

# Cyber Warfare

น.ท.กรกช วีไลลักษณ์

โรงเรียนเสนาธิการทหารเรือ

- 1 สงเคราะห์
- 2 ความมั่นคงปลอดภัยสารสนเทศ
- 3 Best Practices
- 4 Question and Discussion

## วัตถุประสงค์การเรียนรู้

### เมื่อสิ้นสุดการบรรยาย นทน.ฯ ควร

- เข้าใจหลักการปฏิบัติการไซเบอร์
- เข้าใจหลักการรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศและการสื่อสาร
- เข้าใจความเกี่ยวข้องกันของ “PPT” ในปฏิบัติการไซเบอร์
- ประยุกต์ใช้ความรู้ที่ได้รับอย่างเหมาะสม

## Cyber Warfare

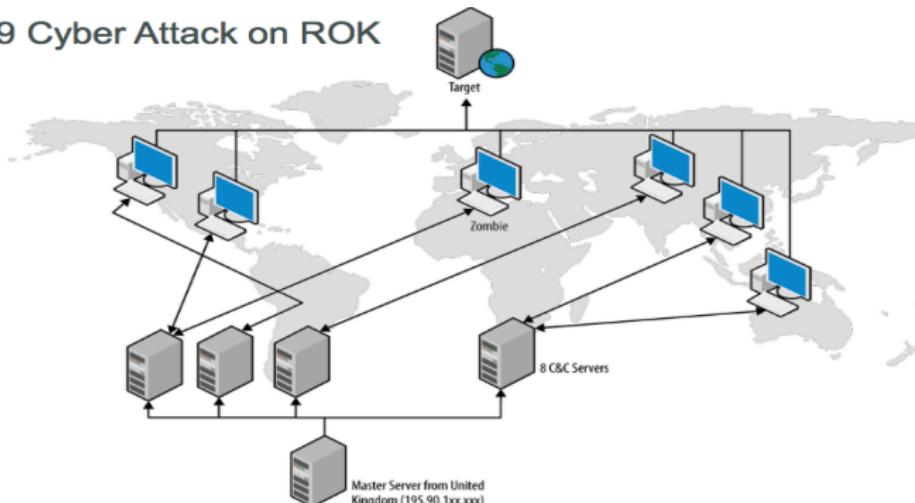
## Clausewitz: On War

We shall not enter into any of the abstruse definitions of War used by publicists. We shall keep to the element of the thing itself, to a duel. War is nothing but a duel on an extensive scale. If we would conceive as a unit the countless number of duels which make up a War, we shall do so best by supposing to ourselves two wrestlers. Each strives by physical force to compel the other to submit to his will: each endeavours to throw his adversary, and thus render him incapable of further resistance.

*War therefore is an act of violence intended to compel our opponent to fulfil our will.*

## MyDoom Attribution Case Study

- 2009 Cyber Attack on ROK



- 166,908 bots scattered across 74 different countries



What does a stealth bomber cost? **\$1.5 to \$2 billion**



What does a stealth fighter cost? **\$80 to \$120 million**



What does a cruise missile cost? **\$1 to \$2 million**



What does a cyber weapon cost? **\$0 to \$50,000**

## What is cyber warfare?

- Information Operation
- ปฏิบัติการทางทหารสาขาหนึ่งของปฏิบัติการข่าวสาร (Information warfare)
- มุ่งทำลาย CIA ของฝ่ายตรงข้าม
- Symmetric or Asymmetric
- JP 3-13 Information Operation

## เหตุใดจึงต้องเรียนรู้?

- Diplomatic
- Information
- Military
- Economy

Cyber space is a battlefield of the Internet and the ubiquitous nature of cyber conflicts being enmeshed into the physical battlefield.

