# แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย

โดย

พลตรี สุชาติ ผ่องพุฒิ
รองเจ้ากรมการทหารสื่อสาร
กองทัพบก กระทรวงกลาโหม

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักรภาครัฐร่วมเอกชน รุ่นที่ ๒๖
ประจำปีการศึกษา พุทธศักราช ๒๕๕๖ – ๒๕๕๗

# บทคัดย่อ

**เรื่อง** แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย

**ลักษณะวิชา** วิทยาศาสตร์และเทคโนโลยี

**ผู้วิจัย** พลตรี สุชาติ ผ่องพุฒิ **หลักสูตร** ปรอ. **รุ่นที่** 26

การทำเอกสารวิจัยฉบับนี้มีวัตถุประสงค์เพื่อหาแนวทางที่เหมาะสมและสามารถดำเนินการได้อย่างเป็นรูปธรรมในการรองรับสงครามไซเบอร์ของกองทัพไทย โดยมีการศึกษาความเป็นมา นิยามต่างๆ อีกทั้งยังมีการรวบรวมข้อมูลแนวทางการรองรับสงครามไซเบอร์ ทั้งในประเทศและต่างประเทศ ที่มีอยู่ในปัจจุบัน ว่าจะสามารถรับมือกับภัยคุกคามต่างๆ เหล่านั้นได้มากน้อย เพียงใด นอกจากนั้นยังจะมีการศึกษายุทธศาสตร์ทางด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ของรัฐบาล และมีการศึกษาเปรียบเทียบกับโครงสร้าง หรือแนวทางของหน่วยงานของกองทัพไทยในปัจจุบัน ตลอดจนการรวบรวมบทเรียนของสงครามไซเบอร์ที่ผ่านมา เพื่อเป็นบรรทัดฐานในงานวิจัย

หลังจากได้ทำการวิจัยด้วยการสัมภาษณ์ การรวบรวมและจำแนกภัยคุกคามทางด้านไซเบอร์ต่อกองทัพไทย ได้พบว่าภัยคุกคามที่กองทัพไทยให้ความสำคัญมีด้วยการ 4 รูปแบบแตกต่างกันในด้านขอบเขต และวัตถุประสงค์ในการดำเนินการ และมีการกำหนด ขอบเขตของการรองรับสงครามไซเบอร์ ในกรอบมุมมองของกองทัพ ตามระดับของภัยคุกคาม แบ่งเป็น 3 ระดับ ได้มีการกำหนดกรอบในการรองรับ ในการดำเนินการทางด้านสงครามไซเบอร์ของกองทัพไทย เพื่อรองรับสงครามไซเบอร์ในอนาคตออกเป็น 4 ด้านอีกด้วย และมีการการกำหนดกรอบระยะเวลาในการดำเนินการทางด้านสงครามไซเบอร์ แบ่งออกเป็น 3 ระยะ มีข้อเสนอแนะเพื่อการปรับภารกิจในภาพรวมของหน่วยในกองทัพเพื่อการปฏิบัติการสงครามไซเบอร์ โดยแยกการดำเนินการออกได้เป็น 2 รูปแบบ ได้แก่ งานสนับสนุนการรบหลัก และ งานในสายเทคนิคหรือผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของกองทัพ ตลอดจากการนำเสนอโครงสร้างหน่วยงานของกองทัพที่จะรองรับสงครามไซเบอร์อย่างเป็นรูปธรรมต่อไป

# คำนำ

ความก้าวหน้าของเทคโนโลยีเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมโยงกันทั่วโลก นอกจากประโยชน์ในด้านการติดต่อสื่อสารทั้งด้านพลเรือน และด้านการทหารแล้ว กิจกรรมของในเครือข่ายคอมพิวเตอร์ดังกล่าว หรือที่รู้จักกันในชื่อว่าเครือข่ายอินเตอร์เน็ต เครือข่ายดังกล่าว ยังสร้างเป็นอาวุธหรือเป็นอาวุธใหม่ในโลกของฝ่ายการทหารและในภาวะสงครามได้ด้วย แน่นอนว่าการทำสงครามย่อมมีการเปลี่ยนแปลงไปจากเดิม

สงครามรูปแบบใหม่โดยการใช้เครือข่ายอินเตอร์เน็ต หรือที่เรียกว่า สงครามไซเบอร์ โดยสงครามนี้ ไม่มีความจำเป็นต้องใช้กำลังอาวุธที่จับต้องได้ หรืออาวุธที่เป็นกายภาพ แต่เพียงการโจมตีเป้าหมายอาศัยเพียงเครื่องคอมพิวเตอร์เท่านั้น ที่จะสร้างความเสียหายอย่างกว้างขวางได้

งานวิจัยนี้ เพื่อสร้างความเข้าใจในสงครามไซเบอร์ให้กองทัพของเราได้มีความตระหนักต่อรูปแบบสงครามรูปแบบใหม่ และมีแนวทางในการรองรับในอนาคต หากเกิดการโจมตีต่อประเทศของเรา จะมีแนวทางรับมือได้อย่างไร

หากงานวิจัยนี้มีขาดตกบกพร่องด้วยประการใด ก็ขออภัยมา ณ โอกาสนี้ด้วย

พลตรี

( สุชาติ ผ่องพุฒิ )
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร ปรอ. รุ่นที่ 26
ผู้วิจัย

# สารบัญ

# สารบัญ (ต่อ)

# สารบัญตาราง

**หน้า**

**ตารางที่**

# สารบัญแผนภาพ

หน้า

**แผนภาพที่**

# บทที่ 1
# บทนำ

## ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศมีบทบาทเป็นอย่างมากในปัจจุบัน ดังจะเห็นได้จากหน่วยงานต่าง ๆ เช่น รัฐบาล ภาครัฐ ภาคเอกชน หรือแม้กระทั้ง ประชาชนทั่วไป ต่างมี แนวความคิดที่จะนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้งานในกิจกรรมต่าง ๆ เพื่อให้กิจกรรมนั้น ๆ เกิดประสิทธิภาพสูงสุด เป็นยุคของสังคมออนไลน์ และเมื่อระบบสารสนเทศ ได้ถูกนำมาใช้กับกิจกรรมต่าง ๆ อย่างแพร่หลาย ย่อมเป็นสิ่งที่หลีกเลี่ยงไม่ได้ที่กิจกรรมทางทหารจะนำสารสนเทศมาใช้งานทั้งทางด้านการบริหารจัดการและในสนามรบ ทำให้สารสนเทศเปรียบเสมือนทรัพยากรที่มีความสำคัญยิ่ง

แน่นอนว่าทรัพยากรทางด้านสารสนเทศ โดยเฉพาะข้อมูลการปฏิบัติการทางทหาร ข้อมูลอาวุธ ยุโธปกรณ์ต่างๆ เมื่อมีการเก็บบันทึกว่าในรูปของข้อมูลดิจิตอล และมีการเชื่อมโยงเพื่อการใช้งานด้วยเครือข่ายคอมพิวเตอร์ ย่อมจะเป็นเป้าหมายของฝ่ายตรงข้าม

เมื่อฝ่ายตรงข้ามต้องการที่จะโจมตีหรือการเจาะข้อมูลที่สำคัญของเรา การรับมือดังกล่าวของกองทัพไทย เพื่อการป้องกันข้อมูล หรือไปถึงขั้นการตอบโต้การโจมตี ต้องมีการดำเนินการอย่างเป็นระบบและมีการกรอบการทำงานที่ชัดเจน เป็นรูปธรรม และเป็นไปตามนโยบายของรัฐบาลที่ได้มีการกำหนดไว้แล้ว

รัฐบาลได้มีการแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee: NCSC) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการ โดยมีหน้าที่หลักในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามในไซเบอร์ ที่กระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ตลอดจนติดตามและประเมินผลการปฏิบัติที่เกี่ยวข้องเพื่อให้เกิดการบูรณาการการทำงานของหน่วยงานต่างๆ ที่เกี่ยวข้อง อันจะก่อให้เกิดประสิทธิภาพและประสิทธิผลในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

จากงานประชุมสัมมนา 25th Annual FIRST Conference 2013 ซึ่งประเทศไทยเป็นเจ้าภาพจัดการประชุม ระหว่างวันที่ 16 – 21 มิถุนายน 2556 ณ ห้อง Grand Ballroom โรงแรม Conrad Hilton กรุงเทพฯ โดยหัวข้อหลักของงานเป็นประเด็น Incident Response : Sharing To Win ที่ประชุมฯ เห็นชอบร่างกรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมียุทธศาสตร์หลัก 3 ด้าน คือ 1) การบูรณาการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ 2) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ และ 3) การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ และ ยุทธศาสตร์รอง 5 ด้าน คือ 4) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ 5) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ 6) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ 7) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ 8) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ ซึ่งรัฐบาลจะนำยุทธศาสตร์ทั้ง 8 นี้เป็นกรอบการพัฒนาความมั่นคงปลอดภัยไซเบอร์สำหรับประเทศไทยใน 5 ปีข้างหน้า โดยมอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA (สพธอ.) เป็นฝ่ายงานเลขานุการ ซึ่งเป็นหน่วยงานในสังกัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารทำหน้าที่เป็นแกนหลักในการขับเคลื่อนยุทธศาสตร์ในภาคเศรษฐกิจและสังคม ขณะที่ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กระทรวงกลาโหม ในฐานะผู้ช่วยเลขานุการ จะทำหน้าที่ผลักดันการพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานด้านความมั่นคงของประเทศ และมีสำนักงานตำรวจแห่งชาติเป็นกำลังสำคัญในการบังคับใช้กฎหมายเพื่อธำรงไว้ซึ่งความสงบเรียบร้อยในราชอาณาจักร

เมื่อพิจารณาถึงนโยบายภาครัฐข้างต้นทำให้ เชื่อได้ว่ามีการกิจกรรมไซเบอร์บางอย่างที่จะเป็นภัยคุกคามที่สำคัญในระบบประเทศ ในที่นี้ก็คือ “สงครามไซเบอร์ “ หรือ Cyber Warfare เป็นสงครามที่ไม่ได้เป็นการใช้อาวุธเข้าสู้รบกัน แต่เป็นการใช้เทคโนโลยีคอมพิวเตอร์เข้าดำเนินการฝ่ายตรงอาจจะเป็นรัฐหรือชาติใดก็ตาม ที่ได้มีการดำเนินการแทรกซึมเข้าไปในเครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของฝ่ายเรา หรือเป้าหมาย เพื่อหวังทำลายหรือสร้างความแตกแยก หรือเพียงแค่การลักลอบขโมยข้อมูล ความลับทางทหารของเป้าหมาย เมื่อเกิดกรณีดังกล่าวขึ้น จะส่งผลที่เป็นอันตรายหรือความไม่ปลอดภัย ต่อการปฏิบัติการทางทหารต่างๆ ทั้งภาคพื้นดิน ภาคพื้นอากาศ และภาคทะเล อย่างกว้างขวาง

## วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวคิดทางด้านสงครามไซเบอร์ ในหลากหลายรูปแบบ
2. เพื่อศึกษาภัยคุกคามทางด้านสงครามไซเบอร์ที่ส่งผลกระกระทบต่อความมั่นคงของชาติ
3. เพื่อการประเมินศักยภาพต่อกองทัพในด้านสงครามไซเบอร์
4. เพื่อเสนอแนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย

## ขอบเขตของการวิจัย

1. เน้นการวิจัยเฉพาะกระบวนการและรูปแบบในการกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ของกองทัพไทย

2. ในส่วนของการปรับปรุงบทบาทและโครงสร้างของหน่วยรับผิดชอบหลัก จะเป็นเพียงการเสนอแนวคิดหรือหลักการกว้าง ๆ โดยไม่พิจารณาลึกในรายละเอียดของผังการจัดหน่วย

3. จะวิจัยเฉพาะนโยบายที่เปิดเผยได้เท่านั้น

## วิธีดำเนินการวิจัย

ครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์กระบวนการ รูปแบบ และลักษณะของนโยบายความมั่นคงทางไซเบอร์ของประเทศไทย และเปรียบเทียบกับต่างประเทศบางประเทศ โดยมุ่งเน้นการวิเคราะห์ความชัดเจน ความเฉพาะเจาะจง ความสามารถในการแปลงไปสู่แผนการปฏิบัติ ความเหมาะสมของเนื้อหากับกรอบเวลา รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิเพื่อให้ได้แนวทางในการกำหนดนโยบายความมั่นคงไซเบอร์แห่งชาติที่เหมาะสมกับกองทัพไทยในห้วงเวลา ซึ่งมีความชัดเจน และแปลงไปสู่แผนการปฏิบัติได้จริง

## ประโยชน์ที่ได้รับจากการวิจัย

1. จะทำให้ได้แนวทางในการปรับปรุงกระบวนการ และรูปแบบในการกำหนดความมั่นคงทางไซเบอร์ ซึ่งจะช่วยให้หน่วยปฏิบัติสามารถออกแผนรองรับได้ในทิศทางเดียวกัน เพื่อให้บรรลุเป้าหมายในภาพรวม

2. ได้แนวคิดในการปรับบทบาท และโครงสร้างของหน่วยรับผิดชอบหลักในการกำหนดความมั่นคงทางไซเบอร์ เพื่อให้สามารถปฏิบัติงานให้ได้นโยบายที่เหมาะสมและปฏิบัติได้จริง

## คำจำกัดความ

| | |
|---|---|
| ไซเบอร์สเปช (Cyberspace) | หมายถึง เป็นภาวะนามธรรมเชิงอุปลักษณ์ ใช้ในด้านปรัชญา หรือคอมพิวเตอร์ เป็นความจริงเสมือนซึ่งแทนโลกในทฤษฎีทางปรัชญาของ คาร์ล ปอปเปอร์ (Karl Popper) ซึ่งรวมทั้งสิ่งต่างๆ ในคอมพิวเตอร์จนถึงระบบเครือข่าย |
| สงครามไซเบอร์ | หมายถึง เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก |
| ความมั่นคงทางไซเบอร์ | หมายถึง การป้องกันอันตรายในโลกออนไลน์ ที่มีผลกระทบต่อตัวผู้ใช้งานและทรัพย์สิน (ข้อมูล) |
| การโจมตีทางไซเบอร์ | หมายถึง เป็นการกระทำของฝ่ายตรงข้ามหรือผู้ก่อการร้ายทำการโจมตีจุดสำคัญที่เป็นหัวใจของระบบคอมพิวเตอร์โดยการผ่านระบบเครือข่ายโทรคมนาคมและเครือข่ายคอมพิวเตอร์ เพื่อให้เป้าหมายได้รับผลกระทบอย่างใดอย่างหนึ่ง |
| อาชญากรรมทางไซเบอร์ | หมายถึง อาชญากรรมทางคอมพิวเตอร์ ที่มีการกระทำดังนี้<br>1.การกระทำการใด ๆ เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และ ผู้กระทำได้รับผลประโยชน์ตอบแทน<br>2.การกระทำผิดกฎหมายใด ๆ ซึ่งใช้เทคโนโลยี คอมพิวเตอร์เป็นเครื่องมือและในการสืบสวน สอบสวนของเจ้าหน้าที่เพื่อนำผู้กระทำผิดมาดำเนินคดีต้องใช้ความรู้ทางเทคโนโลยีเช่นเดียวกัน<br>การประกอบอาชญากรรมทางคอมพิวเตอร์ได้ก่อให้เกิดความเสียหายต่อเศรษฐกิจของประเทศจำนวนมหาศาล อาชญากรรมทางคอมพิวเตอร์ จึงจัดเป็นอาชญากรรมทางเศรษฐกิจ หรืออาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ<br>อาชญากรทางคอมพิวเตอร์ แบ่งได้ดังนี้<br>1. พวกเด็กหัดใหม่ (Novice)<br>2. พวกวิกลจริต (Deranged persons) |

3. อาชญากรที่รวมกลุ่มกระทำผิด (Organized crime)
4. อาชญากรอาชีพ (Career)
5. พวกหัวพัฒนา มีความก้าวหน้า(Con artists)
6. พวกคลั่งลัทธิ ( Dreamer ) / พวกช่างคิดช่างฝัน (Ideologues)
7. ผู้ที่มีความรู้และทักษะด้านคอมพิวเตอร์อย่างดี (Hacker/Cracker )

ภัยคุกคาม (threats) หมายถึง เหตุการณ์ต่างๆ ที่เป็นไปได้หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจส่งผลกระทบหรือสร้างความเสียหายต่อระบบสารสนเทศของกองทัพบก

ช่องโหว่ (vulnerabilities) หมายถึง จุดอ่อนของทรัพย์สินหรือมาตรการ ที่เป็นช่องทางเกิดปัจจัยเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อทรัพย์สินหรือต่อระบบสารสนเทศของกองทัพบก

แฮกเกอร์ ( Hacker ) หมายถึง บุคคลผู้ที่เป็นอัจฉริยะ มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในคอมพิวเตอร์โดยเจาะผ่านระบบ รักษาความปลอดภัยของคอมพิวเตอร์ได้ แต่อาจไม่แสวงหาผลประโยชน์

แคกเกอร์ (Cracker) หมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดี จนสามารถเข้าสู่ระบบได้ เพื่อเข้าไปทำลายหรือลบแฟ้มข้อมูล หรือทำให้ เครื่องคอมพิวเตอร์ เสียหายรวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์

เหตุการณ์ด้านความมั่นคงปลอดภัย (Security incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของกองทัพบกหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรืออาจสร้างความเสียหายได้ในที่สุดซึ่งอาจส่งผลให้

1. เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ เช่น ระบบงานสารสนเทศของหน่วยเกิดการหยุดชะงัก เป็นต้น
2. เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของกองทัพบก

3. เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กำหนดไว้
4. เกิดภาพลักษณ์ที่ไม่ดีต่อกองทัพบกหรือทำให้สูญเสียชื่อเสียง เช่น การไปโพสต์ข้อความ
พาดพิงถึงกองทัพบกในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของกองทัพบก เป็นต้น
5. ตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัย ได้แก่ โปรแกรมไม่พึงประสงค์ การพบจุดอ่อนในซอฟต์แวร์ ระบบงานหรือฮาร์ดแวร์ที่ใช้งาน การแจ้งเตือนของระบบป้องกันการบุกรุก ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต การใช้ทรัพยากรของหน่วยงานผิดวัตถุประสงค์ เช่น การใช้เครือข่ายของหน่วยงานเพื่อกระทำการที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เพื่อกระทำการที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา เพื่อทำการส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่
เป็นต้น ระบบถูกโจมตีจนไม่สามารถให้บริการได้ ระบบอุปกรณ์ ฮาร์ดแวร์ หรือทรัพย์สินในระบบสารสนเทศอื่นๆ ถูกขโมย การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของกองทัพบก การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่นๆ ที่เป็นการละเมิดระเบียบฉบับนี้
6. ตัวอย่างของเหตุการณ์ที่เป็นจุดอ่อน ได้แก่ ประตูศูนย์คอมพิวเตอร์ไม่สามารถปิดให้สนิทได้ ระบบงานสารสนเทศของหน่วยมีช่องทางอื่นในการเข้าสู่ระบบได้โดยไม่ผ่านการพิสูจน์ตัวตนตามปกติ เจ้าหน้าที่รักษาความปลอดภัยของหน่วยไม่เข้มงวดหรือละเลยการปฏิบัติหน้าที่ บุคคลภายนอกสามารถเดินตามเจ้าหน้าที่เข้าห้องระบบสารสนเทศของหน่วยโดยไม่มีการแลกบัตรผ่าน บุคคลภายนอกไม่ได้ลงชื่อก่อนเข้าศูนย์คอมพิวเตอร์

ของหน่วย เจ้าหน้าที่ไม่มีการระบุตัวตนก่อนที่จะเข้าถึงห้องระบบสารสนเทศของหน่วยนั้น

7. เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ที่เป็นจุดอ่อน จำเป็นต้องได้รับรายงานจากผู้ใช้งานเพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสมได้ผลและทันกาล

มัลแวร์ (Malware)

หมายถึง ย่อมาจาก “Malicious Software” โปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์และเครือข่าย ที่บุกรุกเข้าไปติดอยู่ในระบบคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้ และสร้างความเสียหายให้กับระบบคอมพิวเตอร์นั้นๆ และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์เครื่องอื่นๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่าย หรือระบบสื่อสารข้อมูล ไวรัสก็อาจแพร่ระบาดได้เช่นกัน หรือเป็นคำที่ใช้เรียกโปรแกรมที่มีจุดประสงค์ร้ายต่อ ระบบคอมพิวเตอร์ทุกชนิดแบบรวมๆ นั่นเอง โปรแกรมพวกนี้ก็เช่น Virus, Worm, Trojan, Adware, Spyware, Key logger, hack tool, dialer, phishing, toolbar, BHO, Joke, etc

แต่เนื่องจาก ไวรัส (Virus) คือ Malware ชนิดแรกที่เกิดขึ้นบนโลกนี้และอยู่มานาน ดังนั้นโดยทั่วไปตามข่าวหรือบทความต่างๆ ที่ไม่เน้นไป ในทางวิชาการมากเกินไป หรือเพื่อความง่าย ก็จะใช้คำว่า virus แทนคำว่า malware แต่ถ้าจะคิดถึงความจริงแล้วมันไม่ถูกต้อง เพราะ malware แต่ละชนิดไม่เหมือนกัน

คำอธิบายของ Malware แต่ละชนิด :
Virus = แพร่เชื้อไปติดไฟล์อื่นๆ ในคอมพิวเตอร์โดยการแนบตัวมันเองเข้าไป แต่มันไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้ ต้องอาศัยไฟล์พาหะสิ่งที่มันทำคือ สร้างความเสียหายให้กับไฟล์

Worm = คัดลอกตัวเองและสามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้อย่างอิสระ โดยอาศัยอีเมลล์, ช่องโหว่ของระบบปฏิบัติการหรือการเชื่อมต่อที่ไม่มีการป้องกัน มันจะไม่แพร่เชื่อไปติดไฟล์อื่น สิ่งที่มันทำคือ มักจะสร้างความเสียหายให้กับระบบเครือข่าย และระบบอินเทอร์เน็ต

Trojan = ไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้ ต้องอาศัยการหลอกคนใช้ให้ดาวน์โหลดเอาไปใส่เครื่องเอง หรือด้วยวิธีอื่นๆ สิ่งที่มันทำคือ เปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล ซึ่งจะทำอะไรก็ได้ และโทรจันยังมีอีกหลายชนิด

Spyware = ไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้ ต้องอาศัยการหลอกคนใช้ให้ดาวน์โหลดเอาไปใส่เครื่องเอง หรืออาศัยช่องโหว่ของ Web browser และระบบปฏิบัติการในการติดตั้งตัวเองลงในเครื่องเหยื่อ สิ่งที่มันทำคือ รบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้

Hybrid Malware/Blended Threats = คือ Malware ที่รวมความสามารถของ virus, worm, trojan, spyware เข้าไว้ด้วยกัน

Phishing = เป็นเทคนิคการทำ Social Engineer โดยใช้อีเมลล์เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลการทำธุรกรรมทางการเงินบนอินเตอร์เน็ต เช่น บัตรเครดิต หรือพวก online bank account

Zombie Network = เครื่องคอมพิวเตอร์จำนวนมากๆ จากทั่วโลกที่ตกเป็นเหยื่อของ worm, trojan และ malware อย่างอื่น (compromised machine) ซึ่งจะถูก attacker/hacker ใช้เป็นฐานปฏิบัติการในการส่ง spam mail, phishing, DoS หรือเอาไว้เก็บไฟล์หรือซอฟแวร์ที่ผิดกฎหมาย

Key logger = โปรแกรมชนิดหนึ่งที่แฝงตัวเข้ากับระบบคอมพิวเตอร์ เพื่อเก็บข้อมูลการกดแป้นคีย์บอร์ด และดักเอารหัสผ่านต่างๆ เพื่อนำไปให้ผู้ไม่ประสงค์ดีนำเอาไปใช้งาน

| | |
|---|---|
| | Dialer = แอพพลิเคชั่นที่ทำงานโดยการสั่งให้โมเด็มคุณตัดการเชื่อมต่อจาก ISP ที่ใช้บริการ โดยหมุนหมายเลยไปยังผู้ให้บริการในต่างประเทศ ทำให้มีค่าโทรศัพท์ที่สูงขึ้น |
| ดีดีโอเอส ( DDOS) | หมายถึง การโจมตีด้วยการรวมคำสั่งคอมพิวเตอร์ผ่านทางเครือข่ายคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์แม่ข่ายเป้าหมายหยุดการให้บริการ คำว่า DDOS เป็นคำย่อ มาจากคำเต็มว่า Distribute Denial of Service |

# บทที่ 2
# แนวคิด ทฤษฎี ที่เกี่ยวข้อง

## หลักการทั่วไป

ในบทนี้จะได้ศึกษาในเรื่องความหมายของสงครามไซเบอร์ แนวคิดของสงครามไซเบอร์ที่เป็นส่วนหนึ่งของสงครามสารสนเทศ ดังนั้นเราควรทำความเข้าใจในสงครามสารสนเทศในเบื้องต้นก่อนได้นี้

## สงครามสารสนเทศ

เทคโนโลยีสารสนเทศมีบทบาทเป็นอย่างมากในปัจจุบัน ดังจะเห็นได้จากหน่วยงานต่าง ๆ เช่น รัฐบาล ภาครัฐ ภาคเอกชน หรือแม้กระทั้ง ประชาชนทั่วไป ต่างมีแนวความคิดที่จะนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้งานในกิจกรรมต่าง ๆ เพื่อให้กิจกรรมนั้น ๆ เกิดประสิทธิภาพสูงสุด จนมีคำกล่าวว่า ปัจจุบันเป็นยุคของ “สังคมสารสนเทศ”[1]

เมื่อสารสนเทศ ได้ถูกนำมาใช้กับกิจกรรมต่าง ๆ อย่างแพร่หลาย ย่อมเป็นสิ่งที่หลีกเลี่ยงไม่ได้ที่กิจกรรมทางทหารจะนำสารสนเทศมาใช้งาน ทั้งทางด้านการบริหารจัดการและในสนามรบ ทำให้สารสนเทศเปรียบเสมือนทรัพยากรที่มีความสำคัญยิ่ง ที่แต่ละฝ่ายของคู่สงครามต่างที่จะครองความเหนือกว่าทางด้านสารสนเทศ หรือที่เรียกว่า “Information Superiority”

ดังนั้นกิจกรรมใด ๆ ทั้งมวลที่นำมาซึ่งความได้เปรียบทางด้านสารสนเทศของฝ่ายเราที่มีเหนือฝ่ายตรงข้าม และการป้องกันสารสนเทศของฝ่ายเราจากฝ่ายตรงข้าม เราจะเรียกว่า “สงครามสารสนเทศ” หรือ “Information Warfare” เรียกย่อ ๆ ว่า “IW” โดยสารสนเทศในที่นี้จะรวมถึง ข้อมูลสารสนเทศ องค์ความรู้ เทคโนโลยีสารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

เอกสารของ ประธานคณะเสนาธิการร่วมสหรัฐฯ ค.ศ. 1996 ให้คำจำกัดความ ของสงครามข่าวสารไว้ว่า "สงครามข่าวสาร คือ การดำเนินการเพื่อให้เป็นฝ่ายได้เปรียบด้านข่าวสาร โดยการบ่อนทำลาย ข่าวสาร การดำเนินกรรมวิธีต่อข่าวสาร ระบบข่าวสาร และเครือข่ายคอมพิวเตอร์

---

[1] หน่วยบัญชาการต่อสู้อากาศยานและรักษาฝั่งกองทัพเรือ. (ออนไลน์). เข้าถึงได้จาก : http://www.acdc.navy.mi.th/pdf/Information%20Warfare.pdf, 2557.

ของข้าศึก ในขณะเดียวกัน ก็ทำการป้องกัน ข่าวสาร การดำเนินกรรมวิธีต่อข่าวสาร ระบบข่าวสาร และเครือข่ายคอมพิวเตอร์ ของตน จากการบ่อนทำลายของข้าศึก"

ปัจจุบันการแบ่งประเภทของสงครามสารสนเทศนั้นมีการแบ่งประเภทที่แตกต่างกันออกไปมากมาย ทั้งนี้ตามแนวคิดของ Martin Libiciki ที่นำเสนอในบทความชื่อ “What is Information Warfare?” เมื่อปี พ.ศ. 2538 ได้แบ่งสงครามสารสนเทศออกเป็น 7 ประเภท คือ

1. สงครามการควบคุมบังคับบัญชา (Command-and-Control Warfare: C2W) เป็นการปฏิบัติในระดับยุทธศาสตร์ทหารสำหรับการทำสงครามสารสนเทศที่มุ่งสู่การทำลายล้างในสนามรบ โดยการทำลายนั้นจะมุ่งไปสู่การทำลายกระบวนการควบคุมบังคับบัญชาของฝ่ายข้าศึกและรวมไปถึงการป้องกันไม่ให้ฝ่ายข้าศึกทำลายกระบวนการควบคุมบังคับบัญชา แนวความคิดหลัก ๆ ของการทำสงครามควบคุมบังคับบัญชาจะมีอยู่สองแนวความคิดคือ

- ตีหัว (Antihead): แนวความคิดนี้เป็นแนวความคิดที่มุ่งกระทำต่อศูนย์การบังคับบัญชาของข้าศึก

- ปาดคอ (Antineck): นอกจากแนวความคิดในการตีหัวแล้ว การปาดคอ (Antineck) เป็นอีกแนวทางหนึ่งในการทำสงครามการควบคุมบังคับบัญชา เพราะการสั่งการต่าง ๆ ของแม่ทัพนายกองนั้นมีความจำเป็นต้องอาศัยระบบการสื่อสารต่าง ๆ ดังนั้นการทำลายโครงสร้างพื้นฐานทางการสื่อสารของฝ่ายตรงข้ามจึงถือว่าเป็นการทำให้ฝ่ายตรงข้ามไม่สามารถสั่งการใด ๆ ได้จนเป็นอัมพาตในที่สุด

2. สงครามบนบรรทัดฐานของการข่าวกรอง (Intelligence-Based Warfare: IBW) การใช้ข่าวกรองเพื่อการปฏิบัติการทางทหารในปัจจุบันได้เปลี่ยนแปลงไปอย่างมากจากเดิมที่ผู้บังคับบัญชาเป็นผู้ใช้ข่าวกรองเพื่อประกอบในการวางแผนหรือตัดสินใจแต่ในปัจจุบันข่าวกรองบางลักษณะถูกส่งตรงจากอุปกรณ์เซ็นเซอร์ (sensor) ไปยังอาวุธอัตโนมัติ จากนั้นอาวุธอัตโนมัติก็จะทำงานตอบสนองตามข่าวกรองที่เข้ามาทำให้การตอบสนองต่อภัยคุกคามประเภทต่าง ๆ ได้รวดเร็วยิ่งขึ้น นอกเหนือจากการตอบสนองต่อภัยคุกคามที่เกิดแล้ว ข่าวกรองที่ได้มาในปัจจุบันยังมีความละเอียดมากกว่าข่าวกรองที่ได้ในอดีต ทำให้รูปแบบของวงรอบข่าวกรอง (ประกอบไปด้วย การวางแผนรวบรวมข่าวสาร (Planning) การรวบรวมข่าวสาร (Collecting) การวิเคราะห์ข่าวสาร (Analysis) และ การนำไปใช้ (Disseminate)) มีการเปลี่ยนแปลงไปตามความรูปแบบของการดำเนินสงครามในยุคสารสนเทศนั้น สำหรับการสงครามบนบรรทัดฐานของการข่าวกรองนั้นสามารถแบ่งออกได้เป็น 2 ลักษณะคือ

- การสงครามบนบรรทัดฐานของการข่าวกรองเชิงรุก (Offensive IBW): เนื่องจากความเจริญของเทคโนโลยีทำให้การพัฒนาอุปกรณ์สาหรับการตรวจจับอย่าง เซนเซอร์ (sensor) เรดาร์ (RAdio Detection And Ranging:Ladar radar) อินฟาเรด (infrared) ไลดาร์ (LIght Detection And

Ranging: lider) และเลดาร์ (LAser Detection And Ranging: Ladar)ให้มีประสิทธิภาพสูง สามารถนำไปติดตั้งใช้งานได้ในพื้นที่การรบที่แตกต่างและหลากหลายได้

- การสงครามบนบรรทัดฐานของการข่าวกรองเชิงรับ (Defensive IBW): การดำเนินการ IBW เชิงรับนั้นจะมุ่งเน้นไปยังการคุ้มครองป้องกันระบบตรวจจับต่าง ๆ ของฝ่ายเราให้รอดพ้นจากการโจมตีจากฝ่ายข้าศึก

3. สงครามอิเล็กทรอนิกส์ (Electronic Warfare: EW) การทำสงครามอิเล็กทรอนิกส์เป็นกระทำที่มุ่งเน้นต่อการลดขีดความสามารถในการส่งผ่านข้อมูลต่าง ไม่ว่าจะเป็น เสียง ภาพ และข้อมูล

4. สงครามจิตวิทยา (Psychological Warfare: PSYW): เป็นเรื่องของการโฆษณาชวนเชื่อและปฏิบัติการอื่น ๆ ที่มีจุดมุ่งหมายให้เกิดอิทธิพลต่ออารมณ์ ทัศนคติ ทีท่า ความเชื่อ พฤติกรรมของ ฝ่ายตรงข้าม ฝ่ายเรา และฝ่ายเป็นกลาง เพื่อบรรลุวัตถุประสงค์ของชาติ รูปแบบของการทำสงครามจิตวิทยามีอยู่ 4 ลักษณะคือ

4.1 ต่อต้านเจตจำนงแห่งชาติ (Against National Will or Counter-Will): การทำสงครามจิตวิทยาเพื่อต่อต้านเจตจำนงแห่งชาติเป็นเรื่องของกิจกรรมทางสงครามจิตวิทยาที่มุ่งกระทำแล้วส่งผลกระทบต่อเจตจำนงของชาติที่เป็นเป้าหมายให้เปลี่ยนไปจากเดิม

4.2 ต่อต้านผู้บังคับบัญชาฝ่ายตรงข้าม (Against Opposing Commanders or Counter-Commander): การทำสงครามจิตวิทยาประเภทนี้เป็นการดำเนินกิจกรรมทางจิตวิทยาที่มุ่งกระทำต่อผู้นำประเทศหรือผู้นำทางทหารของประเทศเป้าหมาย

4.3 ต่อต้านกองกำลังฝ่ายตรงข้าม (Against Troops or Counterforce): การทำสงครามจิตวิทยาประเภทนี้จะมุ่งกระทำต่อขวัญและกำลังใจฝ่ายตรงข้ามและเพิ่มพูนขวัญและกำลังใจให้กับกำลังฝ่ายเรา การทิ้งใบปลิว (leaflet) เพื่อให้ทหารฝ่ายตรงข้ามมีความสับสนและเสียขวัญ

4.4 ความขัดแย้งทางวัฒนธรรม (Kulturkampf or Cultural-Conflict): (คำว่า Kulturkampf เป็นชื่อเรียกความขัดแย้งระหว่างรัฐเยอรมันกับศาสนาโรมันคาทอลิก เกี่ยวกับการควบคุมระบบการศึกษาและตำแหน่งศาสนา เกิดขึ้นระหว่างปี พ.ศ. 2416 - 2429) ความขัดแย้งทางวัฒนธรรมเป็นหนึ่งในกิจกรรมที่ถือว่าเป็นการดำเนินสงครามจิตวิทยาความขัดแย้งทางวัฒธรรมเป็นการทำกิจกรรมที่มุ่งสร้างความขัดแย้งให้เกิดขึ้นในสังคมใดสังคมหนึ่ง ๆ ด้วยการใช้วัฒนธรรมที่แตกต่างเข้าไปสร้างกระแสความขัดแย้งให้เกิดขึ้นโดยผลที่ตามมาหลังจากนั้นอาจจะเป็นในรูปของการครอบงำทางวัฒนธรรม ค่านิยม และแนวคิด หรืออาจจะสร้างให้เกิดความสับสนวุ่นวายในสังคมนั้น ๆ แล้วใช้กาลังทหารเข้าแทรกแซง

5. สงครามแฮกเกอร์ (Hacker Warfare): การการโจมตีต่อระบบคอมพิวเตอร์ของฝ่ายพลเรือน มีลักษณะของการดำเนินการอยู่ 3 ลักษณะคือ (1) การโจมตีทางกายภาพ (physical) (2) การโจมตีทางไวยกรณ์ (syntactic) และ (3) การโจมตีทางความหมาย (semantic)

6. สงครามสารสนเทศทางเศรษฐศาสตร์ (Economic Information Warfare: EIW): เศรษฐศาสตร์ถือเป็นพลังอานาจของชาติที่ใช้ขับเคลื่อนรัฐ ดังนั้นการกระทำใด ๆ ที่ส่งผลกระทบต่อเศรษฐกิจของกลุ่มเป้าหมาย เช่น ประเทศ หรือกลุ่มที่อยู่ตรงข้าม ย่อมสงผลกระทบโดยรวมต่อเป้าหมายนั้น ๆ สำหรับปัจจุบันการดำเนินสงครามสารสนเทศทางเศรษฐศาสตร์ มีอยู่ 2 ลักษณะคือ

6.1 การปิดกั้นทางสารสนเทศ (Information Blockade): การดำเนินสงครามสารสนเทศลักษณะนี้คือการกระทำทุกวิถีทางที่จะไม่ให้สารสนเทศต่าง ๆ ไหลออกและเข้าไปยังประเทศหรือกลุ่ม ที่เป็นเป้าหมาย

6.2 การแผ่อิทธิพลทางสารสนเทศ (Information Imperialism): การดำเนินการสงครามสารสนเทศทางเศรษฐศาสตร์เป็นสิ่งที่มีบทบาทเป็นอย่างมากในปัจจุบันโดยเฉพาะอย่างยิ่งการเกิดขึ้นของอินเตอร์เน็ตที่ช่วยให้การเข้าถึงข้อมูลเป็นไปได้อย่างแพร่หลายการแผ่อิทธิผลทางสารสนเทศในปัจจุบันเป็นการกระทำร่วมกับการดำเนินสงครามจิตวิทยาด้วยการสร้าง ความขัดแย้งทางวัฒนธรรม (Kulturkampf or Cultural-Conflict) ด้วยการให้กลุ่มเป้าหมายถูกครอบงำโดยสารสนเทศ

7. สงครามไซเบอร์ (Cyber Warfare): คำว่าไซเบอร์หมายถึงอะไรก็ตามที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ดังนั้นการดำเนินการสงครามไซเบอร์จึงเป็นเรื่องที่มีแนวทางในการดำเนินที่แตกต่างและหลากหลาย

## สงครามไซเบอร์ (Cyber Warfare)

“สงครามไซเบอร์” (Cyber Warfare) คือ การใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำสงคราม สงครามไซเบอร์มีการโจมตีกันหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด อาทิ

- การโจมตีเว็บ หรือบล็อคเว็บ
- การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ต
- การเจาะข้อมูลลับ โดยแฮกเกอร์ที่นอกจากได้ข้อมูลลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้
- การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้ หรือทำงานไม่แม่นยำ

- การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก

สงครามไซเบอร์เป็นการปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้าม และต้องทำให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา

โดยสรุปการใช้คอมพิวเตอร์และอินเตอร์เน็ตเพื่อการทำสงคราม ปัจจุบันมีอยู่ 8 รูปแบบ คือ

1. การโจรกรรมทางไซเบอร์
2. การทำลายเว็บไซต์
3. การโฆษณาชวนเชื่อทางอินเตอร์เน็ต (เว็ปไซต์)
4. การรวบรวมและการล้วงความลับข้อมูล
5. การกระจายเพื่อให้ปฏิเสธบริการ
6. การรบกวนเครื่องมือและอุปกรณ์
7. การโจมตีโครงสร้างระบบสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) พื้นฐานที่สาคัญ และ
8. การใช้อุปกรณ์คอมพิวเตอร์หลอกแต่ซ่อนซอฟต์แวร์ไวรัสเอาไว้

## บทเรียนในเรื่องของสงครามไซเบอร์

สงครามไซเบอร์ได้อุบัติขึ้นแล้วในหลายประเทศซึ่งมีทั้งประเภทชัดเจน เปิดเผย และซุ่มเงียบ ซึ่งคาว่า “สงครามเย็น” หรือ Cold War ก็เริ่มกลับนามาใช้กันใหม่อีกครั้ง หลังจากการแพ้สงครามเวียตนามของสหรัฐอเมริกาและการล่มสลายของสหภาพโซเวียตรัสเซีย

ในช่วงสงครามอ่าวที่สหรัฐโจมตีอิรัก และสงครามอิรักครั้งที่สอง สิ่งที่สหรัฐต้องทำก่อนอื่นคือ ทำลายเครือข่ายคอมพิวเตอร์และอีเล็คโทรนิคของอิรักที่ใช้ควบคุมระบบการยิงของอาวุธ ไม่เพียงแต่กรณีสงครามอิรักเท่านั้น ในการสู้รบปัจจุบัน แต่ละฝ่ายต้องหาทางทำลายระบบคอมพิวเตอร์และอิเล็กทรอนิกส์ที่ควบคุมการยิงของอาวุธก่อน

## สงครามไซเบอร์ครั้งแรกของโลก[2]

ในวันที่ 17 เดือนพฤษภาคม ปี 2550 ประเทศเอสโตเนีย ถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะรัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่าง ๆ จนข้อมูลเสียหายพังยับเยิน ถือเป็นสงครามไซเบอร์ครั้งแรกของโลกก็ว่าได้ มีรายละเอียดที่จะใช้เป็นการกรณีศึกษาดังนี้

หลังเอสโตเนีย หนึ่งในอดีตสาธารณรัฐของสหภาพโซเวียต ซึ่งปัจจุบันเป็นทั้งสมาชิกกลุ่มสหภาพยุโรป และนาโต้ ไม่ไว้หน้ารัสเซียด้วยการย้ายรูปปั้นทหารโซเวียตที่รัสเซียสร้างเพื่ออุทิศให้กับทหารหลายล้านชีวิตที่สู้รบกับนาซีเยอรมันในสงครามโลกครั้งที่ 2 จากเขตใจกลางเมืองหลวง ไปไว้ในอีกที่หนึ่งเมื่อปลายเดือนที่แล้ว พวกเขาก็ถูกฝ่ายรัสเซีย (ไม่ยืนยันว่าเป็นทางการ หรือแค่ภาคเอกชนทั่วไป)โจมตีทันที ข่าวบอกว่า ในช่วงต้นๆเท่านั้นที่พบว่ามีการโจมตีออกมาบ้าง จากเครื่องคอมพิวเตอร์ของสถาบันของรัฐในรัสเซีย แต่โดยหลักแล้วการโจมตีนั้นมาจากทั่วทุกมุมโลก ขณะที่นาโต้ ก็ไม่พยายามระบุเฉพาะเจอะจงไปที่ใครกระทำ แต่บอกว่าเรื่องแบบนี้คนธรรมดาทั่วไปทำงานแบบนี้ไม่ได้ และจนถึงสัปดาห์ที่แล้ว มีการโจมตีเข้ามาแล้ว 3 ระลอก

ฝ่ายรัสเซียก็ออกมาปฏิเสธในเรื่องดังกล่าว โดยกล่าวว่าเว็บไซต์ของประธานาธิบดีรัสเซียก็ถูกโจมตีวันละเป็นร้อยครั้ง จากหลักฐานบอกว่าเป็นการโจมตีจากเครื่องคอมพิวเตอร์ของรัฐบาลทั่วโลก แต่รัสเซียก็ไม่เคยออกมาชี้แจงอย่างเป็นทางการ เพราะรู้ดีว่าเรื่องหลักฐานแบบนี้สามารถทำปลอมแปลงได้

การกระหน่ำโจมตีถือเป็นสงครามไซเบอร์ครั้งแรกของโลกเพราะก่อนหน้านี้ แฮ็กเกอร์ไม่เคยพร้อมใจกันโจมตีในวงกว้างขนาดนี้มาก่อน ส่งผลให้ฝ่ายพันธมิตรชาติตะวันตกของเอสโตเนียต้องหาทางแก้ไข นาโต้จึงรีบส่งผู้เชี่ยวชาญมาตรวจสอบวิเคราะห์สถานการณ์และความยุ่งยากวุ่นวายที่อาจจะเกิดขึ้นตามมาแต่ก็ยังจนปัญญาไม่ทราบว่าจะออกมาช่วยเหลือในทางไหน เพราะเมื่อการโจมตีจากรัสเซียไม่ได้มีความหมายของการโจมตีทางทหาร กลุ่มนาโต้ ซึ่งเป็นกลุ่มทางทหาร ก็ไม่มีอำนาจที่จะช่วย แต่ก็มีการชี้แจงเพียงว่า ในอนาคตอันใกล้อาจจะต้องมีการปรับเปลี่ยนหลักการ ในการเข้ามาแทรงแซง เพื่อการแก้ไขปัญหาดังกล่าว

ในการประชุมสุดยอดที่รัสเซียระหว่างปูตินกับนายกรัฐมนตรีหญิงของเยอรมันในฐานะประธานกลุ่มอียู (European Union; EU) เชื่อว่ามีการหารือกันเรื่องทางออกสำหรับเรื่องนี้ แต่ก็

---

[2] คลาร์ก ริชาร์ด เอ. สงครามไซเบอร์-Cyber War . แปลโดยนาย ไพรัตน์ พงศ์พานิชย์. ( กรุงเทพฯ : มติชน, 2555 ). หน้า 37.

