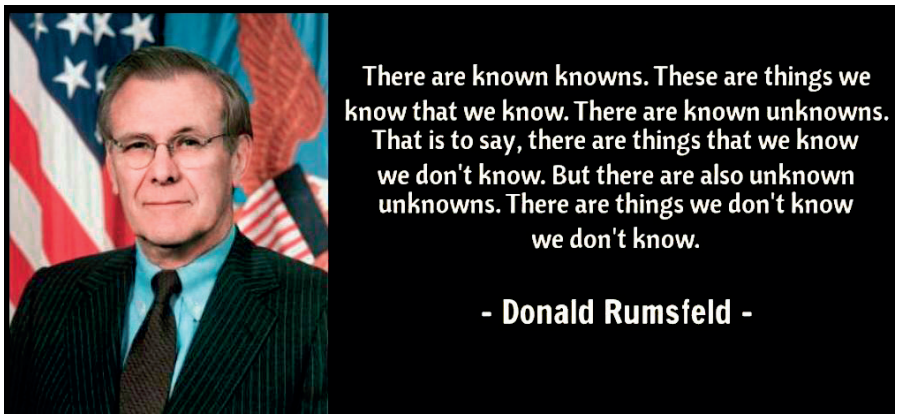
การปฏิวัติในกิจการทหาร : การรับมือการก่อการร้ายบนโลกไซเบอร์

(Revolution in Military Affairs : Handling with Cyber Terrorism)

พันเอก พิศาล อมรรัตนานุภาพ
ผู้ช่วยผู้อำนวยการกองข่าวความมั่นคง สำนักข่าวกรอง กรมข่าวทหาร

"UNKNOWN UNKNOWNS : the ones we don't know we don't know"
(เราไม่รู้ว่า เราไม่รู้อะไร)
Secretary of Defense Donald Rumsfeld : February 12, 2002
(นายโดนัลด์ รัมเฟลล์ รัฐมนตรีว่าการกระทรวงกลาโหมสหรัฐฯ)

เมื่อปี ๒๐๐๒ (พ.ศ.๒๕๔๕) นายโดนัลด์ รัมเฟลล์ รัฐมนตรีว่าการกระทรวงกลาโหมสหรัฐฯ (ในขณะนั้น) ได้ใช้วลีอันเป็นที่โด่งดัง **"UNKNOWN UNKNOWNS : เราไม่รู้ว่า เราไม่รู้อะไร"** ในการแถลงการณ์หลังจากสหรัฐฯ ถูกกลุ่มก่อการร้ายอัล-กออิดะห์ (Al-Qaeda) จี้เครื่องบินของสายการบินสหรัฐฯ และพุ่งเข้าชนสถานที่ที่สำคัญหลายแห่ง (เหตุการณ์ ๙/๑๑) อาทิ สถานที่อันเป็นสัญลักษณ์ทางเศรษฐกิจของสหรัฐฯ และโลก (World Trade Center) ส่งผลให้เศรษฐกิจและตลาดหุ้นวอลล์สตรีท (Wall Street) หยุดชะงักไปในห้วงเวลาหนึ่ง โดยนายรัมเฟลล์ ได้ระบุว่าความสำเร็จของการก่อเหตุ ๙/๑๑ เกิดจากสาเหตุที่เจ้าหน้าที่ด้านการข่าวตกอยู่ในสภาวะที่ตนเองไม่รู้ว่าตนเองไม่รู้อะไร (อาทิ ขีดความสามารถของกลุ่มก่อการร้ายอัล-กออิดะห์ในการก่อเหตุรุนแรงในเขตเมือง) เพื่อเป็นการป้องกันประวัติศาสตร์จะซ้ำรอยเดิม ต่อมาในปี ๒๐๐๕ (พ.ศ.๒๕๔๘) รัฐบาลสหรัฐฯ จึงได้เขียนยุทธศาสตร์ชาติเพื่อใช้ในการวางแผนป้องกันประเทศ และเพื่อเตรียมการสำหรับยุคศตวรรษที่ ๒๑ (National Defence Strategy : NDS) โดยในเอกสารได้เน้นย้ำว่ากระทรวงกลาโหม (ทั้งโลก) จะต้องค้นหา UNKNOWN UNKNOWNS ให้พบและรีบนำมาเปลี่ยนให้เป็น **"เรารู้และเข้าใจว่าไม่รู้อะไร"** หรือที่เรียกว่า "KNOWN UNKNOWS" โดยนัยสำคัญคือการปฏิวัติเทคโนโลยี (Technology Revolution) เพื่อให้มีความพร้อมในการทำสงครามบนโลกดิจิทัลซึ่งเป็นยุคที่มิได้มุ่งเน้นในการทำลายเพื่อให้เกิดการสูญเสียชีวิต หากแต่เป็นการยุทธ์เพื่อขัดขวางระบบและเครือข่าย "System - Disruptive challenges" โดยมีวัตถุประสงค์ไม่ให้ระบบเครือข่ายดำเนินการได้ตามปกติ ส่วนในเรื่องของเป้าหมายการโจมตี ได้แก่ ระบบโครงสร้างสาธารณูปโภคขั้นพื้นฐานที่สำคัญ ๓ ระบบ ได้แก่ การขนส่งพลังงาน การสื่อสารโทรคมนาคมและเครือข่ายคอมพิวเตอร์ ลักษณะเช่นนี้อาจเรียกได้ว่าเป็นสงครามไซเบอร์เพื่อเป็นการเตรียมการระวังป้องกัน ปัจจุบันกองทัพสหรัฐฯ