## คุณลักษณะสนามรบ: ขอบเขตของสนามรบ

- ขอบเขตเชิงตรรกะ (Logical boundary)
- ขอบเขตเชิงกายภาพ (Physical boundary)
- ขอบเขตเชิงการบริหารจัดการ (Organizational boundary)

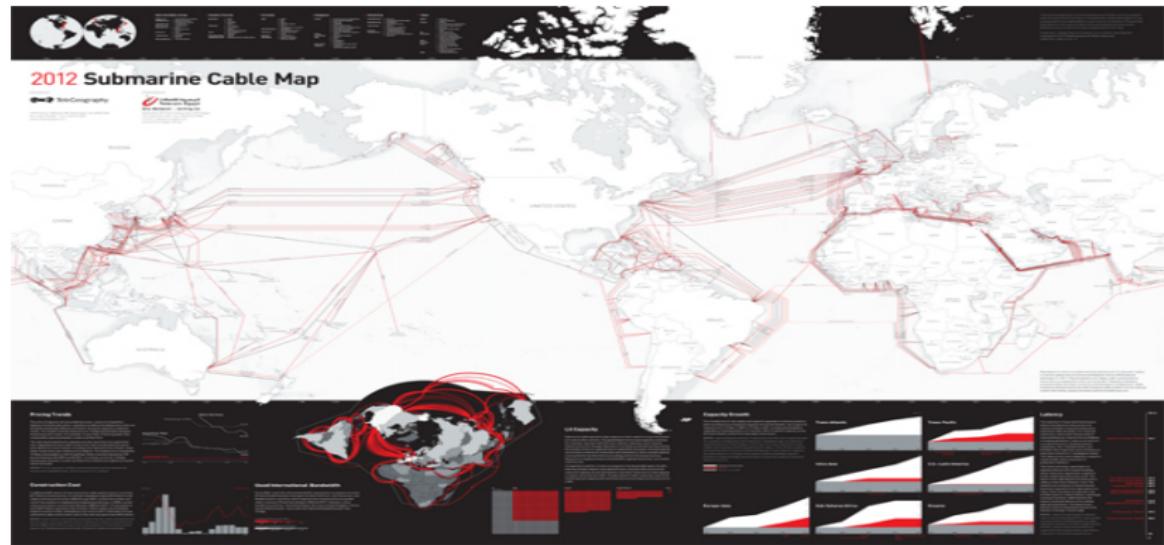
## ຄຸນລັກຂະນະສນາມຮບ: ຂອບເຂດຂອງສນາມຮບ(Cont.)

### ຂອບເຂດເຈີ້ງຕຽກ (Logical boundary)



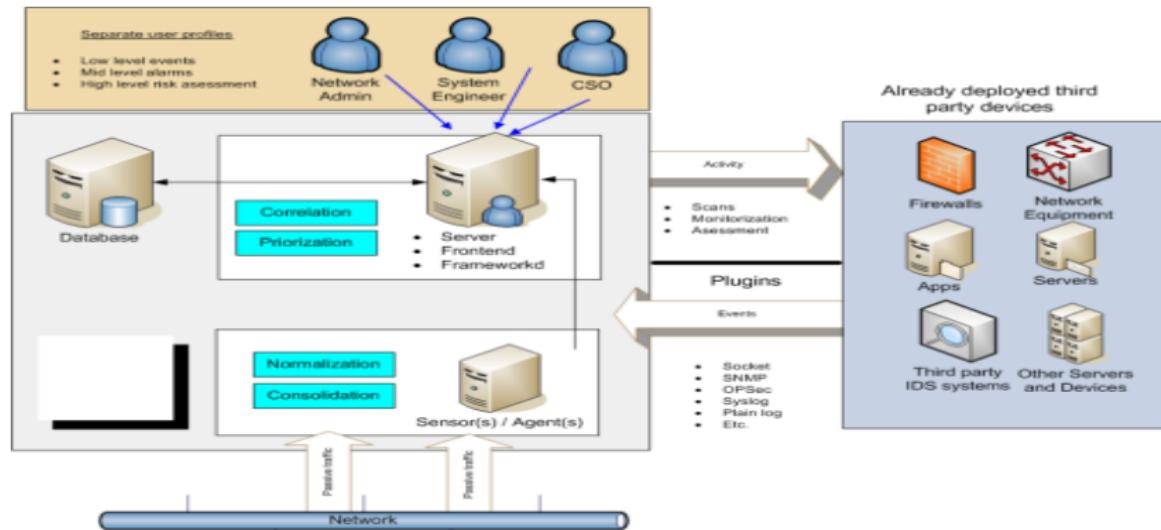
คุณลักษณะสนามรบ: ขอบเขตของสนามรบ(Cont.)

