Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture

Sungyoung Cho, Insung Han, Hyunsook Jeong, Jinsoo Kim, Sungmo Koo, Haengrok Oh and Moosung Park
Agency for Defense Development, Republic of Korea

International Conference on Cyber Situational Awareness, Data Analytics, and Assessment (Cyber SA 2018)
11-12. June. 2018 / Glasgow, Scotland, United Kingdom

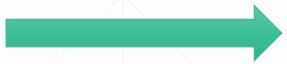
국방과학연구소
Agency for Defense Development

Outline

- Introduction
- Related Work
  - Current Cyber Kill Chain Models
  - Current Cyber Taxonomies
- Proposed Attack Chain Model and Taxonomy
- Visualization of Cyber Situations on CyCOP
  - CyCOP Architecture
  - Visualization of Cyber Threat with Kill Chain Model
- Conclusion and Future Work

Introduction

- Various attacks in Republic of Korea (S. Korea)
  - DDoS Attack (2009.7.7, 2011.3.4, 2013.6.25, …)
  - APT (Advanced Persistent Threat) ((2011.4.12, Finance), (2014.12.9, Power Supply), …)
- Regarded as **Cyber Warfare**
  - Especially against N. Korea
  - Importance on Cyber Situation Awareness



知彼知己

If you know your enemy and yourself, you can win every battle.

- Our paper proposes…
  - Cyber Kill Chain Model, and corresponding cyber attack (threat) taxonomy
  - Application to Cyber Common Operational Picture (CyCOP)
  - As fundamentals for supporting decision-making in cyber warfare

Related Work

Current Cyber Kill Chain Models

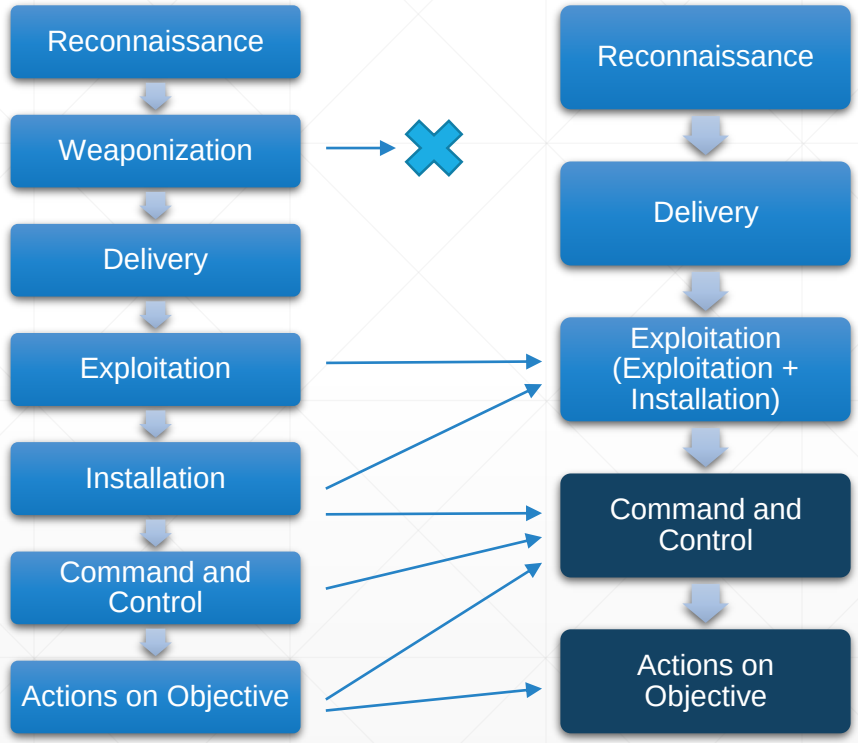
- Various Cyber Kill Chain Models
  - Lockheed Martin's Cyber Kill Chain®
  - Describe the attackers' behavior at multiple attack phase
- Limitation
  - Most are conceptually described
  - Differently described each other
    - Post-exploitation phases
  - Information asymmetry between attackers and CERT team