นายโดนัลด์ รัมเฟลล์ รัฐมนตรีว่าการกระทรวงกลาโหมสหรัฐฯ (ปี ๒๐๐๑ – ๒๐๐๖)

ภายใต้การควบคุมของ กองบัญชาการไซเบอร์ (USCYBERCOM) จึงได้ออกยุทธศาสตร์การตั้งรับบนแนวหน้า “Defend Forward” ที่มีภารกิจสำคัญบนเครือข่ายไซเบอร์ทั่วโลก ๒ ประการ ทั้งเชิงรุกและเชิงรับ กล่าวคือ **ข้อแรก** ในเชิงรุกคือการใช้เพื่อเป็นเครื่องมือในการลาดตระเวน/สอดแนม/หาข่าว (ISR) หรือการจารกรรม “Espionage” โดยสายลับ **ข้อสอง** ในเชิงรับคือการใช้เพื่อรับมือจากปฏิบัติการขัดขวางระบบโครงสร้างพื้นฐานทางโทรคมนาคม

จากข้อค้นพบที่ได้ศึกษาจากเอกสารทางวิชาการที่เขียนโดย Mazanec & Whyte และ Martin & Weinberg พบว่ามีความเห็นพ้องตรงกับนายโดนัลด์ รัมเฟลล์ ในเรื่องของวิวัฒนาการของสงครามแห่งยุคศตวรรษที่ ๒๑ ที่จะเป็นสงครามบนโลกดิจิทัลซึ่งจะดำเนินกลยุทธ์ผ่านสมรภูมิที่ ๕ เป็นหลัก สงครามบนโลกไซเบอร์ โดยตัวแสดง (actor) บนสมรภูมินี้จะมีหลากหลายที่ประกอบด้วย ตัวแสดงที่เป็นรัฐ ไม่ใช่รัฐ ตัวแทนแห่งรัฐ และผู้ก่อการร้าย (State Actor – Non State Actor – Proxies – Terrorists) ในการสร้างความได้เปรียบจะขึ้นอยู่กับความสามารถด้านการใช้เทคโนโลยีของแต่ละฝ่าย ซึ่งฝ่ายรัฐจะต้องเข้าใจและยอมรับว่าบนโลกไซเบอร์ทุกตัวแสดงต่างมีความเสมอภาคในการทำสงคราม อันเนื่องมาจากความง่ายในการเรียนรู้และความสะดวกในการเข้าถึงอุปกรณ์ดิจิทัลและเครือข่ายอีกทั้งมีต้นทุนที่ไม่สูงมาก ในภาพรวมความหมายในเรื่องการปฏิวัติในกิจการทหารในยุคศตวรรษที่ ๒๑ (Revolution in Military Affairs : RMA) หัวใจคือ การเปลี่ยนถ่ายให้องค์กรเป็น **“องค์กรดิจิทัล” (Digital Transformation)** แต่การลงมือจริงยังคงมีประเด็นที่เป็นปัญหาและ

(อดีต) การจารกรรมข้อมูลโดยสายลับ “Espionage” (ภาพยนตร์ Mission Impossible)

