การเสริมสร้างและพัฒนานักรบไซเบอร์ของกองทัพบกสำหรับการปฏิบัติการเชิงรุก

การเปลี่ยนผ่านของยุคสมัย

จากสภาพแวดล้อมด้านความมั่นคงของโลกในยุคปัจจุบัน ทำให้ยากที่จะระบุมิตรแท้หรือศัตรูได้อย่างชัดเจน ในสภาวการณ์ของสงครามที่มีความคลุมเครือสูงเช่นนี้ การประกาศสงครามในลักษณะของการรบตามแบบโดยรัฐที่เป็นปฏิปักษ์ เช่นการเผชิญหน้ากันระหว่างกองกำลังจากประเทศแดงและประเทศน้ำเงิน ดังเช่นกรณีศึกษาที่พบในวิทยาลัยการทัพบก หรือโรงเรียนเสนาธิการทหารบกนั้น มีโอกาสที่จะเกิดขึ้นในยุคปัจจุบันได้น้อยมาก จนบางครั้งไม่สามารถชี้ชัดลงไปว่ากำลังต่อสู้อยู่กับใครหรือกำลังถูกใครมารุกล้ำละเมิดอธิปไตยด้านใดด้านหนึ่งอยู่หรือไม่ ในขณะที่สถานการณ์ความขัดแย้งที่เกิดในหลากหลายมิติ มีแนวโน้มทวีความรุนแรง ซับซ้อนและขยายตัวเป็นวงกว้างมากยิ่งขึ้น จนอาจกล่าวได้ว่าสิ่งนี้เป็นลักษณะของการทำสงครามรูปแบบผสม (Hybrid Warfare)[1] คือการผสมผสานวิธีการทำสงครามในหลากหลายรูปแบบเข้าไว้ด้วยกัน อันประกอบด้วยขีดความสามารถ ในการรบตามแบบ ไม่ตามแบบ การก่อการร้าย การสร้างสถานการณ์ความไม่สงบ การก่ออาชญากรรม การปฏิบัติการข่าวสาร การปฏิบัติการไซเบอร์ การปฏิบัติการสร้างอิทธิพลรวมไปจนถึงการผสมผสานการใช้มาตรการทางการเมือง เศรษฐกิจ ข้อมูลข่าวสาร เครื่องมือทางการทูต สิทธิมนุษยชน หลักมนุษยธรรม และมาตรการที่ไม่ใช่ทางทหารรูปแบบอื่น ๆ (Other Non-Military Measures) เป็นต้น หมายรวมถึงการใช้ศักยภาพการต่อต้านจากประชาชน (The Use of the Population’s Protest Potentials) ซึ่งมีผลกระทบอย่างมากในสภาพแวดล้อมปัจจุบันที่ เราไม่สามารถแบ่งแยกพลเรือนออกจากการปฏิบัติการทางทหารภายใต้ความขัดแย้งระดับต่าง ๆที่เกิดขึ้นได้ ซึ่งคู่ขัดแย้งอาจจะเป็นได้ทั้งระหว่างรัฐต่อรัฐ หรือบทบาทของตัวแสดงที่ไม่ใช่รัฐ(Non-State Actors) เช่นกลุ่มก่อการร้ายอัลกออิดะห์ ISIS ตาลีบัน หรือกลุ่มแบ่งแยกดินแดนในภูมิภาคต่าง ๆ ทั่วโลก

เมื่อรูปแบบของสงครามในอนาคตมีแนวโน้มไปสู่สงครามรูปแบบผสมมากขึ้น จึงทำให้เส้นแบ่งระหว่างสภาวะสงคราม กับสภาวะปกติเลือนหายไป การที่รัฐบาลจะประกาศสงคราม เพื่อกำหนดวัน ร. หรือวัน ป. ในการรบตามแบบได้นั้น ก็จะมาจากการที่สถานการณ์ที่ถูกพัฒนาเปลี่ยนแปลงระดับความรุนแรงของความขัดแย้งในสงครามรูปแบบผสมไปพร้อม ๆ กับการสร้างอิทธิพลโดยใช้ประชาชนเป็นศูนย์กลาง เพื่อให้เกิดแนวร่วมหรือแรงต่อต้านนั่นเอง ดังนั้นจึงเป็นเรื่องท้าทายที่ผู้ปฏิบัติงานด้านความมั่นคงของชาติ ควรทำความเข้าใจอย่างถ่อง

แท้และพร้อมรับสถานการณ์ภัยคุกคามรูปแบบผสมตั้งแต่วันนี้ การได้มาซึ่งความได้เปรียบในสภาวะก่อนสงครามนี้เอง ที่อาจนำไปสู่มูลเหตุแห่งการตัดสินให้เกิดผลการแพ้หรือชนะของสงครามได้ ตั้งแต่ยังไม่มีการประกาศสงคราม หรือการปะทะกันของกำลังขนาดใหญ่เลยก็ตาม

หนึ่งในปัจจัยทั้งหลายที่ถูกนำมาใช้ในการทำสงครามรูปแบบผสมนั้น ขีดความสามารถทางไซเบอร์ (Cyber Capability) ได้ถูกคาดการณ์ไว้ว่าจะเป็นเครื่องมือสำคัญของการทำสงครามยุคใหม่ ดังตัวอย่างเช่นในการประชุมวอร์ซอ ซัมมิท ขององค์กรสนธิสัญญาแอตแลนติกเหนือ (NATO) ร่วมกับประเทศสมาชิกพันธมิตร 28 ประเทศ เมื่อเดือนกรกฎาคม ค.ศ.2016 ได้ประกาศให้การปฏิบัติการไซเบอร์ เป็นอีกหนึ่งมิติทางทหาร หรือไซเบอร์ โดเมน (Cyber Domain)[2] เช่นเดียวกับ มิติทาง บก เรือ อากาศ การประกาศเช่นนี้ นั่นหมายความว่า NATO จะต้องมีการจัดเตรียม จัดตั้งหน่วยให้มีขีดความสามารถในการป้องกันและตอบโต้การโจมตีทางไซเบอร์อย่างมีประสิทธิภาพ โดยประสานความร่วมมือจากชาติสมาชิกอย่างใกล้ชิด เช่นเดียวกับประเทศสหรัฐอเมริกา ที่ได้กำหนดไซเบอร์โดเมน ไว้ในหลักนิยมของกระทรวงกลาโหมตั้งแต่ปี ค.ศ. 2006[3] ถึงแม้ว่าห้วงมิติไซเบอร์(Cyber Space) จะถูกนำมาใช้อย่างแพร่หลายในชีวิตประจำวันของคนส่วนใหญ่ก็ตาม แต่ก็มีเพียงคนส่วนน้อยเท่านั้นที่จะสามารถเข้าใจในความหมายที่แท้จริงโดยเฉพาะอย่างยิ่งในมุมมองด้านความมั่นคงหรือการปฏิบัติการทางทหาร ซึ่งส่งผลอย่างยิ่งต่อความมั่นคงของประเทศและการพิทักษ์รักษาผลประโยชน์ของชาติ

<u>สงครามไซเบอร์คือเรื่องจริงที่เกิดขึ้นแล้วในวันนี้</u>

เชื่อว่าหลายคนคงเคยได้ยินหรือได้ศึกษากันมาบ้าง เกี่ยวกับภัยคุกคามไซเบอร์ เพราะคนส่วนใหญ่ในยุคปัจจุบัน ได้เข้าไปอยู่ในโลกไซเบอร์จนกลายเป็นวิถีชีวิตไปโดยปริยายแล้ว จากข้อมูลของ Internet World Stats[4] ได้บันทึกไว้เมื่อ 31 ธันวาคม 2560 พบว่ามีผู้ใช้งานอินเตอร์เน็ตทั่วโลก จำนวน 4,156,932.140 คน หรือคิดเป็นสัดส่วนต่อประชากรโลกราว 54.4% โดยมีอัตราเติบโตเปรียบเทียบตั้งแต่ปี ค.ศ.2000 – 2018 คิดเป็น 1,052% และมีแนวโน้มที่จะเพิ่มขึ้นเรื่อย ๆ จากตัวเลขดังกล่าว ได้ชี้ให้เห็นว่า โลกไซเบอร์ ได้ขยายขอบเขตและขนาดเพิ่มขึ้น ตามจำนวนประชากรที่เข้ามาใช้งาน ซึ่งอาจจะหมายรวมถึงมีการทำธุรกรรมทุกประเภทในโลกไซเบอร์ เพิ่มขึ้นเป็นเท่าทวีคูณอีกด้วย องค์กรสมัยใหม่ทั้งภาครัฐและเอกชน ล้วนอาศัยเทคโนโลยี เข้ามาขับเคลื่อนการดำเนินกิจการต่าง ๆ แทบทั้งสิ้น ส่งผลให้เกิดการลงทุน หรือจัดสรรงบประมาณทางด้าน ดิจิตอล เทคโนโลยี ในแต่ละปีเป็นจำนวน

มหาศาล ทั้งนี้ก็เพื่อพัฒนาธุรกิจ หรือการบริหารงานภาครัฐให้มีประสิทธิภาพ ในส่วนของการใช้งานประเภทบุคคล การพัฒนาของโมบายเทคโนโลยี ที่ได้ถูกรังสรรค์ขึ้นให้ใช้งานได้ง่าย สะดวก และมีความคล่องตัวอย่างมาก จึงทำให้การใช้งานคอมพิวเตอร์แบบพกพาหรือโทรศัพท์มือถือแบบสมาร์ทโฟน ได้สร้างอรรถประโยชน์อย่างเอนกประสงค์ให้แก่ผู้ใช้งาน จนอาจจะถึงขั้นที่กล่าวได้ว่า การท่องไปในโลกไซเบอร์เป็นอีกปัจจัยหนึ่งที่ขาดไม่ได้ ในการดำเนินชีวิตประจำวันของคนในสังคมยุคปัจจุบัน เกือบทุกภูมิภาคทั่วโลก