Current Cyber Threat Taxonomies

- Existing Attack Taxonomies
  - MITRE CAPEC
    - Categorized by attack mechanism
  - MITREATT&CK
    - Categorized by attack tactics
- Limitation
  - These are not exclusive, interrelated
  - Categorized by different criteria
  - Cannot understand the flow/context of attacks

Proposed Attack Chain Model and Taxonomy

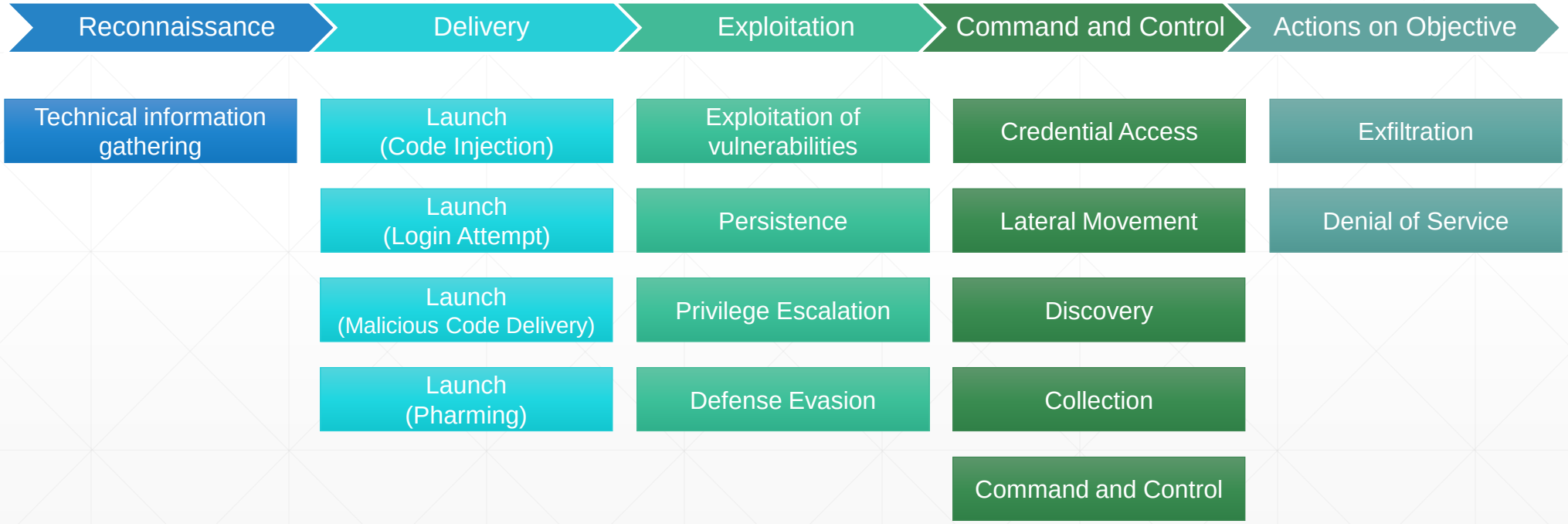
- Idea
  - Propose a cyber kill chain model
  - Map each attack phase to attack techniques listed in CAPEC and ATT&CK



Proposed cyber kill chain model and corresponding taxonomy
will give Unified and consistent cyber threat information to military organizations.

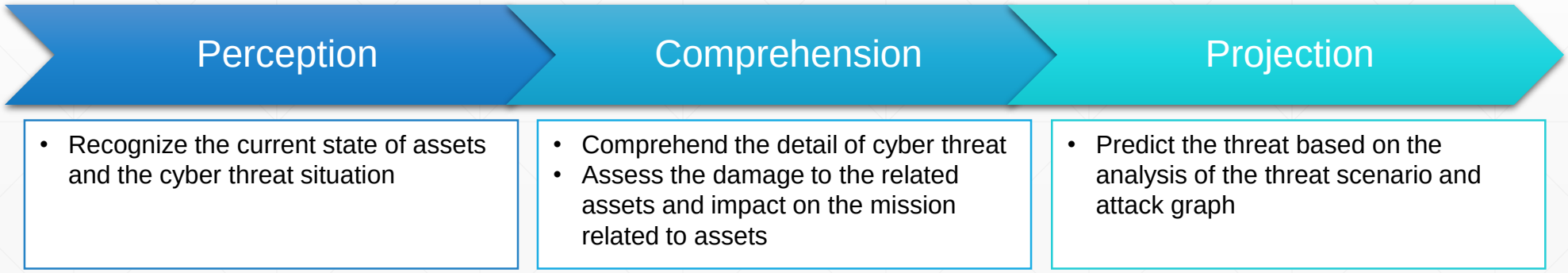
Proposed Attack Chain Model and Taxonomy

