กองทัพเร่งฝึก "นักรบไซเบอร์" รับมือแฮกเกอร์ทั่วโลกโจมตีประเทศไทย

บิ๊กตู่ สั่ง "กองทัพ-สมคิด-อุตตมะ" รับมือสงครามไซเบอร์ (Cyber Warfare) เร่งบูรณาการเศรษฐกิจดิจิตอล ให้ขับเคลื่อนไปพร้อมปกป้องความมั่นคงของชาติ ด้านกองทัพพัฒนาบุคลากรให้มีความเชี่ยวชาญปฏิบัติการไซเบอร์ ทั้งในเชิงรุก-เชิงรับ สกัดกั้นภัยคุกคามในรูปแบบใหม่ ที่แฮกเกอร์ระดับโลกใช้ไทยเป็นเป้าโจมตี จัดตั้ง "ศูนย์ไซเบอร์กองทัพ" รับมือแฮกเกอร์ทั่วโลก ที่เข้ามาสร้างผลกระทบต่อประเทศชาติ ทั้งในด้านการเมือง เศรษฐกิจ และสังคม ด้านผู้เชี่ยวชาญระบบคอมพ์ย้ำ ทหารดูแลดีกว่าให้การเมืองคุมศูนย์ฯ จากสถานการณ์ไซเบอร์ของประเทศไทยในวันนี้ ที่ถูกจัดอันดับว่าเป็นประเทศที่ถูกโจมตีผ่านระบบไซเบอร์เป็นอันดับที่ 33 จาก 250 ประเทศทั่วโลก โดยเฉพาะสถานการณ์การถูกโจมตีเมื่อเดือนสิงหาคมที่ผ่านมานั้น บรรดาหน้าเว็บไซต์ของหน่วยงานราชการ อาทิ เว็บไซต์ของจังหวัดลำพูน และเว็บไซต์ของฝ่ายอำนวยการ 1 บก.อก. กองบัญชาการตำรวจนครบาล (บช.น.) ถูกเจาะระบบเปลี่ยนหน้าโฮมเพจเป็นข้อความเรียกร้องสันติภาพชาวมุสลิม พร้อมระบุว่าเป็นฝีมือของแฮกเกอร์แอลจีเรีย ซึ่งปัญหานี้เกิดขึ้นมาในขณะที่ประเทศไทย ยังไม่มีมาตรการดูแลเรื่องความมั่นคงและปลอดภัยทางด้านไซเบอร์ที่ชัดเจนและรัดกุม เว็บไซต์ของจังหวัดลำพูน เมื่อวันที่ 24 สิงหาคม 2558 หากปล่อยไว้โดยไม่เร่งดำเนินการจัดการจากภัยคุกคามจากโลกไซเบอร์ บรรดาแฮกเกอร์ในที่ต่างๆ ทั่วโลก สามารถใช้จุดอ่อนหรือช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เข้ามาทำลายหรือรบกวนขัดขวางการทำงานโดยโจมตีระบบเครือข่ายคอมพิวเตอร์โครงสร้างพื้นฐานสำคัญของชาติได้ ทั้งนี้เพราะระบบเครือข่ายคอมพิวเตอร์เป็นเครื่องมือในการขับเคลื่อนการปฏิบัติงานของภาครัฐ หน่วยงานรัฐวิสาหกิจ โทรคมนาคม ตลอดจนภาคเอกชนและภาคอุตสาหกรรม รวมถึงการคุกคามในระดับบุคคลและองค์กรซึ่งมีผลกระทบต่อความมั่นคงของประเทศชาติ เศรษฐกิจ และสังคม ดังนั้นรัฐบาลพลเอกประยุทธ์ จันทร์โอชา จึงมีนโยบายและสั่งการเพื่อรับมือกับสงครามไซเบอร์ โดยให้มีการบูรณการ การขับเคลื่อนเศรษฐกิจดิจิตอล ควบคู่ไปกับความมั่นคงปลอดภัยด้านไซเบอร์ระดับชาติ ซึ่งมอบหมายให้กระทรวงกลาโหม เป็นผู้ดูแลภาพรวม

