

“หน่วยรบไซเบอร์” อำนาจกำลังรบไร้ตัวตน

สัมภาษณ์ โดย วรณชัช ไซยะอาด (โพสท์ทูเดย์)

เมื่ออำนาจในโลกไซเบอร์กำลังทรงพลัง...

ปี 2558 พลสารวจของ “ แคลเปอร์สกี แลป ” ผู้ผลิตซอฟต์แวร์ป้องกันไวรัสระดับโลกโดย นายยูริ นามสนิคอฟ นักวิจัยอาวุโสด้านความปลอดภัย จากทีมวิเคราะห์และวิจัยระดับโกลเบล แคลเปอร์สกี แลป เปิดเผยว่า ประเทศไทยมีความเสี่ยงถูกโจมตีทางไซเบอร์เป็นอันดับ 33 จาก 250 ประเทศทั่วโลก เนื่องจากยังมีผู้นิยมใช้ซอฟต์แวร์เถื่อน และไม่นิยมอัปเดตซอฟต์แวร์ รวมทั้งยังไร้มาตรการดูแลเรื่องความมั่นคงและปลอดภัยทางด้านไซเบอร์ที่ชัดเจน และรัดกุม ข้อเท็จจริงดังกล่าว ทำให้กองทัพไทยให้ความสำคัญและเร่งพัฒนาหน่วยงาน ที่เรียกว่า “ศูนย์ไซเบอร์” ขึ้นมา

ทำให้องค์กรสำคัญกับ “ไซเบอร์”

หนทางนำพาประเทศไปสู่ความเจริญ มั่งคั่ง และมีเสถียรภาพ จำเป็นต้องมีพลังทางอำนาจ ใน 5 ด้าน ได้แก่ พลังทางการเมือง เศรษฐกิจ สังคม การทหาร วิทยาศาสตร์และเทคโนโลยี ซึ่งนำหน้าที่รัฐบาลใส่ลงไปในแต่ละด้าน ขึ้นอยู่กับสถานการณ์ และทิศทางการบริหารของแต่ละประเทศ หากว่ากันเฉพาะ “ พลังอำนาจทางทหาร ” กองทัพไทยเริ่มให้ความสำคัญกับ วิทยาศาสตร์และเทคโนโลยี มากขึ้น โดยเฉพาะประเด็น ภัยคุกคามด้านไซเบอร์

พล.ต.ท.สุรทิน อินทรราช ผู้บัญชาการศูนย์เทคโนโลยีทางทหาร บอกว่า พลังอำนาจทางทหาร มีพื้นที่ปฏิบัติการหลักๆ อยู่ 5 ด้าน ได้แก่ พื้นที่ปฏิบัติการบนดิน (Land Domain) , พื้นที่ปฏิบัติการในน้ำ (Sea Domain) พื้นที่ปฏิบัติการในอากาศ (Air Domain) และพื้นที่ปฏิบัติการบนห้วงอวกาศ (Space Domain) ทั้งหมดถูกควบคุม โดย “ไซเบอร์ โดเมน” (Cyber Domain) ซึ่งนับเป็นโดเมนที่สำคัญมาก

“ ต่อให้คุณมีกำลังทหารและอาวุธยุทโธปกรณ์ที่ทันสมัยเต็มไปหมด แต่ไม่สามารถควบคุมสั่งการได้ก็เท่านั้น ไม่เห็นภาพการเคลื่อนไหวทางการรบ เพราะถูกแฮกเข้าไปในระบบ โจมตีในโครงข่าย บิดเบือนข้อมูลต่างๆ นานาจนกองทัพเสียการควบคุมบังคับบัญชา และพ่ายแพ้ ”



ทั้งนี้ ด้วยงบประมาณของพื้นที่ปฏิบัติการอื่นที่มีค่อนข้างมหาศาลเมื่อเทียบกับ “ไซเบอร์โดเมน” ทำให้ประเทศขนาดเล็กหลายประเทศ ที่มีงบประมาณด้านการทหารจำกัด เลือกสร้างศักยภาพทางทหารให้แข็งแกร่งด้วย “ไซเบอร์ วอร์เออร์” หรือ “นักรบไซเบอร์” แทน ในต่างประเทศเราเห็นตัวอย่างของภัยคุกคาม หรือการโจมตีทางไซเบอร์ระดับรุนแรงกันบ่อยครั้ง เช่น การปล่อยไวรัสสตกซ์เน็ต (Stuxnet) ทำลายระบบโรงงานผลิตอูรูนิวเคลียร์ในประเทศอิหร่าน จนทำให้ต้องปิดโรงงานทั้งหมด พล.ต.ท.สุรทิน บอกว่า หน่วยรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ National Cyber security and Integration Center (NCCIC) ของประเทศสหรัฐอเมริกา ได้กำหนดระดับภัยคุกคามด้านไซเบอร์ (Spectrum of Cyber Threats) ไว้ 4 ระดับ ดังนี้