Kill Chain Model and Tactics

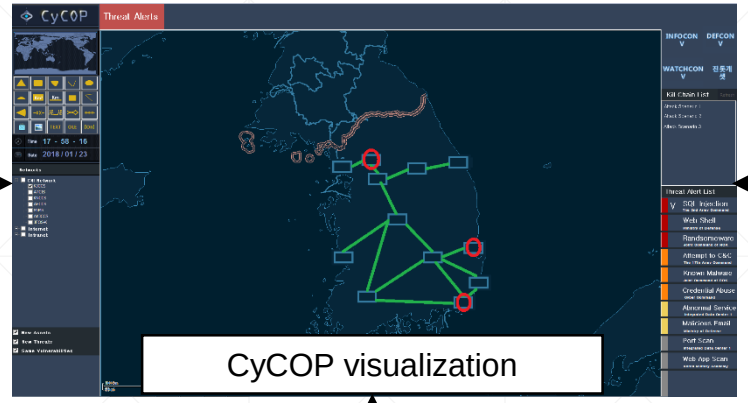


Visualization of Cyber Situations on CyCOP
Overview

- Cyber Common Operational Picture
  - A tool for situational awareness in cyberspace
  - Common Operational Picture
    - A tool for situation awareness in kinetic warfare
    - C4I (Command, Control, Communication, Computer & Intelligence System) in military field
  - Endsley's Situation Awareness Model



CyCOP System Architecture



Asset information visualization

Correlated alert visualization

CyCOP visualization

Assets DB

Cyber attack visualization framework

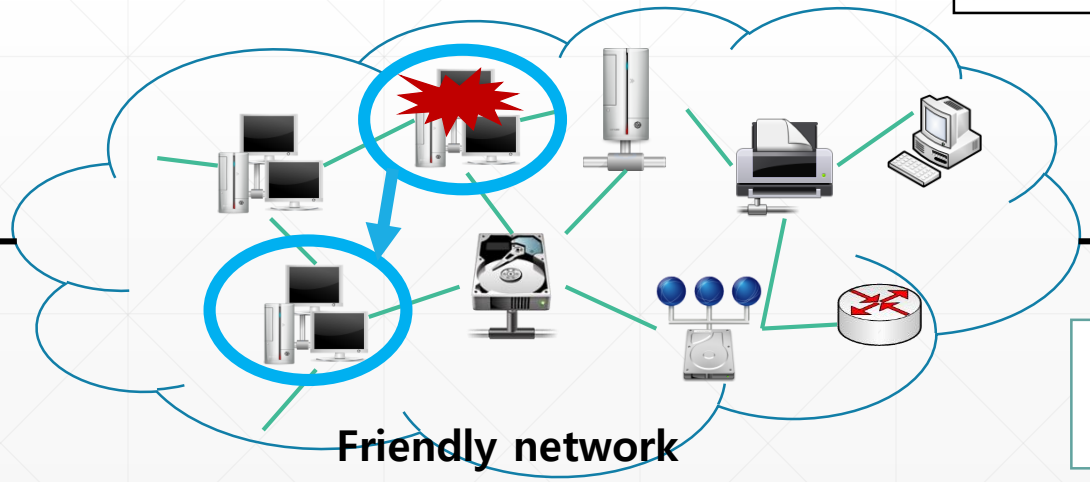
Alert DB

Correlation rule-set framework

Assets Identification/Management

Cyber Threat Taxonomy

SIEM
(Security Information & Event Management)