## ขอบเขตเชิงกายภาพ (Physical boundary)



## ຄຸນລັກຂະນະສານາມຮບ: ຂອບເຂດຂອງສານາມຮບ(Cont.)

### ຂອບເຂດເຈີ່ງການບໍລິຫານຈັດກາ



## Conventional War Fighting

- การปฏิบัติ (เทคนิคการโจมตี) จะแตกต่างกันออกไปขึ้นอยู่กับระดับของ  
    สงคราม
  - Strategic
  - Operational
  - Tactical
- มุ่งทำลาย COG ของเป้าหมายเชิงยุทธศาสตร์
  - กำลังทางบก
  - กำลังทางอากาศ
  - กำลังทางเรือ
  - โครงสร้างพื้นฐานที่เกี่ยวข้องกับการสื่อสารและโทรคมนาคม

## Cyber warfare

- มุ่งทำลาย CIA ของเป้าหมายเชิงยุทธศาสตร์
  - ค้นหาช่องโหว่ของโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสาร
  - ปฏิบัติการข้อมูลข่าวสาร PSYOPS, Disinformation, Diversionary
  - โจมตีผู้สมัครงานกับ Electronic Attack Vectors อื่นๆ
  - ระบบตรวจสอบจับต่างๆ และทำลายโครงสร้างพื้นฐานการควบคุม บังคับบัญชา

## นักรบ

MARINES MOVE TOWARD THE SOUNDS OF TYRANNY, INJUSTICE AND DESPAIR.



 MARINES.COM

ນັກຮບໄຊເບອຣ



## อาวุธเชิงตรรกะ

- Reconnaissance tools
- Scanning tools
- Access and escalation tools
- Exfiltration tools
- Sustainment tools
- Assault tools
- Obfuscation tools

## Information Security

## The CIA triad



- การรักษาความลับ (Confidentiality)
- การรักษาความครบถ้วนสมบูรณ์ (Integrity)
- การรักษาความพร้อมใช้ (Availability)

## The CIA triad



- การพิสูจน์สิทธิ์ (Authentication)
- การกำหนดสิทธิ์ (Authorization)

## Persisting Threats and Attacks: Experimentation

### Experimentation



**Cracker:**  
Computer-savvy  
programmer creates  
attack software



**Script Kiddies:**  
Unsophisticated  
computer users  
execute programs

**Hacker Bulletin Board**  
SQL Injection  
Buffer overflow  
Password Crackers  
Password Dictionaries

Successful attacks!  
Crazyman broke into ...  
CoolCat penetrated...

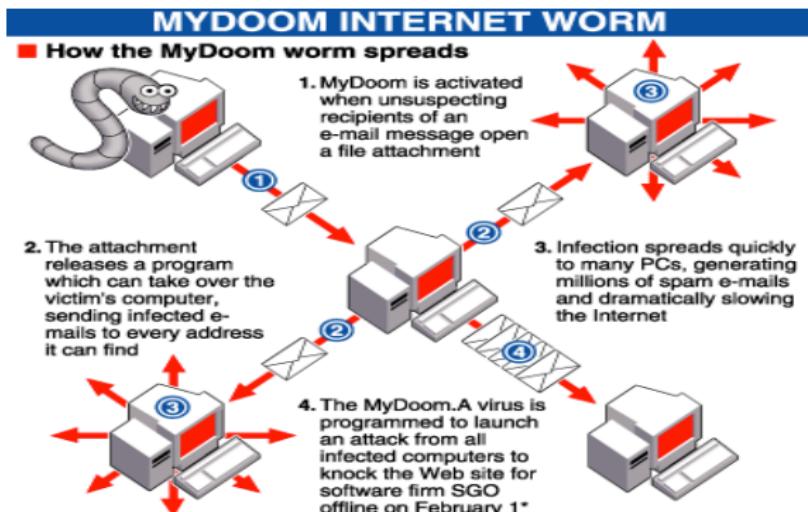


Malware package=\$1K-2K

## Persisting Threats and Attacks (Cont.): Malware



## Persisting Threats and Attacks (Cont.): Worm



\*A second variant dubbed MyDoom.B is timed to attack SCO on February 1 and Microsoft on February 3. It also prevents access to anti-virus sites

Source: Central Command Inc.

