

Cybersecurity Community & National Security



PRINYA HOM-ANEK

CISSP, CSSLP, SSCP, CASP, CFE, CBCI, CSX, ITIL Expert, CDPSE
COBIT 5 Foundation, COBIT 5 Implementation

Eisenhower Fellowships 2013, Member of (ISC)² Asian Advisory Council,
ISACA Bangkok, Thailand Information Security Association (TISA) Board Member,
Cybertron Co., Ltd. – CEO & ACIS Professional Center – Chairman of Executive Committee



ACIS/Cybertron Privacy & Cybersecurity Research LAB



ACIS PROFESSIONAL CENTER
YOUR SATISFACTION IS OUR PRIDE



We have been certified to

ISO 22301:2012 (BCMS)
ISO/IEC 27001:2013 (ISMS) standards.
ISO/IEC 20000-1:2011 (IT-SMS)

History & Revolution of Cyber Domain

1st Gen : Computer Security (1986)

2nd Gen : Information Security (2005)

3rd Gen : Cybersecurity (2013)

4th Gen : Cyber Resilience (2011/2023)

5th Gen : Cyber Dominance (2020/2030)

TOWARDS: RESPONSIVE SECURITY

Fortress Mentality

Are we secure ?

Responsive & Readiness Mentality

Are we ready ?

Risk-based: Value Preservation

“UNKNOWN UNKNOWNNS” => “ KNOWN UNKNOWNNS”

<i>Knowns</i>	<i>Known Knowns</i> <i>Things we are aware of and understand.</i>	<i>Known Unknowns</i> <i>Things we are aware of but don't understand.</i>
	<i>Unknown Knowns</i> <i>Things we understand but are not aware of.</i>	<i>Unknown Unknowns</i> <i>Things we are neither aware of nor understand.</i>
<i>Unknowns</i>	<i>Knowns</i>	<i>Unknowns</i>

“FROM DIGITAL DIVIDE TO DIGITAL INEQUALITY”

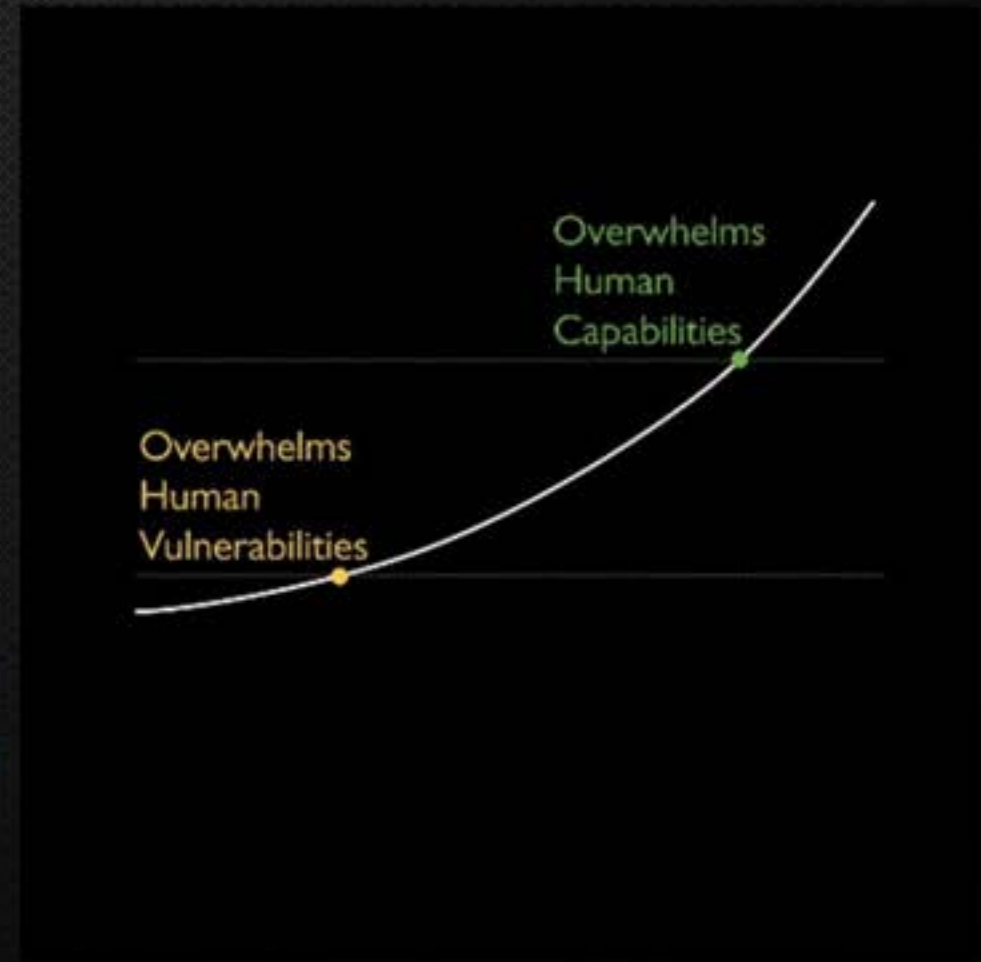
Upgrading technology but downgrading humanity



