการเสวนา Cyber Security สำหรับผู้ตรวจสอบและนักบัญชียุค 4.0, สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. หน้า 5.

[11] อินเทอร์เน็ตของสรรพสิ่ง [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 30 ตุลาคม 2560]. เข้าถึงได้จาก : https://th.wikipedia .org/wiki/อินเทอร์เน็ตของสรรพสิ่ง.

[12] Digital Economy ของประเทศไทยในยุค S-M-I-C และ Internet of Thing กับการเปลี่ยนแปลงทางดิจิทัลของโลกในศตวรรษที่ 21 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 พฤศจิกายน 2560]. เข้าถึงได้จาก : http://mediamonitor.in.th/archives/20525.

[13] เอกชัย สุมาลี และทีมวิจัย. โครงการวิจัยเชิงนโยบายเพื่อเสนอแนะแนวทางการยกระดับอุตสาหกรรมซอฟต์แวร์และอิเล็กทรอนิกส์ ภายใต้กรอบของ Internet of Things และ Smart City (รหัสโครงการ SRI5851206). หน้า 1-1 ถึง 1-2.

[14] ดร.จุรีรัตน์ ประสาร. อุตสาหกรรมสิ่งทอในยุค Industry 4.0, MTEC ม.ค.-มี.ค.60. หน้า 51-55.

[15] ธุรกิจในศตวรรษที่ 21 เป็นรูปแบบ Cyber-Physical Systems ตอนที่ 4 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 ตุลาคม 2560]. เข้าถึงได้จาก : http://www.mplus.co.th/cyber-physical-systems-ตอนที่-4.

[16] การไฟฟ้าส่วนภูมิภาค. ระบบโครงข่ายไฟฟ้าอัจฉริยะ (Smart Grid) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 28 ตุลาคม 2560]. เข้าถึงได้จาก : http://www.pe.eng.ku.ac.th/files/semimar/2017/group1/power-grid.html.

[17] บริษัท TRPC แปลโดย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. 7 ความเสี่ยงของข้อมูลที่เปิดเผยสู่สาธารณะ ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ. หน้า 16.

[18] ดร.เศรษฐพงศ์ มะลิสุวรรณ, พันเอก. ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy) กสทช. หน้า 15..

[19] ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก กระทรวงกลาโหม. ความรู้พื้นฐานการพัฒนาหลักนิยมกำลังรบผสมเหล่า ระดับกรม กรมผสม ทบ.ไทย, หนังสือเผยแพร่ความรู้ กรมยุทธศึกษาทหารบก 2559, พิมพ์ที่ ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก ครั้งที่ 1; พ.ศ.2559. หน้า 3-4.

[20] เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย (Software Park Thailand) ภายใต้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.). ติดปีกเอสเอมอี รองรับลูกค้าดิจิทัล, จุลสารข่าว Smart Industry ฉบับที่ 32; พ.ศ.2560. หน้า 4.

[21] Dictionary ไซเบอร์ [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 27 ตุลาคม 2560]. เข้าถึงได้จาก : https://dictionary. sanook.com/search/dict-computer/cyber.

[22] Dictionary มิติไซเบอร์ [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 27 ตุลาคม 2560]. เข้าถึงได้จาก : https://dictionary. sanook.com/search/dict-computer/cyberspace.

[23] คลื่นแม่เหล็กไฟฟ้าและความถี่วิทยุเพื่อการสื่อสาร (Electromagnetic Spectrum and Radio Frequency Communications) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 27 ตุลาคม 2560]. เข้าถึงได้จาก : http://thaitelecomkm.org/TTE/topic/attach/Electromagnetic_ Spectrum_and_Radio_Frequen_Communications/index.php.

[24] ฤทธี อินทราวุธ, พลตรี. ผู้อำนวยการศูนย์เทคโนโลยีทางทหาร. ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นสูง (Advanced Security Operations Center) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 29 ตุลาคม 2560]. เข้าถึงได้จาก : http://rittee1834. blogspot.com/2014/11/advanced-security-operations-center.html.

[25] พร พิเศก, พันเอก. กองทัพบกกับภัยคุกคามรูปแบบต่าง ๆ, ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก พิมพ์ครั้งที่ 1; พ.ศ. 2557. หน้า 46.

[26] ตะลึง “ไทย" ตกมาตรฐานสกัดภัยคุกคามไซเบอร์ติด 15 เสี่ยงโลก [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 12 มีนาคม 2561]. เข้าถึงได้จาก : https://news.thaipbs.or.th/content/264945.

[27] โจรกรรมไซเบอร์ [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 12 มีนาคม 2561]. เข้าถึงได้จาก : https://rabbitfinance.com /business/glossary/cyber-risk.