แต่ถึงกระนั้นหากจะเปรียบว่าเหรียญมีสองด้านฉันใด สิ่งที่มนุษย์สร้างขึ้นแล้วเกิดคุณประโยชน์อเนกอนันต์ ก็สามารถทำให้เกิดโทษมหันต์ได้หากนำมาใช้เป็นเครื่องมือในการประหัตประหารซึ่งกันและกัน ตัวอย่างเช่น ในสงครามโลกครั้งที่ 2 มูลเหตุสำคัญประการหนึ่งของการเอาชนะสงครามในครั้งนั้นของฝ่ายสัมพันธมิตร ต่อกองทัพนาซีอันเกรียงไกรของเยอรมัน มิได้เป็นเพราะการมีกำลังทหารที่เหนือกว่า ระบบอาวุธที่มีสมรรถนะสูงกว่า หรืออำนาจกำลังรบเปรียบเทียบที่เหนือกว่า แต่ปัจจัยที่สำคัญซึ่งนำมาสู่ชัยชนะนั่นก็คือ การข่าว กรอง และการใช้คอมพิวเตอร์ โดยครั้งนั้น อลัน ทัวริ่ง (Alan Turing)[5] นักคณิตศาสตร์ชาวอังกฤษ เป็นผู้มีส่วนสำคัญในการสร้างเครื่องถอดรหัสลับของฝ่ายเยอรมัน โดยเขาเป็นหัวหน้าของกลุ่ม Hut 8 ที่ทำหน้าที่ในการถอดรหัสของเครื่องอินิกมาที่ใช้ในกองทัพเรือ ของเยอรมันได้สำเร็จ จึงทำให้กองทัพของอังกฤษ สามารถล่วงรู้ความลับในการควบคุมบังคับบัญชาของกองทัพเยอรมัน รวมถึงตำแหน่งและแผนการโจมตีของเรือดำน้ำ ก่อนการปฏิบัติจริง ถือเป็นการโจมตีต่อจุดศูนย์ดุลของฝ่ายตรงข้าม ก็คือระบบการควบคุมบังคับบัญชาและการติดต่อสื่อสารได้สำเร็จ โดย วินสตัน เชอร์ชิล (Winston Churchill) นายกรัฐมนตรีของอังกฤษในขณะนั้นได้กล่าวไว้ว่า ผลงานของ อลัน ทัวริ่ง เป็นการสนับสนุนที่ยิ่งใหญ่แก่กองทัพ จนสามารถนำชัยชนะมาสู่ ฝ่ายสัมพันธมิตรได้สำเร็จ และนี่อาจจะกล่าวได้ว่าคือจุดเริ่มต้นของการทำสงครามไซเบอร์ในยุคแรกๆ

ตามที่กล่าวไปแล้วข้างต้น รูปแบบของสงครามขนาดใหญ่ได้แปรเปลี่ยนมาเป็นความขัดแย้งเฉพาะพื้นที่ หรือสงครามจำกัดขอบเขต ยุคสมัยของการใช้กำลังพลและยุทโธปกรณ์จำนวนมหาศาลเข้าทำการรบประชิดแบบตาต่อตาฟันต่อฟัน เพื่อแลกชีวิตกันในสนามรบ ไม่ว่าจะด้วยหอก ดาบ ธนู หรือปืนเล็กยาว ได้กลายเป็นประวัติศาสตร์ไปแล้ว ส่วนสงครามแห่งอนาคตนั้น จะทำการรบกันในระบบออนไลน์ ทุกวันนี้หากผู้นำประเทศตัดสินใจที่จะทำสงครามโดยใช้กำลังทหารและยุทโธปกรณ์ที่มี เข้าทำการโจมตีเป้าหมายทางทหารใดก็

ตาม ย่อมมีความเสี่ยงอย่างมหาศาลต่อผลกระทบที่จะเกิดขึ้น ทั้งทางการเมือง สิทธิมนุษย์ชน รวมถึงผลกระทบอื่น ๆที่ตามมาอีกมากมาย ดังนั้นในรัฐบาลของหลายๆประเทศ ได้เลือกที่จะเปลี่ยนมาทำสงคราไซเบอร์แทน ซึ่งการทำสงครามไซเบอร์นั้น มีข้อได้เปรียบที่สำคัญที่เหนือกว่า การใช้กำลังทหารหรือการใช้อาวุธทำลายร้ายแรงอื่น ๆ อย่างมากประการหนึ่งนั่นก็คือ การไม่เปิดเผยตัวตน (Anonymity) การใช้งานระบบคอมพิวเตอร์ออนไลน์ ผ่าน VPNs (Virtual Private Networks) TOR Networks หรือการเข้ารหัส ที่ซับซ้อน ย่อมทำให้ไม่สามารถถูกตรวจสอบระบุตัวตนได้โดยง่าย สมมุติว่า มีรัฐบาลของชาติใดชาติหนึ่ง หรือกลุ่มผลประโยชน์ที่ไม่ใช่รัฐ (Non-State Entities) กลุ่มใดกลุ่มหนึ่งมีขีดความสามารถในการโจมตีขนาดใหญ่และรุนแรงต่อระบบเครือข่ายคอมพิวเตอร์ต่อชาติที่เป็นปรปักษ์ โดยไม่เปิดเผยตัวและไม่สามารถถูกตรวจจับได้ จึงทำให้ฝ่ายตรงข้าม ไม่สามารถระบุได้ว่าใครเป็นผู้โจมตี ก็แน่นอนว่าไม่มีทางที่จะตอบโต้กลับไปได้ แต่ถึงกระนั้นก็ตามก็มักจะมีคำถามขึ้นมาเสมอว่า แล้วการโจมตีทางไซเบอร์ จะมีความรุนแรง หรือสร้างความเสียหายได้เทียบเท่ากับการใช้ ปืน กล รถถัง ขีปนาวุธ หรือแม้แต่ระเบิดนิวเคลียร์ได้หรือไม่ คำตอบก็คือ การโจมตีทางไซเบอร์สามารถสร้างความเสียหาย ได้อย่างมาก และกล่าวได้ว่าแนวโน้มของพลังอำนาจในการทำลายล้างนั้น อาจสูงกว่าอาวุธใด ๆในที่เคยมีมาในประวัติศาสตร์เลยทีเดียว อีกประการที่สำคัญมักเกิดการเข้าใจผิดคิดว่า การทำสงครามไซเบอร์นั้น เป็นสงครามแห่งอนาคต มีแต่ในหนังไซไฟเท่านั้น แต่แท้ที่จริงแล้ว สงครามไซเบอร์ได้ อุบัติขึ้นมาแล้วในยุคปัจจุบัน

ในปี ค.ศ.2010 ไวรัสคอมพิวเตอร์ได้เกือบจะเป็นชนวนในการก่อให้เกิดสงครามโลกครั้งที่ 3 โดยไวรัสที่มีชื่อว่า STUXNET[6] อาวุธทางไซเบอร์ตัวแรกของโลก ที่ถูกออกแบบมาเพื่อใช้โจมตีต่อนานาประเทศ ซึ่งเป้าหมายในครั้งนั้นคือประเทศอิหร่าน โดยอาศัยหลักการแพร่กระจายตัวเองในระบบเครือข่ายคอมพิวเตอร์ ไปจนถึงเป้าหมายที่แท้จริงนั่นก็คือโรงงานเก็บสารยูเรเนี่ยม ของประเทศอิหร่านที่มีชื่อว่า NATANZ ซึ่งเก็บรักษาสารยูเรเนี่ยมที่ใช้ในการพัฒนาอาวุธนิวเคลียร์จำนวนกว่า หกพัน ยูนิต ก่อนที่ STUXNET จะเริ่มจู่โจมด้วยคำสั่งทำลายนั้น STUNEX ได้แทรกซึมเข้าไปยังระบบประมวลผลกลาง (PLC Unit) ที่พัฒนาโดยบริษัท Siemens ซึ่งทำหน้าที่ในการควบคุมความเร็วการหมุนของถังบรรจุสารยูเรเนี่ยมให้อยู่ในระดับที่ปลอดภัยตลอดเวลา คือประมาณ 6300 รอบต่อนาที เมื่อ STUXNET สามารถแพร่กระจายเข้าไปในระบบ PLC Unit เรียบร้อยแล้ว เป็นเวลา 13 วันที่ STUXNET ฝังตัวอยู่เฉยๆ เก็บข้อมูลทุกอย่างในระบบ โดยไม่ถูกตรวจพบ หลังจากนั้น ได้เริ่มทำการเร่งความเร็วการหมุนของถังบรรจุยูเรเนี่ยมจนเกินเกณฑ์ปลอดภัย เป็นเวลา 15 นาที จากนั้นลดความเร็ว

ลงเหลือ 2 รอบต่อนาที เป็นเวลาอีก 15 นาที เช่นนี้สลับกันไป ส่งผลให้ท่อบรรจุยูเรเนี่ยม เกิดการแตกร้าว บิดงอ ฉีกขาดหรืออาจถึงขั้นเกิดการระเบิดได้ ผู้เชี่ยวชาญได้เปิดเผยว่า ในระหว่างที่ STUXNET ได้เร่งและลดความเร็วการหมุนอยู่นั้น STUXNET ได้ปล่อยข้อมูลการทำงานแบบปกติที่เก็บรวบรวมไว้ในช่วง 13 วันแรก เพื่อลวงให้วิศวกรที่เฝ้ามอนิเตอร์ติดตามสถานการณ์ทำงาน หรือระบบการตรวจสอบอัตโนมัติอื่นก็ตาม ไม่รู้ถึงความผิดปกติใด ๆ ที่เกิดขึ้น นอกจากนั้น STUXNET ยังสามารถยกเลิกการทำงานของปุ่มฉุกเฉิน ที่จะใช้ในการหยุดระบบเมื่อเกิดเหตุผิดปกติ โดยการโจมตีในครั้งนั้นได้สร้างความเสียหายต่อถังบรรจุยูเรเนี่ยมไปมากกว่า หนึ่งพันถัง ส่งผลให้สามารถชะลอแผนการพัฒนาอาวุธนิวเคลียร์ของประเทศอิหร่าน ได้สำเร็จ แต่ถึงกระนั้นทุกวันนี้ก็ยังไม่มีใครเปิดเผยตัว หรือออกมารับผิดชอบว่าเป็นผู้สร้าง STUXNET แต่ก็มีผู้เชี่ยวชาญจากบางสถาบันได้ออกมาสันนิษฐานว่าเป็นผลงานของรัฐบาลสหรัฐอเมริกา ในโครงการของ NSA ร่วมกับ GCHQ ของอังกฤษ และ UNIT 8200 ของกองทัพอิสราเอล ภายหลังจากการถูกโจมตีดังกล่าวทางฝั่งประเทศอิหร่านเองก็ไม่ได้นิ่งเฉยต่อการโจมตีนั้น ได้ดำเนินการรวบรวมแฮกเกอร์จากทั่วประเทศ ก่อตั้งหน่วยกองทัพไซเบอร์ ตอบโต้ด้วยการโจมตีระบบคอมพิวเตอร์ของบริษัทน้ำมัน Saudi Aramco หยุดยั้งการทำงานระบบออนไลน์แบ็งกิ้ง ของธนาคาร Bank of America ,PNC และ Wells Fargo ซึ่งอิหร่านก็ไม่ได้ออกมายอมรับเช่นเดียวกัน เปรียบเสมือนการบอกสหรัฐอเมริกาเป็นนัยว่า อิหร่านก็มีศักยภาพในการทำสงครามไซเบอร์เช่นเดียวกัน นับได้ว่านี่ก็คือสงครามไซเบอร์ที่เกิดขึ้นเป็นครั้งแรกระหว่าง 2 ประเทศในโลก