Human Vulnerabilities vs. Human Capabilities

Most recent conversations about the future focus on the point where are technology surpasseshuman capability

But they overlook a much earlier point where technology exceeds human vulnerabilities



Critical Thinking



Internet Safety



Digital Plagiarism



Digital Literacy

Digital Search Skills



Online Identity Management



**"FROM CYBER RISK
TO DIGITAL RISK"**

7 Digital RISKS

(You must Concern)



How Thailand will survive from “The Hidden **Data Privacy** Threats”

Acis

Security with Passion

DIGITAL FOOTPRINTS

What do yours say?

BE CAREFUL ABOUT:

- What you share.
- Where you share.
- With whom you share.

BE SMART ABOUT:

- Sites you visit.
- Emails you open.
- Links you click.

BE YOURSELF
but be your best self.

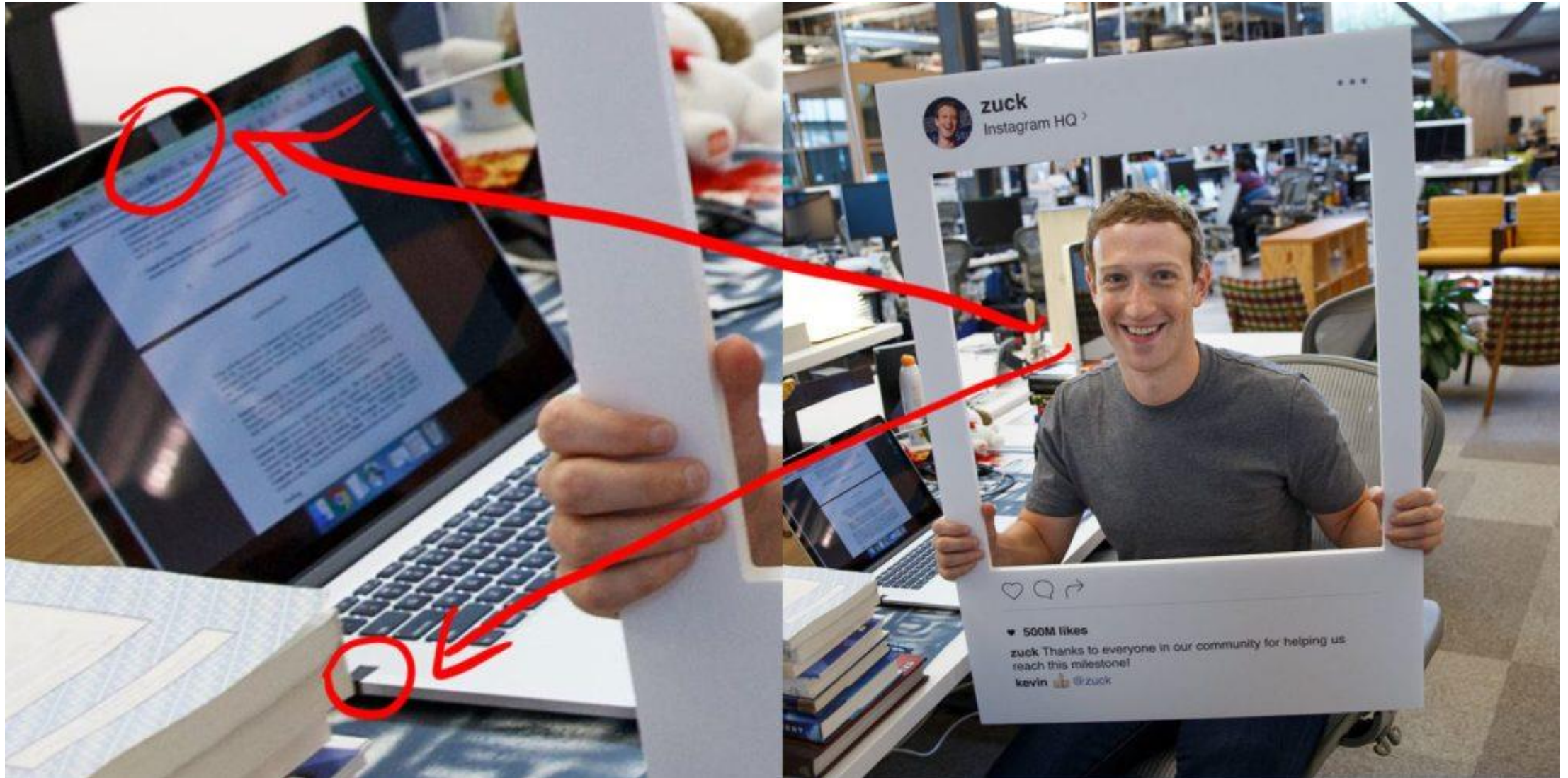


The background is a dark city skyline at night. Overlaid on this are several glowing blue icons: a Wi-Fi symbol, a globe, a smartphone, a dollar sign, and a cloud with an upward arrow. These icons are connected to the city buildings by vertical dotted lines. In the bottom left corner, there is a network diagram consisting of several nodes connected by lines.

“DIGITAL IDENTITY- DIGITAL FOOTPRINT”