Friendly network

Asset information gathering

- Active Remote Asset Detection
- Passive Remote Asset Detection
- SNMP-based Asset Information Gathering
- Local agent-based Asset Information Gathering

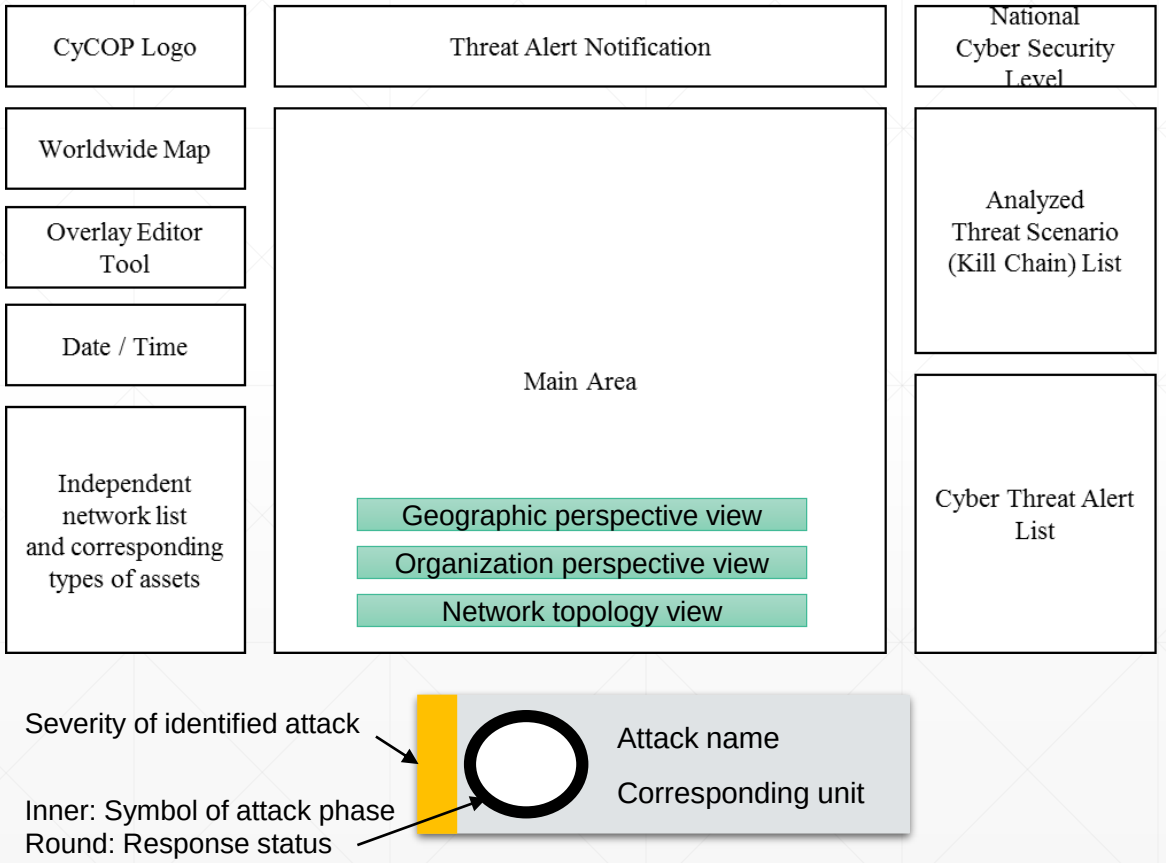
Cyber attack sensing

- System Event Logs
- Web Logs
- Anti-Malware Events
- Security Solutions Events

Visualization of Cyber Threats on CyCOP
Common Screen Structure

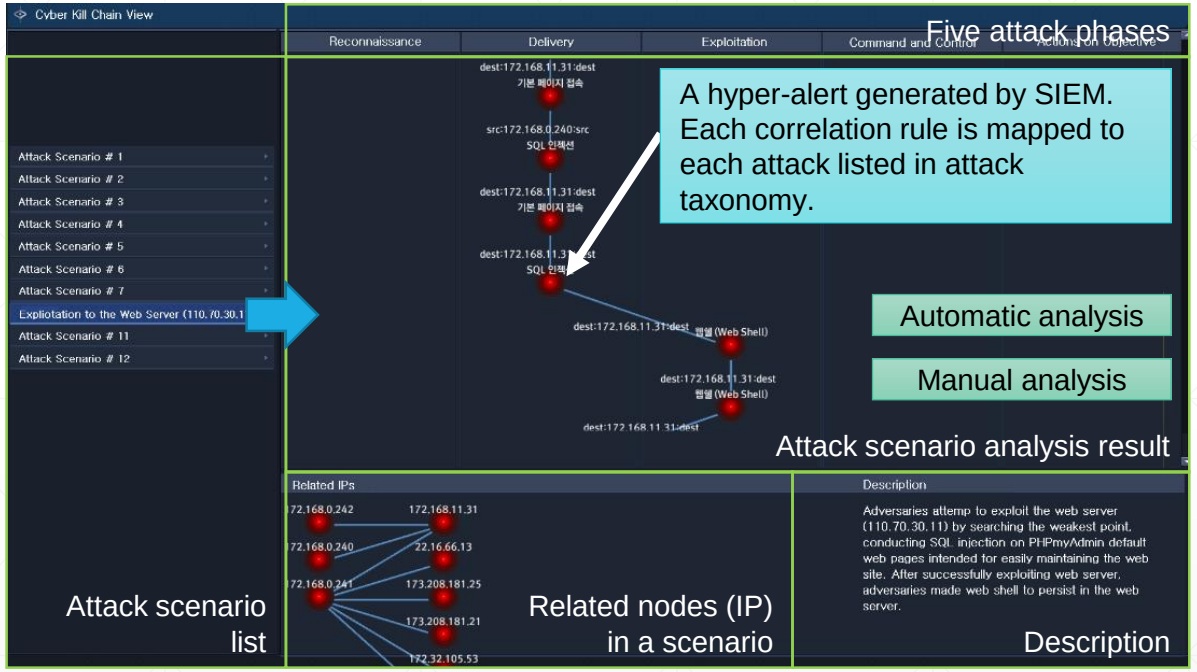
- General use case
