Cyber Warfare

Hybrid War

โดย พลเอก เอกชัย ศรีวิลาศ

ผู้อำนวยการสำนักสันติวิธีและธรรมาภิบาล

สถาบันพระปกเกล้า

Technology/Innovation

- เทคโนโลยีใหม่ ๆ เกิดขึ้นมากมาย อาทิ Internet of Things, Robots, Artificial Intelligence (AI), Drones, Blockchain, Virtual reality, 3D Printing และ Electric vehicle ซึ่งเข้ามามีบทบาทในโลกมากขึ้น

- หากมองในด้านผู้ใช้งานเทคโนโลยีขั้นพื้นฐานอย่าง Internet พบว่าคนไทยมีอัตราการใช้ Internet ต่อหัวมากกว่าค่าเฉลี่ยโลกและกลุ่มประเทศเอเชียแปซิฟิก และใช้เวลากับ Mobile Internet มากที่สุดในโลก เฉลี่ย 4 ชั่วโมงต่อวัน คนไทยในกรุงเทพมหานครใช้ Facebook มากที่สุดในโลก

คำพูดของ Jack Ma ในการบริหารคน

“**ผมไม่รู้อะไรเกี่ยวกับเทคโนโลยีหรือการจัดการก่อนที่จะเริ่มธุรกิจ**เลยข้อเท็จจริงก็คือ คุณไม่จำเป็นต้องรู้อะไรมากมาย **คุณเพียงแค่ต้องหาคนที่ฉลาดกว่าคุณเองมาร่วมทำงานด้วย** ซึ่งเป็นเวลาหลายปีที่ผมพยายามหาคนที่เก่งกว่าผมเสมอ และเมื่อคุณพบคนเก่งมากมายแล้ว **งานของผมก็คือการทำให้แน่ใจว่าคนฉลาดสามารถทำงานร่วมกันได้**”

(อ้างอิงจาก https://www.youtube.com/watch?v=IhPZfLlouLE)

NEWS

ด่วน!! อีเมล์ ถูกแฮก 773 ล้านบัญชีทั่วโลก เราจะเช็คและป้องกันอย่างไร

By Pantawat — On ม.ค. 18, 2019

Share

อีเมล์ ถูกแฮก มากกว่า 773 ล้านบัญชีทั่วโลก

HOME NEWS CULTURE LIFESTYLE OPINION VIDEO PODCAST MAGAZINE CONTACT

WORLD TECH

พบข้อความส่วนตัวของผู้ใช้ Facebook อย่างน้อย 81,000 บัญชี ถูกแฮกและขายในโลกออนไลน์

โดย คมปกิต สกุลหวง
03.11.2018

3.1K

การโจมตีทางไซเบอร์ที่ซอฟต์แวร์แอนตี้ไวรัส ไม่สามารถป้องกันได้

- ระบบป้องกันความปลอดภัยที่อาศัยซอฟต์แวร์แอนตี้ไวรัส (Anti-Virus) ได้พัฒนาถึงที่สุดแล้ว อย่างที่ Brian Dye อดีต SVP ฝ่ายการจัดการความปลอดภัยข้อมูลของ Symantec ซึ่งเป็นบริษัทยักษ์ใหญ่ของผู้จำหน่ายซอฟต์แวร์ความปลอดภัย
- Dye บอกว่า ซอฟต์แวร์แอนตี้ไวรัส (Anti-Virus) ได้สิ้นสุดลงแล้ว เพราะซอฟต์แวร์แอนตี้ไวรัส (Anti-Virus) ตรวจพบการโจมตีทางไซเบอร์ได้เพียง 45% ที่เหลืออีก55% ไม่สามารถตรวจพบได้
- การพัฒนาระบบป้องกันความปลอดภัยในอนาคต จะต้องศึกษาอย่างเร่งด่วน เพื่อคาดการณ์การโจมตีจากไวรัสคอมพิวเตอร์หรือซอฟต์แวร์หรือรหัสคำสั่งที่ไม่พึงประสงค์อื่นๆ เพื่อป้องกันการเกิดความเสียหายด้วยการโจมตีทางไซเบอร์ที่รุนแรงยิ่งขึ้น
- ปัญญาประดิษฐ์ (AI) จะกลายเป็นที่นิยมในการป้องกันความปลอดภัย

https://www.fujitsu.com/th/th/about/resources/featurestories/whitepaper10.html

Jack Ma พูดถึงเรื่องความปลอดภัยกับ AI

Jack Ma: รู้หรือไม่ว่า แต่ละวันมีคนโจมตีอาลีบาบาทางไซเบอร์กว่า 3 ล้านครั้ง แต่เราให้ AI ซึ่งย่อมาจาก Alibaba Intelligence มาจัดการ

"ผมมักจะบอกกับคนที่คอยป้องกันเหตุร้ายทางไซเบอร์ว่า คนเราถ้าจะรักใครสักคน มันไม่มีเหตุผลหรอก แต่เวลาเราเกลียดใครสักคน เราหาเหตุผลร้อยแปดเพื่อเกลียดคนนั้นให้ได้ ฉะนั้น **ถ้าอยากให้ AI จัดการกับภัยคุกคามทางไซเบอร์ เราก็สอนให้ AI รู้จักและจับพฤติกรรมที่เป็นภัยต่ออาลีบาบาแค่นั้นเอง**"

ปรากฏการณ์ของโลกในศตวรรษที่ 21

- สับสน อลหม่าน (Disorder)
- สลับซับซ้อน (Complexity)
- แข่งขันสูง (High Competition)
- พยากรณ์ไม่ได้ (Unpredictable)
- รวดเร็ว (Speed)
- เกี่ยวโยงกัน (Concerned)
- เครือข่าย (Network)

โลกวันนี้

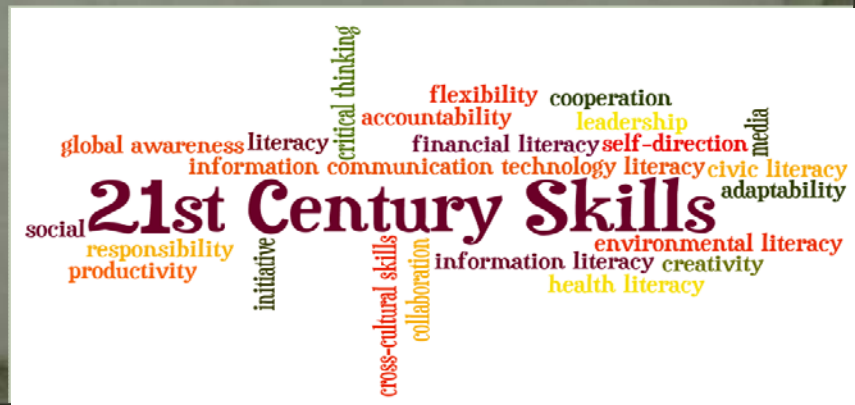
- โลกเรากำลังถูก Disrupt ด้วย 3 กระแสหลัก คือ กระแสโลกาภิวัตน์ กระแสการพัฒนาเทคโนโลยี และกระแสความเป็นใหญ่ของเงินทุน
- เงินเคยเป็นตัวเปลี่ยนอารยธรรมของมนุษย์ โลกาภิวัตน์และเทคโนโลยีทางการเงิน วันนี้เงินกลับมาเป็นตัวขับเคลื่อนโลกในด้านต่าง ๆ อย่างมาก
- อดีตเราต้องทำงานเพื่อแลกเงิน ปัจจุบันเงินสามารถสร้างเงินได้โดยไม่ต้องสร้างมูลค่าจริงทางเศรษฐกิจเลย แถมยังเคลื่อนย้ายได้อย่างรวดเร็ว ซึ่งเงินจะค่อย ๆ พัฒนารูปแบบเป็น Digital มากขึ้น และคนรวยคนจนจะยิ่งมีช่องว่างมากขึ้น
- 3 กระแสหลักนี้ ได้สร้างปรากฏการณ์ทางเศรษฐกิจและสังคมในโลกสมัยใหม่ที่เรียกว่า **'VUCA'**
  - **V: volatility = ความผันผวน รวดเร็วรุนแรง**
  - **U: uncertainty = ความไม่แน่นอน คาดเดาไม่ได้**
  - **C: complexity = ความซับซ้อน เข้าใจยาก**
  - **A: ambiguity = ความคลุมเคลือ ไม่ชัดเจน**

ทักษะในศตวรรษที่ 21

- **ทักษะการเรียนรู้และนวัตกรรม** มีความคิดสร้างสรรค์ ใส่ใจนวัตกรรม มีวิจารณญาณ แก้ปัญหาเป็น สื่อสารดี เต็มใจร่วมมือ
- **ทักษะสารสนเทศ** สื่อ เทคโนโลยี อัพเดตทุกข้อมูล ข่าวสาร รู้เท่าทันสื่อ รอบรู้เทคโนโลยีสารสนเทศ ฉลาดสื่อสาร
- **ทักษะชีวิตและอาชีพ** มีความยืดหยุ่น รู้จักปรับตัว ริเริ่มสิ่งใหม่ ใส่ใจดูแลตัวเอง รู้จักเข้าสังคม เรียนรู้วัฒนธรรม

ความสำคัญของ 4 ทักษะ

- โลกยิ่งเปลี่ยนเร็วเท่าไร = เรายิ่งต้องสร้างทักษะการเรียนรู้ให้เร็วขึ้นโดยการใช้เทคโนโลยีมาช่วย
- โลกยิ่งมีความไม่แน่นอนสูง = เรายิ่งต้องสร้างทักษะการปรับตัวเพื่อรับความผันแปรและความเสี่ยง
- โลกยิ่งมีความซับซ้อนสูง = เรายิ่งต้องมีที่ยืน สร้างจุดแข็งให้กับตัวเอง
- โลกยิ่งมีความไม่ชัดเจนสูง = เรายิ่งต้องสร้างภาวะผู้นำ



สงครามในรูปแบบต่าง ๆ

สงครามผสม (Compound War)

- เป็นสงครามที่มีลักษณะของการเชื่อมโยงทางยุทธศาสตร์ แต่มีการปฏิบัติที่แยกส่วนกันระหว่างกำลังตามแบบ (Regular War) และกำลังนอกแบบ (Irregular War)
- ใช้การประสานสอดคล้องในการปฏิบัติการทางทหารเป็นหลัก การปฏิบัติการทางทหารจะมีการแบ่งแยกเขตความรับผิดชอบหรือพื้นที่ปฏิบัติการกันอย่างชัดเจน

ตัวอย่างของสงครามผสม

- สงครามปฏิวัติของสหรัฐฯ ที่ใช้ทั้งกำลังทหารหลักและกำลังทหารบ้านหรือกำลังประจำถิ่น ในการต่อสู้เพื่อเอกราชจากอังกฤษ
- สงครามเวียดนามที่ฝ่ายเวียดนามเหนือ ได้ใช้การผสมผสานการปฏิบัติทางทหารระหว่าง กองทัพเวียดนามเหนือและเวียดกง

ประเภทของสงคราม

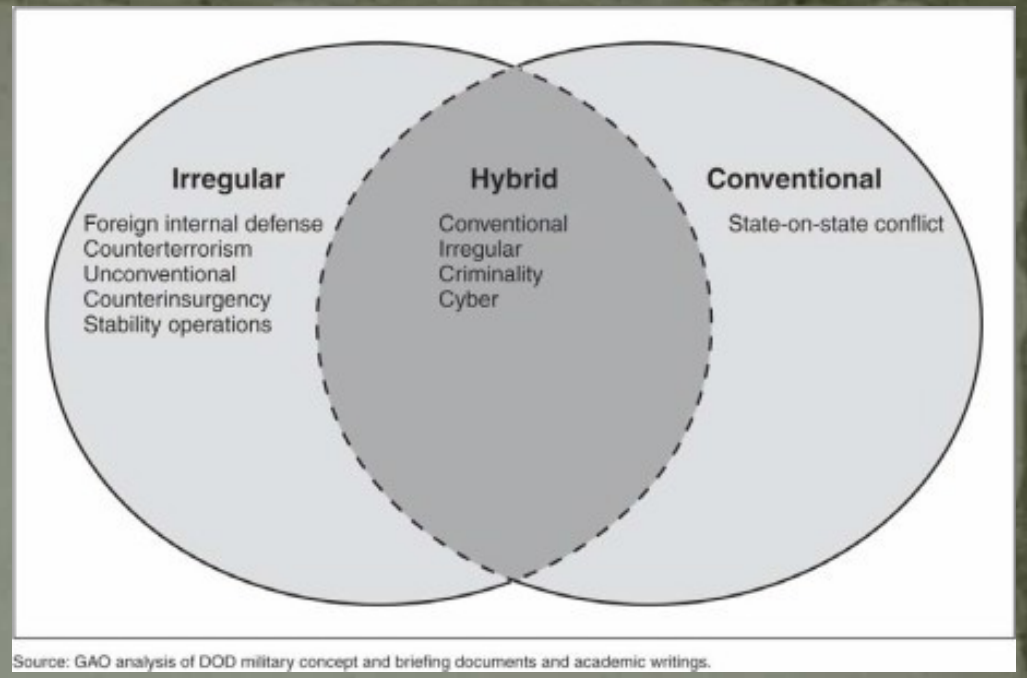
สงครามตามแบบ หรือสมมาตร (Regular Forces)	สงครามนอกแบบ หรืออสมมาตร (Irregular Forces)
1. เป็นการต่อสู้ด้วยกำลังอาวุธ หรือใช้มาตรการทางการทหารเข้าสู้รบกัน	1. เป็นการต่อสู้ด้วยมาตรการต่างๆ ทั้งทางการเมือง เศรษฐกิจ สังคมจิตวิทยา การทูต เทคโนโลยี และการใช้มาตรการทางทหาร
2. เป็นการทำสงครามแบบเปิดเผยตัวตน มีการเผชิญหน้ากันโดยตรงระหว่างกำลังทหารของคู่สงคราม	2. ไม่มีการเผชิญหน้าระหว่างคู่กรณีโดยเปิดเผย
3. เป้าหมายจำกัดที่กำลังทหารเท่านั้น	3. เป้าหมายไม่ได้จำกัดที่กำลังทหารเท่านั้น แต่ยังรวมถึงประชาชนด้วย เป็นสงครามแบบเบ็ดเสร็จ โดยใช้เทคนิคการก่อความไม่สงบและการก่อการร้าย

ประเภทของสงคราม

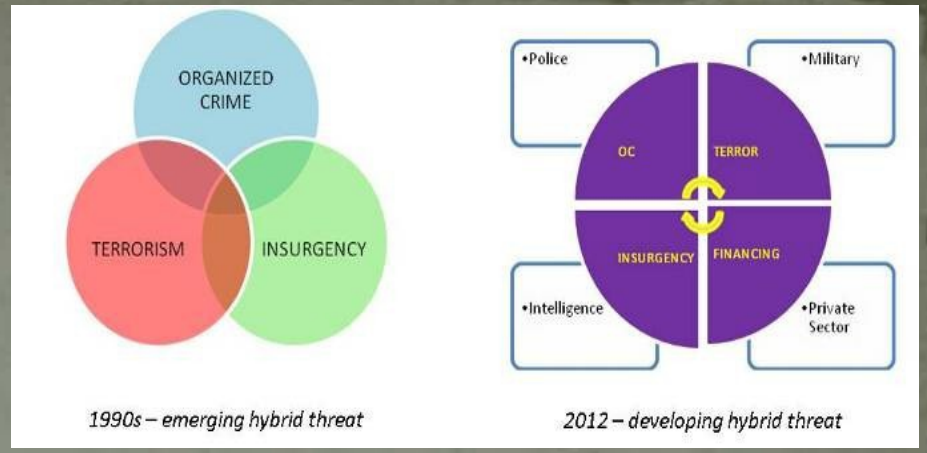
สงครามตามแบบ (Regular Forces)	สงครามนอกแบบ (Irregular Forces)
4. คู่สงครามหรือความขัดแย้งเป็นรัฐต่อรัฐ	4. คู่สงครามหรือความขัดแย้งไม่จำเป็นต้องเป็นรัฐต่อรัฐ แต่จะเป็นรัฐต่อกลุ่มคนที่ไม่ใช่รัฐก็ได้
5. วิธีการดำเนินการแบบพื้นฐาน 3 แบบ คือการยุทธด้วยวิธีรุก ด้วยวิธีรับ และด้วยวิธีร่นถอย รวมถึงการยุทธภายใต้สภาพพิเศษ	5. มีสงครามพิเศษ สงครามการเมือง สงครามนิวเคลียร์ สงครามศาสนา สงครามไซเบอร์ และสงครามประเภทอื่นๆ ที่ไม่สามารถจัดอยู่ในสงครามตามแบบ
6. รวมกำลังเป็นกลุ่มก้อน อันตรายมาก	6. แยกย้ายกระจายกันอยู่ อันตรายน้อย
7. หลักนิยมและยุทธวิธีการรบเป็นระเบียบ ประเมินสถานการณ์ได้ง่าย ข้าศึกทราบหนทางปฏิบัติ และโต้ตอบได้ง่าย	7. ทำการรบไม่มีแบบฉบับ ข้าศึกประมาณสถานการณ์ไม่ถูก ไม่ทราบหนทางปฏิบัติ ตอบได้ยาก

Hybrid War

- Hybrid War เป็นการผสมผสานสงครามหลายรูปแบบ
- ทั้งสงครามตามแบบในระดับต่ำ ปฏิบัติการพิเศษ สงครามไซเบอร์ สงครามอวกาศ และสงครามจิตวิทยา
- ผสมผสานระหว่างขีดความสามารถของสงครามตามแบบ ยุทธวิธีนอกแบบ และการก่อการร้ายที่ใช้ความรุนแรง
- การบีบบังคับขู่เข็นให้เกิดความหวาดกลัว และการก่ออาชญากรรมในรูปแบบต่างๆ



Hybrid War



- เป็นสงครามผสมผสานกำลังตามแบบและกำลังนอกแบบ ปฏิบัติการทางทหารร่วมกันอย่างแยกไม่ออก
- การปฏิบัติการที่มุ่งเป้าหมายไปที่รัฐเสรีประชาธิปไตย และช่องโหว่ของระบบสถาบันผ่านช่องทางต่างๆที่หลากหลาย เช่น การเมือง เศรษฐกิจ ทหาร ประชาชนพลเมือง และข้อมูล...