ความโง่โง่ที่คุณอาจไม่รู้มาก่อน
ต้องระวังทั้งบนโลกเสมือนไปจนถึงการใช้ชีวิตจริง

Mark Zuckerberg @ Facebook HQ



Cyberspace as a FIFTH DOMAIN

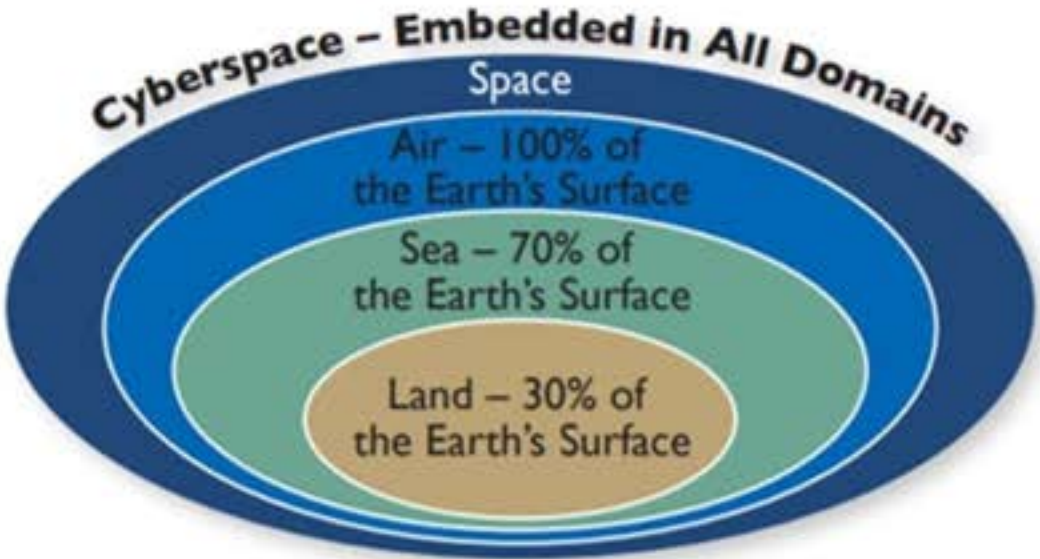