  - Can identify high level alerts generated by SIEM which correlates the low level event data
  - Can identify attack scenario analysis result in "Attack Scenario List"
  - Can identify the threatened assets or corresponding organization (unit) on the main area
  - Can verify detailed alert information when selects the threatened assets or unit

Designated by
- National Intelligence Service (NIS)
- Cyber Command (ROK CC)



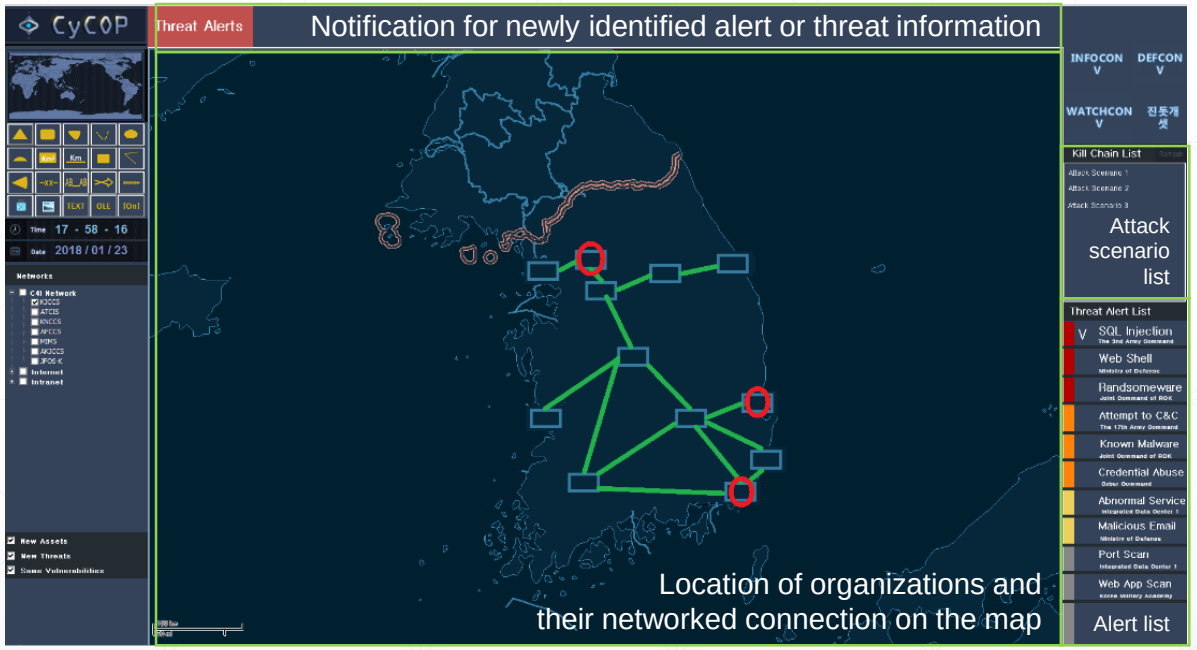
Visualization of Cyber Threats on CyCOP
Cyber Kill Chain view