ไม่มีการเปิดเผยความคืบหน้า เพราะในการแถลงข่าว เห็นนายกฯเยอรมันกล่าวตอบโต้รัสเซียแบบไม่ไว้หน้า ก็พอจะเห็นแล้วว่า ไม่สามารถตกลงอะไรกันได้ ในความร่วมมือการแก้ไขปัญหาดังกล่าว

เอสโตเนียเป็นประเทศเล็กๆ มีประชากรประมาณ 1.4 ล้านคน เมื่อก่อนเคยตกเป็นของรัสเซียหลายครั้งหลายสมัย รวมแล้วเป็นเวลาหลายร้อยปี ทำให้พวกเขาสะสมความเกลียดชังต่อคนรัสเซียอย่างมาก และตะวันตกก็อาศัยประโยชน์จากความเกลียดชังนี้รุกเข้ามาประชิดพรมแดนรัสเซียอยู่ในปัจจุบัน เพื่อหาทางบั่นทอนอิทธิพลของรัสเซีย

เอสโตเนียเป็นสังคมที่มีการออนไลน์กันมากที่สุดแห่งหนึ่งในยุโรป และเป็นผู้บุกเบิกรัฐบาลอิเล็กทรอนิกส์ หรือ อีโกเวอร์เม้นต์ ( E-government) แต่สิ่งที่เป็นจุดแข็งของประเทศ สร้างความเสียหายให้กับประเทศทันทีเมื่อเกิดสงครามไซเบอร์

สำหรับการโจมตีครั้งนี้ ผู้เชี่ยวชาญบอกว่า พวกกลุ่มแฮ็คเกอร์ ใช้วิธีที่เรียกว่า ดีดอส (DDOS – Distribute Denial of Service) นั่นก็คือมีการส่งคำสั่งพร้อมกันเป็นพันเป็นหมื่น เพื่อขอเข้าเว็บเป้าหมาย ทำให้คนอื่นเข้ามาในเว็บนั้นไม่ได้

ส่วนเป้าหมายที่ถูกโจมตีนั้นก็มีทั้งเว็บไซต์ประธานาธิบดีและรัฐสภา กระทรวงเกือบทุกกระทรวง พรรคการเมือง องค์กรสื่อยักษ์ใหญ่ 3 แห่งจาก 6 แห่ง ธนาคารใหญ่ที่สุด 2 แห่ง บริษัทด้านการสื่อสาร ปัจจุบันไม่มีการเปิดเผยว่าความเสียหายเหล่านี้มีมูลค่ามากน้อยแค่ไหน

ในการแก้ปัญหาเฉพาะหน้า เมื่อถูกโจมตี เอสโตเนียได้ปิดเว็บไซต์ที่ถูกโจมตี เพื่อไม่ให้ออนไลน์จากต่างประเทศสามารถเข้ามาได้ เพื่อว่าคนในประเทศยังสามารถใช้งานเว็บไซต์ต่างๆได้ต่อไป ขณะเดียวกันก็มีการตอบโต้กลับไปบ้างเช่นกัน

ภายหลังจากที่ระบบคอมพิวเตอร์ของเอสโตเนียถูกโจมตีโดยรัสเซียไปเมื่อปี 2550 ซึ่งยังผลให้บริษัท, ธนาคาร หน่วยราชการของเอสโตเนียหยุดชะงัก ทำงานไม่ได้ จนองค์กร Nato ต้องส่งผู้เชี่ยวชาญไปให้ความช่วยเหลือในฐานะที่เอสโตเนียเป็นประเทศสมาชิก แล้ว Nato เอง ก็เริ่มหันมาให้ความสำคัญกับ Cyberwar มากขึ้น มีโครงการ ตั้งศูนย์ป้องกันการโจมตีคอมพิวเตอร์ขึ้นเป็นการเฉพาะ โดยทำงานภายใต้ศูนย์คอมพิวเตอร์หลักขององค์กรเอง คือ "Nato Computer Incident Response Capability´s Technical Center" (NITC) เดิมที ในหน่วยงานนี้ มีทหาร 91 นาย และผู้เชี่ยวชาญด้านคอมพิวเตอร์ที่เป็นพลเรือนร่วมทำงานอีก 27 คน แต่เมื่อเพิ่มงานด้านการป้องกันการโจมตีระบบขึ้นมา จึงมีการขยายหน่วยงานขึ้นอีกกว่า 70 เปอร์เซ็นต์ ซึ่งนั่นหมายรวมถึงการค้นหาบุคคลากร และแฮกเกอร์มืออาชีพเข้ามาเพิ่มด้วย นอกจากหน่วยงานป้องกันการโจมตีคอมพิวเตอร์ของ Nato นี้แล้ว ในส่วนของ NCSA (The NATO Communication and Information Systems Services Agency) ซึ่งเป็นหน่วยที่รับผิดชอบดูแลระบบข้อมูล และการติดต่อสื่อสารระหว่างประเทศสมาชิก ก็ต้องเพิ่มมาตรการป้องกันการโจมตีระบบ รวมทั้งคอยแก้ไขปัญหาและให้ความช่วยเหลือด้านระบบรักษาความปลอดภัยคอมพิวเตอร์แก่ประเทศสมาชิกด้วย

## สงครามไซเบอร์ต่างๆ

เมื่อต้นเดือนกันยายน ปี 2550 ตึกเพนทากอน กระทรวงกลาโหม สหรัฐอเมริกา และที่ทำการรัฐบาลของฝรั่งเศส เยอรมัน และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหายอย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา

วันที่ 14 ธันวาคม ปี 2550 เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศเกียร์กีซ (Kyrgyz) ถูกโจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโทเนีย

กรณีที่เว็บไซต์สวีเดนกว่า 5000 เว็บถูกแฮกฯ ทำลายข้อมูล เมื่อเดือนตุลาคม 2550 ซึ่งหนังสือพิมพ์ตุรกี "Zaman" รายงานเองว่า เป็นฝีมือของแฮกเกอร์ชาวมุสลิมตุรกี ด้วยสาเหตุ ไม่พอใจสื่อสวีเดนที่เผยแพร่การ์ตูนล้อเลียนศาสดามูฮัมหมัด นั่นก็ถือเป็น Cyberwar เหมือนกัน

หลังจากตกเป็นฝ่ายรับแบบไม่ทันตั้งตัว แฮกเกอร์สวีเดน ก็โต้กลับด้วยการเจาะระบบเว็บบอร์ด "Ayyildiz" ของตุรกี ขโมยข้อมูล และ Password สมาชิกชาวตุรกีกว่าพันคน มาเปิดเผยบนอินเทอร์เน็ต โดยทิ้งข้อความเย้ยหยันอย่างเปิดเผยว่า เป็นการโต้ตอบจากสวีเดน โทษฐานที่ตุรกีแหยมมาแฮก ฯ เว็บสวีเดนก่อน เท่านั้นยังมิสาแก่ใจ แฮกเกอร์สวีเดนยังจัดการส่งภาพโป๊มูฮัมหมัดไปตามอีเมล หรือเอ็มเอสเอ็นที่แฮก ฯ มา ให้สมาชิกเว็บนั้นดูต่างหน้าอีกด้วย

กลางปี 2551 กลุ่มแฮกเกอร์ Ayyildiz-Team ซึ่งเรียกตัวเองว่า "ทหารแห่งโลกไซเบอร์" ก็พยายามแฮกเว็บไซต์ของ EU เพื่อเผยแพร่คำต่อต้านสหภาพยุโรป ที่กล่าวหาว่า มีกลุ่มผู้ก่อการร้ายอยู่ในประเทศตุรกี และด้วยเหตุผลเดียวกันนี้เว็บไซต์สมาคมฟุตบอล และนิตยสารของออสเตรียก็เคยโดนโจมตีจนได้รับความเสียหาย จากทีมนี้เช่นกัน นอกจากกรณีดัง ๆ เหล่านี้แล้ว ยังมีการโจมตีกันไปมาด้วยเหตุผล และข้อพิพาทอื่น ๆ อีกมากที่ไม่ได้รับการเปิดเผย ทั้งนี้เพราะฝ่ายที่ตกเป็นเหยื่อกลัวว่าฝ่ายตัวจะเสียภาพพจน์

ในปลายปี 2551 ก่อนที่จะเกิดสงครามในโลกจริงระหว่างรัสเซียกับจอร์เจียสาเหตุหรือเหตุจากความขัดแย้งเกิดขึ้นในเขต เซาท์ ออสเซเทีย (South Ossetia) ประเทศจอร์เจีย ดังนั้น แฮกเกอร์รัสเซีย ได้แอบลักลอบไปเปิดสมรภูมิไซเบอร์ เตรียมการไว้ก่อนแล้ว โดยมีรายงานว่า ก่อนที่สงครามจะเริ่มไม่กี่วัน (ก่อน 8 สิงหาคม ) เว็บไซท์รัฐบาล รวมทั้งเว็บกระทรวงหลายแห่งของจอร์เจีย อาทิ เว็บไซต์ประธานาธิบดี Mikheil Saakashvili, เว็บทำเนียบรัฐบาล, หน้า Homepages กระทรวงต่างประเทศ และ กระทรวงกลาโหม ไม่สามารถเข้าถึงได้ บางแห่งเข้าได้แต่ถูกเปลี่ยนเนื้อหา ในขณะที่เซิร์ฟเวอร์ภายในประเทศจอร์เจีย ถูกโจมตีโดยวิธี "ระดมยิงคำสั่งลวง" (Distributed Denial of Service attacks หรือ DDos) จนระบบปฏิบัติการล้มเหลว หรือมิเช่นนั้นก็ถูกควบคุม

เส้นทางจาก Autonomous System ที่อยู่ภายนอกประเทศ Jart Armin เจ้าของบล็อก rnbexploit-Blogs ที่เปิดเผยเรื่องนี้เป็นแห่งแรก วิเคราะห์และแสดงหลักฐานว่า การโจมตีครั้งนี้ แฮกเกอร์รัสเซีย ภายใต้ชื่อเครือข่าย Russia Business Network (RBN) ซึ่งมีความสัมพันธ์กับรัฐบาลรัสเซีย เป็นผู้อยู่เบื้องหลัง ซึ่งต่อมาการวิเคราะห์ของเขาก็ได้รับการยืนยันจากผู้เชี่ยวชาญคนอื่น ๆ

สำหรับการโจมตีครั้งนี้ ผู้เชี่ยวชาญบอกว่า พวกกลุ่มแฮ็คเกอร์ Russia Business Network (RBN) ใช้วิธีที่เรียกว่า ดีดอส (DDOS – Distribute Denial of Service) นั่นก็คือมีการส่งคำสั่งพร้อมกันเป็นพันเป็นหมื่น เพื่อขอเข้าเว็บเป้าหมาย ทำให้คนอื่นเข้ามาในเว็บนั้นไม่ได้ นอกจากนี้ยังมีรายงานว่าเซิร์ฟเวอร์หลายตัวภายในประเทศจอร์เจีย ถูกควบคุมเส้นทางจาก Autonomous System (AS) อีกด้วย

เมื่อ มี.ค.56 มีข่าวแจ้งว่า เกาหลีใต้อาจถูกโจมตีทางไซเบอร์ครั้งใหญ่ มีการเปิดเผยว่าเครือข่ายคอมพิวเตอร์สถานีโทรทัศน์ชั้นนำรวมถึงธนาคารเสียหาย แต่หลักฐานยังไม่ระบุเป็นฝีมือเกาหลีเหนือ ขณะรัฐบาลโสมแดงประณามและขู่ถล่ม หากสหรัฐไม่นำเครื่องบินบี-52 ออกไปให้พ้นคาบสมุทรเกาหลี และหน่วยงานความมั่นคงทางอินเตอร์เน็ตแถลงว่า เครือข่ายคอมพิวเตอร์ที่สถานีโทรทัศน์ 3 แห่ง คือ เคบีเอส, เอ็มบีซี และวายทีเอ็น รวมถึงธนาคารชินฮันและนงฮยอป ส่วนหนึ่งหรือทั้งหมดเสียหายจนใช้การไม่ได้ ซึ่งมีความเป็นไปได้ที่จะเกิดจากการโจมตีทางไซเบอร์ครั้งใหญ่

โฆษกประจำหน่วยงานกล่าวว่า "ขณะนี้เรากำลังดำเนินการสอบสวนอยู่ และยังไม่สามารถบอกได้ว่าพวกเขาถูกแฮ็กเกอร์โจมตีหรือไม่" พร้อมเสริมว่า ผู้ให้บริการอินเทอร์เน็ต แอลจียูพลัส ก็รายงานว่าเครือข่ายคอมพิวเตอร์เสียหายเช่นกัน

ขณะนี้ยังไม่มีการยืนยันว่า ใครหรืออะไรที่เป็นสาเหตุของความเสียหายดังกล่าว แต่ผู้ต้องสงสัยอันดับหนึ่งดูเหมือนว่าจะเป็นเกาหลีเหนือ เพราะการโจมตีครั้งนี้เกิดขึ้นหลังรัฐบาลเปียงยางออกมากล่าวหาว่า สหรัฐและเกาหลีใต้แฮ็กเว็บไซต์ของรัฐบาลหลายเว็บไซต์จนใช้การไม่ได้ถึง 2 วัน

กรณี ประเทศเพื่อนบ้าน พม่าหรือเมียนมาร์ ผู้เชี่ยวชาญด้านความปลอดภัยเผย ในช่วงก่อนการเลือกตั้ง อินเทอร์เน็ตของพม่าถูกโจมตีครั้งร้ายแรงจากต่างประเทศจนใช้การไม่ได้ คล้ายคลึงกันในจอร์เจียและเอสโตเนีย[3]

---

[3] ทิวสน สีอุ่นและชญานิน วิภูษณวรรณ. “สงครามไซเบอร์ ถล่มอินเทอร์เน็ตพม่ารับวันเลือกตั้ง”. (ออนไลน์). เข้าถึงได้จาก:http://prachatai.com/journal/2010/11/31796, 2553.

เมื่อ 7 พ.ย.53 ผู้เชี่ยวชาญด้านความปลอดภัยจากบริษัท Arbor Networks เปิดเผยว่า ในช่วงก่อนการเลือกตั้งวันนี้ อินเทอร์เน็ตพม่าถูกโจมตีจากต่างประเทศจนใช้การไม่ได้ โดยการโจมตีครั้งนี้มีความร้ายแรงกว่าเหตุการณ์ที่คล้ายคลึงกันในจอร์เจียและเอสโตเนีย

ตั้งแต่ช่วงปลายเดือนตุลาคม 53 อินเทอร์เน็ตในพม่าถูกรบกวนทำให้ 'ช้า' จนแทบใช้การไม่ได้ และส่งผลกระทบในวงกว้าง เช่น อินเทอร์เน็ตคาเฟ่ต้องหยุดให้บริการ ประชาชนไม่สามารถดาวน์โหลดเอกสารเพื่อขออนุญาตเดินทางออกนอกประเทศ และบริษัทท่องเที่ยวต้องจองตั๋วเครื่องบินผ่านโทรศัพท์แทน

มีการตั้งข้อสงสัยว่า การรบกวนอินเทอร์เน็ตนี้เป็นความพยายามของรัฐบาลทหารในการจำกัดการเผยแพร่ข่าวสารเกี่ยวกับการเลือกตั้ง ทั้งนี้ มีรายงานว่า ผู้สังเกตการณ์และนักข่าวจากต่างประเทศไม่ได้รับอนุญาตให้เดินทางเข้าพม่าเพื่อรายงานข่าวนี้

การโจมตีดังกล่าว ดร. เครก ลาโบวิตซ์ ผู้เชี่ยวชาญจากบริษัท Arbor Networks ซึ่งจำหน่ายผลิตภัณฑ์ด้านความมั่นคงของระบบเครือข่ายวิเคราะห์ว่า อินเทอร์เน็ตในพม่าถูกโจมตีด้วยวิธีการที่เรียกว่า Distributed Denial of Service (DDoS) หรือการใช้คอมพิวเตอร์จำนวนมากติดต่อเครื่องปลายทางพร้อมๆ กันเกินกว่าที่ระบบจะสามารถรองรับได้

ดร. ลาโบวิตซ์ อธิบายว่า การโจมตีด้วยวิธี DDoS ในครั้งนี้พุ่งเป้าไปที่หมายเลขไอพีในพม่าจำนวนมาก ระบบเครือข่ายทั้งหมดในพม่านั้นรองรับการเชื่อมต่อกับโลกภายนอกที่อัตราการรับส่งข้อมูล 45 เมกะบิตต่อวินาที (ประมาณ 8 เท่าของความเร็วอินเทอร์เน็ตตามบ้านทั่วไปในกรุงเทพมหานคร) แต่ข้อมูลจากผลิตภัณฑ์ของบริษัทแสดงให้เห็นว่า การโจมตีครั้งนี้โดยเฉลี่ยแล้วเป็นการเรียกข้อมูลขนาด 1 กิกะบิตต่อวินาที หรือประมาณ 20 เท่าของระดับที่ระบบเครือข่ายในพม่าจะรองรับได้ และมีความรุนแรงมากที่สุดถึง 15 กิกะบิตต่อวินาที ส่งผลให้การจราจรเครือข่ายทั้งขาเข้าและขาออกประเทศเป็นอัมพาต

การโจมตีพม่าด้วยวิธี DDoS นั้นไม่ใช่เรื่องใหม่ โดยเว็บไซต์ของ Democratic Voice of Burma ที่ตั้งอยู่ในนอร์เวย์ก็เคยถูกโจมตีจนไม่สามารถให้บริการได้มาแล้วในเดือนกรกฎาคม พ.ศ. 2551

ดร. ลาโบวิตซ์ เสริมว่า การโจมตีครั้งนี้มีความซับซ้อน เนื่องจากมีการใช้หลายวิธีการเพื่อกระจายเป้าหมายอย่างทั่วถึง และมาจากหลายสถานที่ แรงจูงใจของการโจมตีนั้นยังไม่เป็นที่ทราบแน่ชัด แต่ที่พบบ่อยคือเรื่องการเมือง การเซ็นเซอร์โดยรัฐบาล การขู่กรรโชก หรือการปั่นหุ้น

เมื่อ มี.ค.56 มีข่าวแจ้งว่า เกาหลีใต้คาดถูกโจมตีทางไซเบอร์ครั้งใหญ่ เผยเครือข่ายคอมพิวเตอร์สถานีโทรทัศน์ชั้นนำรวมถึงธนาคารเสียหาย ชี้สงสัยแต่ยังไม่ฟันธงเป็นฝีมือเกาหลีเหนือ ขณะรัฐบาลโสมแดงประณามและขู่ถล่ม หากสหรัฐไม่นำเครื่องบินบี-52 ออกไปให้พ้นคาบสมุทรเกาหลี

กรณีดังกล่าว หน่วยงานความมั่นคงทางอินเทอร์เน็ตของเกาหลีใต้ กล่าวว่า เครือข่ายคอมพิวเตอร์ที่สถานีโทรทัศน์ 3 แห่ง คือ เคบีเอส, เอ็มบีซี และวายทีเอ็น รวมถึงธนาคารชินฮันและนงฮยอป ส่วนหนึ่งหรือทั้งหมดเสียหายจนใช้การไม่ได้ ซึ่งมีความเป็นไปได้ที่จะเกิดจากการโจมตีทางไซเบอร์ครั้งใหญ่

โฆษกประจำหน่วยงานกล่าวว่า "ขณะนี้เรากำลังดำเนินการสอบสวนอยู่ และยังไม่สามารถบอกได้ว่าพวกเขาถูกแฮ็กเกอร์โจมตีหรือไม่" พร้อมเสริมว่า ผู้ให้บริการอินเทอร์เน็ต แอลจียูพลัส ก็รายงานว่าเครือข่ายคอมพิวเตอร์เสียหายเช่นกัน

ขณะนี้ยังไม่มีการยืนยันว่า ใครหรืออะไรที่เป็นสาเหตุของความเสียหายดังกล่าว แต่ผู้ต้องสงสัยอันดับหนึ่งดูเหมือนว่าจะเป็นเกาหลีเหนือ เพราะการโจมตีครั้งนี้เกิดขึ้นหลังรัฐบาลเปียงยางออกมากล่าวหาว่า สหรัฐและเกาหลีใต้แฮ็กเว็บไซต์ของรัฐบาลหลายเว็บไซต์จนใช้การไม่ได้ถึง 2 วัน

สำหรับในประเทศไทย เมื่อ 8 พ.ค.56 มีรายงานระบุว่า เว็บไซต์สำนักนายกรัฐมนตรี ในส่วนหน้าของรายชื่อคณะรัฐมนตรี http://www.opm.go.th/opminter/mainframe.asp ได้ถูกแฮกเกอร์ในนาม Unlimited Hack Team!!! และได้มีการเปลี่ยนหน้าเว็บไซต์ พร้อมข้อความโจมตีนายกรัฐมนตรี

## แนวคิดของสงครามไซเบอร์ทั้งในและต่างประเทศ

แนวทางป้องกัน Cyber (Cyber Defense) ของ US จาก FM 11-45 6-02.45 (FM 11-45) Signal Support to Theater Operations ทางสหรัฐได้มีการกำหนดสิ่งแวดล้อมด้านยุทธการ และกำหนดภัยคุกคาม หรือแนวโน้มภัยคุกคาม ดังนี้

“ภัยคุกคามจากการโจมตีของผู้ก่อการร้ายต่อต้านรัฐบาลของประชาชนและผลประโยชน์ของทุกชาติทั่วโลกได้กลายเป็น ปัญหาด้านความปลอดภัยเร่งด่วนที่สุดของทุกชาติ แนวโน้มที่จะใช้ความหลากหลายของรูปแบบการโจมตีและอาจรวมถึงการโจมตีไซเบอร์โดยกลุ่มก่อการร้ายมีมากขึ้น”

“แม้มีแนวโน้มที่ผู้ก่อการร้ายแฮกเกอร์ดำเนินการการโจมตีโลกไซเบอร์เพิ่มมากขึ้น โดยที่ขาดแรงจูงใจโดยเฉพาะทางการเมือง ในช่วงไม่กี่ปีที่ผ่านมา ทั่วโลกได้ประจักษ์ว่ามีการเพิ่มขึ้นอย่างชัดเจนของจำนวนแฮกเกอร์ที่ถูกแรงจูงใจทางการเมืองเข้าการโจมตีโลกไซเบอร์ มักจะเกิดการเข้าผสมโรงของแฮกเกอร์จากทั่วโลกมุ่งไปที่ข้อพิพาทในระดับภูมิภาคใดๆก็ได้ นอกจากนี้จำนวนขอบเขต และระดับของความซับซ้อนของไซเบอร์โจมตีที่ไม่ยุ่งเกี่ยวกับความขัดแย้งทางการเมืองใดๆก็มีเพิ่มขึ้นอย่างรวดเร็วโดยการโจมตีชาติที่ค่อนข้างอ่อนแอก่อน การโจมตีล่าสุดมีเป้าหมายที่สำคัญที่

ระบบการสื่อสารและระบบโครงสร้างพื้นฐานที่สำคัญ ในอนาคตการโจมตีทางไซเบอร์จะคงมีต่อไป ถ้าพบการเปิดเผยช่องโหว่ที่ยังไม่ได้มีการป้องกันจากผู้เชี่ยวชาญด้านความปลอดภัยทางคอมพิวเตอร์ ”

## การปฏิบัติการด้าน Cyber Defense ของ สหรัฐฯ ( FM 11-45 )[4]

ไซเบอร์ดีเฟ้นท์ (Cyber Defense) เป็นคำย่อติดปากของระบบเครือข่ายคอมพิวเตอร์กลาโหม (computer network defense(CND)) ไซเบอร์ดีเฟ้นท์เป็นองค์ประกอบย่อยของระบบการประกันข้อมูล(information assurance (IA)) ซึ่งเป็นปรับเปลี่ยนมาจากองค์ประกอบย่อยของระบบเครือข่ายยุทธการ(NETOPS) ภารกิจของหน่วยสื่อสารในสนามรบคือการยืดระบบCNDให้หน่วยรบอย่างมีนัยสำคัญ รวมทั้งให้คงอยู่ในระบบเครือข่ายยุทธการ (NETOPS) ซึ่งก่อนหน้านี้ในอดีตความรับผิดชอบในการวางระบบย่อยในระบบเครือข่ายยุทธการ(NETOPS) ถูกแยกส่วนความรับผิดชอบทำให้กระจัดกระจาย การจัดหน่วยเพื่อรับผิดชอบการปฏิบัติงานเหล่านี้

ขอบเขตภารกิจของ NETOPS, IA และ CND ต่อสารสนเทศและระบบสารสนเทศคือ ทำให้มั่นใจว่าจัดให้ได้, เที่ยงตรงแม่นยำ, ระบุตัวตนได้, ตรวจสอบการเข้าถึงได้, รักษาความลับ, ไม่ปฏิเสธสารสนเทศและระบบสารสนเทศของมิตรประเทศในขณะปฏิเสธข้าศึกในการเข้าถึงสารสนเทศ/ระบบสารสนเทศเดียวกัน IA รวมเอาขีดความสามารถในการป้องกัน, การกลั่นกรอง และปฏิกิริยาตอบโต้ของไซเบอร์ดีเฟ้นท์ รวมถึงการสำรองข้อมูลกลับมาใหม่(Restore Information System) IAให้ความคุ้มครองแบบตลอดเส้นทาง (end-to-end) เพื่อให้มั่นใจว่าข้อมูลและคุณภาพของการป้องกันการเข้าถึงที่จะก่อความเสียหายจากความเลินเล่อหรือการเข้ามาดัดแปลงข้อมูล จะสามารถทำได้ กิจกรรมของไซเบอร์ดีเฟ้นท์(Cyber Defense)ต่อระบบCNDจะกระทำการ ป้องกัน, เฝ้าตรวจ, วิเคราะห์, ปกป้อง, ตอบโต้ต่อกิจกรรมที่ไม่ได้รับอนุญาต ที่จะเกิดต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์กลาโหม (CND) กิจกรรมของไซเบอร์ดีเฟ้นท์(Cyber Defense)ต่อระบบIA จะกระทำกิจกรรมปกป้องและรวมถึงการกระทำโดยเจตนาที่จะดำเนินการแก้ไขการตั้งค่าการประกันหรือเงื่อนไขในการตอบโต้ต่อการแจ้งเตือนภัยคุกคาม CND หรือภัยคุกคามสารสนเทศ

ระบบ IA จะเน้นไปที่การสร้างการป้องกันและจากนั้นการดำเนินการกู้คืนเมื่อมีการป้องกันไม่สมบูรณ์ ในขณะที่ระบบไซเบอร์ดีเฟ้นท์มุ่งเน้นไปที่การปฏิบัติ (ป้องกัน, เฝ้าตรวจ, วิเคราะห์, ปกป้อง, ตอบโต้) และรวมถึงการป้องกันระบบ IA ในการตอบโต้ภัยคุกคามระบบ IA

---

[4] U.S. Headquarters, Department of the Army. “Signal Support to Theater Operations”. ( Field Manual No. 11-45, April 12, 2004).

ไซเบอร์ดีเฟ้นท์ที่สมบูรณ์มีความต้องการดังต่อไปนี้:

1. ความสามารถในการป้องกัน หมายรวมถึง การรักษาความปลอดภัยการส่ง, การรักษาความปลอดภัยการสื่อสาร (COMSEC), การรักษาความปลอดภัยคอมพิวเตอร์ และการรักษาความปลอดภัยอุปกรณ์สารสนเทศเช่น การควบคุมการเข้าถึง, การเข้า-ถอดรหัส, การป้องกันเครือข่าย, และระบบไฟร์วอลล์ โดยที่ทุกการขนส่งข้อมูลและทุกผู้ให้บริการในสนามรบหรือพื้นที่ใดๆในของความรับผิดชอบ(AOR)

2. ความสามารถในการกลั่นกรอง หมายรวมถึงความสามารถที่จะรู้สึกผิดปกติในเครือข่ายผ่านการใช้ที่มีความผิดปกติและการบุกรุกระบบตรวจจับ ตรวจสอบเวลาของความผิดปกติจะรวมการโจมตีความเสียหายหรือการปรับเปลี่ยนที่ไม่ได้รับอนุญาต เป็นกุญแจสำคัญในการเริ่มต้นปฏิบัติการตอบโต้และปฏิบัติการฟื้นฟู (restore)

3. ความสามารถในการตอบโต้ หมายรวมทั้งปฏิบัติการฟื้นฟู ได้ดีเช่นเดียวกันกับกระบวนการการตอบสนองต่อข้อมูลสารสนเทศอื่นๆ ขีดความสามารถในการฟื้นฟูขึ้นอยู่กับกลไกต่างๆที่จัดตั้งขึ้นเพื่อการฟื้นฟูตามลำดับความสำคัญของระบบและเครือข่ายขั้นต่ำที่สุดที่จำเป็น

## การปฏิบัติการเครือข่ายของสหรัฐฯ (เน็ตออป/NETOPS) ( FM 11-45 )

การปฏิบัติการเครือข่าย (เน็ตออป/NETOPS) สร้างขึ้นจาก การจัดหน่วย ระเบียบปฏิบัติและองค์ความรู้ทางเทคนิค รวมกันเพื่อให้มั่นใจว่า ความสุดยอดและความเร็วของข้อมูลข่าวสารของผู้บังคับบัญชาจะไปถึงพลรบ เน็ตออป/NETOPS เชื่อมโยงออกไปอย่างกว้างขวางจากศูนย์ เน็ตออป/NETOPS ผ่านสายการบังคับบัญชา และสร้างแทคติก เทคนิค และขั้นตอน(Tactic Techniques Procedure /TTP)ร่วม ขึ้นมาเพื่อให้มั่นใจว่าจะสามารถทำงานตามขั้นตอนร่วมกันได้ เน็ตออป/NETOPS ต่อขยายจากระดับสูงสุดของ โครงข่ายสารสนเทศกิจการกลาโหม (GLOBAL INFOMATION GRID/GIG) ผ่านการให้บริการระดับต่ำกว่าไปจนถึงหน่วยที่ต่ำที่สุดในเครือข่ายสารสนเทศ NETOPSเป็นกล่องเครื่องมือทางแนวความคิดและframe work สำหรับการบริหารระบบสื่อสารและสารสนเทศกองทัพบก ตามแผนภาพที่ 2-1

แผนภาพที่ 2-1 แสดงภาพปฏิบัติการโครงข่ายสารสนเทศกิจการกลาโหม (GLOBAL INFOMATION GRID/GIG NETOPS)

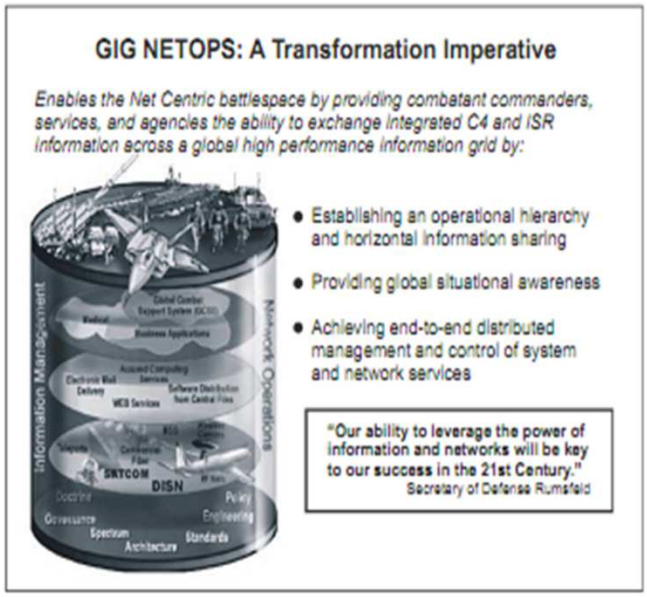



Figure 3-1. GIG NETOPS

เป้าประสงค์ของเน็ตออปหรือการปฏิบัติการเครือข่ายของกองทัพบก (Army NETOPS) คือ

1. จัดให้มีการเข้าถึงอย่างปลอดภัยไปยังบริการโครงข่ายสารสนเทศสำหรับผู้ใช้ทุกคนในกองทัพบกให้สามารถ เข้ารหัส ใช้คนเดียวได้ ลงทะเบียนใช้แบบปลั๊กแอนด์เพล (Secure Single Sign-on plug and play)

2. แสดงผลลัพธ์อย่างเที่ยงตรงแม่นยำ ในภาพรวมและสถานการณ์การณ์ที่พึงระวัง จากโครงข่ายสารสนเทศกิจการกองทัพบก (AEI)

3. พยากรณ์ / คาดเดา ผลกระทบต่อโครงข่ายสารสนเทศกิจการกองทัพบก (AEI) ในเรื่องระบบใหม่ๆหรือข่าวสารใหม่ๆ และแผนการปฏิบัติการฉุกเฉิน

4. Redirect และ Reallocate แหล่งทรัพยากรของโครงข่ายสารสนเทศกิจการกองทัพบก (AEI) ในโหมด Near Real time เพื่อรองรับเหตุการณ์วิกฤตหรือเหตุการณ์ที่ไม่คาดคิด ทุกๆแห่งในพื้นที่รับผิดชอบ

5. จัดให้มีบริการที่คงทนถาวร ทำงานเป็นหุ่นยนต์เพื่อให้บริการขั้นพื้นฐานจากโครงข่ายสารสนเทศระดับพื้นฐานแก่ผู้ใช้ทุกคนที่ได้รับอนุญาต ในต้นทุน(cost)ที่ถูกที่สุดเท่าที่จะเป็นไปได้ภายใต้ข้อจำกัดทางด้านยุทธการของกองทัพบก

6. จัดให้มีบริการโครงข่ายสารสนเทศเพิ่มเติม (สูงกว่าพื้นฐาน)ให้แก่ผู้ใช้บนพื้นฐานซึ่งใช้เงินคืนได้(reimbursable basis)

7. ปฏิบัติการป้องกันการบุกรุกอย่างต่อเนื่องโดยไม่รบกวน/สอดแทรกทางเทคโนโลยี เพื่อเพิ่มพูนระดับการบริการ หรือเพื่อลดค่าใช้จ่ายของการจัดให้มีบริการขั้นพื้นฐาน

8. จัดให้มีขีดความสามารถในการวางแผนยุทธการได้อย่างต่อเนื่อง (continuity of operations / CONOPS)

การปฏิบัติการเครือข่าย (NETOPS) จัดให้มีเทคโนโลยีสารสนเทศและการเฝ้าระวัง, การติดตามสถานการณ์, การปกป้องการไหลของข้อมูลข่าวสาร , และการบริหารจัดการเครือข่าย, การสนธิ IA(Information Assurance) และการบริหารด้านการกระจายข้อมูลข่าวสาร แผนภาพที่ 2-2

แผนภาพที่ 2-2 พื้นที่รับผิดชอบและพันธะกิจของการปฏิบัติการเครือข่าย/ NETOPS


Figure 3-2. NETOPS Mission Areas and Functions

## แนวคิดในการจัดตั้งหน่วยงานไซเบอร์ทั้งในประเทศและต่างประเทศ

ประธานาธิบดีบารัค โอบามา แห่งสหรัฐอเมริกา อนุมัติคำสั่งประธานาธิบดี (executive order) ในประเด็นเรื่องการพัฒนาความปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญของประเทศ (Improving Critical Infrastructure Cybersecurity) มีผลบังคับใช้ตั้งแต่วันที่ 13 กุมภาพันธ์[5]

การอนุมัติคำสั่งครั้งนี้เกิดขึ้นเพราะประธานาธิบดีแห่งสหรัฐอเมริกา ยังไม่สามารถผลักดันกฎหมายระดับพระราชบัญญัติที่เกี่ยวกับความปลอดภัยไซเบอร์ให้ผ่านสภาคองเกรสได้ จึงต้องหันมาใช้วิธี “คำสั่งประธานาธิบดี” ที่มีศักดิ์น้อยกว่า และมีผลบังคับใช้เฉพาะหน่วยงานภาครัฐของสหรัฐอเมริกา

ปัญหาเรื่องสงครามไซเบอร์เริ่มเป็นภัยคุกคามต่อสหรัฐมากขึ้นเรื่อยๆ โดยลีออน พาเนตตา รัฐมนตรีว่าการกระทรวงกลาโหมของสหรัฐเคยออกมาเตือนว่าสหรัฐอาจจะพบกับการโจมตีไซเบอร์ครั้งใหญ่โดยไม่รู้ตัว (ใช้คำว่า Cyber-Pearl Harbor) ในอีกไม่ช้า และช่วงไม่กี่เดือนที่ผ่านมาเราก็เริ่มเห็นความพยายามของรัฐบาลสหรัฐในการรับมือภัยคุกคามใหม่นี้ เช่น การเพิ่มจำนวนบุคคลากรใน “กองกำลังไซเบอร์” ของเพนตากอนจาก 900 เป็น 4,000 ตำแหน่ง

ประธานาธิบดี บารัค โอบามา แห่งสหรัฐอเมริกากับการแถลงนโยบาย State of the Union ปี 2013 ( Obama State of the Union 2013 )

มุมมองของรัฐบาลโอบามาต่อ “ความมั่นคงไซเบอร์” คือ สาธารณูปโภคและโครงสร้างพื้นฐานสำคัญๆ ของประเทศ เช่น ระบบไฟฟ้า ระบบการควบคุมการบินและจราจร ระบบกำจัดขยะและของเสีย โครงข่ายโทรคมนาคม ไปจนถึงโรงไฟฟ้านิวเคลียร์ ซึ่งปัจจุบันถูกควบคุมโดยระบบคอมพิวเตอร์ทั้งหมด ซึ่งอาจเป็นเป้าหมายของศัตรูหรือคนที่ไม่หวังดีต่อสหรัฐ ใช้วิธีการโจมตีทางอิเล็กทรอนิกส์ เช่น การแฮ็ก หรือปล่อยไวรัส-เวิร์ม โจมตีจนระบบเหล่านี้ใช้งานไม่ได้ ส่งผลกระทบต่อเศรษฐกิจและความมั่นคงของประเทศ

หน่วยรัฐบาลไม่ได้เป็นเจ้าของโครงสร้างพื้นฐานเหล่านี้ทั้งหมด ทำให้การป้องกันประเทศจากการโจมตีอิเล็กทรอนิกส์ทำได้ยาก เพราะภาคเอกชนไม่กล้าหรือไม่ประสงค์จะแชร์ข้อมูลด้านการโจมตีให้ ดังนั้นในคำสั่งล่าสุดของประธานาธิบดี จึงมีเป้าหมายเพื่อชักจูงให้ภาคเอกชนหันมาให้ความร่วมมือกับหน่วยงานภาครัฐมากขึ้น

---

[5] Siam Intelligence. (ออนไลน์). เข้าถึงได้จาก : http://www.siamintelligence.com/obama-cyber-security -order/, 2556.