Figure 1. Cyberspace – the Embedded Domain





CYBER DOMINANCE





NAVY CYBER REINFORCEMENTS

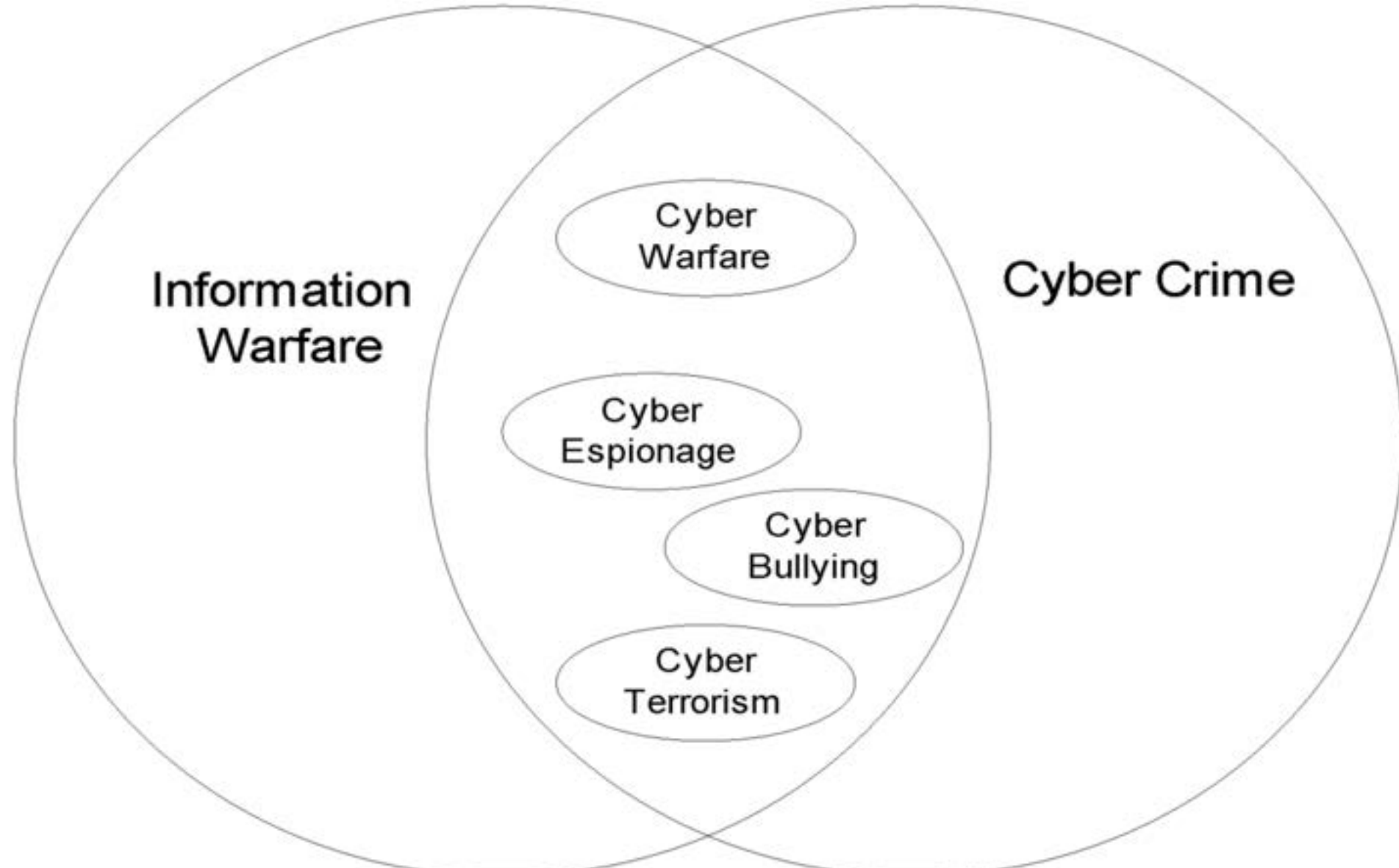
RESERVE CYBER TEAM DELIVERS