สิ่งที่น่ากลัวที่สุดของสงครามไซเบอร์ก็คือการโจมตีต่อระบบสาธารณูปโภค ที่สำคัญ ทำลายชีวิตและทรัพย์สินของประชาชนผู้บริสุทธิ์ เช่นแฮกเกอร์ทำให้รถไฟฟ้าตกราง เครื่องบินตกจากท้องฟ้า ระเบิดท่อแก๊สธรรมชาติ ทำลายระบบไฟฟ้า ประปา ขนส่งมวลชน การติดต่อสื่อสาร หรือการตัดขาดระบบธุรกรรมทางการเงิน เป็นเหตุให้เศรษฐกิจหยุดชะงัก การกระทำดังกล่าว สามารถสร้างความโกลาหล หวาดกลัว แก่มวลชนเป็นวงกว้างได้อย่างรวดเร็ว ดังนั้นการโจมตีจุดศูนย์ดุลทางทหารในสงครามปัจจุบัน อาจไม่ได้อยู่ที่การทำลายขีดความสามารถทางกำลังรบ ระบบการส่งกำลัง หรือแม้แต่ระบบการควบคุมบังคับบัญชาอีกต่อไป การสร้างความยอมรับหรือต่อต้านจากประชาชน หรือการเปลี่ยนความคิดของมวลชนและประชาคมโลกต่างหาก ที่สามารถส่งผลกระทบต่อผู้นำประเทศ รัฐบาล หรือแม้แต่องค์กรนานาชาติ สำหรับสร้างความชอบธรรมในการใช้การปฏิบัติการทางทหารเต็มรูปแบบ ซึ่งสามารถนำไปสู่การแพ้หรือชนะสงครามครั้งนั้นก็เป็นได้

ตามที่กล่าวมาทั้งหมดข้างต้นผู้วิจัยได้ชี้ให้เห็นถึงความสำคัญ อันเป็นรูปธรรมสำหรับมุมมองในด้านความมั่นคงทางทหารที่มีต่อการปฏิบัติการไซเบอร์ ซึ่งนับว่าเป็นเพียงส่วนน้อยเท่านั้น ตราบเท่าที่มนุษย์ได้นำเทคโนโลยี และขีดความสามารถทางไซเบอร์ มาประยุตก์ใช้งานในชีวิตประจำวันมากขึ้นเท่าใด รูปแบบของการปฏิบัติการไซเบอร์ทางทหาร ก็จะถูกพัฒนาและทวีความรุนแรงมากยิ่งขึ้นไปในทิศทางเดียวกัน คำถามชวนคิดประการหนึ่งก็คือแล้วกองทัพบกของไทยมีความพร้อมหรือมีขีดความสามารถเพียงพอแล้วหรือยัง ในการควบคุมห้วงมิติไซเบอร์ ต่อการปฏิบัติการทางทหารใดก็ตาม ที่อาจจะเกิดขึ้นได้ทุกเมื่อทั้งในปัจจุบันและอนาคต

<u>หน่วยงานด้านไซเบอร์ของประเทศไทย</u>

กองทัพบกได้ตระหนักถึงภัยอันตรายจากการสื่อสาร ที่เชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตของระบบเครือข่ายคอมพิวเตอร์นับล้านๆเครื่อง โดยได้เริ่มทำการศึกษาและเตรียมความพร้อมให้แก่กำลังพลเพื่อรับมือ กับการโจมตีทางไซเบอร์ โดย พลเอก ประยุทธ์ จันทร์โอชา อดีตผู้บัญชาการทหารบกในสมัยนั้น ได้มีนโยบาย และอนุมัติหลักการจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ขึ้นเพื่อปฏิบัติงานให้เป็นไปตามนโยบาย ของรัฐบาลโดยร่วมมือกับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security ; NCSC) โดยได้เริ่มทดลองปฏิบัติงานตั้งแต่ 1 ตุลาคม 2557 ซึ่งดำเนินงานไปพร้อมกับเหล่าทัพต่าง ๆ คือ กองบัญชาการกองทัพไทย กองทัพเรือ กองทัพอากาศ และสำนักงานตำรวจแห่งชาติ โดยมีกระทรวงกลาโหม ซึ่งเป็นองค์กรที่กำหนดนโยบายเพื่อเตรียมความพร้อมรับภัยคุกคามทางไซเบอร์ ในระยะเริ่มแรกจัดตั้งขึ้นที่ศูนย์เทคโนโลยีทางทหาร (ศทท.) ได้ดำเนินการปรับปรุงภารกิจและโครงสร้างการจัดหน่วยโดยได้เพิ่มเติมภารกิจ ด้านการปฏิบัติการสงครามไซเบอร์และปรับสายการบังคับบัญชาจากเดิมขึ้นตรงต่อกรมการทหารสื่อสาร มาเป็นหน่วยขึ้นตรงของกองทัพบก (นขต.ทบ.) เพื่อรองรับการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ซึ่งกระทบต่อความมั่นคงของชาติทั้งภายในและภายนอกประเทศ โดยเน้นหนักไปที่ความมั่นคงทางทหาร และการรักษาความสงบเรียบร้อยภายในประเทศ รวมทั้งการทำงานที่ประสานสอดคล้องกับหน่วยงาน ในเหล่าทัพอื่น และกระทรวงกลาโหม นอกจากนั้นยังได้ร่วมมือกับหน่วยงานของภาครัฐและภาคเอกชน ตลอดจน การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations ; NCO) ในปี 2559 ศูนย์เทคโนโลยีทางทหาร (ศทท.) ได้แปรสถานภาพหน่วยมาเป็นศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) มีฐานะเป็นหน่วยขึ้นตรงของกองทัพบกตั้งแต่ 1 ตุลาคม 2559 และเมื่อวันที่ 1

พฤศจิกายน 2559 พลเอก เฉลิมชัย สิทธิสาท ผู้บัญชาการทหารบกได้เปิดศูนย์ไซเบอร์กองทัพบกอย่างเป็นทางการ ซึ่งได้แบ่งโครงสร้างหน่วย เป็นสำนักงานผู้บังคับบัญชา กองธุรการ กองปฏิบัติการไซเบอร์ กองรักษาความปลอดภัยไซเบอร์ กองสนับสนุนปฏิบัติการข่าวสารไซเบอร์ โดยมีอำนาจหน้าที่ที่สำคัญได้แก่ กองปฏิบัติการไซเบอร์ ทำหน้าที่เป็นศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวัง แจ้งเตือน ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์ การเผชิญเหตุฉุกเฉินด้านไซเบอร์ตลอดจนการพัฒนา ขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุก เพื่อให้สามารถโต้ตอบและโจมตีฝ่ายตรงข้าม ได้ในกรณีจำเป็น ต่อมาคือ กองรักษาความมั่นคงปลอดภัยไซเบอร์ ทำหน้าที่เสริมสร้างความรู้ความเข้าใจ สร้างความตระหนักรู้ กำกับดูแลการปฏิบัติของหน่วยตามมาตรการการรักษาความมั่งคงปลอดภัย รวมถึงการเฝ้าระวัง แจ้งเตือนภัยคุกคาม การติดตาม สืบค้น และตรวจสอบช่องโหว่ของระบบ โดยใช้เครื่องมือตรวจหาการบุกรุก การกู้คืนสภาพเมื่อถูกโจมตี (Recovery) รวมถึงการดำเนินการพิสูจน์หลักฐานทางดิจิทัล และสุดท้ายคือ กองสนับสนุนการปฏิบัติการข่าวสารไซเบอร์ ทำหน้าที่ให้การสนับสนุนการปฏิบัติการข่าวสารของกองทัพบกและหน่วยที่เกี่ยวข้อง โดยเฝ้าระวัง แจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ที่ส่งผลกระทบ ต่อสถาบันและความมั่นคงของชาติ รวบรวม วิเคราะห์ทิศทาง แนวโน้ม โครงข่ายความสัมพันธ์ของข้อมูลประเภทสื่อและกลุ่มเป้าหมาย ติดตาม สืบค้น แหล่งที่มาและกำหนดมาตรการป้องปราม ตอบโต้ สกัดกั้นตลอดจนพัฒนาโปรแกรมและเครื่องมือต่าง ๆ เพื่อรองรับงานด้านไซเบอร์นอกจากนี้ยังได้เตรียมการพัฒนาเทคโนโลยีและนวัตกรรมต่าง ๆ โดยแสวงหาความร่วมมือกับหน่วยงานอื่นภายนอกกองทัพบก หน่วยงานภาครัฐ และองค์กรเอกชน ด้านวิชาการ การวิจัยพัฒนา (R&D) การสัมมนาเชิงปฏิบัติการ (Workshop) และการฝึกปฏิบัติต่าง ๆ โดยเฉพาะการฝึกซ้อมแผนเผชิญเหตุด้านไซเบอร์ (Cyber Incident Action Plan Exercise) การฝึกซ้อมแผนฉุกเฉินด้านไซเบอร์ (Cyber Emergency) รวมถึงการดำเนินคดีตามกฎหมายแก่ผู้ที่โจมตีระบบเครือข่ายคอมพิวเตอร์ของกองทัพบก [7]