REUTERS

- Melissa(2000), I love you (2001), Code red and code red II (2001), My Doom (2003), etc.

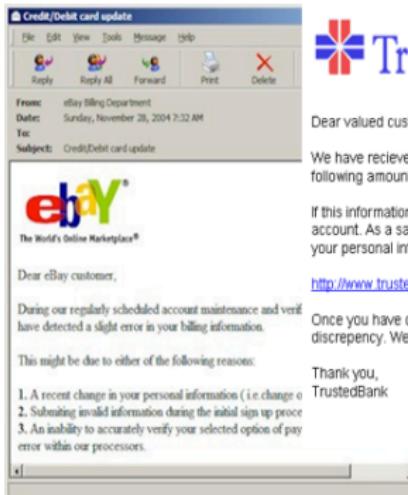
## Persisting Threats and Attacks (Cont.): Social Engineering



- หลอกกลวงผู้ใช้งาน, สอดถามพางาน, ฯลฯ

## Persisting Threats and Attacks (Cont.): Pharming

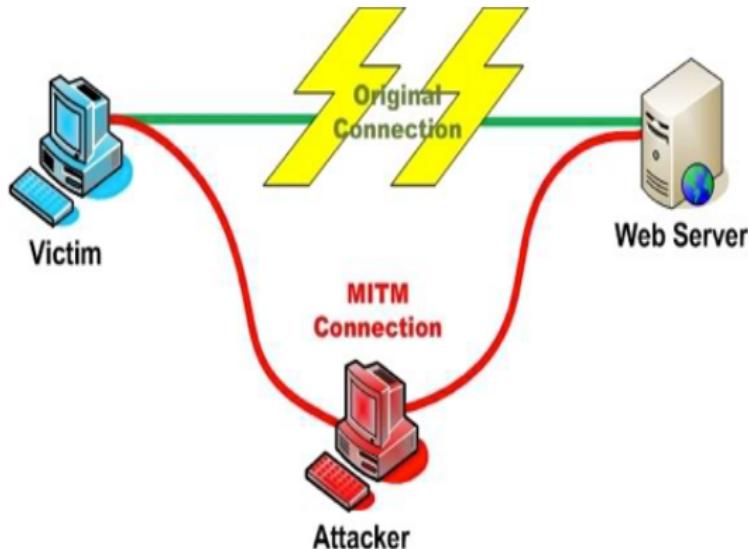
### Pharming = Fake Web Pages



From: [ebay-billing@ebay.com](mailto:ebay-billing@ebay.com) [mailto:[ebay-billing@ebay.com](mailto:ebay-billing@ebay.com)]

Member FDIC © 2005 TrustedBank, Inc.

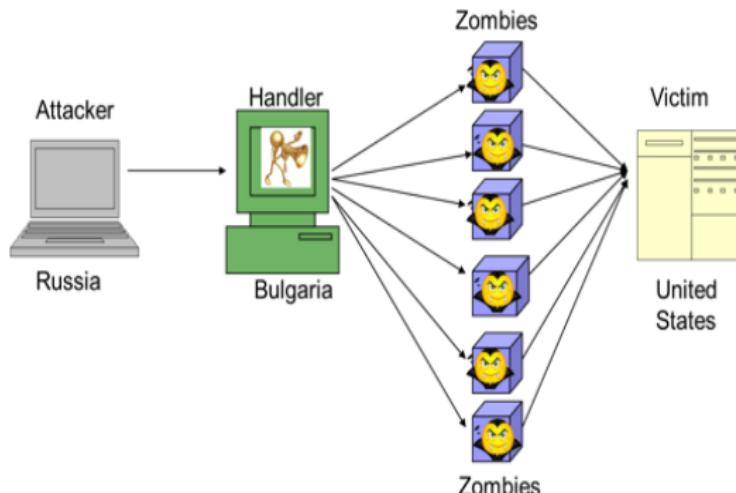
## Persisting Threats and Attacks (Cont.): Man-In-The-Middle