EXPERTISE IN THE BATTLE FOR CYBER

DOMINANCE

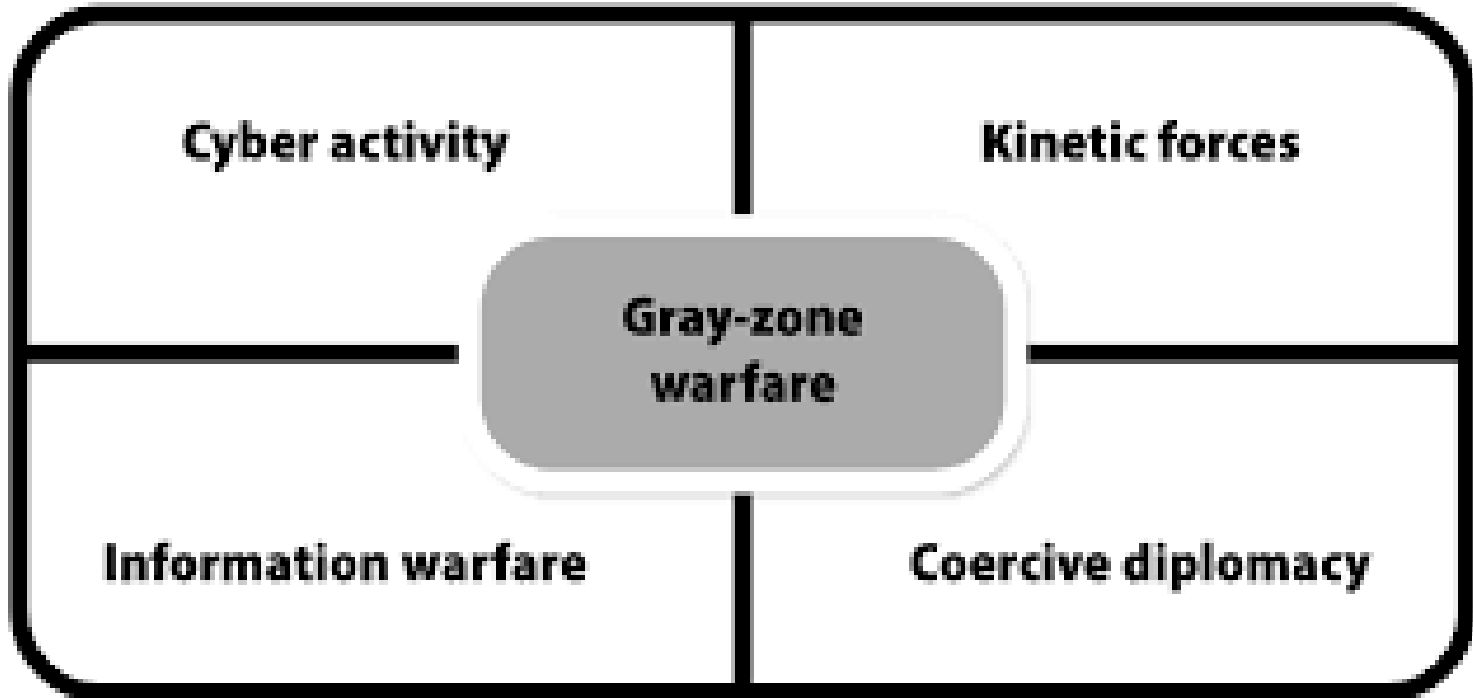
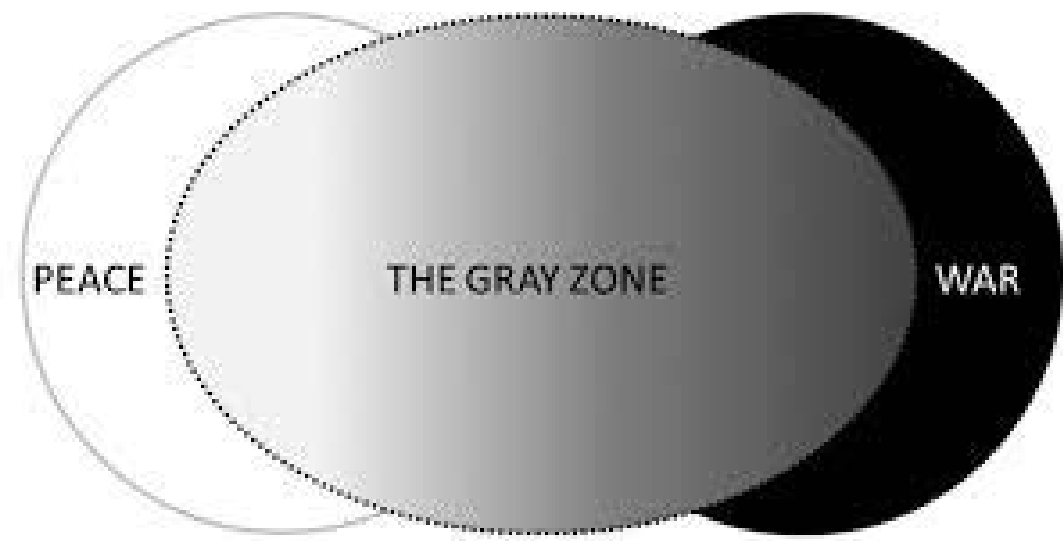
Is your Smartphone hijacking your mind?