- สงครามระหว่างอิสราเอล-เลบานอนครั้งที่ 2 (2006)
  - กลุ่มฮิสบุลเลาะห์ เป็นกลุ่มติดอาวุธ ที่ทำสงครามต่อต้านอิสราเอลในเลบานอน เป็นผู้ก่อตั้งต้นแบบของสงครามพันทาง **Hybrid War**

การปฏิบัติการ Hybrid War ของรัสเซีย

"THE RUSSIAN VIEW OF MODERN WARFARE IS BASED ON THE IDEA THAT THE MAIN BATTLESPACE IS THE MIND."
– NATIONAL DEFENCE ACADEMY OF LATVIA POLICY PAPER

- **เป้าหมายหลัก**

1) การยึดดินแดนโดยไม่ต้องใช้กำลังทหารตามแบบอย่างโจ่งแจ้ง ดังเช่น การผนวกดินแดนที่แหลมไครเมียจากยูเครนในปี 2014

2) สร้างเงื่อนไขในการใช้กำลังทางทหารแบบธรรมดาได้ การผนวกดินแดนไครเมียเป็นสัญญาณว่ารัสเซียสามารถใช้ **Hybrid War** แบบนี้เพื่อผนวกดินแดนในที่อื่นได้ เช่น ในกลุ่มประเทศบอลติก

3) ใช้ Hybrid War เพื่อส่งอิทธิพลทางการเมืองและนโยบายต่อประเทศตะวันตกและที่อื่นๆ เป้าหมายเพื่อท้าทายใหญ่ต่อรัฐบาลตะวันตกและสหรัฐ

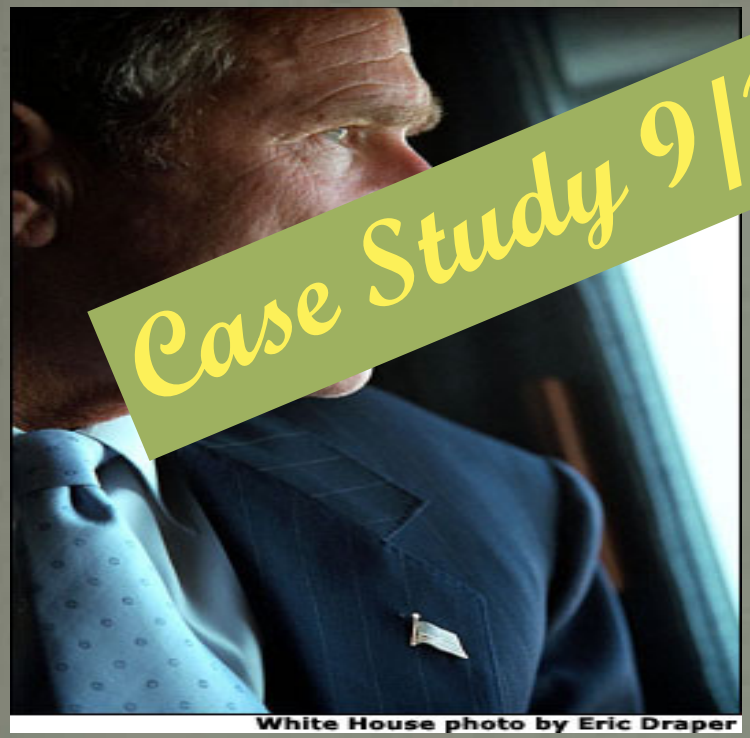
เครื่องมือที่ใช้ใน Hybrid War ของรัสเซีย

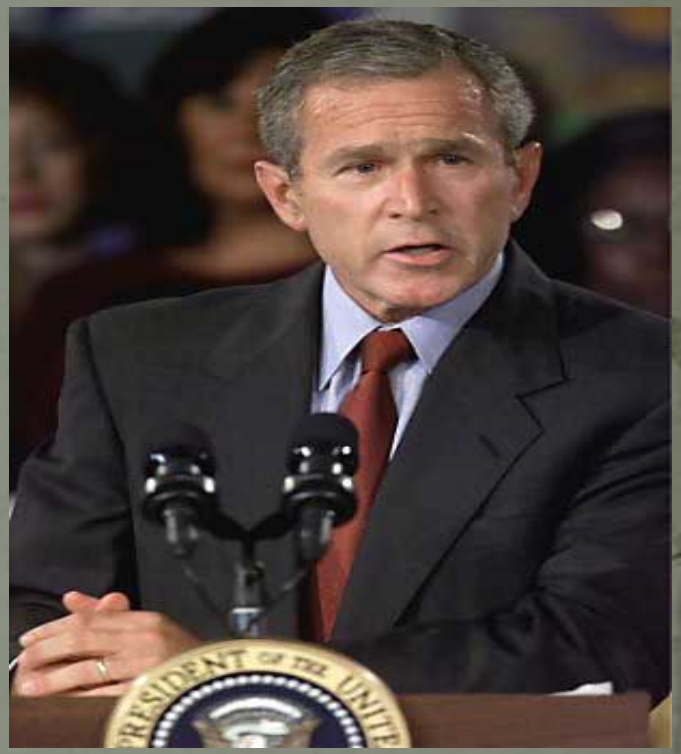
1) **ปฏิบัติการข่าว โดยใช้สื่อ เช่นรัสเซียทูเดย์** เพื่อส่งเสริมทัศนะของรัสเซีย ไปจนถึงการสร้างข่าวปลอม
2) **สงครามไซเบอร์** รัสเซียสร้างนักรบไซเบอร์ขึ้นเป็นจำนวนมากเพื่อล้วงความลับจากระบบข่าวสารตะวันตก
3) **กลุ่มตัวแทนซึ่งมีความเห็นอกเห็นใจในเป้าหมายของรัสเซีย** เช่นกลุ่ม “หมาป่ากลางคืน” ซึ่งเป็นสโมสรนักขับมอเตอร์ไซค์และความบันเทิง
4) **อิทธิพลทางเศรษฐกิจที่สำคัญ** ได้แก่การใช้พลังงานเป็นเครื่องมือทางนโยบายการต่างประเทศ ในหลายประเทศในยุโรปที่ต้องพึ่งพาก๊าซธรรมชาติจากรัสเซียเป็นต้น
5) **มาตรการลับต่างๆ** มีทั้งการติดสินบน การกรรโชก และความพยายามอื่นๆ ในการชักใยนักการเมืองที่มีปัญหาให้สนับสนุนนโยบายของรัสเซีย
6) **อิทธิพลทางการเมือง** ใช้งานทางการทูตธรรมดาๆ เพื่อสนับสนุนบุคคลและพรรคการเมืองที่นิยมหรือเห็นอกเห็นใจรัสเซีย มีการเชิญให้ไปเยือนรัสเซียในฐานะบุคคลสำคัญ

Hybrid War

- การเกิดเหตุก่อวินาศกรรมเมื่อ 9 ก.ย. 2544 หรือ 9/11 ในสหรัฐอเมริกา
  - เป็นการก่อการร้ายที่มีรูปแบบของการปฏิบัติการที่แตกต่างไปจากเดิม ที่มีความรุนแรง และความเสียหายมากขึ้น
  - เป็นขบวนการในทางลับ มีการประสานสอดคล้องอย่างลงตัว และได้สร้างความเสียหายทั้งชีวิต ทรัพย์สินเป็นจำนวนมาก
  - สร้างความหวาดกลัว เสียใจ ความโกรธแค้นให้กับผู้ที่ได้รับผลกระทบโดยตรง ซึ่งส่วนใหญ่ไม่ได้เกี่ยวข้องกับมูลเหตุของความขัดแย้งเพราะเป็นผู้บริสุทธิ์ ที่ถูกเลือกให้เป็นเป้าหมาย

Case Study 9/11 in U.S.A.



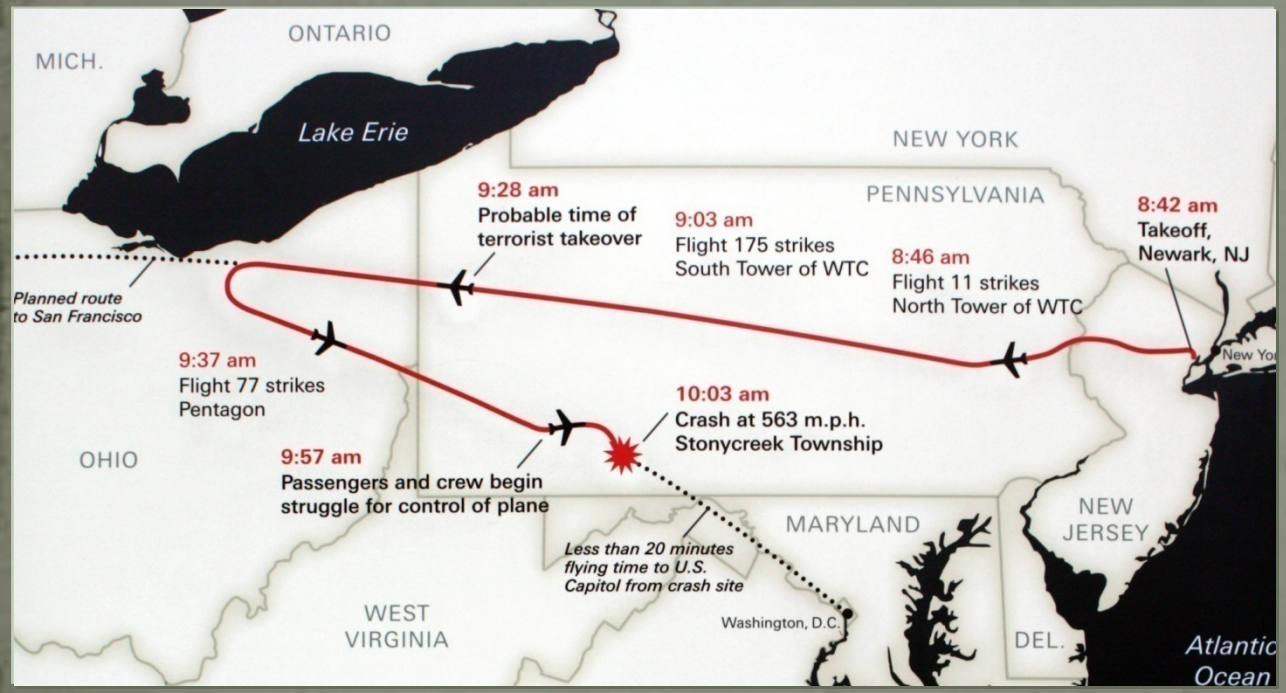


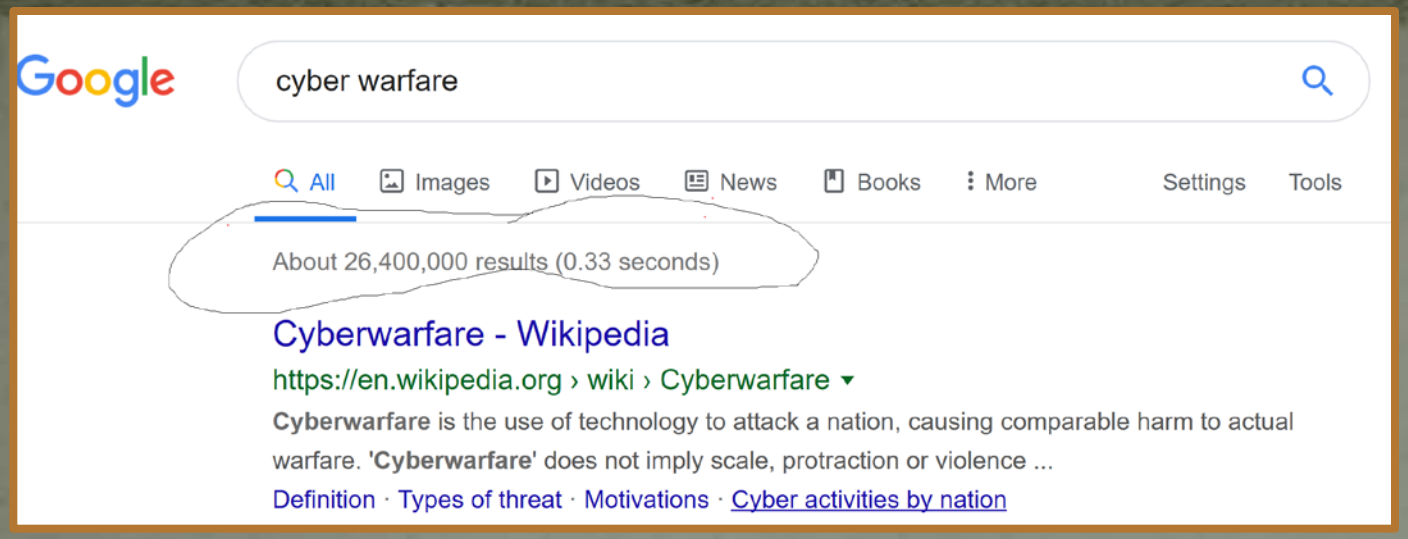
America has stood down enemies before, and we will do so this time.
Bush September, 11, 2001

