แนวคิดและหลักนิยมการปฏิบัติการไซเบอร์

ขอบเขตการบรรยาย

- หลักนิยมกองทัพอากาศ
- แนวคิดการใช้กำลังทางไซเบอร์

ภารกิจ

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๖๐
หมวด ๕ หน้าที่ของรัฐ

พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม
พ.ศ.๒๕๕๑ มาตรา ๒๑

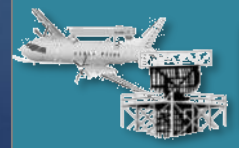
ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๑-๒๕๘๐)

กองทัพอากาศชั้นนำในภูมิภาค
One of the best Air Forces in ASEAN

Royal Thai Air Force Power

AIR Domain


C2


Sensors


Shooters


Network


Support & Service


Human & Behavior

CYBER Domain


Cyber Defense


Cyber Intelligence


Cyber Offense

SPACE Domain

Space Observation

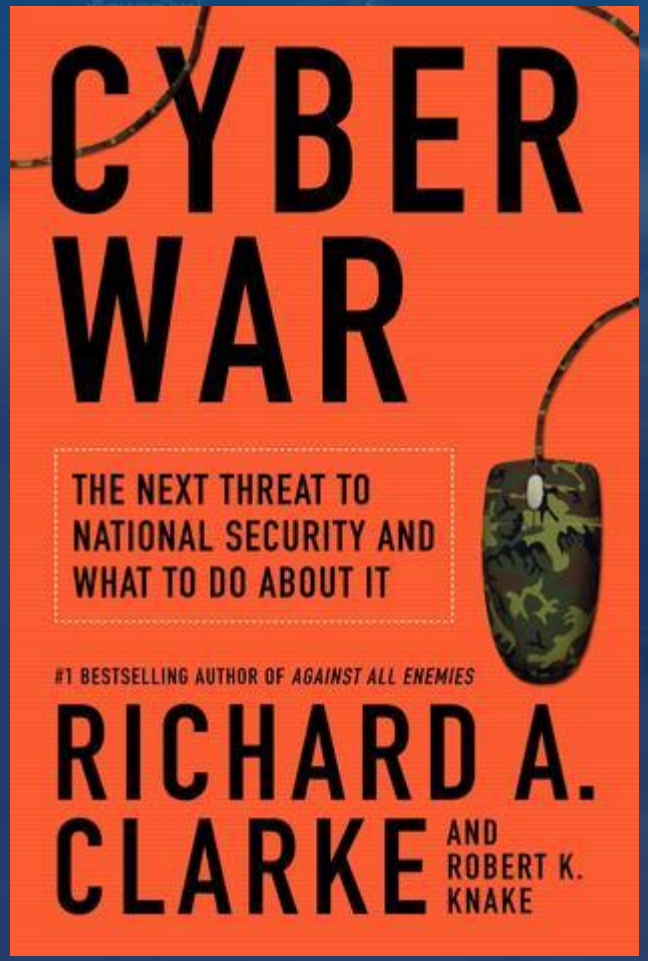
Space Surveillance

Space Defense

หลักนิยมปฏิบัติการไซเบอร์

- คำนิยามสงครามไซเบอร์
- ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น
- หลักนิยมปฏิบัติการไซเบอร์

คำนิยามสงครามไซเบอร์



"สงครามไซเบอร์ เป็นคำที่นิยามขึ้นมาโดย ผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลที่ชื่อ ริชาร์ด เอ. คลาร์ก ในหนังสือที่ชื่อ Cyber War (พฤษภาคม 2010) โดยนิยามว่า "เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก"

ภัยคุกคามทางไซเบอร์

DDos attack

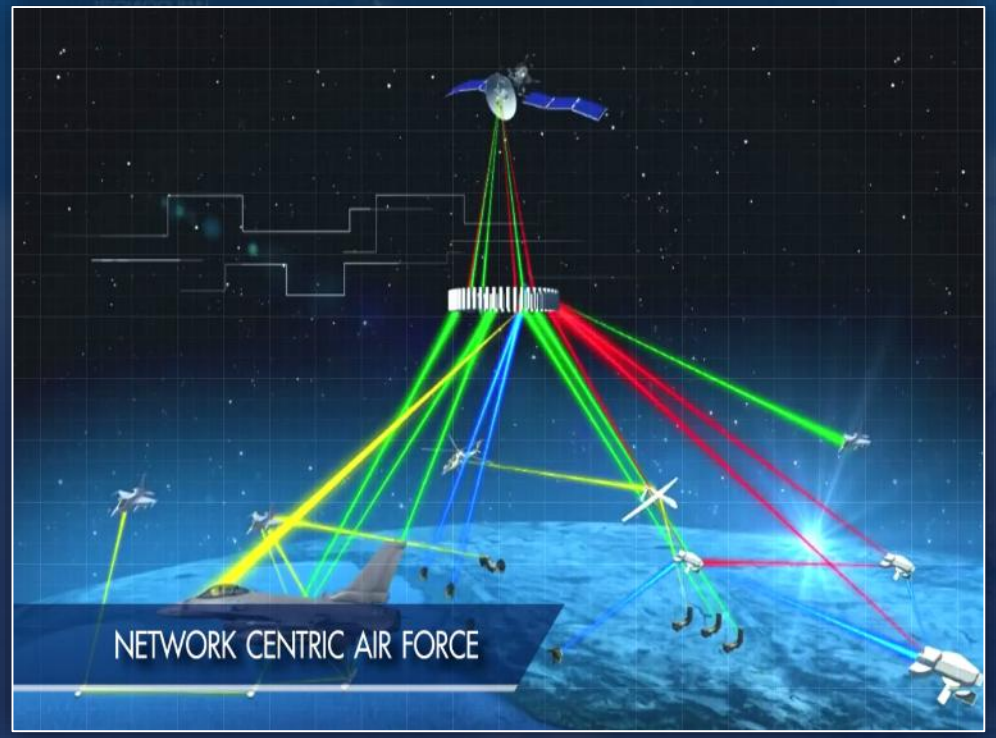
Stuxnet

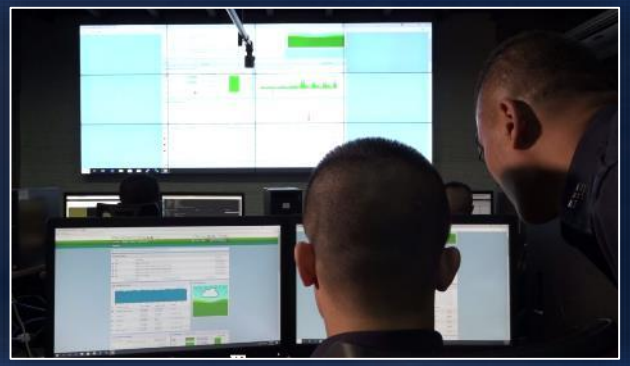
Cybercrime

Ransomware

2007 — 2011 — 2016 — 2017

หลักนิยมการปฏิบัติการไซเบอร์





RTAF Cyber CONOPS
แนวคิดการปฏิบัติการไซเบอร์ ทอ.

Cyber Defense
ป้องกัน

Confidentiality

Integrity — CIA — Availability

Objectives

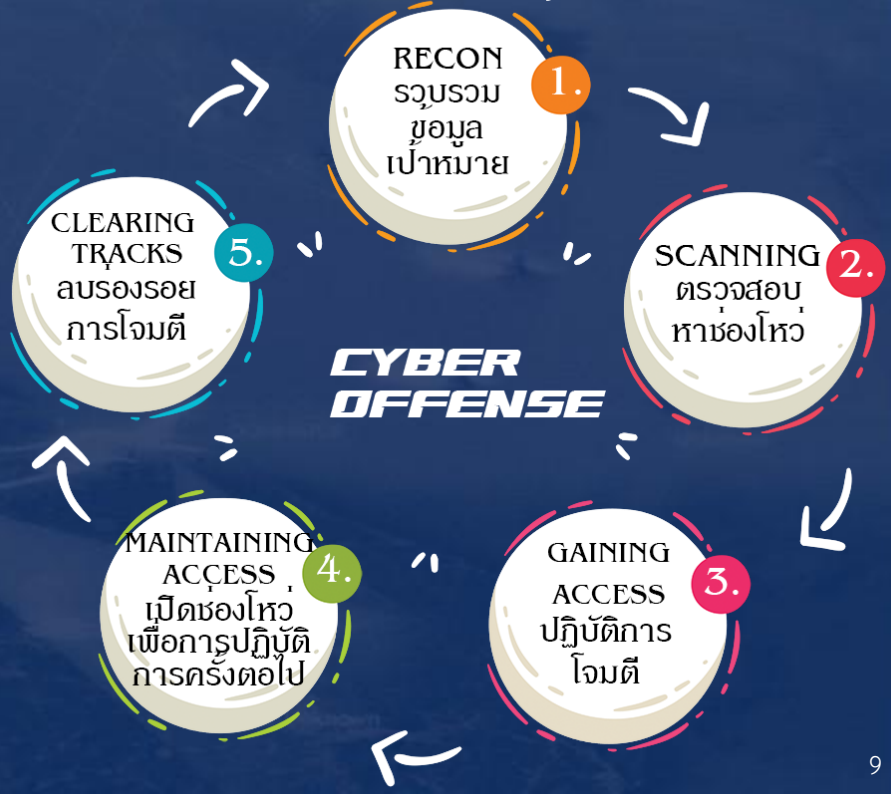
Cyber ISR
(การข่าวกรองเฝ้าตรวจและลาดตระเวนทางไซเบอร์)

Cyber Offense
ป้องปราม

Disclosure

Alteration — DAD — Destruction

Objectives



พัฒนาขีดความสามารถด้านสงครามไซเบอร์

Cyber

เป้าหมาย:

พัฒนาขีดความสามารถด้านสงครามไซเบอร์ของกองทัพอากาศ โดยพัฒนาเทคโนโลยี โครงสร้างพื้นฐาน โครงสร้างองค์กร บุคลากร และองค์ความรู้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุก และแสวงหาความร่วมมือกับหน่วยงานภายในและภายนอกประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์

สาระสำคัญ

- พัฒนาหลักนิยมการปฏิบัติการในมิติไซเบอร์ของกองทัพอากาศทั้งเชิงป้องกันและเชิงป้องปราม
- พัฒนายุทโธปกรณ์ทางไซเบอร์ (Cyber Weapon) อย่างเป็นรูปธรรมในการป้องกัน ติดตาม เฝ้าระวัง แจ้งเตือน และวิเคราะห์เหตุคุกคามทางไซเบอร์ (Cyber Incident Response)
- พัฒนาระบบรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์ของข้าศึก (Cyber Intelligence) เพื่อจัดทำบัญชีเป้าหมายทางไซเบอร์
- จัดให้มีการฝึกจำลองยุทธ์ด้านไซเบอร์ อย่างต่อเนื่อง เพื่อพัฒนาบุคลากรที่เกี่ยวข้องและนักรบไซเบอร์ (Cyber Warrior) ตลอดจนส่งเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Culture) ให้กับกำลังพล
- บูรณาการด้านการพัฒนาซอฟต์แวร์ การปฏิบัติการทางอากาศ อวกาศ และสงครามอิเล็กทรอนิกส์ เพื่อเป็นปัจจัยในการทวีกำลังด้านไซเบอร์
- แสวงหาความร่วมมือกับหน่วยงานภายในและภายนอกประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์