## Persisting Threats and Attacks (Cont.): Rootkits



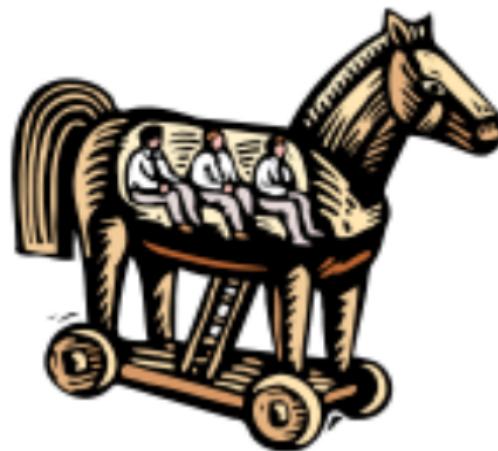
## Persisting Threats and Attacks (Cont.): Botnet



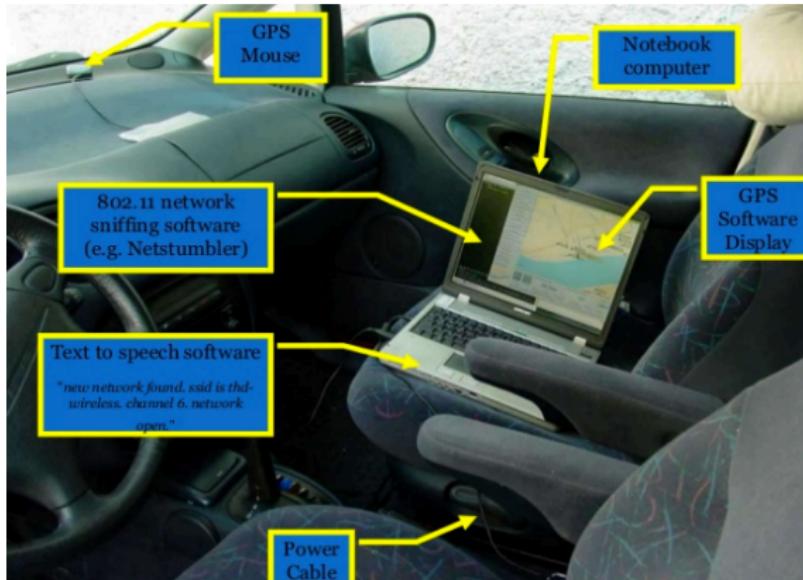
## Persisting Threats and Attacks (Cont.): Key logger