American Land of Power: Political, Economic and Military

World Trade Building

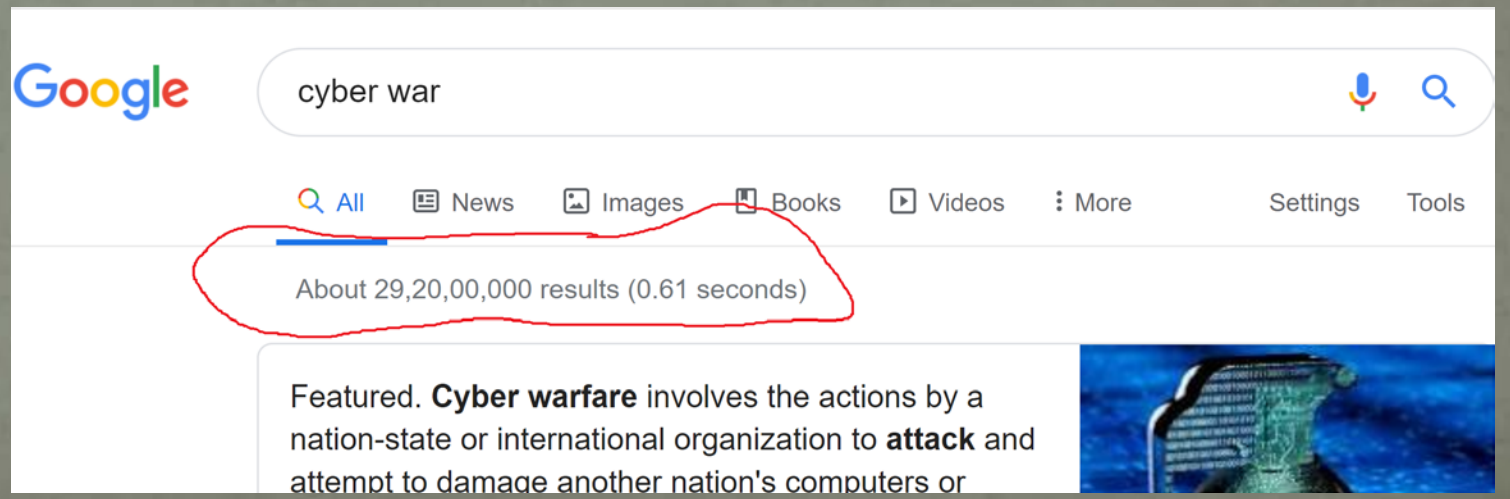
Pentagon building of the
United States Department of Defense


ONTARIO
MICH.
Lake Erie
NEW YORK
PENNSYLVANIA
9:28 am
Probable time of
terrorist takeover
9:03 am
Flight 175 strikes
South Tower of WTC
8:46 am
Flight 11 strikes
North Tower of WTC
8:42 am
Takeoff,
Newark, NJ
Planned route
to San Francisco
9:37 am
Flight 77 strikes
Pentagon
10:03 am
Crash at 563 m.p.h.
Stonycreek Township
OHIO
9:57 am
Passengers and crew begin
struggle for control of plane
MARYLAND
NEW
JERSEY
Less than 20 minutes
flying time to U.S.
Capitol from crash site
WEST
VIRGINIA
Washington, D.C.
DEL.
Atlantic
Ocean



ค้นหาจาก google คำว่า Cyber Warfare พบ 26 ล้าน ข้อความ

Cyber War พบ 29 ล้าน ข้อความ



การพัฒนาเทคโนโลยีดิจิทัล

- ปรากฏการณ์ที่เกิดขึ้นในช่วง 2-3 ปีที่ผ่านมาได้พิสูจน์ว่า การพัฒนาเทคโนโลยีดิจิทัลเพื่อพัฒนาประเทศนั้น จะต้องสร้างเรื่องความมั่นคงปลอดภัยไซเบอร์
- ข้อแนะนำเชิงวิชาการ เช่น จาก Harvard Business Review แก่ผู้นำและผู้บริหารระดับประเทศทั้งภาครัฐและเอกชนที่จะต้องมีความรู้ความเข้าใจอย่างลึกซึ้งในระบบนิเวศไซเบอร์ (Cyber ecosystem) เพราะหากรู้เพียงว่า “ใช่ มันสำคัญ” แต่ไม่รู้ว่า “จะจัดการกับมันอย่างไร” ผลที่ออกมาก็จะเท่ากับว่า เราไม่รู้อะไรเลยนั่นเอง
- การตัดสินใจของประเทศต่างๆ ในการวิ่งเข้าสู่ “ประเทศดิจิทัล” โดยที่ประเทศนั้นๆ มิใช่ผู้คิดค้นนวัตกรรมดิจิทัล ก็จะต้องมียุทธวิธีในการเดินเกมอย่างระมัดระวังและชาญฉลาด
- เพราะเป็นไปไม่ได้ที่ประเทศเหล่านี้จะปฏิเสธการใช้เทคโนโลยี Digital platform ของต่างประเทศที่ใช้กันทั่วโลก อย่างเช่น Google, Youtube, Facebook, Samsung และ iPhone เป็นต้น เพราะเทคโนโลยี่ที่กล่าวมาข้างต้น ได้กลายเป็น Digital platform ในการเชื่อมโยงระบบเศรษฐกิจดิจิทัล (Digital economy) ทั่วโลกไปแล้ว

Cyber

- Digital ลักษณะการเก็บข้อมูลคอมพิวเตอร์ มีวิธีการเก็บสถานะเปิดหรือปิด บวกหรือลบ คอมพิวเตอร์ที่ใช้กันอยู่ในปัจจุบันจะเป็น Digital ร้อยละ 99 ถ้าข้อมูลเป็น analog จะต้องเปลี่ยน เป็น Digital ก่อน จึงจะส่งเข้าไปประมวลผลในคอมพิวเตอร์ได้ ระบบ Digital จะให้ค่าที่เป็นตัวเลข ที่แม่นยำกว่าระบบ analog
- Hybrid หมายถึงลูกผสมข้ามชนิดหรือสายพันธุ์ ยานพาหนะที่มีเครื่องยนต์สองระบบ สิ่งมีชีวิตในเทพนิยายซึ่งร่างกายประกอบด้วยส่วนของสัตว์หลายชนิดผสมกัน คอมพิวเตอร์ลูกผสม ไม้กอล์ฟหัวผสม เช่นหัวกึ่งไม้กึ่งเหล็ก
-

Cyber

- มาจากคำว่า Cybernetics เป็นภาษากรีก แปลว่า ความสามารถในการนำ (Steering) หรือ การปกครอง (Governing)
- Cybernetics เป็นวิชาการเกี่ยวกับระบบควบคุม เช่น ระบบประสาทของสิ่งมีชีวิต เพื่อนำไปใช้พัฒนาระบบอิเล็กทรอนิกส์ หรือระบบที่ทำงานคล้ายคลึงกัน
- ในการควบคุมการพูดและการทำงานของสมองเกี่ยวกับคอมพิวเตอร์และอิเล็กทรอนิกส์ เพื่อการควบคุมในระยะไกล หรือควบคุมเครือข่ายอิเล็กทรอนิกส์
- เป็นระบบเครือข่ายและสังคมเครือข่ายทั่วโลก เช่น อินเทอร์เน็ต (Internet) และ สารสนเทศเสมือนจริง (Virtual) ที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง
- E- ย่อมาจาก อิเล็กทรอนิกส์ (Electronic) ใช้ในนำหน้าผลิตภัณฑ์หรือบริการที่อยู่ในรูปของอิเล็กทรอนิกส์ เช่น จดหมายอิเล็กทรอนิกส์ (e-mail) การค้าอิเล็กทรอนิกส์ (e-commerce) ธุรกิจอิเล็กทรอนิกส์ (e-business) การธนาคารอิเล็กทรอนิกส์ (e-banking) และ หนังสืออิเล็กทรอนิกส์ (e-book) เป็นต้น

Cyber

- Cyber จึงเป็นความหมายในเชิงนามธรรม ซึ่งครอบคลุมมากกว่าคอมพิวเตอร์ ซึ่งมีความหมายในเชิงรูปธรรม แต่ Cyber เป็นส่วนหนึ่ง หรือ Subset ของระบบข้อมูลข่าวสาร (Information System)
- ในทางปฏิบัติระบบข้อมูลข่าวสาร (Information System) ห้วงไซเบอร์ (Cyberspace) และเครือข่ายคอมพิวเตอร์ (Computer Network) จึงไม่สามารถแยกแยะออกจากกันได้
- ห้วงไซเบอร์ (Cyberspace) เป็นขอบเขตที่กำหนดโดยการใช้อุปกรณ์อิเล็กทรอนิกส์ และแถบคลื่นแม่เหล็กไฟฟ้าในการจัดเก็บ แก้ไขเปลี่ยนแปลง และแลกเปลี่ยนข้อมูล ผ่านทางระบบเครือข่ายและโครงสร้างสาธารณูปโภคทางกายภาพที่เกี่ยวข้อง

ภัยคุกคามไซเบอร์

- ภัยคุกคามได้ลุกลามไปทั่วโลก ไม่ว่าจะเป็นการโจมตีระบบธนาคาร 5 แห่งในรัสเซีย
- ข่าวการเจาะระบบการเลือกตั้งของสหรัฐฯ จากแฮ็กเกอร์นอกประเทศ
- แฮ็กเกอร์รัสเซียเจาะระบบ database ของ World Anti-Doping Agency (WADA) องค์กรต่อต้านการใช้สารต้องห้ามโลก และเปิดโปงข้อมูลนักกีฬาสหรัฐฯ
- เหตุการณ์ที่กลุ่ม Anonymous โจมตีออสเตรเลียจนสามารถปิดเว็บไซต์ของหน่วยงานรัฐบาล และรัฐสภา เพื่อประท้วงความพยายามของรัฐบาลออสเตรเลียในการเสนอออกกฎหมายเกี่ยวกับการใช้อินเทอร์เน็ต
- ในทำนองเดียวกันกลุ่ม Anonymous ได้ร่วมกับกลุ่ม Green Party ในการประท้วงการเลือกตั้งในอิหร่าน เป็นต้น

รูปแบบการโจมตีที่เป็น “ภัยคุกคาม” ในปัจจุบัน

1. Malware ความไม่ปกติทางโปรแกรมสูญเสีย C (Confidentiality) I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือทั้งหมด สูญเสียความลับทางข้อมูล สูญเสียเสถียรภาพของระบบปฏิบัติการ จะทำลายข้อมูล หรือเข้าควบคุมระบบคอมฯ เคยสร้างความเสียหายให้กับสหรัฐฯ อังกฤษ จีน รัสเซีย สเปน อิตาลี และไต้หวัน มาแล้ว โดยผู้เชี่ยวชาญทางไซเบอร์แจ้งว่ามีการโจมตีด้วยมัลแวร์นี้ถึง 75,000 ครั้งทั่วโลก
2. Phishing “ภัยคุกคาม” เกิดขึ้นเพราะเปิดไฟล์หรือข้อมูลที่มีความเสี่ยง อาชญากรไซเบอร์รู้จึงใช้ระบบ “Phishing” เพื่อจูงใจให้เปิดไฟล์ที่มีมัลแวร์อันตรายแนบไว้ และเมื่อหลงเปิด “มัลแวร์” จะถูกติดตั้งและโจมตีคอมพิวเตอร์ทันที
3. SQL Injection Attack ภาษาโปรแกรมที่ใช้สื่อสารกับฐานข้อมูลภายในเซิร์ฟเวอร์ อาชญาการไซเบอร์จะโจมตีไปที่ SQL ส่งผลต่อเซิร์ฟเวอร์ ที่เก็บ “ข้อมูลของลูกค้า” “ข้อมูลส่วนบุคคล” “ หมายเลขบัตรเครดิตและระบบการเงิน” จะสร้างปัญหาในระยะยาวหากไม่มีการแก้ไขที่ทันท่วงที

รูปแบบการโจมตีที่เป็น “ภัยคุกคาม” ในปัจจุบัน

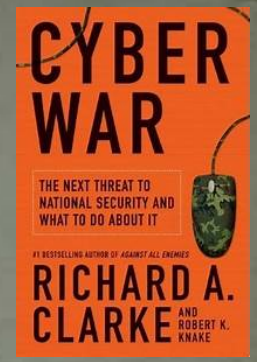
4. Cross-Site Scripting (XSS) โจมตีผ่านเว็บไซต์และเซิร์ฟเวอร์ที่มีช่องโหว่ เพื่อคุกคามฐานข้อมูลต่างๆ โดยเฉพาะข้อมูลด้านการเงิน จะใช้การโจมตีแบบ XSS ที่คล้ายกับการโจมตีแบบ SQL

5. Denial of Service (DoS) โจมตีเหมือนมีคนเข้าเว็บมากเกินไป เกิดความผิดปกติของเซิร์ฟเวอร์หลายๆส่วน พร้อมกันเรียกว่า DDoS หรือ Distributed Denial of Service Attack แก้ไขได้ยากมาก เนื่องจากผู้โจมตีมี IP ที่หลากหลายจากทั่วโลกเข้าสร้างความหนาแน่นของ Traffic บนเซิร์ฟเวอร์

6. Session Hijacking and Man-in-the-Middle Attacks ผู้บุกรุกจะโจมตี Session ด้วยการจับรหัส และวางตัวเองในคอมพิวเตอร์เครื่องที่ร้องขอการใช้งานเสียเอง

7. Credential Reuse การตั้งค่าเข้าสู่ระบบและรหัสผ่าน ช่วยสร้างความปลอดภัยได้ระดับหนึ่ง แต่จะต้องมีรหัสผ่านที่ไม่ซ้ำกันในการเข้าระบบต่างๆ ถ้าตั้งรหัสผ่านไว้แบบเดียวกัน หากโดนขโมยข้อมูลไปจะสร้างความเสียหายครอบคลุมไปในหลายๆส่วน บัญชีหลายๆบัญชีก็จะสามารถถูกแฮ็กได้

สงครามไซเบอร์ ; Cyber war



- **“สงครามไซเบอร์”** เป็นคำนิยามขึ้นมาโดย ริชาร์ด เอ.คลาร์ก ในหนังสือ **“Cyber war”**

(พฤษภาคม 2010) นิยามว่า

“เป็นการกระทำของรัฐ - ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์ หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก”

- การใช้ **“อานุภาพทางไซเบอร์”** ของประเทศใดประเทศหนึ่ง โจมตีประเทศเป้าหมาย เพื่อข่มขู่ คุกคาม หรือทำลายล้าง ประเทศหนึ่งๆ ซึ่งกำลังกลายเป็นภัยคุกคามต่อความมั่นคงในระดับชาติมากขึ้นเรื่อยๆ

สงครามไซเบอร์ Cyber war

- เป็นสงครามที่ไม่ต้องมีการเคลื่อนกำลัง ไม่ต้องมีการยิงปืนใหญ่ ทิ้งระเบิด หรือลั่นกระสุนใดๆ ทั้งสิ้น
- เพียงแค่อยู่หลังคอมพิวเตอร์ก็สามารถจู่โจมระบบการเงิน ระบบสาธารณูปโภค การขนส่ง หรือแม้กระทั้งทำลายระบบการสั่งการทางทหารของประเทศเป้าหมายได้
- จากข่าวการโจมตีธนาคารในหลายแห่งทั่วโลก เช่น ธนาคาร 5 รายใหญ่ในรัสเซียถูกโจมตี เมื่อวันที่ 8 พ.ย. 2016 หรือ การเจาะระบบธนาคารกลางของบังกลาเทศ เมื่อ ก.พ. 2559
- “ความเสี่ยงภัยคุกคามทางไซเบอร์” เป็นความเสี่ยงที่ผู้บริหารระดับสูงต้องให้ความสำคัญ องค์กรใหญ่ต่างๆ ควรที่จะต้องเตรียมการรับมือไว้ด้วย

สงครามไซเบอร์ Cyber War

- เป็นการปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้าม เพื่อให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา
- สงครามไซเบอร์เกิดขึ้นในหลายประเทศทั้งชัดเจน เปิดเผย และซุ่มเงียบ เป็นสงครามเย็นหรือ Cold War เริ่มกลับมาใช้อีกครั้ง หลังจากการแพ้สงครามเวียดนามของสหรัฐอฯ และการล่มสลายของสหภาพโซเวียตรัสเซีย
- ช่วงสงครามอ่าวที่สหรัฐโจมตีอิรักครั้งที่สอง สิ่งที่สหรัฐทำก่อนอื่นคือ ทำลาย เครือข่ายคอมพิวเตอร์ และอิเล็กทรอนิกส์ของอิรักที่ใช้ควบคุมระบบการยิงของอาวุธ
- การสู้รบปัจจุบันต่างฝ่ายหาทางทำลายระบบคอมพิวเตอร์และอิเล็กทรอนิกส์ที่ควบคุมการยิงอาวุธก่อน
- องค์การอวกาศ NASA = National Aeronautics and Space Administration ในปี 2554 เคยถูกโจมตีอย่างน้อย 10 ครั้ง ทั้งๆที่ลงทุนป้องกันกว่า 58 ล้านเหรียญ (ประมาณ 1,740 ล้านบาท)