ขีดความสามารถ (Capability)

Personal
Support and Service

ตัวอย่าง
- AFOC
- AOC
- SOC
- ACCS
- NCOC

Cap : ระบบบัญชาการและควบคุมทางอากาศที่สามารถเชื่อมโยงเครือข่ายเป็นศูนย์กลางกับส่วนตรวจจับทั้งภาคพื้น ภาคอากาศ และภาคอวกาศ รวมทั้งสามารถควบคุมและสั่งการหน่วยปฏิบัติโดยใช้เครือข่ายเป็นศูนย์กลางอย่างมีประสิทธิภาพ

War Room
Air Operation Center

C2

Cyber

Cap : การป้องกันทางไซเบอร์ เพื่อปกป้อง คุ้มกัน ทุกองค์ประกอบของ NCO ซึ่งใช้ ICT Technology ขับเคลื่อนแบบบูรณาการและครบถ้วนทุกภาคส่วน

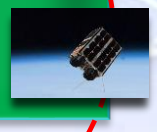
Telecommunication
Computer Network
Tactical Data Link

Decide

Network

Sense *Response*

ตัวอย่าง
-Network Infra
-TDL
-Satellite
(Future plan)



Cap : เครือข่ายทั้งภาคพื้น ภาคอากาศ และอวกาศ ที่ก่อให้เกิดการเชื่อมโยงระหว่างส่วนตรวจจับ ส่วนบัญชาการและควบคุม และหน่วยปฏิบัติแบบบูรณาการ

Personal
Support and Service

Intelligence
Surveillance
Target Acquisition
Reconnaissance
Human

Sensors

Platform
Weapon
Ground Defense

Shooters

ตัวอย่าง
-RDR Air Defense
-Erieye
-Saab EW
-UAV
-DA42 MPP
- Satellite

Cap : การตรวจการณ์ที่ครอบคลุมทั้งภาคพื้น ภาคอากาศ และภาคอวกาศ เชื่อมโยงข้อมูลเข้าสู่ระบบบัญชาการและควบคุมทางอากาศแบบบูรณาการ

Personal
Support and Service

ตัวอย่าง
- Gripen
- F-16 MLU
- F-5 UPG
- T-50TH
- A-Jet Mod
- GBAD
- Weapons
- EWS

Cap : หน่วยปฏิบัติที่มีประสิทธิภาพ มีเทคโนโลยีขั้นก้าวหน้า ความสามารถในการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง สามารถผนึกกำลังตอบโต้ภัยคุกคามได้อย่างมีประสิทธิภาพ

Personal
Support and Service

RTAF Assets

กองทัพอากาศชั้นนำในภูมิภาค
One of the Best Air Forces in ASEAN

- War fighter such as pilot , fighter controller, high skilled workforce

Human & Behavior

Support & Service

- Joint Logistics
- Logistics
- Airworthiness
- Test &training facility
- Air Base System

Cyber

- Cyber Defense
- Cyber Intelligence
- Cyber Offense

Space

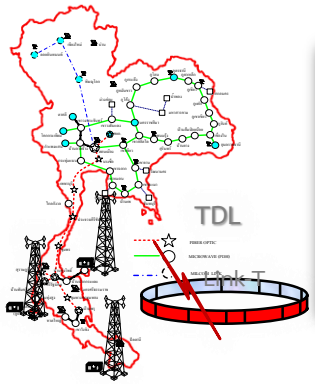
- Space Observation
- Space Surveillance
- Space Defense

- JOC
- AFOC
- AOC - SOC
- GOC
- WWR

War Room
AOC

C2

Telecommunication
Computer Network
Tactical Data Link



- ICT Mgmt
- ICT security
- Backbone Network
- Access Network
- Tactical Data Link
- Radio system

Decide

Network

Sense

Response

Intelligence
Surveillance
Target Acquisition
Reconnaissance
Human

Sensors

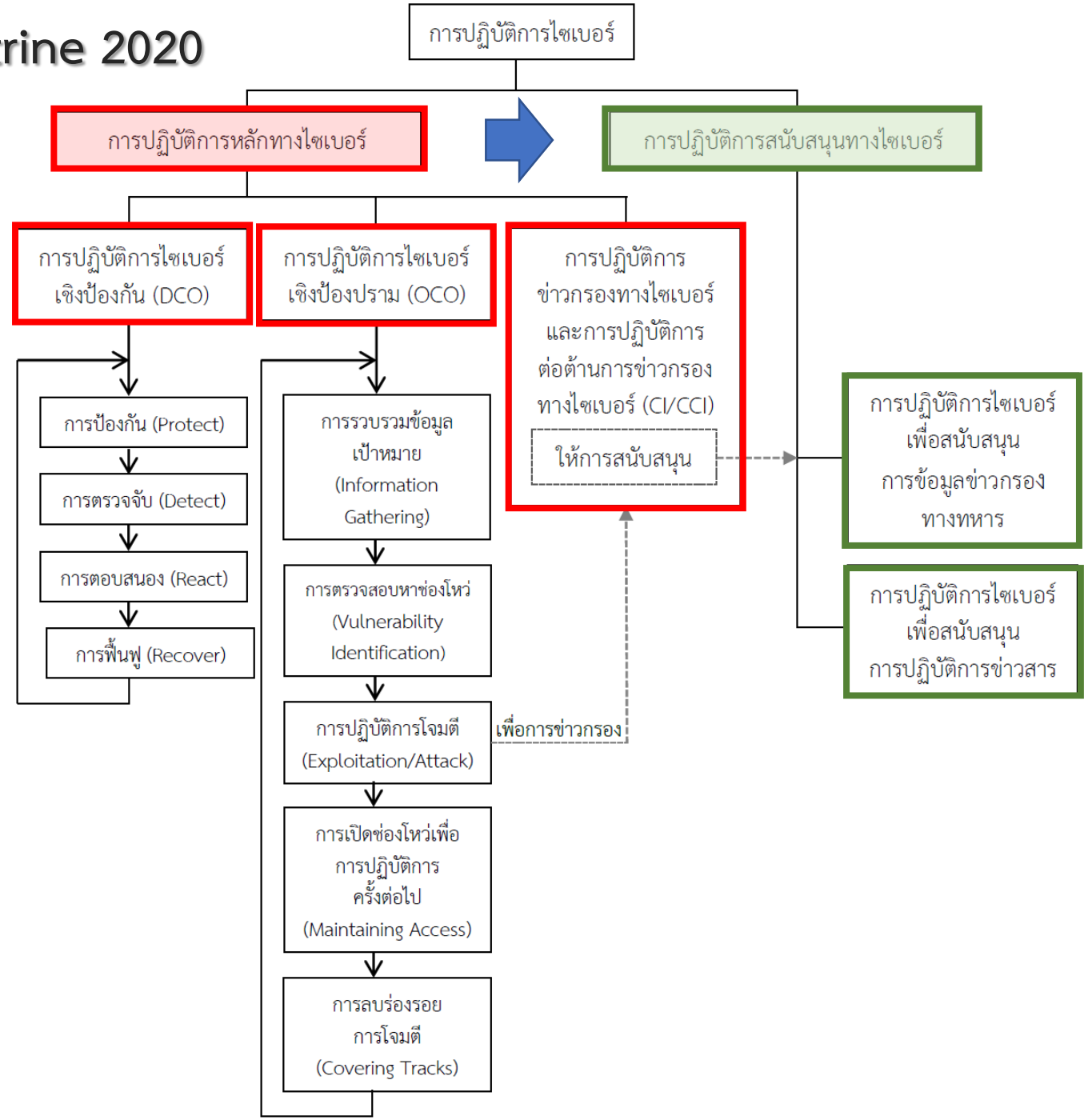
Platform
Weapon
Ground Defense

Shooters

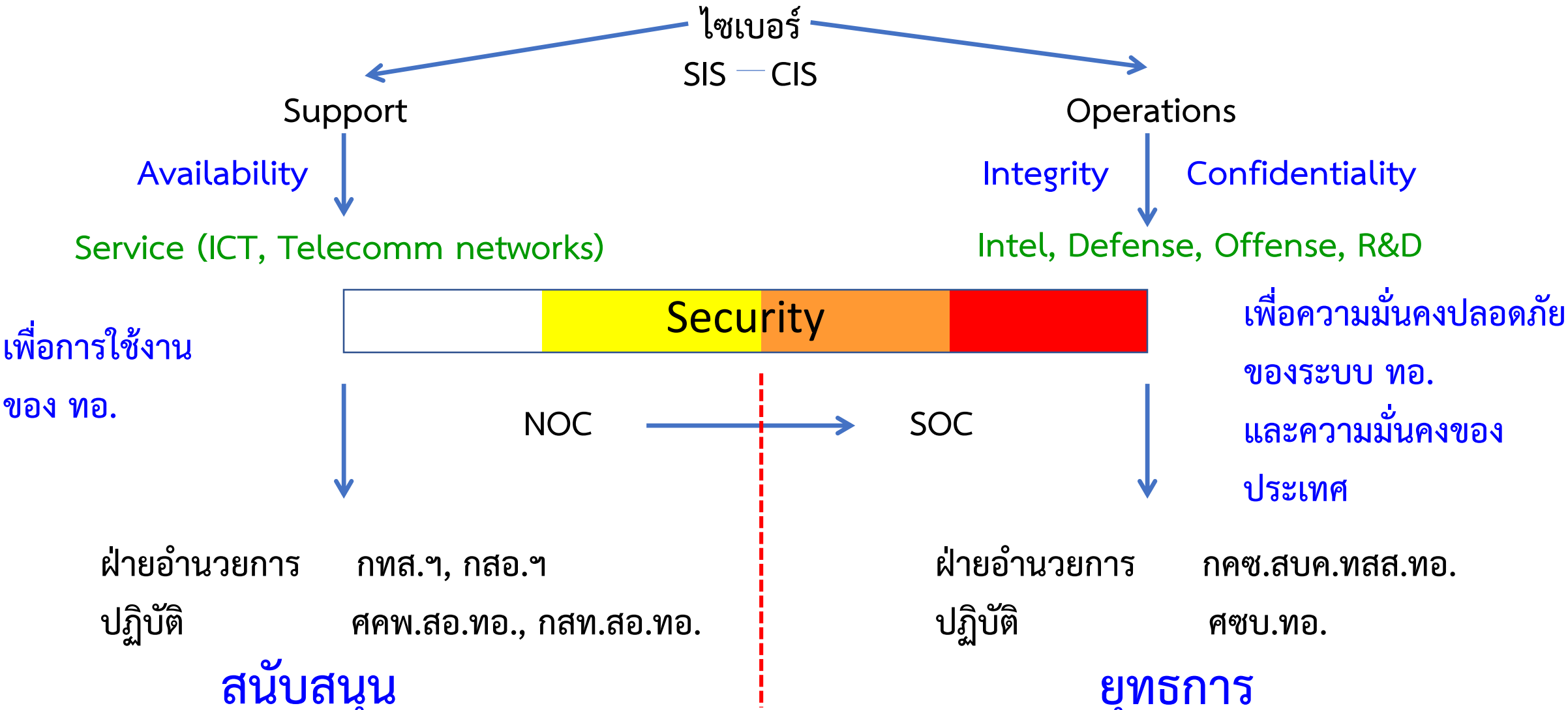
- Ground based radars
- AEW and RWR systems
- Recce/surveillance a/c
- SIGINT
- UAS
- HUMINT

- Fighter/Strike a/c
- Transport
- CSAR
- Air-to-Air armament
- Air-to Ground armament
- Air-to-Surface armament
- Operational Support System
- Electronic Warfare

Cyber Doctrine 2020



ขอบเขตการปฏิบัติงานด้านไซเบอร์ของ ทอ.