หน่วยงานในระดับกระทรวงกลาโหม คือ ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม มีภารกิจเสนอข้อพิจารณา วางแผน อำนวยการ ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับนโยบายและยุทธศาสตร์ด้านไซเบอร์ นำนโยบายด้านไซเบอร์ระดับรัฐบาลไปสู่การปฏิบัติ สนับสนุนภารกิจด้านไซเบอร์เพื่อความมั่นคงของประเทศ ส่งเสริมและสนับสนุนการปฏิบัติการข้อมูลข่าวสารและความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งในและ

ต่างประเทศ การสนับสนุนหน่วยไซเบอร์ระดับปฏิบัติ ตลอดจนการปฏิบัติอื่นตามที่ได้รับมอบหมาย[8]

หน่วยงานระดับกองทัพไทย คือศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย ซึ่งมีภารกิจใกล้เคียงกับ ศูนย์ไซเบอร์ ของกระทรวงกลาโหมและศูนย์ไซเบอร์ของเหล่าทัพต่าง ๆ มีการจัดคือ กองธุรการ กองยุทธการและการข่าว กองวิทยาการ กองปฏิบัติการ และ กองรักษาความปลอดภัย

สำนักงานตำรวจแห่งชาติมีการจัดตั้ง กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี(ปอท.) เป็นหน่วยงานที่บังคับใช้กฎหมายที่มุ่งเน้นการอำนวยความยุติธรรม ป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี และบริการประชาชนอย่างมีมาตรฐานสากล เพื่อให้เกิดความสงบเรียบร้อย มั่นคง แก่ประชาชน สังคม และประเทศชาติ โดยมีภารกิจ ได้แก่ ถวายการรักษาความปลอดภัยสำหรับองค์พระมหากษัตริย์ พระราชินี และพระบรมวงศานุวงศ์ การป้องกันปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี อำนวยความยุติธรรมโดยยึดหลักนิติธรรม รักษาความสงบเรียบร้อยและความมั่นคงภายใน สนับสนุนการปฏิบัติงานของหน่วยงานอื่น ตลอดจนประสานความร่วมมือระหว่างหน่วยงานภายในประเทศและต่างประเทศ รับแจ้งเบาะแสจากประชาชน ให้คำปรึกษาแนะนำ รวบรวมสภาพปัญหา เพื่อเสนอแนะแนวทางในการป้องกันอาชญากรรมทางเทคโนโลยี และงานอื่นที่ได้รับมอบหมาย[9]

ในระดับประเทศมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือ Thai-CERT (Thailand Computer Emergency Response Team) มีพันธกิจสำคัญคือประสานงานกับหน่วยงานในเครือข่ายและหน่วยงานที่เกี่ยวข้องในการดำเนินการแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับแจ้ง สำหรับพันธกิจเชิงรุกให้ความสำคัญกับการพัฒนาทรัพยากรบุคคลเพื่อเพิ่มขีดความสามารถด้านการรักษาความมั่นคงปลอดภัย และสร้างความร่วมมือกับหน่วยงานทุกประเภททั้งในและต่างประเทศในการแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร การสร้างความร่วมมือระหว่างประเทศผ่านเวที FIRST (Forum of Incident Response and Security Teams) และเวที APCERT (Asia Pacific CERT) สำหรับความร่วมมือกับประเทศในภาคพื้นเอเชียแปซิฟิก ด้านการพัฒนาทรัพยากรบุคคล ให้ความสำคัญกับการเผยแพร่ความรู้และข้อมูลข่าวสารเกี่ยวกับ

การรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อเป็นการสร้างภูมิคุ้มกันเบื้องต้นทางด้านไอที และจัดอบรมสัมมนาให้กับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์เฉพาะกลุ่มที่มีความต้องการข้อมูลข่าวสารเป็นการเฉพาะ นอกจากนี้เพื่อให้เกิดความเข้าใจและได้ลงมือปฏิบัติ ยังจัดและร่วมในกิจกรรมซักซ้อมการรับมือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารกับหน่วยงานทั้งในประเทศและต่างประเทศอีกด้วย[10]

ถึงแม้ว่าประเทศไทยจะมีหน่วยงานด้านความมั่นคงทางไซเบอร์หลายหน่วยงาน แต่ก็ยังไม่มีหน่วยงานใดเป็นหน่วยงานรับผิดชอบหลักของรัฐบาลในการบูรณาการเป็นส่วนรวม การปฏิบัติยังคงเป็นการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานของตนเองเป็นหลัก ซึ่งหากเกิดปัญหาหรือถูกโจมตี ก็เป็นหน้าที่ของหน่วยงานนั้น จะต้องเป็นผู้รับผิดชอบตนเอง ส่วนงานด้านสงครามไซเบอร์นั้น กรอบความคิดของหน่วยงานไซเบอร์ทางทหารทั้งในระดับกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพต่างๆ ได้ให้น้ำหนักไปในเชิงการรักษาสมดุล ระหว่างการดำรงขีดความสามารถของเครือข่ายกับการรักษาความปลอดภัยของเครือข่าย ซึ่งก็คือการป้องกันและรักษาความปลอดภัยในระบบคอมพิวเตอร์และข้อมูลของตนเองเป็นอันดับแรก และต่อมาก็คือแนวคิดเรื่องการป้องกันเชิงรุก (Proactive Cyber Defense) หรือการตอบโต้ภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อให้ลดความเสียหายหรือติดตามตัวผู้กระทำความผิด ส่วนแนวคิดที่จะใช้หน่วยรบไซเบอร์เป็นเครื่องมือในการโจมตี หรือสนับสนุนการปฏิบัติในสงครามแบบผสม (Hybrid War) ยังไม่มีข้อมูลปรากฏชัด ทั้งนี้อาจเป็นเพราะประเทศไทยยังอยู่ในช่วงเริ่มต้นของการดำเนินการตามนโยบายของรัฐบาล และยุทธศาสตร์ด้านไซเบอร์ป้องกันประเทศ ซึ่งอยู่ในขั้นตอนของการพัฒนาไปสู่กรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยของไซเบอร์ อีกทั้งหน่วยยังประสบปัญหาขาดแคลนบุคคลกรที่มีขีดความสามารถที่เพียงพอในทุกระดับ ทั้งในระดับบริหาร ระดับอำนวยการ และระดับการปฏิบัติการไซเบอร์ อีกด้วย

<u>แนวความคิดในการพัฒนานักรบไซเบอร์ของชาติต่าง ๆ</u>

ข้อมูลที่เกี่ยวกับการเสริมสร้างและพัฒนานักรบไซเบอร์ของประเทศต่างๆมีทั้งข้อมูลแบบที่เปิดเผยได้ในสื่อสาธารณะ และข้อมูลปิดลับที่ได้มาจากการคาดการของนักวิชาการ ผู้เชี่ยวชาญแขนงต่าง ๆ รวมถึงสื่อมวลชน ในเรื่องของข้อมูลเกี่ยวกับการจัดตั้งหน่วย และเสริมสร้างกำลังนักรบไซเบอร์ รวมไปถึงคุณลักษณะ ขีดความสามารถ และจำนวนนักรบไซเบอร์ที่แท้จริงของแต่ละประเทศว่ามีมากหรือน้อยเพียงใด บางครั้งยังมีการตั้ง

ข้อสังเกตว่า กลุ่มแฮกเกอร์ หรือองค์กรลับบางแห่งอาจจะได้รับการสนับสนุนจากรัฐบาลของบางประเทศ ให้ทำการปฏิบัติการไซเบอร์ หรือการโจมตีครั้งสำคัญในเหตุการณ์บางอย่าง แต่กระนั้นก็ยังไม่เคยมีประเทศใด หรือกลุ่มหนึ่งกลุ่มใด ออกมายอมรับว่าเป็นผู้ให้การสนับสนุนหรือรับผิดชอบต่อเหตุการณ์ต่างๆที่เกิดขึ้น ซึ่งในมิติทางไซเบอร์มีความแตกต่างจากมิติทางกายภาพ ที่สำคัญประการหนึ่งก็คือ การทำสงครามไซเบอร์นั้นไร้พรมแดน การต่อสู้ในมิติของไซเบอร์ระหว่างประเทศ ไม่จำเป็นต้องมีเขตแดนที่ติดกัน ไม่จำเป็นต้องเคลื่อนย้ายกำลัง มาใกล้กัน ดังนั้นปัจจัยการวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ สำหรับประเทศในภูมิภาคเดียวกัน หรือประเทศอื่นๆที่อยู่ห่างไกลออกไป ก็มีโอกาสเป็นภัยคุกคามทางไซเบอร์ได้ไม่ต่างกัน

แนวความคิดในการพัฒนาเสริมสร้างกำลังทางทหารให้มีขีดความสามารถด้านไซเบอร์ ของกองทัพประเทศต่างๆ ทั่วโลก หลายประเทศให้ความสำคัญกับการพัฒนาหรือจัดหาเครื่องมืออุปกรณ์และเทคโนโลยีที่ทันสมัย บางประเทศให้ความสำคัญด้านการจัดตั้งองค์กร บางประเทศให้ความสำคัญกับการพัฒนาบุคลากรที่มีอยู่ในกองทัพ บางประเทศใช้วิธีการรับสมัครจากบุคคลพลเรือน หรือกำลังพลสำรองเพื่อเข้ามาเป็นนายทหารไซเบอร์ หรือรับสมัครทหารเกณฑ์ไซเบอร์แบบตรง ๆก็มี สำหรับประเทศที่ให้ความสำคัญกับการพัฒนาเครื่องมือ อุปกรณ์ การค้นคว้าเทคโนโลยีและสร้างนวัตกรรมที่ทันสมัยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มักเป็นประเทศที่มีความเจริญก้าวหน้าและมีการพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสารมาก่อน จึงสามารถพัฒนาต่อยอดองค์ความรู้ ความเชี่ยวชาญ และประสบการณ์ยิ่งขึ้นไป ทำให้มีศักยภาพในการพัฒนาอย่างต่อเนื่อง ทั้งเพื่อความมุ่งหมายเชิงธุรกิจและเชิงการทหาร ส่วนประเทศที่ให้ความสำคัญกับเสริมสร้างขีดความสามารถด้านไซเบอร์ ด้วยการจัดหาเครื่องมืออุปกรณ์และเทคโนโลยีที่ทันสมัย มักเป็นประเทศที่กำลังพัฒนา หรือประเทศด้อยพัฒนา แต่มีความจำเป็นในการเสริมสร้างขีดความสามารถด้านไซเบอร์ จึงให้น้ำหนักกับการลงทุนใช้จ่ายงบประมาณในด้านนี้เพิ่มขึ้น[11]