Information Warfare vs. Cyber Warfare









Malign Influence Operations

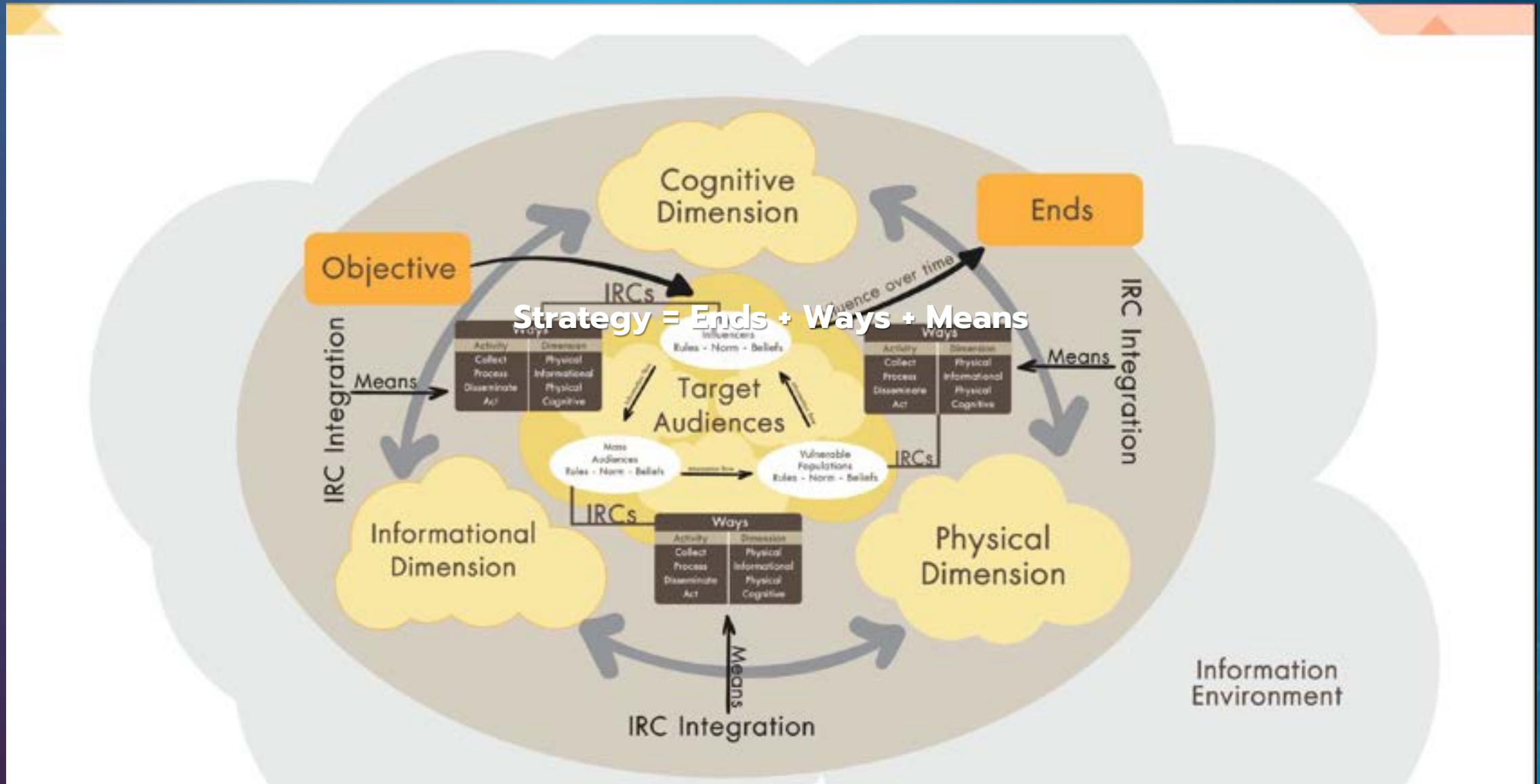
ปฏิบัติการอิทธิพลแอบแฝง



Social Media

ผลกระทบต่อ “GEN Z”

Information-Related Capabilities (IRCs)