โครงสร้างและภารกิจ ศซบ.ทอ.

โครงสร้างการจัดองค์กร

กองทัพอากาศ

- สง.ปรมน.ทอ.
- สพร.ทอ.
- ศกอ.
- ศบพ.
- ศฮพ.
- สคม.ทอ.(เพื่อพลาง)
- ศูนย์สนับสนุนการถวายบิน ๙๐๔ (เพื่อพลาง)

ส่วนบัญชาการ

กพ.ทอ. | ขว.ทอ. | ยก.ทอ. | กบ.ทอ. | กร.ทอ. | ทสส.ทอ. | สปช.ทอ. | ศซบ.ทอ.

สลก.ทอ. | สบ.ทอ. | กง.ทอ. | จร.ทอ. | สนภ.ทอ. | สตน.ทอ. | สธน.ทอ. | สบน.ทอ.

ส่วนกำลังรบ

๑๒ กองบิน... | รร.การบิน | คปอ. | อย. | ศปอว.ทอ.

ส่วนส่งกำลังบำรุง

ชอ. | สอ.ทอ. | สพ.ทอ. | พอ. | พธ.ทอ. | ชย.ทอ. | ขส.ทอ. | ศซว.ทอ.

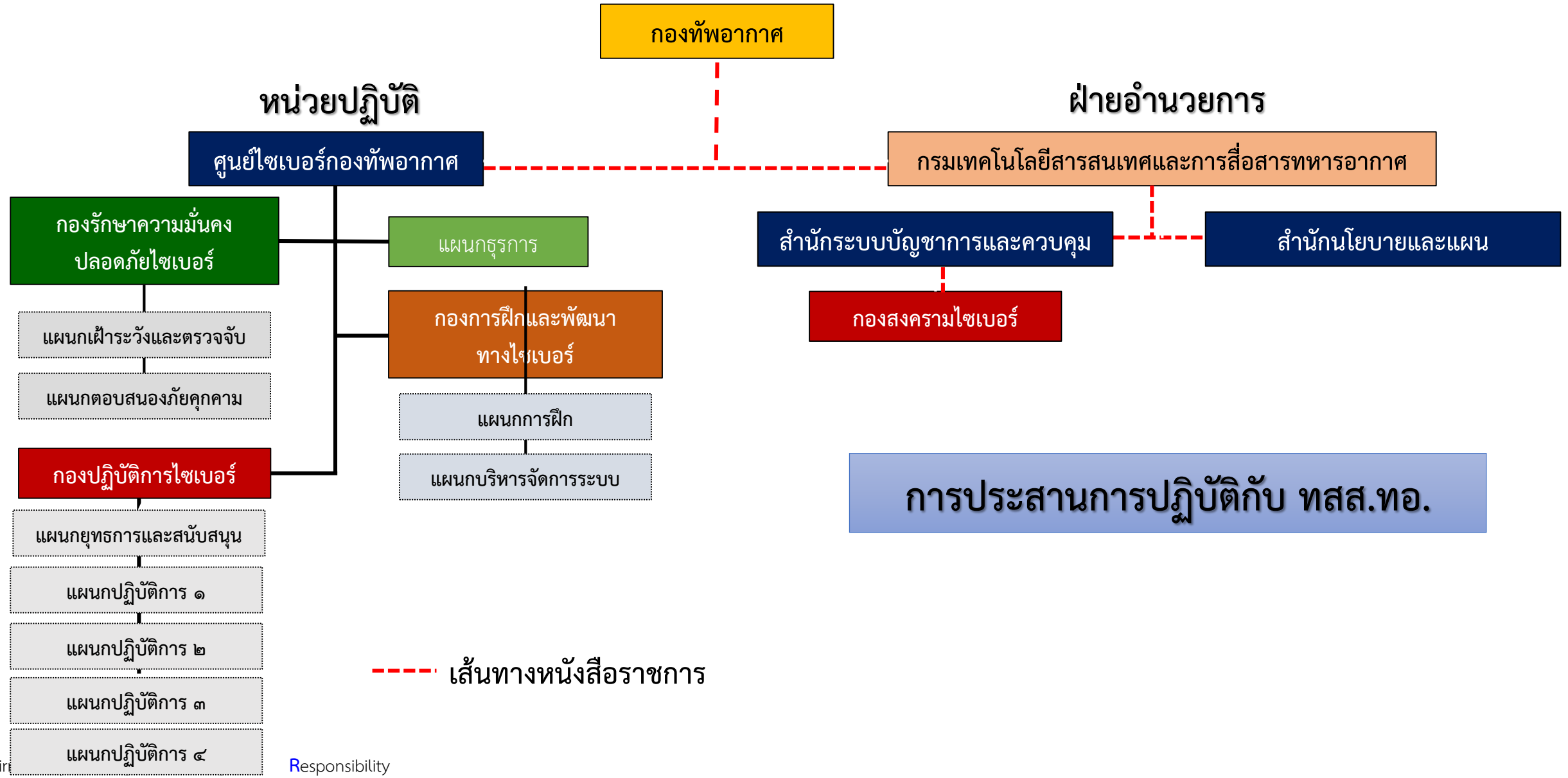
ส่วนการศึกษา

ยศ.ทอ. | รร.นนก.

ส่วนกิจการพิเศษ

สก.ทอ. | ศวอ.ทอ. | สวบ.ทอ. | สน.ผบ.ดม.

โครงสร้างและภารกิจ ศซบ.ทอ. (ปัจจุบัน)



โครงสร้างการใช้กำลัง ทอ.

ตามแผนเฉลิมอากาศฉบับปรับปรุง ปี ๖๓

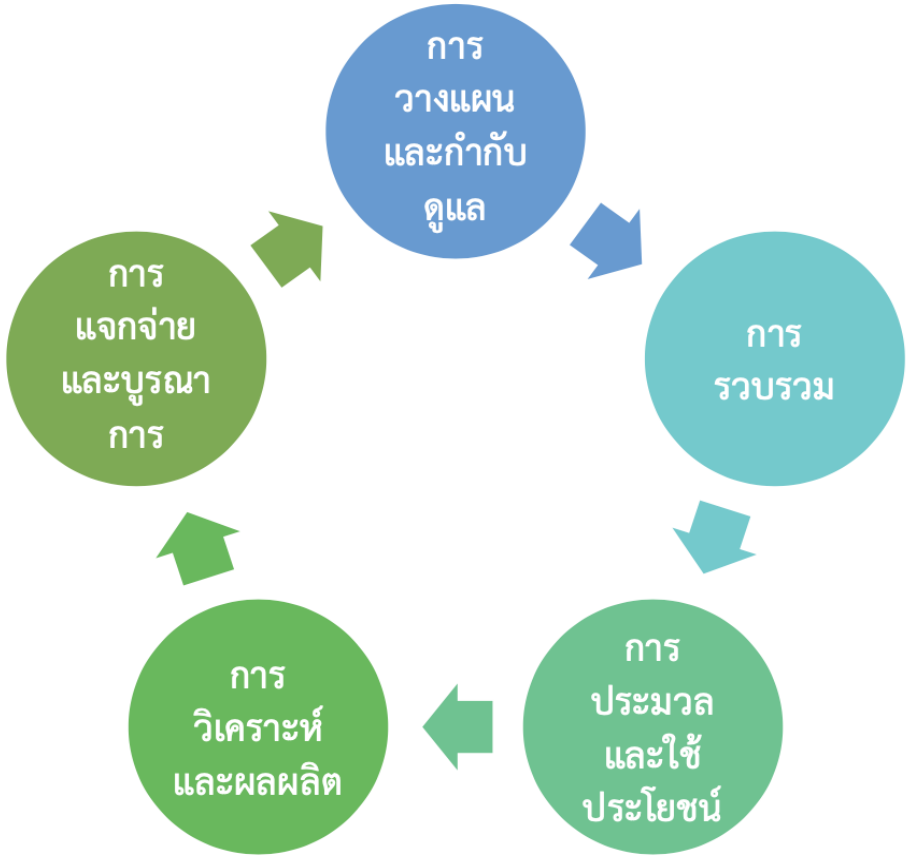
*** เฉพาะในสถานการณ์สู้รบ หรือสงคราม

ความพร้อมการปฏิบัติภารกิจ

การปฏิบัติการไซเบอร์เชิงป้องกัน

- การรู้จักตัวเอง
- การป้องกัน
- การตรวจจับ
- การตอบสนอง
- การฟื้นฟู

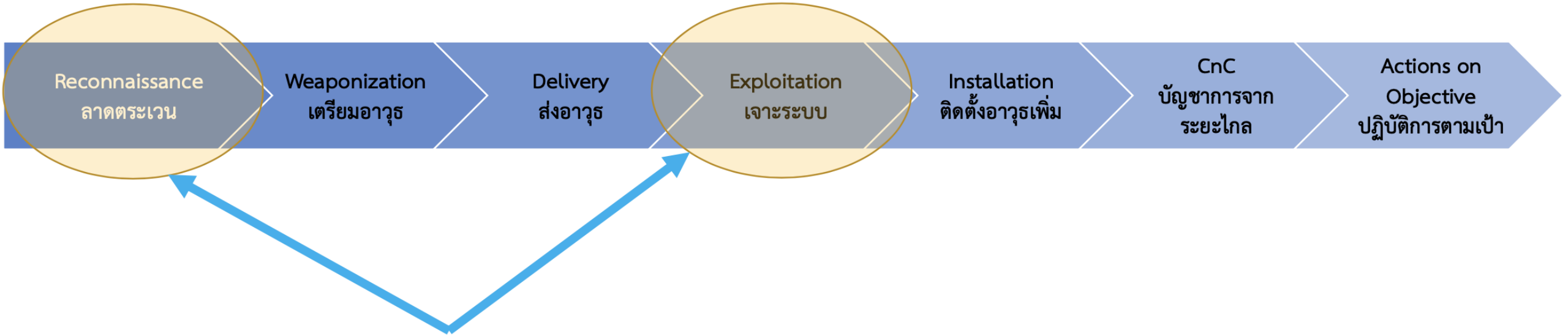
การข่าวกรองเฝ้าตรวจและลาดตระเวนทางไซเบอร์