## Persisting Threats and Attacks (Cont.): Trojan



## Persisting Threats and Attacks (Cont.): War driving



## Persisting Threats and Attacks (Cont.): Ransomware

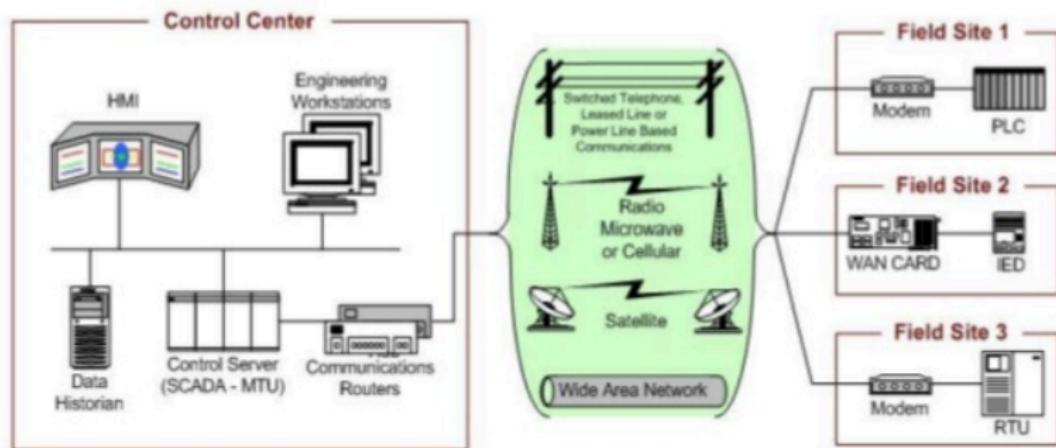


## Persisting Threats and Attacks (Cont.): Password Brute-force

Pattern	Calculation	Result	Time to Guess ( $2.6 \times 10^{18}/\text{month}$ )
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	$26^4$	$5 \times 10^5$	
8 chars: lower case alpha	$26^8$	$2 \times 10^{11}$	
8 chars: alpha	$52^8$	$5 \times 10^{13}$	
8 chars: alphanumeric	$62^8$	$2 \times 10^{14}$	3.4 min.
8 chars alphanumeric +10	$72^8$	$7 \times 10^{14}$	12 min.
8 chars: all keyboard	$95^8$	$7 \times 10^{15}$	2 hours
12 chars: alphanumeric	$62^{12}$	$3 \times 10^{21}$	96 years
12 chars: alphanumeric + 10	$72^{12}$	$2 \times 10^{22}$	500 years
12 chars: all keyboard	$95^{12}$	$5 \times 10^{23}$	
16 chars: alphanumeric	$62^{16}$	$5 \times 10^{28}$	