ประเทศที่ให้ความสำคัญด้านการจัดตั้งองค์กรหรือหน่วยงานด้านไซเบอร์ทางทหาร มักเป็นประเทศที่มีบทบาทสำคัญทางด้านเศรษฐกิจ การค้าและการทำธุรกรรมแบบอิเล็กทรอนิกส์ ซึ่งมีความจำเป็นในการใช้การปฏิบัติการทางทหารในโลกไซเบอร์ จึงจัดตั้งองค์กรหรือหน่วยงานด้านไซเบอร์ทางทหารเป็นการเฉพาะเพื่อรับมือกับภัยคุกคามด้านไซเบอร์โดยตรง แม้บางประเทศการจัดตั้งหน่วยงานด้านไซเบอร์ทางทหาร อาจจะยังไม่มีขีดความสามารถและประสิทธิภาพที่เพียงพอต่อการรับมือกับภัยคุกคามด้านไซเบอร์ได้เท่าที่ควร

แต่ก็ถือว่าเป็นจุดเริ่มต้นของการพัฒนาเสริมสร้าง เพื่อการรับมือกับภัยคุกคามด้านไซเบอร์ในอนาคต สำหรับประเทศที่เน้นการเพิ่มขีดความสามารถด้านไซเบอร์ของกำลังพล นับว่าเป็นความท้าทายด้านการพัฒนาบุคลากรของกองทัพอย่างมาก ด้วยปัจจัยที่เป็นปัญหาและอุปสรรคอันสำคัญเนื่องมาจากพื้นฐานความรู้ ความชำนาญ ความเชี่ยวชาญ และประสบการณ์ จึงต้องมีการลงทุนงบประมาณด้านการพัฒนาบุคลากรค่อนข้างสูง เนื่องจากค่าใช้จ่ายในการศึกษาอบรมวิทยาการด้านนี้ค่อนข้างแพง ผู้ที่มีความรู้ ความชำนาญ ความเชี่ยวชาญ และประสบการณ์ จึงมักถูกชักชวนให้เข้าทำงานในองค์กรภาคธุรกิจเอกชนเป็นหลัก ด้วยอัตราค่าตอบแทนสูง เพื่อให้เกิดผลต่อความมั่นคงปลอดภัย ความต่อเนื่อง และความเชื่อมั่นในทางธุรกิจ ดังนั้นหากกองทัพบกจะยอมลงทุนด้วยงบประมาณจำนวนมากเพื่อพัฒนาบุคคลากรของตนในด้านนี้แล้ว อาจต้องประสบกับความเสี่ยงต่อปัญหาสมองไหลไปสู่ภาคธุรกิจเอกชน ที่มีสิ่งตอบแทนและแรงจูงใจที่ดีกว่ากองทัพ

ประเทศสหรัฐอเมริกา ได้จัดตั้งกองบัญชาการไซเบอร์ หรือ United States Cyber Command (USCYBERCOM) ซึ่งเป็นหน่วยในสังกัดของกระทรวงกลาโหมสหรัฐอเมริกา เป็นหน่วยบัญชาการร่วมทางไซเบอร์ (Joint service to Cyber Command) มีภารกิจในการระดมสรรพกำลังด้านไซเบอร์จากทุกภาคส่วนเพื่อผนึกกำลังในการทำสงครามทุกรูปแบบ เป็นศูนย์กลางการบังคับบัญชาในยุทธการไซเบอร์ เสริมสร้างความเข้มแข็งของขีดความสามารถทางไซเบอร์กระทรวงกลาโหม โดยเริ่มก่อตั้งในปี ค.ศ 2009 มีหน่วยในการบังคับบัญชาประกอบด้วย กองบัญชาการไซเบอร์กองทัพบก (Army Cyber Command) กองบัญชาการไซเบอร์กองทัพเรือ (Fleet Cyber Command/Tenth Fleet) กองบัญชาการไซเบอร์กองทัพอากาศ (Air Forces Cyber/Twenty-Fourth Air Force) และกองบัญชาการไซเบอร์นาวิกโยธิน (Marine Corps Cyberspace Command) จากการสถาปนาหน่วยงานไซเบอร์ของสหรัฐอเมริการนี้ทำให้ประเทศต่าง ๆ ริเริ่มจัดตั้งหน่วยงานและพัฒนานักรบไซเบอร์ของตนขึ้นเช่นเดียวกัน อาทิ เกาหลีใต้ จัดตั้งกองบัญชาการสงครามไซเบอร์ เพื่อตอบโต้กับหน่วยไซเบอร์ของเกาหลีเหนือ นาโต้จัดตั้งศูนย์ความร่วมมือทางไซเบอร์ NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) ประเทศเยอรมันมีศูนย์ป้องกันทางไซเบอร์แห่งชาติ (National Cyber defense Centre) เป็นต้น[12]

สำหรับประเทศในภูมิภาคอาเซียน ก็มีความตื่นตัวและเร่งพัฒนานักรบไซเบอร์ของตนเองให้พร้อมในการปฏิบัติในมิติที่ห้านี้ เช่นเดียวกัน อาทิ สำนักงานไซเบอร์และการเข้ารหัสแห่งชาติ ของอินโดนีเซีย[13] ได้เตรียมการเพิ่มตำแหน่งต่าง ๆ ด้านความมั่นคงทางไซ

เบอร์สำหรับบุคลากรที่มีอยู่ และยังต้องการอีกเพิ่มอีกเป็นจำนวนมาก จึงวางแผนที่จะสรรหาบุคลากรจำนวนหลายร้อยคนในเร็วๆนี้ ซึ่งรวมถึงผู้จบการศึกษาจากสถาบันด้านเทคโนโลยีภายในประเทศและผู้ที่มีความเชี่ยวชาญทางไซเบอร์ที่มีคุณสมบัติครบถ้วนตามต้องการ ส่วนอีกประเทศหนึ่งที่น่าสนใจคือ เวียดนาม ได้ประกาศจัดตั้ง กองบัญชาการปฏิบัติการไซเบอร์สเปซ เมื่อเดือน มกราคม 2561 เพื่อปกป้องคุ้มครองอธิปไตยของประเทศบนโลกอินเทอร์เน็ต โดยนายกรัฐมนตรีของเวียดนามได้อ้างถึงความเสี่ยงในทะเลจีนใต้ และสถานการณ์ในภูมิภาคและโลกที่มีความซับซ้อน หน่วยสงครามไซเบอร์ของเวียดนามที่เพิ่งได้รับการเปิดเผยนี้ มีชื่อว่า กองกำลัง-47 (Force-47) ประกอบด้วย ทหารและพลเรือนที่เชี่ยวชาญด้านคอมพิวเตอร์กว่า 10,000 คน ขณะนี้ได้เริ่มปฏิบัติงานแล้วในหลายภาคส่วน[14] สำหรับประเทศสิงคโปร์ โดยรัฐมนตรีว่าการกระทรวงกลาโหมสิงคโปร์ ประกาศว่า ทางกระทรวงกลาโหมเตรียมจัดตั้งศูนย์บัญชาการไซเบอร์ เพื่อยกระดับมาตรการสกัดการโจมตีออนไลน์ ศูนย์แห่งใหม่นี้จะมีชื่อว่า Defense Cyber Organization (DCO) ซึ่งทำหน้าที่กำหนดมาตรการและยุทธศาสตร์ด้านความมั่นคงทางไซเบอร์ ยกระดับศักยภาพด้านการป้องกันทางไซเบอร์ของกองทัพ และสนับสนุนการทำงานของสำนักงานความมั่นคงทางไซเบอร์แห่งสิงคโปร์นอกจากนี้ยังจะมีการจัดตั้งคณะทำงานด้านการป้องกันทางไซเบอร์ด้วย โดยจะแยกหน่วยปฏิบัติงานเป็น 2 ส่วน เพื่อตรวจสอบเครือข่ายของกองทัพสิงคโปร์ (SAF) และศูนย์ทดสอบและประเมินด้านไซเบอร์ตลอด 24 ชม. กระทรวงกลาโหมสิงคโปร์หวังที่จะฝึกฝนกลุ่มผู้ป้องกันทางไซเบอร์ประมาณ 2,600 ราย ซึ่งคัดเลือกมาจากบุคคลที่ทำหน้าที่รับใช้ประเทศเพื่อให้พร้อมทำหน้าที่ดังกล่าวในในทศวรรษหน้า[15]

<u>แนวทางการเสริมสร้างและพัฒนานักรบไซเบอร์ของประเทศไทย</u>

สำหรับประเทศไทยในระดับชาติ พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี ได้มีนโยบายในการสร้างความมั่นคงปลอดภัยทางไซเบอร์ โดยรัฐบาลได้ตั้งเป้าผลิตนักรบไซเบอร์ จำนวน 1,000 คน ในปี 2561 เพื่อ เฝ้าระวัง รักษาความปลอดภัย แก้ปัญหาหากมีสิ่งผิดปกติเกิดขึ้นในโลกไซเบอร์ทั้งหมด[16] ในระดับกระทรวงกลาโหม ได้มอบนโยบายในการประชุมสภากลาโหมว่า สงครามไซเบอร์ ถือเป็นอีกมิติหนึ่งของการสงครามที่มีความไวสูง โดยต้องมีการเตรียมกำลังและใช้กำลัง เช่นเดียวกับมิติสงครามอื่นๆจึง สั่งการให้ หน่วยขึ้นตรงกระทรวงกลาโหมและเหล่าทัพ ได้ให้ความสำคัญ ในการเร่งรัดเดินหน้าขับเคลื่อนปฏิรูปกองทัพ ตามแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม ในระยะที่ 1 พ.ศ.