การปฏิบัติการไซเบอร์เชิงป้องปราม

- การลาดตระเวน
- การพัฒนา/จัดหาอาวุธ
- การส่งอาวุธ
- การแสวงหาประโยชน์
- การติดตั้งอาวุธ
- การบัญชาการและควบคุม
- การปฏิบัติการ

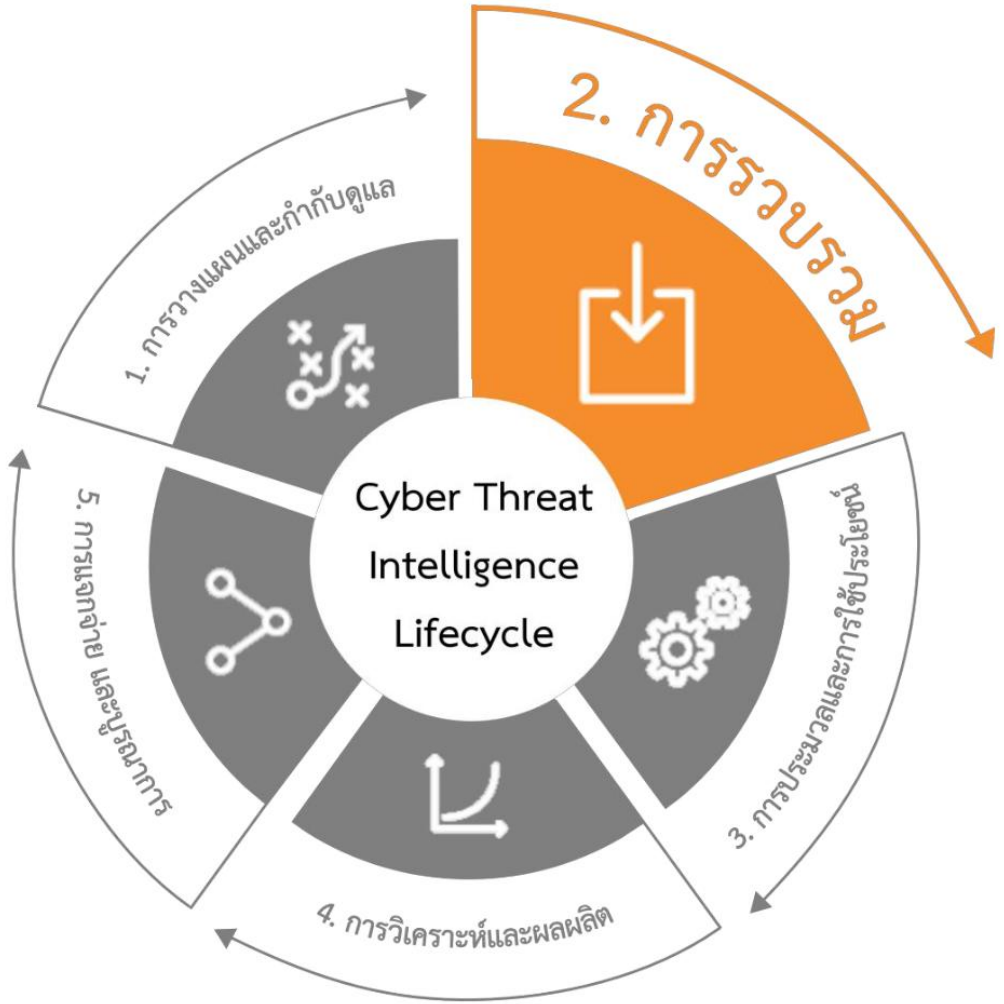
ความพร้อมการปฏิบัติภารกิจ : การปฏิบัติการทางไซเบอร์เชิงป้องปราม



ความสามารถในปัจจุบัน

ตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์เชิงเทคนิค (Pen-test)

ความพร้อมการปฏิบัติภารกิจ : การข่าวกรองเฝ้าตรวจและลาดตระเวณทางไซเบอร์ ด้านเครื่องมือ



External Source
- HUMINT ✗
- OSINT ✓
- Social Listening Tools ✗

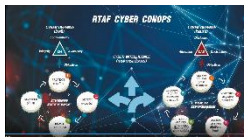
Technical Source
- CTI Feed ✗
- Vulnerability Database ✓

Internal Source
- IDS ✓
- Firewall ✓
- SIEM ✓
- EDR ✓

แนวทางการพัฒนาด้านไซเบอร์
ในยุทธศาสตร์ ทอ. ๒๐ ปี

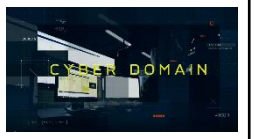
Cyber Domain Road Map

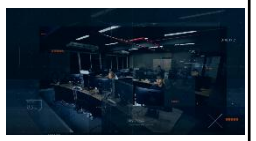
ทิศทางการพัฒนามิติไซเบอร์ (Cyber Domain)

Domain	2561-2565	2566-2570	2571-2575	2576-2580
Cyber       	ด้านนโยบาย ⌖ ทบทวนหลักนิยมและพัฒนาแนวความคิดในการปฏิบัติภารกิจด้านไซเบอร์ของ ทอ. ⌖ กำหนดขอบเขตการปฏิบัติภารกิจด้านไซเบอร์ และกำหนดหน่วยรับผิดชอบ ⌖ จัดตั้งหน่วยงานเพื่อดำเนินงานด้านไซเบอร์ ⌖ ปรับปรุงและพัฒนาโครงสร้างพื้นฐานและสิ่งอำนวยความสะดวกด้านไซเบอร์ ⌖ พัฒนาและดำเนินการจัดทำแผนเผชิญเหตุด้านไซเบอร์ (Incident response plan) ⌖ ริเริ่มสนับสนุนชุดปฏิบัติการไซเบอร์เพื่อแก้ไขสถานการณ์วิกฤตตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านกำลังพล ⌖ กำหนดสมรรถนะหลักและทักษะของกำลังพล/นักรบไซเบอร์ ⌖ กำหนดและจัดตั้งสายวิทยาการไซเบอร์ ⌖ จัดตั้ง Cyber Protection Team (CPT) ⌖ เสริมสร้างความตระหนักรู้ด้านไซเบอร์ให้กำลังพล ทอ. ⌖ ริเริ่มการพัฒนาขีดความสามารถบุคลากรด้านสงครามอิเล็กทรอนิกส์ให้รองรับในทุก Platform หลักของ ทอ.	ด้านนโยบาย ⌖ ริเริ่มและบูรณาการการปฏิบัติงานด้านไซเบอร์เข้ากับการฝึกตามความเหมาะสม ⌖ ประเมินผลหน่วยงานด้านไซเบอร์ และเสนอแนะแนวทางการพัฒนาหน่วยงาน ⌖ บูรณาการขีดความสามารถด้านไซเบอร์และสงครามอิเล็กทรอนิกส์ ⌖ กำหนดแนวทางการปฏิบัติการร่วมทางไซเบอร์ – อวกาศ ⌖ สนับสนุนชุดปฏิบัติการไซเบอร์เพื่อแก้ไขสถานการณ์วิกฤตตามพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านกำลังพล ⌖ สรรหากำลังพล/นักรบไซเบอร์ ซึ่งมีสมรรถนะหลักและทักษะตามที่กำหนด ทั้งในเชิงปริมาณและคุณภาพ ⌖ ริเริ่มจัดตั้งศูนย์ฝึกอบรมด้านไซเบอร์ของ ทอ. ⌖ ส่งเสริมการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ ⌖ พัฒนาการปฏิบัติงานของ Cyber Protection Team (CPT) และเพิ่มผู้เชี่ยวชาญอย่างต่อเนื่อง ⌖ ขยายขีดความสามารถชุดปฏิบัติการด้านสงครามอิเล็กทรอนิกส์ให้รองรับในทุก Platform หลักของ ทอ.	ด้านนโยบาย ⌖ ทบทวนหลักนิยมและพัฒนาแนวความคิดในการปฏิบัติภารกิจด้านไซเบอร์ของ ทอ. ⌖ ทบทวนและประเมินผลหน่วยงานด้านไซเบอร์ และเสนอแนะแนวทางการพัฒนาหน่วยงาน ⌖ ยกระดับขีดความสามารถด้านไซเบอร์และสงครามอิเล็กทรอนิกส์ ⌖ ยกระดับการปฏิบัติการร่วมทางไซเบอร์ – อวกาศ ⌖ ยกระดับการสนับสนุนชุดปฏิบัติการไซเบอร์เพื่อแก้ไขสถานการณ์วิกฤตตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเต็มรูปแบบ ด้านกำลังพล ⌖ สิ่งเสริมการเพิ่มขีดความสามารถของกำลังพล/นักรบไซเบอร์ และ Cyber Protection Team (CPT) ⌖ ยกระดับการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ ⌖ ยกระดับปฏิบัติงานของ Cyber Protection Team (CPT) และเพิ่มผู้เชี่ยวชาญอย่างต่อเนื่อง ⌖ ยกระดับขีดความสามารถชุดปฏิบัติการด้านสงครามอิเล็กทรอนิกส์ให้รองรับในทุก Platform หลักของ ทอ.	ด้านนโยบาย ⌖ ดำเนินงานด้านไซเบอร์อย่างเต็มรูปแบบ ดำรงขีดความสามารถเพื่อสนับสนุนการปฏิบัติการทางอากาศได้ครอบคลุมทุกมิติ ⌖ ทบทวนและประเมินผลหน่วยงานด้านไซเบอร์ และเสนอแนะแนวทางการพัฒนาหน่วยงาน ⌖ ดำรงขีดความสามารถด้านไซเบอร์และสงครามอิเล็กทรอนิกส์ ⌖ ดำรงการปฏิบัติการร่วมทางไซเบอร์ – อวกาศ ด้านกำลังพล ⌖ บรรจุนักรบไซเบอร์ในการปฏิบัติงานด้านการรบ ⌖ ดำรงวัฒนธรรมความปลอดภัยไซเบอร์ ⌖ ดำรงการปฏิบัติงานของ Cyber Protection Team (CPT) และเพิ่มผู้เชี่ยวชาญอย่างต่อเนื่อง ⌖ ดำรงขีดความสามารถชุดปฏิบัติการด้านสงครามอิเล็กทรอนิกส์ให้รองรับในทุก Platform หลักของ ทอ.