[28] เทรนด์ ไมโคร ชี้ Cyber Propaganda และ Ransomware จะเป็นภัยที่น่ากลัว และจะคุกคามองค์กรอย่างต่อเนื่อง [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 มีนาคม 2561]. เข้าถึงได้จาก : http://www.thailandindustry.com/indust_newweb/news_preview.php?cid= 24015.

[29] ตัวอย่างซอฟต์แวร์ระบบ SCADA ที่เป็นที่ใช้งานมากในอุตสาหกรรม [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 2 มีนาคม 2561]. เข้าถึงได้จาก : http://mechatronnic2day.blogspot.com/2015/03/ scada-1.html.

[30] Stuxnet [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 12 ธันวาคม 2560]. เข้าถึงได้จาก : https://th. wikipedia. org/wiki /Stuxnet.

[31] รถที่มีการเชื่อมต่ออินเทอร์เน็ต [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 6 มกราคม 2561]. เข้าถึงได้จาก : https://support. volvocars.com/th/cars/Pages/owners-manual.aspx?mc=Y413&my=2016&sw=15w17&article=e1d9901a18269cc7c0a801e8019c3770.

[32] Home Autumation Part 1, OCTOBER 6, 2017 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 12 มกราคม 2561]. เข้าถึงได้จาก : http://macfeteria.com/tag/iot/.

[33] ความมั่นคงปลอดภัยสารสนเทศ สำนักงานเลขาวุฒิสภา, โปรแกรมประสงค์ร้าย [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 พฤศจิกายน 2560]. เข้าถึงได้จาก : http://www3.senate.go.th/security/index.php? Option =com_glossary&id=21&Itemid=12.

[34] TP CERT, ฟิชชิง (PHISHING) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 10 มีนาคม 2561]. เข้าถึงได้จาก : www.tba.or.th /wp-content/uploads/2018/03/TB-CERT-Phishing-02.pdf.

[35] Barracuda Networks, Dell, F5 Networks, Featured Posts, Fortinet, Imperva, Products, Security, Web Security. SQL Injection กับความเชื่อผิด ๆ May 18, 2014 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 15 กุมภาพันธ์ 2561]. เข้าถึงได้จาก : https://www.techtalkthai.com/fallacy-of-sql-injection/.

[36] srsnet. การโจมตี XXS ตอนที่ 1 March 11, 2009 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 28 ตุลาคม 2560]. เข้าถึงได้จาก : https://srannet.wordpress.com/2009/03/11/การโจมตี-xss-ตอนที่-1/.

[37] การโจมตีโดยปฏิเสธการให้บริการ [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 28 มีนาคม 2561]. เข้าถึงได้จาก : https:// th.wikipedia.org/wiki/การโจมตีโดยปฏิเสธการให้บริการ.

[38] Reusing Credentials [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 28 มีนาคม 2561]. เข้าถึงได้จาก : https://metasploit. help.rapid7.com/docs/reusing-credentials.

[39] 7 รูปแบบทั่วไปของการโจมตี Cybersecurity [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 29 ตุลาคม 2560]. เข้าถึงได้จาก : https://www.monsterconnect.co.th/7-common-types-of-cybersecurity-attacks/.

[40] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ. ราชกิจจานุเบกษา เลม 127 ตอนพิเศษ 78 ง หน้า 132 ลง 23 มิถุนายน 2553 หน้า 152.

[41] นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554.

[42] vision : Chief Information Officer (CIO) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 28 ตุลาคม 2560]. เข้าถึงได้จาก : http://july1962.blogspot.com/.

[43] สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. รายงานการวิเคราะห์ “โครงการศึกษาความเป็นไปได้ในการพัฒนาระบบเตือนภัยการโจมตี และแนวทางการบริหารจัดการของประเทศไทย” ของ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ. หน้า ง.

[44] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550; 1 ธันวาคม 2550; หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ; ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

[45] อรรคเดช ประทีปอุษานนท์ และ ธาราทิพย์ กัลยาณมิตร. แนวทางการพัฒนากองทัพไทยด้านการรักษาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์, วารสารสถาบันวิชาการป้องกันประเทศ. หน้า 11- 23.

[46] ริชาร์ด เอ. คลาร์ก และ โรเบิร์ต คเนค เขียน. ไพรัตน์ พงศ์พาณิชย์ แปล, สงครามไซเบอร์ CYBER WAR, สำนักงานมติชน; 2554.

[47] ศิวลีย์ สิริโรจน์บริรักษ์. การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม, วารสารสถาบันวิชาการป้องกันประเทศ ปีที่ 6 ฉบับที่ 3 พฤษภาคม 2548. หน้า 28.

[48] สงครามไซเบอร์ [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 ตุลาคม 2560]. เข้าถึงได้จาก : https://th.wikipedia.org/ wiki/สงครามไซเบอร์.

