

กองทัพพบกับความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ (Army and National Cyber Security)

โดย พลตรี ฤทธิ อินทรารุช

วิวัฒนาการและความเจริญก้าวหน้า ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของโลกยุคปัจจุบัน นับวันจะเจริญเติบโต ขยายตัว และมีการพัฒนาขีดความสามารถ ประสิทธิภาพ และนวัตกรรมต่างๆ ขึ้นมา เพื่อรองรับความต้องการในการใช้งานของมนุษย์ และองค์กรสมัยใหม่ ที่ต้องการเสริมสร้างศักยภาพของตนเองและองค์กร เพื่อให้เกิดความได้เปรียบในการแข่งขัน รวมถึงการสร้างภาพลักษณ์และจุดยืนของตนให้ทัดเทียม หรือนำหน้ากว่าผู้อื่นๆ เพื่อสร้างความน่าเชื่อถือ และเป็นการแสดงถึงความทันสมัย ไม่ล้าหลังใคร ดังนั้น ทุกองค์กรจึงต่างหันมาให้ความสนใจในการพัฒนาองค์กร โดยใช้เทคโนโลยี สารสนเทศและการสื่อสาร มาเป็นเครื่องมือในการพัฒนาองค์กร รวมถึงการนำเทคโนโลยี สารสนเทศและการสื่อสารมาใช้เป็นกลไกขับเคลื่อนในการพัฒนาประเทศในด้านต่างๆ ทั้งด้านการเมือง เศรษฐกิจ สังคมจิตวิทยา และการทหาร เพื่อเสริมสร้างประสิทธิภาพในการบริหารจัดการให้เกิดศักยภาพ และความทันสมัย

ทุกสรรพสิ่งในโลก ยังมีคุณอนันต์ ก็จะมีโทษมหันต์ ฉันทิ อันความเจริญ ก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร ยิ่งมีการพัฒนาเจริญก้าวหน้า และมีคุณประโยชน์อนันต์มากขึ้นเท่าใด ก็ยังมีโทษภัย มหันต์ติดตามมามากขึ้นเพียงนั้น คงไม่มีใครปฏิเสธถึงคุณประโยชน์ของเทคโนโลยีสารสนเทศและการสื่อสาร ส่วนพิษภัยที่เกิดจากตัวเทคโนโลยีสารสนเทศและการสื่อสารเองโดยตรงนั้นแทบจะมองไม่เห็น แต่ผลที่เกิดจากการนำเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้งานที่ไม่ถูกต้องตามครรลองคลองธรรม หรือการนำมาใช้เพื่อผลทางมิชอบ รวมถึงการนำมาใช้เป็นเครื่องมือทางการทหาร นับเป็นมหันตภัยอันใหญ่หลวง ที่กำลังคุกคามความมั่นคงในด้านต่างๆ บนไซเบอร์ ในวงการสารสนเทศเป็นที่ทราบกันดีว่า ภัยคุกคามด้านไซเบอร์ (Cyber Threats) ถูกนำมาใช้เป็นเครื่องมือทางการทหาร ไม่ว่าจะเป็นการเจาะระบบ (Hack / Crack) , การฝังโปรแกรมลักลอบโจรกรรมข้อมูล เช่น สพายแวร์ (Spyware) หรือ ประตูหลัง (Back Door) , การโจมตีด้วยโปรแกรมมัลแวร์ (Malware) อาทิเช่น ไวรัสคอมพิวเตอร์ (Computer Virus) , หนอนคอมพิวเตอร์ (Computer Worm) หรือ ม้าโทรจัน (Trojan Horse) , การใช้โปรแกรมตั้งเวลาทำงานเพื่อการทำลาย (Logic Bomb) , การโจมตีแบบ DoS/DDos , การใช้โปรแกรมหุ่นยนต์โจมตีเพื่อเป็นฐานโจมตีอุปกรณ์คอมพิวเตอร์บนเครือข่ายสารสนเทศ (BOTNET / Robot Network) , การสร้างข้อมูลขยะ (Spam) เป็นต้น

บางประเทศ ที่เป็นประเทศมหาอำนาจทางด้านเศรษฐกิจ โดยเฉพาะอย่างยิ่งประเทศมหาอำนาจทางการทหาร ได้กำหนด มิติด้านไซเบอร์ (Cyber Domain) เป็นโดเมนที่ ๕ นอกเหนือจาก มิติภาคพื้นดิน (Land Domain) , มิติภาคพื้นน้ำ (Sea Domain) , มิติภาคอากาศ (Air Domain) และมิติด้านอวกาศ (Space Domain) เพื่อรับมือกับภัยคุกคามด้านไซเบอร์ และเสริมแสนยานุภาพในการปฏิบัติการทางทหาร รวมถึงการปฏิบัติการทางทหารที่มีใช้สงคราม (Military Operations Other Than War ; MOOT War) ดังนั้นจึงถือได้ว่าวิวัฒนาการและความเจริญก้าวหน้าด้านเทคโนโลยีสารสนเทศและการสื่อสารในยุคปัจจุบันและในอนาคต ถูกนำมาสร้างเป็น ภัยคุกคามด้านไซเบอร์ มีผลกระทบโดยตรงต่อความมั่นคงของประเทศในด้านต่างๆ รวมถึงผลกระทบต่อความมั่นคงปลอดภัยด้านการใช้งานบนไซเบอร์