Cyber Domain Road Map

Domain	ทิศทางการพัฒนามิติไซเบอร์ (Cyber Domain)			
	2561-2565	2566-2570	2571-2575	2576-2580
Cyber	ด้านเทคโนโลยีการวิจัยและพัฒนา ⌖ สนับสนุนงานวิศวกรรมซอฟท์แวร์ และการปฏิบัติการทางอวกาศให้มีมาตรฐานและมีความมั่นคงปลอดภัย ⌖ ริเริ่มการพัฒนาระบบการฝึกจำลองยุทธ์ด้านไซเบอร์ ⌖ ริเริ่มการนำ AI มาใช้ในการปฏิบัติการด้านไซเบอร์ ⌖ ริเริ่มระบบรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์ของข้าศึก (Cyber Intelligence) ⌖ ริเริ่มระบบเฝ้าระวังและตรวจจับภัยคุกคามด้านไซเบอร์เพื่อสนับสนุนปฏิบัติการทางอวกาศ ด้านความร่วมมือ ⌖ ริเริ่มการทดสอบด้านไซเบอร์ และการฝึกร่วม (Bilateral exercise) กับ ทอ.มิตรประเทศ ⌖ ริเริ่มการฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสม (Multi-lateral) กับ มิตรประเทศ ⌖ ริเริ่มความร่วมมือด้านอุตสาหกรรมภายในประเทศ	ด้านเทคโนโลยีการวิจัยและพัฒนา ⌖ วิจัยและพัฒนาเกี่ยวกับ Internet of things, Big data, Blockchain, 5G and AI หรือเทคโนโลยีขั้นสูงอื่น ๆ ที่มีศักยภาพในอนาคต ⌖ ริเริ่มการพัฒนายุทโธปกรณ์ทางไซเบอร์ (Cyber Weapon) ⌖ พัฒนาระบบรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์ของข้าศึก (Cyber Intelligence) ⌖ พัฒนาระบบเฝ้าระวังและตรวจจับภัยคุกคามด้านไซเบอร์เพื่อสนับสนุนปฏิบัติการทางอวกาศ ⌖ ยกระดับวิศวกรรมซอฟท์แวร์ ให้มีมาตรฐานและมีความมั่นคงปลอดภัย ⌖ ใช้เทคโนโลยีการสื่อสารดาวเทียมเพื่อสนับสนุนปฏิบัติการด้านไซเบอร์ ⌖ ริเริ่มการจัดตั้ง EW Lab เพื่อพัฒนาและทดสอบ EW Library ด้านความร่วมมือ ⌖ ทดสอบด้านไซเบอร์ และการฝึกร่วม (Bilateral exercise) กับ ทอ.มิตรประเทศ ⌖ ฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสม (Multi-lateral) กับ มิตรประเทศ ⌖ ยกระดับความร่วมมือด้านอุตสาหกรรมภายในประเทศ	ด้านเทคโนโลยีการวิจัยและพัฒนา ⌖ วิจัยและพัฒนาเกี่ยวกับ Quantum computing และ Space/GPS Hacking prevention ⌖ พัฒนายุทโธปกรณ์ทางไซเบอร์ (Cyber Weapon) ระบบการฝึกจำลองยุทธ์ และระบบรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์ อย่างต่อเนื่อง ⌖ สามารถพัฒนาซอฟท์แวร์เพื่อสนับสนุนการปฏิบัติการทางอากาศ C2, OFP, Space และ Cyber ได้เอง ⌖ พัฒนาระบบเฝ้าระวังและตรวจจับภัยคุกคามด้านไซเบอร์เพื่อสนับสนุนปฏิบัติการทางอวกาศให้ครอบคลุม ⌖ พัฒนา EW Library (RWR/Jammer) ให้รองรับในทุก Platform หลักของ ทอ. ด้านความร่วมมือ ⌖ ยกระดับการทดสอบด้านไซเบอร์ และการฝึกร่วม (Bilateral exercise) กับ ทอ.มิตรประเทศ ⌖ ยกระดับการฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสม (Multi-lateral) กับ มิตรประเทศ ⌖ ยกระดับความร่วมมือด้านอุตสาหกรรมภายในประเทศ	ด้านเทคโนโลยีการวิจัยและพัฒนา ⌖ เริ่มใช้งาน AI และ Quantum computing ใน ทอ. ⌖ ระบบต่าง ๆ ใน ทอ. มีความแข็งแกร่ง (Cyber Resilience) ⌖ ดำรงการพัฒนายุทโธปกรณ์ทางไซเบอร์ (Cyber Weapon) ระบบการฝึกจำลองยุทธ์ และระบบรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์ อย่างต่อเนื่อง ⌖ ดำเนินการใช้งาน Big data และ Blockchain เมื่อเหมาะสม ⌖ จัดตั้งฝูงบิน (อากาศยาน และ UAV) ทดสอบและประเมินคุณภาพระบบ OFP ที่ ทอ.พัฒนาขึ้น ด้านความร่วมมือ ⌖ ดำรงการทดสอบด้านไซเบอร์ และการฝึกร่วม (Bilateral exercise) กับ ทอ.มิตรประเทศ ⌖ ดำรงการฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสม (Multi-lateral) กับมิตรประเทศ ⌖ ขยายขอบเขตความร่วมมือด้านอุตสาหกรรมภายในประเทศ



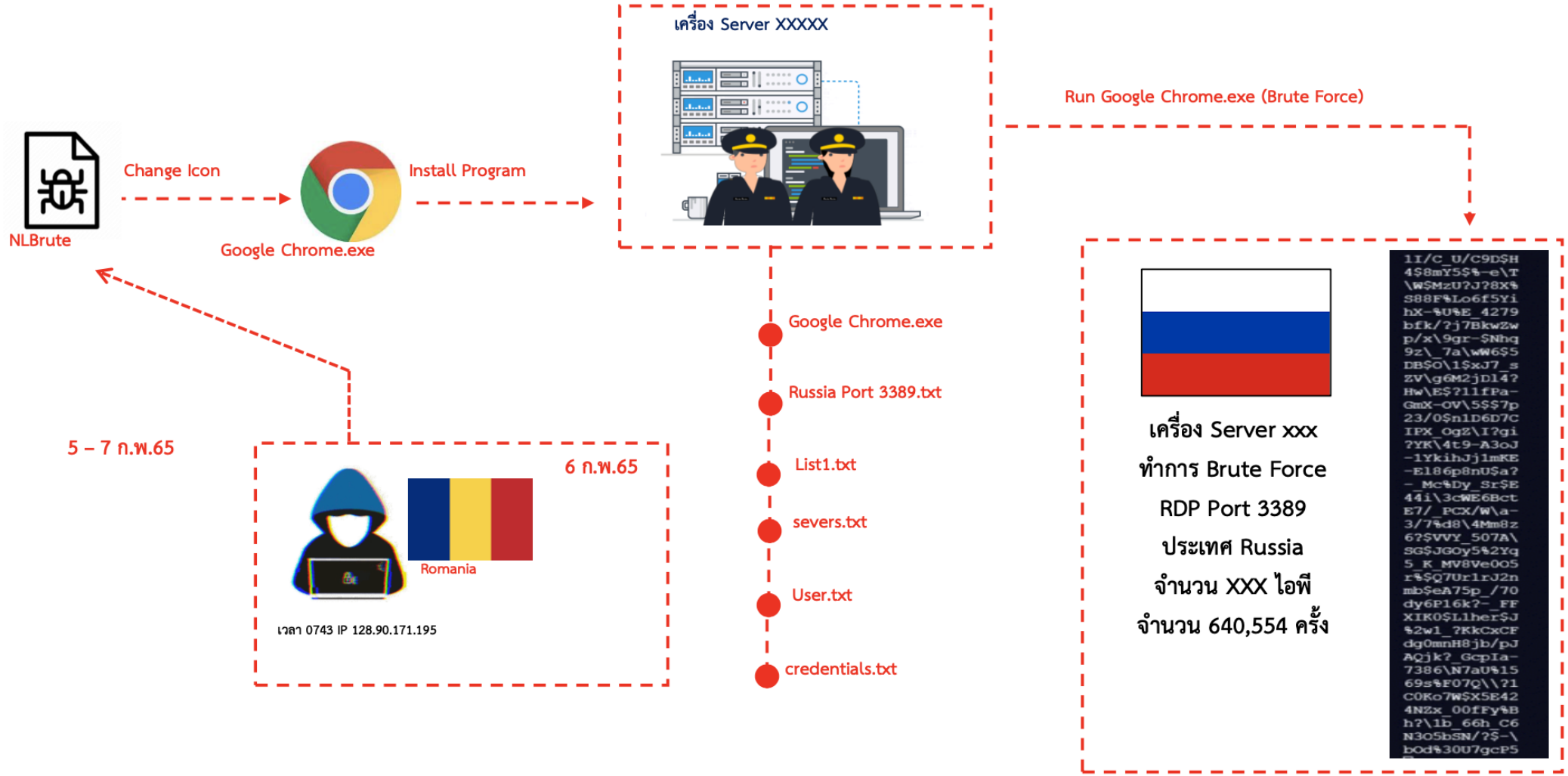


การดำเนินงานด้านไซเบอร์ที่ผ่านมา

ผลการปฏิบัติภารกิจ

ตอบสนองภัยคุกคามด้านไซเบอร์จากกรณีเหตุการณ์ถูกโจมตีจากมัลแวร์

ผลการปฏิบัติภารกิจ



ผลการปฏิบัติภารกิจ

แจ้งเตือนใน email ทอ./Facebook

กลุ่มแฮกเกอร์ Dark Pink

ใช้เทคนิคจู่โจมขั้นสูงพุ่งเป้าไปที่รัฐบาล และกองทัพในภูมิภาคอาเซียน

Group-IB บริษัทผู้ให้บริการรักษาความปลอดภัยไซเบอร์ เปิดเผยว่าค้นพบแฮกเกอร์กลุ่มใหม่ใช้ชื่อว่า Dark Pink โดยมีเป้าหมายโจมตีที่หน่วยงานภาครัฐ และกองทัพในภูมิภาคอาเซียนเป็นหลัก โดยกลุ่ม Dark Pink ได้ใช้เทคนิคที่ซับซ้อน ชุดเครื่องมือที่สร้างขึ้นโดยเฉพาะ กลวิธีเทคนิค และขั้นตอนที่ซับซ้อน ซึ่งมีส่วนสำคัญในการโจมตีที่ประสบความสำเร็จในช่วง 7 เดือนที่ผ่านมา