สงครามไซเบอร์ Cyber war

- เมื่อ พฤษภาคม 2007 ประเทศเอสโทเนีย ถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะ รัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่าง ๆ จนข้อมูลเสียหายพังยับเยิน
- กันยายน ปี 2007 ติกเพนทากอน กระทรวงกลาโหม สหรัฐอเมริกา และที่ทำการรัฐบาล ของฝรั่งเศส เยอรมัน และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหาย อย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา
- วันที่ 14 ธันวาคม ปี2007 เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศเกียร์กีซ (Kyrgyz) ถูก โจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโทเนีย

รูปแบบการทำสงครามทางไซเบอร์

การใช้คอมพิวเตอร์และอินเตอร์เน็ตเพื่อการทำสงคราม ปัจจุบันมีอยู่ 8 รูปแบบ คือ

1. การโจรกรรมหรืออาชญากรรมทางไซเบอร์ (Cyber Crime)
2. การทำลายเว็บไซต์ การโจมตีเว็บ หรือบล็อคเว็บ (Web attacks)
3. การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านทางอินเตอร์เน็ต
4. การเจาะข้อมูลและการล้วงความลับข้อมูล
5. การกระจายเพื่อให้ปฏิเสธหรือหยุดบริการ (Distributed Denial-of-Service หรือ DDoS attacks)
6. การรบกวนเครื่องมือและอุปกรณ์ที่ใช้คอมพิวเตอร์ควบคุมการทำงาน
7. การโจมตีโครงสร้างระบบสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) และโครงสร้างพื้นฐานที่สำคัญ เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์
8. การใช้อุปกรณ์คอมพิวเตอร์หลอกแต่ซ่อนซอฟต์แวร์ไวรัสเอาไว้
9. การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้หรือทำงานไม่แม่นยำ

การโจมตีทำลายระบบ

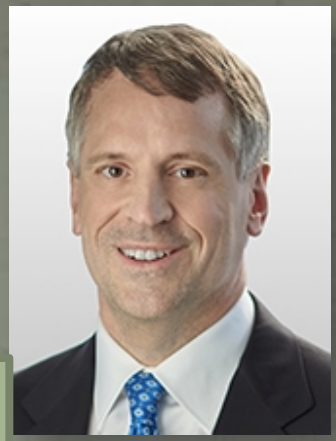
- เมื่อมีพาณิชย์อิเล็กทรอนิกส์มากขึ้นก็มีอาชญากรรมไซเบอร์ (e-crime) เพิ่มขึ้นเป็นเงาตามตัว
- ปี 2554 ยอดเงินอาชญากรรมไซเบอร์สูงถึง 338 พันล้านเหรียญ(ประมาณ 10 ล้านล้านบาท)
- เชื่อกันว่ายอดความเสียหายจากสงครามไซเบอร์จะมากกว่าความเสียหายในพาณิย์อิเล็กทรอนิกส์มากมายหลายเท่า
- ในสงครามไซเบอร์นั้น แทนที่จะใช้กำลังทางกายภาพก็ใช้ซอฟต์แวร์ในการทำลาย:
  - ระบบโทรคมนาคม (Telecommunication)
  - ระบบส่งกำลังไฟฟ้า (Power Grid)
  - โรงกลั่นน้ำมัน (Petro Plant)
  - โรงไฟฟ้านิวเคลียร์ (Nuclear Power Plant)
  - ระบบท่อส่งแก๊ส(Gas System)
  - ระบบน้ำประปา (Water System)
  - ระบบท่อน้ำทิ้ง (Sewer System) ฯลฯ

ในการประชุม World Economic Forum ได้รายงานด้านความเสี่ยงของโลก (Global Risk Report 2019)

ได้จัดให้ **“การจารกรรมข้อมูล”** เป็นความเสี่ยงในอันดับ 4 และ **“การโจมตีทางไซเบอร์”** เป็นความเสี่ยงที่อยู่ในอันดับ 5 ของโลกที่ต้องเร่งป้องกัน

John Drzik

ประธานของ Marsh Global Risk and Digital



“หากมองไปในอนาคต ขณะที่มีการเปิดรับทางไซเบอร์ของธุรกิจเพิ่มขึ้น ด้วยการเพิ่มจำนวนของอุปกรณ์ที่มีการเชื่อมต่อระหว่างกัน ทำให้ขนาดและความซับซ้อนของพื้นผิวการโจมตีกว้างขึ้น”

ดังนั้นจึงมีความจำเป็นสำหรับการลงทุนที่มากขึ้นในการจัดการความเสี่ยงทางไซเบอร์

อุปสรรคสำคัญที่ทำให้เกิดอาชญากรทางไซเบอร์

1) ไม่มีความคล่องตัวในการดำเนินการ

- จะต้องรู้ว่าช่องโหว่ขององค์กรอยู่ที่ใด เพื่อจะป้องกันภัยคุกคามทางไซเบอร์
- บางองค์กรมีความเข้าใจถึงอันตรายที่จะเกิดขึ้นได้อย่างชัดเจน แต่ไม่สามารถปิดช่องโหว่นั้นได้อย่างรวดเร็วเพียงพอ เพราะไม่รับรู้ภัยคุกคามที่เกิดขึ้นแบบ Real time

2) องค์กรไม่มีงบประมาณสำหรับสร้างความมั่นคงปลอดภัยในระบบไซเบอร์

- งบประมาณเป็นปัจจัยสำคัญ หากไม่มีงบประมาณสร้างความมั่นคงปลอดภัยให้ระบบไซเบอร์แล้ว จะทำให้เกิดความเสี่ยงและความเสียหายที่อาจจะเกิดขึ้นได้
- ในการป้องกันภัยคุกคามทางไซเบอร์ต้องใช้งบประมาณ และทรัพยากรมากขึ้น ที่จะทำให้เกิดประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นได้

(แหล่งข้อมูล : อาชญากรรมไซเบอร์ (Cyber Crime) ภัยคุกคามของเศรษฐกิจรูปแบบใหม่โดย พันเอก ดร. เศรษฐพงค์ มะลิสุวรรณ ประธานกรรมการกิจการโทรคมนาคม และรองประธาน กสทช.https://www.it24hrs.com/2015/cyber-crime-cyber-attack/)

อุปสรรคสำคัญที่ทำให้เกิดอาชญากรทางไซเบอร์

3) ขาดทักษะด้านความมั่นคงปลอดภัยไซเบอร์

- ทักษะเป็นอุปสรรคที่สำคัญที่สุดสำหรับการรักษาความปลอดภัยไซเบอร์
- พนักงานหรือผู้บริหารที่ยังขาดความรู้หรือทักษะเกี่ยวกับภัยคุกคามทางไซเบอร์ ทั้งยังขาดแคลนระบบรักษาความปลอดภัยที่มีประสิทธิภาพ หรือไม่มีบุคลลากรผู้รับผิดชอบและดูแลในส่วนนี้โดยตรง
- การดำเนินการขององค์กร ไม่เพียงแค่การป้องกันตัวเองจากการโจมตีทางไซเบอร์เท่านั้น แต่ควรมีความสามารถในการวิเคราะห์ เพื่อคาดการณ์สิ่งที่อาจจะเกิดขึ้น และเพื่อสร้างความเชื่อมั่น และเตรียมความพร้อมในการดำเนินการในสภาพแวดล้อมที่เปลี่ยนแปลงไป

(แหล่งข้อมูล : อาชญากรรมไซเบอร์ (Cyber Crime) ภัยคุกคามของเศรษฐกิจรูปแบบใหม่โดย พันเอก ดร. เศรษฐพงค์ มะลิสุวรรณ ประธานกรรมการกิจการโทรคมนาคม และรองประธาน กสทช.https://www.it24hrs.com/2015/cyber-crime-cyber-attack/)

อุปสรรคสำคัญที่ทำให้เกิดอาชญากรทางไซเบอร์

4)ความเข้าใจเรื่อง Cyber ระหว่างผู้บริหารและทีมงาน IT ที่มีความแตกต่างกัน

- ความเข้าใจเรื่อง Cyber ของผู้บริหารและทีมงาน IT มีความแตกต่างกัน เป็นอุปสรรคสำคัญในการขับเคลื่อนกระบวนการด้าน Cybersecurity
- ผู้บริหารและพนักงานยังไม่ให้ความสำคัญหรือไม่เห็นความจำเป็น เนื่องจากยังเห็นเป็นเรื่องใหม่ หรือยังไม่เคยได้รับผลกระทบจากเหตุการณ์ถูกโจมตีทางไซเบอร์ จึงทำให้บริษัทยังไม่เห็นความสำคัญในจุดนี้
- ความสะดวกในการเข้าถึงระบบโดยใช้ IP Address ทำให้มีการเชื่อมต่อองค์กรกับโลกภายนอกอย่างหลีกเลี่ยงไม่ได้ ซึ่งจะเป็นเป้าหมายอาชญากรทางไซเบอร์ที่สูงขึ้น
- ควรมีแนวทางในการดำเนินการเพื่อพัฒนาวิธีการป้องกันไซเบอร์อย่างจริงจัง โดยให้ความสำคัญใน**การวางยุทธศาสตร์ Cybersecurity**

(แหล่งข้อมูล : อาชญากรรมไซเบอร์ (Cyber Crime) ภัยคุกคามของเศรษฐกิจรูปแบบใหม่โดย พันเอก ดร. เศรษฐพงค์ มะลิสุวรรณ ประธานกรรมการกิจการโทรคมนาคม และรองประธาน กสทช.https://www.it24hrs.com/2015/cyber-crime-cyber-attack/)

มาตราการในรักษาความปลอดภัยไซเบอร์(Cyber Security)

- กห.สหรัฐ ให้ Cyber Security คือกระบวนการที่จำเป็น เพื่อให้องค์กรพ้นจาก**ความเสี่ยง และความเสียหาย** ต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ)
- **ความปลอดภัย**ของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล
- Cyber Security รวมไปถึงการระวังป้องกันอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ
- **ความเสี่ยงของ** Cyber Security ที่ทำลายความเชื่อมั่นและความไว้วางใจของ Stakeholder ที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

มาตรการในการรักษาความปลอดภัยไซเบอร์

- ระบบในการรักษาความปลอดภัยมีหลากหลาย
- เทคนิค Authentication การตรวจสอบและยืนยันตัวบุคคล หรืออุปกรณ์ปลายทางที่ติดต่อสื่อสารระหว่างกัน
- เทคนิค Automated theorem proving และเครื่องมือในการตรวจสอบอื่น ๆ สามารถทำให้กลไกที่ใช้งานระบบรักษาความปลอดภัยตามความต้องการที่ได้กำหนดไว้
- เทคนิค Capability and Access Control List สามารถถูกใช้ในการกำหนดและแยกแยะการควบคุมการเข้าถึงของผู้ใช้งาน
- เทคนิค Chain of Trust สามารถทำให้ซอฟแวร์ที่ถูกใช้งานผ่านการตรวจสอบและยืนยันจากผู้ออกแบบระบบ
- เทคนิคการรหัส (Cryptographic) สามารถถูกใช้ในการป้องกันข้อมูลระหว่างการส่งข้อมูลระหว่างระบบ ลดโอกาสความเป็นไปได้ในการลักลอบเปิดเผยและแก้ไขข้อมูลระหว่างการรับ-ส่ง

มาตรการในการรักษาความปลอดภัยไซเบอร์

- อุปกรณ์ Firewall สามารถป้องกันระบบจากการรุกรานแบบ online โดยกำหนดการผ่านเข้าออกของ Data Package ผ่านเส้นทางการจราจรบนเครือข่ายที่กำหนด ตามที่ผู้ดูแลระบบได้ออกแบบไว้
- การใช้งาน Microkernel ซึ่งเป็นซอฟแวร์ขนาดเล็กภายใต้ Operating System เพื่อป้องกันในระดับล่าง
- **ซอฟแวร์รักษาความปลอดภัยที่จุดติดต่อ** (Endpoint Security Software) เช่น ซอฟแวร์ป้องกันไวรัส ทำหน้าที่ระบุ และทำลายไวรัสคอมพิวเตอร์ และโปรแกรมที่ไม่ต้องการออกจาระบบคอมพิวเตอร์
- **การรักษาความลับ** (Confidentiality) เป็นมาตรการในการปกปิดข้อมูลข่าวสาร ให้รับทราบได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- **การรักษาข้อมูล** (Data Integrity) เป็นการเพิ่มความคงทนและความเที่ยงตรงของข้อมูลที่ถูกจัดเก็บไว้ โดยตรวจสอบการเปลี่ยนแปลงของข้อมูลระหว่างการบันทึกข้อมูล

มาตรการในการรักษาความปลอดภัยไซเบอร์

- **การสำรองข้อมูล** (Back up Data) เป็นการรักษาความปลอดภัยของข้อมูลข่าวสาร ทำโดยการสำเนาของไฟล์คอมพิวเตอร์ที่สำคัญ และเก็บรักษาไว้ในที่ตั้งที่อยู่ห่างจากระบบหลักที่ปฏิบัติอยู่ในสภาวะปกติ รวมทั้งที่ตั้งใหม่นั้นต้องสามารถป้องกันภัยคุกคามในด้านอุบัติภัย และภัยธรรมชาติขนาดใหญ่
- **เทคนิค Honey Pots** การทิ้งช่องโหว่การรักษาความปลอดภัยของระบบทั้งโดยตั้งใจ และไม่ตั้งใจ ซึ่งสามารถใช้ในการจับกุมผู้เจาะระบบ หรือการซ่อมแซมช่องโหว่ของการรักษาความปลอดภัยนั้น ๆ
- **ระบบตรวจจับการบุกรุก** (Intrusion Detection System) เป็นระบบที่ตรวจสอบเครือข่ายเพื่อหาผู้ใช้งานที่ไม่ควรอยู่ในเครือข่าย และ/หรือ ปฏิบัติในสิ่งที่ไม่ควรปฏิบัติ เช่นการทดลอง password หลาย ๆ ครั้ง เป็นต้น
- **เทคนิคการ Pinging** เป็นแนวโน้มในการเจาะระบบเบื้องต้นโดยการค้นหา และตรวจสอบ IP Address ของอุปกรณ์หรือคอมพิวเตอร์ที่ผู้เจาะพยายามเจาะเจ้าไป

การใช้คอมพิวเตอร์และอินเตอร์เน็ตเพื่อการทำสงคราม

- ปัจจุบันมีอยู่ 8 รูปแบบ คือ
  1. การโจรกรรมทางไซเบอร์
  2. การทำลายเว็บไซต์
  3. การโฆษณาชวนเชื่อทางอินเตอร์เน็ต (เว็บไซต์)
  4. การรวบรวมและการล้วงความลับข้อมูล
  5. การกระจายเพื่อให้ปฏิเสธบริการ
  6. การรบกวนเครื่องมือและอุปกรณ์
  7. การโจมตีโครงสร้างระบบสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) พื้นฐานที่สำคัญ
  8. การใช้อุปกรณ์คอมพิวเตอร์หลอกแต่ซ่อนซอฟต์แวร์ไวรัสเอาไว้