- Use case
  - Can understand the flow/context of attack (attack scenario)
  - Can discover the uncertainty between attacks
    - Can direct the analysts to investigate undetected attacks
  - Can predict the next attack phase
    - In terms of attack phase and characteristics



Visualization of Cyber Threats on CyCOP
Geographic Perspective view (Main view)

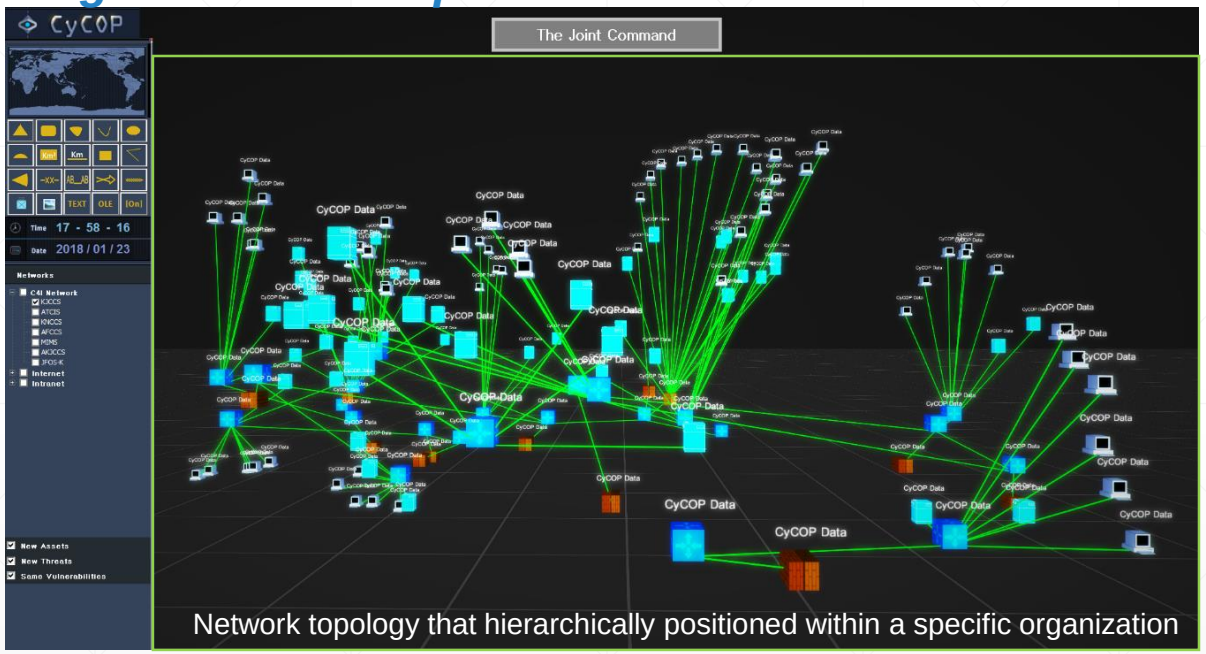
- As the **main view** for commander
- Use case
  - Can identify cyber threats (attacks)
    - by attack itself (high level alert) or
    - by threatened asset and corresponding organization or unit on the map
  - Can verify detailed information
    - Alert information when selects the threatened unit
    - Threatened asset(s) and its (their) information when selects the threatened unit



