FORSVARET

Computer Network Defence in the Norwegian Armed Forces

NISlecture 2013/1

Major Geir Olav Dyrkolbotn (Ph.D.)
Head of Computer Network Defence, CYFOR

NISlecture 2013/1

Goal:

inspire debate

….. and maybe research?

Topic:

- Cyber Defence
- Threats
- Computer Network Defence

The Norwegian Armed Forces - Cyber Defence (CYFOR)

- Established through document of June 2012
- An acknowledgment of a new threat
- A response to a new threat – militarily and for society.
- Responsible for Military Cyber Defence
  - Protection of military networks and systems.
  - Development of information infrastructure.
  - Maintenance of information infrastructure and sensor network.

Our approach to cyber defence

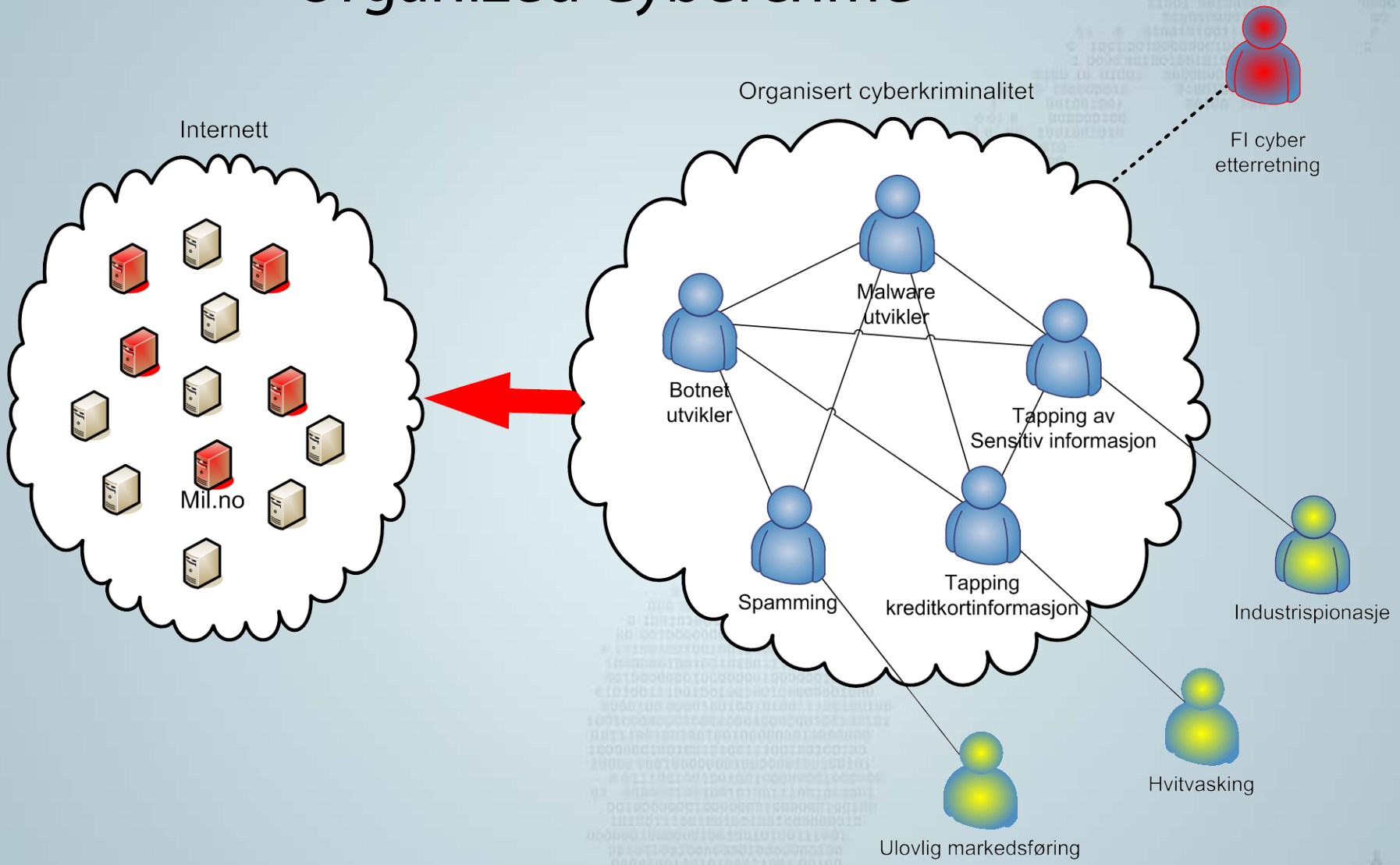
- Technology is an inseparable part of planning and execution of military operations
- Risk is evaluated in an operational context rather than a compliance based context
- Intelligence based threat assessments rather than statistical threat prediction
- Build defendable infrastructures rather than ”secure” infrastructures