ประเทศไทยโดย กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ตั้ง ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operation Center : CSOC) เมื่อปี ๒๕๕๓ โดยมุ่งเน้นการดำเนินการติดตาม ฝ้าระวัง ตรวจสอบวิเคราะห์เว็บไซต์ และข้อมูลอินเทอร์เน็ตที่ไม่เหมาะสม หรือผิดกฎหมายต่างๆ โดยเฉพาะเว็บหมิ่นสถาบัน ต่อมาในปี ๒๕๕๖ รัฐบาลปัจจุบันได้ตระหนักถึง ภัยคุกคามด้านไซเบอร์ ถึงแม้ว่าประเทศไทยจะมีมาตรการทางกฎหมาย และมีหน่วยงานของรัฐกำกับดูแลภัยคุกคามด้านนี้มาแล้วหลายปี แต่แนวโน้มความรุนแรงและการขยายตัวของภัยคุกคามยังมีความต่อเนื่อง แพร่หลายไปกระทบความเชื่อมั่นด้านความมั่นคงของประเทศในด้านต่างๆ ดังนั้นรัฐบาลจึงได้แต่งตั้ง คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC) ซึ่งมีนายกรัฐมนตรีฯ เป็นประธาน และหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการโดยมีเจ้ากรมเทคโนโลยีสารสนเทศและกิจการอวกาศ กลาโหม เป็นเลขานุการฯ โดยมีหน้าที่หลักในการจัดทำ นโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามในไซเบอร์ ที่กระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ตลอดจนติดตามและประเมินผลการปฏิบัติที่เกี่ยวข้องเพื่อให้เกิดการบูรณาการการทำงานของหน่วยงานต่างๆ ที่เกี่ยวข้อง อันจะก่อให้เกิดประสิทธิภาพและประสิทธิผลในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับแนวทางการจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของประชาคมอาเซียน

ในส่วนของวงราชการ นายกรัฐมนตรี/รัฐมนตรีว่าการกระทรวงกลาโหม ได้อนุมัติหลักการให้จัดตั้ง ศูนย์ปฏิบัติการไซเบอร์กลาโหม ขึ้นโดย กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ เตรียมจัดตั้งหน่วยงานด้านไซเบอร์โดยตรง (Cyber Command)

เพื่อขึ้นมารองรับการปฏิบัติงานความมั่นคงปลอดภัยของประเทศ จากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ โดยศูนย์ปฏิบัติการไซเบอร์กลาโหม (Cyber Operations Center) จะเป็นแกนหลักในด้านการพัฒนาบุคลากรด้านนี้ให้กับกำลังพลสังกัดกระทรวงกลาโหม โดยจะมีห้องปฏิบัติการสำหรับการฝึกปฏิบัติด้านสงครามไซเบอร์ (Cyber Warfare) รวมถึงการสร้างภาคี เครือข่าย ประชาคม ทั้งภาครัฐและเอกชน เพื่อเสริมสร้างศักยภาพของประเทศด้านไซเบอร์ในการรับมือกับภัยคุกคามด้านไซเบอร์