เนื้อหาที่สำคัญในคำสั่งของโอบามามีดังนี้

นิยามของ “โครงสร้างพื้นฐานที่สำคัญ” คำสั่งประธานาธิบดีกำหนดนิยมของ “critical infrastructure” ว่าหมายถึงระบบและทรัพย์สิน ทั้งในเชิงกายภาพหรือเสมือน ที่สำคัญต่อสหรัฐในระดับที่ส่งผลกระเทือนต่อความมั่นคงของประเทศ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางสาธารณสุข และความปลอดภัยสาธารณะ

<u>หน่วยงานผู้รับผิดชอบ</u> ให้กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) เป็นแกนหลักในการทำงาน โดยรัฐมนตรีกระทรวงความมั่นคงแห่งมาตุภูมิ เป็นเจ้าหน้าที่รัฐคนสำคัญ ต้องทำงานร่วมกับหน่วยงานอื่นๆ เช่น อัยการสูงสุด ผู้อำนวยการสำนักข่าวกรอง เพื่อปรับระบบป้องกันภัยต่อสาธารณูปโภคพื้นฐานให้มั่นคงขึ้น

<u>การออกรายงานสถานการณ์ความปลอดภัย</u> หน่วยงานทั้งสามคือ กระทรวงความมั่นคงแห่งมาตุภูมิ อัยการสูงสุด สำนักข่าวกรองแห่งชาติ จะต้องสร้างระบบการรายงานสถานการณ์ด้านความปลอดภัยไซเบอร์ ที่ระบุความเสี่ยงหรือจุดเสี่ยงที่จะโดนโจมตี

<u>สร้างความร่วมมือกับภาคเอกชน</u> กระทรวงความมั่นคงแห่งมาตุภูมิ จะต้องขยายโครงการยกระดับความปลอดภัยไซเบอร์ (Enhanced Security Services) จากเดิมที่ครอบคลุมเฉพาะหน่วยงานภาครัฐ ให้ครอบคลุมหน่วยงานภาคเอกชนที่ดูแลโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยหน่วยงานภาคเอกชนสามารถเข้าร่วมโดยสมัครใจ การเข้าร่วมโครงการนี้จะช่วยให้การแชร์ข้อมูลด้านความปลอดภัยของเอกชนและรัฐคล่องตัวมากขึ้น

นอกจากนี้ รัฐมนตรีกระทรวงความมั่นคงแห่งมาตุภูมิ ต้องเร่งกระบวนการคัดกรองบุคคลากรจากภาคเอกชน ที่ดูแลโครงสร้างพื้นฐานของประเทศ ให้เข้าถึงระดับชั้นข้อมูลความปลอดภัยของรัฐได้

<u>ออกกรอบการทำงานด้านความมั่นคงของโครงสร้างพื้นฐาน</u> ให้รัฐมนตรีว่าการกระทรวงพาณิชย์ ออกคำสั่งแก่ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) พัฒนากรอบการทำงาน Cyber security Framework เพื่อลดความเสี่ยงต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยครอบคลุมมาตรฐาน กระบวนการ ขั้นตอนต่างๆ โดยยึดตามมาตรฐานที่ได้รับการยอมรับโดยอุตสาหกรรมอยู่แล้ว

เมื่อกรอบการทำงานเสร็จแล้ว ให้หน่วยงานต่างๆ ของรัฐที่เกี่ยวข้อง พัฒนาระบบจูงใจให้ภาคเอกชนดำเนินการปรับปรุงระบบของตัวเองให้เข้ากับกรอบการทำงาน Cyber Security ทั้งในแง่ผลประโยชน์ (incentive) และข้อมูล-คำแนะนำ (guidance)

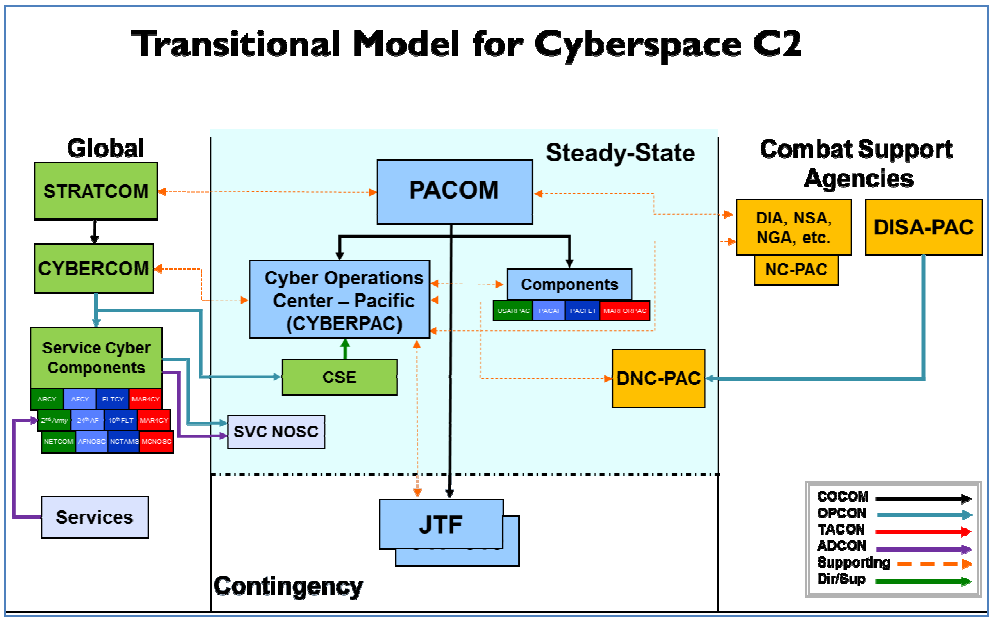
หน่วยงานของรัฐยังต้องนำกรอบการทำงานนี้ไปตรวจสอบกับกฎระเบียบในหน่วยงานของตัวเอง ว่ามีกฎระเบียบใดขัดแย้งกับกรอบการทำงานหรือไม่ และกฎระเบียบในปัจจุบันเพียงพอกับมาตรฐานด้านความมั่นคงที่กำหนดขึ้นมาใหม่หรือไม่ ถ้าไม่เพียงพอต้องพัฒนากฎระเบียบใหม่ให้แล้วเสร็จภายใน 2 ปี

ค้นหาจุดเสี่ยงและแจ้งเตือนผู้ประกอบการ กระทรวงความมั่นคงแห่งมาตุภูมิจะต้องค้นหาและแยกแยะโครงสร้างพื้นฐานส่วนที่มีความเสี่ยงสูง ที่จะส่งผลกระทบในด้านความปลอดภัยสาธารณะ สาธารณสุข ความมั่นคงทางเศรษฐกิจ รวมถึงความมั่นคงของชาติ

เมื่อแยกแยะได้แล้ว กระทรวงฯ จะต้องแจ้งเตือนเจ้าของหรือผู้ให้บริการโครงสร้างพื้นฐานที่มีความเสี่ยงให้รู้ตัว โดยวิธีการแจ้งเตือนในทางลับ และกระทรวงต้องรายงานชื่อองค์กรที่มีความเสี่ยงต่อประธานาธิบดีอย่างน้อยปีละ 1 ครั้ง

## Cyber Command ของสหรัฐ

แผนภาพที่ 2-3 แสดงสายงานของการควบคุมบังคับบัญชาในด้านไซเบอร์ของสหรัฐฯ



สหรัฐฯเป็นประเทศที่ให้ความสำคัญกับเรื่องสงครามไซเบอร์มากที่สุด โดยเริ่มแรกนั้นได้ปรับหลักนิยม (Doctrine) ด้านทหารใหม่ โดยได้เพิ่มสมรภูมิการรบที่ 5 คือ ไซเบอร์ ให้เทียบเท่ากับสมรภูมิรบที่มีอยู่คือ บก ทะเล อากาศ และอวกาศ สมรภูมิบกก็จะมีกองทัพบกรับผิดชอบ สมรภูมิทะเลหรือมหาสมุทรก็จะมีกองทัพเรือดูแลอยู่ ส่วนห้วงอากาศก็จะมีกองทัพอากาศคอยปกป้องอยู่ ส่วนอวกาศนั้นก็จะมีหน่วยทหารที่รับผิดชอบโดยตรงอยู่แต่ยังไม่ถึงกับเรียกว่าเป็นกองทัพอวกาศ ดังนั้นการที่กำหนดให้ไซเบอร์เป็นอีกหนึ่งสมรภูมิแห่งการสู้รบนั้นเพื่อที่จะได้จัดตั้งกองกำลังที่รับผิดชอบในการรบในสมรภูมินี้ ซึ่งไม่แน่ในอนาคตอาจมีกองทัพไซเบอร์เกิดขึ้นในบางประเทศก็ได้ โดยล่าสุดสหรัฐฯได้ก่อตั้งกองกำลังเพื่อต่อสู้ในโลกไซเบอร์ นั่นคือ ไซเบอร์คอมแมนด์ (Cyber Command)

จากแผนภาพที่ 2-3 หน่วยงานไซเบอร์คอมแมนด์ (US CYBERCOM) เป็นกองบัญชาการรบร่วมระดับรอง (sub-unified command) โดยจะขึ้นตรงกับสตราทีจิกคอมแมนด์ (USSTRATCOM) ไซเบอร์คอมแมนด์ตั้งอยู่ในฐานทัพฟอร์ทมีดในมนรัฐแมร์รี่แลนด์ ซึ่งเป็นศูนย์บัญชาการรบร่วมที่รับผิดชอบเกี่ยวกับการปฏิบัติการทางทหารในไซเบอร์สเปซทั้งหมด อย่างไรก็ตามหน้าที่หลักของไซเบอร์คอมแมนด์คือการปกป้องระบบเครือข่ายที่ทหารเป็นผู้รับผิดชอบ ในขณะที่ระบบเครือข่ายของรัฐบาลฝ่ายพลเรือนนั้นจะเป็นหน้าที่ของกระทรวงโฮมแลนด์ซีเคียวลิตี้ ไซเบอร์คอมแมนด์จะมีส่วนของกองกาลังที่อยู่ในสังกัดเหล่าทัพต่างๆ ซึ่งประกอบด้วย 2nd Army (กองทัพบกที่สอง), 10th Fleet (กองทัพเรือที่สิบ), 24th Air Force (กองทัพอากาศที่ยี่สิบสี่) และ กองกำลังไซเบอร์มารีนคอร์ป (US Marine Corps Forces Cyberspace Command) ในส่วนของกองทัพอากาศที่ยี่สิบสี่นั้นจะประกอบด้วย 3 กองบินและหนึ่งศูนย์ปฏิบัติการ ซึ่งประกอบด้วย 67th Network Warfare Wing, 688th Information Operations Wing, 689th Combat Communications Wing และ 624th Operations Center

## หน่วยงานไซเบอร์สาธารณรัฐประชาชนจีน

สาธารณรัฐประชาชนจีนเคยโดนโจมตีทางด้านไซเบอร์ในวันชาติ วันที่ 1 ตุลาคม 2553 จนภาคอุตสาหกรรมต้องหยุดการทำงานเพราะคอมพิวเตอร์ใช้งานไม่ได้ ถือเป็นการโจมตีทางไซเบอร์ ที่โครงสร้างพื้นฐานในการควบคุมสั่งการและประเมินผลของโรงงานในภาคอุตสาหกรรม จีนจึงถึงตระหนักว่าสงครามไซเบอร์อุบัติขึ้นแล้ว จึงจัดตั้งหน่วยดูแลความปลอดภัยทางอินเตอร์เน็ตเพื่อป้องกันการโจมตีทางไซเบอร์ที่มีชื่อว่า Cyber Blue Team

## หน่วยงานไซเบอร์ของเกาหลีใต้

เมื่อ เดือน มิถุนายน 2554 รัฐบาลเกาหลีใต้ได้จัดตั้งโรงเรียนสงครามบนโลกไซเบอร์ที่มหาวิทยาลัยโคเรีย เพื่อสร้างบุคลากรให้รับมือการโจมตีทางอินเตอร์เน็ตจากเกาหลีเหนือ หลักสูตร 4 ปี รับนักศึกษาปีละ 30 คน กองทัพจ่ายค่าเล่าเรียนให้นักศึกษาทุกบาททุกสตางค์ แต่จบมาแล้ว ต้องไปบรรจุเป็นนายทหารชั้นสัญญาบัตร และทำงานด้านสงครามบนโลกออนไลน์เป็นเวลา 7 ปี นอกจากนั้นยังมีการจัดตั้งหน่วยงานระดับชาติที่เรียกว่า National Cyber Security Center

สรุปการการจัดตั้งหน่วยไซเบอร์ในต่างประเทศ

1. สหรัฐฯ จัดตั้งหน่วยบัญชาการไซเบอร์ ( US Cyber Command ) นอกจากนั้น กองทัพอากาศสหรัฐฯ ยังมีการจัดตั้งหน่วย Air Force Cyber Command ( AFCYBER) ซึ่งยังไม่ได้ประกาศเป็นทางการ ปัจจุบันเป็นเพียงข้อเสนอ

2. จีน จัดตั้งหน่วย Cyber Blue Team เพื่อรักษาความปลอดภัยต่อเครือข่ายระบบคอมพิวเตอร์ของกองทัพ และหน่วย Unit 61398 เพื่อการจารกรรมทางไซเบอร์

3. อินเดีย จัดตั้งหน่วย Cyber Command and Control Authority

4. เกาหลีเหนือ จัดตั้งหน่วย Korean People's Army Joint Chiefs Cyber Warfare Unit หรือ Unit 121

5. สหภาพยุโรป จัดตั้งสำนักงาน European Network and Information Security Agency

6. เกาหลีใต้ จัดตั้งหน่วยสงครามไซเบอร์ระดับชาติ เน้นการสร้างขีดความสามารถการโจมตีทางไซเบอร์

7. กระทรวงกลาโหมของประเทศสิงค์โปร์ : IT Security Operations

8. กระทรวงกลาโหมของประเทศมาเลเซีย : Cyber Security Division และ รัฐบาลมาเลเซีย : National ICT Security and Emergency Response Center (NISER)

9. ประเทศพม่าหรือเมียนม่าร์: จัดตั้ง Cyber Warfare Department ( หนังสือ Burma's Military Secrets )

10. ไต้หวัน : จัดตั้ง Military Information Warfare Strategy Policy Committee ซึ่งปัจจุบันได้ขยายและปรับเปลี่ยนเป็น Center ขนาด กองทัพขึ้นตรงกับ General Staff Headquaters (Jane's Intelligence Review, 10 January 2001, หน้า 17)

สรุปหน่วยงานที่เกี่ยวข้องทางด้านไซเบอร์ของกองทัพไทย

1. สำนักงานปลัดกระทรวงกลาโหม : ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยี สารสนเทศและอวกาศกลาโหม (ศรค.ทสอ.กห.)

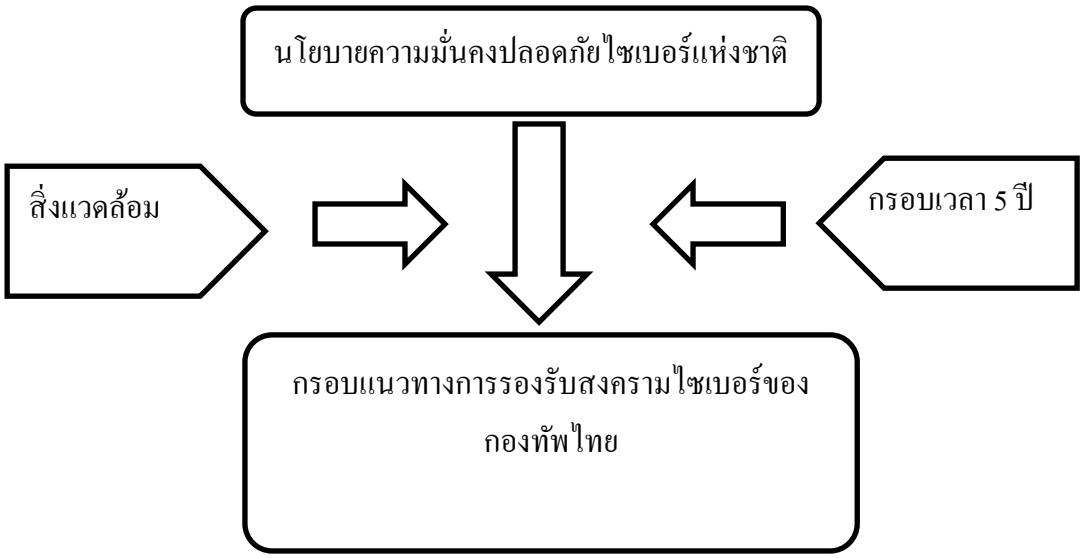
2. กองบัญชาการกองทัพไทย : กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศกรมการสื่อสารทหาร (กรส.ศทส.สส.ทหาร)

3. กองทัพบก : กองการสงครามสารสนเทศ ศูนย์เทคโนโลยีทางทหาร กรมการทหารสื่อสาร (กสสท.ศทท.)

4. กองทัพเรือ : กองปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (กปท.สสท.ทร.)

5. กองทัพอากาศ : กองสงครามอิเล็กทรอนิกส์และสารสนเทศ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (กคส.ทสส.ทอ.)

## กรอบความคิดของการวิจัย



# บทที่ 3
# การรองรับสงครามไซเบอร์ในปัจจุบัน

## ปัญหาและผลกระทบทางด้านสงครามไซเบอร์

ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการควบคุมระบบ หมายถึงใครก็ตามที่พยายามเข้าถึงอุปกรณ์ระบบควบคุมและ / หรือเครือข่ายโดยใช้เส้นทางการติดต่อสื่อสารแบบข้อมูล การเข้าถึงนี้สามารถเข้าถึงได้โดยตรงจากภายในองค์กรโดยผู้ใช้ที่เชื่อถือได้หรือจากสถานที่ห่างไกลโดยบุคคลที่ไม่รู้จัก แต่เป็นการใช้เครือข่ายอินเทอร์เน็ตเท่านั้น ภัยคุกคามที่จะควบคุมระบบสามารถมาจากแหล่งที่แตกต่างกันจำนวนมากรวมถึงรัฐบาลที่เป็นฝ่ายตรงข้ามกับประเทศของเรา กลุ่มก่อการร้าย เจ้าหน้าที่ภายในที่ไม่พอใจหน่วยงานและผู้บุกรุกที่เป็นอันตรายต่างๆ การที่จะป้องกันภัยคุกคามเหล่านี้ จำเป็นต้องมีการสร้างความปลอดภัยไซเบอร์ เพื่อสร้างแนวทางขัดขวางหรือป้องกันต่อระบบควบคุมของเฟ้าเรา รวมทั้งภัยคุกคามอื่น ๆ เช่น ภัยพิบัติทางธรรมชาติ สิ่งแวดล้อมที่เป็นพิษ ความล้มเหลวทางระบบกลไกต่างๆ และการกระทำโดยไม่ได้ตั้งใจของผู้ใช้ที่ได้รับอนุญาตการเข้าถึงระบบ ดังนั้นจะขอแบ่งผลกระทบทางด้านสงครามไซเบอร์ [1] โดยมองที่ระดับภัยคุกคามไว้ดังนี้

1. ภัยคุกคามในระดับรัฐบาลแห่งชาติ ( National Governments )
2. ภัยคุกคามในระดับการก่อการร้าย ( Terrorists )
3. สายลับหรือพวกจารกรรมในภาคอุตสาหกรรม และกลุ่มองค์กรอาชญากรรม ( Industrial Spies and Organized Crime Groups )
4. กลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ ( Hacktivists )
5. กลุ่มแฮ็กเกอร์ ( Hackers )

---

[1] Industrial Control Systems Cyber Emergency Response Team. (ออนไลน์). เข้าถึงได้จาก : https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions, 2544.

**รัฐบาลแห่งชาติ (National Governments)**

แนวทางของสงครามไซเบอร์แห่งชาติ จะต้องไม่ซ้ำซ้อนกัน ในการกำหนดตัวภัยคุกคาม ซึ่งเป็นไปตามภาพที่เห็นหรือสิ่งที่ปรากฏขึ้น โดยวัตถุประสงค์ทั้งหมดของการกำหนดภัยคุกคามนั้น จะพิจารณาที่อาจจะเป็นอันตรายต่อผลประโยชน์ของประเทศชาติ สำหรับภัยคุกคามเหล่านี้ มีตั้งแต่ การโฆษณาชวนเชื่อ หรือแค่การเปลี่ยนแปลงหน้าเว็บไซต์ เพื่อสร้างความรำคาญให้กับหน่วยงานของรัฐบาล ตลอดจนถึงขั้นทำให้เกิดการหยุดชะงักของโครงสร้างพื้นฐาน เช่น ระบบไฟฟ้า ประปา เป็นต้น สำหรับขอบเขตของกระบวนการต่างๆ ของภัยคุกคามนั้น จะมีการกำหนดแผนการปฏิบัติที่ได้รับการสนับสนุนจากภาครัฐฝ่ายตรงข้าม เพื่อให้เกิดความเสียหายเป็นวงกว้าง ต่อรัฐเป้าหมายหรืออีกฝ่ายหนึ่ง โดยเฉพาะเป้าหมายที่โครงสร้างพื้นฐานของประเทศจะถูกกำหนดไว้เป็นเป้าหมายหลักในการดำเนินการ

วิธีปฏิบัติ จะกระทำโดยพวกสายลับมืออาชีพ (tradecraft) ที่มีการใช้เทคโนโลยีที่มีประสิทธิภาพ และเครื่องมือที่ทันสมัยเป็นปัจจัยสำคัญ โดยเฉพาะอย่างยิ่งกับเป้าหมายที่ยากจะดำเนินการ เช่น เครือข่ายการสื่อสารหลักของประเทศ หรือ ส่วนของโครงสร้างพื้นฐานของประเทศที่สำคัญ เป็นต้น

เป้าหมายหลัก ของพวกเขา คือ การสร้างความอ่อนแอ การรบกวน หรือการทำลายประเทศ ส่วนเป้าหมายรอง คือ การจารกรรมเพื่อสร้างการโจมตีต่อเป้าหมายโดยเฉพาะหน่วยงานรัฐหรือหน่วยงานความมั่นคง เพื่อให้ได้ข้อมูลความก้าวหน้าทางด้านเทคโนโลยี การหยุดชะงักของโครงสร้างพื้นฐาน ตลอดจนมุ่งไปสู่การโจมตีต่อระบบเศรษฐกิจของประเทศ นอกจากนั้นการโจมตีชนิดเต็มรูปแบบต่อโครงสร้างพื้นฐาน เป็นการโจมตีเพื่อมุ่งทำลายความสามารถของรัฐอย่างต่อเนื่อง และรัฐเป้าหมายจะไม่สามารถตอบโต้การดำเนินการนั้นๆ ได้

สำหรับการโจมตีในระดับประเทศ จะขอยกตัวอย่างกรณี สตักซ์เน็ต (Stuxnet) คือ หนอนคอมพิวเตอร์ (worm) ที่ถูกตรวจพบเป็นครั้งแรกเมื่อเดือน มิถุนายนปี 2553 สตักซ์เน็ต พิเศษกว่ามัลแวร์ตัวอื่นๆ คือมันถูกสร้างขึ้นเพื่อมุ่งทำลายระบบควบคุมในโรงงานผลิตอาวุธนิวเคลียร์ในประเทศอิหร่านและก็ทำได้สำเร็จด้วย โดยการดำเนินการนั้นสตักซ์เน็ตเข้าไปทำลายระบบควบคุมการประมวลผล SCADA (Supervisory Control and Data Acquisition) ที่ผลิตโดยบริษัท Siemen และใช้ในการควบคุมกระบวนการต่าง ๆ ในโรงงานอุตสาหกรรม และระบบสาธารณูปโภคต่าง ๆ ระบบท่อส่งน้ำมัน ระบบสายส่งไฟฟ้า และระบบโรงงานนิวเคลียร์ทั่วโลก สตักซ์เน็ตสามารถฝังตัวเข้าไปในโปรแกรม Step-7 ซึ่งเป็นโปรแกรมที่ทำงานบน PLCs (Programmable Logic Controllers) ซึ่งเป็น

ตัวควบคุมการทำงานของระบบ ต่างๆในโรงงานอุตสาหกรรม[2]

ทางบริษัท Symantec ได้รายงานว่า เป้าหมายของสตักซ์เน็ต คือเครื่องคอมพิวเตอร์ในประเทศอิหร่าน ซึ่งมากกว่า 60% ของเครื่องคอมพิวเตอร์ที่ถูกโจมตี โดยทางการอิหร่านได้ยอมรับเป็นครั้งแรกว่าสตักซ์เน็ตได้เจาะเข้าไปยังระบบคอมพิวเตอร์ของโรงไฟฟ้านิวเคลียร์ ปัจจุบันมีรายงานว่าสตักซ์เน็ตเริ่มมีการแพร่กระจายไปยังโรงงานอุตสาหกรรมในประเทศจีนอีกด้วยซึ่งมีคำถามที่ตามมาคือ จีนไปเป็นเป้าหมายถัดไปหรือไม่

สตักส์เน็ตเป็นเวิร์มหรือไวรัสที่เชื่อว่าพัฒนาโดยประเทศสหรัฐอเมริกา โดยมีเป้าหมายเพื่อเข้าไปทำลายระบบ SCADA ซึ่งเป็นระบบคอมพิวเตอร์ที่ใช้ควบคุมและพัฒนาระบบอาวุธนิวเคลียร์ของประเทศอิหร่าน และการโจมตีของสตักส์เน็ตนั้นได้ผลจริง ทำให้ประเทศอิหร่านได้ประกาศเลื่อนความสำเร็จของโครงการนิวเคลียร์ออกไปอีก สตักส์เน็ต (Stuxnet) เป็นสิ่งที่พิสูจน์ให้เห็นแล้วว่าสงครามไซเบอร์นั้นเกิดขึ้นจริง การโจมตีของสตักส์เน็ต ซึ่งจากมองสิ่งที่กล่าวนั้นเป็นการโจมตีในระดับชาติก็ย่อมได้

## การก่อการร้าย (Terrorists )

กลุ่มการก่อร้าย ยังคงใช้วิธีการเดิม มุ่งสร้างความเสียหายต่อผลประโยชน์ของประเทศหรือชาติต่างๆ โดยสาเหตุที่การพัฒนาระบบเครือข่ายคอมพิวเตอร์มีข้อจำกัดหลายประการ การดำเนินการภายใต้เครือข่ายคอมพิวเตอร์ของกลุ่มก่อการร้ายย่อมจะทำให้เกิดภัยคุกคามเพียงขอบเขตจำกัดไปด้วย ปกติการก่อการร้ายโดยทั่วไป อาจจะใช้ระเบิดทำลายเป้าหมาย แต่การก่อร้ายทางไซเบอร์ ก็เป็นเพียงใช้รหัสโปรแกรมคอมพิวเตอร์ (Code Program ) เท่านั้น การสร้างความเสียจึงถูกจำกัดตัวลงโดยปริยาย แต่ในอนาคตภัยคุกคามทางไซเบอร์ในส่วนนี้อาจจะได้รับการพัฒนาเทคโนโลยีที่เพิ่มระดับความรุนแรงขึ้นมาก็เป็นได้

ส่วนเป้าหมายหลัก คือการสร้างความหวาดกลัว ไปยังประชาชนในประเทศเป้าหมาย ส่วนเป้าหมายรอง คือการสร้างหรือก่อให้เกิดดการบาดเจ็บล้มตายให้เกิดขึ้น รวมถึงการสร้างความอ่อนแอต่อระบบเศรษฐกิจของประเทศเป้าหมายจากการเกิดขึ้นของสงครามการก่อร้ายไปทั่วโลก

---

[2] น.ท.จตุชัย แพงจันทร์. “สงครามไซเบอร์ได้เริ่มขึ้นแล้ว”. (ออนไลน์). เข้าถึงได้จาก : http://www.rtafa.ac.th. , 2557

## สายลับหรือพวกจารกรรมในภาคอุตสาหกรรม และกลุ่มองค์กรอาชญากรรม (Industrial Spies and Organized Crime Groups )

การจารกรรมขององค์กรระหว่างประเทศและองค์กรเครือข่ายอาชญากรรมต่างๆ เป็นภัยคุกคามระดับกลางของประเทศ โดยที่พวกเขามีขีดความสามารถ ที่จะดำเนินการจารกรรมและการปล้นสะดมต่องบประมาณในระบบอุตสาหกรรมขนาดใหญ่ รวมทั้งความสามารถของพวกเขาที่จะดำเนินการจ้างหรือพัฒนาความสามารถของแฮ็กเกอร์ของกลุ่มของเขาเองได้

เป้าหมายหลักของพวกเขาจะหวังในผลประโยชน์ที่ได้รับเป็นหลัก ส่วนเป้าหมายรองของพวกเขา ก็คือการโจมตีในโครงสร้างพื้นฐานสำหรับคู่แข่งทางการค้าหรือกลุ่มเป้าหมายอื่น ๆ ซึ่งการดำเนินการเบื้องต้นก็เป็นการขโมยความลับทางการค้าและเมื่อพวกเขาได้รับสิทธิเข้าถึงระบบฯ พวกเขาก็จะแบล็กเมล์เพื่อเรียกร้องผลประโยชน์ ส่วนมากแล้วจะโจมตีที่ส่วนอุตสาหกรรมสำหรับการให้บริการประชาชน โดยที่พวกเขาใช้ความเสี่ยงของประชาชนที่ได้รับผลกระทบเกิดขึ้นเป็นภัยคุกคามนั่นเอง

## กลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ ( Hacktivists )

กลุ่มแฮ็กเกอร์ ( Hacker ) ที่มีอุดมการณ์เป็นรูปแบบของกลุ่มเล็กๆมีแรงจูงใจหรือแนวทางเพื่ออุดมการณ์ทางการเมือง หรือบุคคลทางการเมือง รวมทั้งกลุ่มต่อต้านต่างๆ ในระดับประเทศที่เป็นฝ่ายตรงกันข้าม พวกเขาเป็นภัยคุกคามในระดับกลางในการดำเนินการโจมตีกระจายไปในเมืองเป้าหมาย แต่ความเสียหายส่วนใหญ่กลุ่มแฮ็กเกอร์นี้ ( hacktivist) ที่สร้างขึ้นในระหว่างประเทศ มักปรากฏให้เห็นชัดเจนในด้านการโฆษณาชวนเชื่อมากกว่าความเสียหายให้กับโครงสร้างพื้นฐานที่สำคัญ เป้าหมายหลักของพวกเขาคือการสนับสนุนแนวทางหรือวาระทางการเมืองของพวกเขา ส่วนเป้าหมายรองของพวกเขาคือการโฆษณาชวนเชื่อและส่วนความเสียหายที่ก่อให้เกิดนั้นก็เพียงเพื่อให้บรรลุแนวทางที่พวกเขาต้องการให้เป็นไปเท่านั้น

สำหรับตัวอย่างที่น่าสนใจของกลุ่มแฮ็กเกอร์ดังกล่าว ได้แก่กลุ่มที่เรียกว่า Ghostnet เป็นกลุ่มแฮ็กเกอร์ชาวจีน[3] ที่มีข่าวว่ามีการปฏิบัติการโจมตีเพื่อเป้าหมายทางการเมือง เช่น กรณีผู้ดูแลสำนักงานของ องค์ทะไลลามะ (ที่ เมืองธรรมศาลา ประเทศอินเดีย) สงสัยว่าโดนขโมยข้อมูล

---

[3] Mr P 2552. “Ghostnet แฮกเกอร์จีนประกาศศักดาล้วงข้อมูลลับจากประเทศทั่วโลก”. (ออนไลน์). เข้าถึงได้จาก : http://supojcherd.blogspot.com/2009/05/ghostnet.html, 2552.

ซึ่งเป็นเอกสารลับ จึงเชิญ เกร็ก วอลตัน ผู้เชี่ยวชาญจากองค์กรเฝ้าระวังสงครามข้อมูลของแคนาดา ( IWM) มาตรวจสอบ ก็พบว่าข้อมูลของ โค้ด มัลแวร์/โทรจัน ที่โจมตีนี้ บ่งชี้ว่ามาจากเซิร์ฟเวอร์ 3 ตัว ที่ตั้งอยู่ที่ เกาะไหหลำ กวางตุ้ง และที่ซิฉวน ในประเทศจีน แต่ถึงอย่างไรทางรัฐบาลจีนให้การปฏิเสธในเรื่องดังกล่าว และไม่ยอมรับว่ามีกลุ่มแฮ็กเกอร์ดังกล่าวอยู่จริง โดยนาย ซ่ง เสี่ยวจวิน นักวิเคราะห์ทางการทหารและยุทธศาสตร์ในกรุงปักกิ่ง บอกกับไชน่า เดลี่ (นสพ.จีน) ว่า กรณีดังกล่าวเป็นประเด็นการเมืองล้วนๆ โดยกลุ่มตะวันตกพยายามระบายสีต่อเติมเรื่องเกินจริง แต่ถึงอย่างไรองค์กรเฝ้าระวังสงครามข้อมูลของแคนาดา (IWM) เองก็เชื่อว่าอาจจะเป็นกลุ่มแฮ็กเกอร์รับจ้าง หรืออาจจะเป็นกลุ่มแฮ็กเกอร์เอกชนชาวจีน ที่รู้จักกันในนาม "แฮ็กเกอร์รักชาติ" ก็ได้ และได้ส่งเรื่องให้กับเอฟบีไอเพื่อดำเนินการต่อไปเรียบร้อยแล้ว

## แฮ็กเกอร์ ( Hackers )

แม้ว่าการโจมตีไซเบอร์แบบนี้จะเกิดมากที่สุดและมีการประชาสัมพันธ์เผยแพร่อย่างกว้างขวาง โดยมากเหตุการณ์ต่างๆเหล่านั้นมักจะเกิดจากคนเดียวๆ นั่นก็คือจากพวกเหล่าแฮ็กเกอร์มือสมัครเล่นนั่นเอง โดยที่แฮ็กเกอร์ดังกล่าวก็สามารถก่อให้เกิดภัยคุกคามที่สำคัญอย่างกว้างขวางและส่งผลกระทบรวมทั้งการสร้างความเสียหายในระยะยาวให้กับโครงสร้างพื้นฐานในระดับชาติได้ ส่วนมากแล้วพวกแฮ็กเกอร์เหล่านี้ไม่ได้มีความจำเป็นที่จะใช้วิธีปฏิบัติอย่างของสายลับมืออาชีพ (tradecraft) เพื่อคุกคามเป้าหมายที่ยากลำบาก เช่น เครือข่ายที่สำคัญในประเทศเลยแม้แต่น้อย แต่จะใช้เพียงแรงจูงใจที่จะกระทำเท่านั้น แต่ถึงอย่างไรพวกแฮ็กเกอร์เหล่านั้นที่กระจายอยู่ทั่วโลก ก็ยังเป็นกลุ่มของแฮ็กเกอร์ที่มีขนาดใหญ่ และยังเป็นภัยคุกคามที่ค่อนข้างสูง ที่ส่งผลกระทบ ซึ่งขึ้นอยู่กับขอบเขตและการหยุดชะงักของระบบฯ อันก่อให้เกิดความเสียหายอย่างร้ายแรงรวมทั้งความเสียหายต่อทรัพย์สินอย่างกว้างขวางหรือการสูญเสียชีวิตอีกด้วย ในขณะที่ประชากรของกลุ่มแฮ็กเกอร์เหล่านี้มีการขยายตัวเพิ่มขึ้น ถึงแม้ว่าพวกแฮ็กเกอร์เหล่านี้จะไม่ใช่พวกแฮ็กเกอร์ที่มีความเชี่ยวชาญเป็นพิเศษและเป็นอันตรายอย่างร้ายแรง แต่พวกเขาก็อาศัยความพยายามที่ประสบความสำเร็จในการโจมตีดังกล่าวอย่างต่อเนื่องเช่นกัน

นอกจากนี้ปริมาณของกิจกรรมการเจาะระบบ (Hack) ที่มีมากและเกิดขึ้นทั่วโลก จากพวกที่มีฝีมือในการโจมตีไม่มากนัก แต่ก็อาจจะทำให้เกิดการหยุดชะงักของระบบโครงสร้างพื้นฐานที่สำคัญโดยไม่ตั้งใจก็เป็นไปได้เช่นกัน

สำหรับกลุ่มแฮ็กเกอร์ดังกล่าวข้างต้น ยังสามารถจัดแบ่งออกได้เป็นดังนี้

1. กลุ่มสังคมย่อยของเหล่าแฮ็กเกอร์ ( Sub-communities of hackers)

2. Script Kiddies คือแฮ็กเกอร์มือใหม่ที่ยังขาดความชำนาญในการเจาะระบบคอมพิวเตอร์ โดยปกติแล้ว Script Kiddies จะใช้โปรแกรมเจาะระบบที่ถูกพัฒนาโดยพวกแฮ็กเกอร์ ( Hacker ) ที่มีความชำนาญ เชี่ยวชาญสูงๆ มาใช้เจาะระบบคอมพิวเตอร์ที่ตัวเองสนใจด้วยความอยากรู้อยากเห็น หรือทดลองความรู้ในการเจาะระบบของตนเอง เป้าหมายหลัก คือ ความสำเร็จของการเจาะระบบ ส่วนเป้าหมายรอง คือพวกเขาสามารถเข้าถึงระบบฯ และทำการเปลี่ยนแปลงบางอย่างที่เว็บไซต์เป้าหมาย เช่น การเปลี่ยนหน้าเว็บไซต์ เป็นต้น

3. พวกที่เขียนหรือสร้างหนอนและไวรัส[4] (Worm and virus writers) เป็นพวกนักโจมตีระบบที่มีการขยายหรือปล่อยเผยแพร่เชื้อตัวโปรแกรมที่มุ่งประสงค์ร้าย ซึ่งก็คือทั้งหนอนและไวรัสนั่นเอง แต่พวกโปรแกรมฯเหล่านั้นก็ไม่ได้มุ่งเพื่อการเจาะระบบเครื่องที่ติดเชื้อ เป้าหมายหลักคือพฤติกรรมบางอย่างของพวกมัน ซึ่งขึ้นอยู่กับวัตถุประสงค์ในการสร้างของแต่ละตัว ยกตัวอย่างเช่น ไวรัสที่ชื่อว่า ILOVEYOU เป็นไวรัสร้ายแรงที่สร้างความเสียหายกว่า 5 พันล้านดอลลาร์ เครื่องคอมพิวเตอร์กว่า 10% ทั่วโลก ติดเจ้าไวรัสตัวนี้ เริ่มต้นจากส่ง Email ออกไปโดยใช้ชื่อหัวข้อว่า ILOVEYOU หลอกล่อให้กดเข้าไป โดยหลงนึกว่าเป็นจดหมายรัก แต่แอบแฝงไฟล์ร้าย LOVE-LETTER-FOR-YOU.txt. เข้าไปด้วย ถ้าหากว่าเหยื่อเผลอไปกดเข้าละก็ เจ้าไวรัสตัวนี้ก็จะไปดึงชื่อเพื่อนๆของเราที่เก็บไว้ และส่งต่อไปอีก 50 คนทันทีเหมือนจดหมายลูกโซ่ โดยคนที่เขียนไวรัสนี้ขึ้นเป็นคนจากประเทศฟิลิปปินส์ อีกตัวหนึ่งเจ้าหนอนที่ชื่อ Code Red Worm (2001) พฤติกรรมของหนอนชนิดนี้น่าสนใจมากเพราะปกติพอคอมพิวเตอร์ของเราติดเชื้อแล้ว ก็จะแสดงอาการติดเชื้อขึ้นมาทันที แต่สำหรับเจ้านี่มันจะยังไม่แสดงอาการใดๆ โดยช่วงแรกๆมันจะพยายาม กระจายตัวเองอย่างเงียบๆไม่ให้คนที่ติดรู้ตัว ประมาณ 19 วัน หลังจากนั้นจะเริ่มแสดงฤทธิ์เดชความชั่วร้ายออกมา โดยการทำให้คนที่ติดเจ้าหนอนนี้ใช้บริการต่างๆไม่ได้ ไม่เว้นแม้แต่ ทำเนียบขาวก็โดนหนอนตัวนี้ไปแล้วเหมือนกัน หลังจากที่แสดงฤทธิ์เดชไปประมาณ 7 วัน เจ้า code red ก็กลับมาทำตัวสงบเงียบและเริ่มกระจายตัวต่อไปวนเวียนวิธีแบบนี้เรื่อยๆ เป็นต้น

ส่วนเป้าหมายรอง คือ เพื่อให้เกิดการหยุดชะงักของเครือข่ายและการเชื่อมต่อระบบคอมพิวเตอร์ นั่นเอง

1. พวกนักวิจัยทางด้านการรักษาความปลอดภัยและพวกทดสอบการเจอะระบบจากภายใน ( white hat ) แบ่งเป็นสองกลุ่มย่อย ดังนี้ พวกนักล่าความผิดพลาดของโปรแกรม (bug) และรหัสต่างๆ ที่ใช้โจมตีช่องโหว่ ดังนั้นเป้าหมายหลักของพวกเขาก็เพื่อการสร้างผลกำไรและผลประโยชน์แก่ตนเอง ( บางโปรแกรมทางการค้าหรือเว็บไซต์ดังๆ มักจะให้รางวัลหรือสิ่งตอบแก่ผู้

---

[4] พีพีพี2555. “6 สุดยอดไวรัสและหนอนคอมพิวเตอร์อันตรายระดับโลก Dek-d.com”. (ออนไลน์). เข้าถึงได้จาก : http://www.dek-d.com/lifestyle/28367/, 2555.