1. ภัยคุกคามในระดับรัฐบาลแห่งชาติ (National Governments) คือ ภัยที่อาจจะเป็นอันตรายต่อผลประโยชน์ของประเทศชาติ เช่น การโฆษณาชวนเชื่อ การเปลี่ยนแปลงหน้าเว็บไซต์ เพื่อสร้างความรำคาญให้กับหน่วยงานของรัฐ ตลอดจนถึงขั้นทำให้เกิดการหยุดชะงักของโครงสร้างพื้นฐาน เช่น ระบบไฟฟ้า ประปา เป็นต้น

2. การก่อการร้าย และ กลุ่มการก่อการร้าย (Terrorists) มุ่งสร้างความเสียหายต่อผลประโยชน์ของประเทศ รวมทั้งสร้างความหวาดกลัวไปยังประชาชนในประเทศเป้าหมาย

3. สายลับหรือพวกจารกรรมในภาคอุตสาหกรรม และกลุ่มองค์กรอาชญากรรม (Industrial Spies and Organized Crime Groups) การจารกรรมขององค์กรระหว่างประเทศ และองค์กรเครือข่ายอาชญากรรมต่างๆ เป็นภัยคุกคามระดับกลางของประเทศ

4. กลุ่มแฮกเกอร์ที่มีอุดมการณ์ (Hacktivists) กลุ่มแฮกเกอร์ (Hacker) ที่มีอุดมการณ์เป็นรูปแบบของกลุ่มเล็กๆ มีแรงจูงใจหรือแนวทางเพื่ออุดมการณ์ทางการเมือง หรือบุคคลทางการเมือง รวมทั้งกลุ่มต่อต้านต่างๆ ในระดับประเทศที่เป็นฝ่ายตรงกันข้าม

5. แฮกเกอร์ (Hackers) การโจมตีไซเบอร์แบบนี้ จะเกิดมากที่สุด และมีการประชาสัมพันธ์เผยแพร่อย่างกว้างขวาง โดยพวกเหล่าแฮกเกอร์มีอสมัครเล่น สามารถก่อให้เกิดภัยคุกคามที่สำคัญอย่างกว้างขวาง และส่งผลกระทบต่อรวมทั้งการสร้างความปลอดภัยในระยะยาวให้กับโครงสร้างพื้นฐานในระดับชาติได้

5 ข้อดังกล่าวคือภัยคุกคามของประเทศมหาอำนาจอย่างสหรัฐ ซึ่งห่างไกลจากระดับความรุนแรงของเมืองไทย ที่ส่วนใหญ่จำนวนมากเป็นเพียงไวรัส มัลแวร์ , การแฮกหน้าเว็บ และการโจมตีด้วยข้อมูลข่าวสาร ที่สร้างความเสียหาย ซึ่งภัยคุกคามของประเทศ เป็นที่มาของการกำหนดภารกิจ ซึ่งกองทัพพบได้เน้นในเรื่องความมั่นคงของชาติเป็นหลัก โดยให้ความสำคัญกับระดับภัยคุกคามด้านไซเบอร์ 4 ด้าน ได้แก่

1. ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ การใช้ไซเบอร์เพื่อสร้างให้เป็นภัยคุกคามในระดับประเทศ หรือระดับชาติ วิธีการอาจจะเพียงแค่ใช้เว็บไซต์ของประเทศตนเอง เผยแพร่ข่าวสารที่ทำให้เกิดความได้เปรียบทางการเมือง หรือด้านความมั่นคง หรือข้อมูลความลับของชาติ การแพร่กระจายโปรแกรม ไม่พึงประสงค์

2. ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.) เป็นการใช้ไซเบอร์ เพื่อการเผยแพร่ข่าวสารของผู้อั้วความไม่สงบ เพื่อให้สื่อมวลชนกระแสหลักนำไปเผยแพร่ต่อ หรือเพื่อให้ประชาชนทั่วไป รวมทั้งเจ้าหน้าที่รัฐเกิดความกลัวเกรง ถือเป็นปฏิบัติการข่าวสาร (IO) การปฏิบัติการจิตวิทยาอย่างหนึ่ง นอกจากนั้นยังมีการแสดงถึงผลงานของผู้อั้วความไม่สงบที่อาจจะส่งผลกระทบต่อแนวร่วมของผู้อั้วความไม่สงบเพิ่มขึ้น

3. ภัยคุกคามที่ส่งผลกระทบต่อสถาบันฯ เป็นสิ่งที่กระทำได้ง่าย และยากต่อการดำเนินคดีต่อผู้กระทำ การดำเนินการดังกล่าว มีทั้งการเผยแพร่ภาพที่หมิ่นสถาบันฯ การวิจารณ์สถาบันฯ ในทางเสื่อมเสีย โดยกฎหมายที่เกี่ยวข้องไม่อาจจะดำเนินการได้ เนื่องจากสาเหตุหลายประการ อาทิ ผู้กระทำไม่ได้อยู่ประเทศไทย หรือผู้กระทำใช้เครื่องมือของต่างประเทศ ซึ่งกฎหมายของต่างประเทศไม่ได้รับรองความผิดในฐานะความผิดนั้น

4. ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพ เพื่อทำให้ภาพลักษณ์ของกองทัพหรือผู้นำกองทัพเสื่อมเสีย เพื่อลดความน่าเชื่อถือในสังคม ย่อมจะสร้างความไม่เชื่อมั่นต่อการปกป้อง หรือพิทักษ์อธิปไตยของชาติ

