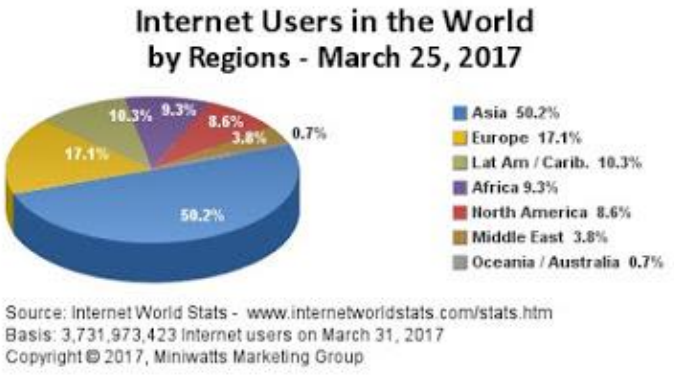
# การพัฒนาขีดความสามารถของกองทัพบก
# ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ในปัจจุบันนี้ เทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ ได้มีความก้าวหน้าไปอย่างมากมาย การเกิดนวัตกรรมใหม่ๆ ของระบบเทคโนโลยีสารสนเทศ (Information Technology) ได้ส่งผลกระทบต่อการดำเนินชีวิตโดยทั่วไปเช่น จากโทรศัพท์แบบเดิม มาเป็นการโทรผ่านแอบพลิเคชั่น line, chat, การประชุมทางไกลผ่าน Video Conference, การสมาคมกับเพื่อนผ่าน Face Book การซื้อขายสินค้าผ่านระบบ E-market และการทำธุรกรรมการเงิน ผ่านระบบออนไลน์ (E-Banking) เป็นต้น จึงเป็นยุคแห่งสังคมการย่อโลกหรือโลกาภิวัตน์ (Globalization) และความก้าวหน้าทางวิทยาศาสตร์เทคโนโลยี ทำให้มนุษย์สามารถเชื่อมต่อกันได้อย่างรวดเร็ว สะดวกและมีปฏิสัมพันธ์กันได้อย่างง่ายดาย แม้ว่าจะอยู่ห่างไกลกันก็ตาม

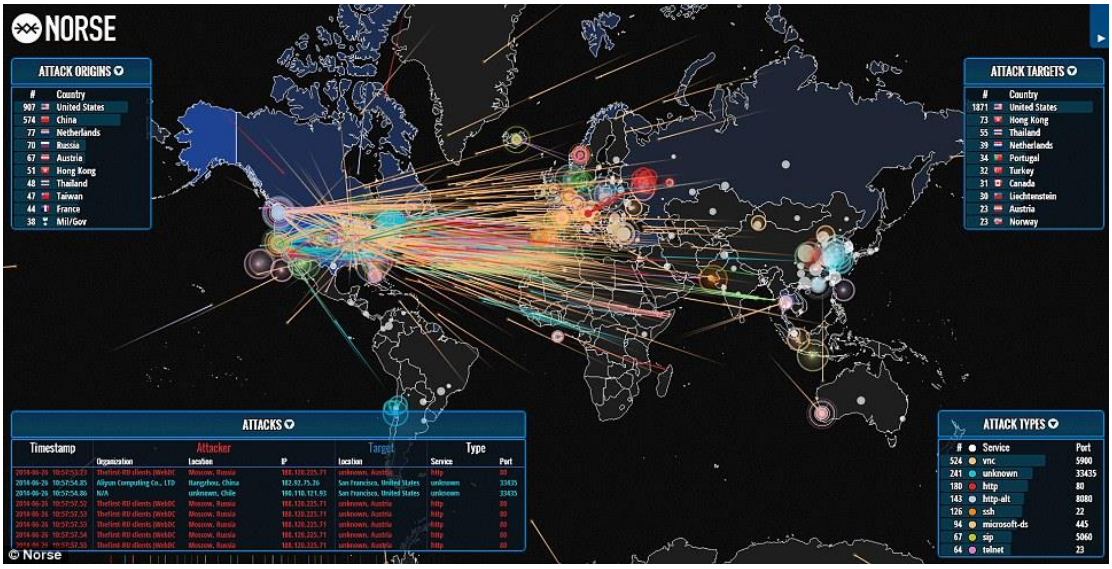



จากข้อมูลของ Internet World Stats, 2017. ทวีปเอเชียมีจำนวนผู้ใช้งานเข้าถึงอินเทอร์เน็ตจำนวนมากที่สุดในโลก โดยประเทศจีนมีผู้ใช้งานอินเทอร์เน็ตมากที่สุดในโลกคือ 721.43 ล้านคน แต่คิดเป็น 52.2% ของประชากรจีนทั้งหมด ส่วนประเทศที่มีอัตราส่วนประชากรต่อการใช้งานอินเทอร์เน็ต 100% คือประเทศไอซ์แลนด์ ประเทศไทยมีการเข้าถึงอินเทอร์เน็ตในอัตราส่วน 42.7% ติดอันดับที่ 24 ของโลก

ความก้าวหน้าทางวิทยาศาสตร์เทคโนโลยีฯ ที่เกิดขึ้น[1] ก่อให้เกิดการเปลี่ยนแปลงของหลายสิ่งที่มนุษย์ต้องมีการปรับตัวเพื่อก้าวให้ทัน และสามารถใช้ประโยชน์จากวิวัฒนาการเหล่านี้ โดยมีทั้งการพัฒนาในรายบุคคลและการพัฒนาในภาพขององค์กรเพื่อเป้าหมาย

ทางการแข่งขันระหว่างองค์กร สำหรับในระดับประเทศนั้น รัฐบาลยังต้องการนำเทคโนโลยีฯ มาเป็นเครื่องมือในการพัฒนาขับเคลื่อนประเทศในด้านต่าง ๆ ทั้งด้านการเมือง, เศรษฐกิจ, สังคมจิตวิทยาและการทหาร เพื่อเสริมสร้างประสิทธิภาพในการบริหารจัดการให้เกิดศักยภาพและความทันสมัย ตามหลักนโยบาย Thailand 4.0 เช่น E-Service, E-Government เป็นต้น แต่ในทางตรงกันข้าม ผลจากการนำเทคโนโลยีฯ มาใช้งานที่ไม่ถูกต้องหรือการนำมาใช้เพื่อผลทางมิชอบ นับเป็นมหันตภัยใหญ่ที่กำลังคุกคามความมั่นคงในด้านต่าง ๆ

ความมั่นคง (Security) อาจจะหมายถึง ความปลอดภัยจากการถูกคุกคามที่พึงรักษาไว้ ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) คือการป้องกันอันตรายในโลกออนไลน์และอินเตอร์เนต ที่มีผลกระทบต่อผู้ใช้งานและทรัพย์สิน[2] หรืออีกนัยหนึ่งคือ มาตรการที่ใช้เพื่อปกป้องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ (เช่นบนอินเทอร์เน็ต) ต่อการเข้าถึงหรือ




การโจมตีที่ไม่ได้รับอนุญาต[3] ปัจจุบันในประเทศไทย องค์กรหลายแห่งได้รับการแจ้งเหตุภัยคุกคามทางไซเบอร์ (Cyber Attack) ในแต่ละปีเป็นจำนวนมาก โดย พ.ศ. 2560 ประเทศไทยมีการแจ้งเหตุภัยคุกคามทางไซเบอร์รวมถึง 67 ครั้ง[4]และมีแนวโน้มเพิ่มมากขึ้นโดยที่ถูกจัดให้อยู่ในลำดับที่ 15 จาก 165 ประเทศทั่วโลกที่มีภัยคุกคามทางไซเบอร์มากที่สุดในโลก[5] แม้ภัยคุกคามในประเทศไทยอาจไม่ใช่เกิดจากประเทศอื่นที่เป็นฝ่ายตรงข้าม แต่ก็เกิดจากกลุ่มอุดมการณ์ กลุ่มการเมืองที่ไม่เห็นด้วยกับรัฐและมีความซับซ้อน สังคมไทยจึง

ต้องตื่นตัวเฝ้าระวังและหาทางรับมือกับภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นยุทธศาสตร์การรักษาความปลอดภัยในโลกไซเบอร์ เป็นหนึ่งในยุทธศาสตร์การพัฒนาเศรษฐกิจและสังคมดิจิทัลของรัฐบาล โดยสหภาพโทรคมนาคมระหว่างประเทศ (ITU)[6] จัดอันดับดัชนีความปลอดภัยในโลกไซเบอร์ (GCI) ประจำปี 2560 ให้ประเทศไทยมีระดับการพัฒนาด้าน Cybersecurity อยู่ในอันดับที่ 20 โดยที่มีสิงค์โปร์เป็นอันดับ 1 และ สหรัฐอเมริกาเป็นอันดับ 2 ของโลก แสดงให้เห็นว่าประเทศไทยได้มีการพัฒนาทุกภาคส่วนไปในระดับหนึ่งแล้ว แต่ยังมีอีกหลายสิ่งที่ต้องพัฒนาให้ดียิ่งขึ้นเพื่อความปลอดภัยในโลกไซเบอร์ ซึ่งนั่นหมายถึงความร่วมมือของทั้งภาครัฐ ภาคเอกชน และประชาชนทั้งประเทศ โดยแบ่งหน่วยงานที่รับผิดชอบตามแบบของภัยคุกคามคือ