2560 – 2564 ที่ต้องเสริมสร้างความสมบูรณ์ ของหน่วยระดับนโยบายและหน่วยปฏิบัติ โดยเฉพาะ การพัฒนากำลังพล โครงสร้างพื้นฐานและเทคโนโลยี ให้มีความพร้อมปฏิบัติในมิติไซเบอร์ ควบคู่ไปกับ การสร้างความร่วมมือด้านไซเบอร์ ทั้งในและต่างประเทศ ให้ห้วง 3 ปีที่ผ่านมากระทรวงกลาโหม ได้ขับเคลื่อนปฏิรูปกองทัพ ด้านไซเบอร์มาโดยต่อเนื่อง สอดรับกับยุทธศาสตร์ชาติ (ด้านความมั่นคง) และยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม

คณะทำงานด้านเทคโนโลยีสารสนเทศ กิจการอวกาศ และไซเบอร์ ได้เสนอแนวความคิดในการนำขีดความสามารถผู้เชี่ยวชาญไซเบอร์พลเรือน ด้วยการ ใช้ สรรพกำลังด้านไซเบอร์ (Cyber Mobilization)[17] เป็น การระดมสรรพกำลัง กำลังสำรอง กำลังพลสำรอง และบุคคลพลเรือนชาย-หญิง ที่มีความรู้ ความสามารถ ความเชี่ยวชาญ มีประสบการณ์ปฏิบัติงาน หรือ ผู้ที่มีความสนใจ งานด้านเทคโนโลยีสารสนเทศและการสื่อสาร งานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การปฏิบัติการทางไซเบอร์ และการปฏิบัติการข่าวสาร เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามด้านไซเบอร์ และเป็นศูนย์กลางการแลกเปลี่ยนความรู้ ประสบการณ์ บทความ ข้อมูลข่าวสาร แจ้งเตือนภัย ตลอดจนการแสดงความคิดเห็นต่าง ๆ ที่เกี่ยวข้อง สำหรับแนวความคิดของ สรรพกำลังด้านไซเบอร์ เป็นการแก้ไขปัญหาความขาดแคลนบุคลากรด้านไซเบอร์ของหน่วยงานความมั่นคง ซึ่งประสบปัญหาในด้านข้อจำกัดเกี่ยวกับระเบียบและกฎเกณฑ์เรื่องค่าจ้าง ค่าตอบแทนในระบบราชการ ที่ต่ำกว่าภาคเอกชนพลเรือน ทำให้ไม่สามารถสร้างแรงจูงใจให้ผู้ที่มีความรู้ ความสามารถในด้านไซเบอร์หันมาสนใจบรรจุในระบบราชการ รวมถึงปัญหาความสูญเปล่าในการผลิต และการบรรจุใช้งานของกำลังสำรอง ที่ไม่ตรงกับคุณวุฒิความรู้ความสามารถ เช่น ผู้ที่จบการศึกษาระดับปริญญาโท ปริญญาเอก ในสาขาวิชาการที่เกี่ยวข้องกับงานด้านไซเบอร์ แต่จับสลากเกณฑ์ทหารได้ใบดำ บรรจุเป็นกองหนุนในตำแหน่ง พลทหาร หรือ นายทหารชั้นประทวน ที่บรรจุในหน่วยกำลังรบ หน่วยสนับสนุนการรบ หน่วยสนับสนุนการช่วยรบ ตามแผนป้องกันประเทศ

ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย ใช้วิธีการรับสมัครบุคคลพลเรือน เข้ารับราชการทหารในตำแหน่งเจ้าหน้าที่ปฏิบัติการด้านเทคนิค โดยทำการทดสอบให้เจาะระบบเพื่อดึงข้อมูลที่ซ่อนไว้ในระบบ พิสูจน์หลักฐานดิจิทัลเพื่อหาข้อมูลตามที่โจทย์กำหนด ทดสอบเขียนโปรแกรม ส่วนฝั่ง security audit เป็นการทดสอบความรู้มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ISO 27000 และทดสอบสมรรถภาพร่างกายตามเกณฑ์ของการรับราชการ โดยมี อัตราเงินเดือนสำหรับปริญญาตรี 15,000 บาท ปริญญาโท 17,550 บาท และปริญญาเอก 21,140 บาท[18] ซึ่งในครั้งนั้นมีผู้มาสมัครคัดเลือกประมาณ 300 คน ผล

การทดสอบ ส่วนใหญ่จะไม่ผ่านเกณฑ์ 50 % ซึ่งเมื่อรับบรรจุเข้ารับราชการแล้ว จำเป็นต้องอบรมเพิ่มเติมและทดลองปฏิบัติงานอีกไม่ต่ำกว่า 1-2 ปี ทั้งนี้ก็ยังไม่สามารถประกันได้ว่ากำลังพลดังกล่าวจะมีขีดความสามารถและคุณลักษณะอันพึงประสงค์ตามที่ต้องการหรือไม่

<u>ทำไมต้องเน้นที่ปฏิบัติการเชิงรุก</u>

คำว่านักรบไซเบอร์(Cyber Warriors)[19] เป็นศัพท์ที่ถูกเรียกขึ้นมาเป็นการเฉพาะกิจ เนื่องจากเป็นคำยืมมาจากภาษาต่างประเทศ และยังมิได้มีการนิยามหรือบัญญัติให้เป็นศัพท์ทางราชการมาก่อน โดยในความหมายของนักรบไซเบอร์ที่ได้มีการให้คำจำกัดความตามพจนานุกรมก็คือ *“เป็นผู้ที่มีความเชี่ยวชาญทางคอมพิวเตอร์ที่สามารถเจาะผ่านเข้าไปในระบบดิจิตอลเพื่อดึงข้อมูล เปลี่ยนแปลง เข้าควบคุม หรือบ่อนทำลาย และในทางกลับกัน ก็สามารถป้องกันและตอบโต้จากการถูกโจมตีระบบจากภายนอกด้วย ทั้งนี้เพื่อผลประโยชน์ทางการเมือง หรือเพื่อให้เกิดความได้เปรียบทางทหาร”* ซึ่งผู้ที่มีขีดความสามารถหรือทักษะในระดับนี้ ก็จะถูกเรียกด้วยชื่อต่าง ๆกันออกไป ขึ้นอยู่กับหน่วยงานที่บุคคลนั้นที่สังกัด หรือจุดประสงค์งานที่ทำ ตัวอย่างเช่น นักทดสอบการเจาะระบบเครือข่าย (Penetration testers หรือ Pentesters) มีหน้าที่ทดสอบ ค้นหา ช่องโหว่ของระบบ ที่อาจถูกโจมตีจากภายนอกได้ให้กับเจ้าของระบบหรือบริษัทที่เป็นนายจ้าง หรือ นักล่าเงินรางวัล (Bug Bounty Hunters) คือผู้ที่เข้าร่วมกับโปรแกรมที่ทางเจ้าของระบบหรือเว็บไซต์เปิดให้บุคคลทั่วไปเข้ามาแฮกระบบของตน เพื่อแจ้งช่องโหว่ที่พบให้แก่เจ้าของระบบจะได้ป้องกันก่อนถูกโจมตีจริง ๆ เพื่อแลกกับเงินรางวัล หรือสิ่งของ นอกจากนั้นยังหมายรวมไปถึง แฮกเกอร์ สายคุณธรรม (Ethical Hackers หรือ White Hat Hackers) และ กลุ่มแฮกเกอร์ ที่กระทำผิดกฎหมาย (Black Hat Hackers) ล้วนแต่มีทักษะในลักษณะทำนองเดียวกัน ดังนั้นหากบุคคลเหล่านี้นำความสามารถไปใช้เพื่อผลประโยชน์ทางการเมือง หรือการทหาร ก็สามารถเรียกได้ว่า เป็นนักรบไซเบอร์นั่นเอง

เนื่องจากลักษณะของโลกไซเบอร์เป็นมิติที่สร้างมาจากระบบดิจิตอล จึงมีความแตกต่างจากโลกทางกายภาพอย่างสิ้นเชิง และเมื่อนำมาใช้เป็นมิติทางการทหารแล้ว หลักนิยมทางไซเบอร์ จึงไม่สามารถนำเอาหลักนิยมของมิติทางทหารอื่นเช่น หลักนิยมทางบก เรือ อากาศ มาปรับใช้ได้กับมิติไซเบอร์ คุณลักษณะอันพึงประสงค์ของนักรบไซเบอร์ก็คือ ขีดความสามารถในการค้นหาช่องโหว่ของระบบ เพื่อใช้ช่องโหว่นั้นในการเข้าถึงข้อมูลสำคัญหรือควบคุมระบบคอมพิวเตอร์นั้นเสียเองซึ่งเป็นคุณสมบัติเชิงรุก ส่วนด้านการป้องกันนั้น ก็คือนำเอาคุณสมบัติเชิงรุกมาทำการค้นหาช่องโหว่ ของระบบตัวเอง โดยผู้ที่จะทำการแก้ไข