ตั้งศูนย์ไซเบอร์กองทัพบกรับมือแฮกเกอร์ทั่วโลก อย่างไรก็ดีกองทัพมีการเตรียมความพร้อมที่จะปฏิบัติภารกิจดังกล่าว ทั้งในเรื่องการพัฒนาบุคลากรทางการทหารให้มีความเชี่ยวชาญการปฏิบัติการด้านไซเบอร์เชิงรับ (Defensive) และการปฏิบัติการด้านไซเบอร์เชิงรุก (offensive) โดยหลายปีที่ผ่านมา มีการนำร่องการอบรมเพิ่มทักษะให้กับกำลังพลของกองทัพ โดยศูนย์เทคโนโลยีทางทหาร กองบัญชาการกองทัพบก ดำเนินการในเรื่องอัตรากำลัง และงบประมาณที่จะฝึกฝนความรู้ทางด้านไซเบอร์ให้บุคลากรนายทหารระดับสูงจนถึงระดับกลาง ตลอดจนการสรรหาคนเก่งปรับจากชั้นประทวนเป็นชั้นสัญญาบัตรและจะสนับสนุนให้เป็นนักรบไซเบอร์หรือทหารรบไซเบอร์ และในปีที่ผ่านมา ยังมีการเปิดรับสมัครคนนอกที่เก่งด้านไซเบอร์เข้ามาติดยศเป็นนายทหารกองบัญชาการกองทัพไทย ปัจจุบันมีการพัฒนาบุคลากรของกองทัพในรูปแบบการแข่งขันระบบงานจำลองการฝึกด้านไซเบอร์ (Cyber Range) ที่จัดขึ้นภายใต้งาน "อาร์มี ไซเบอร์คอนเทสต์ 2015" (Army Cyber Contest 2015) เมื่อวันที่ 9 กันยายน ที่กองบัญชาการกองทัพบก ซึ่งทั้งหมดเป็นการเตรียมความพร้อมที่จะขยายศูนย์เทคโนโลยีทางทหารสู่ "ศูนย์ไซเบอร์ของกองทัพบก" ให้เกิดขึ้นในอนาคตอันใกล้ ภายใต้กรอบการปฏิบัติงานทั้ง "Scope" และ "Scale" ออกเป็น 4 ด้าน คือ

1.ภัยคุกคามที่ส่งผลต่อความมั่นคงของประเทศ
2.ภัยคุกคามที่ส่งผลกระทบต่อสามจังหวัดชายแดนภาคใต้ (จสต.)
3.ภัยคุกคามที่ส่งผลกระทบต่อสถาบัน
4.ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพ

พล.ต.ฤทธี อินทราวุธ
ผู้อำนวยการศูนย์เทคโนโลยีทางทหาร

ด้าน พล.ต.ฤทธี อินทราวุธ ผู้อำนวยการศูนย์เทคโนโลยีทางทหาร กล่าวว่า ถือว่าปีนี้เป็นครั้งแรกที่กองบัญชาการกองทัพไทย กองทัพอากาศ กองทัพเรือ ศูนย์สงครามไซเบอร์ และสำนักปลัดกระทรวงกลาโหม เข้าร่วมการแข่งขัน ซึ่งเป็นจุดเริ่มต้นที่ดีในการฝึกทักษะเพื่อรองรับการปฏิบัติงานความมั่งคงปลอดภัยด้านไซเบอร์ของชาติ (National Cyber Security) และการเตรียมพร้อมด้านบุคลากรซึ่งเป็นนักรบไซเบอร์ในการปฏิบัติการทางทหาร ถือว่ามีความจำเป็นสำหรับยุคนี้ เพราะไซเบอร์สเปซเป็น "โดเมนที่ 5" ซึ่งนอกเหนือจากการฝึกทักษะทั้งทางพื้นดิน ผืนฟ้า อากาศ และอวกาศแล้ว การปฏิบัติการในไซเบอร์โดเมนจะเข้าไปเกี่ยวพันกับการปฏิบัติการในทุกมิติ สำหรับระบบงานจำลองการฝึกด้านไซเบอร์ (Cyber Range) ถือเป็นระบบงานที่หลายหน่วยงานของกองทัพให้ความสนใจและในอนาคตอาจจะถูกบรรจุไว้ใน ระบบของศูนย์ไซเบอร์ของกองทัพอีกด้วย