Threats – Predictions for 2013

- Non-targeted attacks with economic motive
- Targeted attack and cyber espionage
- ”Hacktivism”
- State sponsored cyber weapons

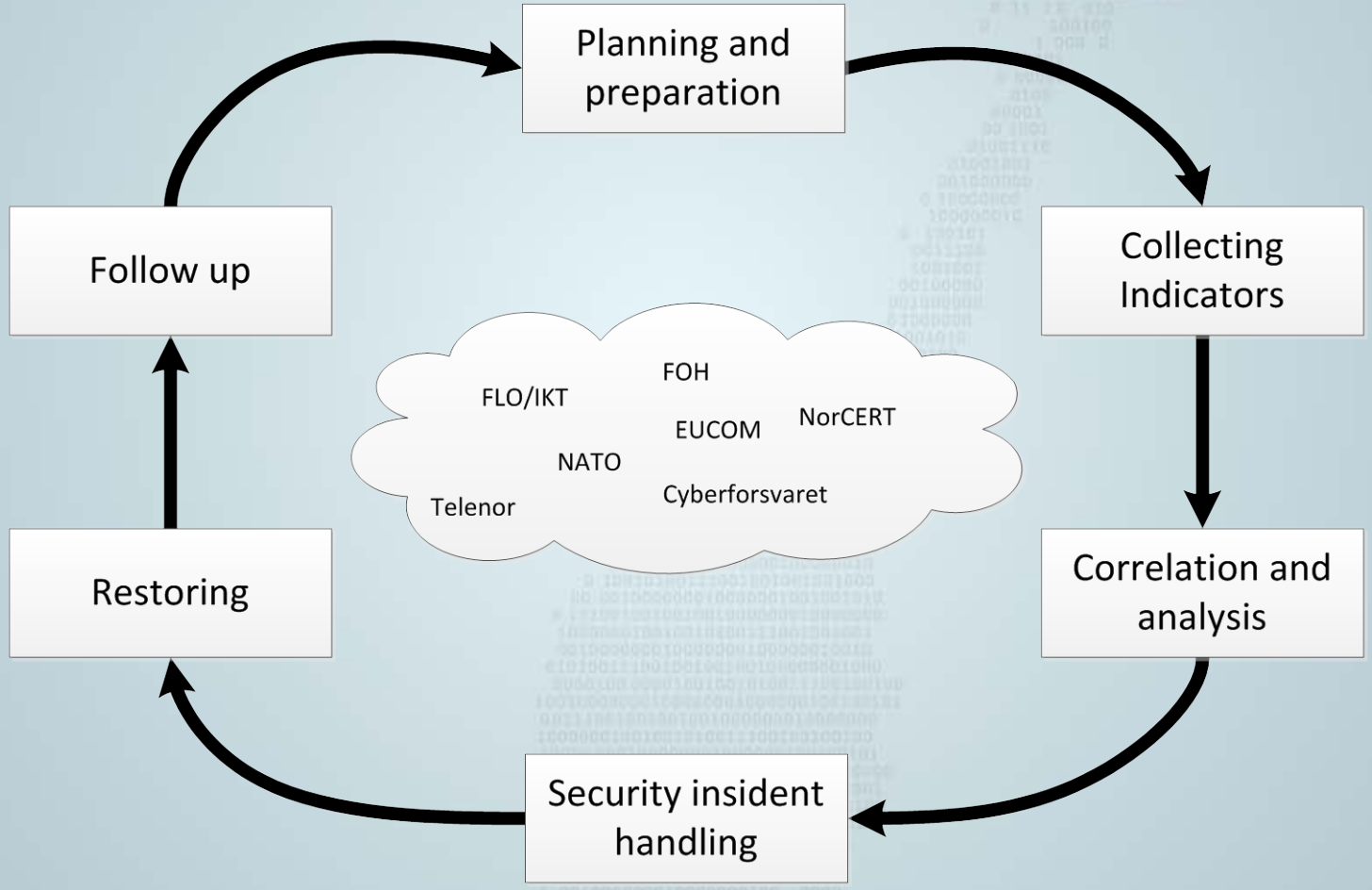
FORSVARET

Organized Cybercrime



FORSVARET

Computer Network Defence Procedures

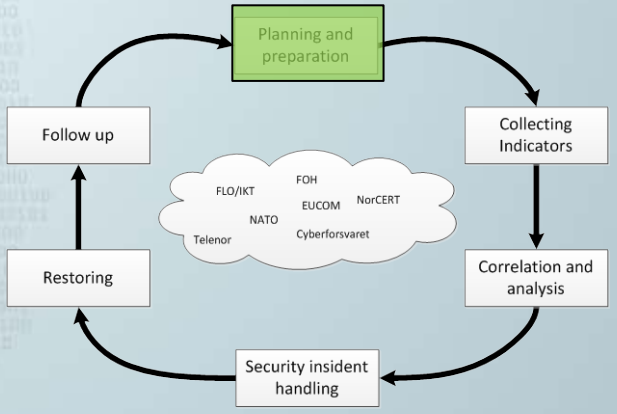


Planning and preparation