(Patch) เพื่อปิดช่องโหว่ได้นั้นก็คือเจ้าของระบบ หรือผู้สร้างแอพพลิเคชั่นนั่นเอง สำหรับช่องโหว่ของระบบ ที่เจ้าของระบบยังไม่สามารถค้นพบ ที่เรียกว่า Zero day Vulnerability ซึ่งอันตรายมาก เพราะกว่าที่เจ้าของระบบจะรู้ ก็คือเมื่อถูกโจมตีแล้วเท่านั้น ส่วนความสามารถในการตอบโต้ และลดความเสียหายให้น้อยที่สุด เพื่อให้ระบบสามารถทำงานต่อไปได้ ก็นับเป็นอีกคุณสมบัติหนึ่งที่สำคัญของนักรบไซเบอร์ ที่จะต้องทำงานร่วมกับผู้ดูแลระบบ สำหรับการให้คำนิยามจากรัฐบาล หรือหน่วยงานที่เกี่ยวข้องของนักรบไซเบอร์ ว่าให้ทำหน้าที่ในการเฝ้าระวังและรักษาความปลอดภัยทางด้านอินเทอร์เน็ต เป็นหลัก ซึ่งการชี้แจงต่อสื่อมวลชนลักษณะนี้ผู้วิจัยเข้าใจว่าเพื่อลดความหวาดระแวงของสังคม เพราะการที่มีนักรบไซเบอร์ที่มีขีดความสามารถเชิงรุก เป็นเครื่องมือสนับสนุนรัฐบาลอยู่นั้น อาจทำให้ประชาชนเกิดความวิตกกังวลถึงสิทธิเสรีภาพของตนและการเข้าถึงข้อมูลส่วนบุคคลจากรัฐบาลได้

<u>ทางออกของปัญหาการขาดแคลนบุคคลกร</u>

การพัฒนาศักยภาพของบุคคลกรด้านความมั่นคงไซเบอร์ พบว่าเป็นปัญหาใหญ่ทั่วโลก เนื่องจากองค์กรหรือ ภาครัฐ ไม่สามารถผลิตและพัฒนาบุคคลได้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี ที่เติบโตแบบก้าวกระโดด และไม่เพียงแต่ภาครัฐเท่านั้นที่ต้องการบุคคลากรดังกล่าว ภาคธุรกิจ เอกชน หรือรัฐวิสาหกิจเอง ก็มีความต้องการด้วยเช่นกัน และยังสามารถให้ข้อเสนอหรือค่าตอบแทนที่สูงกว่าของภาครัฐ หรือหน่วยงานความมั่นคงอีกด้วย ดังนั้นในส่วนของกองทัพบก ผู้วิจัยจึงขอเสนอโมเดลทางออกของการแก้ปัญหา ดังต่อไปนี้

1 ขุนพลของนักรบไซเบอร์ต้องเป็นนักรบไซเบอร์ เปรียบดัง แม่ทัพนายกองทหารที่นำไพล่พลกรีฑาทัพเข้าสู่สมรภูมิรบ ควรจะต้องเป็นนายทหารที่เชี่ยวชาญการศึกสงคราม หากสมมุติว่าผู้บังคับบัญชาเลือกที่จะใช้นักปราชญ์ผู้ทรงปัญญา นักบวชที่น่าเลื่อมใส หรือนักกีฬาผู้เข้มแข็ง นำทัพแทนนายทหารผู้นั้น จริงอยู่ว่าคนเหล่านั้นอาจจะเป็นคนเก่งในสาขาวิชาชีพของตน แต่ถ้าในเรื่องการรบแล้ว นายทหารที่มีประสบการณ์ด้านการรบ ย่อมมีโอกาสนำชัยชนะได้มากกว่า เฉกเช่นเดียวกับหน่วยงานด้านไซเบอร์ ผู้บังคับหน่วย ฝ่ายอำนวยการหลัก หรือแม้แต่นายทหารหัวหน้าชุด ก็มีความจำเป็นที่จะต้องมีทักษะด้านไซเบอร์ที่ดีเพียงพอ จึงจะกำหนดวิสัยทัศน์ และนำพาชุดปฏิบัติการหรือนักรบไซเบอร์ของหน่วยให้บรรลุภารกิจได้ แต่เนื่องจากระบบราชการ หรือระบบอาวุโส ทำให้บางครั้งผู้นำทัพไซเบอร์ อาจถูกคัดเลือกมาจากนักรบในจังหวัดชายแดนภาคใต้ หรือนักบัญชีที่เชี่ยวชาญระบบการเงิน แต่มีความอาวุโสเหมาะสม มาทำหน้าที่นำทัพไซเบอร์ สิ่งที่อยากนำเสนอแก่กองทัพบกก็คือ ยังมีบุคคลกรในกองทัพบกที่มีความชอบ (Passion) หรือสนใจใฝ่รู้ศึกษาด้วยตนเอง กระจายอยู่ตามภูมิภาค

ต่างๆ หลายคนมีความสามารถในระดับที่ทำงานด้านความมั่นคงทางไซเบอร์ให้กับองค์กรภาคธุรกิจเอกชนเลยทีเดียว กองทัพบกจึงต้องแสวงหาบุคคลเหล่านี้ให้เจอ และให้ข้อเสนอที่ดี ดึงเข้ามาร่วมสร้างความเข้มแข็งให้กับหน่วยในช่วงเริ่มก่อตั้ง วิธีการแสวงหาบุคคลเหล่านี้ ก็ด้วยการจัดกิจกรรม จัดอบรม หรือการแข่งขันทางไซเบอร์ ซึ่งบุคคลที่มีความสนใจ หรือชอบในด้านนี้ ก็มักจะมาร่วมด้วยเสมอ โดยจัดให้มีชุดสังเกต สัมภาษณ์ ทดสอบความสามารถและทาบทาม ชักชวนเข้าร่วมงานต่อไป

2 สร้างนายทหารหลักไซเบอร์ ถ้ายอมรับว่าสงครามไซเบอร์ คือภัยคุกคามแห่งอนาคตแล้ว หน่วยงานไซเบอร์ทหาร ก็ต้องพัฒนาไปสู่จุดนั้นเช่นกัน ถ้ากองทัพบกมีความต้องการนายทหารไซเบอร์ (Cyber Officers) ที่มีขีดความสามารถสูง พร้อมรับมือกับภัยคุกคามทางไซเบอร์ทุกรูปแบบในวันข้างหน้า ก็ต้องเริ่มสร้างตั้งแต่วันนี้ ตัวอย่างเช่นกองทัพบกสหรัฐอเมริกา เปิดหลักสูตรไซเบอร์ เพื่อสอนให้กับนักเรียนนายร้อย West Point เพื่อจบออกมาเป็นนายทหารเหล่าไซเบอร์ และมีโรงเรียนไซเบอร์กองทัพบก(U.S. Army Cyber School) ที่ผลิตนายทหารสัญญาบัตร จากพลเรือน เพื่อเป็นทหารประจำการ (Active Duty Officers) ในชั้นยศร้อยโท[20] ดังนั้นผู้วิจัยจึงเสนอให้ โรงเรียนนายร้อยพระจุลจอมเกล้า เปิดหลักสูตรด้าน Cyber Security ให้กับนักเรียนนายร้อย และกองทัพบกต้องกำหนดแนวทางรับราชการให้กับเขาเหล่านั้นให้มีความเจริญก้าวหน้าอย่างชัดเจน ตามลำดับและมีผลตอบแทนพิเศษที่ดีพอ ที่จะไม่ทำให้ถูกซื้อตัวโดยบริษัทเอกชนหรือหน่วยงานอื่นในอนาคต

3 คัดสรรบุคคลที่มีความสามารถเข้าหน่วย แนวทางการคัดสรรบุคคลเข้าบรรจุเป็นข้าราชการโดยการสอบคัดเลือก เป็นวิธีหนึ่งที่ใช้ในหลายๆหน่วยใช้ การกำหนดเกณฑ์มาตรฐานเป็นเรื่องสำคัญว่าหน่วยต้องการนักรบไซเบอร์ในแต่ละระดับ ด้วยมาตรฐานอย่างไร แต่ต้องพึงระวังเรื่องการรับบุคคลบรรจุเข้ารับราชการแล้ว หากมีคุณสมบัติไม่เพียงพอ ก็จะต้องเป็นภาระของหน่วย หรือกองทัพในการปรับไปทำงานอื่นต่อไป สูญเสียอัตราตำแหน่งที่ควรจะได้บรรจุให้กับผู้ที่มีคุณสมบัติเหมาะสม สำหรับแนวคิดการระดมสรรพกำลังด้านไซเบอร์ของกระทรวงกลาโหม ก็เป็นวิธีหนึ่งที่น่าสนใจ แต่ที่ผ่านมาการระดมสรรพกำลังทางทหารหรือการใช้ทหารกองหนุน ยังเป็นเพียงขั้นการฝึก ยังไม่เคยมีการปฏิบัติจริง เห็นควรจะต้องมีการแก้ไขกฎ ระเบียบ และหลักเกณฑ์ต่างๆเพิ่มเติมอีกพอสมควร ซึ่งเป็นอีกหนึ่งแนวทางที่กองทัพบกสามารถนำไปปรับใช้ได้

4 นำระบบจำลองยุทธทางไซเบอร์ (Cyber Range)[21]มาใช้ ระบบการเรียนการสอนด้านไซเบอร์ที่ใช้ฝึกสอนกันอยู่ตามสถาบันการศึกษาพลเรือนทั่วไป ไม่เพียงพอที่จะรองรับความต้องการของบุคคลากรด้านความปลอดภัยไซเบอร์ทางทหาร หรือนักรบไซเบอร์ (Cyber

Warrior) ได้อย่างเต็มที่เนื่องจาก สถาบันการศึกษาพลเรือนจะมุ่งเน้นไปทางด้านการพัฒนาทางธุรกิจ เป็นหลัก โดยระบบจำลองยุทธทางไซเบอร์นี้ เหมาะสำหรับการฝึกเพื่อทำสงครามไซเบอร์โดยเฉพาะ จึงสามารถลดระยะเวลาและต้นทุนการพัฒนาบุคลากร ตลอดจนช่วยเพิ่มขีดความสามารถ จากการฝึกเสมือนจริง สามารถนำไปใช้ประเมินศักยภาพของ นายทหารไซเบอร์ (Cyber Officers) เพื่อวัดความรู้ความสามารถ หรือเพิ่มจำนวนนักรบไซเบอร์ให้เพียงพอสำหรับรับมือกับการโจมตีทางไซเบอร์ ซึ่งนับวันจะรุนแรงขึ้นเรื่อย ๆ ประโยชน์ที่เห็นได้ชัดคือความสมจริงในสถานการณ์รบทางไซเบอร์ ทำให้ผู้ฝึกพัฒนาฝีมือได้เพิ่มขึ้นตามระดับความยากของด่านต่าง ๆ และการแข่งขันกับผู้ฝึกอบรมคนอื่น ๆ ทำให้เกิดความตื่นเต้น ท้าทาย