อาจารย์ปริญญา หอมอเนก
ผู้เชี่ยวชาญทางระบบคอมพิวเตอร์และความมั่นคงปลอดภัยสารสนเทศ (Information Security)

ความมั่นคงด้านไซเบอร์หนุนเศรษฐกิจดิจิตอล ขณะที่ อาจารย์ปริญญา หอมอเนก ผู้เชี่ยวชาญทางระบบคอมพิวเตอร์และความมั่นคงปลอดภัยสารสนเทศ (Information Security) ให้ความเห็นกับ Special scoop ว่าการตั้งกองบัญชาการไซเบอร์ สอดคล้องกับสถานการณ์สงครามไซเบอร์ ที่ประเทศไทยกำลังเผชิญ ซึ่งภายในเวลา 5 เดือน เว็บไซต์ถูกเจาะระบบมากถึง 6,000 แห่ง นอกจากนั้นประเทศไทยยังติดอันดับโลกโดยเป็น 1 ใน 5 ของประเทศที่โดนแฮกมากที่สุด เพราะเว็บไซต์โดนฝังไวรัสโทรจัน หน้าเวบเพจ เป็นว่าเล่น และยังติดอันดับ 7 ประเทศแรกที่โดนเป็นเป้าหมายโจมตีมากที่สุด ซึ่งจากข้อมูลรีเสิร์ชของอเมริการะบุว่า ไทยเป็นประเทศที่เป็นเป้าหมายถูกแฮก ทั้งในมิติเรื่องความมั่นคงรัฐ ด้านธุรกิจ ซึ่งตรงนี้ถึงเวลาแล้วที่จะต้องสร้างระบบความมั่นคงปลอดภัยด้านไซเบอร์ขึ้นมา "เมื่อเร็วๆ นี้เว็บไซต์ภาครัฐถูกแฮกเกอร์เจาะแก้หน้าเว็บไซต์ ซึ่งจุดนี้ก็ต้องยอมรับว่าการรับมือสงครามไซเบอร์ของประเทศไทยยังไม่มีความพร้อม โดยเฉพาะเว็บไซต์ของหน่วยงานภาครัฐ ซึ่งมีเป็นหลักหมื่น ต้องมีการปรับปรุงให้ได้มาตรฐาน เพราะยังกระจัดกระจายต่างคนต่างทำ ยกตัวอย่างองค์การบริการจังหวัดได้งบมาก็ไปเช่าโฮสติ้ง 500 บาทต่อเดือน แถมบางแห่งใช้ชื่อโดเมนลงท้ายว่า .com แทนที่จะใช้ .go.th ปัญหาส่วนหนึ่งเป็นเพราะว่าไม่มีการตั้งหน่วยงานกลางที่รับผิดชอบดูแลโดยตรง" ส่วนแนวทางในการแก้ปัญหามีตั้งแต่การตั้งหน่วยงานขึ้นมาเพื่อตรวจสอบดูแลเว็บไซต์ต่างๆ ที่เป็นของราชการให้ผ่านมาตรฐาน โดยจ้างเอกชนมาทำหน้าที่ตรวจสอบ 10 บริษัทแบ่งให้รายละ 100 เว็บไซต์ แล้วนำมาหรือหากจะยึดการดำเนินการตามแนวทางเดิม โดยหน่วยงานเป็นผู้ดำเนินการเว็บไซต์ด้วยตัวเองนั้น ก็ต้องทำให้มีมาตรฐานมากกว่า

ที่เป็นอยู่ทุกวันนี้ อาจารย์ปริญญา บอกด้วยว่า ในการฝึกทหารไซเบอร์ที่กระทรวงกลาโหม เป็นผู้ดูแลกับการตั้งหน่วยงานขึ้นมาตรวจสอบดูแลเว็บไซต์ สามารถดำเนินการไปด้วยกันได้ เพราะถือเป็นการเตรียมคนเพื่อรับมือกับการเปลี่ยนแปลงด้านความมั่นคงด้านไซเบอร์ (Cyber Security)