Know your infrastructure or cyber landscape

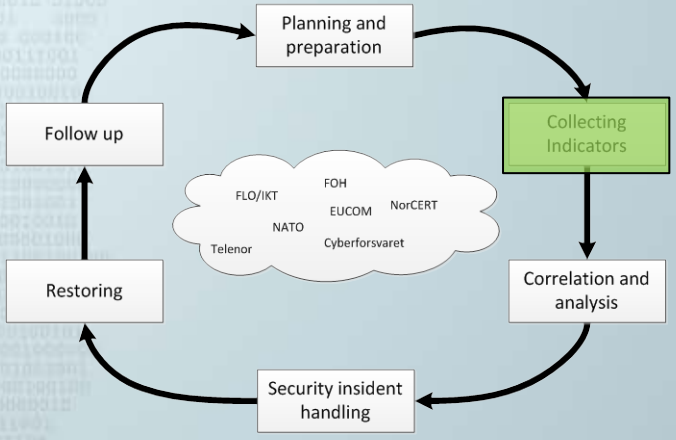
Build a defendable infrastruscture

1. Monitored
2. Controlled
3. Minimized
4. Current
5. Traceability

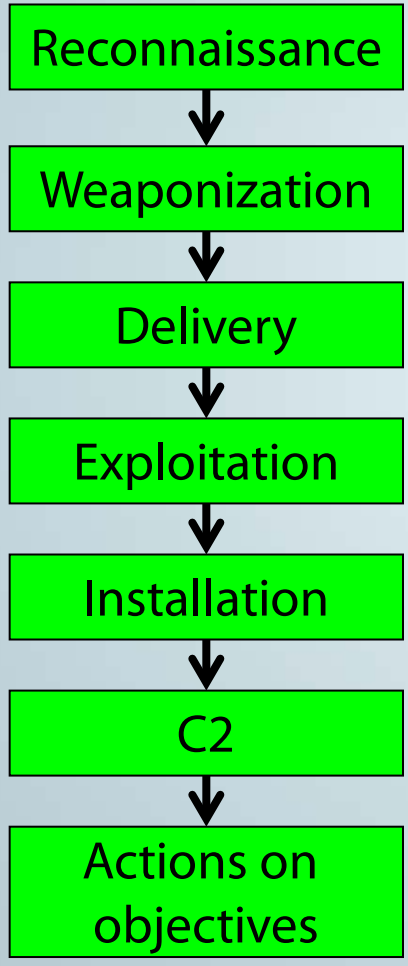


Collecting Indicators

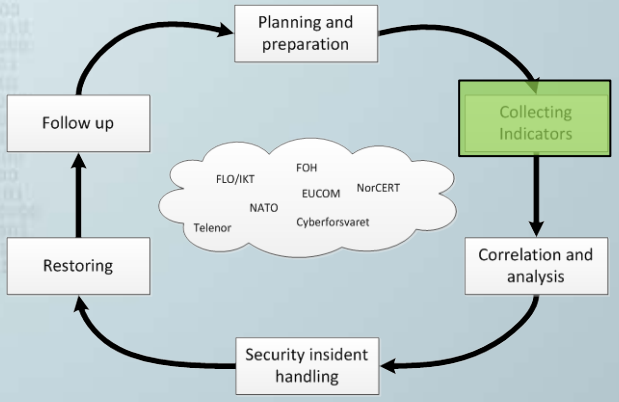
- Alert users
- Alarms
- CND Analyst
- Open and closed sources