อุปสรรคที่สำคัญต่อการเปลี่ยนแปลงที่สามารถจำแนกเป็น ๒ ประเด็นหลักคือ **ข้อแรก** การเตรียมความพร้อมของบุคลากรในการใช้เครื่องมือที่ทันสมัยเพื่อใช้ในการรับมือและ/หรือตอบโต้ภัยคุกคามรูปแบบใหม่ในขั้นพื้นฐานโดยเฉพาะขีดความสามารถเชิงรับ อาทิ การใช้การเข้ารหัสแบบสมมาตร (Symmetric Encryption) เพื่อเป็นการรักษาความปลอดภัยของการเข้ารหัส หรือการรักษาความลับระหว่างการรับ - ส่งข้อมูล **ข้อสอง** การเพิ่มประสิทธิภาพของฝ่ายความมั่นคงในการป้องกันทางกายภาพของโครงสร้างสารสนเทศ (Physical Layer) ที่เปรียบเสมือนกระดูกสันหลังของระบบดิจิทัล อาทิ สายเคเบิ้ลไฟเบอร์ออฟติค ระบบและคลื่นสัญญาณโทรศัพท์และดาวเทียม ซึ่งทั้งหลายทั้งปวงการป้องกันภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพจะต้องเป็นการประสานสอดคล้องระหว่างความสามารถด้านเทคโนโลยีและความรู้ความเข้าใจควบคู่กันไป **คำถามหลักในบทความนี้คือ : กระทรวงกลาโหมไทยและกองทัพไทยได้มีการปฏิวัติในกิจการทหารเพื่อเตรียมตัวในการรับมือภัยจากสงครามไซเบอร์แล้วหรือยัง?**

“กระทำการใดอันก่อให้เกิดความเสียหายอย่างร้ายแรงแก่ ระบบการขนส่งสาธารณะระบบโทรคมนาคม หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ... ถ้าการกระทำนั้นได้กระทำโดยมีความมุ่งหมาย...เพื่อสร้างความปั่นป่วนเพื่อให้เกิดความหวาดกลัวในหมู่ประชาชน ผู้นั้นกระทำความผิดฐานก่อการร้าย...”

ประมวลกฎหมายอาญา มาตรา ๑๓๕/๑ พ.ศ.๒๕๔๖ (ความผิดฐานก่อการร้ายในประเทศไทย)

โดยหากจะอ้างถึงกฎหมายข้างต้นพอจะกล่าวได้ว่าผู้ก่อเหตุ/ผู้โจมตีที่มีวัตถุประสงค์ในการทำลายระบบ/เครือข่ายโทรคมนาคมนับว่าเป็นกลุ่มก่อการร้าย แต่ทั้งนี้ในความเป็นจริงชัยชนะแห่งสงครามนั้นขึ้นอยู่กับการทำลายระบบที่สร้าง