บรรยากาศการแข่งขัน "อาร์มี ไซเบอร์คอนเทสต์ 2015" เมื่อวันที่ 9 กันยายน ที่กองบัญชาการกองทัพบก

ขณะเดียวกันการที่ทหารฝึกนำระบบจำลองยุทธ์ทางไซเบอร์ ซึ่งเป็นการแข่งขันสนามจำลองยุทธ์ ประกอบด้วย 1.เกมเทคโนโลยี 2.เอ็ดดูเคชัน 3.เอนเตอร์เทนเมนต์ รวมกัน ซึ่งเกมนี้ส่งเสริมให้มีทักษะประสบการณ์ทางด้านไซเบอร์ และสร้างศักยภาพกำลังพลของกองทัพด้านไซเบอร์ เพราะมีการฝึกทั้งเชิงรุกและเชิงรับโดยแบ่งเป็น 2 ลักษณะ คือ เรดทีม ทีมเจาะบุกเข้าไปแฮก (Offensive) และบลูทีม (Defensive) เป็นทีมปิด โดยวิธีการนี้จะเพิ่มจำนวนกำลังพลของศูนย์ไซเบอร์กองทัพบกไปถึงเป้าหมายได้อย่างรวดเร็ว คาดว่าภายในเวลา 1 - 2 ปี บุคลากรที่เป็นนักรบไซเบอร์ที่มีความเก่งและความเชี่ยวชาญจะเพิ่มเป็นหลักร้อยคน ที่สำคัญหากประเทศไม่มีความมั่นคงทางไซเบอร์แล้ว แนวคิดการขับเคลื่อนเศรษฐกิจแบบดิจิตอลอีโคโนมีจะเกิดขึ้นได้อย่างไร ที่ผ่านมาเราใช้เศรษฐกิจนำ แต่อันที่จริงแล้วความมั่นคงและเศรษฐกิจจะต้องไปด้วยกัน จะทำให้ดิจิตอลอีโคโนมีมีความชัดเจนดีขึ้นทั้งเศรษฐกิจและความปลอดภัย "สมคิด-อุตตมะ" ต้องบูรณาการ "เศรษฐกิจดิจิตอล-ความมั่นคง" โดยในวันแถลงยุทธศาสตร์ชาติ-ยุทธศาสตร์ทหาร พ.ศ. 2559-2563 ของวิทยาลัยป้องกันราชอาณาจักร (วปอ.) ที่ผ่านมา พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี กล่าวขณะเยี่ยมชมบูทศูนย์เทคโนโลยีทางทหาร ได้เล็งเห็นถึงความสำคัญของภัยบนโลกไซเบอร์ จึงให้นโยบายและแนวทางกับ ดร.สมคิด จาตุศรีพิทักษ์ รองนายกรัฐมนตรีด้านเศรษฐกิจ และ ดร.อุตตมะ สาวนายน รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร นำไปสานต่อ "ให้นำแนวความคิด การปฏิบัติการไซเบอร์ และการต่อต้านสงครามไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ใส่ไว้ใน "Digital Economy" จัดเชื่อมโยงเครือข่าย และขยายผลในระดับชาติ รวมไว้ในโครงสร้างระบบเศรษฐกิจแบบ "Digital Economy" ของรัฐบาลและให้กระทรวงกลาโหมไปดูภาพรวม" อาจารย์ปริญญา ระบุว่าการให้นโยบายครั้งนี้สอดคล้องกับบทบาทและศักยภาพการปฏิบัติงานของ "ศูนย์ไซเบอร์กองทัพบก" ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และรับมือกับภัยคุกคามที่มองไม่เห็นบนเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร จึงกำหนดให้ "ดิจิตอลอีโคโนมีจะต้องเชื่อมต่อกับไซเบอร์ซีเคียวริตี้ เพราะที่ผ่านมาต่างคนต่างทำไม่มีการเชื่อมโยงและบูรณาการดิจิตัลไปในภาคเศรษฐกิจ ขณะที่กองทัพดำเนินการทางด้านความมั่นคงทางไซเบอร์" "การที่พลเอกประยุทธ์ให้การบ้านรองนายกฯ และ รมว.