โดยในเดือนธันวาคม 2565 กลุ่ม Dark Pink ได้ทำการเจาะระบบป้องกันทางไซเบอร์ของ 6 องค์กร ในอาเซียนทั้งในกัมพูชา อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และเวียดนาม ซึ่งการโจมตีที่ประสบความสำเร็จครั้งแรก เกิดขึ้นในเดือนมิถุนายน 2565 โดยการเจาะเข้าถึงเครือข่ายของกลุ่มศาสนาในเวียดนาม และจู่โจมองค์กรในเวียดนามอีกครั้ง ในช่วงเดือนสิงหาคม และในช่วง 4 เดือนสุดท้ายของปี กลุ่ม Dark Pink ทำการเจาะระบบมากขึ้น โดยโจมตีหน่วยงานของกองทัพฟิลิปปินส์ในเดือนกันยายน สาขาการทหารของมาเลเซียในเดือนตุลาคม ตามด้วยองค์กรของรัฐในกัมพูชา และอินโดนีเซียในเดือนพฤศจิกายนและธันวาคม ตามลำดับ แต่ยังไม่มีข้อมูลการโจมตีองค์กรในประเทศไทยแต่อย่างใด

คำแนะนำ

ขอแนะนำให้ข้าราชการ และผู้ดูแลระบบสารสนเทศ นขต.ทอ. ปฏิบัติตามระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.2563 เพื่อเป็นการป้องกันการโจมตีที่อาจเกิดขึ้น

RTAF Security Awareness

แหล่งที่มา :Group-IB, Entechreview

แฮกเกอร์ใช้ Google Ads

โฆษณาเว็บแฝงมัลแวร์ไว้บนสุดของผลการค้นหา

พบว่าแฮกเกอร์มีการใช้ Google Ads เพื่อแสดงผลเว็บไซต์หลอกให้ดาวน์โหลดโปรแกรมฟรีซึ่งได้แก่ 7-Zip, Blender 3D, Capcut, CCleaner, Notepad++, OBS, Rufus, VirtualBox, VLC, Media Player, WinRAR, และ Putty ซึ่งทุกไฟล์ถูก Virus Total ตรวจพบว่าอันตรายทั้งสิ้น หากผู้ใช้ดาวน์โหลดและติดตั้งโปรแกรม ตัวโปรแกรมที่ดาวน์โหลดไปนี้จะมีมัลแวร์ติดไปด้วย ซึ่งแฮกเกอร์จะใช้ประโยชน์จากมัลแวร์นี้ทำการโจมตีจากระยะไกล อาจขโมยข้อมูลที่สำคัญ อย่างรหัสผ่าน และบัตรเครดิตได้ และพบว่ามีโดเมนอย่างน้อย 70 โดเมนที่หลอกให้ดาวน์โหลดมัลแวร์บน Google Ads

ล่าสุดมีผู้โดนโจมตีด้วยวิธีนี้แล้ว ก็คือ Alex ในวงการ Crypto ทำการติดตั้งโปรแกรม Open Broadcaster Software (OBS) มาจากเว็บไซต์ปลอมที่ขึ้นอยู่ในรูปแบบโฆษณาของผลการค้นหาบน Google ทำให้ถูกขโมยบัญชี Twitter, ประวัติการเข้าเว็บไซต์ของ Browser, ข้อมูลรหัสผ่านที่เก็บไว้บน Browser, Cookies, Discord Tokens และกระเป๋าเงิน cryptocerrency

คำแนะนำ

เพื่อเป็นการป้องกัน ก่อนจะคลิกลิงก์ดาวน์โหลดโปรแกรมควรตรวจสอบและเช็คให้มั่นใจเสียก่อนว่าเป็นลิงก์ที่ถูกต้องและน่าเชื่อถือหรือไม่
และควรใช้ ad-blocker เพื่อเป็นการเสริมการป้องกันอีกชั้นหนึ่ง

RTAF Security Awareness

แหล่งที่มา : bleepingcomputer, beartai

เตือนภัยข่าวปลอม !!!

พบข่าวปลอมอ้างเป็นกรมสวัสดิการทหารอากาศ แจกข้าวสารหอมมะลิแก่ข้าราชการ อย่าคลิก! อย่าแชร์! ทำให้ถูกหลอกโจรกรรมข้อมูลส่วนตัว โดน SMS ดูดเงินโทรศัพท์ และตกเป็นเหยื่อของผู้ไม่หวังดีได้

ข้อควรระวัง

- เว็บไซต์จากแหล่งที่มาไม่น่าเชื่อถือ
- ใช้คำพูดหลอกล่อให้สนใจ
- ไม่คลิกลิงก์ที่น่าสงสัย
- ไม่กรอกข้อมูลสำคัญถ้าไม่แน่ใจว่าปลอดภัย

RTAF Security Awareness

ผลการปฏิบัติภารกิจ

ตรวจสอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์เชิงเทคนิคให้กับส่วนกำลังรบ

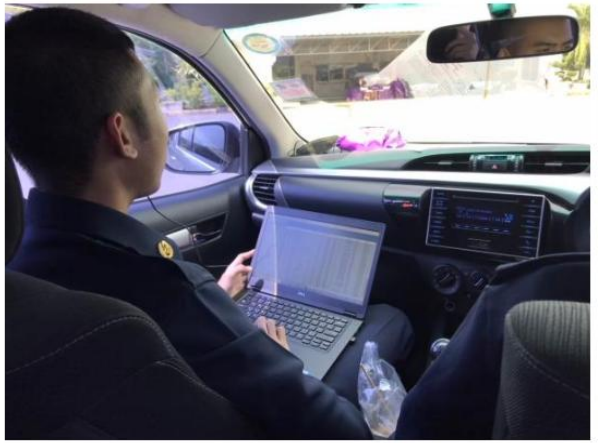
ผลการปฏิบัติภารกิจ

ตรวจสอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์เชิงเทคนิค เพื่อตอบสนองนโยบาย ผบ.ทอ.



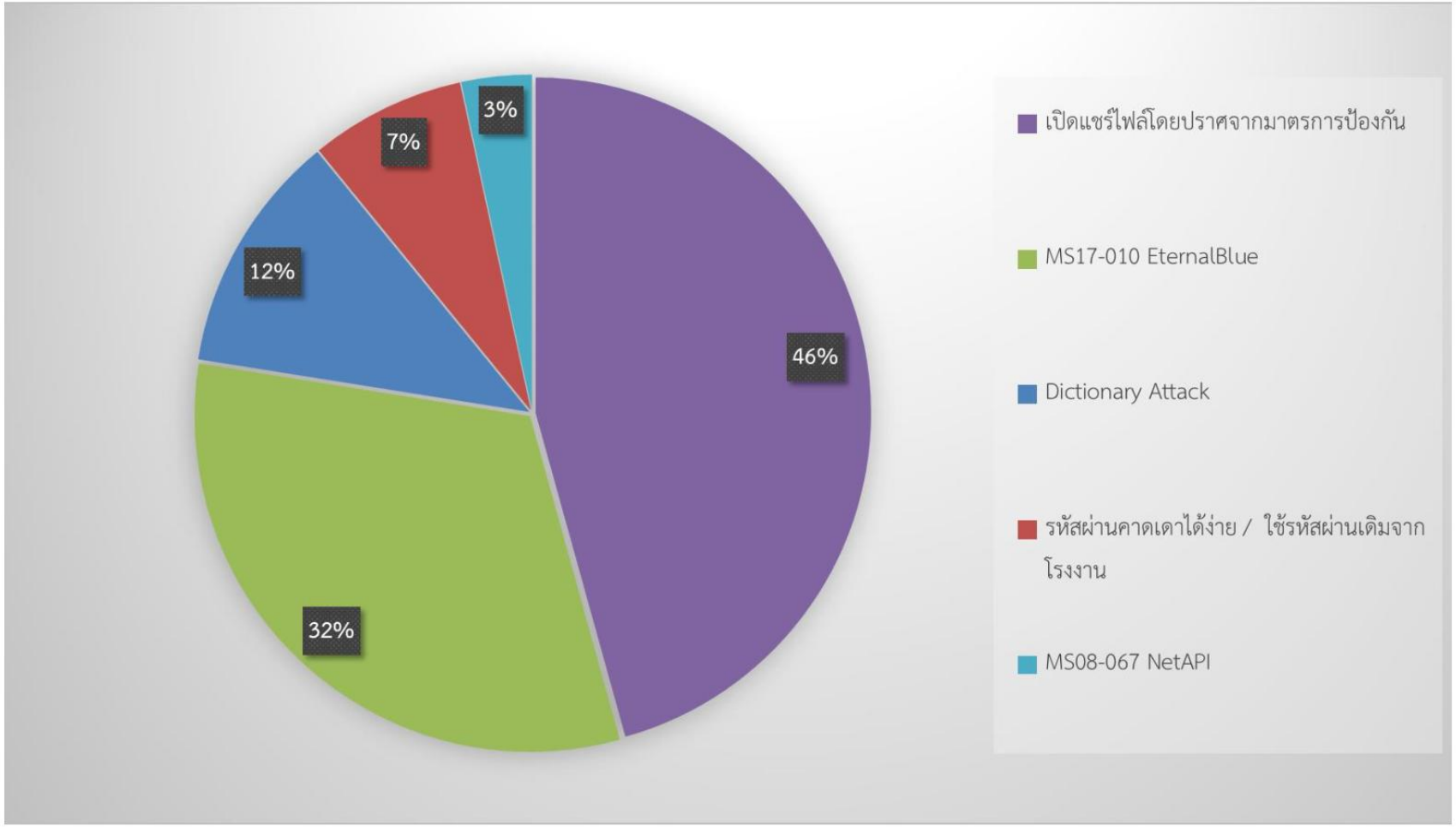






ผลการปฏิบัติภารกิจ

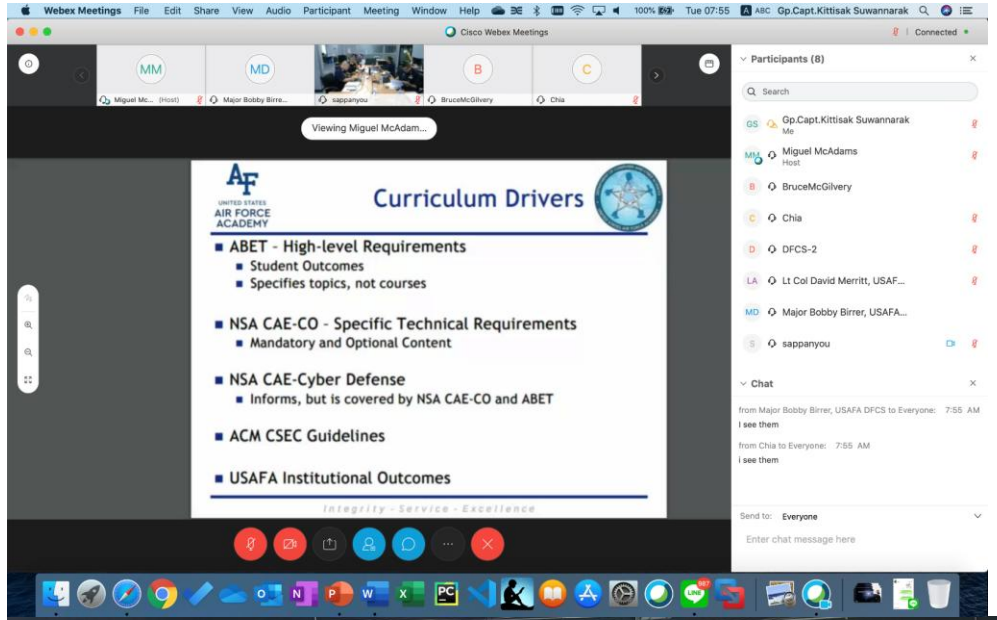
ตรวจสอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์เชิงเทคนิคให้กับส่วนกำลังรบ