[49] พระราชบัญญัติ สอบสวนคดีพิเศษ พ.ศ.2547, ราชกิจจานุเบกษา เล่ม 121 ตอนที่ 8 ก หน้า 1 ลง 19 มกราคม 2547.

[50] พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 และ พ.ศ.2551, ราชกิจจานุเบกษา เล่ม 118 ตอนที่ 112 ก หน้า 26 ลง 4 ธันวาคม 2544.

[51] พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 ราชกิจจานุเบกษา เล่ม 134 ตอนที่ 10 ก หน้า 24 ลง 24 มกราคม 2560.

[52] สำนักงานสภาความมั่นคงแห่งชาติ (สมช.). นโยบายความมั่นคงแห่งชาติ พ.ศ.2558-2564, สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา; 1 มิถุนายน 2558. หน้า 17-18.

[53] สำนักงานสภาความมั่นคงแห่งชาติ กระทรวงมหาดไทย กระทรวงกลาโหม. นโยบายการเตรียมความพร้อมแห่งชาติ; หน้า 3-7.

[54] พระราชบัญญัติการจัดการระเบียบราชการกระทรวงกลาโหม พ.ศ.2551. ราชกิจจานุเบกษา เล่ม 125 ตอนที่ 26 ก หน้า 38 ลง 1 กุมภาพันธ์ 2551.

[55] เรื่องเดียวกัน, หน้า 40-45.

[56] ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559 ว่าด้วยรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กร.

[57] ฤทธี อินทราวุธ, พันเอก. รองผู้อำนวยการศูนย์เทคโนโลยีทางทหาร. โดเมน ที่ 5 / โลกไซเบอร์กับ ความมั่นคงของมนุษย์ (The 5th Domain / Cyberspace and Human Security) วันพุธที่ 4 ธันวาคม พ.ศ. 2556 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 ตุลาคม 2560]. เข้าถึงได้จาก : http://rittee1834 .blogspot.com/2013/.

[58] Cyber Kill Chain 3 Phase 7 ขั้นตอน เครื่องมือเจาะระบบเพื่อโจมตีทางไซเบอร์ [อินเทอร์เน็ต]. [เข้า ถึงเมื่อ 1 ธันวาคม 2560]. เข้าถึงได้จาก : http://www.tangerine .co.th /news-events/cyber-kill-chain-3-phase/.

[59] เรื่องเดียวกัน.

[60] อ.ปริญญา หอมเอนก ผู้เชี่ยวชาญ ด้านความปลอดภัยสารสนเทศของไทย. 5 ภัยมืดใกล้ตัวในยุคไซเบอร์ 2012 ที่ทุกคนควรรู้ วันพุธ ที่ 26 ธันวาคม 2555 เวลา 18:35 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 10 ธันวาคม 2560]. เข้าถึงได้จาก : https://www.isranews.org/isranews-article/18478-5-ภัยมืดใกล้ตัวในยุคไซเบอร์-2012-ที่ทุกคนควรรู้.html.

[61] เจ้าหน้าที่ฟอรัม. พฤติกรรมที่ไม่สามารถคาดเดาได้; นิตยสาร INDO-ASIA-PACIFIC DEENSE FORUM ชุดที่ 42 ฉบับที่ 4; 2560. หน้า 11.

[62] ทศพนธ์ นรทัศน์. สงครามไซเบอร์ : สงครามที่มาพร้อมยุคดิจิทัล World War 3 : Cyber Warfare Top 20 Global Mega Trends [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 1 กรกฎาคม 2560]. เข้าถึงได้จาก : http://www.microvsmart.com/สงครามไซเบอร์-สงครามที/.

[63] Diagrams the relation between the ‘five domains’ of US military operations (air, land, sea, space and cyberspace) and the electromagnetic spectrum. The other side of NSA [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 1 กรกฎาคม 2560]. เข้าถึงได้จาก : https://geographicalimaginations .com/tag/cyberspace/.

[64] สหรัฐพัฒนาแนวคิด Multi-Domain Battle [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 1 กรกฎาคม 2560]. เข้าถึงได้จาก : http://www.yanyong.org/?p=1028.

[65] โรงเรียนเสนาธิการทหารบก. คู่มือการปฏิบัติการข่าวสาร (INFORMATION OPERATIONS (IO) HANDBOOK); พิมพ์ครั้งที่ 1; พ.ศ. 2557 พิมพ์โดย ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก. หน้า 5.

[66] กองศึกษาวิจัยทางยุทธศาสตร์และความมั่นคง ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ. เอกสารศึกษาเฉพาะกรณี “การสื่อสารทางยุทธศาสตร์ (Strategic Communication : SC) และการปฏิบัติการข่าวสาร (Information Operations : IO) ของกองทัพไทย : แนวทางการดำเนินงานในอนาคต”; ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ; พิมพ์ครั้งที่ 1;มิถุนายน 2559. หน้า 29.