ผลกระทบต่อวิถีชีวิตของประชาชนในแนวหลังของฝ่ายตรงข้าม (System - Disruptive challenges) เนื่องจากมีผลทางจิตวิทยา โดยจะส่งผลด้านความเชื่อมั่นในขีดความสามารถของฝ่ายความมั่นคงซึ่งหากจะกล่าวถึง ยุทธการทำลายระบบ/เครือข่ายนั้น มิได้เป็นเรื่องใหม่แต่อย่างใดหากแต่เป็นเหล้าใหม่ในขวดเก่า เพราะที่ผ่านมาได้ใช้เป็นเครื่องมือทางทหาร โดยสามารถศึกษาได้จากบทเรียนของสงครามอ่าวเปอร์เซีย ปี ๑๙๙๐ และ สงครามอิรัก ปี ๒๐๐๓ (พ.ศ. ๒๕๓๓ และ ๒๕๔๖) ที่กองทัพสหรัฐฯ และพันธมิตรเลือกที่จะโจมตีแนวหลังของกองทัพอิรักเพื่อทำลายระบบโครงสร้างพื้นฐานที่สำคัญ และระบบควบคุมบังคับบัญชา (C4I) เพื่อส่งผลให้เกิดปัญหาความล้มเหลวต่อระบบการบริหารจัดการและการให้บริการของรัฐ ซึ่งสุดท้ายประชาชนที่ได้รับผลกระทบจึงไม่ให้ความร่วมมือกับฝ่ายตนเองและนำไปสู่การต่อต้านรัฐบาลนายซัดดัมฯ จากบทเรียนของสงครามดังกล่าวฯ ส่งผลให้ทุกฝ่ายตระหนักดีว่าฝ่ายความมั่นคงที่จะต้องป้องกันไม่ให้ภัยคุกคามส่งผลกระทบต่อแนวหลังอย่างเด็ดขาด โดยหากวิเคราะห์ภัยคุกคามทางไซเบอร์พบว่าทุกตัวแสดง (Actors) ล้วนมีขีดความสามารถในปฏิบัติการเพื่อขัดขวางระบบฯ ทางไซเบอร์ทั้งทางเปิดและทางปิด แต่ส่วนใหญ่มุ่งเน้นไปในการก่อเหตุผ่านยุทธการทางปิด ซึ่งสามารถจำแนกองค์ประกอบได้ ๓ ประการ คือ **ประการแรก : การสร้างเครือข่ายและระดมพลผ่านโลกโซเชียล** โดยทำการเผยแพร่เนื้อหาที่เป็นภัย (Abusive Content) หรือการสร้างข่าวปลอม (Faked News) เพื่อให้เกิดความแตกแยกทางสังคมผ่านความเชื่อแบบสุดโต่งซึ่งรวมไปถึงการสอนวิธีการก่อเหตุรุนแรง โดยจากการศึกษาพบว่ากลุ่มก่อการร้ายไอเอสนับว่าเป็นตัวอย่างที่ควรนำมาศึกษา เพราะได้ประสบความสำเร็จในการใช้ระบบสารสนเทศเพื่อขยายอิทธิพล และใช้ระดมพลกลุ่มผู้สนับสนุนจากต่างประเทศ (Foreign Terrorist Fighters : FTFs) จำนวนมากกว่าร้อยละ ๔๑ ซึ่งมีอายุเฉลี่ย ๒๘ - ๓๑ ปี ที่ได้รับข้อมูลข่าวสารมาจากทางสื่อสังคมออนไลน์ อาทิ Facebook, Youtube และ Ask.fm เป็นต้น **ประการที่สอง : Computer Network Attack (CNA)** ในอดีตได้แก่ การจารกรรม “Classic Espionage” ซึ่งเป็นการก่อเหตุโจมตีในแนวหลังโดยฝีมือของสายลับแต่ในยุคปัจจุบันทุกตัวแสดงนั้นได้ปฏิวัติองค์กรและสมาชิกในการเพิ่มขีดความสามารถเพื่อแสวงประโยชน์จากเทคโนโลยีสมัยใหม่โดยไม่จำเป็นต้องส่งสายลับไปแนวหลังของฝ่ายตรงข้ามอีกต่อไป แต่สามารถปฏิบัติภารกิจด้วยการจารกรรมทางไซเบอร์ (Cyber Espionage) หรือเรียกว่าการแฮ็ก (Hack) เพื่อเข้าถึงข้อมูลต่างๆ เช่น ข้อมูลทางการเงิน ข้อมูลทางด้านเศรษฐกิจ ข้อมูลส่วนตัว **ประการที่สาม ซึ่งเป็นองค์ประกอบที่สำคัญที่สุด คือ การโจมตีที่ออกแบบมาเพื่อขัดขวางการทำงาน “disruptive operations”** โดยเป็นการโจมตีไปยังระบบคอมพิวเตอร์ที่ควบคุมโครงสร้างพื้นฐานที่สำคัญของประเทศ ระบบการเงินการธนาคาร รวมถึงระบบงานต่างๆ ของภาครัฐที่ให้บริการประชาชนผ่านช่องโหว่ของเบราว์เซอร์และแอพพลิเคชั่นต่างๆ ของระบบปฏิบัติการ หรือโจมตีโดยโปรแกรม “มัลแวร์” (Malware)

(ปัจจุบัน) การจารกรรมข้อมูลโดยสายลับ “Espionage”

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ : หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ”

มาตรา ๓ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒

กองทัพไทยในศตวรรษที่ ๒๑ : ฝ่ายความมั่นคงมีความเข้าใจและตระหนักถึงความสำคัญในการป้องกันโครงสร้างพื้นฐาน รวมถึงระบบโทรคมนาคมเป็นอย่างดี จึงได้มีการออกกฎหมายเพื่อเตรียมการป้องกันไว้เป็นเวลาพอสมควร (ประมวล