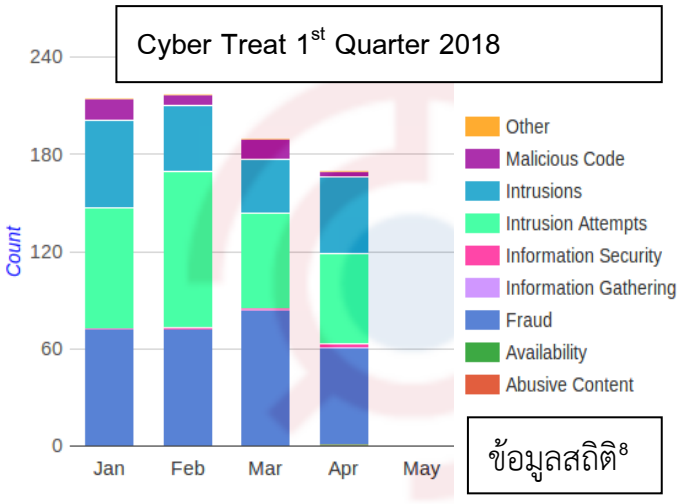
- สำนักงานตำรวจแห่งชาติ ทำการบังคับใช้กฎหมายที่เกี่ยวข้องกับการกระทำผิดทางด้านไซเบอร์หรือติดตามข่าวกรองอาชญากรรมทางด้านไซเบอร์ให้มีประสิทธิภาพ
- กระทรวงดิจิทัลฯ ควรพัฒนาศักยภาพเพื่อให้รองรับ ความมั่นคงปลอดภัยทางด้านไซเบอร์กับระบบเศรษฐกิจและสังคมยุคใหม่
- เพิ่มศักยภาพการป้องกันความมั่นคงปลอดภัยทางด้านไซเบอร์ ของระบบสาธารณูปโภคต่างๆ
- หน่วยงานด้านความมั่นคงของประเทศในทุกระดับเช่น กระทรวงกลาโหม หรือกองทัพ ต้องหาทางหยุดยั้งและรับมือกับภัยคุกคามให้ได้ประสิทธิภาพ
- ร่างพรบ.ว่าด้วยความมั่นคงปลอดภัยไซเบอร์ มาตรา 35 จะทำให้เจ้าหน้าที่ที่ได้รับมอบหมาย มีอำนาจในการเข้าถึงข้อมูลการติดต่อสื่อสารทุกชนิด (ที่กระทบต่อสิทธิและเสรีภาพน้อยที่สุด)

**รูปแบบภัยคุกคามทางด้านไซเบอร์**

การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี[7] มาใช้เป็นภัยคุกคามและใช้ในการทำลายสร้างความเสียหายให้เกิดขึ้นในรูปแบบต่าง ๆ ดังนี้

1. การเจาะระบบ (Hacking) เป็นการกระทำด้วยมนุษย์หรือใช้ซอฟแวร์

2. การใช้ Spyware หรือ Back Door คือการฝังโปรแกรมลับเข้าไปในระบบเพื่อลอบโจรกรรมข้อมูลหรือทำความเสียหาย




3. การใช้โปรแกรม Malware สั่งให้ทำความเสียหายต่อระบบ

4. การใช้ Computer Virus เข้าไปในเครื่องหรือเครือข่ายคอมพิวเตอร์เพื่อให้เกิดความเสียหายกับระบบ

5. การใช้หนอนคอมพิวเตอร์ (Computer Worm) ซึ่งแพร่กระจายโดยไม่ต้องผ่านการใช้

6. การใช้ระเบิดเวลา (Logic Bomb) หรือระเบิดตรรกะ โดยจะกำหนดเป็นวันที่หรือการกดปุ่มบนแป้นพิมพ์ เพื่อให้มีการปิดระบบหรือเครือข่ายทั้งหมด

7. การใช้ Trojan เพื่อเข้าทำอันตรายต่อระบบคอมพิวเตอร์ และทำการขโมยข้อมูล

8. การใช้หุ่นยนต์ (Botnet) เป็นการส่งโปรแกรมไปติดตั้งและรอรับคำสั่ง และโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์นั้น


9. การโจมตีแบบ (DoS/DDos) การโจมตีสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ โดยสร้างการโจมตีจากหลายๆ ที่ โดยแต่ละที่จะโจมตีเป้าหมายเดียวกันในเวลาเดียวกัน เพื่อทำให้บริการต่าง ๆ ของระบบฯ ไม่สามารถให้บริการได้ตามปกติ จนกระทั่งระบบไม่สามารถให้บริการได้ต่อไป

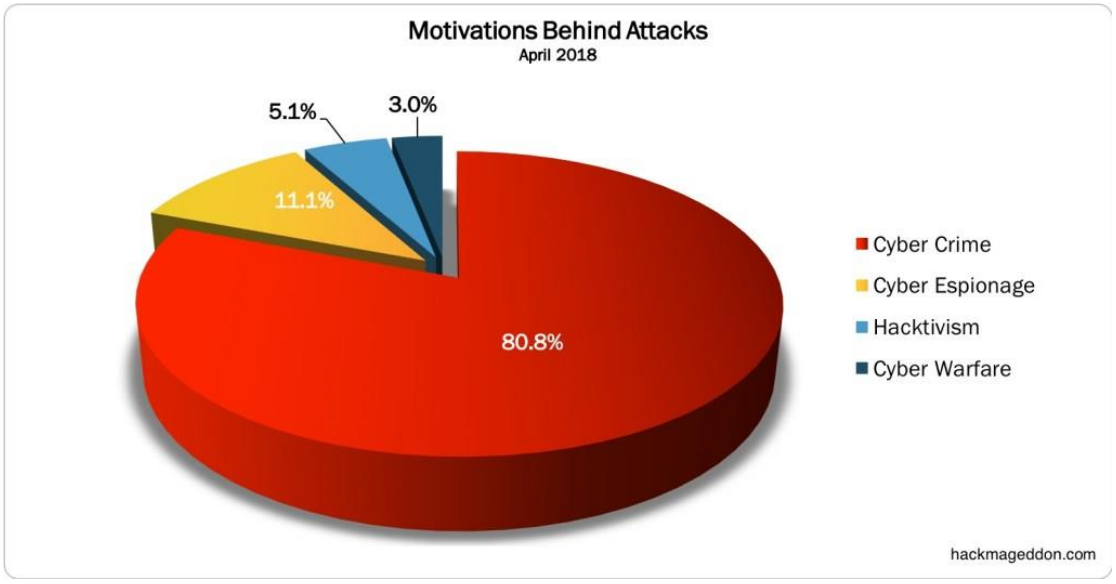
10. การโจมตีด้วย Ransomware ใช้การเข้ารหัสลับกับไฟล์ข้อมูลหรือปิดกั้นไม่ให้ผู้ใช้เข้าถึงข้อมูลจนกว่าเหยื่อจะจ่ายเงินเพื่อจะได้รับกุญแจปลดล็อกการใช้งาน

โดยในกลุ่มที่ 1-8 จะเป็นการส่งหรือแฝงเอาโปรแกรมย่อยเข้าไปในระบบและสร้างความเสียหาย ซึ่งเราอาจใช้โปรแกรมพวก Anti-Virus, Anti-Spam/Malware ทำงานร่วมกับ OS Firewalls-Defender ก็จะแก้ไขและป้องกันได้ โดยในกลุ่มที่ 9 และ 10 จะเป็นวิธีการ

ที่กลุ่มก่อการร้ายทางไซเบอร์ชอบใช้ เพราะสามารถสร้างความเสียหายที่ชัดเจนในวงกว้าง และเรียกร้องค่าไถ่เป็นการตอบแทนได้และจากสถิติภัยคุกคาม การเจาะเข้าระบบ (Intrusions) และความพยายามในการเจาะระบบ (Intrusion Attempts) ก็ยังครองความนิยมเป็นอันดับ 1 และ 2 ตามมาด้วยภัยจากการหลอกลวง (Fraud) เป็นอันดับ 3 ในช่วงไตรมาสแรกของปี 2018

**ประเภทของภัยคุกคามทางไซเบอร์ในปัจจุบัน**

ในการวางแผนยุทธศาสตร์ด้านความมั่นคงทางไซเบอร์เพื่อรับมือกับภัยคุกคามนั้น ในทางสากลสามารถแบ่งประเภทของภัยคุกคามด้านไซเบอร์ตามลักษณะปัญหา[9]และวัตถุประสงค์ของภัยคุกคามออกเป็น 4 ลักษณะ




**C** คือ **Cybercrime** เป็นปัญหาการก่ออาชญากรรมทางไซเบอร์โดยมีวัตถุประสงค์ทางการเงินเช่นการเจาะบัญชีธนาคารหรือธุรกรรมออนไลน์ต่าง ๆ

**H** คือ**Hacktivism**เป็นการเจาะข้อมูลลับไม่ว่าจะของทางการหรือเอกชนแล้วนำมาเผยแพร่ต่อสาธารณะเพื่อเปิดโปงหรือสร้างความอับอายแก่เจ้าของข้อมูล

**E** คือ **Espionage** เป็นการจารกรรมข้อมูลเพื่อนำไปใช้ประโยชน์ต่อ เช่นการเจาะข้อมูลนวัตกรรมต่าง ๆ การเจาะข้อมูลทางการทหารความพยายามขโมยเอกสารที่มีชั้นความลับ

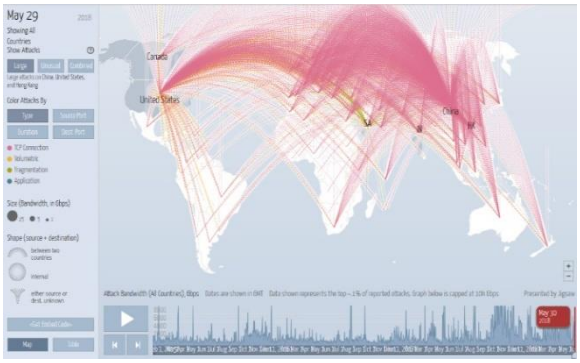
**W** คือ **War** หรือ **Cyberwarfare**คือสงครามไซเบอร์ เช่นการทำลายฐานผลิตอาวุธนิวเคลียร์โดยไม่ต้องใช้กำลังพลด้วยการส่งคำสั่งเข้าไปให้เครื่องยนต์ทำลายตนเอง หรือ