ความเสี่ยงในการใช้เทคโนโลยี

- ประเทศต้องยอมรับการใช้เทคโนโลยี ซึ่งทำให้ตกอยู่ในความเสี่ยงหลายประการ
- เช่นการสูญเสียอำนาจในการควบคุมสื่อ การกระจายตัวของสื่อ การผลิตสื่อ การเซ็นเซอร์สื่อ
- จนถึงขีดความสามารถในการหาผู้กระทำความผิดในไซเบอร์ เพราะ ระบบ server ที่ควบคุมการทำงานและการบันทึกพฤติกรรมการใช้งานของผู้ใช้ ตั้งอยู่ในต่างประเทศ
- ซึ่งจะมีผลกระทบโดยตรงต่อการวางยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ไปจนถึงการออกกฎหมายที่เกี่ยวข้องที่มีผลกระทบต่อการใช้งานอินเทอร์เน็ตของภาคธุรกิจและประชาชน
- ที่สำคัญคือ “เราไม่ใช่ผู้ควบคุมข้อมูลข่าวสารของประเทศเราได้เหมือนในอดีตที่ผ่านมาอีกต่อไปแล้ว”

ความเสี่ยงในการใช้เทคโนโลยี

- ภัยคุกคามที่รัฐบาลประเทศต่างๆ ทั่วโลกต้องตระหนัก เช่น การใช้ Digital platform ของ Google ซึ่งทรงประสิทธิภาพขึ้นทุกขณะ (มองเห็นการเคลื่อนไหวของประชาชนแบบ realtime)
- ไม่เพียงแต่ระบบ search engine ที่ทรงพลังเท่านั้น ยังรวมไปถึงระบบจราจรแบบ realtime ที่เรียกว่า Google traffic ซึ่งเป็นส่วนหนึ่งของระบบแผนที่ Google Maps ที่เรารู้จักกันดี โดยที่ระบบ Google traffic เป็นที่นิยมใช้กันมากในประเทศที่มีการจราจรติดขัด เพราะมันสามารถบอกถึงสถานะการจราจรบน smartphone แบบ realtime ได้อย่างดีโดยแสดงบน Google Maps
- ระบบ Google traffic จะได้รับข้อมูลตำแหน่งจาก GPS ของโทรศัพท์เคลื่อนที่ทุกเครื่อง ทุกประเทศที่ใช้ Google โดย Google traffic จะทำการคำนวณความเร็ว ระยะทาง และเวลา แล้วจึงมาแสดงผลสถานะการจราจรเป็นสีเขียว แดง เหลือง บน Google Maps แบบ realtime

การก่อการร้ายในยุค IT

- การเปลี่ยนแปลงสิ่งต่างๆอย่างต่อเนื่องในปัจจุบัน ทำให้เกิดการเปลี่ยนแปลงวิธีการของการก่อการร้ายเช่นกัน
- มุมมองต่อการก่อการร้ายและการต่อต้านการก่อการร้าย มีความสลับซับซ้อนมากขึ้น มีการเปลี่ยนแปลงไปสู่วิธีคิด รูปแบบ ขั้นตอน และการปฏิบัติการในรูปแบบใหม่ๆ
- หากกองทัพยังคงใช้กรอบแนวคิด หลักนิยม แผนและระเบียบปฏิบัติประจำเดิมๆ ในการเผชิญกับการก่อการร้ายที่เกิดขึ้นจะไม่ดีนัก เพราะจะไม่สามารถยุติหรือเอาชนะกลุ่มก่อการร้ายที่เปลี่ยนรูปแบบ วิธีการ และวิธีคิดไปแล้วได้
- การศึกษาถึงรูปแบบการก่อการร้ายในยุค IT จึงมีความจำเป็นที่กองทัพ และส่วนงานที่เกี่ยวข้อง และผู้ที่สนใจจะต้องทำความเข้าใจ เพื่อที่จะได้มีความเข้าใจสภาวะภัยคุกคามและปัญหาที่มาจากภัยก่อการร้ายในปัจจุบันได้ดียิ่งขึ้น

เรากำลังเข้าสู่ยุคสงครามที่ไม่รู้ว่าใครเป็นผู้ก่อการร้ายกันแน่

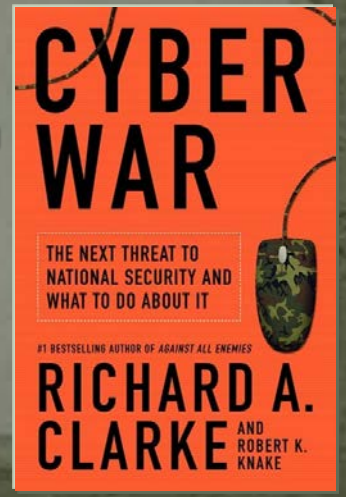
หน่วยงานความมั่นคงทั่วโลกเปลี่ยน mindset

- ปรับโครงสร้างและวิธีคิด มุ่งเน้นการสร้างความร่วมมือระหว่างประเทศทั้งกับภาครัฐและภาคเอกชน
- การประสานงาน และร่วมมือแลกเปลี่ยนข้อมูลกับบริษัทเอกชน เช่น Google, Facebook, Youtube โดยส่งเจ้าหน้าที่และผู้บริหารระดับสูงไปเข้าร่วม Cybersecurity forum ต่างๆ จนถึงงานประชุมในทุกระดับ
- Best practices ในหลายประเทศพบว่า เข้าร่วมในฐานะ Partnership จะทำให้เกิดความร่วมมือและช่วยเหลือจากบริษัทเหล่านั้นในเชิงลึก เพื่อช่วยสกัดกั้น content ที่เป็นภัยต่อความมั่นคง ไปจนถึงการให้ข้อมูลเชิงลึกต่อการติดตามจับกุมผู้กระทำความผิดได้โดยง่ายอีกด้วย
- Landscape ของความมั่นคงของชาติได้เปลี่ยนไปแล้วในวันนี้ เส้นเขตแดนของประเทศถูกทำลายลงจากความก้าวหน้าของเทคโนโลยี ผู้นำและผู้บริหารทั้งภาครัฐและภาคเอกชนจำเป็นต้องเปลี่ยนวิธีคิด (mindset) โดยต้องร่วมมือกัน และต้องมองขาดว่าสิ่งที่เรากำลังเผชิญไม่สามารถแก้ปัญหาด้วยวิธีคิดเดิมๆ ได้อีกต่อไป

ถ้าไม่มีแผนป้องกันจะไม่ปลอดภัยอาจเกิด

CHEW (Crime , Hacktivism , Espionage , War)

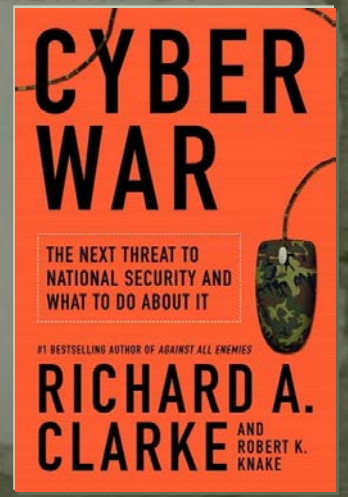
- **C อาชญากรรม (Crime)**
- กรณีเกาหลีเหนือขโมยเงินทางธุรกรรมจากประเทศฟิลิปปินส์ และบังกลาเทศ Hacker สามารถเจาะเข้าไปในระบบและทำการโอนเงินไปในหลายๆ ที่ ทำให้การตามหาผู้กระทำผิดหรือได้เงินคืนเป็นเรื่องยาก
- ภาพรวมองค์การอาชญากรรมทางไซเบอร์ มีศักยภาพในการขโมยเงินได้มากกว่ากลุ่มค้ายาเสพติดหลายเท่า ถึงจะส่งผลกระทบแต่ไม่สามารถจับกุมได้ เนื่องจากมีการติดสินบนทั้งตำรวจหรือคนในระดับรัฐบาล
- ขณะที่ทั้ง NSA และ FBI มีการระบุว่าเป็นคนๆหนึ่งทราบชื่อแล้ว แต่เมื่อให้ทางประเทศรัสเซีย หรือประเทศอื่นๆ ช่วยตามจับกุมก็จะไม่สามารถพบตัวตนที่แท้จริงได้ ทำให้ประเทศเหล่านั้นเป็นพื้นที่หลบซ่อน การโจมตีทางไซเบอร์จึงยังคงอยู่ต่อไป
- ในขณะเกิดการโจมตีอย่างธนาคารก็จะประเมินความเสียหาย หากไม่สามารถนำกลับมาได้ ก็ต้องชดใช้ลูกค้า นั่นคือแม้ธนาคารจะโดนโจมตี แต่ประชาชนหรือลูกค้าก็ถูกขโมยเงินเช่นกัน



Richard A. Clarke (Cyber warfare : Richard A. Clarke's Point of view)

ถ้าไม่มีแผนป้องกันจะไม่ปลอดภัยอาจที่จะเกิดดังนี้
CHEW (Crime , Hacktivism , Espionage , War)

- H แฮกติวิสซึม (Hacktivism)
- การเจาะข้อมูลเพื่อการเผยแพร่ต่อสาธารณะ เพื่อให้เกิดความอับอายทั้งภาครัฐและเอกชน โดยจะถูกนำไปตีพิมพ์ไว้ที่ Wikileak
- Richard A. Clarke เคยส่ง E-mail ลับ ระหว่างเอกอัครราชทูตฯ เนื้อหาบางส่วนเป็นการตำนิประธานาธิบดีฯ หากถูกเผยแพร่ออกไป ตัวเขาคงกลับไปทำงานในทำเนียบขาวไม่ได้แล้ว
- ในกรณี E-mail ของนาง ฮิลลารี คลินตัน ที่ถูกเปิดเผยออกมาทำให้ส่งผลเสียในการเลือกตั้ง ทำให้แพ้การเลือกตั้ง ซึ่งข้อมูลลับที่เปิดเผยออกมาทำลายทั้งองค์กร หรือถึงขั้นการไม่ได้เป็นประธานาธิบดี ได้เช่นกัน

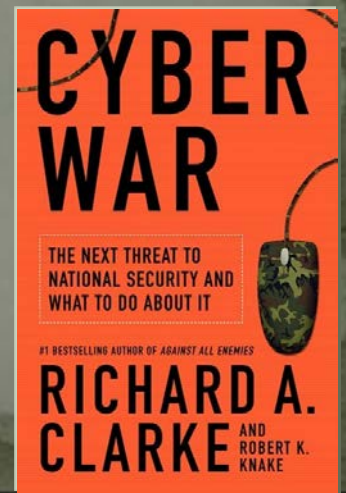


Richard A. Clarke (Cyber warfare : Richard A. Clarke's Point of view)

ถ้าไม่มีแผนป้องกันจะไม่ปลอดภัยอาจที่จะเกิดดังนี้
CHEW (Crime , Hacktivism , Espionage , War)

- **E จารกรรม** (Espionage)
- การจ้างสายลับเพื่อขโมยเอกสารลับออกมาเปิดเผย หรือส่งไปให้สายลับอีกคนหนึ่ง
- การขโมยข้อมูลลับวันนี้ สามารถเจาะข้อมูลจากที่บ้านได้เลย
- ขณะนี้มีโดรน (Drone) เคยไปงานเกี่ยวกับอากาศยานแล้วพบว่าแบบแปลนดังกล่าว ทางเราไม่เคยขายออกไป แต่เราพบโดรนที่มาจากประเทศจีนซึ่งจีนอาจจะมีนักเจาะข้อมูลเพื่อขโมยแบบแปลนดังกล่าว
- บริษัทมักจะถูกเจาะระบบทุกวัน โดยเฉพาะคู่แข่งทางการค้า บางบริษัทฯ ต้องลงทุนวิจัยใช้งบประมาณมากมาย แต่ก็ต้องโดนคู่แข่งผลิตของเลียนแบบ ซึ่งถือเป็นอาชญากรรมทางเศรษฐกิจ

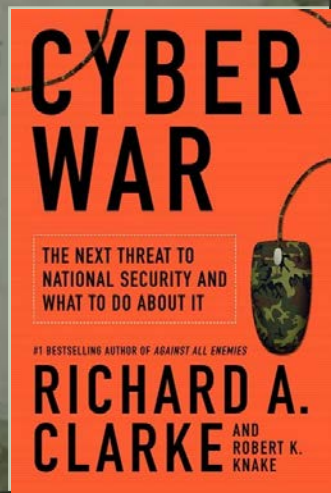
Richard A. Clarke (Cyber warfare : Richard A. Clarke's Point of view)



ถ้าไม่มีแผนป้องกันจะไม่ปลอดภัยอาจที่จะเกิดดังนี้
CHEW (Crime , Hacktivism , Espionage , War)

- **W สงคราม (War)**
- ช่วง 7 ปี ที่ Richard A. Clarke ได้เขียนหนังสือ Cyber War มีหลายคนบอกว่ามันไม่มีทางเป็นไปได้
- แต่เหตุการณ์ที่รัสเซียบุกจอร์เจีย ก่อนเอารถถังบุก ระบบสื่อสาร ธนาคารของประเทศล่มหมด ทำให้ไม่สามารถเผยแพร่หรือรายงานการโจมตีออกไปสู่ภายนอกได้
- ในเรื่องของ Stuxnet virus ที่มีการโจมตีโรงงานไฟฟ้านิวเคลียร์ประเทศอิหร่าน ถึงแม้ว่าเป็นระบบภายใน (Intranet) ไม่ได้ต่อออกสู่ภายนอก แต่ทั้งสหรัฐและอิสราเอลก็สามารถหาทางเจาะเข้าไปได้ ส่งผลให้เครื่องคอมพิวเตอร์ของโรงงานฯกว่า 800 เครื่องถูกทำลาย เป็นการทำลายทางกายภาพโดยตรง สำหรับคำสั่งการโจมตีเป็นเพียงหนอนไวรัส (Worm) และโปรแกรมไม่พึงประสงค์ (Malware) ซึ่งมีการกระจายไปทั่วโลก

Richard A. Clarke (Cyber warfare : Richard A. Clarke's Point of view)



การจัดทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถาม 6 คำถาม

1. เราจะรุกและรับอะไร? การรุกเป็นวิธีที่รวดเร็ว ประหยัดได้ผลสุด แต่ไม่สำคัญเท่าการรับ

- ในยุทธการระดับประเทศ การป้องกันถือเป็นยุทธศาสตร์แรก
- การโจมตีหรือรุกอาจจะมีค่าใช้จ่ายจัดตั้งทีมเจาะระบบสูงกว่า 2 ล้านเหรียญสหรัฐ แต่การป้องกันต้องใช้งบประมาณเป็น 1,000 ล้านเหรียญสหรัฐ
- เมื่อเดือน ธ.ค. 2559 มีการโจมตีโครงข่ายการไฟฟ้าของยูเครนโดยรัสเซีย ยูเครนต้องใช้เวลาถึง 6 ชม.ในการฟื้นฟูระบบฯ และหากเกิดเหตุการณ์แบบนี้ในประเทศไทย เราจะไม่มีไฟฟ้าใช้ 6 เดือน อะไรจะเกิดขึ้น ดังนั้นการตั้งรับจึงเป็นสิ่งสำคัญเป็นอันดับแรก

Richard A. Clarke's Point of view

การจัดทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถาม 6 คำถาม

2. คำถามเกี่ยวกับภาคเอกชน

- ซึ่งมีทั้งในวงการแพทย์ ตลาดหุ้น ธนาคาร หน่วยงานเหล่านี้ มีการพิจารณาด้านความปลอดภัยในส่วนงานของตนเองหรือไม่? หรือรอให้ภาครัฐเข้าไปดำเนินการกำกับดูแล
- ปกติเอกชนไม่อยากให้ภาครัฐเข้าไปยุ่งเกี่ยวด้านความปลอดภัย จริงๆแล้วการกำกับดูแลของภาครัฐก็มีข้อจำกัด เพราะไม่รู้ว่าเอกชนทำงานอย่างไร?
- จึงควรมีความร่วมมือระหว่างกัน รัฐจะต้องกำหนดเป้าหมายด้านความปลอดภัยร่วมกับภาคเอกชน และมีการตรวจสอบจากภาครัฐอีกครั้งหนึ่ง ในอุตสาหกรรมสำคัญ เช่น โรงไฟฟ้า ธนาคาร โรงพยาบาล เป็นต้น
- ในห้วงที่ผ่านมาโรงพยาบาลในสหรัฐถูกโจมตีด้วย Wanna Cry, Pet Ya ต้องปิดการให้บริการ ทางโรงพยาบาลเองก็ไม่ทราบจะจัดการเรื่องดังกล่าวอย่างไร ดังนั้นรัฐต้องควบคุมแต่ไม่ได้บังคับ หรือจะบังคับต้องอาศัยวิธีการที่ชาญฉลาดพร้อมการตรวจสอบไปในตัว

