Information Operations

Pillar- CND

OOAT,

Cyber Command Center,

Training by OnNet, 2018

Why Information Operations

- Information security died mid 2000s
- Cyber Security Journalism oriented name
- Approaching the era of Information Operations

Pillars of Information Operations (I.O.)

- Computer Network Operations CNO
- Operation Security OPSEC
- Military Deception MILDEC
- Military Information Support Operations MISO (**KE version DISO**)
- Electronic Warfare EW

Main discussion is CNO

- Computer Network Defense (CND)
- Computer Network Exploitation (CNE)
- Computer Network Attack (CNA)

Computer Network Defense

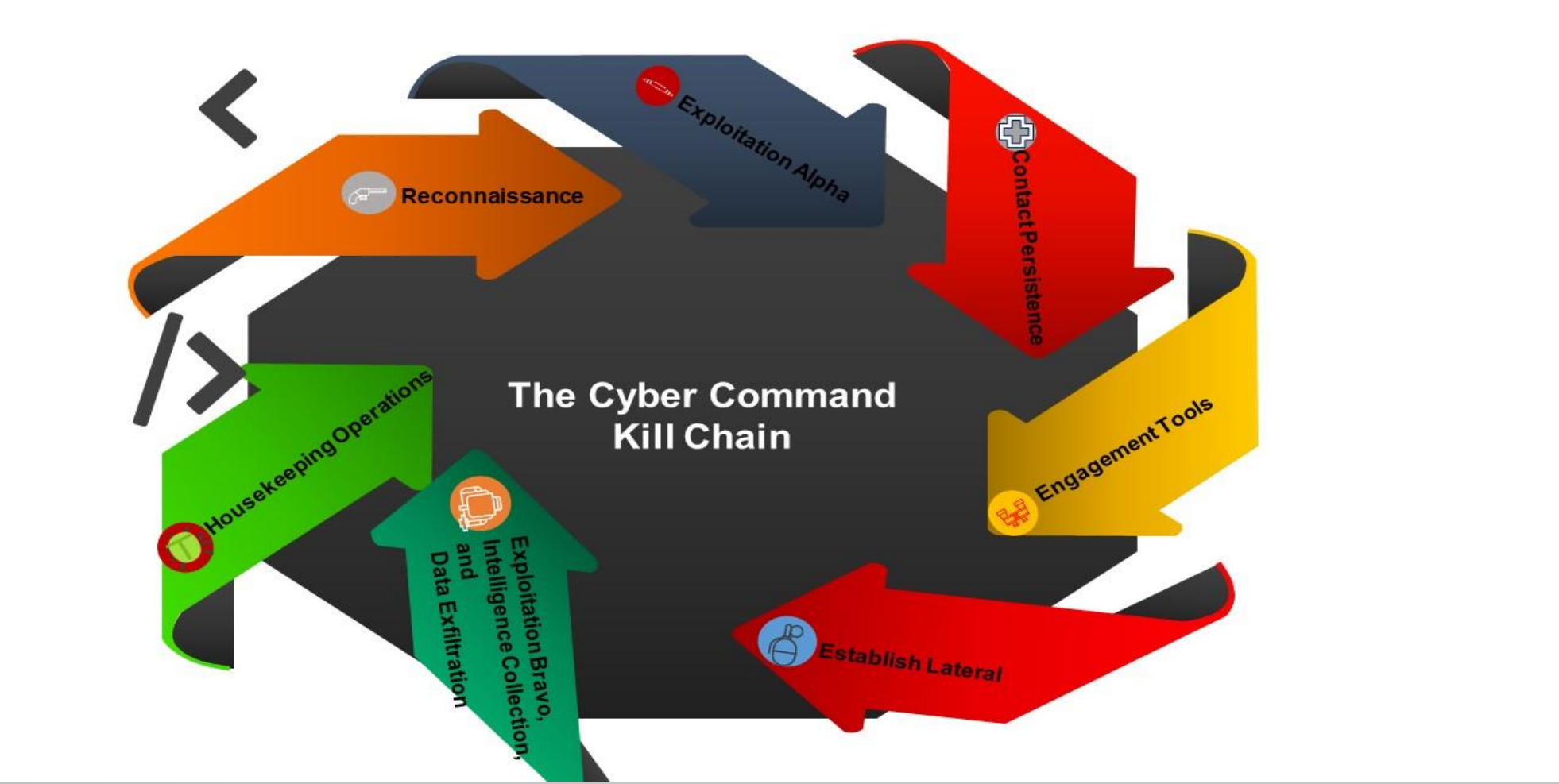
- Computer hardening
- Network hardening
- Application Security and Security Development In Mind
- Incidence Response
- Cyber Threat Intelligence
- Counter-Cyber (Sometimes leads to CNA and CNE)
- Covert Collection for Defense
- Business Continuity Plan
- Threat Hunting
- Forward Hunting and Defend Forward (often leads to CNA and CNE)

Application Security and Security Development

- Clean code
- Check the programming style up to standards
- Testing looping
- Understand the imports/includes/modules/use
- Validate input
- Check and fix compiler warning
- Deny access
- Sanitize data
- Defense in depth
- Effective quality assurance techniques
- Model threat analysis

Understand Cyber Command Kill chain

- Developed inhouse.
- Used for both OCOs and DCOs.



PRACTICALS