เพื่อให้การสื่อสารและพลังงานของปฏิปักษ์ล่มหรือการใช้ภัยคุกคามไซเบอร์อื่นๆ ในการทำลายล้าง

โดยจากข้อมูลสถิติจาก Hackmageddon.com ในช่วงเดือนเมษายนของปี 2018[10] นั้น อาชญากรรมทางไซเบอร์ (Cyber Crime) มีมากถึง 80.8% ตามมาด้วย การจารกรรมข้อมูล (Espionage) 11.1% โดยที่มี การเจาะข้อมูลลับ (Hacktivism) 5.1% และสงครามไซเบอร์ (Cyberwar) มีเพียง 3.0%

**เป้าหมายของภัยคุกคาม**

เป้าหมายโดยทั่วไปของนักเจาะระบบ (Hacker) คือเพื่อทดสอบความสามารถหรือต้องการท้าทายเจ้าของระบบ หรือเพื่อต้องการทำลายระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศโดยการเจาะระบบให้สำเร็จ ระบบสารสนเทศก็อาจมีรูรั่วหรือช่องโหว่ของความมั่นคง ไม่ว่าจะเป็นเรื่องของการออกแบบที่ผิดพลาด หรือที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว้เพื่อเป็นกลไกลลับทางซอฟต์แวร์หรือฮาร์ดแวร์ จึงทำให้ผู้ไม่ประสงค์ดีสามารถใช้ช่องโหว่นี้เจาะเข้ามาในระบบ และสร้างความเสียหายต่อระบบคอมพิวเตอร์ได้ ภัยคุกคามทางไซเบอร์ (Cyber Threats) ถูกนำมาใช้เป็นเครื่องมือและถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจและความมั่นคงของประเทศ โดยมีจุดมุ่งหมายในกาทำลายภาพลักษณ์ด้านความมั่นคงและเสถียรภาพในระบบเทคโนโลยีฯ และสร้างความปั่นป่วนให้กับระบบเศรษฐกิจ การเมือง และการทหาร[11]โดยเมื่อมองลึกถึงต้นตอของภัยคุกคามด้านไซเบอร์ก็จะพบว่า มีที่มาจากวิวัฒนาการและความเจริญด้านเทคโนโลยีฯ แต่ถูกนำมาสร้างเป็นภัยคุกคาม การโจมตีแต่ละครั้งล้วนสร้างความเสียหายอย่างมหาศาล ทั้งต่อความมั่นคงความปลอดภัยของระบบฯ ตลอดจนระบบเศรษฐกิจและความมั่นคงของประเทศ โดยในปัจจุบันก็มีการเอาอำนาจคุกคามกับแนวโน้มความเสียหายที่อาจเกิดขึ้นมาเป็นข้อต่อรอง เพื่อเรียกร้องทรัพย์สินหรือค่าไถ่จากการที่ระบบเสียหายหรือหยุดการทำงานอันเนื่องมาจากภัยคุกคามอีกด้วย



ประเทศที่เป็นมหาอำนาจทางด้านเศรษฐกิจและการทหาร[12] ได้กำหนดยุทธศาสตร์ด้านความมั่นคงของชาติ และพลังอำนาจทางการทหารไว้ 5 ด้าน โดยที่พื้นที่ปฏิบัติการด้านไซเบอร์ (Cyber Domain) เป็นโดเมนที่ 5 ซึ่งมีความสำคัญมาก ประเทศที่มีกำลังทหารมากและมีอาวุธที่ทันสมัยแต่หากไม่สามารถควบคุมไซเบอร์โดเมน (Cyber Domain) ซึ่งเป็นส่วนควบคุมหรือบังคับบัญชาได้ก็ไม่มีประโยชน์ เพราะสงครามในยุคใหม่จะไม่เห็นภาพการเคลื่อนกำลังทหารในการรบ แต่จะมีการควบคุมสั่งการของกองทัพผ่านเครือข่ายคอมพิวเตอร์[13] ถ้าหากระบบควบคุมสั่งการของกองทัพได้ถูกทำลายไป ระบบบังคับบัญชาและระบบสั่งการใช้ไม่ได้ กองทัพในยุคสมัยใหม่ก็จะพ่ายแพ้ในสมรภูมิการรบ

## แนวโน้มภัยคุกคามไซเบอร์ ในปี 2018

ในสถานการณ์ปัจจุบัน ได้มีการสรุปแนวโน้มภัยคุกคามไซเบอร์ในปี 2018[14] เพื่อเป็นข้อมูลในการวางแผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยด้านไซเบอร์อย่างเหมาะสม

1. Machine learning เริ่มถูกนำมาใช้เพื่อค้นหาช่องโหว่และพฤติกรรมต้องสงสัย ในฝั่งแฮกเกอร์เองก็นำ Machine Learning มาใช้เพื่อสนับสนุนการโจมตีของตนเช่นเดียวกัน เป็นการปะทะกันระหว่างเทคนิค Machine Learning ของฝั่งโจมตีและฝั่งป้องกัน

2. Ransomware รูปแบบใหม่ที่มีเทคโนโลยี-เป้าหมายและค่าไถ่ต่างไปจากเดิม มีการไปใช้บริการ Ransomware as a Service มากขึ้น และยังมีการเพิ่มการทำลายข้อมูลและการขัดขวางธุรกิจเข้าไปด้วย

3. แอปพลิเคชัน Serverless เริ่มแพร่หลายจึงมีการโจมตีแบบ Privilege Escalation (การยกระดับสิทธิ์) และ Application Dependencies (การโจมตีแอปฯที่เกี่ยวข้องเพื่อให้ส่งผลกระทบต่อแอปฯหลัก) รวมไปถึงการโจมตีข้อมูลที่ส่งผ่านไปมาข้ามระบบเครือข่ายและ DDoS

4. ข้อมูลจากครัวเรือนอัจฉริยะถูกแอบเก็บไปใช้ประโยชน์โดยไม่สนความเป็นส่วนบุคคล หลังเริ่มนำเอาอุปกรณ์อัจฉริยะเข้ามาใช้งานเพิ่มขึ้นเรื่อย ๆ มีการเก็บข้อมูลการใช้งานเพื่อนำไปใช้ประโยชน์ทางการตลาด

5. ข้อมูลออนไลน์ของผู้เยาว์จะถูกนำไปใช้อ้างถึงตัวตนในอนาคตกลุ่ม Gen Z หรือกลุ่มวัยเด็กที่เติบโตมาพร้อมกับเทคโนโลยี ข้อมูลดิจิทัลต่าง ๆ บนโลกออนไลน์จะถูกรวบรวมและถูกนำใช้อ้างอิงถึงตัวตนในอนาคต มีผลทั้งในแง่ดี-ร้าย

6. ปัญหาภัยคุกคามไซเบอร์ผ่านเครือข่ายเข้ารหัสข้อมูล เป็นการเข้ารหัสเครือข่ายข้อมูล (Encryption) ที่ชื่อว่า Tor Network เพื่อหลีกเลี่ยงการค้นหา ตรวจจับ หรือการติดตามตัว Hacker

**การรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ ในระดับสากล**

Cybersecurity[15] คือกระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ) ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cybersecurity[16] ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ ความเสี่ยงของ Cybersecurity อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้ถือผลประโยชน์ร่วม (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้นการรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงานและผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติประเทศต่างๆ ในอาเซียนโดยเฉพาะประเทศไทยถูกใช้เป็นฐานในการโจมตีทางไซเบอร์มากขึ้น เพราะการรักษาความมั่นคงทางไซเบอร์ไม่เพียงพอ มีคอมพิวเตอร์และอุปกรณ์เครือข่ายแบบต่างๆ ถูกใช้เป็นเครื่องมือในการโจมตีขนาดใหญ่ หรือใช้เป็น Gateway เพื่อการเชื่อมต่อการโจมตีไปยังจุดอื่นๆ ซึ่งระดับความรุนแรงของการโจมตีสามารถสร้างความเสียหายอย่างกว้างขวางและพัฒนาขึ้นเป็นความรุนแรงในขั้นสงครามได้อย่างไม่ยากเย็น

สงครามไซเบอร์ (Cyberwarfare)[17] นิยามขึ้นมาโดย ริชาร์ด เอ. คลาร์ก ผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลอเมริกาว่า “เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไป

ยังระบบคอมพิวเตอร์หรือเครือข่ายมีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก ” Cyberwarfare สามารถเป็นเหตุให้เกิดสงครามที่กลายเป็นเรื่องอันตรายต่อการปฏิบัติการ ซึ่งเราจะเห็นได้ว่ามีการให้ความสำคัญเกี่ยวกับความมั่นคงทางไซเบอร์ (Cyber Security) ในทุก ๆ ประเทศ แม้จะไม่ใช่ประเทศมหาอำนาจก็ตาม ภัยคุกคามทางไซเบอร์จึงถือได้ว่าเป็นภัยอันตรายต่อความมั่นคงระดับชาติ หน่วยรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber security and Integration Center: NCCIC) ของประเทศสหรัฐอเมริกา ได้กำหนดระดับภัยคุกคามด้านไซเบอร์ไว้ 5 ระดับ[18]ดังนี้

1. ภัยคุกคามในระดับรัฐบาลแห่งชาติคือภัยอันตรายต่อประเทศชาติเป็นการปล่อยข่าวที่ไม่น่าเชื่อถือ หรือการเจาะระบบของโครงสร้างพื้นฐาน ระบบสาธารณูปโภค
2. ภัยจากการก่อการร้ายสากล โดยเฉพาะการโจมตีต่อประเทศคู่ขัดแย้งทางการเมือง มุ่งทำลายผลประโยชน์ทางการเมือง
3. ภัยจากสายลับหรือพวกจารกรรมข้อมูลในภาคอุตสาหกรรม เครือข่ายอาชญากรรม
4. ภัยจากกลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ใกล้เคียงกัน เกิดจากการรวมกลุ่มของพวกแฮ็กเกอร์กลุ่มเล็ก ๆ
5. ภัยจากกลุ่มแฮ็กเกอร์มือสมัครเล่น โดยกลุ่มฯ จะประชาสัมพันธ์ทางเว็บไซต์เพื่อรวบรวมพวกมือสมัครเล่น ให้ร่วมกันโจมตีเว็บไซต์ของหน่วยงานภาครัฐและภาคเอกชน

**ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ (Cyber Security)**

ประเทศไทยมีภัยคุกคามทางด้านไซเบอร์เป็นจำนวนมาก[19] ระบบคอมพิวเตอร์ของไทยถูกใช้เป็นฐานในการโจมตีไปยังประเทศอื่น ทำให้เกิดความเสียหายเป็นวงกว้าง หรือเสียหายต่อภาพลักษณ์และความเชื่อมั่นต่อประเทศ ทางภาครัฐก็ได้มีการกำหนดนโยบายต่างๆ เพื่อผลักดันให้เกิดความมั่นคงปลอดภัยทางไซเบอร์ขึ้นภายในประเทศ

**นโยบายในระดับประเทศ**

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและหน่วยงานที่เกี่ยวข้องได้มีการเตรียมการและพัฒนาแผนงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ที่สำคัญคือ

- ตั้งศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operation Center : CSOC) เมื่อปี2553
- นโยบายเทคโนโลยีสารสนเทศของประเทศในระยะที่สอง ครอบคลุมเวลา 10 ปี (พ.ศ. 2554-2563) หรือ IT2020 โดยกำหนดบทบาทของเทคโนโลยีสารสนเทศในฐานะเครื่องมือในการขับเคลื่อนการพัฒนาประเทศทั้งด้านเศรษฐกิจและสังคม
- แต่งตั้ง “คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC) ในปี 2556 เพื่อจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558–2564 นโยบายที่ 10 เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์
    1. ปกป้อง ป้องกัน และเสริมสร้างความปลอดภัยจากภัยคุกคามด้านไซเบอร์และสงครามไซเบอร์
    2. พัฒนาการบังคับใช้กฎหมายและระเบียบ สำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์
    3. พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ ส่งเสริมการวิจัยพัฒนา
- ระเบียบ ว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อ 19 กันยายน 2560 เพื่อกำหนดนโยบายและแผนระดับชาติด้าน ความมั่นคงไซเบอร์ เพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์

**นโยบายในระดับกระทรวงกลาโหม**

ในส่วนของทางกระทรวงกลาโหมได้มีการกำหนด ยุทธศาสตร์เกี่ยวกับไซเบอร์ที่สำคัญดังนี้

- ยุทธศาสตร์ป้องกันประเทศของกระทรวงกลาโหมระหว่างปี 2560-79 ในระยะที่ 1 มีเป้าหมายในการพัฒนาขีดความสามารถด้านกิจการไซเบอร์ และกิจการอวกาศ
- ยุทธศาสตร์ไซเบอร์ป้องกันประเทศของกระทรวงกลาโหมซึ่งได้รับความเห็นชอบจากสภากลาโหมเมื่อวันที่ 29 ก.พ. 2559 ระบุถึงไซเบอร์ว่าเป็นภัยคุกคามด้านความมั่นคงของประเทศ ไซเบอร์ถูกใช้เป็นเครื่องมือในการปฏิบัติการทางทหารและชิงความได้เปรียบ

- ร่างแผนแม่บทในการป้องกันประเทศปี 2560-64 มีการจัดตั้งองค์กรเพื่อรองรับนโยบายด้านไซเบอร์ของรัฐบาลมีแผนป้องกันระบบโครงสร้างพื้นฐาน จัดทำแผนพัฒนาไซเบอร์เชิงรุก การร่วมมือผนึกกำลังด้านไซเบอร์กับภาคเอกชน และมิตรประเทศ
- กระทรวงกลาโหม ได้อนุมัติให้จัดตั้งศูนย์ปฏิบัติการไซเบอร์กลาโหมขึ้น โดยกองบัญชาการกองทัพไทย และ กองทัพบก กองทัพเรือและกองทัพอากาศได้เตรียมจัดตั้งหน่วยงานด้านไซเบอร์โดยตรง (Cyber Command) เพื่อขึ้นมารองรับการปฏิบัติงาน
- ศูนย์ปฏิบัติการไซเบอร์กลาโหม (Cyber Operations Center) เป็นแกนหลักในด้านการพัฒนาบุคลากร มีห้องปฏิบัติการสำหรับการฝึกปฏิบัติด้านสงครามไซเบอร์ (Cyber Warfare) และการสร้างภาคีเครือข่ายประชาคมทั้งภาครัฐและเอกชนเพื่อเสริมสร้างศักยภาพของประเทศด้านไซเบอร์

**การรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ ในระดับกองทัพบก**

กองทัพบกไทย มีหน้าที่หลักในการรักษาเอกราชและความมั่นคงของชาติ ถือเป็นหน่วยงานหลักด้านความมั่นคงของประเทศ เป็นองค์กรขนาดใหญ่ที่สุดของประเทศ ประกอบด้วยกำลังพลทั้งหมดกว่า 300,000 นาย มีหน่วยงานของกองทัพบกตั้งกระจายอยู่ในพื้นที่ทั่วประเทศไทย โดยหน่วยงานหลักในภูมิภาคก็คือ กองทัพภาคทั้ง 4 กองทัพภาค ความรับผิดชอบหลักของกองทัพบกคือ ต้องรักษาความมั่นคงภายในราชอาณาจักรและรักษาความสงบเรียบร้อยของชาติ[20]ในขณะที่ภัยคุกคามด้านไซเบอร์ (Cyber threat) ก็มุ่งกระทำต่อประชาชนของประเทศ โดยการทำให้เกิดความสับสน เข้าใจผิด และเกิดความวุ่นวายจากการได้รับข้อมูลข่าวสารที่ผิดพลาดและบิดเบือน ทำให้กองทัพบกต้องเข้ามารับผิดชอบต่อภัยคุกคามด้านไซเบอร์ของประเทศ และภัยที่มุ่งโจมตีต่อกองทัพบกโดยตรง ฝ่ายความมั่นคงและกองทัพบกจึงต้องดำเนินการจัดตั้งศูนย์ไซเบอร์กองทัพบก เพื่อปกป้องการกระทำจากกลุ่มผู้ไม่หวังดีที่ใช้เครือข่ายมุ่งโจมตีหน่วยงานของรัฐ หรือการเผยแพร่ข่าวสารอันเป็นเท็จที่ส่งผลกระทบต่อความมั่นคงของชาติ การจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) จึงเกิดขึ้นเพื่อปฏิบัติงานให้เป็นไปตามนโยบายของ

รัฐบาลโดยร่วมมือกับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security ; NCSC) โดยได้เริ่มทดลองปฏิบัติงานตั้งแต่ 1 ตุลาคม 2557 ซึ่งเป็นการปฏิบัติไปพร้อมกับเหล่าทัพต่าง ๆ โดยมีกองบัญชาการกองทัพไทย กองทัพเรือ กองทัพอากาศ สำนักงานตำรวจแห่งชาติและกระทรวงกลาโหม ซึ่งเป็นองค์กรที่กำหนดนโยบายเพื่อเตรียมความพร้อมกับภัยคุกคามทางไซเบอร์

**ศูนย์ไซเบอร์กองทัพบก (Army Cyber Center)**

ในปี 2559 กองทัพบกได้มีนโยบายและอนุมัติให้ศูนย์เทคโนโลยีทางทหาร (ศทท.)[21] ได้ดำเนินการปรับปรุงภารกิจและโครงสร้างการจัดหน่วย โดยเพิ่มเติมภารกิจด้านการปฏิบัติการสงครามไซเบอร์และปรับสายการบังคับบัญชาจากเดิมจากหน่วยขึ้นตรงกรมการทหารสื่อสาร ให้เป็นหน่วยขึ้นตรงกองทัพบก (นขต.ทบ.) และได้แปรสถานภาพหน่วยมาเป็นศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) และเมื่อวันที่ 1พฤศจิกายน 2559 ได้มีการปรับปรุงยกระดับหน่วยศูนย์ไซเบอร์กองทัพบก เพื่อเตรียมรองรับการปฏิบัติงานความมั่นคงปลอดภัยด้านไซเบอร์ โดยเฉพาะความมั่นคงทางการทหารและการรักษาความสงบเรียบร้อยภายในประเทศ รวมถึงการปฏิบัติการที่ประสานสอดคล้องกับกระทรวงกลาโหม กองบัญชาการกองทัพไทยและเหล่าทัพต่างๆ และร่วมมือกับหน่วยงานของภาครัฐและภาคเอกชนตลอดจน การปฏิบัติการร่วม ที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations ; NCO) โดยศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.)[22] ได้แบ่งโครงสร้างการจัดหน่วยเป็นสำนักงานผู้บังคับบัญชา กองธุรการ กองปฏิบัติการไซเบอร์ กองรักษาความปลอดภัยไซเบอร์ และกองสนับสนุนปฏิบัติการข่าวไซเบอร์ ซึ่งมีอำนาจหน้าที่ดังนี้

1. **กองปฏิบัติการไซเบอร์** ทำหน้าที่เป็นศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวัง แจ้งเตือน ป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์
    - การเผชิญเหตุฉุกเฉินด้านไซเบอร์เป็นหน่วยปฏิบัติการและเตรียมจัดตั้งกองรักษาความปลอดภัยด้านไซเบอร์ (Cyber Security Division) ซึ่งเป็นหน่วยปฏิบัติการด้านไซเบอร์เชิงรับ (Cyber Defensive Operations)
    - พัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุก เพื่อให้สามารถปฏิบัติการเชิงรุกและโต้ตอบโจมตีฝ่ายตรงข้ามได้ในกรณีจำเป็น