Intrusion Kill Chain [Hutchins et al.]

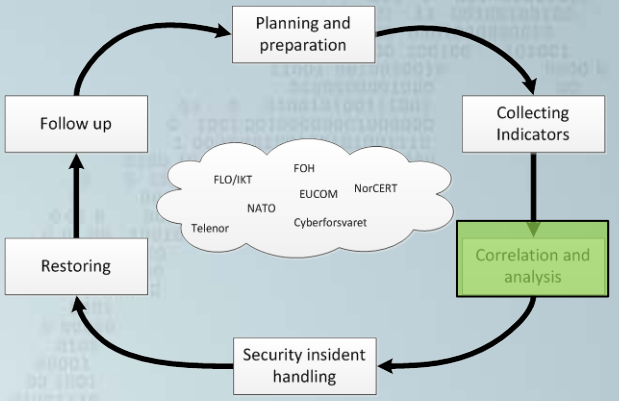


- Series of actions necessary to obtain the desired effect on a target
- CND prosess, necessary actions to defend agains ”kill chain”



FORSVARET

Correlation and Analysis



Analysis ← Late Detection

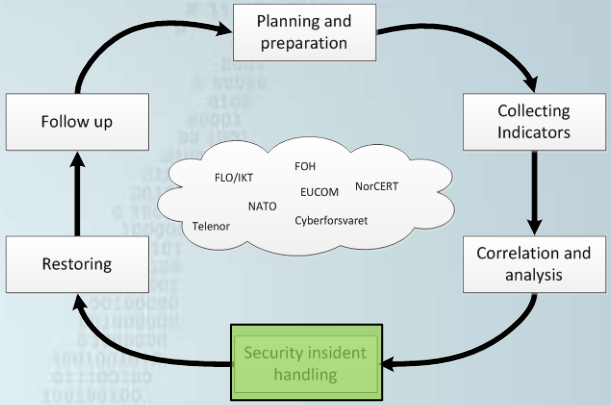
Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C2	Actions on objectives

Analysis ← Earlier Detection → Synthesis

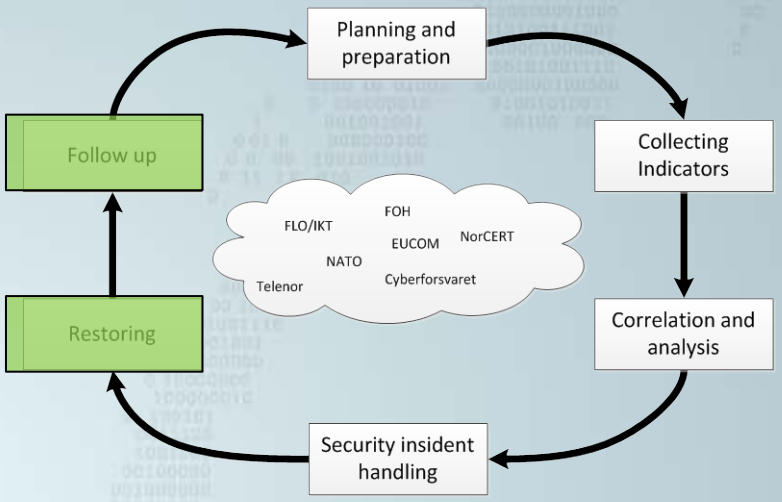
Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C2	Actions on objectives

Incident handling

- Develope a course of action (Operational plan)
- Coordinate



Restoring and follow up



- Reestablish a secure state
- Strengthening

(hopefully we learned something)

FORSVARET

Thank you!

Questions & Comments?

Geir Olav Dyrkolbotn
geirolav.dyrkolbotn@gmail.com