※ For security reasons, the location and connections are modified, and described as “Major Cities” and “Highways”

Visualization of Cyber Threats on CyCOP

Organization Perspective view

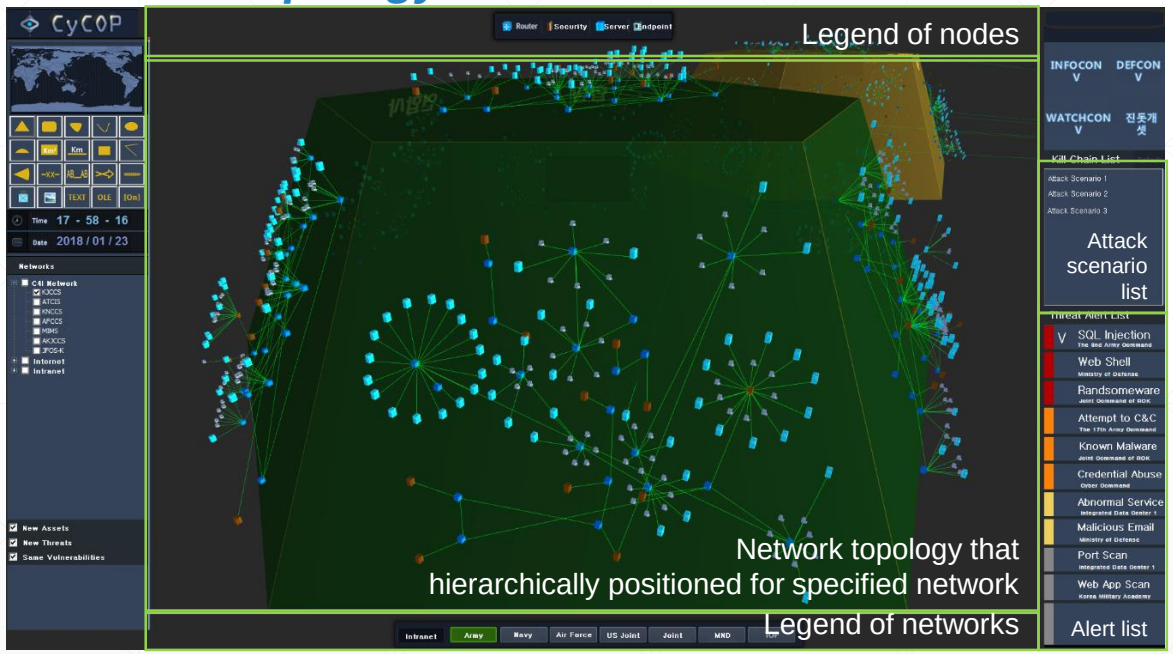


Network topology that hierarchically positioned within a specific organization

Layer of node

- Server / Endpoint
- Switch
- Network Security Device
- Router/Network Device

Network Topology view



Network topology that hierarchically positioned for specified network

Layer of node

- Server / Endpoint
- Switch
- Network Security Device
- Router/Network Device

Conclusion

- **Cyber kill chain model** and corresponding **cyber attack taxonomy**
  - Analyze existing cyber kill chain models
  - Reconstruct the attackers' behavior as the cyber kill chain model
  - Classify attack TTPs for each attack phase by using CAPEC, ATT&CK (Pre-ATT&CK)
- Application to **Cyber Common Operational Picture (CyCOP)**
  - CyCOP system architecture, and a role of attack taxonomy model
  - Use case of several views related to cyber kill chain model

Thank you!

Q&A

sycho@add.re.kr or *sycho@sycho.kr*