- มีการบรรจุและพัฒนากำลังพลที่มีความรู้ความเชี่ยวชาญและได้รับการฝึกฝนด้านการปฏิบัติการไซเบอร์ปฏิบัติหน้าที่เป็นนักรบไซเบอร์ (Cyber Warriors) อยู่ในชุดปฏิบัติการไซเบอร์ (Cyber Operation Teams ; COT) และชุดเตรียมพร้อมเผชิญเหตุฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Teams ; CERT)

2. **กองรักษาความมั่นคงปลอดภัยไซเบอร์** ทำหน้าที่เสริมสร้างความรู้ความเข้าใจ สร้างความตระหนัก ติดตาม กำกับดูแลการปฏิบัติของหน่วยตามมาตรการการรักษาความมั่งคงปลอดภัย
    - การเฝ้าระวัง แจ้งเตือนภัยคุกคาม การติดตาม สืบค้น และตรวจสอบช่องโหว่ของระบบ โดยใช้เครื่องมือระบบตรวจหาการบุกรุก
    - การดำเนินการพิสูจน์หลักฐานทางดิจิทัลดำเนินการด้านระเบียบการรักษาความปลอดภัยสารสนเทศ, การป้องกันเฝ้าระวังตรวจสอบช่องโหว่[4]โดยใช้เครื่องมือระบบตรวจหาการบุกรุก (Intrusion Detection System : IDS) และระบบป้องกันการบุกรุก (Intrusion Protection System : IPS)
    - การกู้คืนสภาพเมื่อถูกโจมตี (Recovery) ตลอดจนการพัฒนาโปรแกรมและเครื่องมือต่างๆ เพื่อรองรับงานด้านไซเบอร์
3. **กองสนับสนุนการปฏิบัติการข่าวสารไซเบอร์**ให้การสนับสนุนการปฏิบัติการข่าวสารของกองทัพบกและหน่วยที่เกี่ยวข้อง
    - ทำหน้าที่เฝ้าระวัง แจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ที่ส่งผลกระทบต่อสถาบันและความมั่งคงของชาติ
    - รวบรวม วิเคราะห์ทิศทาง แนวโน้ม โครงข่ายความสัมพันธ์ของข้อมูลประเภทสื่อ และกลุ่มเป้าหมาย ติดตาม สืบค้น แหล่งที่มาและเป้าหมาย
    - กำหนดมาตรการป้องปราม ตอบโต้สกัดกั้น ตลอดจนพัฒนาโปรแกรมและเครื่องมือต่าง ๆ เพื่อรองรับงานด้านไซเบอร์

นอกจากนี้ทางศูนย์ไซเบอร์ฯ ยังได้เตรียมการด้านการพัฒนาเทคโนโลยีและนวัตกรรมต่างๆ ด้านไซเบอร์โดยแสวงหาความร่วมมือกับหน่วยงานต่าง ๆ ทั้งภายในกองทัพบกและ

ภาครัฐ และองค์กรเอกชนในด้านวิชาการ การวิจัยพัฒนา (R&D) การสัมมนาเชิงปฏิบัติการ (Workshop) และการฝึกปฏิบัติต่าง ๆ โดยเฉพาะ

- การฝึกซ้อมแผนเผชิญเหตุด้านไซเบอร์ (Cyber Incident Action Plan Exercise)
- การฝึกซ้อมแผนฉุกเฉินด้านไซเบอร์ (Cyber Emergency)
- การประสานงานเพื่อดำเนินการตามกฎหมายกับผู้ที่โจมตีระบบเครือข่ายคอมพิวเตอร์

การจัดตั้งศูนย์ไซเบอร์กองทัพบกจะมุ่งเน้นการปกป้องงานของกองทัพบก เพื่อป้องกันการถูกแทรกแซงจากแฮกเกอร์ต่าง ๆ รวมทั้งงานที่เกี่ยวข้องกับด้านการข่าว โดยเน้นหนักไปในเรื่องการพัฒนากำลังคนและเครื่องมือ โดยเฉพาะที่กองทัพมีพื้นฐานรองรับงานต่าง ๆ ไว้แล้ว กองทัพบกได้มองเห็นปัญหาของภัยคุกคามทางไซเบอร์ซึ่งมีการใช้เทคโนโลยีเข้ามาทำลายความมั่นคงของประเทศ จึงได้เร่งพัฒนาเสริมศักยภาพของกองทัพไว้ให้พร้อมกับภัยที่กำลังเกิดขึ้น การรักษาความปลอดภัยทางไซเบอร์ของกองทัพบกจะมุ่งที่ความร่วมมือกับหน่วยงานภาครัฐและองค์กรภาคเอกชนโดยร่วมมือทั้งเรื่ององค์ความรู้และการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ที่เป็นภัยคุกคามร้ายแรงต่อระบบเครือข่ายคอมพิวเตอร์ มีการฝึกผู้เชี่ยวชาญด้านไซเบอร์ โดยเน้นในเรื่องการรักษาความประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัย

**แนวทางการปฏิบัติงานของ ศูนย์ไซเบอร์กองทัพบก**

ศูนย์ไซเบอร์กองทัพบก[23] มีภาระกิจในการ เฝ้าระวัง ตรวจสอบ การเตรียมความพร้อมเพื่อรับมือกับ ภัยคุกคามทางด้าน ความมั่นคงปลอดภัยทางด้านไซเบอร์ (Cyber Security) ดังกล่าวโดยการจัดหาเครื่องมือที่จำเป็น พร้อมทั้งการฝึกกำลังพลให้สามารถแก้ไขหรือตอบโต้ได้ในกรณีที่ถูกโจมตีทางไซเบอร์ และกำหนดให้การรักษาความมั่นคงทางด้านไซเบอร์เป็นภารกิจที่สำคัญในด้านความมั่นคงของชาติ โดยได้กำหนดระดับภัยคุกคามทางด้านไซเบอร์เป็น 4 ด้าน ดังนี้

1. ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ เป็นภัยคุกคามในระดับประเทศหรือระดับชาติ ผู้ที่ก่อภัยคุกคามอาจใช้วิธีเผยแพร่ข่าวสารเหล่านั้นให้เผยแพร่เข้ามาสู่ประเทศไทยจนสงผลกระทบต่อความมั่นคงภายในประเทศไทย และทำให้เกิดความได้เปรียบทางการเมืองหรือด้านความมั่นคง รวมทั้งการเผยแพร่ข้อมูลความลับของประเทศ

ไทย และการแพร่กระจายโปรแกรมไม่พึงประสงค์สำหรับการทำลายเครือข่ายระบบคอมพิวเตอร์

2. ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.) เป็นการใช้ไซเบอร์ที่เป็นภัยคุกคามต่อความมั่นคงของชาติในการเผยแพร่ข่าวสารของผู้ก่อความไม่สงบ เช่น การเผยแพร่ข่าวลือ ข่าวที่ไม่เป็นจริง โดยการกล่าวหาว่าเจ้าหน้าที่ของรัฐทำการละเมิดสิทธิมนุษยชน เพื่อให้สื่อมวลชนกระแสหลักนำข่าวไปเผยแพร่ต่อเพื่อต้องการให้ประชาชนทั่วไปหวาดกลัวจนทำให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่รัฐถือเป็นการปฏิบัติการข่าวสาร (Information Operation) ที่เป็นการปฏิบัติการจิตวิทยาอย่างหนึ่ง นอกจากนั้นยังมีการเผยแพร่ผลงานของผู้ก่อความไม่สงบที่อาจจะส่งผลกระทบทำให้เกิดแนวร่วมของผู้ก่อความไม่สงบเพิ่มมากขึ้น

3. ภัยคุกคามที่ส่งผลกระทบต่อสถาบันของชาติเป็นสิ่งที่กระทำได้ง่ายและยากต่อการดำเนินคดีต่อผู้กระทำผิดคือการเผยแพร่ภาพที่หมิ่นสถาบันพระมหากษัตริย์การวิจารณ์สถาบันในทางเสื่อมเสียซึ่งเจ้าหน้าที่ของรัฐบาลไทยไม่สามารถดำเนินการตามกฎหมายไทยได้เพราะส่วนหนึ่งของผู้กระทำความผิดไม่ได้อยู่ในประเทศไทยแต่ได้ใช้เว็บไซต์หรือสื่อโซเชียลในต่างประเทศเผยแพร่ข่าวสารเข้ามายังประเทศไทย

4. ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพไทย ทำให้ภาพลักษณ์ของผู้นำกองทัพไทยเสียหายหรือลดความน่าเชื่อถือในสังคมไทย รวมทั้งลดความเชื่อมั่นของประชาชนต่อการปกป้องประเทศไทย และการบังคับบัญชาของเหล่าทัพ ซึ่งส่งผลกระทบต่อการพิทักษ์อธิปไตยของชาติไทย

**แนวทางการพัฒนาศูนย์ไซเบอร์กองทัพบก**

ศูนย์ไซเบอร์กองทัพบกในปัจจุบันได้มีการ เตรียมความพร้อมเพื่อเผชิญกับภัยคุกคามทางด้านไซเบอร์ โดยจะเน้นไปในด้านความมั่นคงทางด้านไซเบอร์ความมั่นคงทางด้านทหาร ความมั่นคงของชาติเป็นภารกิจที่สำคัญ และได้ทำงานประสานกับหน่วยงานรัฐอื่น ๆ อีก เช่น หน่วยงานไทยเซิร์ตสังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งมีหน้าที่สำคัญในการรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์ต่างในภาคเศรษฐกิจและสังคม ดังนั้นศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) ในฐานะที่เป็นหน่วยรับผิดชอบงานความมั่นคงปลอดภัยทางไซเบอร์ จึงเน้นการพัฒนาขีดความสามารถของกำลังพล[25]ของกองทัพบกให้