Richard A. Clarke’s Point of view

การจัดทำยุทธศาสตร์ด้านไซเบอร์ต้องตอบคำถาม 6 คำถาม

3. องค์กร NGO อยากจะได้รับความเป็นส่วนตัว

- ถ้ารัฐเข้ามากำกับดูแลก็ถูกมองว่าเป็นการควบคุม ในด้านความมั่นคงและความเป็นส่วนตัวมีความขัดแย้งกันในตัว
- มีกรณีประวัติการรักษาพยาบาลถูกเจาะข้อมูลนำไปเผยแพร่ทางอินเทอร์เน็ต เป็นเรื่องการละเมิดความเป็นส่วนตัว การจะป้องกันเรื่องนี้ ต้องใช้ด้านความมั่นคงเข้าไปจัดการ ที่ไม่ต้องมีความคิดเห็นที่ขัดแย้งกันเพราะทั้งสองด้านไม่มีใครผิดไม่มีใครถูก
- รัฐต้องดูแลทั้งความปลอดภัยและความเป็นส่วนตัวไปพร้อมกันด้วย เช่น กรณีรัฐบาลสหรัฐมีการดักฟังโทรศัพท์ โดยดูข้อมูลที่เป็น Meta Data เมื่อมีการร้องเรียนก็ต้องมีหมายศาลในเรื่องดังกล่าว โดยศาลเองก็ต้องมีกระบวนการที่รวดเร็วในการออกหมาย
- ศาลปกติจะไม่เข้าใจเรื่องไซเบอร์ ในสหรัฐจึงจัดตั้งศาลเฉพาะด้านนี้ที่มีความรู้ความเข้าใจด้านโทรคมนาคมและการสื่อสาร ศาลเข้าสู่ยุคสารสนเทศเช่นเดียวกัน ถือเป็นบริการภาครัฐในการป้องกันข้อมูลส่วนบุคคลและระบบสารสนเทศ

Richard A. Clarke's Point of view

การจัดทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถาม 6 คำถาม

4. เวลาที่เราต้องลงทุน

- การลงทุนในซอฟต์แวร์เพื่อค้นหาข้อมูลสินค้าเมื่อลูกค้าหาสินค้าที่ต้องการเจอ และสั่งสินค้า บริษัทจะส่งสินค้าไปถึงมือลูกค้าให้ปลอดภัยไม่เสียหาย
- ในเรื่องซอฟต์แวร์หรือเรื่องบุคคล จะต้องลงทุนในเรื่องคนก่อน ซึ่งสามารถช่วยป้องกันระบบเครือข่ายขายสินค้าของเราได้
- ถ้าเราไม่มีผู้เชี่ยวชาญ เราจะปกป้องสิ่งเหล่านี้ไม่ได้ โดยเฉพาะด้านการทหาร บุคคลที่เก่งมักจะไม่เข้ามาในวงการทหาร สาเหตุเพราะไม่อยากเป็นทหาร ไม่อยากแต่งเครื่องแบบ หากเราต้องการคนที่มีความเชี่ยวชาญก็ต้องเปิดรับคนใหม่ๆ
- ในประเทศรัสเซีย และอิสราเอล ถ้าจับกุมวัยรุ่นที่เป็น Hacker ได้เขาจะส่งไปเป็นทหาร มีการฝึกอบรมบุคลากร เพื่อรับมือกับภัยคุกคามใหม่ๆ จากตำแหน่งงานที่ว่างในหน่วยงานหลายแห่งต้องการผู้เชี่ยวชาญทางไซเบอร์เข้ามาทำงาน แม้จะมีการศึกษามีทุนเรียนด้านไซเบอร์เพื่อให้เข้ามาทำงานภาครัฐ แต่ก็ยังมีตำแหน่งว่างอยู่ดี

Richard A. Clarke’s Point of view

การจัดทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถาม 6 คำถาม

5. นวัตกรรม

- ทุกคนจะผลิตสิ่งใหม่ๆ เพื่อขายในตลาด โดยไม่สนใจเรื่องความปลอดภัย
- มีอุปกรณ์นับพันล้านชิ้นที่ต่อเชื่อมอินเตอร์เน็ต และ**ในปี 2020 จะมีอุปกรณ์เชื่อมต่อถึงกันได้มากกว่า 8 หมื่นล้านเครื่องและผู้ใช้อินเทอร์เน็ตจะมีประชากรเพิ่มขึ้น 5 พันล้านคน**
- ในอีก 3 ปีข้างหน้า อาจจะเพิ่มขึ้นในระดับพันล้านชิ้น สำหรับแนวคิดเรื่อง IoT -Internet of Thing ทุกอุปกรณ์สามารถเชื่อมต่อเข้าสู่อินเตอร์เน็ตด้วยตัวมันเอง เช่นเครื่องขายน้ำอัดลมแบบหยอดเหรียญ ก็ต้องต่ออินเตอร์เน็ตเพื่อจะได้ทราบว่าสินค้าหมดแล้วหรือยัง
- แม้แต่ลิฟต์ก็ต้องมีการต่อเชื่อมอินเตอร์เน็ตเพื่อจะทราบข้อมูลการเข้าไปดูแลรักษาตามห้วงเวลา ถ้านวัตกรรมเชื่อถือไม่ได้จะเกิดปัญหา เช่น มีการเจาะเข้าไปในคาสิโน โดยอาศัยเครื่องคอมพิวเตอร์ที่ควบคุมอ่างเลี้ยงปลาในการควบคุมปริมาณออกซิเจนและใช้มันเป็นเครื่องมือเจาะเครื่องอื่นๆต่อไป นอกจากเครื่องควบคุม CCTV ก็มีโอกาสเป็นเหยื่อด้วยเช่นกัน
- ถ้าให้เลือกน้ำหนักของนวัตกรรม กับความน่าเชื่อถือ Richard A. Clarke ให้น้ำหนักทางความน่าเชื่อถือมากกว่า

Richard A. Clarke's Point of view

การจัดทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถาม 6 คำถาม

6. ด้านการออกแบบยุทธศาสตร์

- จะเน้นเรื่องการป้องกันหรือฟื้นฟูหลังการโจมตีในระบบคอมพิวเตอร์ ทุกเครื่องจะถูกโจมตี ในเครือข่ายลับก็ถูกโจมตี แม้แต่หน่วยงานลับ CIA ก็เคยถูกโจมตี
- ประเทศต่างๆ ต้องเผชิญกับฝ่ายตรงข้ามอย่างรัสเซีย จีน ที่มีขีดความสามารถสูง ซึ่งเชื่อว่าเขาทำได้อย่างแน่นอน เราอาจจะป้องกัน Hacker ทั่วไปได้ แต่ระดับมืออาชีพนั้นไม่มีทางป้องกันได้ ฉนั้นหลังถูกโจมตีต้องฟื้นฟูให้เร็วที่สุด
- โดยปกติทุกภาคส่วนมักจะคิดป้องกันการเจาะระบบเพื่อลดความเสียหาย การแบ่งแยกระบบงานและเครือข่าย และต้องมีการฟื้นฟู มีระบบสำรอง (Backup) ให้ระบบกลับมาใช้งานตามปกติให้เร็วที่สุด
- หากทุกคนต้องทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถามทั้ง ๖ ข้อให้ได้ แผนที่ทำไม่ใช่สั่งจากบนลงล่างอย่างเดียว ทั้งหมดต้องมีส่วนร่วมในการวางแผน มีการโต้เถียงกันให้ได้ข้อยุติ ในประเทศไทยเรามีความเข้มแข็ง แต่จะไม่ปลอดภัยหากไม่มีการป้องกันทางไซเบอร์

Richard A. Clarke’s Point of view

หน่วยบัญชาการไซเบอร์ (Cyber Command)

- หน่วยบัญชาการไซเบอร์สหรัฐมีการรวมทั้ง 3 เหล่าทัพขึ้นตรงต่อ รมว.กห.สหรัฐฯ
- ประเทศกว่า 20 ประเทศมีการจัดตั้งหน่วยดังกล่าว มีทั้งเล็กใหญ่ตามรูปแบบของแต่ละประเทศ หากเราไม่มี Cyber Command จะไม่มีใครสนใจด้านไซเบอร์
- ประเทศไทยต้องออกแบบการพัฒนาไซเบอร์ และมองให้ออกว่ามันได้ประโยชน์ต่อประเทศอย่างไร ต้องหาผู้เชี่ยวชาญ รวมคนเหล่านั้นเข้าด้วยกัน
- กรณี 9/11 เราให้ความสำคัญหน่วยงานที่เป็นโครงสร้างพื้นฐาน สร้าง Red Team เพื่อการซักซ้อมแผนเผชิญเหตุ ซักซ้อมการโจมตี การวางแผนสำรองกรณีฉุกเฉิน ให้กระทรวงทั้งหมดปรับการทำงาน โดยไม่ต้องมีการสั่งการจากศูนย์บัญชาการเพียงอย่างเดียว แม้จะมีศูนย์บัญชาการสำรองอาจจะไม่มีคนเพียงพอ ก็ต้องพยายามเฝ้าระวังในทุกๆวันอย่างต่อเนื่อง
- การฝึกด้านไซเบอร์ต้องทำบ่อยๆ แผนในเอกสารไม่มีประโยชน์ จะต้องทำจริง ปฏิบัติจริง เรื่องอาชญากรรมข้ามชาติต้องมีความร่วมมือในการติดตามจับกุมและมีมาตรการลงโทษประเทศที่ไม่ให้ความร่วมมือ

หน่วยงานที่มีบทบาทในการเฝ้าระวังการโจมตีทางไซเบอร์ของประเทศไทย

- ประเทศไทยมีหน่วยงานภาครัฐที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) 2 แห่ง คือ

1. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
(Thailand Computer Emergency Response Team : ThaiCERT)

2. ศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (จีเซิร์ต)
(Government Computer Emergency and Readiness Team : G-CERT)
ในกำกับ ดูแลของ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.)

หน่วยงานที่มีบทบาทในการเฝ้าระวังการโจมตีทางไซเบอร์ของประเทศไทย

1) **ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)** ในการกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.)

หน้าที่หลัก คือ

- เฝ้าระวัง และจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ให้ทั้งหน่วยงานภาครัฐ และภาคเอกชน
- ให้การสนับสนุนที่จำเป็น และให้คำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์
- ติดตาม และเผยแพร่ข่าวสาร และเหตุการณ์ทางด้านความมั่นคงปลอดภัย ทางด้านคอมพิวเตอร์ต่อสาธารณชน
- ทำการศึกษา และพัฒนาเครื่องมือ และแนวทางต่างๆ ในการปฏิบัติ เพื่อความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ต

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

หน่วยงานที่มีบทบาทในการเฝ้าระวังการโจมตีทางไซเบอร์ของประเทศไทย

2) ศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (จีเซิร์ต)
ในกำกับดูแลของ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.)

หน้าที่หลัก คือ

- จัดการและตอบสนองเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์ และระบบเครือข่ายให้เฉพาะหน่วยงานของภาครัฐ
- สร้างเครือข่ายพันธมิตรเพื่อให้เกิดความมั่นคงปลอดภัยและช่วยลดความเสี่ยงต่อการเกิดอาชญากรรมทางคอมพิวเตอร์

ความท้าทายของภาคการเงินการธนาคารในปัจจุบัน

การรักษาความปลอดภัยขั้นสูง เพื่อปกป้องข้อมูลและทรัพย์สินของลูกค้า ให้มีประสิทธิภาพ :

- การรักษาความปลอดภัยทางไซเบอร์ถือเป็นเรื่องที่สำคัญมาก
- การดำเนินธุรกิจในปัจจุบัน หากมีมาตรการป้องกันที่มีประสิทธิภาพ จะสามารถประหยัดค่าใช้จ่ายในองค์กรได้อย่างมหาศาล

การคุ้มครองข้อมูลส่วนบุคคลของลูกค้าและสร้างความโปร่งใสในการให้บริการ :

- การนำข้อมูลของลูกค้าไปใช้งานย่อมต้องได้รับอนุญาตจากลูกค้าที่เป็นเจ้าของข้อมูลเสียก่อน
- การยินยอมแบ่งปันข้อมูลควรมีการกำกับว่าข้อมูลชนิดใดที่ไม่ควรนำไปใช้ หรือเปิดเผย
- ประเด็นที่ท้าทายคือ เราจะนำเทคโนโลยีใหม่ๆ มาใช้อย่างมีประสิทธิภาพ ถูกต้อง และมีจริยธรรมได้อย่างไร

ความท้าทายของภาคการเงินการธนาคารในปัจจุบัน (ต่อ)

- การนำเทคโนโลยีและนวัตกรรมมาใช้ในธุรกิจ :
  - เนื่องจากการปรับตัวเพื่อรองรับกับการเปลี่ยนแปลงสิ่งต่างๆ เพื่อให้ทันกับพฤติกรรมและความต้องการของลูกค้าที่เปลี่ยนแปลงไป โดยมีการประยุกต์ใช้เทคโนโลยี หรือการร่วมมือกับ Fintech (Financial Technology) ใหม่ๆ ที่ช่วยในให้บริการทางการเงิน
  - การเปลี่ยนแปลงสิ่งต่างๆ เหล่านี้ ล้วนส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ขององค์กรด้วย ซึ่งถือเป็นความท้าทายของหน่วยงานเหล่านี้ในการสร้างสมดุลระหว่างการรักษาความปลอดภัยและการอำนวยความสะดวกสบายให้แก่ลูกค้า

- **การให้ความรู้แก่ลูกค้าเรื่องความปลอดภัย :**
  การให้ความรู้แก่ลูกค้าเกี่ยวกับการใช้งานอุปกรณ์ที่เชื่อมต่อกับระบบอินเตอร์เน็ต ให้มีความปลอดภัย โดยการปรับปรุงด้านการยืนยันตัวตนและระบบความปลอดภัย

ผลกระทบจากการโจมตีสถาบันการเงินทางไซเบอร์

- การโจมตีทางไซเบอร์ต่อธนาคารต่างๆ อาจสร้างผลกระทบสะเทือนต่อระบบการเงินของทั้งโลกได้
- มูลค่าความเสียหายที่ที่เกิดขึ้นจะมีมูลค่ามหาศาลหากถูกโจมตีจากอาชญากรทางไซเบอร์
- มูลค่าของการเยียวยาผู้เสียหายจากเหตุการณ์โจมตีจะมีมูลค่าสูงทั้งด้านการเงินและความเชื่อมั่นในระบบธนาคาร
- การสูญเสียความน่าเชื่อถือและความไว้วางใจในระบบรักษาความปลอดภัยของสถาบันการเงินนั้นๆ และมีโอกาสสูงที่จะสูญเสียฐานลูกค้าไปได้
- มูลค่าค่าใช้จ่ายในการกู้คืนข้อมูลที่สูญหายจากการโจมตีทางไซเบอร์ที่มีราคาแพงมาก
- ส่งผลต่อการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต และกระทบต่อระบบเศรษฐกิจและความมั่นคงของประเทศ

สถิติการละเมิดข้อมูล

- Data Breach คือ การละเมิดข้อมูล หรือการถูกปล่อยข้อมูลส่วนตัว หรือข้อมูลที่เป็นความลับไปสู่สภาพแวดล้อมที่ไม่น่าเชื่อถือ เช่น การเปิดเผยข้อมูลที่ไม่ได้ตั้งใจ การรั่วไหลของข้อมูลและการถูกแฮ็กข้อมูล

- การรั่วไหลของข้อมูลขนาดใหญ่ที่เพิ่มขึ้น แสดงให้เห็นว่าไม่เพียงแต่จำนวนการละเมิดความปลอดภัยที่เพิ่มขึ้นเท่านั้น แต่ยังเพิ่มความรุนแรงเช่นกัน

- ในปี 2016 มีบัญชีของ Yahoo ถึง 3,000 ล้านบัญชี ที่ถูกแฮกในการละเมิด ซึ่งเป็นหนึ่งในการละเมิดครั้งใหญ่ที่สุดครั้งหนึ่ง โดยข้อมูลที่หลุดไป มีทั้ง ชื่อ-นามสกุล อีเมล หมายเลขโทรศัพท์ วันเกิด รหัสผ่านที่เข้ารหัสไว้ และคำถาม-คำตอบเวลาผู้ใช้ลืมรหัสผ่านทั้งแบบเข้าและไม่เข้ารหัส (Oath.com)

YAHOO!