ที่ตรวจพบความผิดพลาดของโปรแกรมหรือการค้นพบช่องโหว่ใหม่ของโปรแกรมที่พวกเขาผลิตขึ้น ) ส่วนเป้าหมายรอง ก็เพื่อให้เกิดการปรับปรุงระบบการรักษาความปลอดภัย อาจจะมีเรื่องของเงินรางวัลบ้างบางส่วนแต่เหนือกว่านั้นก็คือการได้รับการยอมรับว่าเป็นผู้ประสบความสำเร็จในการค้นพบสิ่งที่สามารถโจมตีช่องโหว่ที่พบได้นั่นเอง

2. พวกที่เป็นนักเจาะระบบจากภายนอกอย่างมืออาชีพ (Professional hacker-black hat ) เป็นคนที่ได้รับสิ่งตอบแทนจากการเขียนรหัสเพื่อการเจาะช่องโหว่ที่ค้นพบ หรือการเจาะเครือข่ายอย่างจริงจัง ยังคงอยู่ในพวกกลุ่มย่อยๆ สองกลุ่มข้างต้น ได้แก่ พวกนักล่าความผิดพลาดของโปรแกรม (bug) และ รหัสต่างๆ ที่ใช้โจมตีช่องโหว่ เป้าหมายหลักคือเรื่องของผลประโยชน์ต่างตอบแทนนั่นเอง

## ชุมชนการรักษาความปลอดภัยคอมพิวเตอร์ที่เกิดขึ้นโดยธรรมชาติ

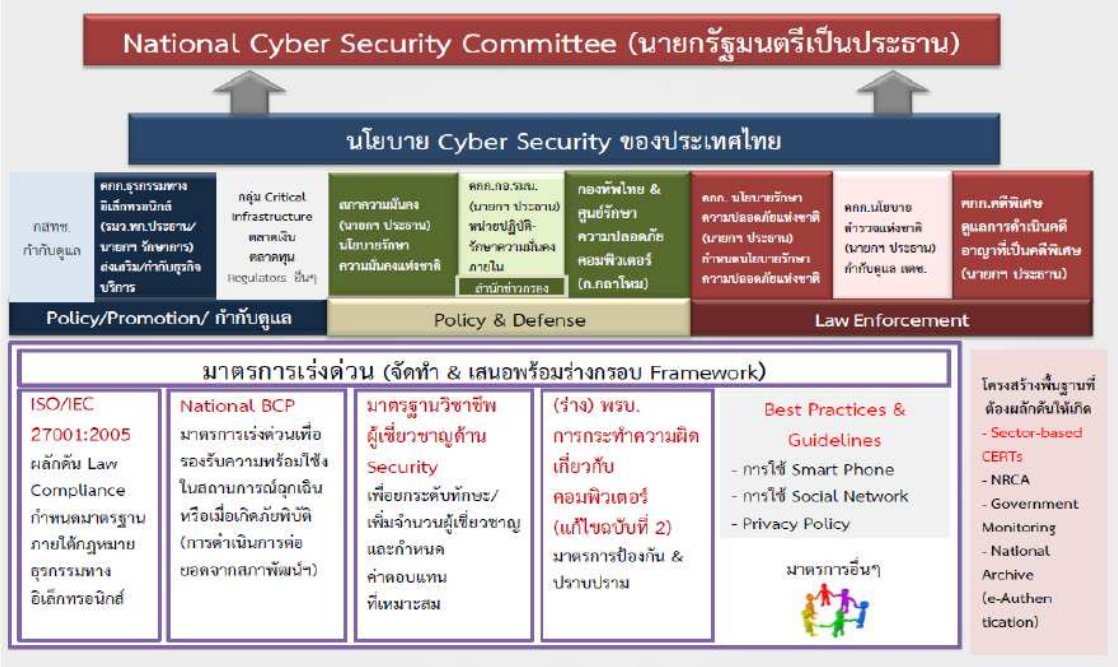
นอกจากที่กล่าวข้างต้นแล้ว สำหรับกลุ่มแฮ็กเกอร์ต่างๆ ก็ยังเกิดมีชุมนุมหรือกลุ่มสังคมด้านการรักษาความปลอดภัยคอมพิวเตอร์ที่เกิดขึ้นเองโดยตามธรรมชาติ โดยการสร้างชุมนุมหรือกลุ่มเหล่านี้ โดยเหล่าแฮ็กเกอร์และนักวิจัยที่มีปฏิสัมพันธ์พบปะพูดคุยกันเพื่อหารือเกี่ยวกับผลสิ่งที่ก่อให้เกิดประโยชน์ร่วมกันทางความปลอดภัยคอมพิวเตอร์โดยไม่คำนึงถึงว่าใครเป็นกลุ่มไหนหรืออยู่ในด้านมืดหรือด้านสว่าง แฮ็กเกอร์และนักวิจัยที่มีความเชี่ยวชาญในคนละด้านกัน เมื่อมีการแลกเปลี่ยนความคิดเห็นกันย่อมจะสร้างความเชี่ยวชาญขึ้น และการแลกเปลี่ยนเครื่องมือต่างๆ ก็เป็นการเพิ่มขีดความสามารถของพวกเขาในแต่ละส่วนที่ตนเองรับผิดชอบอีกด้วย ข้อมูลเกี่ยวกับการวิจัยการรักษาความปลอดภัยคอมพิวเตอร์ มีความเคลื่อนไหวช้า ไม่รวดเร็ว อีกทั้งยังจำกัดเฉพาะภายในวงของนักวิจัยที่ดีที่สุดและกลุ่มแฮ็กเกอร์นั้นๆ ดังนั้นในโลกรักษาความปลอดภัยคอมพิวเตอร์ การแลกเปลี่ยนกันทั้งสองฝ่ายย่อมเกิดกระแสความเคลื่อนไหวขึ้นได้อย่างแน่นอน

## ยุทธศาสตร์และแนวทางการรองรับสงครามไซเบอร์ที่มีอยู่เดิม

จากปัญหาและผลกระทบทางด้านไซเบอร์มีหลากหลาย ในส่วนของกองทัพไทยได้มีการวางยุทธศาสตร์ โดยการดำเนินการให้เป็นไปตามที่ภาครัฐ ได้มีการแต่งตั้ง คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ( National Cyber Security Committee : NCSC ) โดยมีนายกรัฐมนตรีเป็นประธาน และมีหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการฯ โดยมีหน้าที่หลักในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจาก

สถานการณ์ด้านภัยคุกคามในไซเบอร์ ที่กระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ตลอดจนติดตามและประเมินผลการปฏิบัติที่เกี่ยวข้อง กรอบการนโยบายและกรอบการทำงานของคณะกรรมการฯ แสดงตามแผนภาพที่ 3-1 ดังนี้

แผนภาพที่ 3-1 แผนภาพแสดงกรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ




## กรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

วิสัยทัศน์: ประเทศไทยมีความมั่นคงปลอดภัยด้านไซเบอร์เป็นที่เชื่อถือและยอมรับในระดับสากล

เป้าหมายหลัก:

1. สังคมมีวัฒนธรรมการตระหนักถึงความเสี่ยง (Risk-aware culture) จากการใช้งานบนโลกไซเบอร์ และประชาชนมีความรู้และทักษะในการใช้ประโยชน์จากโลกไซเบอร์ได้อย่างมั่นคงปลอดภัย

2. มีการกำกับดูแลการใช้งานบนโลกไซเบอร์ให้มีความมั่นคงปลอดภัย โดยคำนึงถึงสิทธิเสรีภาพของประชาชน

3. มีขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบได้อย่างมีประสิทธิภาพ (คน กระบวนการ เครื่องมือ) เพื่อรักษาเสถียรภาพทางเศรษฐกิจ ความมั่นคงแห่งชาติ และ คุณภาพชีวิตของประชาชน

4. มีการคุ้มครองข้อมูลส่วนบุคคล (Privacy) และข้อมูลแสดงตัวตน (Identity) และมีการรักษาความมั่นคงปลอดภัยในการทางธุรกรรมทางอิเล็กทรอนิกส์ในทุกภาคส่วน

5. มีความร่วมมือทั้งระหว่างองค์กรภายในประเทศ และองค์กรระหว่างประเทศเพื่อเสริมศักยภาพการรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบาย/ยุทธศาสตร์:

1. วางโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีความชัดเจนใน บทบาทหน้าที่ ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และประสานงานกับผู้ที่รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานอื่นๆ การดำเนินการเรื่องตรวจสอบและประเมิน การประเมินความเสี่ยงของระบบสารสนเทศใน ระดับระเทศ การพัฒนาบุคลากร การวิจัยและพัฒนา และการเตรียมความพร้อมในการรักษา ความมั่นคงปลอดภัยไซเบอร์ โดยมีกลไกประสานเชื่อมโยงกับคณะกรรมการนโยบายระดับชาติที่ เกี่ยวข้อง (Governance and Organizational Structure)

2. สร้างความพร้อมเชิงรับและเชิงรุกในการรับมือภัยคุกคาม (Cybersecurity Emergency Readiness)

3. ปกป้องโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (National Critical Information Infrastructure Readiness)

4. ทำงานร่วมกันระหว่างภาครัฐและเอกชนในการสร้างขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบได้อย่างมีประสิทธิภาพ (คน กระบวนการ เครื่องมือ) เพื่อรักษา เสถียรภาพทางเศรษฐกิจ ความมั่นคงแห่งชาติ และคุณภาพชีวิตของประชาชน (Public-Private Partnership)

5. พัฒนาบุคลากรในบทบาทต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (ประชาชน ผู้เชี่ยวชาญเฉพาะทาง และผู้รักษากฎหมาย) และสร้างวัฒนธรรมการรักษาความมั่นคงปลอดภัย ไซเบอร์ (Capacity& Capability Building)

6. ปรับปรุงกฎหมายให้ทันสมัย บังคับใช้ได้ มีแนวปฏิบัติตามกฎหมายที่ชัดเจน และสอดคล้องกับ หลักกฎหมาย/แนวปฏิบัติสากล (Legal Measures)

7. มีกลไกสร้างความเป็นเลิศด้านการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ให้ ประเทศให้พึ่งพาตัวเองได้อย่างยั่งยืน (Research and Development)

8. เป็นพันธมิตรที่น่าเชื่อถือในเครือข่ายการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ (International Cooperation)

การดำเนินการตามยุทธศาสตร์ดังกล่าว ตอนนี้ยังไม่เห็นผลออกมาเป็นรูปธรรมชัดเจนมากนักเนื่องจากมีปัจจัยในหลายๆ ด้านที่ส่งผลกระทบให้เกิดการหยุดนิ่งของกระบวนการ แต่ก็ถือว่าเป็นจุดเริ่มต้นที่ดีในการที่จะมีการพัฒนาในเรื่องดังกล่าว เพื่อให้เกิดการรองรับสงครามไซเบอร์ที่จะเกิดขึ้นในอนาคต สำหรับการดำเนินการตามยุทธศาสตร์ที่ผ่านมา สิ่งที่พอจะเห็นหรือจับต้องได้ก็จะขอกล่าวถึงตั้งแต่ในระดับกระทรวงและหน่วยงานที่เกี่ยวข้องไปจนถึงระดับกองทัพไทย

## กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ตั้ง ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ ( Cyber Security Operation Center : CSOC ) เมื่อปี 2553 โดยมุ่งเน้นการดำเนินการติดตามเฝ้าระวังตรวจสอบวิเคราะห์เว็บไซต์ และข้อมูลอินเทอร์เน็ตที่ไม่เหมาะสม หรือผิดกฎหมายต่างๆ โดยเฉพาะเว็บหมิ่นสถาบัน จากนั้นยังมีบทบาทในการเป็นส่วนหนึ่งของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ( National Cyber Security Committee : NCSC ) อีกด้วย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน )[5] (Electronic Transactions Development Agency (Public Organization) หรือ สพธอ. (ETDA) ได้จัดตั้งขึ้นเมื่อ 22 กุมภาพันธ์ พ.ศ.2554 ภายใต้การกำกับของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่หลักคือ เพื่อพัฒนาส่งเสริม และสนับสนุนการทำธุรกรรมหรือการให้บริการทางอิเล็กทรอนิกส์ทั้งในภาคธุรกิจและในภาครัฐ ดังนั้น ภายใต้วัตถุประสงค์การจัดตั้ง สพธอ.จึง กำหนดให้ สพธอ.มีบทบาทสำคัญในการศึกษาวิจัยทางวิชาการ และให้ข้อเสนอแนะเกี่ยวกับนโยบาย กฎหมาย มาตรฐาน ความมั่นคงปลอดภัย และทำหน้าที่สำรวจความต้องการเกี่ยวกับโครงสร้างพื้นฐานที่ภาคธุรกิจหรือภาครัฐต้องการ ซึ่งเอื้อต่อการทำ ธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งการให้บริการเกี่ยวกับโครงสร้างพื้นฐานที่จำเป็นสำหรับการทำธุรกรรมทางออนไลน์ ตลอดจนพัฒนาบุคลากร ที่มีทักษะสูงด้านความมั่นคงปลอดภัย เพื่อให้มีจำนวนเพียงพอต่อความต้องการของภาคธุรกิจและภาครัฐ และเพื่อให้เกิดความ

---

[5] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (ออนไลน์). เข้าถึงได้จาก : http://www.etda.or.th/, 2557.

มั่นใจว่า บุคลากรที่มีความรู้ ความเชี่ยวชาญด้านความมั่นคงปลอดภัยนั้น จะสามารถประยุกต์ใช้ความรู้ ความเชี่ยวชาญของตน ช่วยลดความเสี่ยงจากภัยคุกคามใด ๆ ทางออนไลน์ ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสียหายและทำลายความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่นับวันจะรุนแรงเพิ่มมากขึ้นทุกขณะ หากแต่ประเทศไทยก็ยังคงมีข้อจำกัดอย่างมาก ในการผลิตผู้เชี่ยวชาญด้านดังกล่าวเพื่อให้ทันและเพียงพอกับความต้องการของประเทศ

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์[6] เกิดจากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551 กำหนดให้มี คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกอบด้วยรัฐมนตรีว่าการกระทรวง เทคโนโลยีสารสนเทศและการสื่อสารเป็นประธานกรรมการ ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นรองประธานกรรมการและกรรมการอื่นอีกจำนวน 12 คน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิ ที่ได้รับการสรรหาจากภาครัฐและภาคเอกชนใน 6 ด้าน คือ การเงิน การพาณิชย์อิเล็กทรอนิกส์ นิติศาสตร์ วิทยาการคอมพิวเตอร์ วิทยาศาสตร์หรือวิศวกรรมศาสตร์ สังคมศาสตร์ ทั้งนี้ ผู้ทรงคุณวุฒิคนหนึ่งของแต่ละด้านต้องมาจากภาคเอกชน มีวาระการดำรงตำแหน่งคราวละ 3 ปี โดยมีหัวหน้าสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นกรรมการและเลขานุการ ทั้งนี้คณะรัฐมนตรีได้มีมติแต่งตั้งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ชุด แรกเมื่อวันที่ 23 กันยายน 2546

ปัจจุบันสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทำหน้าที่เป็นหน่วยงานที่รองรับภารกิจของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยมีนางสมใจ ประเสริฐจีรังกุล ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ทำหน้าที่เป็นกรรมการและเลขานุการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และคณะรัฐมนตรีได้มีการแต่งตั้งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ชุดปัจจุบัน (ชุดที่ 3) เมื่อวันที่ 7 มกราคม 2553 แทนคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ชุดที่ 2 ที่หมดวาระไป

ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้กำหนดให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีอำนาจหน้าที่ดังต่อไปนี้

1.เสนอแนะต่อคณะรัฐมนตรีเพื่อวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนแก้ไขปัญหา และอุปสรรคที่เกี่ยวข้อง (มาตรา 37)

2.ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

3.เสนอแนะหรือให้คำปรึกษาต่อรัฐมนตรี (รัฐมนตรีว่าการกระทรวงเทคโนโลยี

---

[6] คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (ออนไลน์). เข้าถึงได้จาก : http://www.etcommission.go.th/, 2557.

สารสนเทศและการสื่อสาร) เพื่อการตราพระราชกฤษฎีกาตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (มาตรา37) ทั้งนี้ตามบทบัญญัติแห่งพระราช บัญญัติฯ ดังกล่าวให้อำนาจในการตราพระราชกฤษฎีกา จำนวน 4 ฉบับ กล่าวคือ

3.1 พระราชกฤษฎีกาตามความในมาตรา 3 กำหนดประเภทธุรกรรมที่มิให้ใช้วิธีการทางอิเล็กทรอนิกส์

3.2 พระราชกฤษฎีกาตามความในมาตรา 25 กำหนดวิธีการแบบปลอดภัย

3.3 พระราชกฤษฎีกาตามความในมาตรา 32 กำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็น กิจการที่ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาต

3.4 พระราชกฤษฎีกาตามความในมาตรา 35 กำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ

4.ออกระเบียบหรือประกาศเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เพื่อให้เป็นไปตามพระราชบัญญัติ หรือตามพระราชกฤษฎีกาที่ออกตามพระราชบัญญัติ (มาตรา37)

5.ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัติฉบับนี้ หรือตามกฎหมายอื่น (มาตรา37)

6.แต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างหนึ่งอย่างใดแทนคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 42)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย[7] (Thailand Computer Emergency Response Team) หรือ ThaiCERT คณะรัฐมนตรีได้มีมติให้จัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และได้มีการโอนภารกิจของศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย หรือ ไทยเซิร์ต จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี มายัง สพธอ. เพื่อให้การดำเนินงานของ สพธอ. ด้านการสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์มีความเข้มแข็ง

---

[7] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (ออนไลน์). เข้าถึงได้จาก : http://www.etda.or.th/etda_website/content/background-of-thaicert.html, 2557.

ไทยเซิร์ตได้เปิดให้บริการอย่างเต็มรูปแบบภายใต้ สพธอ. มาตั้งแต่วันที่ 1 กรกฎาคม 2554 และได้ปรับเปลี่ยนชื่อทางการของไทยเซิร์ตเป็น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) โดยมีวิสัยทัศน์ให้สังคมออนไลน์มีความมั่นคงปลอดภัย เกิดความเชื่อมั่นกับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ พันธกิจของไทยเซิร์ต มุ่งเน้นการประสานงานกับหน่วยงานในเครือข่าย และหน่วยงานที่เกี่ยวข้องในการดำเนินการแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับแจ้ง นอกจากนี้ไทยเซิร์ตยังมีพันธกิจเชิงรุกที่ให้ความสำคัญกับการพัฒนาทรัพยากรบุคคลเพื่อเพิ่มขีดความสามารถด้านการรักษาความมั่นคงปลอดภัย

เนื่องจากงานของไทยเซิร์ตมีลักษณะเป็นการประสานงานกับหน่วยงานต่างๆไทยเซิร์ตจึงมุ่งมั่นที่จะสร้างความร่วมมือกับหน่วยงานทุกประเภททั้งในและต่างประเทศในการแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร เช่น ผู้ให้บริการอินเทอร์เน็ต และ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ไทยเซิร์ตสร้างความร่วมมือระหว่างประเทศผ่านเวที FIRST (Forum of ) สำหรับความร่วมมือกับประเทศทั่วโลก และเวที APCERT (Asia Pacific CERT) สำหรับความร่วมมือกับประเทศในภาคพื้นเอเชียแปซิฟิก

ด้านการพัฒนาทรัพยากรบุคคล ไทยเซิร์ตให้ความสำคัญกับการเผยแพร่ความรู้และข้อมูลข่าวสารเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการสร้างภูมิคุ้มกันเบื้องต้นทางด้านไอที และจัดอบรมสัมมนาให้กับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์เฉพาะกลุ่มที่มีความต้องการข้อมูลข่าวสารเป็นการเฉพาะ เช่น กลุ่มธุรกิจการเงินการธนาคาร หรือกลุ่มสถาบันวิจัยและสถาบันการศึกษา นอกจากนี้เพื่อให้เกิดความเข้าใจและได้ลงมือปฏิบัติ ไทยเซิร์ตยังจัดและร่วมในกิจกรรมซักซ้อมการรับมือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารกับหน่วยงาน ทั้งในประเทศและต่างประเทศอีกด้วย

1. บริการของไทยเซิร์ต ในการสนับสนุนให้สังคมออนไลน์มีความมั่นคงปลอดภัยและเกิดความเชื่อมั่นกับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ ไทยเซิร์ต ให้บริการหลัก คือ บริการประสานงานแก้ไขภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร บริการข้อมูลข่าวสารความมั่นคงปลอดภัยสารสนเทศ และบริการวิชาการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

2. บริการประสานงานแก้ไขภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ปัจจุบันไทยเซิร์ตให้บริการประสานงานแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์และทางอีเมลแก่บุคคลทั่วไป สถาบันการศึกษาและสถาบันวิจัย หน่วยงานภาครัฐและเอกชนทั่วโลก เมื่อได้รับแจ้งเหตุผู้เชี่ยวชาญของไทยเซิร์ตจะตรวจสอบข้อมูลที่ได้รับแจ้งเพื่อยืนยันว่าเหตุภัยคุกคามที่ได้รับแจ้งได้เกิดขึ้นและมีอยู่จริง แล้วจึงวิเคราะห์ข้อมูลต่อเพื่อหา

หน่วยงานที่เป็นต้นเหตุของปัญหา และดำเนินการประสานงานไปยังหน่วยงานดังกล่าวเพื่อให้ดำเนินการแก้ไขปัญหา ไทยเซิร์ตมีระบบการติดตามความคืบหน้าของการจัดการปัญหาภัยคุกคามและได้กำหนดมาตรฐานการให้บริการไว้คือ ไทยเซิร์ตจะดำเนินการแจ้งหน่วยงานที่เกี่ยวข้องเพื่อแก้ปัญหาที่ได้รับแจ้งและรายงานสถานะการดำเนินงานภายใน 2 วันทำการ มีการติดตามผลการดำเนินงานทุก 3 วันทำการ

3. บริการข้อมูลข่าวสารความมั่นคงปลอดภัยสารสนเทศไทยเซิร์ตอยู่ในเครือข่ายความร่วมมือของหน่วยงานที่มีบทบาทในการตอบสนองต่อการแจ้งเหตุภัยคุกคาม (Computer Security Incident Response Team: CSIRT หรือ Computer Emergency Response Team: CERT) ซึ่งมีภารกิจในการแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับแจ้งจากหน่วยงาน CSIRT อื่นๆในเครือข่ายหรือที่ตรวจพบกับผู้ใช้งานภายในประเทศไทยเพื่อสร้างความตระหนักและความพร้อมในการรับมือต่อภัยคุกคามที่เกิดขึ้น โดยผู้เชี่ยวชาญของไทยเซิร์ตจะวิเคราะห์ข้อมูลภัยคุกคามที่มีผลกระทบสูงกับผู้ใช้งาน พร้อมเสนอแนะข้อควรปฏิบัติในการรับมือแก้ไขหรือป้องกันภัยคุกคามในบทความแจ้งเตือนภัยคุกคามของไทยเซิร์ต นอกจากนั้น ไทยเซิร์ตจัดทำข้อมูลเชิงสถิติของภัยคุกคามที่รายงานมาที่ไทยเซิร์ตเผยแพร่บนเว็บไซต์ไทยเซิร์ตเป็นรายเดือนเพื่อใช้วิเคราะห์แนวโน้มของภัยคุกคามที่เกิดภายในประเทศไทย

4. บริการวิชาการในการรักษาความมั่นคงปลอดภัยสารสนเทศไทยเซิร์ตมีผู้เชี่ยวชาญที่มีศักยภาพและความรู้ที่สามารถให้บริการวิชาการในการรักษาความมั่นคงปลอดภัยสารสนเทศกับหน่วยงานทั้งภายในและต่างประเทศ ไทยเซิร์ตให้บริการกับหน่วยงานภายในประเทศในส่วนของการให้คำปรึกษาในการวิเคราะห์ข้อมูลภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร การจัดทำแผนและนโยบายทางด้านเทคโนโลยีสารสนเทศ เพื่อให้สอดคล้องกับมาตรฐานสากลทางด้านเทคโนโลยีสารสนเทศและสอดคล้องกับข้อกำหนดของกฎหมาย จัดฝึกอบรมสัมมนา เพื่อสร้างความตระหนักหรือเสริมสร้างศักยภาพของบุคลากรของหน่วยงานให้สามารถป้องกันและแก้ไขภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารจัดการซักซ้อมรับมือภัยคุกคามเพื่อเสริมทักษะและสร้างความพร้อมในการรับมือภัยคุกคามของหน่วยงาน รวมถึงการสนับสนุนวิทยากรในการบรรยาย เพื่อสร้างความตระหนักและให้ความรู้กับหน่วยงานทั้งในและต่างประเทศ

สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ[8] (Thailand Information Security Association - TISA) เป็นสมาคมหลัก(ไม่แสวงหากำไร)ของกลุ่มนักวิชาชีพด้านความมั่นคงปลอดภัย

---

[8] สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ. (ออนไลน์). เข้าถึงได้จาก : http://www.tisa.or.th/, 2557.

สารสนเทศในประเทศไทย มีภารกิจในการพัฒนากระบวนการและบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศให้ได้มาตรฐานเป็นที่ยอมรับในระดับสากล

## กระทรวงกลาโหม

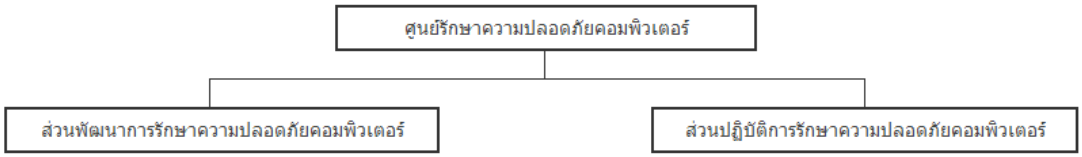
การดำเนินการทางสงครามไซเบอร์ของกระทรวงกลาโหม มุมมองทางด้านไซเบอร์นั้นได้กำหนดภัยคุกคามไว้ 2 ด้าน ได้แก่ ด้านความมั่นคงของประเทศ และด้านการทหาร สำหรับด้านความมั่นคงของประเทศนั้น จะให้ความสำคัญกับเรื่องการโจมตีทางด้านไซเบอร์ในภาพรวมทั้งหมด ไม่ว่าจะเป็นการโจมตีเว็บไซต์ ไปจนกระทั่งการโจมตีในส่วนสาธารณูปโภคหลักของประเทศ สำหรับด้านการทหาร คงหนีไม่พ้นในเรื่องของสงครามไซเบอร์ที่เป็นหัวใจหลักในด้านดังกล่าว ความพร้อมด้านไซเบอร์ของกลาโหมนั้น นอกจากยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม พ.ศ.2555 แล้ว พร้อมในเรื่องของความสามารถในการป้องกันตนเอง เป็นสิ่งที่กลาโหมให้ความสำคัญเป็นอันดับแรก สำหรับยุทธศาสตร์การป้องประเทศ กห. พ.ศ.2555 ได้กำหนดให้กลาโหมต้องมีขีดความสามารถสงครามไซเบอร์ การปฏิบัติการสงครามสารสนเทศ สงครามอิเล็กทรอนิกส์ สงครามจิตวิทยา รวมทั้งสามารถโจมตีฝ่ายตรงข้ามได้ด้วย นับว่าได้ว่าเป็นความพร้อมในด้านนโยบายและยุทธศาสตร์สำหรับการรองรับสงครามไซเบอร์นั่นเอง

สำหรับหน่วยงานในระดับกลาโหม ได้แก่ สำนักงานปลัดกระทรวงกลาโหม ( สป. ) มีหน่วยขึ้นตรงที่ชื่อว่า กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (ศรค.ทสอ.กห.) ภายในกรมฯ ดังกล่าวได้มีการจัดตั้ง ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ (ศรค.) Defence Information and Space Technology Department Computer Emergency Response Team (DISTCERT) โดยมีหน้าที่พิจารณา เสนอความเห็น วางแผน อำนวยการ ประสานงาน กำกับการและดำเนินการเกี่ยวกับการรักษาความปลอดภัยคอมพิวเตอร์ และการสงครามสารสนเทศของกระทรวงกลาโหม รวมทั้งปฏิบัติงานอื่นตามที่ได้รับมอบหมาย โดยมีผู้อำนวยการศูนย์รักษาความปลอดภัยคอมพิวเตอร์[9] เป็นผู้บังคับบัญชารับผิดชอบ มีโครงสร้างตามแผนภาพที่ 3-2 ดังนี้

---

[9] ศูนย์รักษาความปลอดภัยคอมพิวเตอร์. (ออนไลน์). เข้าถึงได้จาก : http://csc.mod.go.th/about, 2557.

แผนภาพที่ 3-2 แสดงผังการจัดศูนย์รักษาความปลอดภัยคอมพิวเตอร์

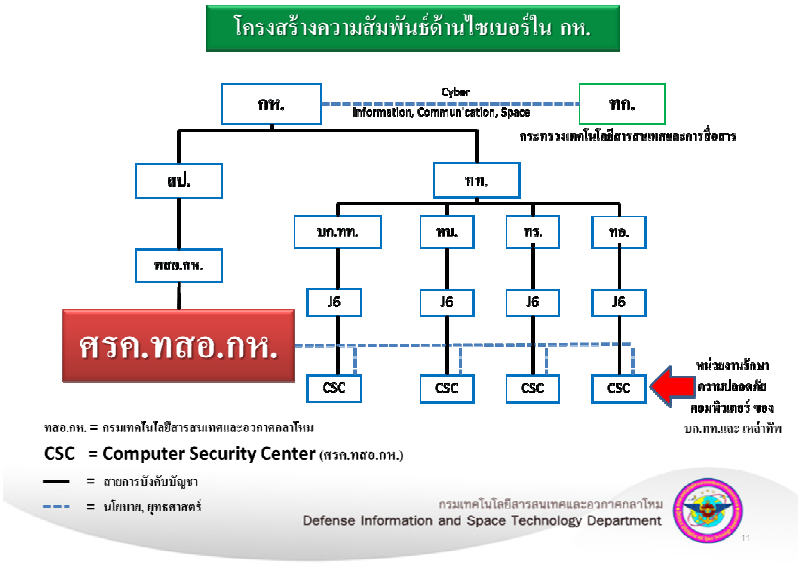



หน่วยงานข้างต้นมีส่วนผลักดันกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ( ทก. )ให้เกิดการจัดทำแผนแม่บทความมั่งคงปลอดภัยไซเบอร์แห่งชาติ ร่วมทั้งการสร้างความตระหนักและเครือข่ายความร่วมมือกับหน่วยงานภาครัฐและเอกชนถึงภัยคุกคามจากไซเบอร์อีกด้วย

แต่ผลที่ตามทำให้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มีแนวทางในการจัดแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยแห่งชาติโดยมี นรม. เป็นประธาน เพื่อจัดทำ นโยบายและแผนแม่บทฯ อีกทั้งยังมีการจัดสัมมนาความมั่งคงปลอดภัยไซเบอร์แห่งชาติปีละ 1 ครั้ง รวมถึง สร้างประชาคมความมั่งคงปลอดภัยไซเบอร์และมีการจัดประชุม 2 เดือน/ครั้ง อย่างต่อเนื่องอีกด้วย นับว่าหน่วยงานนี้ สร้างความพร้อมในการรองรับสงครามไซเบอร์ได้อย่างดีเยี่ยม

นอกจากนั้นยังมีส่วนการกำหนดโครงสร้างความสัมพันธ์ด้านไซเบอร์ใน กห. เพื่อให้เกิดการประสานการปฏิบัติระหว่างหน่วยงานในกองทัพไทย อย่างเป็นรูปธรรมและเป็นจุดเริ่มต้นของการบูรณาการทางด้านไซเบอร์ของกองทัพไทยอีกด้วย ดังแสดงตามแผนภาพที่ 3-3 ดังนี้

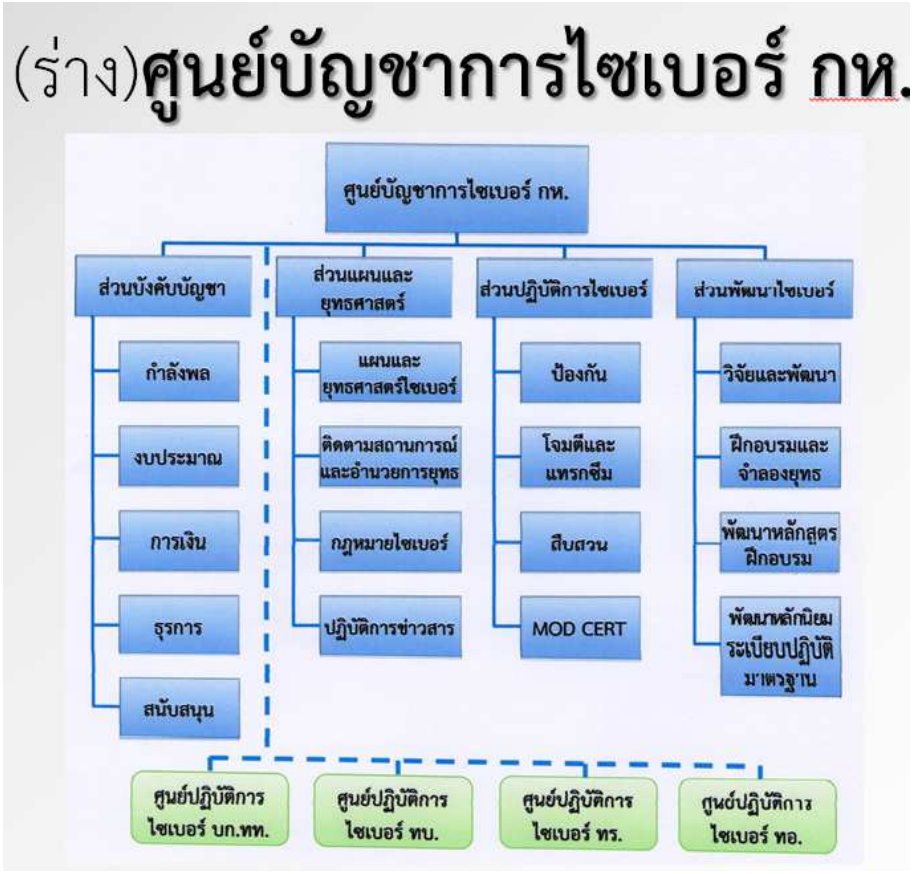
แผนภาพที่ 3-3 แสดงโครงสร้างความสัมพันธ์ด้านไซเบอร์ใน กห.



ภายใต้นโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ นายกรัฐมนตรี/รัฐมนตรีว่าการกระทรวงกลาโหม ได้อนุมัติหลักการให้จัดตั้ง ศูนย์ปฏิบัติการไซเบอร์กลาโหม ขึ้นโดยกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ เตรียมจัดตั้งหน่วยงานด้านไซเบอร์โดยตรง ( Cyber Command ) เพื่อขึ้นมารองรับการปฏิบัติงานความมั่งคงปลอดภัยของประเทศจากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ โดยศูนย์ปฏิบัติการไซเบอร์กลาโหม ( Cyber Operations Center ) จะเป็นแกนหลักในด้านการพัฒนาบุคลากรด้านนี้ให้กับกำลังพลสังกัดกระทรวงกลาโหม โดยจะมีห้องปฏิบัติการสำหรับการฝึกปฏิบัติด้านสงครามไซเบอร์ ( Cyber Warfare ) รวมถึงการสร้างภาคี เครือข่าย ประชาคม ทั้งภาครัฐและเอกชน เพื่อเสริมสร้างศักยภาพของประเทศด้านไซเบอร์ในการรับมือกับภัยคุกคามด้านไซเบอร์

ถึงแม้ว่าจะมีการอนุมัติให้ดำเนินการในเรื่องขอศูนย์ปฏิบัติการไซเบอร์กลาโหมแล้ว แต่โครงสร้างก็ยังอยู่ในระหว่างการดำเนินการ ภาพโครงร่างบางส่วนของศูนย์ปฏิบัติการไซเบอร์กลาโหม ดังกล่าวมีแสดงตามแผนภาพที่ 3-4 ดังนี้

แผนภาพที่ 3-4 แสดงร่างโครงสร้างศูนย์บัญชาการไซเบอร์ กห.



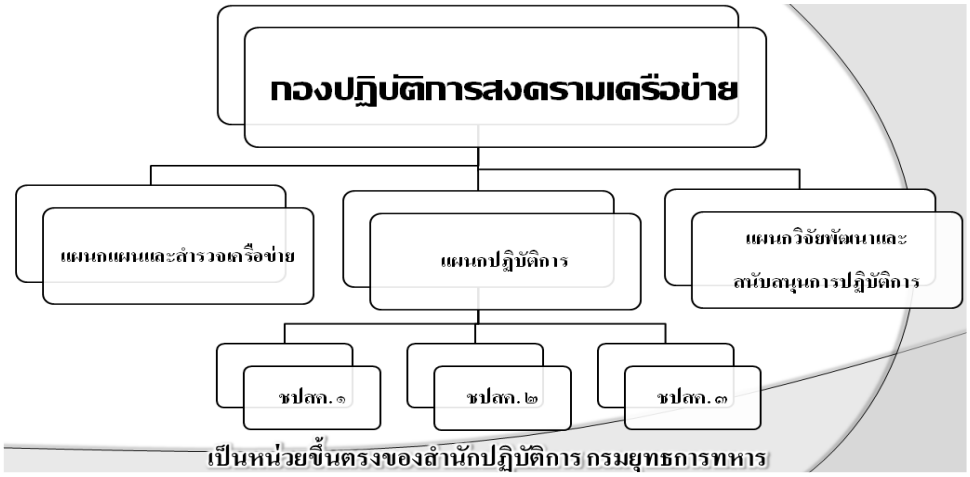
นอกจากการรองรับที่มุ่งเน้นไปในด้านการปรับโครงสร้างแล้ว ในด้านการอบรมหรือด้านต่างๆ เพื่อการเตรียมความพร้อมและการสร้างความตะหนักต่อบุคคลากรในด้านดังกล่าว ยังมีกิจกรรมที่สร้างเสริมในเรื่องดังกล่าวที่สำคัญได้แก่ ประชุมคณะทำงานคณะทำงานป้องกันไซเบอร์ร่วมไทย-สหรัฐ ประจำปี พ.ศ. 2557 , ICDW ( International Cyber Defense Workshop ) , การสัมมนานานาชาติ เรื่อง “สงครามไซเบอร์ สิ่งท้าทายความร่วมมือในอนาคตของอาเซียน” (Cyber Warfare : A Challenge of ASEAN Cooperation in Future) เป็นต้น

## กองบัญชาการกองทัพไทย

การรองรับสงครามไซเบอร์ของกองบัญชาการกองทัพไทย คงเช่นเดียวกับทางด้านของกลาโหม ได้มีความพยายามที่จะจัดตั้งหน่วยงานที่รับผิดชอบทางด้านไซเบอร์โดยตรง ตามร่างมติสภากลาโหม ครั้งที่ 5/ 2556 เรื่อง ภัยคุกคามด้านไซเบอร์ ได้กำหนดให้ บก.ทท. นำข้อมูลไปศึกษาและพิจารณาแนวทางการดำเนินการจัดตั้งหน่วยไซเบอร์ ขึ้นมารับผิดชอบภัยคุกคามด้านไซเบอร์เป็นการเฉพาะ โดยใช้การปรับเกลี่ยอัตราที่มีอยู่ให้เกิดประโยชน์สูงสุด

แต่เดิมหน่วยงานที่รับผิดชอบ หรือเกี่ยวข้องกับทางด้านไซเบอร์ ได้แก่ กองรักษาความปลอดภัยสารสนเทศ (กรส.) ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) กรมการสื่อสารทหาร (สส.ทหาร) แต่เนื่องจาก กองรักษาความปลอดภัยสารสนเทศ และหน่วยงานต่างๆ ของศูนย์เทคโนโลยีสารสนเทศทหาร ได้ปฏิบัติงานด้านเชิงรับ ในการป้องกันระบบเครือข่ายเทคโนโลยีสารสนเทศ ของ บก.ทท. เป็นหลัก ทำให้จำเป็นต้องมีหน่วยงานที่เป็นการปฏิบัติการเชิงรุกขึ้น จึงได้มีการเสนอโครงสร้างของหน่วยงานใหม่ที่เรียกว่า “กองปฏิบัติการสงครามเครือข่าย” มีร่างของผังการจัดตามแผนภาพที่ 3-5 ดังต่อไปนี้

แผนภาพที่ 3-5 แสดงผังกร่างการจัดกองปฏิบัติการสงครามเครือข่าย กรมยุทธการทหาร บก.ทท.