สามารถรองรับภัยคุกคามทางไซเบอร์ได้หลากหลายรูปแบบ โดยจัดการฝึกอบรมกำลังพลของกองทัพบกซึ่งเป็นนายทหารสัญญาบัตรและชั้นประทวนประจำปีใน 7 หลักสูตร เพื่อให้แผนพัฒนาบุคคลากร สามารถตอบสนองภารนะกิจของศูนย์ไซเบอร์ได้ นอกจากนี้ยังได้เตรียมการด้านการพัฒนาเทคโนโลยีและนวัตกรรมต่างๆด้านไซเบอร์โดยแสวงความร่วมมือกับหน่วยงานต่างๆ ทั้งภายในและภายนอกกองทัพทั้งภาครัฐและองค์กรเอกชนในด้านวิชาการการวิจัยพัฒนา (R&D) การสัมมนาเชิงปฏิบัติการ(Workshop) และการฝึกปฏิบัติต่างๆ โดยเฉพาะ

- การฝึกซ้อมแผนเผชิญเหตุด้านไซเบอร์ (Cyber Incident Action Plan Exercise)
- การฝึกซ้อมแผนฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Exercise)
- การฝึกซ้อมการปฏิบัติการไซเบอร์ (Cyber Operations Exercise)
- การฝึกจำลองสงครามไซเบอร์ (Cyber Warfare Simulation Exercise)

โดยทางศูนย์ไซเบอร์กองทัพบก มีการวางแนวทางในการเพิ่มขีดความสามารถของการรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ (Cyber Security) ไว้ดังนี้

**การเพิ่มขีดความสามารถส่วนการสงครามสารสนเทศ (Information Warfare)**

กองทัพบกในปัจจุบันมีหน่วยหลักที่ให้บริการด้านเครือข่าย และระบบสารสนเทศ[26] คือ ศูนย์เทคโนโลยีทางทหาร ซึ่งมีหน้าที่หลัก และความสำคัญ คือ

- การให้การบริการอินเตอร์เน็ต มีการออกแบบ และกำหนดจุดกระจายสัญญาณตามพื้นที่ของหน่วยงานต่าง ๆ
- ตลอดจนรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations; NCO)
- การยกระดับการพัฒนาให้กองทัพบกเป็นองค์กรที่มีความเท่าเทียมกับองค์กรอื่น ๆ เป็นเรื่องที่จำเป็นและสำคัญ
- การเตรียมการรักษาความปลอดภัยหรือป้องกันการโจมตีระบบคอมพิวเตอร์ การติดตามสถานการณ์และเตรียมความพร้อมในการรับมือในสถานการณ์ฉุกเฉิน

การนำระบบคอมพิวเตอร์มาใช้เป็นจำนวนมากภายในองค์กรเพื่อเพิ่มประสิทธิภาพในการทำงานและเชื่อมต่อกับองค์กรภายนอกไม่ว่าจะอยู่ในพื้นที่ใดในโลก ก็เป็นการเปิดช่องทาง

การเข้าถึงของผู้ที่ไม่หวังดีต่อองค์กรสามารถเข้ามาโจมตีระบบเครือข่ายคอมพิวเตอร์ซึ่งเรียกกันโดยทั่วไปว่าแฮกเกอร์ (Hacker) คือการเข้าโจมตีระบบเครือข่ายคอมพิวเตอร์จนทำให้ระบบล่มและไม่สามารถใช้งานได้ทำให้เกิดความเสียหายจนเสียระบบการควบคุมโดยการโจมตีผ่านเครือข่ายอินเทอร์เน็ตจากส่วนหนึ่งส่วนใดในประเทศต่าง ๆ ในโลกนี้ การเสริมสร้างการรักษาความปลอดภัยของระบบให้แข็งแรงจึงเป็นสิ่งที่จำเป็น

**การเพิ่มขีดความสามารถสงครามไซเบอร์ (Cyber Warfare)**

ในสังคมยุคไซเบอร์[27]การเสริมสร้างกำลังทางทหารเพื่อการรบในพื้นที่ปฏิบัติการต่าง ๆ นั้นต้องใช้งบประมาณทางทหารเป็นจำนวนมากเพราะงบประมาณทางทหารเป็นรายได้ที่จัดเก็บจากภาษีรายได้จากประชาชนทั้งประเทศ

- การจัดตั้งกองกำลังไซเบอร์ที่เข้มแข็ง ให้เท่าเทียมอำนาจภัยคุกคามในระยะเวลาอันสั้นเป็นเรื่องที่ท้าทาย
- การเพิ่มศักยภาพของหน่วยเป็นสิ่งที่จำเป็น โดยเฉพาะการเฟ้นหาบุคคลกรที่มีคุณภาพตามความสามารถที่ต้องการทางเทคนิค
- การเสริมกำลังของหน่วย เกี่ยวข้องกับการวางแผนงบประมาณ และการจัดสรร และรวมถึงภาวะสภาพเศรษฐกิจ
- การมีงบประมาณรายจ่ายทางทหารมากก็จะกลายเป็นภาระของประเทศ ทำให้หน่วยงานตระหนักในเรื่อง แผนพัฒนาศักยภาพ กับภาวะภัยคุกคามร้ายแรงที่พัฒนาด้วยเช่นกัน
- กองทัพมีการพัฒนาด้วยการสร้างไซเบอร์วอริเออร์ Cyber Warrior) หรือเรียกว่านักรบไซเบอร์ในความหมายของการรักษาความมั่นคงในปัจจุบันเรียกว่าอำนาจการรบที่ไร้ตัวตนขึ้นเพื่อตอบโต้กับ ภัยคุกคามทางด้านไซเบอร์ (Cyber Threats)

**การเตรียมความพร้อมรับมือกับภัยคุกคามทางด้านไซเบอร์ของกองทัพบก**

จากนโยบายและแนวความคิดในการดำเนินการของหน่วยงานด้านไซเบอร์[24]ของกองทัพบกจะเห็นได้ว่า ความพร้อมในด้านการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยด้านไซเบอร์ของชาติยังอยู่ในขั้นของการเตรียมการ ซึ่งจะพอมองเห็นถึงความเป็นไปได้ใน

การดำเนินการไปสู่ขั้นของการปฏิบัติและผลสัมฤทธิ์ตามเจตนารมณ์ของผู้บังคับบัญชา กองทัพบกจะต้องเร่งดำเนินการแปลงนโยบายไปสู่การปฏิบัติอย่างเป็นรูปธรรมโดยเร็ว โดยเฉพาะในส่วนของ

- การเร่งดำเนินการด้านการปรับปรุงหรือการปฏิรูปโครงสร้างองค์กร (Organization Reform)
- การบรรจุกำลังพลที่มีความเชี่ยวชาญเฉพาะด้าน (Specialist)
- การพัฒนากำลังพล (Human Resource Development) ให้มีขีดความสามารถในด้านไซเบอร์

ภัยคุกคามทางด้านไซเบอร์ในวงการทหารถือว่าเป็นภัยที่คุกคามความมั่นคงของชาติซึ่งเชื่อมโยงไปสู่ด้านต่าง ๆ การกระทำทั้งหมดนั้นเป็นภัยที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในทางที่ผิดกฎหมายรวมทั้งการละเมิดต่อศีลธรรมและความสงบสุขของสังคม เป็นภัยร้ายแรงอีกรูปแบบหนึ่งในด้านการทหาร

**ความจำเป็นในการพัฒนานโยบาย Cyber security**[28]

การพัฒนานโยบายและคำถามพื้นฐาน 6 ข้อที่ต้องตอบเพื่อการกำหนดนโยบายได้อย่างถูกต้อง ได้แก่

1. การเลือกพัฒนาระบบโจมตี หรือจะพัฒนาระบบป้องกัน (Offense vs. Defense) โดยจริงแล้วภัยของการคุกคามทางไซเบอร์คือการถูกโจมตี ซึ่งเกิดขึ้นเวลาใดก็ได้ การขาดระบบป้องกันที่ดีกลับจะทำให้เราเป็นฝ่ายแพ้อย่างราบคาบ การพัฒนาระบบรับมือการโจมตีจึงควรเป็นสิ่งสำคัญลำดับแรก การป้องกันให้ไม่สามารถถูกโจมตี ถือเป็นชัยชนะโดยที่ยังไม่ได้ทำการต่อสู้
2. การปกป้องโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งรัฐมิได้ควบคุมด้วยตนเองโดยตรง จะเลือกนโยบายเสรีให้ต่างคนต่างรับผิดชอบตนเอง หรือต้องมีนโยบายกำกับดูแล (Market forces vs. Regulation) โครงสร้างพื้นฐานในยุคดิจิทัลล้วนเชื่อมต่อออนไลน์ และเสี่ยงต่อภัยคุกคามโดยมีความสัมพันธ์โดยตรงกับเสถียรภาพของรัฐ จึงจำเป็นต้องมีการกำกับดูแล โดยการออก Smart Regulation ตามด้วยการ

ตรวจสอบการปฏิบัติตามกติกา การทดสอบการโจมตีทางไซเบอร์ และการปรับปรุงพัฒนาระบบให้มีความปลอดภัย