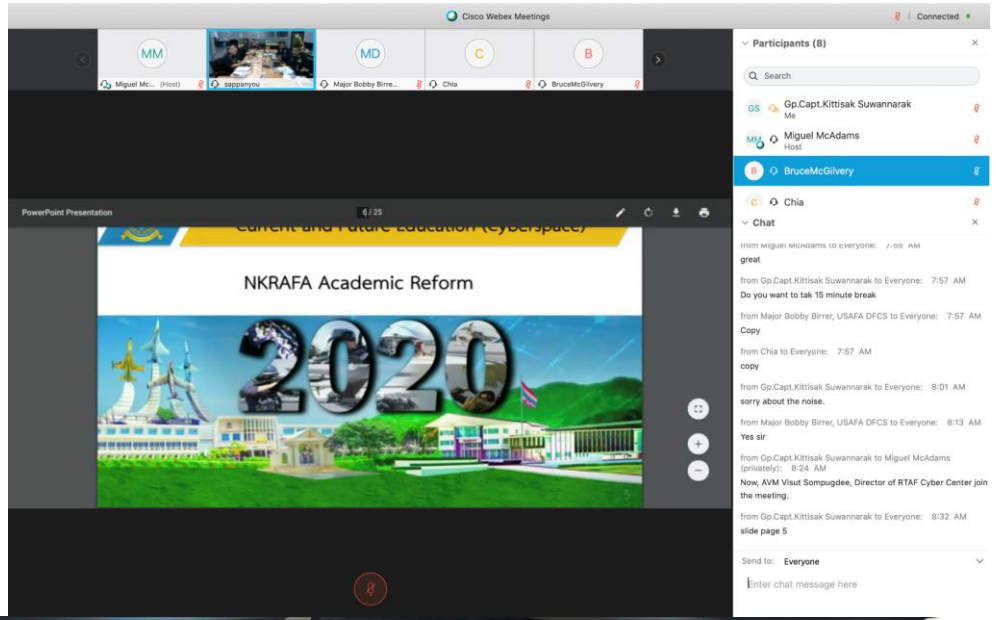


การประชุม Cyber SMEE

***จัดประชุมแล้ว แต่ไม่มีงบประมาณจัดสรรให้ ศซบ.

NKRAFA-USAFA-PACAF-WAANG





Airmanship Integrity and allegiance Responsibility

ผลการปฏิบัติภารกิจ : อื่นๆ

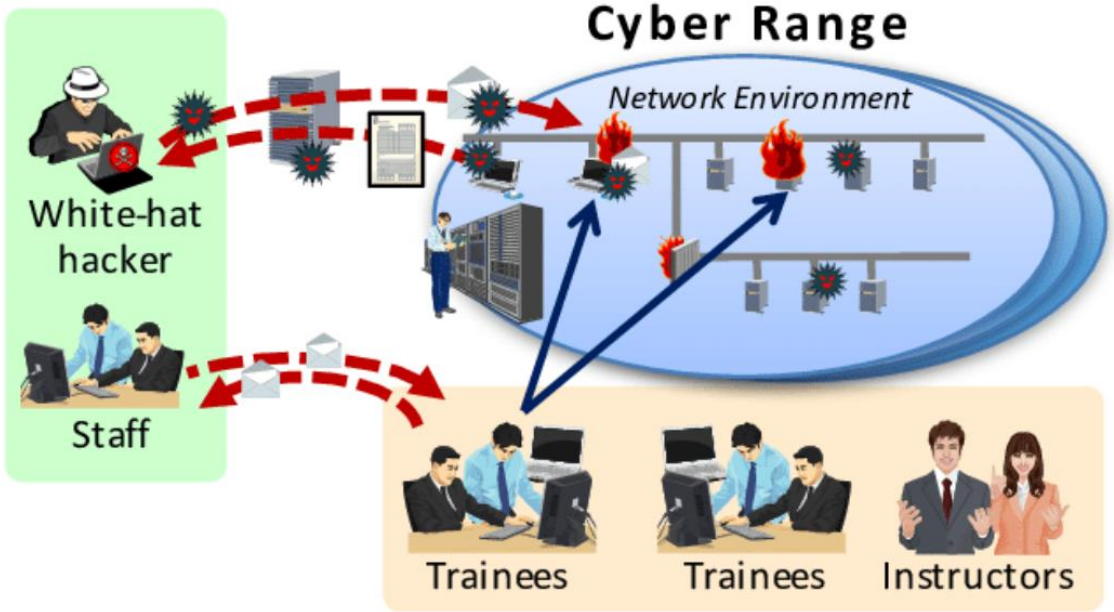
การฝึกด้านไซเบอร์ ในการฝึกร่วม/ผสม Cobra Gold

- เข้าร่วมการฝึก Cyber FTX

แผนงานขับเคลื่อน และพัฒนาหน่วยตามนโยบาย ผบ.ทอ.

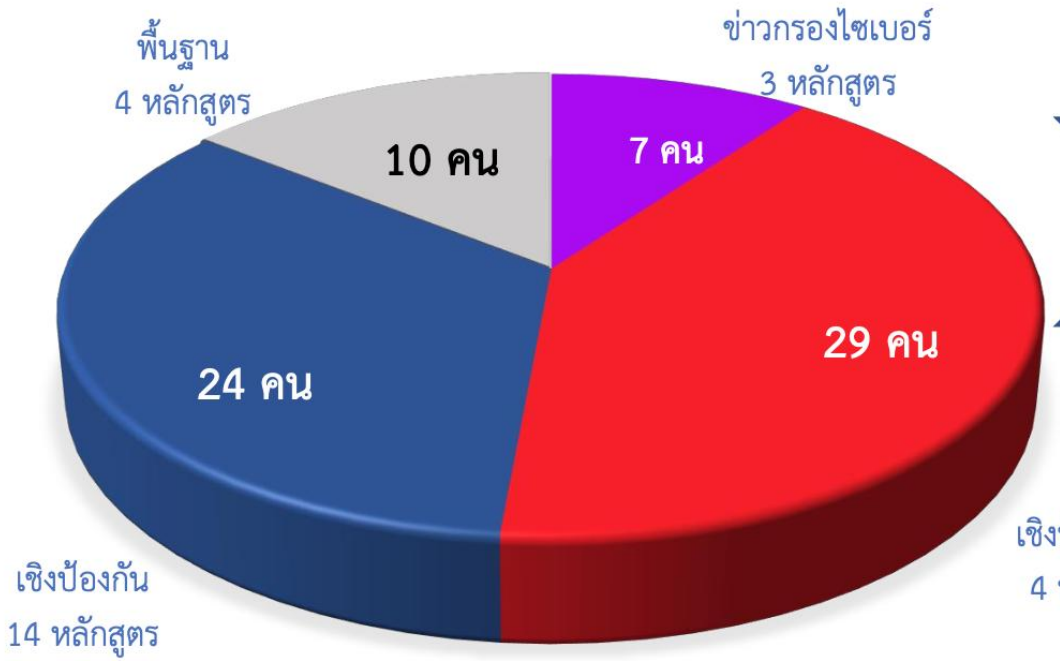
พัฒนาระบบจำลองยุทธ์ทางไซเบอร์ (Cyber Range)

ลำดับ	แผนงาน
๑.	เสนอความต้องการขอใช้งบประมาณกลางปี ๖๖ จัดหาระบบระบบจำลองยุทธ์สำหรับปฏิบัติการทางไซเบอร์
๒.	จัดการฝึกและทดสอบผู้ปฏิบัติงานด้านไซเบอร์ของ ทอ.ด้วยระบบ Cyber Range



แผนงานขับเคลื่อน และพัฒนาหน่วยตามนโยบาย ผบ.ทอ.

การฝึกและศึกษาด้านไซเบอร์ของกำลังพล ศซบ.ทอ.
ด้วยโครงการทั้งภายในและภายนอก ทอ. จำนวน ๒๕ โครงการ



การทดสอบใช้กำลัง ทอ.

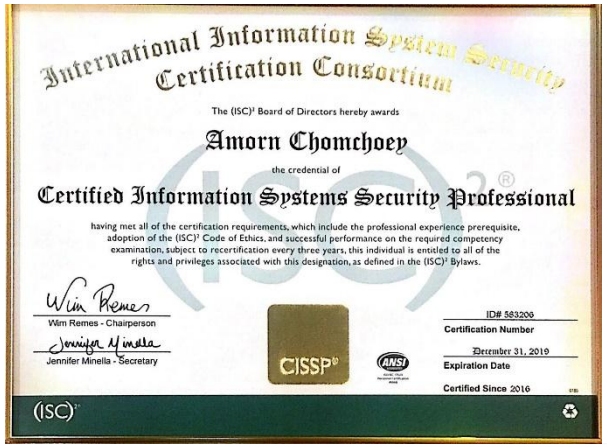
การฝึกการรักษาความมั่นคงปลอดภัย
ทางไซเบอร์แบบเป็นหน่วย (บก.ทท.)