กองทัพบก ได้มีนโยบายและอนุมัติหลักการให้ ศูนย์เทคโนโลยีทางทหาร (ศทท.) ดำเนินการปรับปรุงภารกิจและโครงสร้างการจัดหน่วย โดยเพิ่มเติมภารกิจด้านการปฏิบัติการสงครามไซเบอร์ และปรับสายการบังคับบัญชาจากเดิม เป็นหน่วยขึ้นตรงกรมการทหารสื่อสาร มาเป็นหน่วยขึ้นตรงกองทัพบก (นขต.ทบ.) เพื่อเตรียมรองรับการปฏิบัติงานความมั่นคงปลอดภัยด้านไซเบอร์ ที่ส่งผลกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ โดยเฉพาะความมั่นคงทางการทหาร และการรักษาความสงบเรียบร้อยภายในประเทศ รวมถึงการปฏิบัติการที่ประสานสอดคล้องกับกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพต่างๆ ตลอดจนรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations ; NCO) โดยแนวความคิดเบื้องต้นในการเตรียมการดำเนินการพัฒนาปรับปรุงภารกิจ โครงสร้างการจัดหน่วย และการพัฒนาศักยภาพของกำลังพล ให้มีคุณวุฒิการศึกษา คุณลักษณะ ซึ่ดความสามารถ ประสบการณ์ และความถนัดเฉพาะด้านที่สอดคล้องกับตำแหน่งหน้าที่การงาน (put the right man to the right job) เพื่อให้การปฏิบัติการที่ได้รับมอบเป็นไปอย่างมีประสิทธิภาพ โดยเน้นการปรับเกลี้ย โยกย้าย และการบรรจุกำลังพลด้านปฏิบัติการเป็นหลักมากกว่างานทางธุรการ ในสัดส่วนไม่น้อยกว่า ๗๐ : ๓๐ สำหรับในด้านการปรับปรุงโครงสร้างการจัดหน่วย โดยแปรสภาพ กองการสงครามสารสนเทศ เป็น กองปฏิบัติการไซเบอร์ (Cyber Operations Division) ซึ่งเป็นหน่วยปฏิบัติการด้านไซเบอร์เชิงรุก (Cyber Offensive Operations) ดำเนินการด้านการตรวจสอบสภาพแวดล้อมของภัยคุกคาม การวางแผนควบคุม การปฏิบัติ และการปฏิบัติการไซเบอร์ โดยจะมีการบรรจุและพัฒนากำลังพลที่มีความรู้ ความเชี่ยวชาญ และได้รับการฝึกฝนด้านการปฏิบัติการไซเบอร์ ปฏิบัติหน้าที่เป็นนักรบไซเบอร์ (Cyber Warriors) อยู่ในชุดปฏิบัติการไซเบอร์ (Cyber Operation Teams ; COT) และชุดเตรียมพร้อมเผชิญเหตุฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Teams ; CERT) เป็นหน่วยปฏิบัติการ และเตรียมจัดตั้ง กองรักษาความปลอดภัยด้านไซเบอร์ (Cyber Security Division) ซึ่งเป็นหน่วยปฏิบัติการด้านไซเบอร์เชิงรับ (Cyber Defensive Operations) ดำเนินการด้านระเบียบการรักษาความปลอดภัยสารสนเทศ การป้องกัน ฝ้าระวัง ตรวจสอบช่องโหว่

โดยใช้เครื่องมือระบบตรวจหาการบุกรุก (Intrusion Detection System : IDS) และระบบป้องกันการบุกรุก (Intrusion Protection System : IPS) รวมถึงการกู้คืนสภาพเมื่อถูกโจมตี (Recovery) ตลอดจนการพัฒนาโปรแกรมและเครื่องมือต่างๆ เพื่อรองรับงานด้านไซเบอร์ นอกจากนี้ยังได้เตรียมการด้านการพัฒนาเทคโนโลยีและนวัตกรรมต่างๆ ด้านไซเบอร์ โดยแสวงความร่วมมือกับหน่วยงานต่างๆ ทั้งภายในและภายนอกกองทัพ ทั้งภาครัฐและองค์กรเอกชนในด้านวิชาการ การวิจัยพัฒนา (R&D) การสัมมนาเชิงปฏิบัติการ (Workshop) และการฝึกปฏิบัติต่างๆ โดยเฉพาะการฝึกซ้อมแผนเผชิญเหตุด้านไซเบอร์ (Cyber Incident Action Plan Exercise) การฝึกซ้อมแผนฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Exercise) การฝึกซ้อมการปฏิบัติการไซเบอร์ (Cyber Operations Exercise) และการฝึกจำลองสงครามไซเบอร์ (Cyber Warfare Simulation Exercise) เป็นต้น

จากนโยบายและแนวความคิดในการดำเนินการของหน่วยงานด้านไซเบอร์ของกองทัพบก จะเห็นได้ว่า ความพร้อมในด้านการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ ยังอยู่ในขั้นของการเตรียมการ ซึ่งจะพอมองเห็นถึงความเป็นไปได้ในการดำเนินการไปสู่ขั้นของการปฏิบัติ และผลสัมฤทธิ์ตามเจตนารมณ์ของผู้บังคับบัญชา ทั้งนี้ กองทัพบกจะต้องเร่งดำเนินการเปลี่ยนนโยบายไปสู่การปฏิบัติอย่างเป็นรูปธรรมโดยเร็ว โดยเฉพาะการเร่งดำเนินการด้านการปรับปรุงหรือการปฏิรูปโครงสร้างองค์กร (Organization Reform) การบรรจุกำลังพลที่มีความเชี่ยวชาญเฉพาะด้าน (Specialist) และการพัฒนากำลังพล (Human Resource Development) ให้มีขีดความสามารถในด้านไซเบอร์ เพื่อรองรับการปฏิบัติงานความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ (National Cyber Security) และการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations ; NCO) ของกองทัพบกในอนาคตอันใกล้นี้ ตามที่กองทัพบกได้มีนโยบายประกาศให้ปี ๒๕๕๗ เป็น “ ปีแห่งการเตรียมความพร้อมกองทัพบกสู่อนาคต ” (The Royal Thai Army’s Preparation Year Towards the Future) ซึ่งจะต้องมีการพัฒนาควบคู่กันไปทั้งสองด้าน เพื่อลดความเสี่ยง และเป็นหลักประกันความสำเร็จทั้งด้านการปฏิบัติการ และความมั่นคงปลอดภัยจากภัยคุกคามด้านไซเบอร์

.....