3. การคุ้มครองความเป็นส่วนตัว หรือการคุ้มครองความปลอดภัย (Privacy vs. Security) สังคมมีความกังวลเกี่ยวกับการถูกละเมิดความเป็นส่วนตัวเพราะรัฐมักจะยกข้ออ้างเรื่อง Cybersecurity แต่หากไม่มี Cybersecurity ก็ไม่มีความเป็นส่วนตัว เพราะข้อมูลของเราจะถูกเจาะและลักลอบนำไปใช้ได้ตลอดเวลา สังคมต้องยอมรับให้ได้หากการเปิดเผยข้อมูลนั้นเป็นไปตามคำสั่งศาลโดยชอบด้วยกฎหมาย แต่ภัยคุกคามนั้นก็ต้องรับมือโดยเร็วให้ทันการณ์ โดยเรื่องนี้ทางศาลต้องตอบสนองปัญหาได้เร็วที่สุดแทนระบบการออกหมายศาลแบบเดิม
4. การลงทุนด้านซอฟต์แวร์ หรือการลงทุนพัฒนาคน (Software vs. People) ต้องให้ความสำคัญกับคนมากกว่าเน้นการซื้ออุปกรณ์หรือมุ่งพัฒนาระบบแล้วคิดว่าได้เตรียมการรับมือเรียบร้อยแล้ว และเราต้องค้นหาแฮ็คเกอร์ฝีมือดีแล้วเปลี่ยนให้เป็นบุคลากรด้าน Cybersecurity ของประเทศซึ่งก็ยังขาดแคลนเป็นอย่างมาก
5. นวัตกรรม หรือความน่าเชื่อถือ (Innovation vs. Reliability) ในยุคอินเตอร์เน็ตของสรรพสิ่ง มีอุปกรณ์เชื่อมต่อออนไลน์หลายพันล้านชิ้น และจะเพิ่มเป็นหลายหมื่นล้านชิ้นในอีกสามปีข้างหน้า ที่ผ่านมามีการเจาะระบบกล้องวงจรปิดนับแสนตัว เพื่อเข้าควบคุมและใช้เป็นฐานเพื่อโจมตี DDoS ไปยังระบบคอมพิวเตอร์เป้าหมาย หากอุปกรณ์หลายหมื่นล้านชิ้นเสี่ยงต่อภัยคุกคาม ความเสียหายจะมากขนาดไหน
6. การป้องกันการบุกรุก หรือความยืดหยุ่นในการรับมือการบุกรุก (Prevention of attack vs. Resilience) การป้องกันการบุกรุกคือความพยายามไม่ให้ผู้โจมตีเข้าสู่ระบบได้ แต่ความยืดหยุ่นในการรับมือ คือเมื่อผู้บุกรุกเข้ามาในระบบ จะจำกัดขอบเขตของปฏิบัติการโจมตีได้ในระดับใด และหากเกิดผลกระทบแล้วจะฟื้นฟูระบบให้กลับสู่ปกติโดยเร็วได้ หมายความว่าแต่ละระบบต้องมีข้อมูลสำรองและระบบสำรอง และต้องมีการฝึกซ้อมการกู้ระบบอย่างสม่ำเสมอ ไม่ต่างจากการซ้อมรับอัคคีภัยในอาคาร

**ข้อเสนอแนะจากงานวิจัย สำหรับการพัฒนาขีดความสามารถของกองทัพบกทางด้านการรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์**

1. กำหนดให้การป้องกันและกำจัดภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นหนึ่งในภารกิจหลักของกองทัพ ต้องมีการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber security) ที่มีความเหมาะสมกับองค์กรและมีประสิทธิภาพ และเร่งดำเนินการแปลงนโยบายไปสู่การปฏิบัติอย่างเป็นรูปธรรมและจริงจัง
2. ผลักดันให้มี กฎหมายว่าด้วยการกระทำผิดทางไซเบอร์ด้านความมั่นคง เพื่อเป็นเครื่องมือให้กับเจ้าหน้าที่ผู้ปฏิบัติงานในส่วนความมั่นคงให้หน่วยงานมีตวามสามารถในการบังคับใช้กฎหมายได้ด้วยตนเอง โดยในปัจจุบันมีเพียงกฎหมายว่าด้วยการกระทำผิดทางคอมพิวเตอร์ และต้องใช้หน่วยงานอื่นในการบังคับใช้กฎหมายเท่านั้น
3. ให้ความรู้เกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์แก่กำลังพลทุกระดับของกองทัพเพื่อเป็นการพัฒนากำลังพล (Human Resource Development) ให้มีความรู้ความสามารถและศักยภาพด้านวิทยาศาสตร์และเทคโนโลยี นอกเหนือจากความสามารถพื้นฐานทางการทหาร
4. การพิจารณาปรับปรุงหรือการปฏิรูปโครงสร้างขององค์กร (Organization Reform) ศูนย์ไซเบอร์กองทัพบก โดยให้มีการจัดอัตรากำลังพลด้านไซเบอร์และกำลังพลที่มีความเชี่ยวชาญเฉพาะด้าน (Specialist) เข้าเสริมในโครงสร้างของหน่วยระดับกองพันและกองกำลังผสมของกองทัพ ที่จะเปลี่ยนรูปแบบการจัดหน่วยให้มีขนาดเล็กและคล่องตัวในอนาคต โดยกำลังพลที่จะเพิ่มเติม อาจเป็นแบบพลเรือน-ทหารตามแนวทางลดกำลังพลที่เป็นทหารประจำการของกระทรวงกลาโหมก็เป็นได้
5. การมุ่งเน้นการพัฒนาศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ให้มีศักยภาพสามารถรับมือกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในกองทัพ และเชื่อมโยงร่วมมือกับหน่วยไซเบอร์นอกกองทัพได้อย่างมีประสิทธิภาพกองทัพบกจะต้องเน้นความร่วมมือกับหน่วยงานภาครัฐและองค์กรภาคเอกชนโดยร่วมมือทั้งเรื่ององค์ความรู้และการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ที่เป็นภัยคุกคามร้ายแรงต่อระบบเครือข่ายคอมพิวเตอร์โดยเพิ่มเติมเรื่องการฝึกผู้เชี่ยวชาญด้านไซเบอร์ในสถานการณ์ต่างๆ

6. การสร้างไซเบอร์วอริเออร์หรือเรียกว่านักรบไซเบอร์ ในความหมายของการรักษาความมั่นคงในปัจจุบันที่เรียกว่าอำนาจการรบที่ไร้ตัวตนขึ้นตอบโต้กับภัยคุกคามทางด้านไซเบอร์ (Cyber Threats) นั้น สามารถนำนโยบายการใช้หน่วยทหารอาสาไซเบอร์ และอาสาสมัครไซเบอร์มาทำงานเพื่อการป้องกันประเทศ โดยอาจจะเป็นตัวเลือกในการทำการสร้างไซเบอร์วอริเออร์ที่คุ้มค่า เหมาะกับแผนงบประมาณและความต้องการอันเร่งด่วน และสามารถสร้างกำลังพลให้กับหน่วยอย่างเพียงพอ ในระยะเวลาอันจำกัดได้ เช่น
    - การจัดตั้ง ทหารพรานไซเบอร์ (Cyber Para Military) เป็นกองกำลังเทคนิคและการข่าวแบบประจำถิ่นแบบมีค่าตอบแทน
    - ใช้กำลังสำรองจาก หน่วยบัญชาการรักษาดินแดน ที่มีจำนวนกำลังสำรองที่ได้รับการฝึกพื้นฐานทางด้านการทหารกระจายอยู่ตามภูมิภาค มาเพิ่มเติมความรู้ทางด้านความมั่นคงปลอดภัยทางไซเบอร์ให้เป็นองค์ความรู้พื้นฐาน เข้ากับภารกิจเดิม เช่นโครงการ “ร.ด.จิตอาสา”
    - จัดตั้งโครงการ “อาสาสมัคร ความมั่นคงปลอดภัยไซเบอร์ กองทัพบก” โดยเริ่มตั้งแต่ระดับเยาวชน ที่มีวุฒิภาวะเหมาะสม เช่น
        - อายุ 15-20 ปีเป็นระดับ “ยุวชนอาสาความมั่นคงปลอดภัยไซเบอร์ กองทัพบก”
        - อายุ 20 ปีขึ้นไป ถือเป็นระดับ “อาสาพัฒนาความมั่นคงปลอดภัยไซเบอร์ กองทัพบก”
        - คัดเลือกจากบุคคลทั่วไปที่สนใจเพื่อเป็น “อาสาสมัครความมั่นคงปลอดภัยไซเบอร์ กองทัพบก”
7. กองทัพบกต้องมีการฝึกซ้อมแผนเผชิญเหตุด้านไซเบอร์ (Cyber Incident Action Plan Exercise) และแผนฉุกเฉินด้านไซเบอร์ (Cyber Emergency) ร่วมกับหน่วยไซเบอร์นอกกองทัพอย่างสม่ำเสมอ เพราะภัยคุกคามทางด้านไซเบอร์ มีอำนาจการคุกคามเป็นวงกว้างในการสร้างวิกฤตการในครั้งเดียว เหตุการณ์คุกคามด้านไซเบอร์ (Cyber Incident) เหตุการณ์เดียว อาจจะมีผลกระทบในความเสียหาย ในหลายๆ องค์กรพร้อมๆกัน