5 มุ่งสู่การปฏิบัติการเชิงรุก จากการรวบรวมข้อมูลของผู้ปฏิบัติงานด้านไซเบอร์ทางทหาร หลายคนยังไม่เห็นด้วยเกี่ยวกับการนำนักรบไซเบอร์ไปใช้ในการปฏิบัติการเชิงรุก สาเหตุหลักมาจาก กฎหมาย ระเบียบหรือข้อบังคับต่างๆยังไม่เอื้อต่อการปฏิบัติการเชิงรุก และการเปิดเผยขีดความสามารถเชิงรุก อาจสร้างความตื่นตระหนกแก่บุคคลทั่วไป หรือเป็นการท้าทายกลุ่มแฮกเกอร์อื่นๆ เข้ามาทดสอบความสามารถ ดังนั้นในหลายประเทศการพัฒนานักรบไซเบอร์ในการปฏิบัติการเชิงรุก มักจะเก็บไว้เป็นความลับ แต่กระนั้น การสร้างนักรบไซเบอร์ให้มีขีดความสามารถในการปฏิบัติการเชิงรุกได้นั้น ใช้เวลานานและต้องพัฒนาตนเองอย่างสม่ำเสมอต่อเนื่อง ประกอบกับความใฝ่รู้ส่วนบุคคล ที่ต้องการเพิ่มพูนความรู้ที่ทันสมัยตลอดเวลาไปจนถึงทักษะเฉพาะตัวที่ผ่านการฝึกฝนมาเป็นอย่างดี ดังนั้นหน่วยงานใดมีนักรบไซเบอร์ที่เก่งกาจ ก็จะเป็นเครื่องมือสำคัญ ทั้งงานด้านการข่าวลับ การปฏิบัติการจิตวิทยา หรือแม้แต่การแทรกซึมและบ่อนทำลาย ขีดความสามารถทางไซเบอร์ของฝ่ายตรงข้ามได้ และในทางกลับกัน ก็จะสามารถตอบโต้การจารกรรมทางไซเบอร์ (Cyber Espionage) จากศัตรูได้อีกด้วย หากคิดที่จะป้องกันแต่เพียงอย่างเดียว ในโลกของไซเบอร์แล้ว ไม่มีระบบใดที่สามารถป้องกันได้ 100% แนวคิดจากการป้องกันทางไซเบอร์ (Cyber Security) ได้ถูกพัฒนาไปสู่ความทนทานทางไซเบอร์ (Cyber Resilience) ซึ่งก็คือความสามารถในการกลับสู่สภาพเดิมหรือลดความเสียหายให้มากที่สุด ตอบโต้หรือหยุดยั้งการโจมตีอย่างรวดเร็ว จะเป็นเรื่องที่ควรให้ความสำคัญมากยิ่งขึ้นในการพัฒนาขั้นต่อไป

6 พัฒนาไปสู่ความยั่งยืน หากมีความประสงค์ที่จะพัฒนาหน่วยงานไซเบอร์ให้เป็นรูปธรรมแล้ว แผนยุทธศาสตร์ทหารไซเบอร์ จะต้องมีแผนการดำเนินการที่ครบทั้งระบบ ตั้งแต่ระบบการผลิต การพัฒนา การจัดการฝึกศึกษา การกำหนดมาตรฐานรับรอง การใช้งาน การทดแทน นั่นหมายความว่า ศูนย์ไซเบอร์กองทัพบก จะต้องมีแผนการพัฒนาหน่วย ตามลำดับด้วยเช่นกัน โดยมีเป้าหมาย ไปสู่การเป็นกรมฝ่ายเสนาธิการ ในการให้ข้อพิจารณาการใช้กำลัง

ของหน่วยไซเบอร์ เป็นศูนย์บัญชาการของหน่วยปฏิบัติ ที่มีความพร้อมทั้งการป้องกันเครือข่ายของกองทัพบก และตอบโต้ขีดความสามารถทางไซเบอร์ของข้าศึก เป็นหน่วยสายวิชาการที่สามารถผลิต และพัฒนานักรบไซเบอร์ ต่อยอดพัฒนาองค์ความรู้ กำหนดหลักนิยมร่วมกับหน่วยงานด้านไซเบอร์ของทุกภาคส่วน เป็นหน่วยที่มีขีดความสามารถการส่งกำลังทางไซเบอร์ให้กับหน่วยงานต่าง ๆในอนาคต ซึ่งหน่วยในระดับกองพลหรือเทียบเท่านับว่ามีความจำเป็นที่จะต้องมีตำแหน่งนายทหารปฏิบัติการไซเบอร์คอยดูแลระบบของหน่วยด้วย ดังนั้นในอนาคตกองทัพบก อาจจะต้องพิจารณาแผนการเสริมสร้างความพร้อมรบทางทหารด้านไซเบอร์ ให้มีเหล่าไซเบอร์ โดยแปรสภาพหน่วยเป็นกรมไซเบอร์ หรือกองบัญชาการไซเบอร์กองทัพบก ซึ่งงบประมาณที่นำมาใช้ในการจัดหายุทโธปกรณ์และพัฒนาหน่วย ในมิติทางไซเบอร์นั้น หากเปรียบเทียบกับงบประมาณที่ใช้พัฒนามิติทางทหารอื่น ๆ นับว่าน้อยกว่ามาก แต่ในทางกลับกันขีดความสามารถนี้ก่อให้เกิดอำนาจกำลังรบเปรียบเทียบได้สูง หากนำไปใช้งานได้อย่างถูกต้องเต็มขีดความสามารถ

<u>บทสรุป</u>

การพัฒนาของเทคโนโลยีมีการเปลี่ยนแปลงอย่างต่อเนื่องตลอดเวลาและเกิดขึ้นอย่างรวดเร็วแบบก้าวกระโดด การเปลี่ยนแปลงทางดิจิตอล (Digital Transformation) ทำให้เกิดสิ่งใหม่ และทดแทนสิ่งเก่าจนหายไป ซึ่งเรียกว่าปรากฏการณ์นี้ว่า Digital Disruption ส่งผลให้องค์กรหรือหน่วยงานที่ไม่ได้เตรียมการปรับตัวไว้ก่อน ขาดความสามารถในการแข่งขันทางธุรกิจ สำหรับสายงานด้านความมั่นคงแล้ว หน่วยงานของรัฐที่ปรับตัวไม่ทันต่อการเปลี่ยนแปลงอาจก่อให้เกิดผลเสียหายร้ายแรง ต่อความมั่นคงของประเทศ และผลประโยชน์ของชาติเลยทีเดียว ในหลายโอกาสที่วิทยาลัยการทัพบก ได้เชิญวิทยากร หรือผู้ทรงคุณวุฒิ มาบรรยายให้ความรู้แก่นักศึกษาหลักสูตรหลักประจำ ส่วนใหญ่มักจะกล่าวไปในทำนองเดียวกันว่า ภัยคุกคามทางไซเบอร์ เป็นเรื่องที่สำคัญมากเป็นอันดับต้น ๆ ของโลกในปัจจุบันไปจนถึงอนาคต และก็มักจะจบลงแค่นั้น ทิ้งไว้เป็นปริศนาให้ขบคิดว่าควรจะต้องทำอย่างไรต่อไป ด้านผู้บังคับบัญชาระดับสูงทางทหารของเหล่าทัพ จำเป็นต้องปรับตัวเพื่อเรียนรู้และเข้าใจถึงความสำคัญในมิติไซเบอร์อย่างถ่องแท้ ซึ่งอาจเป็นเรื่องยาก สำหรับผู้ที่ถือกำเนิดขึ้นมาก่อนยุคสมัยที่คอมพิวเตอร์จะถูกนำมาใช้อย่างแพร่หลาย แต่ถ้าหากปรับตัวพร้อมรับการเปลี่ยนแปลงได้แล้ว เชื่อมั่นว่า การนำนักรบไซเบอร์มาใช้ในกิจการเพื่อความมั่นคงทางทหารจะเป็นเครื่องมือที่มีประสิทธิภาพสูง และอาจจนำไปสู่ทางออกของปัญหาต่าง ๆ ที่ยังไม่

สามารถแก้ไขได้ในขณะนี้ ปัจจุบันการโจมตีทางไซเบอร์ไม่ได้เป็นเพียงการโจมตีต่อระบบคอมพิวเตอร์เท่านั้น แต่ยังสามารถเข้าถึงทุกสิ่งที่อยู่ในสถานะออนไลน์ ไม่ว่าจะเป็นโทรศัพท์มือถือ นาฬิกา รถยนต์ กล้องวงจรปิด โทรทัศน์ หลอดไฟฟ้า ฯลฯ ที่รวมเรียกว่า Internet of Things (IOT) ยิ่งไปกว่านั้น นักรบไซเบอร์ในหลายประเทศยังทำงานร่วมกับนักจิตวิทยา เพื่อทำการแฮกเข้าไปในจิตใจของคน (Hijacking Mind) ส่งผลการชี้นำหรือเปลี่ยนแปลงแนวความคิดบางอย่างของกลุ่มคนเป้าหมายจำนวนมากได้ในเวลาอันรวดเร็ว ดังเช่นตัวอย่าง การชนะการเลือกตั้งของประธานาธิบดี โดนัลด์ ทรัมป์ หรือการลงประชามติออกจากสหภาพยุโรปของสหราชอาราจักร (Brexit) ซึ่งมีความเชื่อมโยงต่อกระบวนการเปลี่ยนแปลงทางความคิดโดยใช้มิติทางไซเบอร์เข้ามาจัดการ ดังนั้นการรักษาความมั่นคงทางไซเบอร์ (Cyber Security) มิได้อยู่ที่ขีดความสามารถของหน่วยงานไซเบอร์ของประเทศนั้น ๆ แต่เพียงอย่างเดียว หากอยู่ที่แต่ละบุคคลจะมีความรู้ทางดิจิตอล (Digital Literacy) ดีเพียงใด เพราะ *“คน”* คือจุดอ่อนที่ง่ายที่สุดของการโจมตีทางไซเบอร์