ไอซีที ถือเป็นจุดเริ่มต้นว่าจะเอาจริงเอาจัง เรื่องไซเบอร์บูรณาการเชื่อมโยงกับนโยบายดิจิตอลอีโคโนมีความชัดเจนมากขึ้น" ในเรื่องความมั่นคงปลอดภัยด้านไซเบอร์ของประเทศชาติ (National Cyber security) เป็นเรื่องที่จะต้องมีความยั่งยืนตลอดไป จึงเป็นบทบาทของกระทรวงกลาโหม เพราะหากให้ฝั่งการเมืองคุมเบ็ดเสร็จ ทุกอย่างในความปลอดภัยที่เป็นส่วนตัว Security Privacy อยู่ภายใต้รัฐมนตรีทั้งหมด และเมื่อเปลี่ยนรัฐบาลนั้นจะมีความเสี่ยงสูงมาก ดังนั้นการที่ให้กระทรวงกลาโหมเข้ามามีส่วนในการดูแลนั้นมีข้อดีคือ สามารถขับเคลื่อนได้ง่าย มีความปลอดภัยมั่นคงและยั่งยืน เพราะเป็นสถาบันที่อยู่กับประเทศชาติตลอดไป ทั้งนี้เพราะความมั่นคงปลอดภัยด้านไซเบอร์ไม่ได้มีเฉพาะมิติด้านบุคลากรเท่านั้น ยังมีมิติอื่นๆ อีก เช่นมิติด้านเศรษฐกิจ มิติด้านความมั่นคง หรือความปลอดภัย ความเป็นส่วนตัวของคน อาจารย์ปริญญา ยังยกตัวอย่างให้เห็น เช่น ข้อมูลบุคคลโดนคนขายประกันโทร.มา ไม่ใช่เรื่องความมั่นคงแต่เป็นเรื่องสิทธิส่วนบุคคลเจอในสิ่งที่ไม่ต้องการ เพราะในมุมมองนี้คือ ต้องได้รับการยอมรับก่อนที่จะนำข้อมูลของเราไปให้คนอื่น เรื่องนี้ยังไม่มีกฎหมายปกป้องสิทธิ อย่างมากทำได้เพียงบ่นต่อว่าร้องเรียนเท่านั้น ซึ่งตัวอย่างการคุ้มครองด้านไซเบอร์ส่วนบุคคล ในอนาคตอาจจะขึ้นตรงกับกระทรวงพาณิชย์ ที่จะมีบทบาทดูแลความมั่นคงและความปลอดภัยของ "คน" ซึ่งครอบคลุมถึงการพาณิชย์อิเล็กทรอนิกส์ การทำธุรกรรมอิเล็กทรอนิกส์สำคัญที่สุด คือ การออกแบบกฎหมายคุมเข้มเรื่องนี้ ต้องไม่มองความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Securrity) ด้านเดียวเท่านั้น เพราะความมั่นคงปลอดภัยด้านไซเบอร์เป็นเรื่องหลัก ส่วนเรื่องความมั่นคงปลอดภัยของ "คน" เป็นเรื่องรองลงมาเข้าทำนองที่ว่า "เรื่องชาติเป็นเรื่องหลัก แต่ถ้าคนรั่วชาติก็รั่ว จึงต้องขับเคลื่อนไปด้วยกัน อย่างไรก็ดีการดำเนินการเรื่องนี้ ยังเป็นเพียงการนำร่องที่พลเอกประยุทธ์ฝากเป็นการบ้านให้หัวหน้าทีมเศรษฐกิจของรัฐบาลดำเนินการ ซึ่งการจะสามารถบูรณาการทั้ง "เศรษฐกิจดิจิตอล" และ "ความมั่นคงปลอดภัยด้านไซเบอร์"ทั้ง 2 ด้าน ให้ดำเนินการควบคู่กันไปได้ จนสามารถปฏิบัติการในเชิงรับและรุกสงครามไซเบอร์ระดับโลกที่ขยับเข้าใกล้ประเทศไทยมากขึ้นทุกขณะได้เพียงไร คงต้องติดตามกันต่อไป

ขอขอบคุณที่มา www.manager.co.th