8. การเพิ่มการวิจัยและพัฒนาไซเบอร์เพื่อความมั่นคง เพื่อให้เกิดการกระจายตัวและตื่นตัวกับระบบไซเบอร์เพื่อความมั่นคงในภาควิชาการ การวิจัยและการให้ทุนวิจัยในระดับมัธยมศึกษาและอุดมศึกษา โดยเป็นการเพิ่มแนวร่วมในการใช้ความรู้ความสามารถในทางสารสนเทศ และทักษะในการใช้งาน Social Network มาเพื่อพัฒนา ระบบไซเบอร์เพื่อความมั่นคง แบบพึ่งพาตนเองในอนาคตต่อไป
9. กองทัพบกควรต้องออกระเบียบการปฏิบัติงานและค่าตอบแทนของกำลังพลใหม่ โดยเฉพาะในเรื่องการปฏิบัติงานที่ต้องเกี่ยวข้องกับระบบคอมพิวเตอร์ และเทคโนโลยีสารสนเทศ การกำหนดค่าตอบแทนส่วนเพิ่ม สำหรับกำลังพลที่ได้รับการฝึกอบรมหรือมีความรู้ความสามารถทางด้านเทคนิคเพิ่มเติม มีวุฒิการศึกษาเพิ่มขึ้นเฉพาะทาง เพื่อจูงใจและเสนอความก้าวหน้าในชีวิตราชการกับบุคลากรด้านเทคนิค การบรรจุกำลังพลใหม่ ต้องรัดกุมในการคัดเลือกกำลังพลเข้ารับราชการ ป้องกันไม่ให้บุคคลที่มีความเสี่ยงต่อการก่อภัยไซเบอร์เข้ามาอยู่ในกองทัพ
10. ข้อเสนอในการทำงานทางเทคนิค ของศูนย์ไซเบอร์กองทัพบก
    - ควรเลือกใช้เทคนิค Machine Learning และนำเทคนิคดังกล่าวมาผสานรวมกับกลยุทธ์การตอบสนองต่อภัยคุกคาม เพื่อให้เข้าใจถึงรูปแบบการโจมตีของแฮกเกอร์และสามารถดำเนินการตัดสินใจเพื่อรับมือกับการโจมตีได้อย่างรวดเร็ว ถึงแม้ว่าจะไม่เคยพบรูปแบบการโจมตีนั้นมาก่อนก็ตาม
    - ศูนย์ไซเบอร์กองทัพบก อาจจะจะเริ่มกระบวนการพัฒนาระบบของแอปพลิเคชัน Serverless ตามความทันสมัยของเทคโนโลยีในปัจจุบัน การโจมตีข้อมูลที่ส่งผ่านไปมาข้ามระบบเครือข่ายและการโจมตีแบบ Denial of Service บนสถาปัตยกรรมแบบ Serverless มีมากขึ้น ควรมีการพิจารณาถึงประเด็นด้านความมั่นคงปลอดภัย การขยายระบบในอนาคต และการใช้ VPN หรือการเข้ารหัสข้อมูลเพื่อเพิ่มความมั่นคงปลอดภัย ในการปกป้องทราฟฟิกบนระบบเครือข่าย
    - การเก็บข้อมูลพฤติกรรมการใช้งาน บนอุปกรณ์อัจฉริยะ รูปแบบต่าง ๆ ที่ถูกนำมาใช้ในชีวิตประจำวัน อาจมีการดักจับและเก็บข้อมูลการใช้งานเพื่อนำไปใช้ประโยชน์ทางการตลาด โดยที่อุปกรณ์เหล่านี้อาจถูกนำมาใช้งานใน

หน่วยงาน หรือภายในครัวเรือนของกำลังพล ทั้งที่อยู่ในหรือนอกหน่วยที่ตั้งซึ่งอาจจะเป็นช่องทางที่ทำให้ข้อมูลด้านความมั่นคงอาจรั่วไหลโดยไม่ตั้งใจ

**ทางเลือกทางนโยบายในการพัฒนาศูนย์ไซเบอร์กองทัพบก**

การนำเสนอการเปรียบเทียบนโยบายการจัดและบริหารองค์กรทางด้าน Cyber Security สำหรับงานด้านความมั่นคง ของกระทรวงกลาโหมและเหล่าทัพ

1. แบบแยกกันบริหารงานด้วยการตั้งและใช้งาน Cyber Center ของแต่ละเหล่าทัพ, กองบัญชาการกองทัพไทย และ กรมเทคโนโลยีและอวกาศกลาโหม ตามนโยบายในปัจจุบัน เป็นการแบ่งหน้าที่ความรับผิดชอบด้าน Cyber Security ตามภูมิสภาพของหน่วยเพื่อให้ผู้บังคับบัญชาของหน่วย สามารถบริหารงานได้สะดวก โดยมีการเชื่อมโยงข้อมูลในระดับเหล่าทัพ ผ่านศูนย์ไซเบอร์กองทัพไทย แต่อาจไม่มีเอกภาพในการบูรณาการข้อมูล อาจไม่ตอบสนองการป้องกันภัยคุกคามด้านไซเบอร์ ที่มีลักษณะสามารถสร้างความเสียหายได้รวดเร็ว รุนแรง และเป็นวงกว้างได้
2. แบบรวมศูนย์บริหาร การตั้งและใช้งาน Cyber Center ของแต่ละเหล่าทัพโดยยกระดับบางหน่วยขึ้นเป็นหน่วยบัญชาการไซเบอร์ (Cyber Command) เพื่อการบริหารงาน Cyber Security อย่างมีเอกภาพ และมีประสิทธิภาพ ซึ่งต้องใช้งบประมาณสูงและแผนการพัฒนากำลังพลอย่างเร่งด่วนในการจัดตั้งหน่วยขั้นต้นให้มีขีดความสามารถ เช่นเดียวกันกับแนวทางของประเทศมหาอำนาจทางการทหาร
3. แบบผสม โดยเป็นแนวคิดจากการวิจัย ใช้การตั้งเป็นลักษณะ ศูนย์บัญชาการไซเบอร์แบบผสม (Hybrid Cyber Command) เพื่อรวมศูนย์การปฏิบัติเชิงนโยบายแต่แยกกันบริหาร ตามภูมิสภาพของหน่วย
    - การจัดให้มี ศูนย์บริหารนโยบายไซเบอร์เพื่อความมั่นคงกลาโหม (MOD Cybersecurity Policy & Management Center) เพื่อการควบคุมและบริหารงานเชิงนโยบายความมั่นคงไซเบอร์ ในระดับกระทรวงกลาโหม
    - การจัดตั้ง ศูนย์อำนวยการร่วมความมั่นคงไซเบอร์ (Joint Cybersecurity Directorate Center) ในระดับของกองทัพไทย เพื่อการปฏิบัติการร่วม

ความมั่นคงไซเบอร์ระหว่างเหล่าทัพ กองทัพไทย และกลาโหม ผ่านการควบคุมด้วยโครงข่าย (Network Centric Cybersecurity Operation) ตามลักษณะของการจัดหน่วยเพื่อการปฏิบัติการแบบผสมเหล่าตามแผนยุทธศาสตร์ความมั่นคง ของกระทรวงกลาโหม

- การตั้งและใช้งาน Cyber Center ของแต่ละเหล่าทัพเพื่อการบริหารงานด้านความมั่นคงไซเบอร์ตามภูมิสภาพอย่างอิสระ ตามนโยบายเดิมของกระทรวงกลาโหม
- เพิ่มการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพบกขึ้นเป็นหน่วยบัญชาการไซเบอร์ (Army Cyber Command) เพื่อเป็นหน่วยหลักในการปฏิบัติภาระกิจด้านไซเบอร์ของกองทัพบก ตามภูมิภาคต่างๆ เพื่อขยายความรับผิดชอบให้เหมาะสมกับระดับความสำคัญของภัยคุกคามในมิติที่ 5 ($5^{th}$ Domain) ในระดับยุทธศาสตร์

ภัยคุกคามด้านไซเบอร์ (Cyber Threats) เป็นภัยคุกคามรูปแบบใหม่ที่เป็นอันตรายใหญ่หลวงต่อประเทศชาติ มีลักษณะที่แตกต่างไปจากภัยคุกคามในอดีต ผู้ก่อเหตุสามารถโจมตีต่อทุกองค์กร ในหลายๆ องค์กรพร้อม ๆ กัน ไม่เว้นแม้กองทัพ โดยที่ไม่สามารถเข้าถึงตัวผู้ก่อการร้ายนี้ได้ในเวลาที่จำกัด การกระทำดังกล่าวก่อให้เกิดความเสียหายและมีผลกระทบต่อสังคมอย่างกว้างขว้างและเป็นภัยคุกคามที่ร้ายแรงที่บุคคลหรือองค์กรเล็กๆที่มีประสิทธิภาพ อาจสร้างความเสียหายได้อย่างมหาศาลในวงกว้าง การออกแบบองค์กรที่เหมาะสม จะเป็นแนวทางสำคัญไปสู่ความสำเร็จในการปฏิบัติ

ปัญหาหลักๆ ของการจัดการ รักษาความมั่นคงปลอดภัยไซเบอร์ในแทบจะทุก ๆ องค์กร คือ ผู้บริหารระดับสูง ไม่มีความเข้าใจในปัญหาและการจัดการกับปัญหา จึงไม่ให้ความสำคัญในเรื่องการสนับสนุนงบประมาณและอุปกรณ์เครื่องมือที่ใช้ในการทำงานจะเห็นความสำคัญเป็นครั้งคราว ก็ต่อเมื่อมีเหตุการณ์ถูกโจมตีทรัพยากรของหน่วย ผู้บริหารระดับนโยบายที่มีอำนาจก็ไม่มีความรู้ความเชี่ยวชาญที่ทันยุคทันสมัยและไม่ได้พยายามที่จะแสวงหา ด้านเจ้าหน้าที่ระดับปฏิบัติการก็ต้องทำงานโดยใช้ทรัพยากรเท่าที่มีมาปรับใช้

การเจริญเติบโตในสายงานที่ไม่ชัดเจน กำลังพลที่ความชำนาญเฉพาะทาง ส่วนใหญ่ทำงานไปในระยะหนึ่ง ก็จะเริ่มให้ความสำคัญกับค่าตอบแทน และเบนเข็มสู่ภาคธุรกิจและเอกชน

Cybersecurity ในระดับกองทัพ ต้องได้รับการยอมรับความสำคัญ จากผู้บังคับบัญชา มีการสร้างหลักนิยม และมีแนวทางการปฏิบัติทางยุทธวิธี ที่หลากหลายไม่ใช่การกำหนดนโยบายฝ่ายเดียวจากหน่วยงานแล้วใช้บังคับกับหน่วยที่ดำเนินกลยุทธ์ต้องสร้างความตระหนักรู้ และความเข้าใจแก่หน่วยในกองทัพอย่างจริงจังเพื่อให้เกิดการยอมรับแล้วการจัดการกับภัยคุกคามของความมั่นคงทางไซเบอร์จึงจะเกิดผล