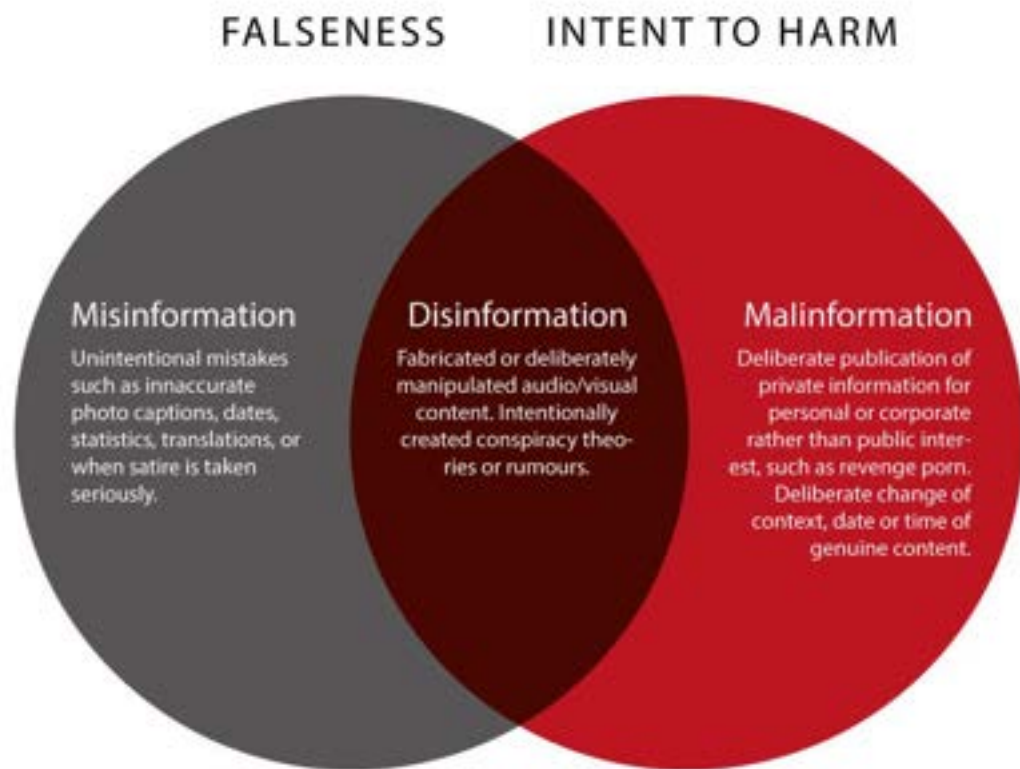
INFORMATION DISORDER

ถูกหลอกโดยไม่รู้ตัว “หลอกลงทุน และ ความ
ผิดปกติของข้อมูลข่าวสาร



INFORMATION DISORDER

TYPES OF INFORMATION DISORDER

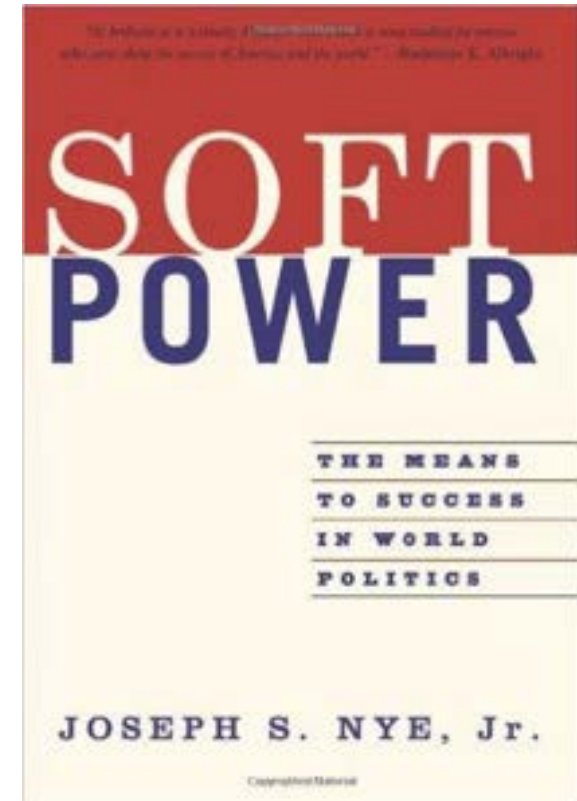


รวมทั้งสหภาพยุโรปยังได้ขยายความ Information Disorder ออกเป็น 3 ประเภท ได้แก่ 1. Misinformation หรือ ข้อมูลที่ผิด 2. Disinformation หรือ ข้อมูลบิดเบือน และ 3. Malinformation หรือ ข้อมูลที่แฝงเจตนาร้าย

Soft Skill



Soft Power



Question #1

How has the evolving cyber threat landscape impacted the role of the cybersecurity community in ensuring national security?



Answer Question #1

1. **Broaden Scope**
 2. **State-Sponsored Cyber Attacks**
 3. **Increased Collaboration**
 4. **New Forms of Warfare : Cyber Dominance , From IO to IA**
 5. **Emphasis on Resilience**
 6. **Regulatory and Policy Evolution**
 7. **Talent Gap**
 8. **Private Sector Engagement**
- 

Question #2

What are some successful examples of public and private sector collaboration in responding to cyber threats and enhancing national cybersecurity?



Answer Question #2

1. **Cybersecurity Law 2019**
2. **PDPA 2019**
3. **NCSA + TISA, CISO training**
4. **PDPC + TISA, DPO training**
5. **Bank of Thailand + TB-CERT+NCSA+PDPC**

Question #3

What role does the cybersecurity community play in identifying and mitigating insider threats that could compromise national security?

Answer Question #3

1. **Security Awareness Training + BAS**
2. **Cyber Drill**
3. **CTF with Cyber Range**
4. **Whistleblower Programs**
5. **Regular Audits and Assessments**
6. **Threat Intelligence Sharing**
7. **Incident Response (plan + drill)**
8. **Internal Fraud Detection**
9. **Change to Cyber Resilience Mindset**

Further reading links

ACIS : <https://www.acisonline.net>

Cybertron : <https://www.cybertron.co.th>

My Blog : <https://www.prinya.org>

**Conference 29-30 Nov 2023 @ BITEC :
<https://www.cdicconference.com>**

○○○○

THANK YOU
Further
Reading,
Please visit

 <https://www.prinya.org>