กองที่เกิดขึ้นใหม่ดังกล่าวมีภารกิจ มีหน้าที่พิจารณาเสนอความเห็น นโยบาย วางแผน อำนวยการ ประสานงาน บูรณาการ กำกับดูแล และปฏิบัติการสงครามเครือข่าย ทั้งเชิงรับ และเชิงรุก

สำหรับขอบเขตความรับผิดชอบและหน้าที่ที่สำคัญ ได้แก่ 1. พิจารณาเสนอความเห็น นโยบาย วางแผน อำนวยการ ประสานงาน และกำกับดูแล การปฏิบัติ การต่างๆ ที่เกี่ยวข้องกับสงครามเครือข่าย ทั้งเชิงรับ และเชิงรุก 2. ดำเนินการปฏิบัติการสงครามเครือข่ายคอมพิวเตอร์ ได้ทั้งเชิงรับ (Defense) และเชิงรุก (Offense) 3.ดำเนินการบูรณาการ การปฏิบัติงานระหว่างหน่วยงานหรือบุคลากรต่างๆ ที่มีความเชี่ยวชาญ และ มีเครื่องมือหรือยุทโธปกรณ์ต่างๆ ที่เกี่ยวข้องกับการปฏิบัติการสงครามเครือข่ายในทุกมิติ

ทางด้านหลักนิยม ได้มีการร่างหลักนิยมกองทัพไทยสำหรับการปฏิบัติการข่าวสารร่วม เล่มนี้ จัดทำขึ้นโดยคณะกรรมการจัดทำหลักนิยมการปฏิบัติการข่าวสาร ซึ่งจัดตั้งขึ้นตามคำสั่ง บก. ทหารสูงสุด (เฉพาะ) ที่ 1392/50 ลง 14 ก.พ.50 โดยแปลจากหลักนิยมของประเทศสหรัฐอเมริกา (Joint Publication 3-13, Information Operations ฉบับเดือนกุมภาพันธ์ ค.ศ.2006) ถึงแม้ว่าจะเป็นความพยายามที่จะศึกษาแนวทางจากประเทศสหรัฐฯ ก็ถือว่าเป็นความพยายามที่จะให้กองทัพไทย มีความเข้าใจในเรื่องที่เกี่ยวข้องกับไซเบอร์ หลักนิยมดังกล่าว มีเนื้อหาบางส่วนกล่าวถึง การปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations: CNO) เพื่อสนับสนุนการปฏิบัติการข่าวสาร ซึ่งการปฏิบัติการเครือข่าวคอมพิวเตอร์ดังกล่าว ก็ถูกนำมาใช้ในเรื่องของสงครามไซเบอร์ได้เช่นเดียวกัน

ในด้านการศึกษา ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ ได้มีการจัดประชุมเชิงสัมมนาทางวิชาการ ศูนย์อาเซียนศึกษา ครั้งที่ 1/2557 เรื่อง “ความร่วมมือของอาเซียนกับการจัดตั้งศูนย์แลกเปลี่ยนข้อมูล และแจ้งเตือนภัยไซเบอร์” ถือเป็นครั้งแรกที่หน่วยงานทางด้านวิชาการทหารชั้นสูง ให้ความสำคัญในด้านของสงครามไซเบอร์อย่างจริงจัง

## กองทัพบก

สำหรับกองทัพบกนั้น กรมยุทธการทหารบก ถือว่าเป็นหน่วยงานที่เป็นฝ่ายอำนวยการหลักของเรื่องสงครามไซเบอร์ แต่บทบาทที่เป็นภาพรวมโดยมากแล้วจะเน้นในด้านการปฏิบัติการข่าวสาร ทำให้ในด้านของสงครามไซเบอร์ ยังขาดหน่วยงานที่รับผิดชอบอย่างจริงจัง ถึงแม้ว่าการปฏิบัติการข่าวสาร จะมีเรื่องของการปฏิบัติการเครือข่ายคอมพิวเตอร์สนับสนุนการปฏิบัติการข่าวสารเป็นส่วนในกระบวนการปฏิบัติก็ตาม ก็ยังมองเห็นแนวทางและความรับผิดชอบไม่เด่นชัดมากนัก ทำให้กองทัพบกต้องมีนโยบายและอนุมัติหลักการให้ ศูนย์เทคโนโลยีทางทหาร ( ศทท. ) ดำเนินการปรับปรุงภารกิจและโครงสร้างการจัดหน่วย โดยเพิ่มเติมภารกิจด้านการปฏิบัติการสงครามไซเบอร์

และปรับสายการบังคับบัญชาจากเดิม เป็นหน่วยขึ้นตรงกรมการทหารสื่อสาร มาเป็นหน่วยขึ้นตรงกองทัพบก ( นขต.ทบ. ) เพื่อเตรียมรองรับการปฏิบัติงานความมั่งคงปลอดภัยด้านไซเบอร์ ที่ส่งผลกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ โดยเฉพาะความมั่นคงทางการทหาร และการรักษาความสงบเรียบร้อยภายในประเทศ รวมถึงการปฏิบัติการที่ประสานสอดคล้องกับกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพต่างๆ ตลอดจนรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ( Network Centric Operations ; NCO ) โดยแนวความคิดเบื้องต้นในการเตรียมการดำเนินการพัฒนาปรับปรุงภารกิจ โครงสร้างการจัดหน่วย และการพัฒนาศักยภาพของกำลังพล ให้มีคุณวุฒิการศึกษา คุณลักษณะ ขีดความสามารถ ประสบการณ์ และความถนัดเฉพาะด้านที่สอดคล้องกับตำแหน่งหน้าที่การงาน ( put the right to the right job ) เพื่อให้การปฏิบัติภารกิจที่ได้รับมอบเป็นไปอย่างมีประสิทธิภาพ โดยเน้นการปรับเกลี่ย โยกย้าย และการบรรจุกำลังพลด้านปฏิบัติการเป็นหลักมากกว่างานทางธุรการ ในสัดส่วนไม่น้อยกว่า 70 : 30 สำหรับในด้านการปรับปรุงโครงสร้างการจัดหน่วย โดยแปรสภาพ กองการสงครามสารสนเทศ เป็น กองปฏิบัติการไซเบอร์ ( Cyber Operations Division ) ซึ่งเป็นหน่วยปฏิบัติการด้านไซเบอร์เชิงรุก ( Cyber Offensive Operations ) ดำเนินการด้านการตรวจสอบสภาพแวดล้อมของภัยคุกคาม การวางแผนควบคุมการปฏิบัติ 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 เฝ้าระวัง 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 ทั้งนี้กองทัพบกจะต้องเร่งดำเนินการแปลงนโยบายไปสู่การปฏิบัติอย่างเป็นรูปธรรมโดยเร็ว โดยเฉพาะการเร่งดำเนินการด้านการปรับปรุงหรือการปฏิรูปโครงสร้างองค์กร ( Organization Reform ) การบรรจุกำลังพลที่มีความเชี่ยวชาญเฉพาะด้าน ( Specialist ) และการพัฒนากำลังพล ( Human Resource Development ) ให้มีขีดความสามารถในด้านไซเบอร์ เพื่อรองรับการปฏิบัติงานความมั่งคงปลอดภัยด้านไซเบอร์ของชาติ ( 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

ทางการด้านหลักนิยมของกองทัพบก ได้มีการจัดทำ “คู่มือปฏิบัติการข่าวสารกองทัพบก” ( Information Operation) ซึ่งเป็นไปตาม ความริเริ่มของ เสธ.ทบ. (พล.อ.พงษ์เทพ เทศประทีป) ในขณะนั้น และได้รับการจัดทำขึ้นโดยคณะทำงานจัดทำร่างหลักนิยมการปฏิบัติการข่าวสารของกองทัพบกโดยได้รับการพิจารณาความเหมาะสมในขั้นต้นแล้วจากผู้แทนหน่วยที่เข้าร่วม การสัมมนาเรื่อง “แนวความคิดในการปฏิบัติการข่าวสารของ ทบ.” ซึ่งจัดขึ้น ณ ยก.ทบ. เมื่อ 9 – 11 ส.ค.47 อีกทั้งได้ผ่านการกลั่นกรองมาเป็นลำดับจนมี ความพร้อมที่จะนำไปสู่การพัฒนาเป็นหลักนิยมของ ทบ. ฉบับถาวรต่อไป

ทางด้านนโยบายการรักษาความปลอดภัยสารสนเทศ กองทัพในฐานะหน่วยงานในระดับกรม ของกลาโหม ได้ดำเนินการจัดทำให้เป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ม.5 หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ จากกฎหมายดังกล่าวทำให้เกิดการ อนุมัติ เสธ.ทบ./ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ ทบ. รับคำสั่ง ผบ.ทบ. ให้ สส.(ศทท.) ศึกษารายละเอียดในเรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ เพื่อเตรียมการดำเนินการที่จำเป็นสำหรับการกำหนดนโยบายและการปฏิบัติในการ รปภ.ระบบสารสนเทศของ ทบ. ตลอดจนการดำเนินการของ คณะอนุกรรมการประสานงานและกลั่นกรองมาตรฐานด้านเทคโนโลยีสารสนเทศกองทัพบก โดยมี จก.สส. เป็นประธาน และ ยก.ทบ.เป็นเลขาฯ ได้มอบหมายให้ ศทท. ร่าง

แนวนโยบายและแนวปฏิบัติฯ ดังกล่าวแล้วนำเรียน เสธ.ทบ./ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ ทบ. ให้ความเห็นชอบ และส่งร่างดังกล่าวให้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นประธานกรรมการ ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นรองประธานกรรมการ และกรรมการอื่นอีกจำนวน 12 คน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิ ที่ได้รับการสรรหาจากภาครัฐและภาคเอกชนใน 6 ด้าน อนุมัติให้เป็นนโยบายและแนวปฏิบัติทางด้านการรักษาความปลอดภัยสารสนเทศ ของกองทัพบก สำหรับนโยบายและแนวปฏิบัติดังกล่าว กองทัพบกใช้ชื่อว่า “ระเบียบกองทัพบกว่าด้วยการรักษาความปลอดภัยสารสนเทศ พ.ศ.2555 “

นอกจากระเบียบฯ ดังกล่าวแล้ว กองทัพบกได้มีการกำหนดแนวทางและการแบ่งมอบความรับผิดชอบการดำเนินงาน ตามคำรับรองการปฏิบัติราชการประจำปีงบประมาณ 2552 ตัวชี้วัดที่ 12 หมวด 4 การวัด การวิเคราะห์ และการจัดการความรู้ ซึ่งการกำหนดแนวทางและแบ่งมอบความรับผิดชอบดังกล่าวนั้น กองทัพบก โดยสำนักงานปลัดบัญชี กองทัพบก ได้มอบหมายให้ศูนย์เทคโนโลยีทางทหาร รับผิดชอบจัดทำร่าง “แผนบริหารจัดการความเสี่ยงระบบสารสนเทศกองทัพบก” ซึ่งถือว่ามีความจำเป็นและมีความสำคัญอย่างยิ่งยวด ต่อสภาวะการณ์ยุคข้อมูลข่าวสารในปัจจุบัน ในอันที่จะป้องกัน บรรเทา และควบคุมปัญหา ที่อาจเกิดขึ้นจากปัจจัยความเสี่ยงด้านสารสนเทศ และสร้างความเสียหายต่อการปฏิบัติราชการของกองทัพบก ทั้งในปัจจุบันและอนาคต ส่งผลกระทบต่อการทำงานและความสำเร็จขององค์กรในภาพรวม แผนบริหารฯ ความเสี่ยงดังกล่าวเป็นจุดเริ่มต้นที่กองทัพบกจะต้องให้ความสนใจในด้านทรัพย์สินที่กองทัพบกรับผิดชอบ และมีการสำรวจตรวจสอบทรัพย์สินเหล่านั้นว่า มีความเสี่ยงที่จะถูกโจมตีหรือการจารกรรมทางไซเบอร์หรือไม่มากน้อยเพียงใด เพื่อกำหนดมาตรฐานการในการดำเนินการป้องกันทรัพย์สินดังกล่าวต่อไป

การปฏิบัติการด้านไซเบอร์ในระดับนโยบาย มีหน่วยงานที่เกี่ยวข้องที่สำคัญ ได้แก่ คณะกรรมการปฏิบัติการข่าวสารกองทัพบก และ เครือข่ายผู้ใช้งานอินเทอร์เน็ตกองทัพบก ทั้งสองภารกิจอยู่ภายใต้การกำกับของกรมยุทธการทหารบก

ด้านการศึกษาศูนย์เทคโนโลยีทางทหาร เปิดการอบรมหลักสูตรสงครามสารสนเทศ เป็นประจำทุกปี ปีละ 1 รุ่น เพื่อให้บุคคลากรของกองทัพได้เข้าใจทางด้านนโยบาย และแนวปฏิบัติการรักษาความปลอดภัยสารสนเทศ และเพิ่มพูลบุคคลากรของกองทัพบกในมีความเข้าใจทางด้านสงครามไซเบอร์อย่างต่อเนื่อง

นอกจากหลักสูตรประจำปีแล้ว ยังมีความพยายามที่จะมีการดำเนินการแลกเปลี่ยนความรู้ ความเข้าใจทางด้านไซเบอร์กับต่างประเทศ จึงเกิดมีการประชุม Executive Steering Group (ESG) ระหว่าง ทบ.ไทย กับ ทบ.สหรัฐฯ ในระหว่างวันที่ 29 – 30 พ.ค.57 โดย ยก.ทบ.ได้เป็นเลขาฯ เนื้อหาการประชุมครั้งนั้นเป็นหัวข้อที่เกี่ยวกับการป้องกันทางไซเบอร์ ( Cyber Defense ) สรุปผลการ

ประชุมทำให้มีมติให้มีการจัด ประชุม Cyber Security - Subject Matter Expert Exchange หรือ Cyber SMEE ขึ้นเป็นครั้งแรก ระหว่าง ทบ.ไทบ กับ ทบ.สหรัฐฯ ในระหว่างวันที่ 25-27 ก.พ.57 โดยมีวัตถุประสงค์ของการประชุมดังนี้ 1. เพื่อเป็นการแลกเปลี่ยนผู้เชี่ยวชาญทางด้านไซเบอร์ 2. การแลกเปลี่ยนข้อมูลข่าวสารทางด้านการปฏิบัติการ Cyber 3. การอบรมและให้คำแนะนำในเรื่องการประกันข้อมูลข่าวสาร ( Information Assurance ) 4. การสร้างความตะหนักในด้านของ Cyber 5. การให้องค์ความรู้ในเรื่องการปฏิบัติการเครือข่ายทางไซเบอร์ของสหรัฐฯ (Network Operations)

## กองทัพเรือ

กองปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ (กปท.)[10] หน่วยงานในสังกัดกรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (สสท.ทร.) ถือเป็นหน่วยงานหลักที่เกี่ยวข้องกับสงครามไซเบอร์ของกองทัพเรือ มีหน้าที่อำนวยการ กำกับดูแล และดำเนินการเกี่ยวกับการปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศของกองทัพเรือ รวมทั้งประเมินความเสี่ยงของกองทัพเรือด้านสงครามข้อมูลข่าวสาร รวบรวมข้อมูลและสถิติ วิเคราะห์และประเมินผล ตลอดจนการเผยแพร่และแจกจ่ายให้แก่หน่วยที่เกี่ยวข้อง

ระเบียบกองทัพเรือว่าการรักษาความปลอดภัยสารสนเทศ[11] พ.ศ.2554 เป็นระเบียบที่กำหนดแนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ เพื่อเป็นแนวทางให้ข้าราชการ ทร. ยึดถือปฏิบัติ เพื่อให้การใช้งานระบบสารสนเทศเป็นไปด้วย ความเรียบร้อย ปลอดภัย คุ้มค่า และเกิดประโยชน์สูงสุดต่อทางราชการ

นอกจากระเบียบฯ แล้วยังมีการออกแนวทางการใช้งานระบบสารสนเทศ[12] ของ ทร. เพิ่มเติมอีกด้วย

---

[10] กองปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ. (ออนไลน์). เข้าถึงได้จาก : http://www.navy.mi.th/ncit/history.php, 2557.

[11] กองทัพเรือ. “ระเบียบกองทัพเรือว่าการรักษาความปลอดภัยสารสนเทศ พ.ศ.2554”. (ออนไลน์). เข้าถึงได้จาก : http://www.ctbdc.navy.mi.th/it_ctbdc/rabiabnavy_2554.pdf, 2554.

[12] กองทัพเรือ. “แนวทางการใช้งานระบบสารสนเทศ” . (ออนไลน์). เข้าถึงได้จาก : http://www.logis.navy.mi.th/data/loganalyse/it_appr.pdf, 2557.

## กองทัพอากาศ

กองสงครามอิเล็กทรอนิกส์และสารสนเทศ (กคส.) หน่วยงานในสังกัด กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) ถือเป็นหน่วยงานหลักที่เกี่ยวข้องกับสงครามไซเบอร์ของกองทัพกองทัพอากาศ มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการพัฒนา และดำเนินงานเกี่ยวกับ การสงครามอิเล็กทรอนิกส์ และสงครามสารสนเทศของกองทัพอากาศ

คณะกรรมการปฏิบัติการข่าวสารเชิงสร้างสรรค์ของกองทัพอากาศ จากนโยบายผู้บัญชาการทหารอากาศ เมื่อปี พ.ศ.2556 ด้านกิจการพลเรือนและประชาสัมพันธ์ ข้อ 5.3 ความว่า “การประสัมพันธ์เชิงรุก โดยการเผยแพร่ข้อมูลข่าวสารของกองทัพอากาศไปสู่กำลังพล ครอบครัวและสาธารณชน ผ่านทางสื่อมวลชนและสื่อประชาสัมพันธ์ต่างๆ ทั้งภายในและภายนอกกองทัพอากาศ เพื่อเสริมสร้างภาพลักษณ์ของกองทัพอากาศ รวมถึงเสริมสร้างความร่วมมือและสัมพันธ์อันดีระหว่างกองทัพอากาศ หน่วยงานภาครัฐ ภาคเอกชน และสาธารณชน” และข้อ 5.4 ความว่า “ดำเนินการปฏิบัติการข่าวสารเชิงสร้างสรรค์ โดยการสร้างเครือข่ายในการสื่อสารสาธารณะเกี่ยวกับข้อมูลข่าวสาร เพื่อสนับสนุนการปฏิบัติภารกิจของกองทัพอากาศ”

ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ.2552 และ คู่มือการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารหน่วยงานขึ้นตรงกองทัพอากาศ เป็นนโยบายที่เกี่ยวข้องกับการรองรับทางด้านไซเบอร์ของกองทัพอากาศที่เห็นออกมาเป็นรูปธรรม ต่อมาภายหลังได้มีการจัดทำและประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศ[13] พ.ศ.2556 เพื่อให้เป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ม.๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

---

[13] กองทัพอากาศ. “แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศ”. (ออนไลน์ ). http://imgcdn.rtaf.mi.th/2556/admin/rtaf_25561102015313.pdf, 2557.

## ขอบเขตของการรองรับสงครามไซเบอร์

สำหรับขอบเขตของสงครามไซเบอร์ ในมุมมอง และสิ่งที่ปรากฏของสงครามไซเบอร์ที่ผ่านมา ย่อมจะสามารถกำหนดขอบเขตได้ตามระดับของภัยคุกคามดังนี้

1. ระดับประเทศ ขอบเขตการโจมตีหรือคุกคาม ก็คือระดับประเทศ ดังนั้นสิ่งที่เป็นโครงสร้างพื้นฐานของประเทศ ไม่ว่าจะเป็นระบบไฟฟ้า ระบบการจราจร ระบบขนส่งต่างๆ ต้องได้รับการป้องกัน หน่วยงานที่ควรจะต้องเข้ามาเกี่ยวข้อง ไม่เฉพาะหน่วยงานด้านความมั่นคง หรือกองทัพ แต่ควรเป็นทุกภาคส่วนทั้งภาครัฐและภาคเอกชน ที่ต้องเข้ามามีส่วนเกี่ยวข้อง การบูรณาการทั้งมวลของหน่วยงานต่างๆ ย่อมจะสร้างความเชื่อมั่น และสร้างความตระหนัก ให้หน่วยงานต่างๆ เหล่านั้นได้เป็นอย่างดี

นโยบายทางด้านรักษาความปลอดภัยสารสนเทศของภาครัฐ เป็นเครื่องมือสำคัญที่มีส่วนในการกำหนดนิยาม ขอบเขต ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง กำหนดการประสานการปฏิบัติของหน่วยงานต่างๆ อีกทั้งยังเป็นช่องทางที่จะช่วยให้หน่วยงานของภาครัฐ ได้มีการจัดองค์กรของตนเอง เพื่อรองรับสงครามไซเบอร์ อย่างน้อยจุดเริ่มต้น ก็คือการสร้างความตระหนัก การเตรียมการในเรื่องดังกล่าว การกำหนดในเรื่องของการตอบสนองต่อเหตุการณ์หรือภัยคุกคาม ในระดับประเทศ ซึ่งถ้ากล่าวถึงเรื่องของเหตุการณ์ ด้านความมั่นคงปลอดภัย (Security incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของโครงสร้างพื้นฐานของประเทศ ตลอดจนเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรืออาจสร้างความเสียหายได้ในที่สุดซึ่งอาจส่งผลให้โครงสร้างของประเทศเกิดการหยุดชะงักหรือไม่สามารถให้บริการได้ อาทิเช่น โรงงานผลิตกระแสไฟฟ้าหยุดทำงาน ระบบการผลิตหรือการจ่ายน้ำประปาไม่ทำงาน หรือแม้กระทั้งระบบขนส่งมวลชนสำคัญๆ ได้แก่ ระบบรถไฟฟ้าขัดข้อง เป็นต้น สิ่งเหล่านี้เป็นเหตุการณ์ที่อาจจะเกิดขึ้นจากการโจมตีทางไซเบอร์ก็เป็นไปได้ เพียงแต่ว่า ผู้รับผิดชอบในแต่ละภาคส่วนจะรับรู้รับทราบถึงสิ่งเหล่านั้นได้อย่างไร ใครหรือหน่วยงานจะเป็นผู้ที่รับผิดชอบถ้าเกิดเหตุการณ์ดังกล่าว การรับมือต่อเหตุการณ์ดังกล่าว จะใช้เวลารับรู้ และตอบสนองให้ระบบกลับมาเป็นปกติ ใช้เวลาเท่านั้น การจะทำแผนสำรองกรณีฉุกเฉิน เพื่อรับมือต่อเหตุการณ์เหล่านี้ จึงเป็นหัวใจสำคัญ และที่ภาครัฐมีหน่วยงานอย่างเช่น Thai CERT ถือว่าเป็นหลักประกันส่วนหนึ่งที่จะสร้างความมั่นใจต่อเรื่องของการตอบสนองต่อเหตุการณ์ ( Incident Response ) ที่เกิดขึ้นได้ในระดับหนึ่ง

บทบาทของกลาโหม และ กองทัพไทย การที่หน่วยงานมีการใช้งานเครือข่ายสื่อสารข้อมูล ที่กระจายไปตามส่วนต่างๆ ของประเทศ การเฝ้าระวังเครือข่ายของตนเอง ยอมจะเป็นเพียงระดับในการป้องกันทางไซเบอร์เท่านั้น สำหรับบทบาทอื่นๆ กรณีถ้าหากว่าเราเกิดมีการทำสงครามในระหว่างประเทศเกิดขึ้น กองทัพต้องกำหนดขอบเขต ความรับผิดชอบ ในเรื่องของเฉพาะเครือข่าย

สารสนเทศ เครือข่ายสื่อสารข้อมูลของกองทัพเท่านั้น ที่จะต้องได้รับการปกป้อง จากการโจมตีทางไซเบอร์ แต่ถ้าหากกองทัพมีการใช้งานเครือข่ายของภาครัฐอื่นๆ ภาคเอกชน การกำหนดขอบเขตของความรับผิดชอบในเรื่องของสงครามไซเบอร์ อาจจะต้องครอบคลุมไปในภาคส่วนเหล่านั้นด้วย การกำหนดหน่วยของงานกองทัพที่ค่อยเฝ้าระวังและตอบสนองต่อเหตุการณ์ที่เกิด ยอมเป็นส่วนหน่วยที่อยู่ในส่วนหนึ่งขอบเขตความรับผิดชอบดังกล่าวอีกด้วย ขอบเขตความรับชอบของกองทัพในระดับประเทศ จะมีความชัดเจนมาก เนื่องจากมีผลกระทบในระดับความมั่นคงของประเทศนั่นเอง

2. ระดับการก่อการร้าย และอาชญากรรมต่างๆ ในระดับนี้กองทัพไทย อาจจะต้องมีบทบาทเพียงการเฝ้าระวังและแจ้งเตือน เท่านั้น เพราะขอบเขตความรับผิดชอบ จะมีเรื่องของกฎหมายที่เกี่ยวข้อง อาธิเช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หมวดที่ ๒ พนักงานเจ้าหน้าที่ ที่ได้รับการแต่งตั้งจากรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดทางคอมพิวเตอร์ ทำให้กองทัพ ถ้าไม่มีพนักงานเจ้าหน้าที่ ย่อมจะไม่สามารถเข้าไปดำเนินการใดๆ หรือเข้าไปตอบสนองต่อเหตุการณ์ทางอาชญากรรมไซเบอร์ได้ เนื่องจากกฎหมายไม่ได้ให้อำนาจไว้ ยกเว้นแต่ว่ากองทัพต้องมีส่วนสนับสนุนในด้านที่จะลดความเสียหายที่เกิดขึ้น ร่วมทั้งการฟื้นฟูในภายหลัง ถ้าเหตุการณ์นั้นเกิดขึ้นแล้วมีผลกระทบ และร้ายแรง จนอาจจะมองได้ว่าเป็นอาชญากรรมระดับชาติ และความเสียหายนั้นกว้างขวาง จนเจ้าหน้าที่ตามกฎหมายไม่มีกำลังพลเพียงพอที่จะเข้าไประงับเหตุการณ์ที่เกิดขึ้นนั้น

3. ระดับแฮ็กเกอร์ ขอบเขตของกองทัพต่อภัยคุกคามในระดับนี้ ย่อมจะมีส่วนคล้ายกับในระดับการก่อการร้าย และอาชญากรรมต่างๆ การปฏิบัติก็ใกล้เคียงกัน บทบาทของกองทัพ ถ้าหากว่ายังไม่สามารถเข้าไปดำเนินการในระดับนี้ การสร้างองค์ความรู้ สร้างความตระหนัก หรือการสร้างเจ้าหน้าที่ของกองทัพ ที่มีความรู้ในด้านการรักษาความปลอดภัยสารสนเทศ ควรเป็นขอบเขตที่กองทัพไทย สามารถที่จะดำเนินการได้ เพียงแต่ว่ากองทัพควรจะกำหนดในเรื่องของแผนแม่บทความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารกองทัพให้ชัดเจนต่อไป

## สถานภาพและความพร้อมในการรับมือกับสงครามไซเบอร์

ต้องยอมรับในเรื่องของสถานภาพและความพร้อมว่า กองทัพของเรา ยังขาดความพร้อมในการรองรับสงครามไซเบอร์ ทั้งในด้านนโยบาย ทั้งโครงสร้างของหน่วย ต่างๆ

## กำลังพลและเครื่องมือในเรื่องสงครามไซเบอร์และการจัดตั้งหน่วยงานรองรับในกองทัพไทย

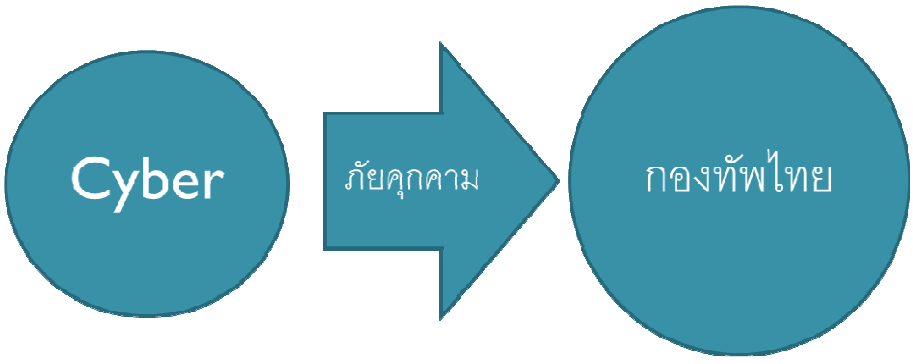
กำลังพลก็เช่นเดียวกัน บุคคลากร ในด้านนี้มีน้อยมาก และขาดแคลน เนื่องจากปัญหาของการทำงานที่เป็นโครงสร้างในแบบสายการบังคับบัญชา ทำให้เกิดการทำงานที่อาจจะตอบสนองต่อเหตุการณ์ เป็นเรื่องกระทำได้ช้าและไม่ทันต่อเหตุการณ์ อีกทั้งกองทัพยังไม่มีหน่วยงานที่รับผิดชอบอย่างชัดเจน ทำให้แนวทางการศึกษาอบรม ตลอดจนการจัดหาอุปกรณ์ต่างๆ กระทำได้ยากลำบาก เนื่องจากโครงสร้างผังการจัดหน่วยยังมีเรื่องอัตราสิ่งอุปกรณ์เข้ามาเกี่ยวข้องอย่างชัดเจน ถ้าไม่มีการวางโครงสร้างรองรับไว้ก่อน การจัดหาทั้งคนและเครื่องมือ จะไม่สามารถหาเหตุผลในการดำเนินการได้เลย

# บทที่ 4
# แนวทางการรองรับสงครามไซเบอร์ในอนาคต

## การประเมินภัยคุกคามของสงครามไซเบอร์

จากปัญหาและผลกระทบของสงครามไซเบอร์ ตลอดความพร้อมและปัญหาในด้านโครงสร้างตลอดจนกำลังพลของหน่วยงานของกองทัพไทย ทำให้เกิดผลกระทบในเรื่องของการรับมือกับสงครามไซเบอร์ที่อาจจะเกิดขึ้นในอนาคต สิ่งที่เป็นความท้าทายของกองทัพไทย ที่ต้องเผชิญกับเรื่องดังกล่าว คงต้องมาพิจาณาแนวโน้มของการใช้งานเครือข่ายคอมพิวเตอร์ของกองทัพไทย ที่มีแนวโน้มมีการใช้งานเพิ่มมากขึ้น ตลอดจนยุทโธปกรณ์ของกองทัพ ตลอดจนระบบการปฏิบัติงานต่างๆ มีการเชื่อมโยงและการใช้งานเครือข่ายคอมพิวเตอร์เป็นหลัก และมีการขยายตัวเพิ่มขึ้นตลอดเวลา ภัยคุกคามทางด้านไซเบอร์ ในมุมมองของกองทัพไทยตามแผนภาพที่ 4-1

แผนภาพที่ 4-1 แผนภาพแสดงความสัมพันธ์ทางไซเบอร์ที่เป็นภัยคุกคามต่อกองทัพ




ภัยคุกคามดังกล่าว กองทัพให้ความสำคัญ ด้วยกัน 4 ด้าน ได้แก่ 1 . ภัยคุกคาม ที่ส่งผลต่อความมั่นคงของประเทศ 2. ภัยคุกคาม ที่ส่งผลกระทบต่อสามจังหวัดชายแดนภาคใต้( จชต. ) 3.ภัยคุกคาม ที่ส่งผลกระทบต่อ สถาบันฯ 4. ภัยคุกคาม ที่ส่งผลกระทบต่อ ภาพลักษณ์ของ กองทัพ

## ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ

การใช้ไซเบอร์ เพื่อเป็นภัยคุกคามในระดับประเทศ หรือระดับชาติ วิธีการอาจจะเพียงแค่ใช้เว็บไซต์ของประเทศตนเอง เผยแพร่ข่าวสารที่ทำให้เกิดความได้เปรียบทางการเมือง หรือด้านความมั่นคง ยกตัวอย่างกรณีการเผยแพร่ข่าวสารของประเทศเพื่อนบ้าน เพื่อชี้แจงกรณีพิพาทเขาพระวิหาร เป็นต้น กรณีดังกล่าว การดำเนินการชี้แจงข้อเท็จจริง หรือ ตอบโต้ด้วยข้อเท็จจริง หน่วยงานที่เกี่ยวข้องหน่วยงานอันดับต้นๆ ได้แก่ กระทรวงการต่างประเทศ จนไปถึงในระดับรัฐบาล ทางฝ่ายกองทัพคงจะต้องใช้การดำเนินการในระดับกระทรวงกลาโหม เป็นผู้รับผิดชอบในการดำเนินการ เพราะภัยคุกคามในระดับนี้ ข้อมูลต่างๆ มีความสุ่มเสี่ยง ส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศแทบทั้งสิ้น หรือยกตัวอย่างกรณีของเว็บไซต์วิกิลีกส์ ซึ่งสร้างความโด่งดังไปทั่วโลก เพราะมีการนำข้อมูลความลับของสถานทูตสหรัฐทั่วโลก รวมทั้งของประเทศไทยด้วย และแฟ้มลับสงครามอิรัก และอัฟกานิสถาน ประมาณ 250,000 ซึ่งทำให้จูเลียน อัสซานจ์ ผู้ก่อตั้งที่อยู่เบื้องหลังวิกิลีกส์กลายเป็นบุคคลที่สหรัฐอเมริกาต้องการตัวมากที่สุดในโลกมาจนถึงปัจจุบัน [1] การเปิดเผยความลับนี้ถือว่าข้อมูลที่ได้มาต้องมีความร่วมมือของเหล่าบรรดาแฮ็กเกอร์ ที่อยู่ในเครือข่ายไซเบอร์ทั่วโลก และอาจจะรวมทั้งเหล่าผู้ที่ไม่พอใจประเทศสหรัฐ ที่มีอยู่ทั่วโลก ดังนั้นในโลกของไซเบอร์ การเปิดเผยความลับต่างๆ ที่เป็นในระดับข้อมูลรายงานทางการทูต หรือข้อมูลความลับของชาติ ก็ถือว่าเป็นภัยคุกคามในระดับความมั่นคงของประเทศนั่นเอง

## ภัยคุกคามที่ส่งผลกระทบต่อสามจังหวัดชายแดนภาคใต้( จชต. )

ภัยคุกคามทางไซเบอร์ดังกล่าว เป็นการใช้โลกของไซเบอร์ เพื่อการเผยแพร่ข่าวสารของผู้ก่อความไม่สงบ ยกตัวอย่างเช่น การเผยแพร่การลอบวางระเบิด ทำให้เกิดการสูญเสียของเจ้าหน้าที่ของรัฐ เพื่อให้สื่อมวลชนกระแสหลักนำไปเผยแพร่ต่อ หรือเพื่อให้ประชาชนทั่วไป รวมทั้งเจ้าหน้าที่รัฐเกิดความกลัวเกรง ถือเป็นเหมือนการปฏิบัติการจิตวิทยาอย่างหนึ่ง นอกจากนั้นยังมีการแสดงถึงผลงานของผู้ก่อความไม่สงบที่อาจจะส่งผลกระทบ ทำให้เกิดแนวร่วมของผู้ก่อความไม่สงบเพิ่มขึ้น ซึ่งการเผยแพร่หรือแชร์ข้อมูล หรือภาพเหล่านั้น คนที่กระทำอาจจะกลายเป็น

---

[1] เดวิด ลีห์, ลุค ฮาร์ดิ้ง. Wikileaks ความลับเขย่าโลก. แปลโดยศิริพงษ์ วิทยวิโรจน์. (กรุงเทพฯ:สำนักพิมพ์มติชน, 2556). หน้า 9.

แนวร่วมมุมกลับโดยไม่รู้ตัวก็เป็นไปได้ นอกจากนั้นยังมีกรณีของการสร้างเว็บไซต์ที่กลุ่มผู้ก่อความไม่สงบใช้เป็นแหล่งการพบปะ แหละแจ้งข่าวสารของกลุ่มของตนเอง เพื่อหลีกเลี่ยงการเฝ้าติดตามของเจ้าหน้าที่รัฐ หรือบางกรณีการอาจลุกลามไปถึงขั้นกระทบในระดับความมั่นคงของประเทศ ยกตัวอย่างเช่นการจัดทำเว็บไซต์พูโล หรือรัฐปัตตานี ซึ่งการสร้างเว็บไซต์ดังกล่าวนอกจากจะเป็นแหล่งในการเผยแพร่ข่าวสาร แล้วยัง เป็นการตอกย้ำถึงการดำรงอยู่ของกลุ่มผู้ก่อความไม่สงบที่ มีตัวตน มีองค์ของตนเอง และพร้อมที่จะต่อต้านการปกครองของรัฐบาลนั่นเอง

## ภัยคุกคาม ที่ส่งผลกระทบต่อ สถาบันฯ

ภัยคุกคามที่ส่งผลกระทบต่อสถาบันฯ ต่อราชวงศ์ของไทย นั้น ทางด้านไซเบอร์ เป็นสิ่งที่กระทำได้ง่าย และยากต่อการดำเนินคดีต่อผู้กระทำ การดำเนินการดังกล่าว มีทั้งการเผยแพร่ภาพที่หมิ่นสถาบันฯ การวิจารณ์สถาบันฯ ในทางเสื่อมเสีย การกล่าวร้าย ป้ายสี ให้สถาบันฯ เกิดความเสื่อมศรัทธาต่อประชาชน และอีกหลายประเด็น ล้วนแล้วแต่อาศัยโลกไซเบอร์เป็นเครื่องมือในการถ่ายทอดทั้งมวล กฎหมายที่เกี่ยวข้องไม่อาจจะดำเนินการได้ สาเหตุหลายประการ ผู้กระทำไม่ได้อยู่ประเทศไทย หรือผู้กระทำใช้เครื่องมือของต่างประเทศ ซึ่งกฎหมายของต่างประเทศไม่ได้รับรองความผิดในฐานความผิดนั้น หรือความผิดนั้นในต่างประเทศอาจจะมองเป็นแค่ในระดับความคิดในฐานหมิ่นประมาท ซึ่งไม่ร้ายแรงเหมือนกฎหมายในประเทศไทย ซึ่งการดำเนินการในเรื่องดังกล่าว ถึงแม้จะมีหน่วยงานต่างๆ ทั้ง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ หรือกระทั้งใช้กระบวนการตุลาการของไทย ในการปิดกั้นการเผยแพร่ดังกล่าว ก็มีขอบเขตการดำเนินการจำกัดอยู่เฉพาะประเทศไทยเท่านั้น การเข้าถึงข้อมูลในต่างประเทศก็ยังสามารถเข้าถึงข้อมูลเหล่านั้นอยู่ หรือในประเทศไทยถ้าหากว่ามีผู้ใดสามารถใช้เทคโนโลยีที่เรียกพล็อกซี่ ( Proxy) หรือ เครือข่ายส่วนตัวเสมือน ( Virtual Private Network: VPN) ก็สามารถที่จะเข้าไปรับรู้ข้อความหรือเนื้อหาเหล่านั้นได้อยู่ดี การปิดกั้นดังกล่าวเป็นเรื่องกระทำแทบไม่ได้เลย

## ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพ

ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพ การใช้ไซเบอร์เพื่อทำให้ภาพลักษณ์ของกองทัพเสื่อมเสีย หรือลดความน่าเชื่อถือในสังคม ย่อมจะสร้างความไม่เชื่อมั่นต่อ

การปกป้องหรือพิทักษ์อธิปไตยของชาติ อาจจะเป็นการแสดงให้ประชาชนเชื่อว่ากองทัพมีแต่กำลังพลที่ขาดวินัยไม่รักษากฎระเบียบของกองทัพ การกระทำผิดกฎหมายของประเทศ ล้วนแล้วแต่เป็นหัวข้อที่ผู้ที่ต้องการกระทำต่อกองทัพใช้เป็นประเด็นหลักๆ ในการดำเนินการ สิ่งเหล่านั้นหรือข้อมูลที่ได้รับอาจจะได้มาจากการกระผิดของกำลังพลเพียงบางคนของกองทัพ แต่เมื่อมีการเผยแพร่ในโลกไซเบอร์ จะเกิดผลกระทบในวงกว้างและจะขยายผลเหตุการณ์ต่างๆ ดำเนินไปได้อย่างรวดเร็วมาก การพยายามจะชี้แจงข้อเท็จของกองทัพอาจจะต้องดำเนินการภายหลังจากเหตุการณ์ทางไซเบอร์เกิดขึ้นแล้ว หรืออาจจะแค่การประชาสัมพันธ์ในเชิงตอบโต้ผ่านทางสื่อกระแสหลักทั้งหลาย สำหรับการแก้ไขปัญหาทางไซเบอร์กระทำได้ยาก เนื่องจากการเผยแพร่หรือกระจายข่าวสารเป็นการกระทำในแบบเครือข่าย หรือกลุ่มเครือข่าย การรับรู้ก็จะเป็นเฉพาะกลุ่ม ที่เชื่อมต่อกันไปเรื่อยๆ ไม่รู้จบ อาจจะพยายามหาจุดเริ่มต้น หรือผู้เผยแพร่คนแรกๆ ที่กระทำนั้น แทบจะไม่ได้เลย การฟ้องร้องหรือการดำเนินการกฎหมายจึงเป็นไปไม่ได้เช่นกัน นอกจากนั้นยังมีประเด็นที่เกี่ยวข้องกับด้านการเมือง หรือในด้านของความไม่พอใจของคนในกองทัพเป็นการส่วนตัว ก็เป็นประเด็นที่จะสร้างความเสื่อมเสียภาพลักษณ์ต่อกองทัพในภาพรวมได้เช่นกัน ยกตัวอย่างการพยายามเผยแพร่ว่ากองทัพไม่เป็นกลางทางการเมือง หรือในกรณีมีการเผยแพร่เพื่อใส่ร้ายป้ายสีผู้นำกองทัพ หรือเรื่องเล็กๆ น้อยแค่เรื่องของคนในครอบครัวของกองทัพ มีการวิวาทกัน ก็อาจจะทำให้มีการนำข้อมูลที่เสื่อมเสียของอีกฝ่ายหนึ่งมาเผยแพร่ อาจจะกล่าวหาว่าอีกฝ่ายมีเรื่องของการทุจริตในหน้าที่เป็นต้น ถึงจะเป็นเล็กๆ สายตาของคนทั่วไป แต่เมื่อถูกเผยแพร่ไปสู่สาธารณะ หรือภายในเครือข่ายของไซเบอร์ อาจจะส่งผลกระทบต่อภาพลักษณ์ได้เช่นกัน นอกจากนั้นยังมีประเด็นสำคัญที่มักจะเกิดขึ้นบ่อยๆ เช่น เอกสารลับของทางราชการ ถูกนำไปเผยแพร่ในโลกไซเบอร์ ผู้กระทำอาจจะต้องการเพียงเพื่อให้ประชาชนทั่วไป หรือฝ่ายที่ไม่พอใจของกองทัพ ได้นำไปเผยแพร่ ขยายผล แต่กลับส่งผลกระทบต่อหน่วยงานที่เกี่ยวข้องอย่างมาก เพราะนอกจากเสื่อมเสียภาพลักษณ์แล้ว ยังจะแสดงถึงการขาดประสิทธิภาพในการทำงาน การรักษาความลับของทางราชการกระทำไม่ได้ตามที่ระเบียบกำหนดไว้นั่นเอง

## กรอบในการดำเนินการทางด้านสงครามไซเบอร์

ดังนั้นกองทัพไทยควรจะต้องมีการกำหนดแนวทางหรือกรอบในการดำเนินการในด้านสงครามไซเบอร์ออกเป็น 4 ด้านดังนี้

1. ด้านนโยบาย

2. ด้านความรู้
3. ด้านโครงสร้างองค์กร
4. ด้านการปฏิบัติงาน

1. ด้านนโยบาย ควรจะต้องดำเนินการจัดทำแผนแม่บททางด้านสงครามไซเบอร์ของเหล่าทัพ ( Master Plan ) ตลอดจนแผนแม่บททางด้านการรักษาความปลอดภัยสารสนเทศ อีกด้วย จากนั้นเป็นการกำหนดระเบียบปฏิบัติ ข้อบังคับต่างๆ ( Regulations ) รวมถึงการประชุมชี้แจง ( Explanations ) ตรวจเยี่ยม แนะนำ ติดตาม ประเมิน ตรวจสอบการปฏิบัติฯ ( Inspection ) การจัดตั้งคณะกรรมการฯ ( Committee ) เพื่อประชุมติดตาม กำกับการดำเนินการตามนโยบายฯ และการรับรองระบบ ( Certification and Accreditation ; C&A )

1.1 แผนแม่บททางด้านสงครามไซเบอร์ เป็นแผนที่ใช้เป็นต้นแบบหลักในการวางแผนปฏิบัติ โดยแผนปฏิบัติย่อยๆ ที่ต่อยอดจากแผนแม่บทดังกล่าวนั้น จะต้องสอดคล้องต้องกัน และเป็นไปในทิศทางเดียวกับแผนแม่บทหลักเสมอ แผนแม่บทเนื้อหาจะประกอบไปด้วย วิสัยทัศน์ เป้าหมาย ยุทธศาสตร์ รวมทั้งแผนงานปฏิบัติต่างๆ และควรกำหนดเป็นแผนที่มีระยะเวลาเกิน 5 ปี ขึ้นไป

1.2 การกำหนดระเบียบปฏิบัติข้อบังคับต่างๆ ในแต่ละเหล่าทัพต้องมีการออกระเบียบอย่างน้อย 2 ระเบียบหลัก ได้แก่ ระเบียบการรักษาความปลอดภัยสารสนเทศ และระเบียบการรักษาความปลอดภัยข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามที่กฎหมายกำหนด ได้แก่ พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 นอกจากนั้นควรสร้างความเข้าใจ และสร้างความตระหนักแก่กำลังพลของกองทัพ เพื่อให้มีความเข้าใจต่อภัยคุกคาม และนำระเบียบฯ ของกองทัพไทยไปปฏิบัติได้อย่างถูกต้อง