“ ปัจจุบันมีการมอเนเตอร์ เฟ้าะวัง ข้อมูลข่าวสาร เนื้อหาต่างๆ ที่มีความเกี่ยวข้องและสร้างผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของประเทศตลอดเวลา สิ่งไหนที่สามารถตอบโต้ได้ก็ทำไปด้กฎหมาย เราที่จะพยายามสร้างเนื้อหา เพื่อสร้างความเข้าใจที่ถูกต้องแก่พี่น้องประชาชน ขณะเดียวกันยังตรวจสอบไปยังแหล่งที่มาของการสร้างความเสียหาย เพื่อประสานกับหน่วยงานที่เกี่ยวข้องไม่ว่าจะเป็นสำนักงานตำรวจแห่งชาติ กระทรวงไอซีที เพื่อดำเนินการตามกฎหมายต่อไป ” พอ.ศุภชัยไซเบอร์กล่าว และว่านอกจากเรื่องระบบข้อมูลแล้ว ศูนย์ไซเบอร์ยังมีหน้าที่รณรงค์ปลูกฝังให้ความรู้แก่ ข้าราชการทหารและประชาชนให้เกิดความ

ตระหนัก ในการใช้เครื่องมือสื่อสารอย่างชาญฉลาดปลอดภัยไม่ตกเป็นเหยื่อ หรือเป็นพาหะในการแพร่กระจายความผิด โดยไม่รู้อะไรถึงการณ์อีกด้วย ”

เร่งพัฒนาับรบอย่างต่อเรื่องทั้งเชิงรุกและเชิงรับ

พล.ต.ฤทธิ บอกรว่า การปฏิบัติการของศูนย์ไซเบอร์ในปัจจุบันให้น้ำหนักไปที่เชิงรับ คือการพัฒนาาระบบป้องกันเครือข่ายข้อมูลของหน่วยงานในกองทัพ ส่วนเชิงรุกเนื่องจากประเทศไทยยังไม่มิกฎหมายรองรับ แต่ก็ได้สร้างและพัฒนาคนไว้อย่างต่อเนื่อง ดังเช่นการแข่งขันระบบงานจำลองการฝึกด้านไซเบอร์ (Cyber Range) ภายใต้งาน “อาร์มี ไซเบอร์คอนเทสต์ 2015” (Army Cyber Contest 2015) ที่ผ่านมานั่นเอง

“ ในเชิงรุก ยืนยันว่ากองทัพไม่ได้มีพัฒนาคนเพื่อไปละเมิดกฎหมายหรือสิทธิเสรีภาพของประชาชนอย่างแน่นอน เป็นหลักของการปฏิบัติงานในหน่วยงานอยู่แล้ว ”

ขณะเดียวกัน พล.ต.ฤทธิ บอกรอีกว่า ในอนาคตกองทัพเตรียมพัฒนาหลักสูตรไซเบอร์เป็นของตัวเอง เนื่องจากปัจจุบันสร้างคนจากหลักสูตรของสถาบันและบริษัทเอกชนอื่นที่มีหลักสูตรเรื่องการรักษาความ

ปลอดภัยด้านสารสนเทศ หรือ ไซเบอร์ซีเคียวริตี้ และอีกหนึ่งความคาดหวังของ พอ.ไซเบอร์ ก็คือ การลงทุนกับเทคโนโลยีที่ทันสมัย

“ มนุษย์มีข้อจำกัดทางด้านสมอง และร่างกาย เพราะฉะนั้นจึงจำเป็นต้องมีเครื่องมือเทคโนโลยีที่ทันสมัยเข้ามาช่วยเฟ้าะวัง คัดกรองข้อมูล หรือจัดการกับภัยคุกคามแทนคนมากกว่าที่เป็น เนื่องจากปัจจุบันมีการกระทำผิดในโลกไซเบอร์เยอะมาก ส่วนตัวเชื่อว่าอำนาจกำลังรบที่ไม่มีตัวตน และลงทุนน้อยเป็นที่เรื่องควรให้ความสำคัญ เพราะเป็นเครื่องมือที่จะช่วยรักษาความมั่นคงของประเทศที่ค่อนข้างได้ผลไม่น้อยหน้ากว่าอาวุธยุทโธปกรณ์ แสนยานุภาพกำลังรบอื่นๆ เพราะแฮกเกอร์คนเดียว อาจะหยุดกองทัพได้ทั้งกองเลยก็ได้ ”

สงครามไซเบอร์กำลังทรงพลัง และทรงประสิทธิภาพมากกว่าการใช้อาวุธยุทโธปกรณ์ เราสามารถที่จะใช้การปฏิบัติการไซเบอร์สร้างความเข้าใจ บิดเบือน ชี้นำ หรือควบคุมอาวุธยุทโธปกรณ์ของฝ่ายตรงข้ามให้หันไปทางอื่น หรือโจมตีกันเองก็ได้ นับเป็นการเปลี่ยนวิถีการรบในอนาคตอย่างแท้จริง