Source: www.varonis.com/blog/cybersecurity-statistics/

สถิติการละเมิดข้อมูล

- ในปี 2017 มี User Accounts จำนวน 412 ล้านบัญชี ถูกขโมยจากเว็บไซต์ของ Friendfinder (เป็นเว็บหาคู่ออนไลน์) (LeakedSource)

- ในปี 2017 ผู้บริโภค 147.9 ล้านคน ได้รับผลกระทบจากการที่บริษัท Equifax ถูกละเมิดข้อมูล (บริษัทข้อมูลเครดิตรายใหญ่ของสหรัฐอเมริกา) ข้อมูลที่ถูกแฮ็กมีทั้ง ชื่อ หมายเลขประกันสังคม วันเกิด ที่อยู่ หมายเลขใบขับขี่ หมายเลขบัตรเครดิต ฯลฯ ซึ่งข้อมูลเหล่านี้สามารถนำไปใช้ปลอมแปลงตัวบุคคลได้ (Equifax)

- จากสถิติของปี 2017 พบว่ามีการเจาะข้อมูลโดยมีเป้าหมายขนาดใหญ่กว่า 130 รายการในสหรัฐอเมริกาต่อปี และจำนวนการเจาะข้อมูลเพิ่มขึ้นโดยเฉลี่ย 27 เปอร์เซ็นต์ต่อปี (Accenture)

Source: www.varonis.com/blog/cybersecurity-statistics/

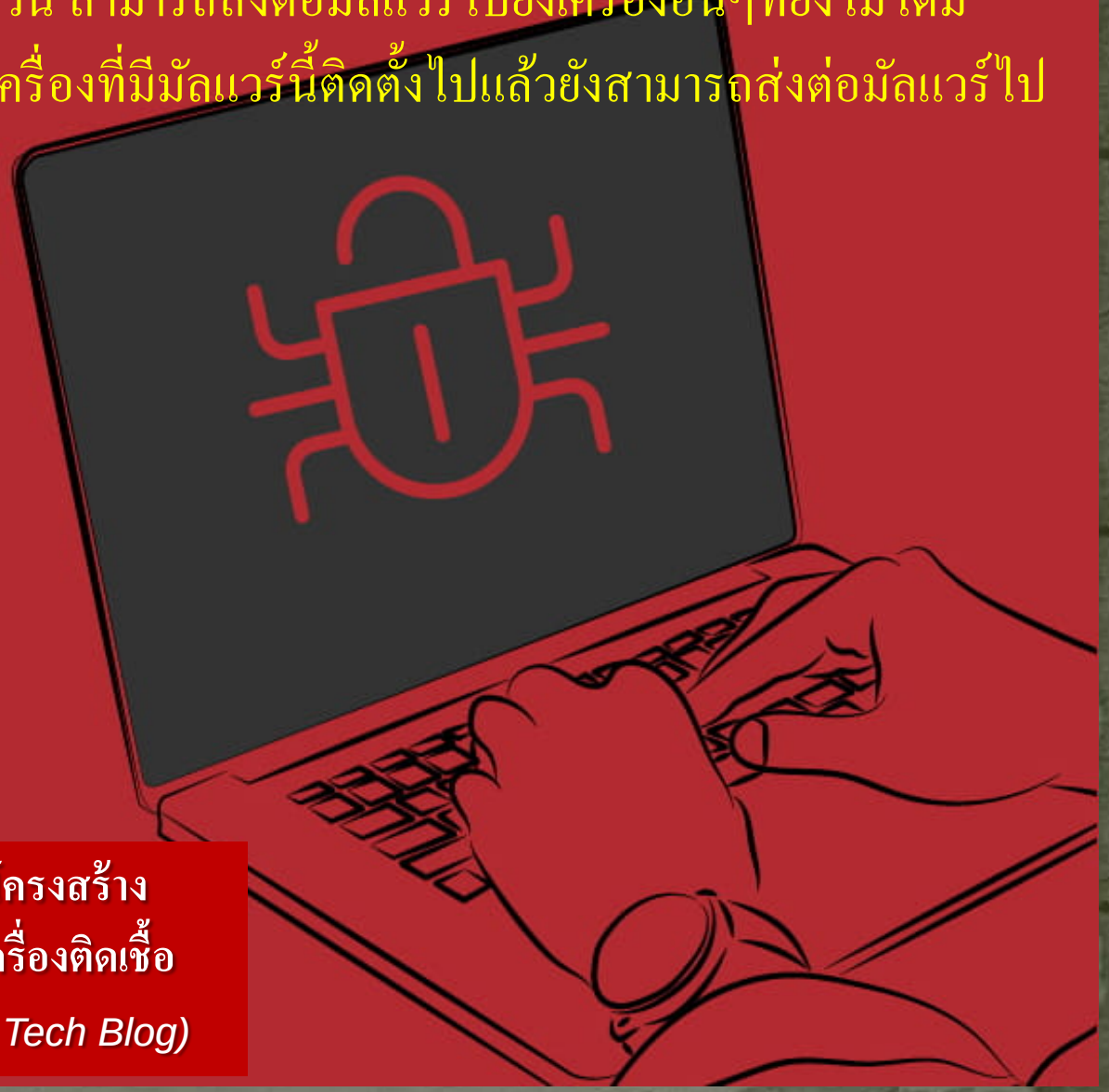
- การโจมตีแบบ cryptojacking เพิ่มขึ้นแบบก้าวกระโดดกว่า 8,500 เปอร์เซ็นต์ ในปี 2017 (Symantec)
- ถ้าอยู่ๆ เราพบว่าอินเทอร์เน็ตเล่นได้ช้าลง คอมพิวเตอร์อืด เครื่องร้อน และได้ยินเสียงพัดลมทำงานอย่างหนัก ... นั่นมีโอกาสสูงที่จะตกเป็นเหยื่อของการโจมตีแบบ Cryptojacking แล้ว
- Cryptojacking เป็นภัยคุกคามไซเบอร์รูปแบบใหม่ที่เจ้าของเว็บไซต์หรือแฮกเกอร์แอบรันสคริปต์บางอย่างบนเว็บเบราเซอร์ของผู้ใช้ เพื่อเขาเข้าใช้ทรัพยากรบนเครื่องของผู้เข้าชมเว็บไซต์ในการขุดเหมืองเงินดิจิทัล เช่น Bitcoin หรือ Monero

ทำความรู้จักภัยคุกคามรูปแบบใหม่ Cryptojacking

เพื่อสร้างรายได้ให้แก่ตนเอง เป็นการขโมยทรัพยากรคอมพิวเตอร์มาใช้งานโดยที่ผู้ใช้ไม่รู้ตัว

Source: www.varonis.com/blog/cybersecurity-statistics/

WannaCry มัลแวร์เรียกค่าไถ่ สามารถแพร่กระจายไปยังเครื่องอื่นๆโดยอัตโนมัติ ไม่ต้องอาศัยผู้ใช้งานส่งต่อมัลแวร์โดยรู้เท่าไม่ถึงการณ์เหมือนที่ผ่านมา เครื่องที่มีมัลแวร์ตัวนี้ สามารถส่งต่อมัลแวร์ไปยังเครื่องอื่นๆที่ยังไม่ได้มีการอัปเดตแพตช์ใน Local network ได้เอง นอกจากนี้เครื่องที่มีมัลแวร์นี้ติดตั้งไปแล้วยังสามารถส่งต่อมัลแวร์ไปยังเครื่องอื่นๆผ่านอินเตอร์เนตได้อีกด้วย



WannaCry คืออะไร

WHY YOU ARE AT RISK

ในปี 2017 31%ขององค์กรที่มีประสบการณ์การถูกโจมตีทางไซเบอร์ในโครงสร้างพื้นฐานเทคโนโลยี จาก 100,000 กลุ่ม ใน 150 ประเทศ และกว่า 400,000 เครื่องติดเชื้อไวรัส **Wannacry** มีค่าใช้จ่ายรวมประมาณ 4 พันล้านเหรียญ *(Malware Tech Blog)*

สถิติการละเมิดข้อมูล

- มี App มือถือที่เป็นอันตรายราว 24,000 รายการ ที่ถูกบล็อกทุกวัน (Symantec)

- ผลจากการศึกษาของสถาบัน Ponemon ในปี 2017 จำนวนที่ถูกละเมิดข้อมูลที่ถูกบันทึกตามประเทศต่างๆ เฉลี่ยแล้วมี 24,089 ครั้ง มากที่สุดต่อปี คืออินเดียที่มีไฟล์มากกว่า 33k ไฟล์ สหรัฐอเมริกามี 28.5k

Source: www.varonis.com/blog/cybersecurity-statistics/

การโจมตีระบบธนาคาร 5 แห่งในรัสเซีย เมื่อ 8 พ.ย 2559

- ธนาคาร 5 รายใหญ่ในรัสเซีย ได้แก่ **ธนาคาร** Sberbank, Alfa Bank, Bank of Moscow, Rosbank และ Moscow Exchange มีเครื่องคอมพิวเตอร์และอุปกรณ์ IoT กว่า 24,000 เครื่อง
- ถูกโจมตีอุปกรณ์ในรูปแบบของ distributed-denial-of-service (DDoS) ซึ่งเป็นการส่งคำสั่งไปยัง Server จำนวนล้านครั้ง เพื่อทำให้ระบบทั้งหมดเข้าสู่สถานะ Offline แล้วแฮ็คเกอร์ก็ทำการขโมยข้อมูล
- ธนาคารต้องใช้เวลาถึง 2 วันในการทำให้ระบบกลับสู่สภาพปกติ แต่เนื่องจากธนาคารจากรัสเซียได้มีการเตรียมพร้อมสำหรับการโจมตีที่ดีอยู่แล้ว จึงสามารถรับมือกับการโจมตีครั้งนี้ได้ และยังคงให้บริการผู้ใช้งานได้อย่างต่อเนื่อง
- ธนาคาร Sberbank แห่งรัสเซียที่ตกเป็นหนึ่งในเหยื่อการโจมตีครั้งนี้ ก่อนหน้านี้ก็เคยถูกกโจมตี DDoS มาก่อนแล้ว 68 ครั้ง ภายในปีนี้ปีเดียว
- การโจมตีครั้งนี้เกินกว่าครึ่งมาจาก ประเทศสหรัฐอเมริกา อินเดีย ไต้หวัน และอิสราเอล

การเจาะระบบธนาคารกลางของบังกลาเทศ

- **ลักษณะการก่อการร้าย :** แฮกเกอร์เจาะระบบ SWIFT (Society for Worldwide Interbank Financial Telecommunication) เป็นระบบเครือข่ายที่ใช้สื่อสาร โดยใช้ Malware โจมตีระบบด้านการเงินระหว่างธนาคารผ่านระบบคอมพิวเตอร์ที่ใช้ในธนาคารทั่วโลก
- **ความเสียหาย :** มีการโจรกรรมหรือถ่ายโอนเงินทุนสำรองไปยังศรีลังกาและฟิลิปปินส์ ทำให้เกิดความเสียหายมูลค่ากว่า 3 หมื่นล้านบาท

- **มัลแวร์(Malware)** คือ ไวรัสตัวหนึ่งที่ถูกปล่อยลงไปในระบบ เพื่อให้ระบบรวนและเสียหาย หลังจากนั้น กลุ่มคนร้ายก็ใช้ระบบใหม่ที่ตัวเองเตรียมมาใส่ครอบระบบที่เสียหายดังกล่าวเข้าไป เพื่อสามารถสั่งการ และซ่อนหลักฐาน และหลบเลี่ยงการถูกตรวจจับ

การเจาะระบบธนาคารกลางของบังกลาเทศ

สาเหตุ :

- จากการสอบสวนพบว่า มาจากการใช้อุปกรณ์รักษาความปลอดภัยราคาถูก และ Firewalls ไม่ได้ทำงานเต็มประสิทธิภาพ เนื่องจากติดปัญหาด้าน License
- ทางเจ้าหน้าที่ไม่ทำการติดตั้งระบบป้องกัน Firewalls ระหว่างระบบ RTGS และระบบ SWIFT เพื่อป้องกันการโจมตีจาก Malware เถื่อน
- ผู้ที่ทำการติดตั้งสวิชระบบเพื่อควบคุมการเชื่อมต่อเข้าสู่ระบบ SWIFT เจ้าหน้าที่เหล่านี้กลับเลือกใช้วิธีการที่ล้าสมัย ซึ่งไม่เคยใช้ในระบบธนาคาร มากกว่าที่จะเลือกใช้วิธีการที่มีความปลอดภัยสูงและล้ำสมัยเพื่อทำให้ทางธนาคารสามารถควบคุมการผ่านเข้าสู่ระบบ
- นอกจากนี้ยังพบว่าคนในมีส่วนเกี่ยวข้องด้วยจึงอาจเป็นเหตุผลหนึ่งที่ทำให้ระบบมีช่องโหว่จำนวนมากที่ทำให้ระบบคอมพิวเตอร์ของธนาคารกลางบังกลาเทศตกอยู่ในความเสี่ยง

การเจาะระบบธนาคารกลางของบังกลาเทศ

แนวทางการป้องกัน :

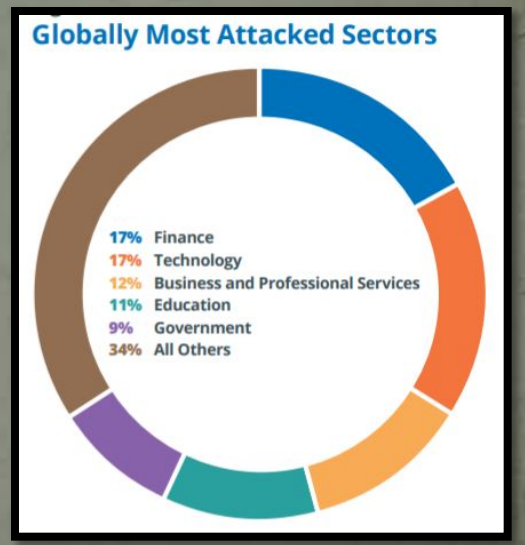
- หมั่นดำเนินการตามกระบวนการตรวจสอบความปลอดภัยของระบบ เพื่อตรวจสอบว่ามีช่องโหว่ทางด้านความปลอดภัยหรือไม่ เพื่อเร่งปิดช่องโหว่เหล่านั้น รวมทั้งตรวจสอบการทำงานของพนักงานภายในที่ดูแลระบบความปลอดภัยนี้ด้วย
- หมั่นตรวจสอบความเป็นไปรอบตัวทั้งในและนอกองค์กร
- ธนาคารควรแลกเปลี่ยนข้อมูลความเคลื่อนไหวของกลุ่มแฮกเกอร์ให้เป็นที่รับทราบระหว่างกัน
- ทำให้ระบบเป็นเอกเทศ โดยการติดตั้งระบบให้อยู่ในระบบ LAN เพื่อให้ไม่สามารถเชื่อมต่อเข้ากับระบบเครือข่ายคอมพิวเตอร์ส่วนกลางของทางธนาคารกลาง หรือไม่สามารถเข้าระบบจากภายนอกผ่านทางอินเตอร์เน็ตได้
- การใช้รหัสผ่านที่คาดเดาได้ง่าย
- เทคโนโลยีด้านความปลอดภัยนั้นไม่ใช่แค่การติดตั้งซอฟต์แวร์ หรือฮาร์ดแวร์ แต่ต้องเกิดจากการทำงานร่วมกัน ทั้งคนและเครื่องจักร รวมถึงระบบการทำงาน ความปลอดภัยของเครือข่ายจึงจะเกิดขึ้นได้จริง