กฎหมายอาญา มาตรา ๑๓๕/๑ พ.ศ. ๒๕๔๖ : ความผิดก่อการร้ายในประเทศไทย) โดยเพื่อให้สอดคล้องกับสงครามบนโลกดิจิทัลจึงได้มีการเตรียมพร้อมเพื่อรับมือภัยคุกคามทางไซเบอร์ โดยได้มีการออก พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒ ซึ่งได้กำหนดให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. (National Cyber Security Committee : NCSC) เป็นองค์กรที่กำหนดทิศทางและควบคุมการดำเนินงาน โดยมีนายกรัฐมนตรีเป็นประธาน แต่ในการดำเนินงานจะมีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ซึ่งมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธาน และมีกรรมการโดยตำแหน่ง ได้แก่ ผู้บัญชาการทหารสูงสุด และผู้บริหารองค์กรที่เกี่ยวข้องด้านโครงสร้างพื้นฐาน ๖ กลุ่ม โดยรับหน้าที่เป็นผู้ที่กำหนดแนวทางปฏิบัติของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งกลุ่มความมั่นคงและบริการภาครัฐที่สำคัญให้เป็นการกำกับดูแลภายใต้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและกระทรวงกลาโหม เป็นหลัก ทั้งนี้ ใน พ.ร.บ.ไซเบอร์ ปี ๖๒ ฉบับนี้ยังระบุว่าหากเป็นภัยคุกคามระดับ “ร้ายแรง” ขึ้นไป กมช. สามารถมอบอำนาจให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ/หรือ ผู้บัญชาการทหารสูงสุด เป็นผู้ควบคุมการปฏิบัติการโดยมียุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม (ปี ๖๐ - ๖๔) และกำหนดให้ไซเบอร์เป็นมิติหนึ่งของสงครามที่ต้องจัดเตรียมกำลังและใช้กำลัง เช่นเดียวกับมิติของการสงครามอื่นๆ และกองบัญชาการกองทัพไทย ได้จัดทำยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย ไว้เพื่อรองรับต่อสถานการณ์ภัยคุกคามทางไซเบอร์ไว้เป็นที่เรียบร้อยแล้วเช่นกัน ในเรื่องการเพิ่มขีดความสามารถของกำลังพลทุกกองทัพของไทยได้เน้นการฝึกทักษะขีดความสามารถเชิงรับ เช่น ด้านการป้องกันโครงสร้างพื้นฐานและด้านการเฝ้าระวัง

จากการที่รัฐบาลไทยออกกฎหมาย (พ.ร.บ.ไซเบอร์ ๖๒) อีกทั้งได้ทำการปฏิรูปกองทัพให้มุ่งหน้าสู่ “Digital Transformation” นั้นย่อมเป็นหลักฐานเชิงประจักษ์ว่าฝ่ายความมั่นคงมีความเข้าใจและตระหนักถึงผลกระทบจากภัยคุกคามรูปแบบใหม่บนโลกไซเบอร์ โดยได้มีการสถาปนาหน่วยงานด้านไซเบอร์ อาทิ ศูนย์ไซเบอร์กระทรวงกลาโหม และหน่วยไซเบอร์ระดับปฏิบัติการของเหล่าทัพ อีกทั้งยังมีกฎหมายรองรับให้การทำงานเป็นไปด้วยความถูกต้องตามมาตรฐานสากล ดังนั้น คำตอบ : ของคำถามถามหลักในบทความนี้จึงสามารถระบุได้ว่า : **กระทรวงกลาโหมและกองทัพไทยได้มีการปฏิวัติในกิจการทหารเพื่อเตรียมตัวในการรับมือภัยจากสงครามไซเบอร์ โดยได้ทำการเปลี่ยนสิ่งที่เราไม่รู้ว่าเราไม่รู้ (UNKNOWN UNKNOWNS) มาเป็นสิ่งที่เรารู้ว่าเราไม่รู้ (KNOWN UNKNOWNS) เป็นที่เรียบร้อยแล้ว** ⊙

Reference

Fridman, O 2018, Russia *‘Hybrid Warfare’: Resurgence and Politicisation,* Hurst& Company, London

Martin, S & Weinberg, L 2017, *The Role of Terrorism in Twenty-First-Century Warfare,* Manchester University Press, Manchester

Mazanec, B & Whyte, C 2019, *Understanding Cyber Warfare: Politics, Policy and Strategy,* Routledge, New York

Mulliins, S 2016, *‘Home-Grown’ Jihad: Understanding Islamist Terrorism in the US and UK,* Imperial Col lege Press, London

Pomerleau M 2019, Here’s how Cyber Command is using ‘defend forward’, 12th November, *CyberCon,* viewed 4th June 2020<https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/>

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 (2019), 27th May, viewed 29th May 2020 <http://www.ratchakitcha.soc.go.th/DATA PDF/2562/A/069/T_0020.PDF>