ระยะเวลาที่ใช้ในการสุมเดาพาสเวิร์ด

## อาชญากรรมทางภาพ: SCADA



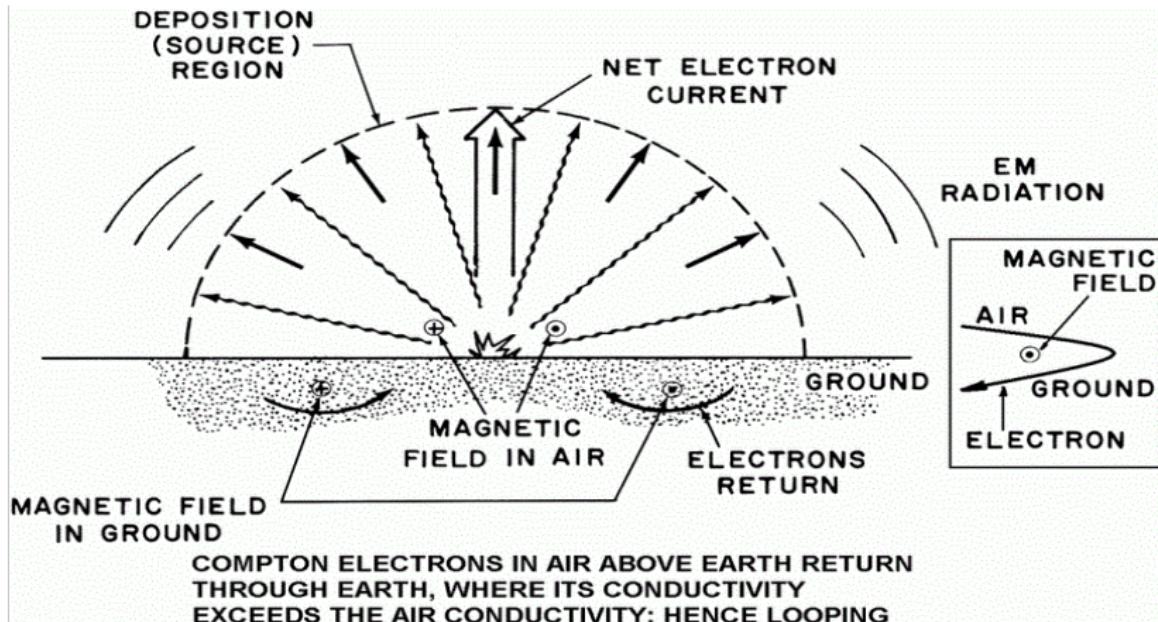
HMI – Human-Machine Interface

M/RTU – Master/Remote Terminal Unit

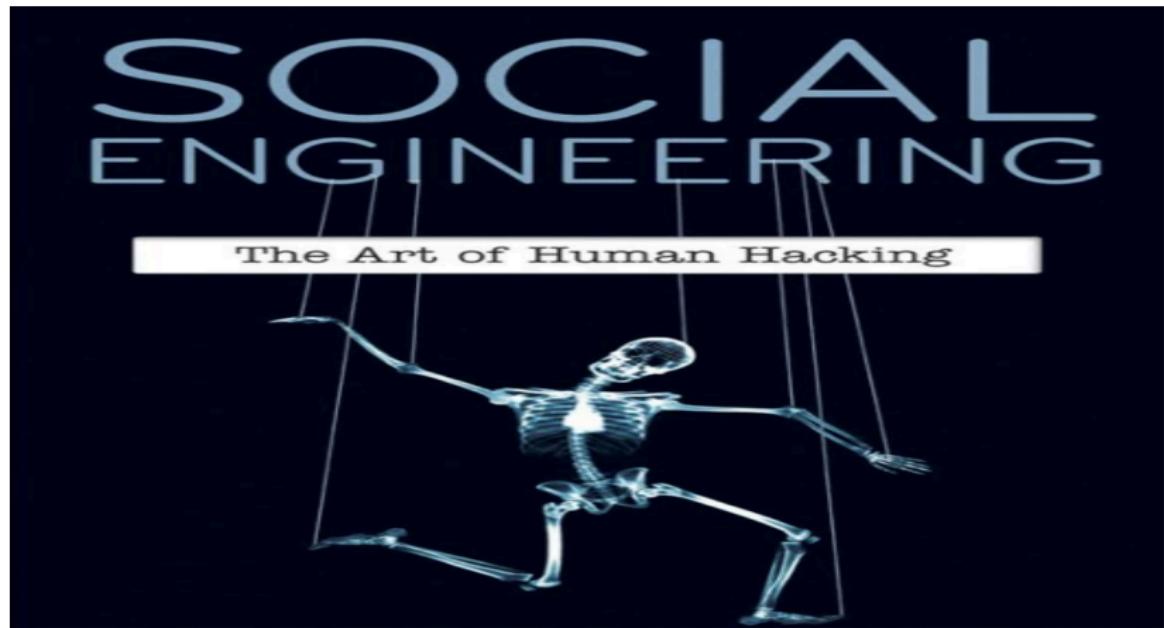
PLC – Programmable Logic Controllers

IED – Intelligent Electronic Devices

## อาวุธเชิงกายภาพ: Electro Magnetic Pulse Weapons



อาชีวะเชิงจิตวิทยา



## ความท้าทายของสังคมไซเบอร์

- P eople = Skills + Organization
- P olicy = Organization + Processes
- T echnology = Processes + Skills

## คำแนะนำระดับชาติ

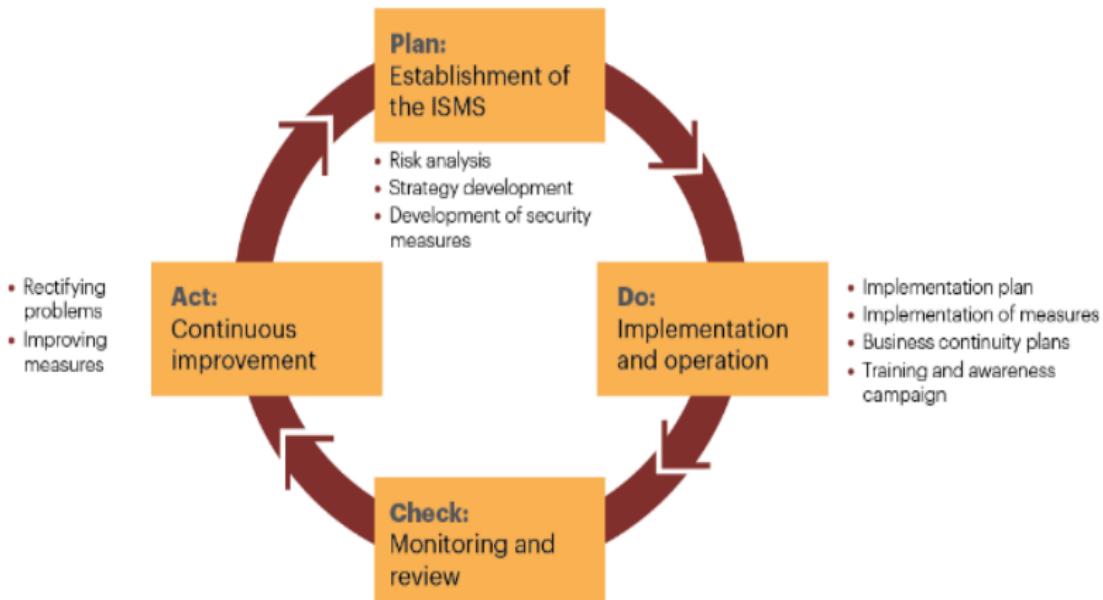
- ปรับตัวและสร้างความตระหนักรู้ในระดับผู้บริหาร
- สร้างมาตรฐาน กฎหมาย และความร่วมมือกับชาติพันธมิตร
- พัฒนาโครงสร้างพื้นฐานที่เกี่ยวข้อง (PPT)