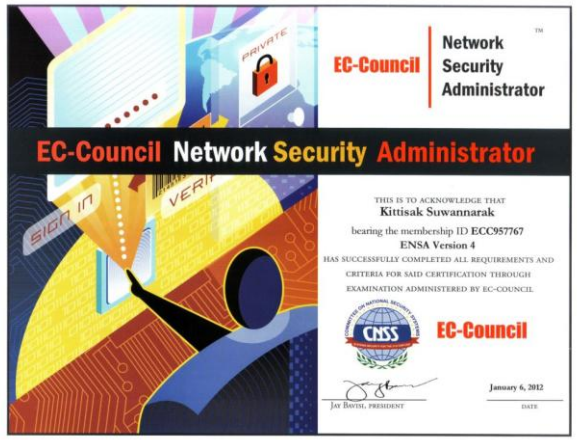
การฝึก Cobra Gold

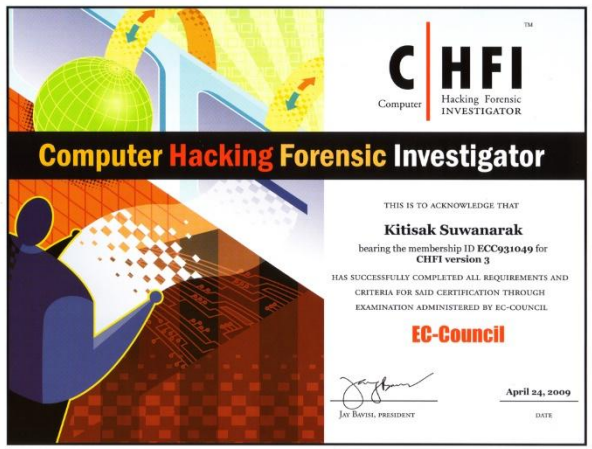
การฝึกด้านไซเบอร์ระดับประเทศโดย สกมช

ขีดความสามารถกำลังพล ศซบ.ทอ.

- ใบรับรองเชิงป้องกัน

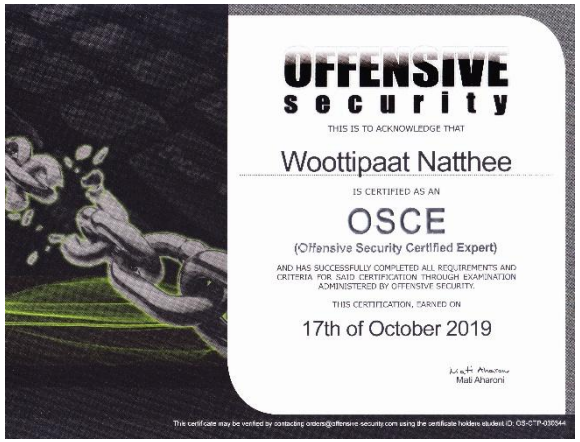


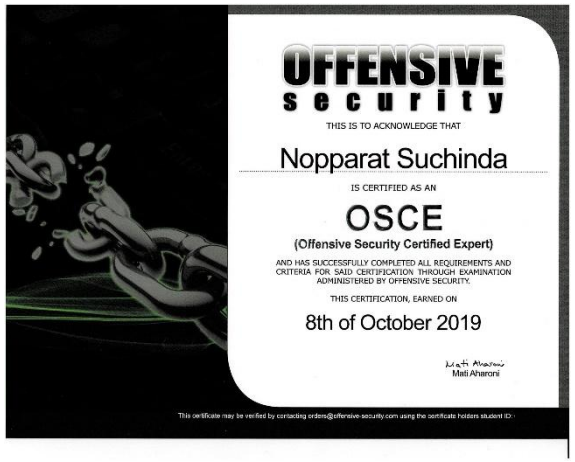


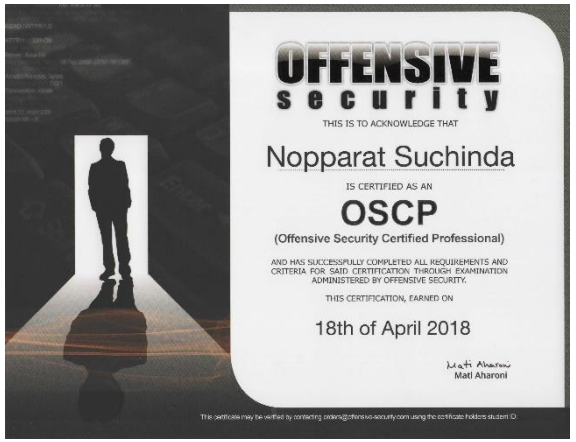


ขีดความสามารถกำลังพล ศซบ.ทอ.

- ใบรับรองเชิงป้องปราม







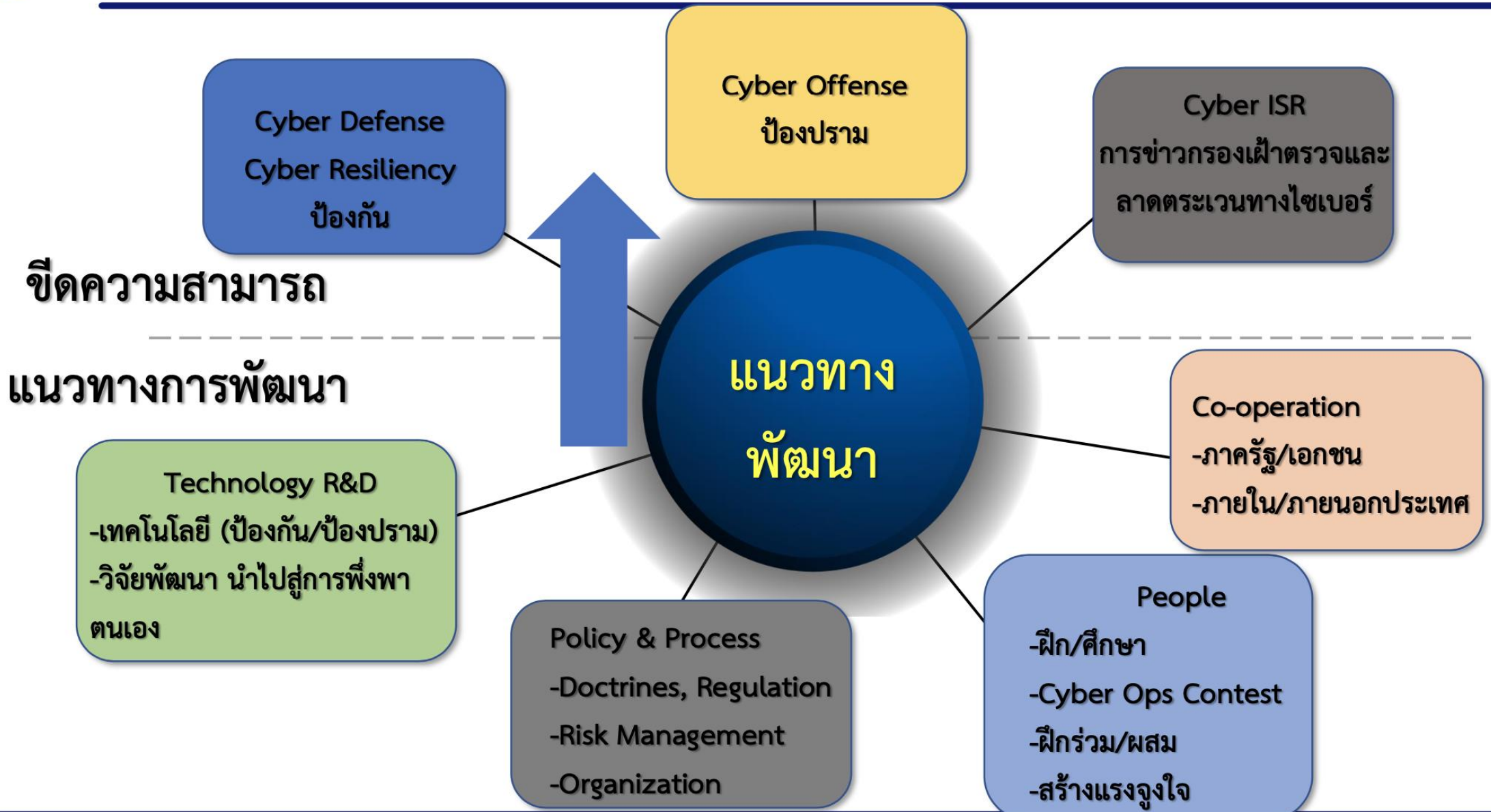
แผนงานขับเคลื่อน และพัฒนาหน่วยตามนโยบาย ผบ.ทอ.

เสริมสร้างขีดความสามารถกำลังพลกองทัพอากาศให้มีองค์ความรู้ในการปฏิบัติการข่าวกรองทางไซเบอร์และการปฏิบัติการไซเบอร์เชิงรุก

ลำดับ	แผนงาน
๑.	โครงการสัมมนาเชิงปฏิบัติการเพื่อรับมือภัยคุกคามไซเบอร์ รุ่นที่ ๒ (สำหรับ น.ทสส นขต.ทอ.)
๒.	จัดอบรมการปฏิบัติการไซเบอร์ขั้นต้น สำหรับ นขต.ทอ. (สำหรับ น.ทสส นขต.ทอ.)
๓.	รวบรวม และวิเคราะห์ข่าวกรองภัยคุกคามทางไซเบอร์
๔.	การจัดอบรมหลักสูตรการปฏิบัติการทางไซเบอร์ของ ทอ. รุ่นที่ ๑ (สำหรับ น.ทสส นขต.ทอ.)
๕.	เข้าร่วมการฝึกและการแข่งขันด้านไซเบอร์ของหน่วยงานภายนอก ทอ.
๖.	จัดทำฐานข้อมูลผู้ปฏิบัติงานด้านไซเบอร์ของ ทอ.

แนวทางการพัฒนางานด้านไซเบอร์ในอนาคต

งานพัฒนาหน่วยปี ๖๖ และแผนงานพัฒนาหน่วยปี ๖๗

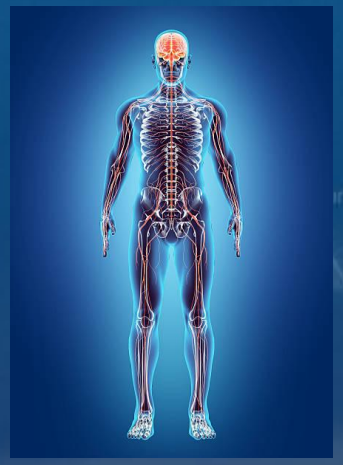


การพัฒนาด้านไซเบอร์ในอนาคต

- กำหนดตัวชี้วัดในการประเมินความพร้อมด้านไซเบอร์ ของ ทอ.
- พัฒนาบุคลากรให้มีความรู้ ความสามารถ ทั้งเชิงปริมาณและคุณภาพ
- พัฒนาระบบการป้องกัน และระบบสำรอง เพื่อให้สามารถรองรับการโจมตีทางไซเบอร์ในอนาคตได้โดยไม่ส่งผลกับภารกิจ (Cyber Resiliency)
- พัฒนาขีดความสามารถการปฏิบัติการข่าวกรองไซเบอร์

การพัฒนาด้านไซเบอร์ในอนาคต (ต่อ)

- เข้าร่วม การฝึกร่วม/ผสมทางไซเบอร์ กับมิตรประเทศ
- พัฒนาชุดปฏิบัติการไซเบอร์
- วิจัยและพัฒนายุทโธปกรณ์
- สร้างแรงจูงใจให้ผู้ปฏิบัติงานด้านไซเบอร์



Synchronization

กองทัพอากาศในอนาคต