1.3 การจัดประชุมชี้แจง หน่วยและกำลังพลของหน่วยควรจะต้องกระทำอย่างต่อเนื่อง ถ้ามีข่าวสารที่มีการแจ้งเตือนว่ามีภัยคุกคามทางด้านไซเบอร์ หรือเป็นข่าวสารตามสื่อต่างๆ ควรมีการชี้แจงกำลังพลให้ทราบตลอดเวลา เพื่อให้เกิดความตื่นตัวแก่กำลังพลของหน่วย นอกจากนั้นอาจจะมีการจัดการประชุมทั้งภายในหน่วย และนอกหน่วย รวมทั้งให้การสัมมนาต่างๆ เพิ่มเติม เพื่อให้ได้รับความรู้จากวิทยากร หรือผู้ทรงคุณวุฒิในด้านไซเบอร์เพิ่มเติม

1.4 ตรวจเยี่ยม แนะนำ ติดตาม ประเมิน ตรวจสอบการปฏิบัติฯ เป็นการดำเนินการของหน่วยเหนือที่กระทำต่อหน่วยรอง หรือหน่วยงานที่มีอำนาจในการดำเนินการ เพื่อให้เกิดผลในการบังคับใช้ระเบียบปฏิบัติหรืออาจจะเพื่อให้หน่วยได้มีการประเมินตนเองก่อน และเป็นรับทราบ

ความรู้ความเข้าใจของกำลังพลของหน่วยว่า มีความเข้าใจในด้านไซเบอร์มากน้อยเพียงใด ควรมีการดำเนินการเป็นประจำทุกๆ ปี

1.5 การจัดตั้งคณะกรรมการฯ ในกองทัพมีคณะกรรมการต่างๆ เพื่อการติดตามหรือประเมินผลในด้านต่างๆ บางครั้งการแต่งตั้งคณะกรรมการฯ ก็เป็นการจัดตั้งเพื่อการแก้ไขปัญหาเฉพาะหน้าในบางเรื่อง ที่ต้องการความรอบรู้ของกรรมการต่างๆ เหล่านั้น งานด้านไซเบอร์ในภาครัฐ หรือในระดับรัฐบาลก็มีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้น เหล่าทัพในฐานะเป็นหน่วยงานด้านความมั่นคง ก็ควรจะต้องมีการจัดตั้งคณะกรรมการด้านการรักษาความปลอดภัยไซเบอร์ โดยมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ( CIO) ของเหล่าทัพเป็นประธานฯ เพื่อให้สอดรับกับคณะกรรมการฯ ในระดับรัฐบาล และถือเป็นการสนองตอบนโยบายของภาครัฐในเรื่องดังกล่าวต่อไป

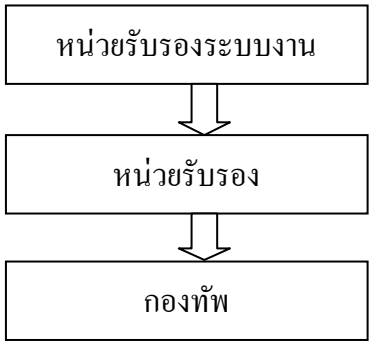
1.6 การออกใบรับรองและการรับรองระบบฯ ( Certification and Accreditation ; C&A) เป็นเรื่องใหม่พอสมควรที่เหล่าทัพจะต้องให้ความสนใจและพัฒนาอย่างต่อเนื่อง

การออกใบรับรอง (Certification ) เพื่อให้ได้มาตรฐานใดมาตรฐานหนึ่งนั้น จะต้องมีหน่วยงานใดหน่วยงานหนึ่งเป็นผู้ดำเนินการ เช่น การรับรองมาตรฐานความปลอดภัยทางด้านสารสนเทศ ก็อาจจะต้องได้รับใบรับรองที่เป็นมาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799 ซึ่งอาจจะต้องมีหน่วยงาน หรือองค์กรผ่านนอกเข้ามารับรอง เพื่อให้ระบบงาน หน่วยงาน ได้มาตรฐานความปลอดภัยดังกล่าว ซึ่งหน่วยงานรับรองนั้นจะเรียกว่า Certification Body

การรับรองระบบงาน (Accreditation) คือ การยอมรับอย่างเป็นทางการว่าหน่วยรับรอง (Certification Body) มีความสามารถในการดำเนินการให้การรับรองกิจกรรมใดกิจกรรมหนึ่ง เช่น การรับรองระบบงานของหน่วยภาครัฐทางด้าน มาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799 เป็นต้น

หน่วยรับรอง (Certification Body) คือ บุคคลที่สามที่ให้บริการการตรวจประเมินและรับรองหรือจดทะเบียนการเป็นไปตามเกณฑ์กำหนดของกิจกรรม ซึ่งความสัมพันธ์ของกระบวนการออกใบรับรองแสดงดังแผนภาพที่ 4-2

แผนภาพที่ 4-2 แผนภาพความสัมพันธ์ระหว่างหน่วยรับรองระบบงานกับหน่วยงาน




2. ด้านความรู้ ควรจะต้องดำเนินการจัดการประชุมแลกเปลี่ยนผู้เชี่ยวชาญด้านไซเบอร์อย่างต่อเนื่องเป็นประจำทุกปี เพื่อติดตามการเปลี่ยนแปลงของโลก การจัดการองค์ความรู้ด้านไซเบอร์ ( Cyber Knowledge Management ; KM ) รวมถึงการศึกษาดูงานต่างๆ การดำเนินการฝึกอบรมฯ ( Training ) ทั้งหลักสูตรภายใน-ภายนอก รวมถึงการขอรับการสนับสนุนทุนต่างประเทศ และการจัดประชุมสัมมนาเชิงปฏิบัติการ ( Seminar ) เป็นประจำทุกปี เพื่อเพิ่มพูนความรู้และแลกเปลี่ยนประสบการณ์ระหว่างเจ้าหน้าที่ฝ่ายเทคนิคที่เกี่ยวข้องของกองทัพนั่นเอง

2.1 ประชุมแลกเปลี่ยนผู้เชี่ยวชาญด้านไซเบอร์ อาจจะเป็นการจัดการประชุมกับทางต่างประเทศ เช่น ประชุมแลกเปลี่ยนผู้เชี่ยวชาญด้านไซเบอร์ ไทย-สหรัฐ ( Cyber Security – Subject Master Expert Exchange ( SMEE ) เป็นต้น เพื่อให้เกิดองค์ความรู้ใหม่ๆ ที่กองทัพจะได้ประโยชน์จากต่างประเทศ ข้อสรุปจากการประชุมอาจจะได้มาซึ่ง Road Map หรือแผนผังแนวทางการทำงานในอนาคตร่วมกัน นอกจากนั้นยังจะได้ความสัมพันธ์อันดีกับต่างประเทศอีกด้วย ความสัมพันธ์ดังกล่าวเราจะได้รับความร่วมมือในการแก้ไขปัญหาในอนาคต ถ้าเกิดมีเหตุการณ์ทางด้านสงครามไซเบอร์ที่กระทบต่อความมั่นคงต่อประเทศของเราก็เป็นไปได้

2.2 การจัดการองค์ความรู้ด้านไซเบอร์ ที่เรียกว่า Knowledge Management (KM) ซึ่งเป็นนโยบายหลักของกองทัพอยู่แล้วที่จะมีการดำเนินการทางด้านจัดการองค์ความรู้ในทุกๆ ด้าน ซึ่งทางด้านไซเบอร์ก็ควรจะมีการส่งเสริมให้ขยายวงกว้างมากขึ้น

2.3 การศึกษาหรือดูงาน ทั้งในและต่างประเทศ กองทัพควรจะต้องมีการจัดสรรงบประมาณ เป็นงบประจำปี เพื่อให้กำลังพลและหน่วยงานได้เรียนรู้ ข้อมูลใหม่นั่นเอง

2.4 การฝึกอบรม คงเช่นเดียวกันกับการศึกษาดูงาน ถือเป็นการต่อยอดจากการศึกษาดูงานจากภายนอก กำลังพลเหล่านั้นเมื่อกลับมาแล้ว ควรจะต้องมีการถ่ายทอดความรู้ในรูปแบบของการจัดหลักสูตรอบรมต่างๆ ขึ้นภายในหน่วยงานของตนเอง และมีการแจ้งประกาศให้หน่วยงานอื่นๆ ได้รับทราบอีกด้วย

2.5 การจัดประชุมสัมมนาเชิงปฏิบัติการ ถือเป็นการดำเนินการขยายผล และวัดผลการฝึกอบรมต่างๆ อาจจะจัดในรูปของการจัดการแข่งขัน เพื่อวัดประสิทธิภาพของกำลังพล ของหน่วยงานที่เกี่ยวข้องกับไซเบอร์ เช่น การสร้างแบบจำลองสถานการณ์การถูกโจมตีทางไซเบอร์ แล้วมีการจัดทีมของหน่วยต่างๆ มาเพื่อแก้ไขปัญหา และตอบปัญหา ในเวลาที่กำหนด การประเมินผลก็ให้คะแนนตามปัญหาที่ให้แต่ละทีมดำเนินการแก้ไข เป็นต้น

3. ด้านโครงสร้างองค์กร ควรจะต้องเร่งดำเนินการปรับปรุงโครงสร้าง ภารกิจการจัดองค์กร และแนวทางการบรรจุอัตรากำลังพลของกองทัพ เพื่อให้มีขีดความสามารถพร้อมรับมือกับภัยคุกคามด้านไซเบอร์ และเป็นไปตามนโยบายของหน่วยเหนือ โดยเฉพาะอย่างยิ่งการดำเนินการออกคำสั่งฯ จัดตั้งหน่วยปฏิบัติการด้านไซเบอร์ ( ใช้เพื่อพลาง ) เป็นการเฉพาะ เช่น ศูนย์ปฏิบัติการไซเบอร์ของกองทัพ เป็นต้น

4. ด้านการปฏิบัติการ ควรจะต้องเร่งดำเนินการจัดตั้งภาคีเครือข่ายหรือประชาคมไซเบอร์ ( Communities ) การใช้บริการจดหมายอิเล็กทรอนิกส์ ( e-mail ) ของกองทัพ การพัฒนาโปรแกรมและระบบงานต่างๆ เพื่อการใช้งานของกองทัพ ( Applications ) ให้มีมาตรฐานด้านการรักษาความปลอดภัย การติดตั้งอุปกรณ์เครื่องมือด้านการรักษาความปลอดภัยไซเบอร์ ( Tools ) เช่น ระบบ Intrusion Detection System ( IDS ) Intrusion Protection System ( IPS ) รวมถึงการฝึกปฏิบัติการด้านไซเบอร์ ( Workshop ) โดยดำเนินการแสวงหาความร่วมมือกับ กระทรวงกลาโหม และหน่วยงานภายนอกทั้งภาครัฐและธุรกิจเอกชน หากกองทัพ ดำเนินการตามแนวความคิดดังกล่าว ก็จะเป็นประโยชน์ต่อกองทัพและประเทศชาติโดยส่วนรวมในด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ ( Cyber Security ) เพราะทำสิ่งทุกอย่างจะก่อเกิดเป็นรูปธรรมได้จริง ก็มักจะขึ้นอยู่กับความสำเร็จในการปฏิบัติ มิเช่นนั้นก็จะเป็นเพียงทฤษฎีบทหนึ่ง ซึ่งไม่สามารถนำไปใช้ให้ก่อเกิดประโยชน์อะไรได้อย่างเต็มที่

## กรอบระยะเวลาในการดำเนินการทางด้านสงครามไซเบอร์

จากปัญหาภัยคุกคามดังกล่าวที่แนวโน้มจะมีมากขึ้นทุกวัน ทำให้ กองทัพไทยต้องมีการปรับระบบงานต่างๆให้มีความสอดคล้องกัน มีแนวทางในการรองรับสงครามไซเบอร์ให้ชัดเจน ทั้งแผนงานการพัฒนาบุคคลากรให้มีความเชี่ยวชาญ การปรับโครงสร้างองค์กร และการกำหนดมาตรการต่างๆ เพื่อตอบสนองต่อภัยคุกคามรูปแบบต่างๆ อย่างเป็นขั้นเป็นตอน โดยแนวทางในการดำเนินการควรแบ่งออกเป็น 3 ระยะ ดังนี้.-

ระยะแรก : (ปี 2557 - ปี 2559)

1. ปรับภารกิจ พันธกิจงานให้สอดคล้องกับสถานการณ์ภัยคุกคามด้านสงครามไซเบอร์ในปัจจุบัน

2. จัดหาบุคคลากรที่มีความรู้ความสามารถในด้านระบบเครือข่าย ระบบโปรแกรม ระบบสารสนเทศ รวมทั้งด้านไซเบอร์ ที่เกี่ยวข้องเพื่อศึกษาและรับผิดชอบงานด้านสงครามไซเบอร์

3. การจัดทำและปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายกำหนด

4. การจัดทำแผนแม่บททางด้านการรักษาความปลอดภัยทางไซเบอร์ของเหล่าทัพ

5. การจัดหน่วยงาน ชุดฝึกอบรม ที่จะทำให้กำลังพลของกองทัพ ได้เห็นและเข้าใจภัยคุกคามไซเบอร์ เป็นการสร้างความตะหนักทางด้านการรักษาความปลอดภัยสารสนเทศ และการป้องกันภัยคุกคามทางไซเบอร์ การอบรมนี้จะเป็นการเตือนภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ผู้บริหาร และ ผู้บังคับบัญชา ในทุกระดับให้เห็นถึงความสำคัญและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศที่ละเลยเรื่องความปลอดภัย ซึ่งจะมีผลกระทบกับระบบโดยรวม อีกทั้งอาจมีความผิด ตาม พ.ร.บ. การกระทำความผิดทางคอมพิวเตอร์อีกด้วย

6. จัดทำระบบ การตรวจสอบสิทธิ์ (Authentication) เน้นการปฏิบัติตามนโยบายและแนวปฏิบัติ โดยเฉพาะการควบคุมการเข้าถึงระบบ (Access Control) ให้กำลังพลของกองทัพมีความเข้าใจและปฏิบัติให้ถูกต้อง และป้องกันการคุกคามรูปแบบใหม่ๆ ที่จะเกิดในอนาคต

7. จัดเตรียมบุคคลากรให้มีความพร้อมในการทำงาน โดยส่งเข้ารับการอบรมหลักสูตรต่างๆ ตั้งแต่ขั้นพื้นฐาน ขั้นการปฏิบัติ และขั้นการบริหารองค์กร เพื่อให้เกิดความปลอดภัย

8. ตรวจสอบ ทบทวน และปรับปรุงระเบียบการรักษาความปลอดภัยสารสนเทศของกองทัพ ให้มีความทันสมัย อ่อนตัว ปฏิบัติได้จริง ตอบสนองกับการคุกคามระบบได้อย่างมีประสิทธิภาพ

9. จัดหาอุปกรณ์ระบบรักษาความปลอดภัยสารสนเทศ และเครื่องมือในการบริหารจัดการระบบรักษาความปลอดภัยสารสนเทศที่มีประสิทธิภาพสูงสุด เช่น Vulnerability Assessment : VA, อุปกรณ์ Log Analysis, Application Firewall, IPS เป็นต้น

10. กำหนดมาตรการในการควบคุมการใช้งานในระบบเครือข่ายสารสนเทศ รวมถึงเครือข่ายแบบไร้สาย ให้มีการใช้งานในระบบอย่างปลอดภัย คุ้มค่าและมีประสิทธิภาพมากที่สุด

11. มีการกำหนดหน่วยงานและผู้รับผิดชอบ รวมทั้งจัดทำระเบียบปฏิบัติ ในการดำเนินการ กรณีเกิดภัยคุกคามด้านไซเบอร์ รูปแบบการเตือนภัย ตามระดับของภัยคุกคาม รวมถึงมีการระวังป้องกันไม่ให้เกิดปัญหาขึ้นอีกในอนาคต ตามตารางที่ 4-1 ดังนี้

ตารางที่ 4-1 การกำหนดระดับของภัยคุกคามทางไซเบอร์

| ระดับภัยคุกคาม | ขอบเขตของผลกระทบ | ภัยคุกคามทางไซเบอร์ |
|---|---|---|
| 5. รัฐบาลแห่งชาติ ( National Governments ) | 4<br>3<br>2<br>1 | ระบบงานด้านความมั่นคงของประเทศหยุดทำงาน<br>ระบบสาธารณูปโภคของประเทศหยุดทำงาน<br>ระบบการเงิน การธนาคารหยุดทำงาน<br>สื่อมวลชน สถานีโทรทัศน์ หยุดทำงาน |
| 4.การก่อการร้าย (Terrorists) | 4<br>3<br>2<br>1 | ระบบงานด้านความมั่นคงของประเทศเสียหาย<br>ระบบสาธารณูปโภคบางส่วนเสียหาย<br>มีความพยายามโจมตีโรงงานไฟฟ้า<br>การโจมตี ทำลายข้อมูลของธนาคาร |
| 3.สายลับหรือพวกจารกรรมในภาคอุตสาหกรรม และกลุ่มองค์กรอาชญากรรมต่าง ( Industrial Spies and Organized Crime Groups ) | 2<br>1 | การขโมยข้อมูลที่เป็นความลับทางการค้า<br>การพยายามเจาะระบบของโรงงานอุตสาหกรรม |
| 2.กลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ ( Hacktivists ) | 3<br>2<br>1 | การพยายามเจาะข้อมูลหน่วยงานของรัฐบาล<br>การดักรับข้อมูล ดักฟังหน่วยงานของรัฐบาล<br>การ scan ข้อมูลเครือข่ายคอมพิวเตอร์หน่วยงานรัฐ |
| 1.กลุ่มแฮ็กเกอร์ ( Hackers ) | 3<br>2<br>1 | การเจาะข้อมูลองค์กรทั่วไป<br>การดักข้อมูลขององค์กรต่างๆ<br>การค้นหาช่องโหว่ของอุปกรณ์คอมพิวเตอร์ |

การปรับระดับของภัยคุกคาม

1. สามารถปรับข้ามระดับได้ ทั้งนี้ขึ้นอยู่กับความรุนแรง หรือผลกระทบที่ได้รับ
2. การปรับระดับขึ้นอยู่กับแผนหรือมาตรการที่ใช้ในการปฏิบัติการทางไซเบอร์

3. การกำหนดระดับเริ่มต้น อาจขึ้นอยู่กับโอกาสของความน่าจะเป็น และความถี่ของเหตุการณ์จะเกิด

4. การกำหนดระดับและการปรับระดับ เป็นไปตามสั่งการของผู้บังคับบัญชาโดยมีการมอบอำนาจในการสั่งการในแต่ละระดับว่า ผู้บังคับบัญชาระดับใด สามารถสั่งการให้ดำเนินการอย่างไรกับภัยคุกคามในระดับใด เนื่องจากภัยคุกคามจากไซเบอร์ บางกรณีไม่สามารถรอการตัดสินใจจากผู้บังคับบัญชาได้ บางครั้งต้องมีการปิดระบบโดยทันที เพื่อป้องกันผลกระทบที่ลุกลามไปอย่างรวดเร็ว

ระยะกลาง : (ปี 2559 - ปี 2561)

1. จัดทำระบบมาตรฐาน ด้านระบบรักษาความปลอดภัย (Security Standard) ตลอดจนศึกษามาตรฐานต่าง ๆ เช่น ISO/IEC 27001 และ ITIL ตลอดจน CoBIT เป็นต้น จากนั้นนำแนวทางจากมาตรฐานมาประยุกต์ใช้ในองค์กรให้สอดคล้องกับแนวคิด GRC (Governance Risk Compliance) เพื่อช่วยเสริมภาพลักษณ์และความน่าเชื่อถือให้กับระบบสารสนเทศของกองทัพ อีกทั้งยังสร้างความมั่นใจในด้านการบริการข้อมูลสารสนเทศ และการป้องกันทางไซเบอร์อีกด้วย

2. การจัดตั้งหน่วยงาน Army Computer Emergency Response Team ( Army CERT) หรือหน่วยงานทางด้านตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ของเหล่าทัพ พร้อมโครงข่ายการเชื่อมโยง แลกเปลี่ยนข้อมูลซึ่งกันและกัน

3. การจัดตั้ง Security Operation Center (SOC) ของเหล่าเหล่าทัพ เพื่อจัดหาระบบความมั่นคงภายใน ความปลอดภัยระดับสูง ทั้ง Hardware และ Software และจัดตั้งห้องปฏิบัติการระบบรักษาความปลอดภัยสารสนเทศเพื่อความมั่นคง และรองรับด้านไซเบอร์ด้วย

4.พิจารณาโครงสร้างในการบริหารจัดการด้านระบบรักษาความปลอดภัย สารสนเทศและด้านไซเบอร์โดยเฉพาะการแต่งตั้ง ผู้บริหารระดับสูงด้านนี้ เช่น Chief Security Officer (CSO), Chief of Cyber Command เป็นต้น

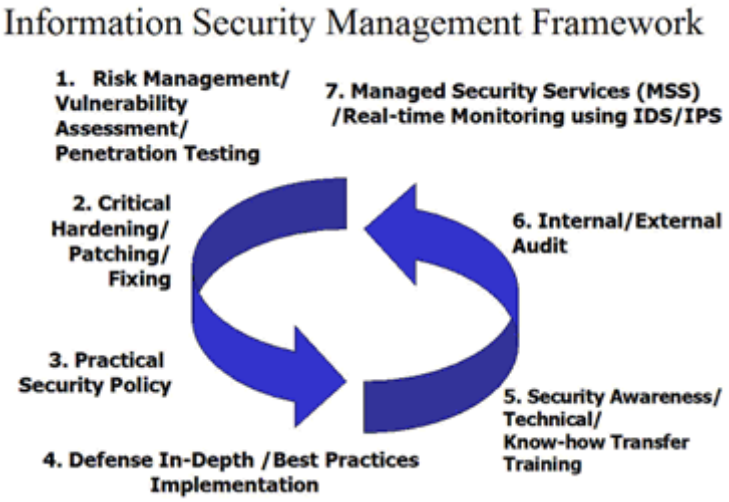
5. พัฒนาบุคคลากรระดับผู้เชี่ยวชาญ รวมถึงการพิจารณาผลตอบแทนที่ได้รับเพิ่มขึ้น ซึ่งควรจะสอดคล้องกับโครงสร้างใหม่ของกองทัพ ที่มีการแยกการทำงานด้านสายการบังคับบัญชาและด้านสายเทคนิค หรือผู้เชี่ยวชาญ แยกจากกันอย่างเด็ดขาด เพื่อการทำงานที่มี เอกภาพในการปฏิบัติต่อไป

ระยะยาว : (ปี 2561 - ปี 2563)

1. จัดตั้งทีมงานในหน่วยงานของกองทัพเอง ให้มีความเชี่ยวชาญ สามารถทำการทดสอบการเจาะข้อมูล (Hack) ของหน่วยงาน เอง เพื่อหาช่องโหว่ที่เกิดขึ้น เพื่อจะได้ดำเนินการ

แก้ไขได้ทันที นอกจากนั้นควรด้วยดำเนินการในเรื่องของ Information Security Management Framework (ISMF) 7 ขั้นตอน[2] ตามแผนภาพที่ 4-3

แผนภาพที่ 4-3 แผนภาพแสดง ของ Information Security Management Framework (ISMF)




การจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพโดยนำ ISMF มาใช้นั้น ควรปฏิบัติจาก ขั้นตอนที่ 1 ไปจนถึง ขั้นตอนที่ 7 จากการที่ได้ปฏิบัติตาม ISMF จนครบทั้ง 7 Steps เพื่อให้ได้ผล เราควรจะทำตาม ISMF ทุกๆ 3 เดือน หรือ ขั้นต่ำ 2 ครั้งต่อปี เพื่อเป็นหลักประกันความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ที่ กองทัพใช้งานอยู่ว่ามีความน่าเชื่อถือ และ ความมั่นคงต่อการโจมตีของของแฮ็กเกอร์ และไวรัสคอมพิวเตอร์ ที่มีอยู่มากมายในเวลานี้ และ เพื่อให้สอดคล้องกับหลักการ ICT Governance คือ การนำเทคโนโลยีสารสนเทศ (ICT) มาใช้ในการทำงานขององค์กรอย่างมีประสิทธิภาพและ ประสิทธิผล ทำให้เพิ่มความน่าเชื่อถือ ให้กับ หน่วยงานภายใน และสร้างความเชื่อถือต่อหน่วยงานภายนอก ให้เกิดความมั่นใจในระบบการรักษาความปลอดภัยข้อมูลของกองทัพ เพราะมีหลักการในการปฏิบัติอย่างจริงจัง และถูกต้องตามมาตรฐานสากล

---

[2] Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf1.htm, 2546.

ISMF นั้นได้นำเอาหลักการด้าน Information Security Policy ของมาตรฐานสากล ISO17799 ตลอดจน มาตรฐาน Cobit ของ ISACA (www.isaca.org) และ CBK (Common Body of Knowledge) ของ ISC2 (www.isc2.org) มาประยุกต์ใช้ให้ได้ประโยชน์สูงสุด และสามารถนำมาปฏิบัติได้จริงในสภาวะแวดล้อม ICT ในปัจจุบัน การดำเนินการเป็นขั้นตอนดังนี้

ขั้นตอนที่ 1 คือ "Risk Management, Vulnerability Assessment และ Penetration testing" สำหรับขั้นตอนที่ 1 จากทั้งหมด 7 ขั้นตอนนี้เป็นขั้นตอนแรกที่ต้องปฏิบัติและมีความสำคัญส่งผลกระทบไปยังขั้นตอนต่อ ๆ ไป โดยรวมเราเรียกขั้นตอนนี้ว่า "การวิเคราะห์ และประเมินความเสี่ยงของระบบ ICT" ขั้นตอนนี้ จะรวมถึงการ วิเคราะห์ตรวจหาช่องโหว่ในระบบ ที่เรียกว่า "Vulnerability Assessment" และ การทดสอบเจาะระบบเพื่อนำเอาข้อมูลที่สำคัญ เช่น Username และ Password ออกมาจากระบบโดยการทดลอง Hack (Ethical Hacking) เสมือนว่า มี Hacker เข้ามา เจาะระบบโดยเราเรียกขั้นตอนนี้ว่า "Penetration Testing" การทำ Penetration Testing นั้น จะรวมไปถึงการทดสอบความแข็งแกร่งของระบบโดยการจำลอง Attack แบบ "DoS Attack" หรือ Denial Of Services Attack เพื่อให้ระบบใช้งานไม่ได้ (ขั้นตอนนี้ต้องทำด้วยความระมัดระวังและควรแจ้งให้ผู้ใช้งาน ทราบก่อนล่วงหน้าจะได้มีการเตรียมตัวให้พร้อมกับการทดสอบ)

การทำ Penetration Testing นั้น แบ่งออกเป็น 2 ประเภทคือ Black-Box และ White-Box การทำ Black-Box Penetration Testing เป็นการเจาะระบบ โดยที่ผู้ที่รับจ้างเจาะระบบจะไม่ได้รับข้อมูลจากผู้ว่าจ้างนอกจากเป้าหมายที่เป็น Web Site หรือเป็น IP Address เท่านั้น ที่เหลือผู้รับจ้างต้องพยายามเจาะเข้ามาจาก Internet โดยใช้ความสามารถของผู้รับจ้างเอง การทดสอบเจาะระบบแบบ Black-Box Penetration Testing

มีข้อดี ก็คือ เราสามารถประเมินความแข็งแกร่งของระบบเราได้ จากภายนอกก็คือจากพวก Hacker ที่เจาะเข้ามาจากทาง Internet โดยตรง แต่ ข้อเสียก็คือผู้รับจ้างอาจจะไม่สามารถเจาะเข้ามาได้เพราะข้อมูลไม่เพียงพอ หรือ ความสามารถของผู้รับจ้างมีไม่มากพอที่จะเจาะเข้าสู่ระบบได้

แต่การเจาะระบบในแบบ White-box Penetration Testing นั้น จะเป็นการเจาะระบบที่ผู้รับจ้างจะต้องเข้ามาที่ Office และ On-line เข้าสู่ระบบ LAN หรือ Intranet ของผู้ว่าจ้าง เรียกว่าเป็นการเจาะจากข้างใน เพื่อเป็นการประเมินความเสี่ยงภายในองค์กร เช่น อาจจะมีผู้ใช้คอมพิวเตอร์บางคนติด Virus และ Virus สามารถแพร่กระจายใน LAN เราก็สามารถประเมินความเสียหายโดยผู้รับจ้างจะลองทดสอบ Penetrate ระบบโดยทำตัวเป็น Virus และพยายามเข้าสู่ระบบจากภายใน

ข้อดีของวิธีเจาะระบบแบบ White-Box Penetration Testing ก็คือ เราสามารถประเมินความเสี่ยงได้ใกล้เคียงกับสถานะ การณ์จริงมากกว่าแบบ Black-Box Penetration Testing เพราะผู้รับจ้างเจาะระบบ จะมีข้อมูลภายในมากกว่าแบบแรก แต่ข้อเสียก็คือ เราไม่สามารถประเมินจากภายนอกได้เหมือนแบบแรก

ในขั้นตอนที่ 2[3] จะเน้นไปที่การปิดช่องโหว่หรือการ “Harden” ระบบ ซึ่งเราเน้นไปที่ช่องโหว่ที่เป็นแบบ “High Risk” ก่อน เพราะมีผลกระทบกับระบบมากที่สุดหากเราละเลยไม่ปิดช่องโหว่เหล่านั้น หลักการในการ “Harden” ระบบนั้นหัวใจสำคัญก็คือไม่เปิดใช้บริการที่เราไม่มีความจำเป็นต้องใช้ เช่น ถ้าเราใช้เครื่องทำเป็น Web Server อย่างเดียว เราก็ควรเปิดใช้บริการเฉพาะพอร์ต 80 (http) และพอร์ต 443 (https) เท่านั้น แต่ปัญหาก็คือ เครื่องที่เรานำมาใช้งานเป็น Web Server นั้น ยกตัวอย่างเช่น Windows Platform มีการเปิดใช้งานบริการอื่นๆ โดยเป็นค่า “Default” มาจากการติดตั้งระบบในตอนแรก เช่น จะมีการเปิดพอร์ต TCP 135 ซึ่งเป็น RPC (Remote Procedure Call) Service เป็นผลให้ติด Virus Worm Blaster หรือ Nachi เป็นต้น นอกจากนี้ ยังเปิดพอร์ต TCP139 และ TCP/IP445 เป็นค่าโดยกำหนด ซึ่งเป็นการให้บริการ “File & Print Sharing” เช่นการ Map Network Drive เป็นต้น จะเห็นว่าไม่มีความจำเป็นต้องเปิดพอร์ตดังกล่าว ถ้าเรานำเครื่องมาใช้เป็น Web Server

ดังนั้นการ “Harden” ก็คือการปิดพอร์ตที่ผมได้กล่าวมาแล้วในตอนต้น วิธีการก็มีหลายวิธีเช่น การไป “Stop Service” ที่เราไม่มีความจำเป็นต้องใช้งาน หรือใช้ TCP Filter ซึ่งเป็นความสามารถที่ Windows NT/2000/2003 Server มีมาให้เราใช้งานอยู่แล้ว เรียกได้ว่าเป็น Firewall ให้กับเครื่องแบบไม่ต้องลงทุน บางท่านอาจจะใช้โปรแกรมประเภท Personal Firewall ในการป้องกันและตรวจจับ IP Address ของผู้บุกรุก หรือพวก Virus Worm ทั้งหลายก็จะช่วยได้อีกระดับหนึ่ง

การ “Harden” ที่ได้กล่าวมาแล้วเป็นการทำที่ตัว Host หรือ Server ที่เราใช้งานอยู่โดยตรง ไม่ได้เป็นการไปปิดพอร์ตหรือบริการต่างๆ ที่ Border Firewall หรือ Border Router ของระบบ ซึ่งการที่เราทำการปิดพอร์ตที่ตัวเครื่องโดยตรงจะทำให้เครื่องมีความปลอดภัย มากกว่าการปิดเฉพาะที่ Firewall หรือ Router ลักษณะการปิดพอร์ตเฉพาะที่ตัว Host หรือ Server เราเรียกว่าการทำเครื่องให้เป็น “Bastion Host” ที่มีความปลอดภัยสูงถึงแม้ Hacker จะเจาะผ่าน Firewall มาได้ก็ยังมาติดที่ตัวเครื่องอยู่ดี การใช้งาน Border Firewall หรือ Border Router ACL (Access Control

---

[3] Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf2.htm, 2546.

List) ในการปิดช่องโหว่นั้นก็เป็นสิ่งจำเป็นที่ยังต้องทำอยู่ เพราะจะเป็นการผ่อนหนักให้เป็นเบา โดยการ Harden เสริมที่ตัวเครื่อง จะทำให้เกิดความปลอดภัยมากขึ้น

สำหรับการ “Patch” หรือการลง “Hotfix” ให้กับระบบนั้น ก็เป็นสิ่งจำเป็นที่ต้องทำ นอกเหนือจากการปิดบริการหรือพอร์ตที่เราไม่ได้ใช้ งานเช่นกัน เพราะบริการที่เราใช้อยู่เช่น พอร์ต 80 ที่เปิดบริการ Web Server นั้น อาจจะมีช่องโหว่ที่ตัว Web Server เอง และเราก็จำเป็นต้องเปิดใช้บริการ ดังนั้น เราจึงต้องมีการติดตามลง “Patch” หรือโปรแกรมแก้ไขช่องโหว่ที่เกิดขึ้นในระบบ ซึ่งช่องโหว่ของระบบโดยทั่วไปจะเกิดขึ้นทุกเดือน (ดูข้อมูลได้ที่ www.cert.org หรือ www.securityfocus.com) เราจึงต้องคอยติดตามข่าวช่องโหว่ใหม่ๆ และเข้าไป Download “Patch”, “Service Pack” หรือ “Hotfix” มาลงในเครื่องของเราให้ปลอดจากช่องโหว่ที่มีการค้นพบกันทุกเดือน ยกตัวอย่างถ้าใช้ Windows Platform อยู่ ให้ไปดูที่ www.microsoft.com/securityเป็นต้น

จะเห็นได้ว่าการ Harden ระบบนั้น ไม่ใช่ทำเสร็จแล้วจะจบเลย การ Harden ครั้งแรกจนระบบปลอดจากช่องโหว่นั้นเราเรียกว่า “Get Secure” แต่ปัญหาก็คือ เราจะทำอย่างไรให้ “Stay Secure” นั่นคือ เราต้องคอยติดตามข่าวสารช่องโหว่ใหม่ๆ รายเดือน บางทีอาจเป็นรายสัปดาห์หรือรายวันก็มี และเราต้องคอยลง Patch, Horfix ตลอดจน Service Pack ต่างๆ ที่จะออกมาเป็นระยะๆ เพื่อให้ระบบของเรามีความปลอดภัยอยู่เสมอ

ขั้นตอนที่ 3[4] คือ "Practical Information Security Policy" ซึ่งเป็นขั้นตอนที่มีความสำคัญกับกองทัพอย่างมากในการจัดการกับระบบรักษา ความปลอดภัยข้อมูลคอมพิวเตอร์อย่างได้ประสิทธิผลในการปฏิบัติจริง เพราะหากองค์กรไม่มีการกำหนด "นโยบายการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตอย่างปลอดภัย" ก็จะทำให้ระบบยังคงมีปัญหาได้ อาทิ ระบบติดไวรัส, แฮกเกอร์ใช้ Trojan Horse เจาะเข้าระบบจากความผิดพลาดของผู้ใช้งาน (User) ที่โดนแฮกเกอร์ใช้เทคนิค "Social Engineering" เจาะเข้ามา เป็นต้น ไม่ว่าเราจะติดตั้ง Firewall, IDS ตลอดจน Anti Virus Software อย่างเต็มระบบแค่ไหน ก็เป็นเพียงการป้องกันในระดับเทคนิค (Technical Level) เท่านั้น เรายังขาดการป้องกันในระดับบริหารจัดการ (Administrative Level) ซึ่งหมายถึงเรื่อง Policy , Standard, Guideline และ Procedure ที่ต้องถูกนำมาใช้เป็นนโยบายใน การปฏิบัติของผู้ใช้ IT ในองค์กร ตามแผนภาพที่ 4-4

---

[4] Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf3.htm, 2546.

แผนภาพที่ 4-4 แผนภาพแสดง Access Control Layers


โดยปกติแล้วองค์กรมักจะนิยมเขียนนโยบายด้านความปลอดภัยข้อมูลคอมพิวเตอร์โดยอิงจากมาตรฐาน BS ISO/IEC 17799:2000 ตามแผนภาพที่ 4-5 ซึ่งประกอบไปด้วยหัวข้อต่างๆ 10 เรื่อง โดยเน้นในรูปของภาพรวมไม่เจาะลึกด้านปฏิบัติ

แผนภาพที่ 4-5 แผนภาพแสดง BS ISO/IEC 17799:2000 Structure


ดังนั้นในบางองค์กรเช่น ธนาคารหรือสถาบันการเงิน อาจนำหลักการด้านนโยบายจากหน่วยงานอื่นที่ไม่ใช่ ISO มาเป็นต้นแบบก็ได้ เช่น มาตรฐาน CobiT (Control Objectives for Information and Related Technology) Framework ของ สถาบัน IT Governance Institute (www.itgi.org) ซึ่งเน้นในการตรวจสอบโดยผู้ตรวจสอบด้าน Information System โดยตรงคือ CISA (Certified Information System Auditor) ที่ได้รับการรับรองจากสถาบัน ISACA

(www.isaca.org) ซึ่งเป็นผู้ที่ช่วยกำหนดมาตฐานในการตรวจสอบ (Audit) ระบบ Information System ตามขั้นตอนและอ้างอิงมาตรฐาน CobiT

นอกจาก BS ISO/IEC 17799:2000 และ CobiT แล้วก็ยังมีแนวทางการกำหนดนโยบาย ด้านการรักษาความปลอดภัยระบบ คอมพิวเตอร์อีกจาก 2 หน่วยงานที่มีบทบาทสำคัญและเน้นการนำไปใช้งานจริง กล่าวคือ เป็น Information Security Policy ที่ได้รับการขัดเกลาและประยุกต์แล้ว ได้แก่ CBK (Common Body of Knowledge) ตามแผนภาพที่ 4-6 จาก ISC2.org และ SANS/FBI Top 20 ของ SANS Institute ซึ่งร่วมมือกับ FBI (รายละเอียดเพิ่มเติมที่ www.sans.org/top20)

แผนภาพที่ 4-6 แผนภาพแสดง CISSP CBK (Common Body of Knowledge)


CBK นั้น เป็นองค์ความรู้ที่ สำคัญ และ จำเป็น ในการกำหนดนโยบายด้านความปลอดภัยระบบข้อมูลคอมพิวเตอร์ คิดค้นขึ้นโดยสถาบัน (ISC)2 (www.isc2.org) ผู้ที่ต้องการศึกษาอย่างลึกซึ้ง ควรลองเข้าไปสอบ CISSP (Certified Information Systems Security Professional) ซึ่งเป็นใบรับรอง (Certificate) ที่จะทำให้เรามีความเข้าใจลึกซึ้งใน CBK ทั้ง 10 โดเมน มากขึ้นและสามารถนำมาใช้ในภาคปฏิบัติกับองค์กรของเราได้อย่างดี

ส่วน SANS/FBI Top 20 Vulnerabilities นั้นเหมาะสำหรับผู้ดูแลระบบหรือ System Administrator ที่จะนำไปใช้กับ Platform ที่ตนเองดูแลอยู่ ได้แก่ UNIX Platform Top 10 Vulnerabilities และ Windows Platform Top 10 Vulnerabilities

ความหมายของ Policy หมายถึง นโยบายในภาพรวมที่กระชับและได้ใจความ เรียกว่า "Goal" หรือ เป้าหมายที่เราต้องการบรรลุ , Standard หมายถึง มาตรฐานที่ต้องบังคับในการปฏิบัติจริง เช่น รหัสผ่านต้องมีความยาวไม่ต่ำกว่า 8 ตัวอักษร เป็นต้น , Guideline หมายถึง แนวทางในการปฏิบัติที่ไม่ได้บังคับ แต่แนะนำเพื่อให้ผู้ปฏิบัติให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น และ Procedure หมายถึง รายละเอียดปลีกย่อยเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่ง Standard ที่ได้วางไว้ ตามแผนภาพที่ 4-7

แผนภาพที่ 4-7 แผนภาพแสดง Policy, Standards, Guidelines, And Procedures


การกำหนดรายละเอียดของนโยบายด้านการรักษาความปลอดภัยระบบข้อมูลคอมพิวเตอร์ จึงต้องประกอบไปด้วย 4 ส่วนหลักๆ นี้ใน การพัฒนารายละเอียดต่างๆ ในนโยบาย ซึ่งนโยบายของแต่ละองค์กรอาจจะไม่เหมือนกัน ขึ้นกับการทำงานด้าน Information System ขององค์กรนั้นๆ อาทิ พฤติกรรมของผู้ใช้งาน, ทิศทางของผู้บริหารระดับสูงด้าน Information System หรือ Platform ที่เลือกใช้ อาจต้องมีการกำหนด "Best Practices" ให้กับ Platform ที่เราใช้อยู่โยเฉพาะ เช่นเราใช้ "Apache" เป็น Web Server อยู่เราก็ใช้ "Best Practices"

สำหรับ Web Server Apache โดยเฉพาะ ซึ่งก็จะมีรายละเอียดและข้อกำหนดต่างๆ ที่เราสามารถนำไปจัดการใช้กับ Web Server ได้ในทางปฏิบัติ

จะเห็นได้ว่า เราไม่สามารถนำ Information Security Policy จากสถาบันต่างๆ ดังได้กล่าวมาแล้วทั้ง 4 สถาบัน มาใช้งานได้ทันที เนื่องจาก เราต้องมีการประเมินสถานการณ์ความเสี่ยงขององค์กรเราเสียก่อน ซึ่งก็คือขั้นตอนที่ 1 ของ ISMF (Risk Management / Vulnerability Assessment / Penetration Testing) นั่นเอง หากปราศจากขั้นตอนนี้ แล้วเรามาทำนโยบายก่อน จะทำให้เราขาดข้อมูลประกอบการตัดสินใจในการกำหนดนโยบายให้ใช้งานได้จริง เพราะฉะนั้น การกำหนดนโยบายต้องทำภายหลังจากการประเมินความเสี่ยงแล้ว

ปัญหาใหญ่ๆ อีกอย่างหนึ่งสำหรับองค์กรที่มีนโยบายที่ดีและได้ลงทุนลงแรงไปมากกับการพัฒนานโยบายความปลอดภัยข้อมูล คอมพิวเตอร์ หน่วยงานบางแห่งใช้เวลามากกว่า 2 ปีในการทำงานนโยบาย แต่กลับพบว่าเมื่อได้คลอดนโยบายออกมาเป็นรูปธรรม เพื่อให้คน IT ในองค์กรได้ปฏิบัติ แล้ว ผลลัพธ์ออกมาไม่เป็นอย่างที่คาดหวังไว้ เพราะหลายๆ คนไม่ยอมทำตามนโยบาย บางคนอ่านแล้วไม่เข้าใจ บอกว่าศัพท์เทคนิคมากเกินไป บางคนบอกว่าไม่ตรงกับงานที่รับผิดชอบอยู่นำมาใช้งานจริงไม่ได้ เป็นต้น ทางแก้ปัญหาที่ถูกต้องคือ ต้องมีการทำ Security Awareness Training ให้กับผู้ใช้ IT เสียก่อน ตั้งแต่ระดับผู้บริหารกระทั่งถึง ระดับผู้ใช้ทั่วไป เพื่อให้มีความตระหนักถึงภัยจากการใช้งานอินเทอร์เน็ตอย่างไม่ระมัดระวังและไม่ถูกต้อง

ขั้นตอนที่ 4[5] ได้แก่ "Defense-In-Depth" และ "Best Practices Implementation" เป็นขั้นตอนที่ใช้เวลานานและมีผลกับองค์กรในระยะยาว ดังนั้น ขั้นตอนนี้จึงเป็นขั้นตอนที่ค่อนข้างละเอียดและต้องการกำลังคนและเวลาในการปฏิบัติ ตลอดจนความรู้เชิงลึกในด้าน Information Security เพื่อทำให้ระบบขององค์กรมีความปลอดภัยทั้งในปัจจุบันและอนาคต เรียกได้ว่าเป็นการจัดการ Information Security แบบบูรณาการ

คำว่า 'Defense-In-Depth" นั้นเน้นการจัดการแบบ "Layered Security" คือมีการป้องกันระบบเป็นชั้น ๆ เปรียบเสมือนมีประตูหลายชั้นก่อนจะเข้าถึงตัวระบบได้ และมีการแบ่งระบบออกเป็นหลายส่วน ในทางเทคนิคเราเรียกว่า "Compartmentalization" เช่น การทำ VLAN แยกระบบที่สำคัญออกจากกัน หรือการแบ่ง DMZ (Demilitarized Zone) ออกเป็นหลาย ๆ DMZ

---

[5] Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf4.htm, 2546.