## คำแนะนำหน่วยงานความมั่นคง

- บังคับใช้มาตรการที่จำเป็นเพื่อรักษาความมั่นคงปลอดภัย
- นำแนวทางการบริหารจัดการความมั่นคงปลอดภัยมาประยุกต์ใช้ (ISO2700x)
- หมั่นตรวจสอบความมั่นคงปลอดภัยตามแนวทางที่กำหนดขึ้น
- ประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง (ThaiCert)

## คำแนะนำหน่วยงานความมั่นคง

### "Plan-Do-Check-Act" (PDCA) information security cycle per ISO 2700x



## คำแนะนำในระดับปัจเจกบุคคล

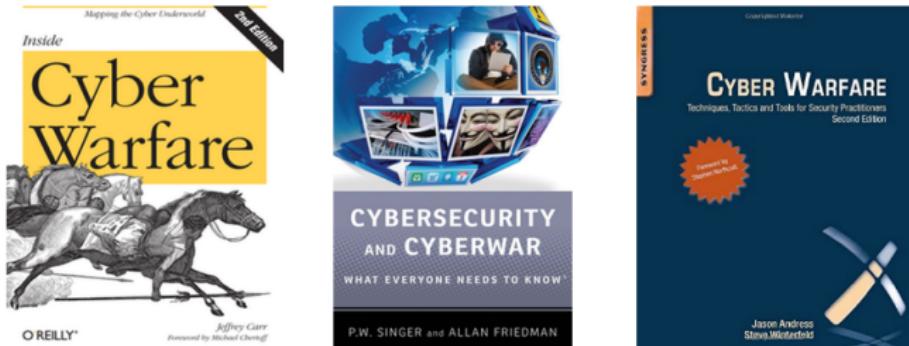
- ตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ และใช้เทคโนโลยีอย่างมั่นคงปลอดภัย
- ติดตั้งซอฟต์แวร์ตรวจจับไวรัส มัลแวร์
- ตระหนักรู้ถึงการโจมตีแบบวิศวกรรมเชิงสังคมและมัลแวร์
  - ไม่เปิดไฟล์ที่แนบมากับอีเมล์ที่ไม่น่าไว้วางใจ
  - เปิด ดาวน์โหลดและซอฟต์แวร์จากแหล่งที่น่าเชื่อถือ
  - อัปเดตระบบปฏิบัติการให้ทันสมัยอยู่เสมอ
  - หลีกเลี่ยงการใช้พาราเซมอลที่ง่ายต่อการคาดเดา
  - สำรองข้อมูลอยู่เสมอๆ เปลี่ยนพาสเวิร์ดบ่อยๆ

## Question and Discussion



โทรศัพท์มือถือ และเครื่องคอมพิวเตอร์ที่ท่านใช้...มีความมั่นคงปลอดภัยหรือไม่???

## References



J. Carr, Inside **Cyber Warfare, 2nd edition**, O'Reilly Media Inc, CA95472, USA, ISBN: 978-1-449-31004-2, 2011

P.W. Singer, A. Friedman, **Cybersecurity and Cyberwar: What everyone needs to know**, Oxford University Press, NY10016, USA, ISBN: 978-0-19-991809-6, 2011

J. Andress, S. Winterfeld, **Cyber Warfare - Techniques, Tactics, and Tools for Security Practitioners**, Syngress, MA02451, USA, ISBN:978-1-59749637-7, 2011