การเจาะระบบเครื่อง ATM ของธนาคารออมสิน

- **ลักษณะการก่อการร้าย :**
- เมื่อวันที่ 23 ส.ค. 2559 แฮกเกอร์ได้เจาะระบบเครื่อง ATM ของธนาคารออมสิน อาศัยช่องโหว่ของซอฟต์แวร์ภายในตู้ ATM โดยใช้โปรแกรม Malware เข้าไปหลอกเครื่องว่ากำลังมีคนกดเงิน และทำให้เครื่อง ATM รวม 21 ตู้ปล่อยเงินออกมา โดยพบว่าเป็นการโจรกรรมเงินเฉพาะเครื่อง ATM ที่ติดตั้งนอกสถานที่ (Stand Alone)
- **ความเสียหาย :** เงินที่ถูกโจรกรรมไปรวมกว่า 12 ล้านบาท

การโจมตีภาคการเงินทั่วโลก ทางไซเบอร์ (Cyber attacks)

- ภัยคุกคามของการรั่วไหลของข้อมูลยังคงเพิ่มขึ้นอย่างต่อเนื่อง ภาคการเงินทั่วโลก มักเป็นเป้าหมายหลักของการโจมตีทางไซเบอร์ เนื่องจากมูลค่ามหาศาลของข้อมูลที่องค์กรเหล่านี้สามารถเข้าถึงได้
- บริษัทที่ให้บริการทางการเงิน (Financial services firms) ได้รับผลกระทบจากการโจมตีทางไซเบอร์ บ่อยครั้งมากกว่าธุรกิจในอุตสาหกรรมอื่นๆ
- NNT Security เปิดเผยว่า อุตสาหกรรมการเงินยังคงติดอันดับการถูกโจมตีทางไซเบอร์มากที่สุดในรอบ 6 ปีที่ผ่านมาโดยคิดเป็น 17% ของการโจมตีทั้งหมด
- รูปแบบการโจมตีที่พบมากที่สุดในภูมิภาคเอเชียแปซิฟิก คือ**การโจมตีบนเว็บ** คิดเป็น 36% ของทั้งหมด ถือเป็นรูปแบบการโจมตีที่มีสูงที่สุดในทุกภูมิภาค



Global Threat Intelligence Report 2019
by NTTSecurity

ประเทศต่าง ๆที่มีนัก Hacker ปฏิบัติงานมากน้อยตามลำดับดังนี้

1.ประเทศจีน เป็นประเทศที่มีแฮกเกอร์มากที่สุดในโลก มีหลายกลุ่มและมีการตั้งเป็นองค์กร ท้าทายรัฐบาลที่ลิดรอนเสรีภาพ ฝ่ายกองทัพเองก็มีสายสัมพันธ์กับบางกลุ่ม โดยดึงเข้ามาร่วมงาน มอบภารกิจให้โจมตีไซเบอร์ที่รัฐบาลเห็นว่าเป็นภัยความมั่นคงของประเทศ

2.ประเทศอเมริกา เป็นมหาอำนาจที่สามารถเจาะข้อมูลได้อย่างชำชอง แฮกเกอร์มีหลายกลุ่มและมีอิทธิพลสูงมาก อย่างกลุ่ม MOD, LOD ซึ่งบรรดาเหล่าแฮกเกอร์นี้ถือเป็นกลุ่มที่มีความสามารถในการเจาะข้อมูลต่างๆได้อย่างขั้นเทพ

3.ประเทศรัสเซีย เป็นประเทศที่ให้บรรดาเหล่าแฮกเกอร์มีอำนาจในการแฮกข้อมูลประเทศต่างๆ และแฮกเกอร์ส่วนใหญ่ก็เป็นแฮกเกอร์ที่สร้างความเสียหายได้ระดับโลก โดยบริษัทยักษ์ใหญ่อย่าง Microsoft, Apple พวกนี้มักจะโดนแฮกเกอร์รัสเซียท้าทายอยู่บ่อยครั้ง

4.ประเทศตุรกี ตุรกีเป็นประเทศที่มีแฮกเกอร์ที่มีความชำนาญสูง มีการตั้งกลุ่มทำงานกันเป็นทีม จะทำการแฮกเว็บไซด์เป็นจำนวนมาก ซึ่งกลุ่มมักจะกล่าวอ้างอยู่เสมอว่า สิ่งที่พวกเขาทำก็เพื่อสันติภาพและยุติสงครามอันเลวร้าย

5.ประเทศบราซิล บราซิลเป็นศูนย์กลางของบรรดาเหล่านักแฮกเกอร์ที่ชอบแฮกข้อมูลทั้งในทวีปเอเชียและยุโรป ประชากรส่วนใหญ่ของประเทศ**มักจะชอบทำธุรกรรมทางการเงินผ่านระบบออนไลน์** จึงเป็นจังหวะดีที่แฮกเกอร์ขโมยเงินในบัญชีทางอินเตอร์เน็ต ซึ่งมีข่าวให้เห็นอยู่บ่อยครั้ง

ประเทศต่าง ๆที่มีนัก Hacker ปฏิบัติงานมากน้อยตามลำดับดังนี้

6.ไต้หวัน เป็นประเทศอิสระ แต่จีนถือว่าเป็นมลฑลหนึ่งเท่านั้น ปัญหาทางการเมืองทำให้แฮกเกอร์โจมตีอยู่ต่อเนื่อง ซึ่งระบบอินเตอร์เน็ตของไต้หวันถือเป็นศูนย์กลางที่มักจะโดนพวกมัลแวร์โจมตีอยู่บ่อยๆ

7.ประเทศอินเดีย เป็นประเทศผู้นำทางด้านไอทีและคอมพิวเตอร์ จึงมีแฮกเกอร์เก่งๆอยู่เป็นจำนวนมาก ซึ่งแฮกเกอร์ส่วนมากเป็นนักรณรงค์ต่อต้านเรื่องต่างๆ จากการแฮกและพยายามท้าทายระบบเซ็นเซอร์อินเตอร์เน็ต

8.ประเทศโรมาเนีย เป็นประเทศที่มีขนาดเล็ก แต่มีแฮกเกอร์เก่งๆจำนวนมาก ที่อยู่ของแฮกเกอร์จะอยู่ในเมืองขนาดเล็ก ซึ่งถือเป็นสถานที่ที่ปลอดภัยและเป็นสวรรค์ในการกบดานของบรรดาเหล่านักอาชญากร

9.ประเทศฮังการี เป็นประเทศเล็ก แต่ก็มีการโจมตีจากเหล่าแฮกเกอร์มาก ประเทศในแถบยุโรปจะมีการป้องกันการโจมตีของเหล่าแฮกเกอร์เอาไว้เป็นอย่างดี แต่สำหรับประเทศฮังการีเป็นประเทศที่ตกเป็นเป้าหมายจากบรรดาเหล่าแฮกเกอร์ให้ทดสอบอยู่เสมอ

10.ประเทศอิตาลี มักจะโดนโจมตีจากกลุ่มไซเบอร์อยู่บ่อยครั้ง คิดแล้วประมาณ 1.6 เปอร์เซ็นต์เมื่อเทียบกับประชากรทั้งโลก โดยมีเหล่าแฮกเกอร์ที่มีชื่อเสียงได้ทำการแฮกเว็บไซต์ของรัฐบาลและก็เจาะข้อมูล

การจัดอันดับ Global Cybersecurity Index (GCI) 2017

- 10 อันดับประเทศที่ได้คะแนนสูงสุด จากทั้งหมด 164 ประเทศทั่วโลก ได้แก่

อันดับ	ประเทศ
1	สิงคโปร์
2	สหรัฐอเมริกา
3	มาเลเซีย
4	โอมาน
5	เอสโตเนีย
6	มอริเชียส
7	ออสเตรเลีย
8	จอร์เจีย และ ฝรั่งเศส
9	แคนาดา
10	รัสเซีย

Global Cybersecurity Index ranking 2017

Country	GCI score*	2017 ranking	2015 ranking
Singapore	**0.92**	**1**	**6**
United States	0.91	2	1
Malaysia	0.89	3	3
Oman	0.87	4	3
Estonia	0.84	5	5
Mauritius	0.82	6	9
Australia	0.82	7	3
Georgia	0.81	8	12
France	0.81	9	9
Canada	0.81	10	2

*Normalised

Source: U.N. INTERNATIONAL TELECOMMUNICATION UNION
STRAITS TIMES GRAPHICS

- หน่วยงาน National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา ทำหน้าที่กำหนดมาตรฐานเทคโนโลยีสารสนเทศ ได้วางแนวทางการรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity framework) เพื่อให้หน่วยงานของภาครัฐ เอกชน รวมถึงสถาบันการเงินต่างๆ ใช้เป็นแนวทางในการปฏิบัติ
- ธนาคารกลางของอังกฤษ สหรัฐอเมริกา และสิงคโปร์ ได้จัดให้มีการทดสอบการรับมือ Cyber Attack ในระดับประเทศมาตั้งแต่ปี 2554

ยุทธศาสตร์ความมั่นคงไซเบอร์ของสิงคโปร์

- การขับเคลื่อนสังคมและเศรษฐกิจด้วยเทคโนโลยีดิจิทัลภายใต้แนวคิด Internet of Things ทำให้ความมั่นคงไซเบอร์กลายเป็นเรื่องที่รัฐบาลสิงคโปร์ต้องให้ความสำคัญเป็นพิเศษ เนื่องจากจำเป็นต้องรับมือความเสี่ยงที่จะถูกโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์ที่เพิ่มจำนวนขึ้น
- รายงานของสำนักงานตำรวจแห่งชาติสิงคโปร์ในปี 2015 ระบุว่า อาชญากรรมไซเบอร์ในสิงคโปร์เพิ่มสูงขึ้นจากปีก่อนถึงร้อยละ 95
- ขณะที่รายงานของ AIG บริษัทประกันภัยชั้นนำ แสดงให้เห็นว่า ในปี 2016 ธุรกิจประกันภัยทางไซเบอร์ในสิงคโปร์เติบโตขึ้นกว่าร้อยละ 50 เนื่องจากธุรกิจเอกชนจำนวนมากเริ่มตระหนักถึงความเสี่ยงต่อการถูกคุกคามทางไซเบอร์ ซึ่งอาจส่งผลเสียต่อภาพลักษณ์ของบริษัทและก่อให้เกิดความเสียหายทางการเงินมหาศาล
- รัฐบาลสิงคโปร์จึงวางแผนจัดสรรงบประมาณร้อยละ 8 ของงบประมาณ ด้านเทคโนโลยีสารสนเทศ (ICT) ให้กับการเสริมสร้างความมั่นคงทางไซเบอร์
- รัฐบาลสิงคโปร์ได้ก่อตั้งหน่วยงานความมั่นคงไซเบอร์ (Cyber Security Agency-CSA) โดยให้ขึ้นตรงต่อสำนักนายกรัฐมนตรี เพื่อกำกับดูแลงานด้านความมั่นคงไซเบอร์ในภาพรวม และพัฒนาระบบไอทีของหน่วยงานรัฐและเอกชนมีความมั่นคงปลอดภัยดีขึ้น และการร่างกฎหมายความมั่นคงไซเบอร์ฉบับใหม่ที่เริ่มใช้เมื่อปี 2017

ยุทธศาสตร์ความมั่นคงไซเบอร์ของสิงคโปร์(ต่อ)

- หน้าที่ของ CSA (Cyber Security Agency-CSA) มี 4 อย่าง ได้แก่
  (1) สนับสนุนให้อุตสาหกรรมตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์
  (2) พัฒนาอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ให้มีกำลังคนเพียงพอต่อความต้องการ
  (3) ปกป้องโครงสร้างพื้นฐานของประเทศ เช่น พลังงาน และธนาคาร
  (4) อำนวยการให้มีความร่วมมือในการรับมือกับภัยต่างๆ

- **แผนยุทธศาสตร์ความมั่นคงไซเบอร์แห่งชาติ (National Cybersecurity Strategy)** ได้ระบุแนวทางในการส่งเสริมความมั่นคงไซเบอร์ของสิงคโปร์ไว้ 4 ประการ ได้แก่
  (1) สร้างโครงสร้างพื้นฐานทางไซเบอร์ให้ฟื้นคืนสภาพเดิมได้จากภัยคุกคามที่อาจเกิดขึ้นในอนาคต
  (2) สร้างความปลอดภัยให้โลกไซเบอร์
  (3) การพัฒนาระบบนิเวศทางความมั่นคงไซเบอร์ที่ตื่นตัวและมีชีวิตชีวา และ
  (4) ส่งเสริมความร่วมมือกับนานาชาติ

ความร่วมมือทาง Cybersecurity

- Olga Dergunova รองประธานและประธานคณะกรรมการบริหารของ VTB Bank (ธนาคารอันดับ 2 ของรัฐเซีย) ได้กล่าวไว้ใน International Cybersecurity Congress 2018 : in the spirit of collaboration ว่า

“เมื่อการดำเนินการบทบาทของคุณในฐานะธนาคารที่มีมาตรฐานที่ดี
สำหรับลูกค้าของคุณ จะส่งผลให้มีหลายดวงตาที่หันมามองคุณมากขึ้น
สิ่งเดียวที่สามารถทำได้เท่าที่ทรัพยากรดำเนินไป คือ
การปกป้องขอบเขตธุรกิจของตัวเอง และร่วมมือกับหน่วยงานอื่น ๆ
เพื่อป้องกัน ซึ่งไม่ใช่เฉพาะตัวคุณเองเท่านั้น แต่เพื่ออุตสาหกรรมโดยรวมด้วย”

ความร่วมมือทาง Cybersecurity

- การทำให้ระบบรักษาความปลอดภัยที่ซับซ้อนมีความสะดวกมากขึ้น ด้วยวิธีกำหนดมาตรฐานสำหรับกรอบความปลอดภัย (standards for security frameworks) ที่สามารถอนุญาตให้ระบบต่างๆ ทำงานได้อย่างรวดเร็วและมีประสิทธิภาพ

- สิ่งที่จะทำให้สิ่งเหล่านี้เกิดขึ้นได้ คือ **“ความร่วมมือ”** โดยเราจำเป็นต้องร่วมมือพัฒนากลไกการทดสอบเทคโนโลยีปัจจุบันและเทคโนโลยีใหม่ๆ ที่มาสนับสนุนการให้บริการทางการเงิน (Cross-bank sandbox) **เพื่อ “ทดสอบเทคโนโลยีและอันตรายของวันพรุ่งนี้”** ได้อย่างเหมาะสม และเพื่อให้เทคโนโลยีปัจจุบันและเทคโนโลยีใหม่ๆ ปลอดภัยมากขึ้น มีประสิทธิภาพ และเชื่อถือได้

- หากกลไกการทดสอบยังไม่ได้รับการพัฒนาอย่างเหมาะสม การควบคุมให้ระบบใหม่ ๆ ที่เราพัฒนา จะไม่สามารถพิสูจน์สิ่งที่เป็นช่องโหว่ด้านความปลอดภัยได้ตั้งแต่เริ่มต้น

แหล่งข้อมูลสำหรับติดตามความเคลื่อนไหวของภัยคุกคามทางไซเบอร์

- **ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)**
  สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
  https://www.thaicert.or.th/
- **ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ภาคการธนาคาร** (Thailand Banking Sector CERT (TB-CERT) ที่ถูกจัดตั้งเพื่อเตรียมพร้อมรับมือกับภัยคุกคามไซเบอร์ทางการเงิน
- **ธนาคารแห่งประเทศไทย**

Thank you

www.facebook.com/ekkachai.srivilas
www.elifesara.com