เช่น Web Sever ไม่ควรอยู่กับ Mail Server ใน DMZ เดียวกัน หรือ Primary DNS ไม่ควรอยู่กับ Secondary DNS ใน DMZ เดียวกันเป็นต้น เพื่อที่จะป้องกันในกรณีที่ Hacker เจาะ Server หรือ Host ใด Host หนึ่งใน DMZ สำเร็จ Hacker ก็จะเจาะ Host ที่อยู่ในบริเวณ DMZ เดียวกันได้ง่าย แต่ถ้าเราแบ่งระบบออกเป็น "หลายชั้น/หลายส่วน" Hacker ก็ต้องใช้ความพยายามมากขึ้นที่จะ "Compromised" หรือ "Hacked" ระบบของเราทั้งหมด

หัวข้อสำคัญที่เราต้องพิจารณาเวลานำยุทธศาสตร์ "Defense-In-Depth" มาใช้ประกอบไปด้วย 5 หัวข้อดังนี้

1. "Re-Design Network Perimeter Architectures" / "ออกแบบระบบป้องกันอย่างรัดกุมและให้ความปลอดภัยสูงสุด" หมายถึง ในกรณีที่มีการใช้สถาปัตยกรรมป้องกันระบบ (Network Perimeter Architecture) แบบเดิมอยู่แล้วให้พิจารณาอย่างละเอียดว่า มีการออกแบบที่ได้ความปลอดภัยสูงสุดแล้วหรือยัง เช่น ภายใน DMZ เดียวกันมีทั้ง Web Server, Applications Server และ Database Server แม้จะอยู่หลัง Firewall ถ้า Hacker เจาะ Web Server ได้ก็มีโอกาสที่จะเจาะ Applications Server และ Database Serverได้อย่างไม่ยากนัก ดังนั้นเราควรแยกออกเป็น 3 ส่วนคือ แยก Applications Server ออกจาก Zone ของ Web Server และแยก Database Server ไปอยู่ใน Zone เฉพาะของ Database Server เท่านั้น เพราะข้อมูลที่อยู่ใน Database Server นั้น ถือเป็นข้อมูลที่มีผลกระทบกับองค์กรอย่างมาก และมีความสำคัญกว่าข้อมูลที่อยู่ใน Web Server หาก Hacker เจาะ Web Server ได้ ข้อมูลใน Database Server ก็ยังไม่มีผลกระทบในทันที Hacker จะต้องใช้ความพยายามในการเจาะผ่านเข้าสู่ DMZ ของ Database Server อีกทีหนึ่งเป็นต้น

จะเห็นว่าสถาปัตยกรรมที่ใช้หลักการ "Defense-In-Depth" นั้นจะต้องใช้งบประมาณในการติดตั้งและออกแบบระบบค่อนข้างสูงกว่าสถาปัตยกรรมแบบปกติ แต่ก็ให้ผลลัพธ์ที่น่าพอใจในมุมมองของความปลอดภัยข้อมูล

2. "In-Depth Host and Network Devices Hardening"/"ปรับแต่ง Host และ Network Devices ให้มีช่องโหว่น้อยที่สุดเท่าที่จะทำได้" หมายถึง การป้องกันที่ Firewall อย่างเดียวคงไม่เพียงพอ การป้องกันที่ดีที่สุดคือทำในระดับ Host หรือ Network Devices โดยตรงเลย การปิดช่องโหว่ตลอดจน การลง Patch/Hot Fix ให้กับ Host หรือ Network Devices นั้น เป็นเรื่องจำเป็นที่ต้องทำอย่างต่อเนื่องและทำ อย่างเป็นระบบ เพราะช่องโหว่ (Vulnerability) ของระบบนั้น มีให้เห็นในอินเทอร์เน็ตเป็นประจำทุกเดือน

3. "Change Management/Log Monitoring" / "การจัดการกับความเปลี่ยนแปลง" "Change Management" นั้นถือเป็นเรื่องสำคัญที่อยู่ใน ISMF ขั้นตอนที่ 4 เพราะถ้ามีการเปลี่ยนแปลงเกิดขึ้นในระบบ เราก็ควรที่จะบันทึก Event ลง Audit Trail (Audit Log) เพื่อสามารถ

นำมาตรวจสอบหรือ ทำ "Forensics" ในภายหลังได้ ปัญหาที่เราพบเป็นประจำก็คือ เราไม่ค่อยได้บันทึกความเปลี่ยนแปลงที่เกิดขึ้นในระบบทำให้เราไม่สามารถที่จะตรวจสอบหรือ "Audit" ระบบได้อย่างมีประสิทธิภาพ ดังนั้น "Change Management" เป็นเรื่องที่ไม่สามารถที่จะมองข้ามได้เลย

การใช้ Software จัดการกับ "Integrity" ของระบบ เช่น TripWire ว่านับเป็นความคิดที่ดีในการทำ "Change Management" ตลอดจนการใช้ Software ประเภท "Application Firewall" เช่น URLScan/IISLockDown ของ Microsoft หรือ SecureIIS ของ Eeye ก็เป็นวิธีที่สามารถป้องกันระบบในเชิงลึกได้ดีเช่นกัน การติดตั้ง IDS (Intrusion Detection Systems) และ การจัดการกับ Log อย่างเป็นระบบ (Centralized Logging Systems) ก็เป็นสิ่งที่แนะนำให้ทำให้หัวข้อนี้เช่นกัน

4. "Securing your Database and Web Application"/"จัดการระบบความปลอดภัยใน Web Application และ Database Server ในเชิงลึก" หมายถึง หากเราเขียน Source Code เช่น ASP หรือ PHP ของ Web Application โดยไม่ระมัดระวัง เรามีโอกาสที่จะถูก Hacker เจาะระบบผ่านทาง Port 80 หรือ Web Application Security Hacking โดย Firewall และ IDS ไม่สามารถที่จะป้องกันได้เลย

การใช้ SSL กับ Web Server นั้นก็ไม่สามารถที่จะป้องกัน Hacker ได้ 100% Hacker ที่ใช้วิธี Hack แบบ "Man-In-The Middle Attack" สามารถ Hijack SSL Session ของเราได้ ดังนั้นวิธีการป้องกันที่ดีที่สุดก็คือ ต้องให้ Web Programmers มี "Awareness" เรื่องความปลอดภัยของ Web Application เสียก่อน เช่น สอนให้รู้เรื่อง Session ID Hacking, Cookies Hijacking, SSL Hackings SQL injection, Cross-Site Scripting ตลอดจนช่องโหว่ต่าง ๆ ทั้ง 10 ข้อของ Web Application จาก OWASP www.owasp.org (Open Web Application Security Project) สำหรับ Database Server ไม่ว่าเราจะใช้ Oracle, IBM DB2, Microsoft SQL Server หรือ Open Source MySQL เราก็ต้องคำนึงถึงช่องโหว่ (Vulnerability) และค่าโดยกำหนด (Default Parameter) ต่าง ๆ ที่มากับตัว Database ที่ทำให้เกิดช่องโหว่ เราควรทำ "Presentation Testing" จาก ISMF ในขั้นตอนที่หนึ่ง และดำเนินการปิดช่องโหว่ในขั้นตอนนี้โดยละเอียด

5. "Thinking on Business Continuity Planning/Disaster Recovery Planning"/ "แผนกู้ระบบฉุกเฉินและแผนการจัดการกับความเสียหายของระบบสารสนเทศโดยไม่ให้กระทบกับธุรกิจ" หมายถึง เราต้องคำนึงในความจริงว่าไม่มีระบบใดที่ปลอดภัย 100% สักวันหนึ่งระบบของเราก็อาจจะถูก Hack และเกิดความเสียหายให้กับธุรกิจ ดังนั้น เราควรเตรียมแผนสำรองฉุกเฉินและดำเนินการกู้ระบบให้เร็วที่สุด (Minimized Downtime) เพื่อให้ผลเสียจากการถูก Hacker มา Compromised (Hacked) ระบบ มีผลกระทบน้อยที่สุดกับธุรกิจ DRP (Disaster Recovery Planning) นั้นเป็นแผนกู้ระบบฉุกเฉินขณะที่ BCP เป็นแผนใหญ่ที่ใช้ในการจัดการกับความปลอดภัยของระบบในระยะยาวเพื่อทำให้ระบบมี Availability ได้ตาม SLA (Services Level Agreement) ที่ฝ่าย

IT ต้องทำให้ผู้ใช้คอมพิวเตอร์ตลอดจนผู้บริหารมีความพอใจในระดับหนึ่ง และ ทำให้องค์กรนำ IT มาใช้งานได้อย่างมีประสิทธิภาพ

ส่วนของ "Best Practices" นั้นเป็นส่วนหนึ่งของหลักการ "IT Governance Implementation" กล่าวคือ "Best Practices" นั้น หมายถึง การนำเอาสูตรสำเร็จ หรือ ตัวอย่างการ Implement ที่ดีมาจัดการกับระบบของเรา เช่น ถ้าเราใช้ Microsoft IIS 5.0 เป็น Web Server อยู่ เราก็ควรนำ "IIS 5.0 Best Practices" มาใช้เป็นหลักการในการติดตั้งและตรวจสอบ Web Server ของเรา ซึ่ง "Best Practices" จะประกอบไปด้วยรายละเอียดทางด้านเทคนิคของ Microsoft IIS 5.0 ที่เราควรนำมาปฏิบัติ ตั้งแต่การติดตั้งไปจนถึงการใช้งานรายวันว่าเราควรพิจารณาปิดช่องโหว่ในส่วนใดบ้าง เช่น การจัดการกับค่าโดยกำหนด (Default) ต่างๆ และ การลบไฟล์ตัวอย่าง (Examples Files) ที่ไม่จำเป็นต้องใช้งาน เป็นต้น

ขั้นตอนที่ 5[6] นั้น กล่าวถึง การฝึกอบรมความรู้ความเข้าใจด้านการรักษาความปลอดภัยข้อมูลให้กับ ผู้บริหารตลอดจนพนักงานให้มีความเข้าใจและมีความตระหนักให้ระวังภัยจากการใช้งานคอมพิวเตอร์โดยเฉพาะอินเทอร์เน็ตโดยไม่ระมัดระวังเพียงพอ ซึ่งอาจก่อให้เกิดความเสียหายกับองค์กรได้โดยไม่รู้ตัว

ขั้นตอนนี้เป็นขั้นตอนที่หลายๆคนมองข้าม และมองว่าควรจะมีการฝึกอบรมเฉพาะฝ่าย IT และฝ่าย Security แต่ในความเป็นจริงแล้ว ผู้บริหารระดับสูง และ ระดับกลาง ตลอดจนพนักงานที่ใช้งานคอมพิวเตอร์ในองค์กร ก็มีความจำเป็นที่จะต้องถูกฝึกอบรม "Security Awareness Training" ด้วยเช่นกัน เพราะการแก้ปัญหาด้านความปลอดภัยเครือข่าย โดยเฉพาะปัญหา "Virus Computer" ซึ่งนับวันจะทวีความรุนแรงมากขึ้นเรื่อยๆ เช่น อาจมีพนักงานบางคนหมุนโทรศัพท์โดยใช้ Local Modem ที่อยู่ในเครื่อง Notebook ต่อเข้าอินเตอร์เน็ต ขณะที่ตนเองใช้ระบบ LAN ของบริษัทอยู่ ทำให้ Virus สามารถแพร่เข้าสู่ระบบ Internal LAN ของบริษัทได้อย่างง่ายดาย หรือผู้บริหารอาจใช้ Notebook ที่บ้านและติด Virus มาจากการเล่นอินเตอร์เน็ต จากนั้นก็นำ Notebook ดังกล่าวมาใช้ในระบบ Internal LAN ขององค์กรก็เท่ากับว่า ผู้บริหารท่านนั้นนำ Virus มาแพร่ภายในองค์กรโดยไม่รู้ตัว เป็นต้น

---

[6] Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf6.htm, 2546.

ดังนั้น วิธีการที่จะทำให้ระบบมีความปลอดภัยจาก Virus ดังกล่าว นอกจากการติดตั้งโปรแกรมประเภท Anti-virus แล้วก็คือ การฝึกอบรมให้ผู้บริหารและพนักงานที่ใช้คอมพิวเตอร์ในการทำงานเป็นประจำทุกวันรู้เท่าทันถึงภัยจากการใช้งานอินเตอร์เน็ตและเครือข่ายโดยไม่ระมัดระวัง วิธีการก็คือ การฝึกอบรมต้องมีการแสดงกรณีตัวอย่าง หรือ Case Study ให้ผู้เข้ารับการอบรมเห็นว่า Hacker และ Virus มีวิธีการในการโจมตีเราได้อย่างไร เมื่อทุกคนได้เห็นตัวอย่างแล้วก็จะเกิดความตระหนักได้ด้วยตนเองว่า จากนี้ต้องใช้งานเครือข่ายและอินเทอร์เน็ตด้วยความระมัดระวังมากขึ้นโดยไม่ต้องมีฝ่าย IT คอยบังคับหรือคอยบอกโดยไม่เข้าใจว่าทำไมต้องทำตามคำแนะนำของฝ่าย IT เช่น เมื่อฝ่าย IT แนะนำให้ใช้ Personal Firewall ส่วนใหญ่แล้วผู้ใช้คอมพิวเตอร์ทั่วไปก็มักจะรำคาญหรือไม่เข้าใจประโยชน์จากการติดตั้ง Personal Firewall ในเครื่องของตนเอง บางคนขอให้ฝ่าย IT ช่วยเอาโปรแกรม Personal Firewall ออกจากเครื่องก็มี

จะเห็นว่า "Security Awareness Training" เป็นเครื่องสำคัญที่ถูกมองข้ามและถูกเข้าใจผิดว่าเป็นเรื่องที่ทำเฉพาะฝ่าย IT เท่านั้น แต่ในความเป็นจริงต้องมีการฝึกอบรมเป็นประจำทุกปีและควรฝึกอบรมให้ครบ 6 กลุ่มดังนี้

กลุ่มที่ 1 ผู้บริหารระดับสูง (Top Management)
กลุ่มที่ 2 ผู้บริหารระดับกลาง (Middle Management)

การฝึกอบรม "Security Awareness Training" ให้กับผู้บริหารระดับสูงนั้นควรจะเป็นเรื่องความเสี่ยงที่มีอยู่ในอินเทอร์เน็ตทุกวันนี้ (Information Security Risk), โอกาสที่จะเกิดความเสียหายขึ้นจากการจู่โจมของ Hacker หรือ Virus Computer, ความจำเป็นที่ระบบต้องมีการควบคุมด้วย "Control" เช่น การติดตั้ง Enterprise Firewall และ Intrusion Detection System ตลอดจนการติดตั้ง Personal Firewall และ Anti-Virus ในทุก workstation การฝึกอบรมควรใช้ระยะเวลาสั้นๆ ไม่เกิน 3 ชั่วโมงและไม่ควรใช้ศัพท์เทคนิคมากเกินไป

ผลที่ได้จากการฝึกอบรมผู้บริหารจะทำให้ผู้บริหารมีความเข้าใจเรื่อง Information Security มากขึ้น และมีผลอย่างมากกับองค์กร เนื่องจากผู้บริหารจะให้ความสนับสนุนฝ่าย IT มากยิ่งขึ้น หลังจากที่ได้ทำความเข้าใจกับปัญหาทางด้านความปลอดภัยคอมพิวเตอร์หลังจากการฝึกอบรมแล้ว

กลุ่มที่ 3 กลุ่มผู้ดูแลระบบ (System Administrators)
กลุ่มที่ 4 กลุ่มผู้ดูแลความปลอดภัยคอมพิวเตอร์โดยตรง (Security Administrators)

กลุ่มที่ 5 กลุ่มผู้ตรวจสอบระบบสารสนเทศ (IT Auditors)

การฝึกอบรมทั้ง 3 กลุ่มนี้ควรเน้นเนื้อหาทางด้านเทคนิคเพิ่มขึ้นจากการฝึกอบรมผู้บริหาร และควรมีกรณีศึกษา (Security Incident case study) ของระบบต่างๆ และ แสดงให้เห็นถึงวิธีการโจมตีของ Hacker และ Virus ตลอดจน วิธีการป้องกันที่ถูกต้องและมีประสิทธิภาพ โดยอาจมีรายละเอียดและระยะเวลาในแต่ละกลุ่มแตกต่างกัน ตั้งแต่ 6 ชั่วโมง จนถึง 30 ชั่วโมง ในกรณีที่ต้องการให้มีความเข้าใจมากขึ้น ควรมี "Hand-on" ให้ผู้เข้าอบรมได้ใช้คอมพิวเตอร์ฝึกปฏิบัติในห้องเรียนด้วย (ซึ่งการอบรมในกลุ่มที่ 1 และ 2 ไม่จำเป็นต้องให้ผู้เข้าอบรมใช้คอมพิวเตอร์ก็ได้)

กลุ่มที่ 6 กลุ่มผู้ใช้งานคอมพิวเตอร์ทั่วไป (Users)

กลุ่มนี้เป็นกลุ่มที่มีความเสี่ยงสูงที่จะปล่อย Virus เข้าสู่ระบบโดยไม่รู้ตัว พอๆ กับกลุ่มที่ 1 และ 2 เนื่องจากไม่มีความรู้พื้นฐานทางเทคนิคเพียงพอ ดังนั้น การฝึกอบรมต้องแสดงให้เห็นถึงการใช้งานคอมพิวเตอร์รายวันที่ผู้ใช้ต้องใช้คอมพิวเตอร์ในการทำงานของตนเองเป็นประจำอยู่แล้ว เช่น การเข้าไปหาข้อมูลใน Web site และ การรับ-ส่ง e-Mail การฝึกอบรมควรจะแสดงให้เห็นถึงภัยต่าง ๆ จากการเข้า Web site ที่ไม่เหมาะสม หรือ การถูกโปรแกรม Spy Ware ประเภท Key Logger มาฝังในเครื่องโดยผ่านทาง Attached file ที่มากับ e-Mail การใช้งานอินเทอร์เน็ตโดยไม่มี Personal Firewall ก็เป็นอีกปัญหาหนึ่งของผู้ใช้งานโดยทั่วไปที่ต้องเน้นในการฝึกอบรมเช่นกัน

หลังจากการฝึกอบรม "Security Awareness Training" และการฝึกอบรม "Technical Know-how Transfer Training" ในเชิงลึกด้านเทคนิคแล้ว จะทำให้ทั้ง 6 กลุ่มซึ่งก็คือพนักงานทุกคนในองค์กร มีความเข้าใจเรื่องภัยจากอินเทอร์เน็ตรวมทั้งวิธีการป้องกันตนเองและองค์กรให้พ้นภัยจากเหล่า Hacker และ Virus ได้ดียิ่งขึ้น ส่งผลให้ระบบมีความปลอดภัยและมีเสถียรภาพเพิ่มมากขึ้น ฝ่าย IT ก็ทำงานง่ายขึ้นด้วย เพราะฉะนั้นโปรแกรมนี้ควรถูกบรรจุเข้าไว้ใน IT Master Plan ขององค์กรและควรเตรียมงบประมาณไว้ให้เพียงพอสำหรับค่าใช้จ่ายด้านการฝึกอบรมในแต่ละปีด้วย เพื่อที่องค์กรของเราจะได้ลดปัญหาทางด้านความปลอดภัยคอมพิวเตอร์ลงไม่ให้มีผลกระทบรุนแรงอย่างเช่นในทุกวันนี้

ขั้นตอนที่ 6[7] จะเน้นเรื่องการ "ตรวจสอบ" หรือ "IT Auditing" ซึ่งเป็นส่วนหนึ่งของแนวคิด "IT Governance" ที่องค์กรสมัยใหม่นิยมนำมาประยุกต์ใช้ หลังจากที่เราได้ทำการประเมินความเสี่ยงของระบบและปิดช่องโหว่ของระบบแล้ว เราจะทราบได้อย่างไรว่าช่องโหว่ที่มีผลกระทบกับระบบได้ถูกจัดการแก้ไขอย่างถูกต้อง ดังนั้น เราจึงต้องทำการตรวจสอบซ้ำเป็นครั้งที่ 2 การตรวจสอบทำโดยการทำ Re-Assessment รายละเอียดเหมือน ISMF ขั้นตอนที่ 1 แต่จะสรุปผลออกมาในภาพรวมมากขึ้น โดยมีการเปรียบเทียบกับผลจากขั้นตอนที่ 1 ก่อนที่เราจะ "Hardening" หรือ ปิดช่องโหว่ในขั้นตอนที่ 2 เราจะได้ความแตกต่างจาก "GAP Analysis" แสดงให้เห็นถึงผล "ก่อน Hardening" และ "หลัง Hardening" ว่ามีความแตกต่างกันอย่างไร ถ้าการ Hardening ยังไม่สมบูรณ์ก็ต้องมีการ Re-Hardening อีกครั้งเพื่อให้แน่ใจว่าได้ปิดช่องโหว่จนความเสี่ยงอยู่ระดับที่ยอมรับได้ (Risk Acceptance Level) การตรวจสอบระบบนั้นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) ควรมี "Compliance Checklist" เพื่อนำไปตรวจสอบระบบต่างๆ และนำผลลัพธ์มาทำ "GAP Analysis" ว่าระบบที่ใช้อยู่นั้นได้มีการจัดการด้านระบบรักษาความปลอดภัยเป็นไปตาม "IT Security Policy" ขององค์กรหรือไม่และได้ทำตาม "Best Practices" ที่เหมาะสมกับระบบนั้นๆ แล้วหรือยัง

หลักการในการตรวจสอบระบบสารสนเทศที่ถูกต้องก็คือ ต้องมีการประเมินความเสี่ยง (Risk Assessment) ขององค์กรเสียก่อน ซึ่งมีขั้นตอนสำคัญที่ต้องปฏิบัติ เช่น การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยง และ การระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Identification), การวิเคราะห์ความเสี่ยง (Risk Analysis) และการบริหารจัดการกับความเสี่ยง (Risk Management)

การตรวจสอบระบบสารสนเทศต้องพิจารณาเรื่องของ Control หรือ การควบคุม ว่าได้มีการจัดการอย่างถูกต้องหรือไม่ การตรวจสอบการควบคุมแบ่งออกเป็น 3 ประเภทใหญ่ๆ คือ

1. การควบคุมแบบป้องกันล่วงหน้า (Preventive Control)
2. การควบคุมแบบค้นหาประวัติเหตุการณ์ที่เกิดขึ้น (Detective Control)
3. การควบคุมแบบแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้น (Corrective Control)

IT Auditor ควรจะพิจารณาการควบคุม (Control) ไปพร้อมๆกันทั้ง 3 มุมมอง ได้แก่

1. มุมมองทางด้านการบริหารจัดการ (Administrative Control)

---

[7] Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf6.htm, 2546.

2. มุมมองทางด้านเทคนิค (Technical Control)

3. มุมมองทางด้านกายภาพ (Physical Control)

IT Auditor ต้องมีความรู้ความเข้าใจในขั้นตอนกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Process) ตลอดจนมีความรู้ด้านเทคนิคเชิงลึก (IT Audit Technical Know-how) ในระบบที่ต้องเข้าไปตรวจสอบ เราสามารถแบ่งประเภทของงานตรวจสอบระบบสารสนเทศออกเป็น 7 ประเภทใหญ่ๆ ดังนี้

1. การตรวจสอบระบบปฏิบัติการ (NOS Audit) เช่น การตรวจสอบระบบ Server ที่ใช้ MS Windows เช่น Windows NT, Window 2000 Server ตลอดจน Workstation ที่ใช้ Windows XP เป็นต้น การตรวจสอบควรจะครอบคลุมถึงระบบปฏิบัติการอื่นด้วย เช่น การตรวจสอบระบบปฏิบัติการ Unix เช่น Sun Solaris, HP/UX, IBM AIX และ ระบบปฏิบัติการ Linux ที่ได้รับความนิยมเพิ่มขึ้นเรื่อยๆ

2. การตรวจสอบอุปกรณ์เครือข่าย (Network Devices Audit) เช่น การตรวจสอบ Router, การตรวจสอบ Switching และ การตรวจสอบ Remote Access Server ตลอดจน การตรวจสอบโครงสร้างของเครือข่าย (Network Infrastructure Audit) และ ประสิทธิภาพของเครือข่าย (Network Performance Audit) โดยใช้โปรแกรมตรวจสอบประเภท Packet Sniffer หรือ RMON Probe เป็นต้น

3. การตรวจสอบอุปกรณ์รักษาความปลอดภัย (Security Devices Audit) เช่น การตรวจสอบ Firewall, การตรวจสอบ Intrusion Detection System (IDS), การตรวจสอบ Intrusion Prevention System (IPS), การตรวจสอบโปรแกรม Enterprise Anti-Virus, การตรวจสอบ VPN Server เป็นต้น การตรวจสอบอุปกรณ์รักษาความปลอดภัยนั้นเป็นสิ่งที่มีความจำเป็นอย่างสูง เพราะถ้าอุปกรณ์รักษาความปลอดภัยมีปัญหาเสียเอง หรือโดน Hacker เจาะเข้ามา compromised ก็จะทำให้เกิดปัญหากับความปลอดภัยของระบบโดยรวม ผู้ตรวจสอบควรเป็นผู้ชำนาญงานด้านการใช้งาน Firewall หรือ IDS/IPS มาก่อนด้วยจะช่วยได้มาก

4. การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit) เช่น การตรวจสอบ Oracle, IBM DB2, Microsoft SQL Server, Informix, SYBASE หรือ MySQL RDBMS การตรวจสอบโปรแกรมฐานข้อมูลควรกระทำควบคู่ไปกับการตรวจสอบระบบปฏิบัติการที่โปรแกรมฐานข้อมูลทำงานอยู่ เช่น Oracle ทำงานบน Unix เป็นต้น เพื่อที่จะเจาะลึกลงไปในด้านความปลอดภัยของตัวโปรแกรมฐานข้อมูลเองว่ามีช่องโหว่หรือไม่ ผู้ตรวจสอบควรเป็นผู้เชี่ยวชาญการใช้งานโปรแกรมฐานข้อมูลนั้นๆมาก่อน เพราะการตรวจสอบต้องใช้ความรู้เชิงลึกทางด้าน RDBMS ด้วย

5. การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะ Server

(Application Specific Audit) เช่น การตรวจสอบ Web Server IIS บน Microsoft Windows Platform และ การตรวจสอบ Web Server Apache บน Unix/Linux Platform ซึ่งทั้ง 2เป็นโปรแกรม Web Server ยอดนิยมอยู่ในขณะนี้ นอกจากการตรวจสอบ Web Server แล้ว IT Auditor ควรตรวจสอบ Mail Server, FTP Server, LDAP Server, RADIUS Server ตลอดจน DNS Server ซึ่งถือเป็นหัวใจหลักของระบบ หาก DNS Server มีปัญหาจะทำให้ระบบไม่สามารถอ้างอิง Hostname ได้ ซึ่งจะก่อให้เกิดปัญหาใหญ่กับระบบโดยรวม

6. การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control) จากข้อ 1 ถึง ข้อ 5 เป็นการตรวจสอบในมุมมองทางด้านเทคนิค (Technical Control) การตรวจสอบในมุมมองการบริหารจัดการนั้น ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่าครอบคลุม และ มีการปฏิบัติตามหรือไม่ ในขั้นตอนนี้รวมถึงการตรวจสอบว่าองค์กรมีการจัดฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) หรือไม่ ซึ่งตามปกติควรจะ มีเป็นประจำทุกปี การตรวจสอบการบริหารจัดการนั้นต้องพิจารณาจากโครงสร้างหน่วยงาน, การแบ่งแยกหน้าที่ต่างๆในหน่วยงาน, การจัดทำแผนสำรองฉุกเฉิน และแผนรับเหตุการณ์ (Business Continuity Planning, Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management)

7. การตรวจสอบด้านกายภาพ (Physical Control) ได้แก่ การตรวจสอบระบบควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์, การตรวจสอบ Hardware ระบบ Backup/Restore และ ระบบไฟสำรอง เช่น มี UPS เพียงพอหรือไม่ การตรวจสอบอุปกรณ์เฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) เป็นต้น

ISMF ขั้นตอนที่ 6 นั้นเป็นขั้นตอนที่สำคัญและต้องการบุคลากร IT Auditor ที่มีประสบการณ์และมีความรู้จริงในการตรวจสอบระบบ เพื่อให้ผลจากการตรวจสอบเข้าใกล้ความเป็นจริงมากที่สุด เพราะปัญหาส่วนใหญ่ในการตรวจสอบระบบสารสนเทศ ก็คือ IT Auditor ยังขาดประสบการณ์เพราะความรู้ เทคนิคยังไม่ลึกพอที่จะเข้าไปตรวจสอบระบบ เช่น

- ความรู้ด้าน Vulnerability Assessment และ Penetration Testing ในลักษณะ Ethical Hacking หรือ White Hat Hacking
- ความรู้พื้นฐานทางด้านเครือข่าย เช่น ISO OSI Layer Model, TCP/IP Protocol Suite
- ความรู้การใช้งานระบบปฏิบัติการพื้นฐาน คือ Microsoft Windows และ Unix/Linux

- ความรู้พื้นฐานในการใช้งานอุปกรณ์เครือข่าย Router หรือ Switching ซึ่ง IT Auditor ควรมีความรู้พื้นฐานในระดับ CCNA (Cisco Certified Network Associate)

- ความรู้ทางด้านความปลอดภัยข้อมูล เช่น Concept ของ CIA TRIAD (Confidentiality, Integrity and Availability), การทำงานของ Firewall และ IDS ในบริเวณ Network Perimeter ขององค์กร ตลอดจนวิธีการบุกรุกของ Hacker และ การทำงานของ Virus

ดังนั้น IT Auditor ควรจะมี CISA Certification เพื่อแสดงถึงความรู้ในด้าน IT Audit Process แล้ว ก็ควรจะมีความรู้พื้นฐานทางด้านเทคนิคด้วย ทั้งด้านระบบเครือข่ายและระบบปฏิบัติการที่ตนเองต้องเข้าไปตรวจสอบ ทางแก้ปัญหาในเชิงบูรณาการก็คือ IT Auditor ต้องเข้ารับการฝึกอบรมทางด้านเทคนิคเพิ่มเติม หรือ หาความรู้เพิ่มด้วยตนเองจากการติดตามข่าวสารเทคโนโลยีด้านความปลอดภัยใหม่ๆอยู่ตลอดเวลา เพื่อให้ทันกับยุคที่การสื่อสารไร้พรมแดน และภัยอินเตอร์เน็ต ไม่ว่าจะเป็น Hacker และ Virus ที่นับวันจะทวีความรุนแรงมากขึ้น ในโลกยุค Digital ที่มีความเปลี่ยนแปลงอยู่ตลอดเวลา

ขั้นตอนที่ 7[8] "Managed Security Services (MSS) / Real-time Monitoring using IDS/IPS" หลังจากที่เราได้จัดการกับระบบความปลอดภัยข้อมูลคอมพิวเตอร์อย่างเป็นขั้นตอนด้วย Information Security Management Framework (ISMF) จาก ISMF ขั้นตอนที่ 1 จนถึง ISMF ขั้นตอนที่ 6 แล้วนั้น เราพบว่าช่องโหว่ของระบบที่ถูกค้นพบขึ้นใหม่ (New Vulnerability) เกิดขึ้นอยู่ตลอดเวลา เพราะทางกลุ่ม Black Hat Hacker มีความพยายามในการทำ Research & Development (R&D) เพื่อที่จะค้นพบช่องโหว่ใหม่ๆ ของระบบปฏิบัติการหรือโปรแกรมประยุกต์ที่เรานิยมใช้ เมื่อบรรดา Black Hat Hacker หรือ Hacker ฝ่ายอธรรมได้ค้นพบช่องโหว่ใหม่ๆ ก็จะมีการรายงานผ่านทาง Security Web Site ต่างๆ ที่เกี่ยวข้องกับด้าน Vulnerability Report เช่น www.securityfocus.com จากนั้นก็จะมีการพัฒนาโปรแกรมที่ใช้ในการเจาะช่องโหว่ที่เพิ่งถูกค้นพบ ซึ่งเราเรียกว่า "Exploit"

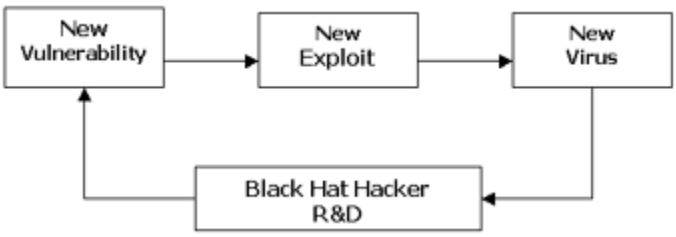
Exploit ส่วนใหญ่จะเป็น Secure Code โปรแกรมภาษา C ที่สามารถทำงานได้บน Linux Platform และหลังจากที่ Exploit ถูก Upload ให้บรรดา Black Hat Hacker ได้ลองใช้งานกัน สักระยะหนึ่งก็จะมีพัฒนาการต่อเป็น Virus ออกมา และ Virus ก็จะพัฒนาเป็น Version ต่างๆ เช่น

---

[8] Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf8.htm, 2546.

Bagle.A, Bagle.B, Bagle.H, Bagle.Q ไปเรื่อยๆ จนกว่าบริษัทที่ผลิต Anti-Virus จะตรวจพบ เป็นไปตามแผนภาพที่ 4-8

แผนภาพที่ 4-8 แสดงภาพวงจรการพัฒนา Exploit/Virus ของ Black Hat Hacker




ดังนั้นแม้ว่าเราจะจัดการกับระบบความปลอดภัยข้อมูลคอมพิวเตอร์ตามขั้นตอน ISMF จาก 1 ถึง 6 แล้ว เมื่อเวลาผ่านไประบบก็มีโอกาสที่จะเกิด Vulnerability ใหม่ๆ อยู่ตลอดเวลา และ เราก็ต้องคอยตามลง Patch หรือ Hotfix ต่างๆ ให้กับระบบอย่างทันท่วงที เรียกว่า วัดกันที่ความเร็วว่าใครจะรู้ข่าวก่อนกัน ถ้าเรารู้ข่าวช่องโหว่ใหม่ แล้วรีบทำการปิดช่องโหว่เสียก่อนโอกาสที่จะติด Virus หรือโดน Hack ก็จะน้อยลง แต่ถ้าเราละเลยไม่สนใจข่าวสารเรื่องการค้นพบ Vulnerability ใหม่ๆ หรือรู้ข่าวแต่ยังนิ่งนอนใจไม่ลง Patch ให้กับระบบ โอกาสที่จะถูกจู่โจมโดย Hacker หรือ Virus ก็จะมีมากขึ้น

จากปัญหาข้างต้น เราพบว่าเมื่อเวลาผ่านไป เราต้องกลับไปทำ ISMF ในขั้นตอนทั้ง 6 อีกเป็นระยะๆ เรียกว่าเป็น "Continuous Process" ที่หยุดไม่ได้ ดังนั้นเราจึงต้องคอยศึกษาและติดตามข้อมูลข่าวสารด้าน Information Security อยู่ตลอดเวลา ซึ่งต้องเสียทั้งกำลังคนและทรัพยากรต่างๆ ในองค์กรพอสมควร ตลอดจนต้องมีการเฝ้าระวังการจู่โจมจาก Hacker หรือ Virus โดยระบบ IDS/IPS และ ยังต้องมีเจ้าหน้าที่ดูแลวิเคราะห์ Log และ สถานการณ์ต่างๆ ที่เกิดขึ้นจากอุปกรณ์ IDS/IPS ตลอดจน Firewall Log, Network Device Log และ Host Log เช่น Windows 2000 Log หรือ Unix/Linux SysLog เป็นต้น

การเฝ้าระวังโดยการวิเคราะห์ Log ด้วยบุคลากรภายในองค์กรของเราเองนั้น นอกจากจะใช้เวลาค่อนข้างมากแล้วยังต้องการผู้เชี่ยวชาญที่แยกแยะระหว่าง Fault Alarm กับ Real Attack Alarm ซึ่งผู้เชี่ยวชาญต้องมีความชำนาญเป็นพิเศษด้านการวิเคราะห์การบุกรุกระบบ (Intrusion Analyst) ตลอดจนในปัจจุบันค่าตัวของบุคลากรที่มีความเชี่ยวชาญดังกล่าวก็ค่อนข้างสูงอยู่พอสมควร

จากปัญหาดังกล่าวจึงเกิดแนวคิดในการ "Outsource" ด้านการจัดการระบบรักษาความปลอดภัยซึ่งเรียกว่า "Managed Security Services" หรือ "MSS" การจัดจ้าง Outsource ด้าน Security โดยเฉพาะ เป็นแนวคิดที่ต้องการให้ Outsource มาช่วยในการจัดการบริหารความเสี่ยง และ ช่วยลดความเสี่ยงให้กับระบบโดยรวม (Risk Management & Risk Mitigation)

บริษัทที่ให้บริการ Outsource Security เราเรียกว่า MSSP หรือ Managed Security Service Provider ควรมีการให้บริการครอบคลุมในหัวข้อต่างๆ ดังนี้

1. บริหารจัดการ และ เฝ้าระวัง (Managing and Monitoring) Network Perimeter Security ที่ External Firewall, Border Router, IDS/IPS, VPN ตลอดจน Server ในบริเวณ DMZ

2. บริหารจัดการ Vulnerability ให้กับระบบขององค์กรอย่างต่อเนื่อง เช่น การทำ Vulnerability Assessment และ Penetration Testing รายเดือน เป็นต้น

3. เฝ้าระวัง Internal Network จาก Virus และ Hacker ตลอดจน Internal Firewall and Server Farm ภายในระบบ LAN ขององค์กร

4. รับปรึกษาปัญหาเวลาเกิด Security Breach Incident, รับแก้ปัญหาในลักษณะ Incident Response และ Digital Forensic

5. บริหารจัดการ Centralized Log Management และ Centralized Patch Management อย่างเป็นระบบ

6. บริการแจ้งข่าวสารความเคลื่อนไหวด้าน Information Security โดยเฉพาะเรื่อง New Vulnerability/Exploit และ New Virus ให้ทราบในลักษณะวันต่อวัน (Day by Day report)

การเลือก MSSP จึงเป็นหัวใจสำคัญ สำหรับผู้บริหารระบบต้องมีการกำหนด SLA (Services Level Agreement) ให้ชัดเจนใน RFP (Request for Proposal) โดยควรมีรายละเอียดให้มากที่สุดเท่าที่จะทำได้ เช่น ขอบเขตในการให้บริการของ MSSP, ระยะเวลาในการให้บริการ และการตอบสนองของ MSSP, ค่าใช้จ่ายที่เกิดขึ้นในแต่ละเดือน ตลอดจนความรับผิดชอบของ MSSP ในแง่กฎหมายและบทปรับหาก MSSP ปฏิบัติไม่ได้ตาม SLA ที่ได้ตกลงกันไว้ใน Contact เป็นต้น

การ Outsource Security นั้นจะช่วยลดต้นทุนให้กับองค์กรในด้านของอัตรากำลังของบุคลากรผู้เชี่ยวชาญ ตลอดจน Hardware และ Software ต่างๆ ที่ลงทุนโดย MSSP และ องค์กรยังได้รับข่าวสารใหม่ๆ ด้าน Information Security เช่น การค้นพบ Vulnerability และ Virus ใหม่ๆ เพื่อที่องค์กรจะได้เตรียมตัวรับความเสี่ยงที่อาจเกิดขึ้น นอกจากนี้ MSSP ควรจะมีผู้เชี่ยวชาญ หรือ Security Expert คอยให้คำปรึกษา และ คอยเตือนภัยทางอินเตอร์เน็ตให้องค์กรทราบอยู่ตลอดเวลา