[67] สถาบันการข่าวกรอง สำนักข่าวกรองแห่งชาติ. ปฏิบัติการข่าวสาร (Information Operations); จุลสารความมั่นคงศึกษา ฉบับที่ 78 พิมพ์ครั้งที่ 1; มิถุนายน 2553. หน้า 1.

[68] คู่มือปฏิบัติการทางยุทธวิธีของกองทัพบก พ.ศ.2555 ทหารสื่อสารสนับสนุนกองพล. หน้า 22-26

[69] การฝึกทักษะเพื่อปรับเปลี่ยนและพลิกแพลงเพื่อเอาชนะ. หนังสือเผยแพร่ความรู้ กรมยุทธศึกษาทหารบก 2557; ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก; พิมพ์ครั้งที่ 1; 2557. หน้า 210.

[70] คู่มือระบบปฏิบัติการในสนามรบ. หนังสือเผยแพร่ความรู้ กรมยุทธศึกษาทหารบก 2560; ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก. หน้า 233.

[71] คู่มือยุทธศาสตร์สำหรับกองทัพบก**.** หนังสือเผยแพร่ความรู้ กรมยุทธศึกษาทหารบก 2560; ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก. หน้า 162.

[72] พระราชบัญญัติประกอบกิจการกระจายเสียงและกิจการโทรทัศน์ พ.ศ.2551. ราชกิจจานุเบกษา เล่ม 125 ตอนที่ 42 ก หน้า 61 ลง 4 มีนาคม 2551.

[73] พระราชบัญญัติประกอบกิจการโทรคมนาคม พ.ศ.2551. ราชกิจจานุเบกษา เล่ม 118 ตอนที่ 106 ก หน้า 11 ลง 16 พฤศจิกายน 2544.

[74] สุทัศน์ จารุมณี, พันเอก. ปฏิรูปการฝึก เพื่อเอาชนะสงครามอนาคต (Training Transformation (T2) To win the Future War). การฝึกทักษะเพื่อปรับเปลี่ยนและพลิกแพลงเพื่อเอาชนะ. หนังสือเผยแพร่ความรู้ กรมยุทธศึกษาทหารบก 2557; พิมพ์ครั้งที่ 1; 2557; ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก. หน้า 149.

[75] ศิลป์ พันธุรังษี, นาวาโท. บทบาทของสงครามโฟตอนกับสงครามในอนาคต (Photonic Warfare); นิตยสารนาวิกศาสตร์ เล่มที่ กันยายน 2546; กองโรงพิมพ์ กรมสารบรรณทหารเรือ. หน้า 4.

[76] ไตรรงค์ ทองเนื้อสุก, พันเอก. หลักนิยมการปฏิบัติการทางบกของกองทัพอังกฤษ; ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก; หจก.อรุณการพิมพ์ พิมพ์ครั้งที่ 1; พศ. 2553. หน้า 241.

[77] ชัยย์ณรงค์ โพธิ์น้อย, พลอากาศโท. การพัฒนาระบบเครือข่ายการสื่อสารของกระทบวงกลาโหมเพื่อความมั่นคง, เอกสารวิจัย ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี; หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 56; ประจำปีการศึกษา 2556-2557. หน้า 37.

[78] ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก. แนวทางพัฒนาการรบที่มีเครือข่ายเป็นศูนย์กลางตามหลักนิยมการรบอากาศ-พื้นดิน; จุลสารยุทธศาสตร์ด้านความมั่นคง. หน้า 13-14.

[79] Network Centric Warfare [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 1 ธันวาคม 2560]. เข้าถึงได้จาก : http://tactdb. blogspot.com/2014/06/network-centric-warfare.html.

[80] Network Centric Warfare [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 1 ธันวาคม 2560]. เข้าถึงได้จาก : mobileenterprise strategies.blogspot.com

[81] Network Centric Operation [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 1 ธันวาคม 2560]. เข้าถึงได้จาก : http:// www.bsipk.net/solution_networkcentric.html.

[82] ยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ.2558. หน้า 4.

[83] สมภพ แสนสมรส, นาวาเอก. Cyber War สถานการณ์เปลี่ยน จุดเปลี่ยน “ความมั่นคงปลอดภัยด้านไซเบอร์”; นิตยสาร นาวิกศาสตร์ เล่มที่ 2 กุมภาพันธ์ 2560; กองโรงพิมพ์กรมสารบรรณทหารเรือ. หน้า 38-40.

[84] ชัยยศ ลิลิตวงษ์, พลตรี. การเสริมสร้างศักยภาพไซเบอร์ ในระดับกระทรวงกลาโหม; เอกสารวิจัย หลักสูตรวิทยาลัยการทัพเรือ กรมยุทธศึกษาทหารเรือ รุ่นที่ 46; ประจำปีการศึกษา 2557. หน้า 27.