สำหรับปัญหาจากการ Outsource Security ที่เราควรคำนึงถึงก็มีเช่นกัน กล่าวคือ ถ้าสัญญาที่ทำกับ MSSP ไม่รัดกุมพอก็จะทำให้เกิดปัญหาในการปฏิบัติได้ ตลอดจนปัญหาในการ

เลือก MSSP ที่ไม่มีความเชี่ยวชาญเพียงพอก็อาจทำให้ไม่คุ้มค่าในการลงทุนกับการ Outsource Security ในกรณีที่เกิดปัญหาแล้ว MSSP ไม่สามารถแนะนำหรือให้คำปรึกษาได้ตามที่องค์กรคาดหวังว่าจะได้รับจาก MSSP เป็นต้น

กล่าวสรุปโดยรวม ข้อดีในการจ้าง MSSP ก็ยังมีมากกว่าข้อเสียที่ได้กล่าวมาแล้ว การตกลงทำงานร่วมกันกับ MSSP ในลักษณะที่ช่วยเหลือซึ่งกันและกัน โดยงานที่เป็นลักษณะที่ต้องใช้ความสามารถเฉพาะทางก็มอบให้ MSSP เป็นผู้จัดการให้ ส่วนองค์กรมีหน้าที่ในการ Audit ตรวจสอบ MSSP ว่ามีการปฏิบัติตาม SLA หรือไม่ จะทำให้ไม่เกิดปัญหาในระยะยาวจากการจัดจ้าง MSSP และ เป็นการบริหารความเสี่ยงด้าน IT ที่ถูกหลักการเป็นไปตามยุคสมัยของความนิยมในเรื่อง "IT Outsourcing"

2. การบริหารจัดการระบบอย่างสมบูรณ์ (Security Management) ซึ่งต้องสอดคล้องกับโครงสร้างในการทำงานที่เหมาะสม มีผู้บริหารที่รับผิดชอบโดยตรง มีอำนาจในการตัดสินใจได้ในทุกเรื่องที่เกี่ยวข้องกับความมั่นคงด้านไซเบอร์

3.จัดตั้งหน่วยงานดูแลด้านการปฏิบัติการไซเบอร์หรือหน่วยงานที่เป็นศูนย์บัญชาการไซเบอร์ในระดับกระทรวงกลาโหม ขึ้นตรงกับ รัฐมนตรีว่าการกระทรวงกลาโหม เพื่อให้มีขีดความสามารถ ในการดำเนินการตามนโยบายได้อย่างเป็นรูปธรรม

# บทที่ 5
# สรุป และข้อเสนอแนะ

## สรุป

บทเรียนในเรื่องของสงครามไซเบอร์ สงครามไซเบอร์ที่เกิดขึ้นครั้งแรกใน ปี 2550 ประเทศเอสโตเนีย ถูกโจมตีด้วยไซเบอร์ เป้าหมายอยู่ที่ รัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่าง ๆ จนทำให้ข้อมูลเสียหาย จากการกระทำของฝ่ายข้าม ซึ่งมีความเชื่อว่าเป็นการโจมตีมาจาก กลุ่มแฮกเกอร์ของรัสเซีย หลังจากนั้นก็มีสงครามไซเบอร์เกิดขึ้นตามมาอย่างต่อเนื่อง

แนวคิดของสงครามไซเบอร์ในต่างประเทศ โดยเฉพาะทางประเทศสหรัฐอเมริกา จากคู่มือปฏิบัติการภาคสนามของสหรัฐ FM 11-45 ได้กล่าวถึง การปฏิบัติการด้าน Cyber Defense ของ สหรัฐฯ ซึ่งมุ่งเน้นไปที่การปฏิบัติ การป้องกัน, เฝ้าตรวจ, วิเคราะห์, ปกป้อง และ ตอบโต้ ตลอดจนการป้องกันระบบข่าวสาร ( Information Assurance - IA ) ซึ่งเป็นมาตรการป้องกันภัยคุกคามที่จะเกิดขึ้น ซึ่งมีองค์ประกอบที่สำคัญในด้านต่างๆ ดังนี้ 1. ความสามารถในการป้องกันภายในหน่วย 2. ความสามารถในการกลั่นกรองภัยคุกคาม 3. ความสามารถในการตอบโต้ภัยคุกคามที่เกิดขึ้น

นอกจากนั้น ยังมีการกำหนดระบบเครือข่ายที่มีความปลอดภัยเรียกว่า การปฏิบัติการเครือข่ายของสหรัฐฯ (เน็ตออป/NETOPS) เป็นการสร้างเครือข่าย การปฏิบัติงาน ที่มีการเชื่อมโยงในสายการบังคับบัญชา ทั้งหน่วยเหนือ หน่วยรอง ตลอดจนถึงผู้ปฏิบัติ มีการจัดให้มีเทคโนโลยีสารสนเทศและการเฝ้าระวัง, การติดตามสถานการณ์, การปกป้องการไหลของข้อมูลข่าวสาร , และการบริหารจัดการเครือข่าย, การสนธิ IA(Information Assurance) และการบริหารด้านการกระจายข้อมูลข่าวสาร เป็นทั้งเครื่องมือ และแนวความคิด ในการปฏิบัติ สำหรับการบริหารระบบสื่อสารและสารสนเทศของกองทัพบกสหรัฐฯ

แนวคิดในการจัดตั้งหน่วยงานไซเบอร์ในต่างประเทศ จากประเทศสหรัฐอมเริกา ได้กำหนดนโยบายจากประธาธิบดีฯ อนุมัติคำสั่งประธานาธิบดี ในประเด็นเรื่องการพัฒนาความปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยมอบหมายให้ กระทรวงความมั่นคงแห่งมาตุภูมิ เป็นแกนหลักในการทำงานด้านไซเบอร์

หน่วยงานทางทหารที่สำคัญ ได้แก่ หน่วยงานไซเบอร์คอมแมนด์ (US CYBERCOM) เป็นกองบัญชาการรบร่วมระดับรอง (sub-unified command) โดยจะขึ้นตรงกับสตราทีจิกคอมแมนด์ (USSTRATCOM) สำหรับไซเบอร์คอมแมนด์ มีหน้าที่หลัก คือ การปกป้องระบบเครือข่ายที่ฝ่ายทหารเป็นผู้รับผิดชอบ ในขณะที่ระบบเครือข่ายของรัฐบาลฝ่ายพลเรือนนั้นจะเป็นหน้าที่ของกระทรวงโฮมแลนด์ซีเคียวลิตี้

การรองรับสงครามไซเบอร์ในปัจจุบัน นั้นควรมีข้อพิจารณาถึงปัญหาและผลกระทบทางด้านสงครามไซเบอร์ ซึ่งในทางสากลได้กำหนดระดับภัยคุกคามทางด้านไซเบอร์ ออกเป็นระดับดังนี้ ภัยคุกคามในระดับรัฐบาลแห่งชาติ ( National Governments ) ภัยคุกคามในระดับการก่อการร้าย ( Terrorists ) สายลับหรือพวกจารกรรมในภาคอุตสาหกรรม และกลุ่มองค์กรอาชญากรรมต่าง ๆ ( Industrial Spies and Organized Crime Groups ) กลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ ( Hacktivists ) และ กลุ่มแฮ็กเกอร์ ( Hackers )

ยุทธศาสตร์และแนวทางการรองรับสงครามไซเบอร์ที่มีอยู่เดิมของประเทศ ในเรื่องนี้มีเพียง คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ( National Cyber Security Committee : NCSC ) โดยมีนายกรัฐมนตรีเป็นประธาน ซึ่งเป็นยุทธศาสตร์หลักในปัจจุบัน นอกจากในระดับรัฐบาลแล้ว ในระดับกระทรวง ที่สำคัญอย่าง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดตั้งหน่วยงานต่างๆ ได้แก่ ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ ( Cyber Security Operation Center : CSOC ) , ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) หรือ ThaiCERT และ อื่นๆ เป็นต้น

สำหรับในระดับกระทรวงกลาโหม มีการจัดตั้ง ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ (ศรค.) และ การเสนอร่างศูนย์ปฏิบัติการไซเบอร์กลาโหม ส่วนในกองบัญชาการกองทัพไทย นั้นเริ่มดำเนินการเสนอโครงสร้างของหน่วยงานใหม่ที่เรียกว่า กองปฏิบัติการสงครามเครือข่าย ในระดับเหล่าทัพต่างๆ กองทัพบก กองทัพเรือ กองทัพอากาศ ก็ยังอยู่ในระหว่างการปรับปรุงโครงสร้างหน่วยงานใหม่เพื่อรองรับสงครามไซเบอร์ในอนาคตต่อไป

ขอบเขตของการรองรับสงครามไซเบอร์ ในกรอบมุมมองของกองทัพ สามารถกำหนดขอบเขตได้ตามระดับของภัยคุกคามดังนี้ 1.ระดับประเทศ ในระดับนี้ความรับผิดชอบ ไม่แต่เพียงหน่วยงานด้านความมั่นคง หรือกองทัพ แต่ควรเป็นทุกภาคส่วนทั้งภาครัฐและภาคเอกชน มีส่วนร่วมในการป้องกันภัยภัยคุกคามทางไซเบอร์ 2.ระดับการก่อการร้าย และอาชญากรรมต่างๆ ความรับผิดชอบของกองทัพ ยังคงใช้การเฝ้าระวัง และแจ้งเตือน มีการทำงานที่สอดคล้องกัน และเป็นส่วนหนึ่งของเครือข่ายในระดับประเทศ 3. ระดับแฮ็กเกอร์ ความรับผิดชอบของกองทัพยังคงใช้การเฝ้าระวัง และแจ้งเตือน และสร้างเครือข่ายภายในกองทัพเอง ตลอดจนการดำเนินการ

สร้างความตระหนัก และกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดปลอดภัยในระบบของกองทัพ

แนวทางการรองรับสงครามไซเบอร์ในอนาคต กองทัพมีการประเมินภัยคุกคามของสงครามไซเบอร์ ในส่วนของกองทัพเอง ซึ่งภัยคุกคามดังกล่าว กองทัพได้ให้ความสำคัญ ด้วยกัน 4 ด้าน ได้แก่ 1 . ภัยคุกคาม ที่ส่งผลต่อความมั่นคงของประเทศ 2. ภัยคุกคาม ที่ส่งผลกระทบต่อสามจังหวัดชายแดนภาคใต้( จชต. ) 3.ภัยคุกคาม ที่ส่งผลกระทบต่อ สถาบันฯ 4. ภัยคุกคาม ที่ส่งผลกระทบต่อ ภาพลักษณ์ของ กองทัพ และได้กำหนดกรอบในการดำเนินการทางด้านสงครามไซเบอร์ ของกองทัพไทย เพื่อรองรับสงครามไซเบอร์ในอนาคต ออกเป็น 4 ด้านดังนี้ ด้านนโยบาย ด้านความรู้ ด้านโครงสร้างองค์กร และ ด้านการปฏิบัติงาน

นอกจากนั้น ยังมีการกำหนดกรอบระยะเวลาในการดำเนินการทางด้านสงครามไซเบอร์ แบ่งออกเป็น 3 ระยะ ระยะแรก : (ปี 2557 - ปี 2559) ระยะกลาง : (ปี 2559 - ปี 2561) และระยะยาว : (ปี 2561 - ปี 2563)

ในที่สุดแล้วสิ่งท้าทายในอนาคตต่อภัยคุกคามทางด้านไซเบอร์นับวันมีแต่จะเพิ่มปริมาณมากขึ้น จนกระทั้งถ้าหากว่ามีการเกิดความขัดแย้งกันในระดับประเทศ ก็อาจจะยกระดับไปสู่การทำสงครามไซเบอร์ ขึ้น สิ่งต่างๆ เหล่านี้ล้วนแล้วเป็นสิ่งที่อาจจะเกิดขึ้นหรือไม่เกิดขึ้นก็ย่อมได้ แต่เราในฐานะกองทัพของชาติ ซึ่งมีความรับผิดชอบด้านความมั่นคงปลอดภัยของชาติ จะต้องคำนึงถึงบทบาททางด้านไซเบอร์ เพิ่มเติมจากการรบในรูปแบบปกติ ถึงแม้ว่าการทำสงครามไซเบอร์ อาวุธต่างๆ ที่ใช้ล้วนแล้วแต่จับต้องไม่ได้ กองทัพต้องมีความพยายามที่จะต้องสร้างความเข้าใจ และเข้าถึงเทคโนโลยีสมัยใหม่ ตลอดจนกฎหมาย ระเบียบวิธี การปฏิบัติการรบ ต้องเปลี่ยนแปลง ไปตามสิ่งที่กองทัพต่อเผชิญหน้ากับข้าศึกที่มองไม่เห็นในอนาคตนั่นเอง

สำหรับรัฐบาลได้มีนโยบายที่จะให้หน่วยต่าง ๆ ได้มีการพัฒนาโครงสร้างของหน่วยงานต่าง ๆ รวมทั้งกองทัพ ปรับปรุงให้รองรับงานทางด้านไซเบอร์มากขึ้น และหลายหน่วยงานในกองทัพกำลังพยายามดำเนินการอยู่ แต่ก็ถือได้ว่า เป็นเพียงจุดเริ่มต้นเท่านั้น หากว่าการปรับปรุงโครงสร้างไม่ควรมองแค่ในด้านของอัตรากองทัพ หรือการขยายอัตราเป็นหลัก แต่ควรคำนึงถึงสิ่งที่เป็นกระบวนการทำงาน ที่รองรับด้านสงครามไซเบอร์ได้อย่างแท้จริงอีกด้วย

หน่วยต่าง ๆ ที่มีการพัฒนา และส่งเสริม ด้านการรักษาความปลอดภัยทางคอมพิวเตอร์หลายหน่วยงานล้วนแล้วแต่กองทัพ จะต้องมีการประสานความร่วมมือ แลกเปลี่ยน ประสบการณ์ตลอดจนการขอรับการสนับสนุนการให้องค์ความรู้แก่องค์กรของกองทัพ ซึ่งจะเป็นประโยชน์ทั้งด้านการประสานความร่วมมือแล้ว ยังได้ประโยชน์ในด้านประหยัดงบประมาณอีกด้วย

ทางผู้วิจัยได้เสนอแนวความคิดในของการรองรับทางงานด้านไซเบอร์ในอนาคต โดยหลักการแล้ว จะมุ่งเน้นในด้านการปฏิบัติการเชิงรับ หรือการป้องกันไซเบอร์เป็นหลัก ซึ่งการปฏิบัติการเชิงรุกนั้น ในสภาวะปกติ การกระทำดังกล่าวอาจจะต้องระมัดระวัง หรือเข้าใจข้อกฎหมายหรืออำนาจในการดำเนินการด้วย

## ข้อเสนอแนะ

สำหรับความคิดเห็นด้านโครงสร้างของของหน่วยงานทางด้านไซเบอร์ของกองทัพ ซึ่งนอกจากแต่ละหน่วยงานกำลังพยายามดำเนินการในปัจจุบัน ผู้วิจัยมีแนวคิดในเรื่องโครงสร้างหน่วยสงครามไซเบอร์ ดังกล่าว ดังนี้

ภารกิจของหน่วยมีดังนี้

1. ภารกิจในภาพรวมของหน่วยคือการปฏิบัติการสงครามไซเบอร์โดยแยกการดำเนินการออกได้เป็น 2 รูปแบบ ได้แก่ (1) การปฏิบัติการสงครามไซเบอร์ในฐานะเป็นงานสนับสนุนการรบหลัก ซึ่งมีการปฏิบัติการในเชิงรุก และเชิงรับ (2) การปฏิบัติการสงครามไซเบอร์ในฐานะเป็นฝ่ายเทคนิคหรือผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของกองทัพ

2. สำหรับโครงสร้างของหน่วยประกอบไปด้วย

2.1 ส่วนบัญชาการ/บังคับการ ประกอบไปด้วย ผู้บังคับบัญชา ส่วนอำนวยการและวางแผน ส่วนการจัดการบุคลากร ส่วนฝึกอบรมและทดสอบ เป็นส่วนงานที่ควบคุมการปฏิบัติการทั้งในงานสนับสนุนการรบ และในงานสายงานผู้เชี่ยวชาญ ในภาพรวม

2.2 ส่วนปฏิบัติการรักษาความปลอดภัยไซเบอร์และ ประกันข้อมูลข่าวสารสำหรับในส่วนนี้ถือว่าเป็นการปฏิบัติการสงครามไซเบอร์ ในฐานะผู้เชี่ยวชาญด้านการรักษาความปลอดภัย งานที่ปฏิบัติเป็นเรื่องของการจัดทำนโยบายความปลอดภัย การทดสอบช่องโหว่ การจัดทำการบริหารความเสี่ยงของทรัพย์สินของกองทัพ ตลอดจนการสนับสนุนผู้เชี่ยวชาญในด้านการรักษาความปลอดภัยและประกันข้อมูลข่าวสาร

2.3 ส่วนปฏิบัติการสงครามไซเบอร์ ประกอบไปด้วยทั้งเชิงรุก และเชิงรับ ทางด้านไซเบอร์ เช่น งานเฝ้าระวังทางไซเบอร์ งานแจ้งเตือนเหตุการณ์ที่กระทบด้านไซเบอร์ สนับสนุนการเจาะข้อมูลทางไซเบอร์ ตลอดจนการฝึกและสนับสนุนกำลังพลที่มีขีดความสามารถในด้านการปฏิบัติการไซเบอร์

# บรรณานุกรม

## ภาษาไทย

### หนังสือ


คลาร์ก ริชาร์ด เอ. สงครามไซเบอร์-Cyber War . แปลโดยนาย ไพรัตน์ พงศ์พานิชย์. กรุงเทพฯ : มติชน, 2555. หน้า 37.

เดวิด ลีห์, ลุค ฮาร์ดิ้ง. Wikileaks ความลับเขย่าโลก. แปลโดยศิริพงษ์ วิทยวิโรจน์. กรุงเทพฯ: สำนักพิมพ์มติชน, 2556. หน้า 9.


### ฐานข้อมูลอิเล็กทรอนิกส์


กองทัพเรือ. “แนวทางการใช้งานระบบสารสนเทศ” . (ออนไลน์). เข้าถึงได้จาก : http://www.logis.navy.mi.th/data/loganalyse/it_appr.pdf, 2557.

กองทัพเรือ. “ระเบียบกองทัพเรือว่าการรักษาความปลอดภัยสารสนเทศ พ.ศ.2554”. (ออนไลน์). เข้าถึงได้จาก : http://www.ctbdc.navy.mi.th/it_ctbdc/rabiabnavy_2554.pdf, 2554.

กองทัพอากาศ. “แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศ”. (ออนไลน์ ). http://imgcdn.rtaf.mi.th/2556/admin/rtaf_255611 02015313.pdf, 2557.

กองปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ. (ออนไลน์). เข้าถึงได้จาก : http://www.navy.mi.th/ncit/history.php, 2557.

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (ออนไลน์). เข้าถึงได้จาก : http://www.etcommission.go.th/, 2557.

ความมั่นคงปลอดภัยระบบสารสนเทศ.,สมาคม. (ออนไลน์). เข้าถึงได้จาก : http://www.tisa.or.th/, 2557.

จตุชัย แพงจันทร์.,น.ท.. “สงครามไซเบอร์ได้เริ่มขึ้นแล้ว”. (ออนไลน์). เข้าถึงได้จาก : http://www.rtafa.ac.th.

ทิวสน สีอุ่นและชญานิน วิภูษณวรรณ. “สงครามไซเบอร์ ถล่มอินเทอร์เน็ตพม่ารับวันเลือกตั้ง”. (ออนไลน์). เข้าถึงได้จาก:http://prachatai.com/journal/2010/11/31796, 2553.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน,สำนักงาน). (ออนไลน์). เข้าถึงได้จาก : http://www.etda.or.th/, 2557.

พีพีพี2555. “6 สุดยอดไวรัสและหนอนคอมพิวเตอร์อันตรายระดับโลก Dek-d.com”. (ออนไลน์). เข้าถึงได้จาก : http://www.dek-d.com/lifestyle/28367/, 2555.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย.(ออนไลน์). เข้าถึงได้จาก : http://www.etda.or.th/etda_website/content/background-of-thaicert.html, 2557.

ศูนย์รักษาความปลอดภัยคอมพิวเตอร์. (ออนไลน์). เข้าถึงได้จาก : http://csc.mod.go.th/about, 2557.

หน่วยบัญชาการต่อสู้อากาศยานและรักษาฝั่งกองทัพเรือ. (ออนไลน์). เข้าถึงได้จาก : http://www.acdc.navy.mi.th/pdf/Information%20Warfare.pdf, 2557.

Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf1.htm, 2546.

Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf2.htm, 2546.

Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf3.htm, 2546.

Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf4.htm, 2546.

Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf5.htm, 2546.

Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf6.htm, 2546.

Information Security Management Framework. ( ออนไลน์ ). เข้าถึงได้จาก : http://www.acisonline.net/article_prinya_ismf7.htm, 2546.

Mr P 2552. “Ghostnet แฮกเกอร์จีนประกาศศักดาล้วงข้อมูลลับจากประเทศทั่วโลก”. (ออนไลน์). เข้าถึงได้จาก : http://supojcherd.blogspot.com/2009/05/ghostnet.html, 2552.

Siam Intelligence. (ออนไลน์). เข้าถึงได้จาก : http://www.siamintelligence.com/ obama-cyber-security -order/, 2556.

# ภาษาต่างประเทศ


## Journals

U.S. Headquarters, Department of the Army. "Signal Support to Theater Operations". ( Field Manual No. 11-45, April 12, 2004).

## Electronic Data Base

Industrial Control Systems Cyber Emergency Response Team. (Online). Available : https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions, 2544.

# ประวัติย่อผู้วิจัย

**ชื่อ** พล.ต. สุชาติ ผ่องพุฒิ

**วัน เดือน ปี เกิด** 30 กรกฎาคม 2502

**การศึกษา** รร.เตรียมทหาร รุ่นที่ 18

รร.นายร้อยพระจุลจอมเกล้า รุ่นที่ 29

หลักสูตรชั้นนายร้อย เหล่าทหารสื่อสาร รุ่นที่ 23

หลักสูตรชั้นนายพัน เหล่าทหารสื่อสาร รุ่นที่ 23

รร.เสนาธิการทหารบก ชุดที่ 28

หลักสูตร เทคโนโลยีคอมพิวเตอร์ รร.ส.สส. รุ่นที่ 2

**ประวัติการทำงานโดยย่อ**

ผบ.มว.ศูนย์ข่าวและนำสาร ร้อย.วิทยุและศูนย์ข่าว ส.พัน.21

รอง ผบ.ร้อย.บก.ส.พัน.21

ผบ.ร้อย.บก.ส.พัน.21

รอง ผบ.ส.พัน.21

อจ.รร.ส.สส.

ผบ.ส.พัน.2 พล.ร.2 รอ.

ผบ.ส.1 พัน.102

ผบ.ส.1 พัน.101

ผอ.กวก.สส.

ผบ.ส.1

รอง ผอ.ศทท.

ผอ.ศทท.

**ตำแหน่งปัจจุบัน** รอง จก.สส.

# สรุปย่อ


**ลักษณะวิชา** วิทยาศาสตร์และเทคโนโลยี

**เรื่อง** แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย

**ผู้วิจัย** พลตรี สุชาติ ผ่องพุฒิ **หลักสูตร** ปรอ. **รุ่นที่** 26

**ตำแหน่ง** รองเจ้ากรมการทหารสื่อสาร

## ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศมีบทบาทเป็นอย่างมาก ดังจะเห็นได้จากหน่วยงานต่าง ๆ เช่น ภาครัฐบาล ภาคเอกชน หรือแม้กระทั้ง ประชาชนทั่วไป ต่างมี แนวความคิดที่จะนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้งานในกิจกรรมต่าง ๆ เพื่อให้กิจกรรมนั้น ๆ เกิดประสิทธิภาพสูงสุด เป็นยุคของสังคมออนไลน์ และเมื่อระบบสารสนเทศ ได้ถูกนำมาใช้กับกิจกรรมต่าง ๆ อย่างแพร่หลาย ย่อมเป็นสิ่งที่หลีกเลี่ยงไม่ได้ที่กิจกรรมทางทหารจะนำเทคโนโลยีสารสนเทศมาใช้งานทั้งทางด้านการบริหารจัดการและในสนามรบ ทำให้สารสนเทศเปรียบเสมือนทรัพยากรที่มีความสำคัญยิ่ง

แน่นอนว่าทรัพยากรทางด้านสารสนเทศ โดยเฉพาะข้อมูลการปฏิบัติการทางทหาร ข้อมูลอาวุธ และยุโธปกรณ์ต่างๆ เมื่อมีการเก็บบันทึกไว้ในรูปของข้อมูลดิจิตอล และมีการเชื่อมโยงเพื่อการใช้งานด้วยเครือข่ายคอมพิวเตอร์ ย่อมจะเป็นเป้าหมายของฝ่ายตรงข้าม

เมื่อฝ่ายตรงข้ามต้องการที่จะโจมตีหรือเจาะข้อมูลที่สำคัญของฝ่ายเรา การรับมือดังกล่าวของกองทัพไทย เพื่อการป้องกันข้อมูล หรือไปถึงขั้นการตอบโต้การโจมตี ต้องมีการดำเนินการอย่างเป็นระบบและมีกรอบการทำงานที่ชัดเจน เป็นรูปธรรม และเป็นไปตามนโยบายของรัฐบาลที่ได้มีการกำหนดไว้แล้ว

รัฐบาลได้มีการแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee: NCSC) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการ โดยมีหน้าที่หลักในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามทางไซเบอร์ ที่กระทบต่อ

ความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ตลอดจนติดตามและประเมินผลการปฏิบัติที่เกี่ยวข้องเพื่อให้เกิดการบูรณาการการทำงานของหน่วยงานต่างๆ ที่เกี่ยวข้อง อันจะก่อให้เกิดประสิทธิภาพและประสิทธิผลในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

เมื่อพิจารณาถึงนโยบายภาครัฐข้างต้นทำให้ เชื่อได้ว่ามีกิจกรรมไซเบอร์บางอย่างที่จะเป็นภัยคุกคามที่สำคัญในระบบของประเทศ ในที่นี้ก็คือ “สงครามไซเบอร์ “ หรือ Cyber Warfare ซึ่งเป็นสงครามที่ไม่ได้เป็นการใช้อาวุธเข้าสู้รบกันโดยตรง แต่เป็นการใช้เทคโนโลยีคอมพิวเตอร์เข้าดำเนินการ ฝ่ายตรงอาจจะเป็นรัฐหรือชาติใดก็ตาม ที่ได้มีการดำเนินการแทรกซึมเข้าไปในเครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของฝ่ายเรา หรือเป้าหมาย เพื่อหวังทำลายหรือสร้างความแตกแยก หรือเพียงแค่การลักลอบขโมยข้อมูล ความลับทางทหารของเป้าหมาย เมื่อเกิดกรณีดังกล่าวขึ้น จะส่งผลที่เป็นอันตรายหรือความไม่ปลอดภัย ต่อการปฏิบัติการทางทหารต่างๆ ทั้งภาคพื้นดิน ภาคพื้นอากาศ และภาคทะเล อย่างกว้างขวาง

## วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวคิดทางด้านสงครามไซเบอร์ ในหลากหลายรูปแบบ
2. เพื่อศึกษาภัยคุกคามทางด้านสงครามไซเบอร์ที่ส่งผลกระกระทบต่อความมั่นคงของชาติ
3. เพื่อการประเมินศักยภาพต่อกองทัพในด้านสงครามไซเบอร์
4. เพื่อเสนอแนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย

## ขอบเขตของการวิจัย

1. เน้นการวิจัยเฉพาะกระบวนการและรูปแบบในการกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ของกองทัพไทย

2. ในส่วนของการปรับปรุงบทบาทและโครงสร้างของหน่วยรับผิดชอบหลัก จะเป็นเพียงการเสนอแนวคิดหรือหลักการกว้าง ๆ โดยไม่พิจารณาลึกในรายละเอียดของผังการจัดหน่วย

3. ดำเนินการวิจัยเฉพาะนโยบายที่เปิดเผยได้เท่านั้น

## วิธีดำเนินการวิจัย

ครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์กระบวนการ รูปแบบ และลักษณะของนโยบายความมั่นคงทางไซเบอร์ของประเทศไทย และเปรียบเทียบกับต่างประเทศบางประเทศ โดยมุ่งเน้นการวิเคราะห์ความชัดเจน ความเฉพาะเจาะจง ความสามารถในการแปลงไปสู่แผนการปฏิบัติ ความเหมาะสมของเนื้อหากับกรอบเวลา รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิเพื่อให้ได้แนวทางในการกำหนดนโยบายความมั่นคงไซเบอร์แห่งชาติที่เหมาะสมกับกองทัพไทยในห้วงเวลาซึ่งมีความชัดเจน และแปลงไปสู่แผนการปฏิบัติได้จริง

## ผลการวิจัย

บทเรียนในเรื่องของสงครามไซเบอร์ สงครามไซเบอร์ที่เกิดขึ้นครั้งแรกใน ปี 2550 ประเทศเอสโตเนีย ถูกโจมตีด้วยไซเบอร์ เป้าหมายอยู่ที่ รัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่าง ๆ จนทำให้ข้อมูลเสียหาย จากการกระทำของฝ่ายข้าม ซึ่งมีความเชื่อว่าเป็นการโจมตีมาจาก กลุ่มแฮกเกอร์ของรัสเซีย หลังจากนั้นก็มีสงครามไซเบอร์เกิดขึ้นตามมาอย่างต่อเนื่อง

แนวคิดของสงครามไซเบอร์ในต่างประเทศ โดยเฉพาะทางประเทศสหรัฐอเมริกา จากคู่มือปฏิบัติการภาคสนามของสหรัฐ FM 11-45 ได้กล่าวถึง การปฏิบัติการด้าน Cyber Defense ของ สหรัฐฯ ซึ่งมุ่งเน้นไปที่การปฏิบัติ การป้องกัน, เฝ้าตรวจ, วิเคราะห์, ปกป้อง และ ตอบโต้ ตลอดจนการป้องกันระบบข่าวสาร ( Information Assurance - IA ) ซึ่งเป็นมาตรการป้องกันภัยคุกคามที่จะเกิดขึ้น ซึ่งมีองค์ประกอบที่สำคัญในด้านต่างๆ ดังนี้ 1. ความสามารถในการป้องกันภายในหน่วย 2. ความสามารถในการกลั่นกรองภัยคุกคาม 3. ความสามารถในการตอบโต้ภัยคุกคามที่เกิดขึ้น

นอกจากนั้น ยังมีการกำหนดระบบเครือข่ายที่มีความปลอดภัยเรียกว่า การปฏิบัติการเครือข่ายของสหรัฐฯ (เน็ตออป/NETOPS) เป็นการสร้างเครือข่าย การปฏิบัติงาน ที่มีการเชื่อมโยงในสายการบังคับบัญชา ทั้งหน่วยเหนือ หน่วยรอง ตลอดจนถึงผู้ปฏิบัติ มีการจัดให้มีเทคโนโลยีสารสนเทศและการเฝ้าระวัง, การติดตามสถานการณ์, การปกป้องการไหลของข้อมูลข่าวสาร , และการบริหารจัดการเครือข่าย, การสนธิ IA(Information Assurance) และการบริหารด้านการกระจายข้อมูลข่าวสาร เป็นทั้งเครื่องมือ และแนวความคิด ในการปฏิบัติ สำหรับการบริหารระบบสื่อสารและสารสนเทศของกองทัพบกสหรัฐฯ

แนวคิดในการจัดตั้งหน่วยงานไซเบอร์ในต่างประเทศ จากประเทศสหรัฐอมเริกา ได้กำหนดนโยบายจากประธาธิบดีฯ อนุมัติคำสั่งประธานาธิบดี ในประเด็นเรื่องการพัฒนาความปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยมอบหมายให้ กระทรวงความมั่นคงแห่งมาตุภูมิ เป็นแกนหลักในการทำงานด้านไซเบอร์

หน่วยงานทางทหารที่สำคัญ ได้แก่ หน่วยงานไซเบอร์คอมแมนด์ (US CYBERCOM) เป็นกองบัญชาการรบร่วมระดับรอง (sub-unified command) โดยจะขึ้นตรงกับสตราทีจิกคอมแมนด์ (USSTRATCOM) สำหรับไซเบอร์คอมแมนด์ มีหน้าที่หลัก คือ การปกป้องระบบเครือข่ายที่ฝ่ายทหารเป็นผู้รับผิดชอบ ในขณะที่ระบบเครือข่ายของรัฐบาลฝ่ายพลเรือนนั้นจะเป็นหน้าที่ของกระทรวงโฮมแลนด์ซีเคียวลิตี้

สรุปการจัดตั้งหน่วยไซเบอร์ในต่างประเทศ

1. สหรัฐฯ จัดตั้งหน่วยบัญชาการไซเบอร์ ( US Cyber Command )
2. จีน จัดตั้งหน่วย Cyber Blue Team
3. อินเดีย จัดตั้งหน่วย Cyber Command and Control Authority
4. เกาหลีเหนือ จัดตั้งหน่วย Korean People's Army Joint Chiefs Cyber Warfare Unit หรือ Unit 121
5. สหภาพยุโรป จัดตั้งสำนักงาน European Network and Information Security Agency
6. เกาหลีใต้ จัดตั้งหน่วยสงครามไซเบอร์ระดับชาติ
7. กระทรวงกลาโหมของประเทศสิงค์โปร์ : IT Security Operations
8. กระทรวงกลาโหมของประเทศมาเลเซีย : Cyber Security Division
9. ประเทศพม่าหรือเมียนม่าร์: จัดตั้ง Cyber Warfare Department
10. ไต้หวัน : จัดตั้ง Military Information Warfare Strategy Policy Committee

หน่วยงานที่เกี่ยวข้องทางด้านไซเบอร์ของกองทัพไทยในปัจจุบัน

1. สำนักงานปลัดกระทรวงกลาโหม : ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยี สารสนเทศและอวกาศกลาโหม (ศรค.ทสอ.กห.)
2. กองบัญชาการกองทัพไทย : กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยี สารสนเทศกรมการสื่อสารทหาร (กรส.ศทส.สส.ทหาร)
3. กองทัพบก : กองการสงครามสารสนเทศ ศูนย์เทคโนโลยีทางทหาร กรมการทหารสื่อสาร (กสสท.ศทท.)

4. กองทัพเรือ : กองปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ
กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (กปท.สสท.ทร.)
5. กองทัพอากาศ : กองสงครามอิเล็กทรอนิกส์และสารสนเทศ กรมเทคโนโลยี
สารสนเทศและการสื่อสารทหารอากาศ (กคส.ทสส.ทอ.)

การรองรับสงครามไซเบอร์ในปัจจุบัน นั้นควรมีข้อพิจารณาถึงปัญหาและผลกระทบทางด้านสงครามไซเบอร์ ซึ่งในทางสากลได้กำหนดระดับภัยคุกคามทางด้านไซเบอร์ ออกเป็นระดับดังนี้

- ภัยคุกคามในระดับรัฐบาลแห่งชาติ ( National Governments )
- ภัยคุกคามในระดับการก่อการร้าย ( Terrorists )
- สายลับหรือพวกจารกรรมในภาคอุตสาหกรรม และกลุ่มองค์กรอาชญากรรมต่าง ๆ ( Industrial Spies and Organized Crime Groups )
- กลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ ( Hacktivists )
- กลุ่มแฮ็กเกอร์ ( Hackers )

ยุทธศาสตร์และแนวทางการรองรับสงครามไซเบอร์ที่มีอยู่เดิมของประเทศ ในเรื่องนี้มีเพียง คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ( National Cyber Security Committee : NCSC ) โดยมีนายกรัฐมนตรีเป็นประธาน ซึ่งเป็นยุทธศาสตร์หลักในปัจจุบัน นอกจากในระดับรัฐบาลแล้ว ในระดับกระทรวง ที่สำคัญอย่าง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดตั้งหน่วยงานต่างๆ ได้แก่ ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ ( Cyber Security Operation Center : CSOC ) , ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) หรือ ThaiCERT และ อื่นๆ เป็นต้น

สำหรับในระดับกระทรวงกลาโหม มีการจัดตั้ง ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ (ศรค.) และ การเสนอร่างศูนย์ปฏิบัติการไซเบอร์กลาโหม ส่วนในกองบัญชาการกองทัพไทย นั้นเริ่มดำเนินการเสนอโครงสร้างของหน่วยงานใหม่ที่เรียกว่า กองปฏิบัติการสงครามเครือข่าย

ในระดับเหล่าทัพต่างๆ กองทัพบก กองทัพเรือ กองทัพอากาศ ก็ยังอยู่ในระหว่างการปรับปรุงโครงสร้างหน่วยงานใหม่เพื่อรองรับสงครามไซเบอร์ในอนาคตต่อไป

ขอบเขตของการรองรับสงครามไซเบอร์ ในกรอบมุมมองของกองทัพ สามารถกำหนดขอบเขตได้ตามระดับของภัยคุกคามดังนี้

-ระดับประเทศ ในระดับนี้ความรับผิดชอบ ไม่แต่เพียงหน่วยงานด้านความมั่นคง หรือกองทัพ แต่ควรเป็นทุกภาคส่วนทั้งภาครัฐและภาคเอกชน มีส่วนร่วมในการป้องกันภัยภัยคุกคามทางไซเบอร์

- ระดับการก่อการร้าย และอาชญากรรมต่างๆ ความรับผิดชอบของกองทัพยังคงใช้การเฝ้าระวัง และแจ้งเตือน มีการทำงานที่สอดคล้องกัน และเป็นส่วนหนึ่งของเครือข่ายในระดับประเทศ

-ระดับแฮ็กเกอร์ ความรับผิดชอบของกองทัพ ยังคงใช้การเฝ้าระวัง และแจ้งเตือน และสร้างเครือข่ายภายในกองทัพเอง ตลอดจนการดำเนินการสร้างความตระหนัก และกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดปลอดภัยในระบบของกองทัพ

แนวทางการรองรับสงครามไซเบอร์ในอนาคต กองทัพมีการประเมินภัยคุกคามของสงครามไซเบอร์ ในส่วนของกองทัพเอง ซึ่งภัยคุกคามดังกล่าว กองทัพได้ให้ความสำคัญ ด้วยกัน 4 ด้าน ได้แก่ 1 . ภัยคุกคาม ที่ส่งผลต่อความมั่นคงของประเทศ 2. ภัยคุกคาม ที่ส่งผลกระทบต่อสามจังหวัดชายแดนภาคใต้( จชต. ) 3.ภัยคุกคาม ที่ส่งผลกระทบต่อ สถาบันฯ 4. ภัยคุกคาม ที่ส่งผลกระทบต่อ ภาพลักษณ์ของ กองทัพ

และได้กำหนดกรอบในการดำเนินการทางด้านสงครามไซเบอร์ ของกองทัพไทย เพื่อรองรับสงครามไซเบอร์ในอนาคต ออกเป็น 4 ด้านดังนี้

- ด้านนโยบาย
- ด้านความรู้
- ด้านโครงสร้างองค์กร
- ด้านการปฏิบัติงาน

นอกจากนั้น ยังมีการกำหนดกรอบระยะเวลาในการดำเนินการทางด้านสงครามไซเบอร์ แบ่งออกเป็น 3 ระยะ

- ระยะแรก : (ปี 2557 - ปี 2559)
- ระยะกลาง : (ปี 2559 - ปี 2561)
- ระยะยาว : (ปี 2561 - ปี 2563)

## ข้อเสนอแนะ

จากผลการวิจัย จะเห็นได้ว่า หน่วยงานในกองทัพ มีความพยายามที่จะปรับปรุง การจัดตั้งหน่วยงาน เพื่อให้สอดรับกับ นโยบายของรัฐบาลฯ ผู้วิจัยมีแนวคิดในเรื่องโครงสร้างหน่วยสงครามไซเบอร์ ดังกล่าว ดังนี้

ภารกิจของหน่วยมีดังนี้

1. ภารกิจในภาพรวมของหน่วยคือการปฏิบัติการสงครามไซเบอร์ โดยแยกการดำเนินการออกได้เป็น 2 รูปแบบ ได้แก่ (1) การปฏิบัติการสงครามไซเบอร์ในฐานะเป็นงานสนับสนุนการรบหลัก ซึ่งมีการปฏิบัติการในเชิงรุก และเชิงรับ (2) การปฏิบัติการสงครามไซเบอร์ในฐานะเป็นฝ่ายเทคนิคหรือผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของกองทัพ

2. สำหรับโครงสร้างของหน่วยประกอบไปด้วย

2.1 ส่วนบัญชาการ/บังคับการ ประกอบไปด้วย ผู้บังคับบัญชา ส่วนอำนวยการและวางแผน ส่วนการจัดการบุคคลากร ส่วนฝึกอบรมและทดสอบ เป็นส่วนงานที่ควบคุมการปฏิบัติการทั้งในงานสนับสนุนการรบ และในงานสายงานผู้เชี่ยวชาญ ในภาพรวม

2.2 ส่วนปฏิบัติการรักษาความปลอดภัยไซเบอร์และ ประกันข้อมูลข่าวสาร สำหรับในส่วนนี้ถือว่าเป็นการปฏิบัติการสงครามไซเบอร์ ในฐานะผู้เชี่ยวชาญด้านการรักษาความปลอดภัย งานที่ปฏิบัติเป็นเรื่องของการจัดทำนโยบายความปลอดภัย การทดสอบช่องโหว่ การจัดทำการบริหารความเสี่ยงของทรัพย์สินของกองทัพ ตลอดจนการสนับสนุนผู้เชี่ยวชาญในด้านการรักษาความปลอดภัยและประกันข้อมูลข่าวสาร

2.3 ส่วนปฏิบัติการสงครามไซเบอร์ ประกอบไปด้วยทั้งเชิงรุก และเชิงรับ ทางด้านไซเบอร์ เช่น งานเฝ้าระวังทางไซเบอร์ งานแจ้งเตือนเหตุการณ์ที่กระทบด้านไซเบอร์ สนับสนุนการเจาะข้อมูลทางไซเบอร์ ตลอดจนการฝึกและสนับสนุนกำลังพลที่มีขีดความสามารถในด้านการปฏิบัติการไซเบอร์

---