GraMSec June 22nd 2020:

Breaking the cyber kill chain by modelling resource costs

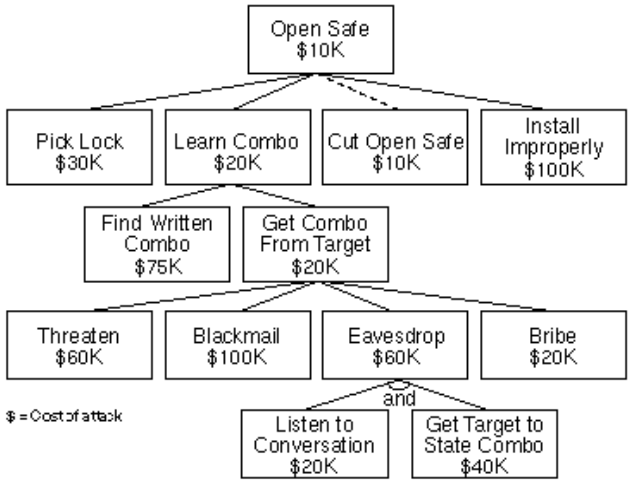
Kristian Haga

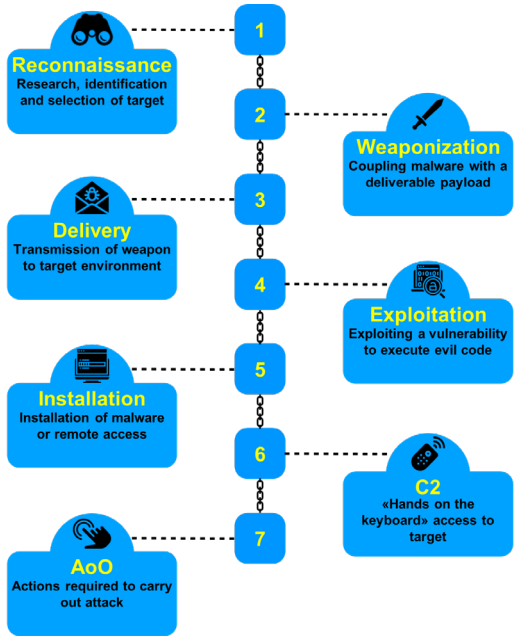
Per Håkon Meland

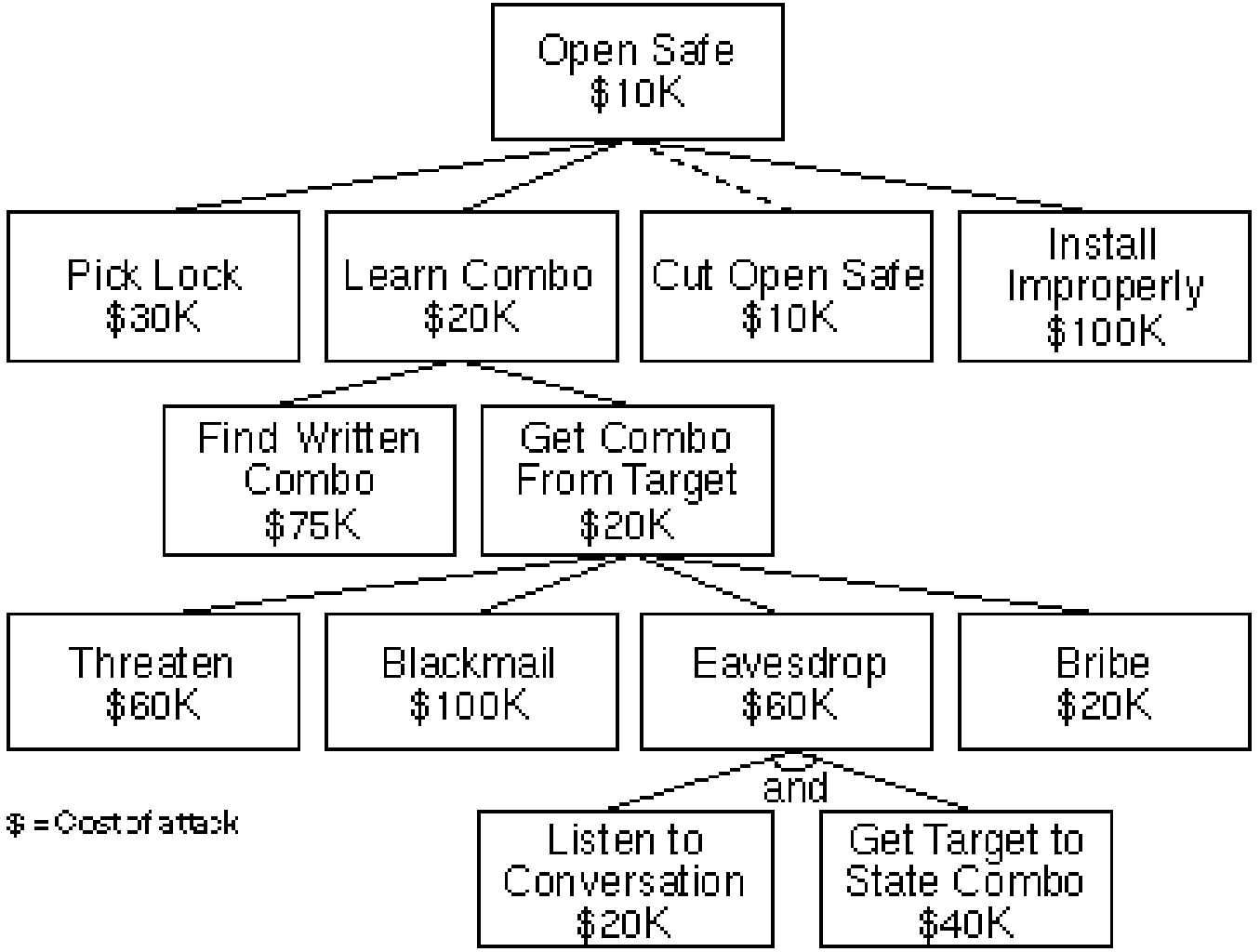
Guttorm Sindre

Resource Cost Model (RCM)

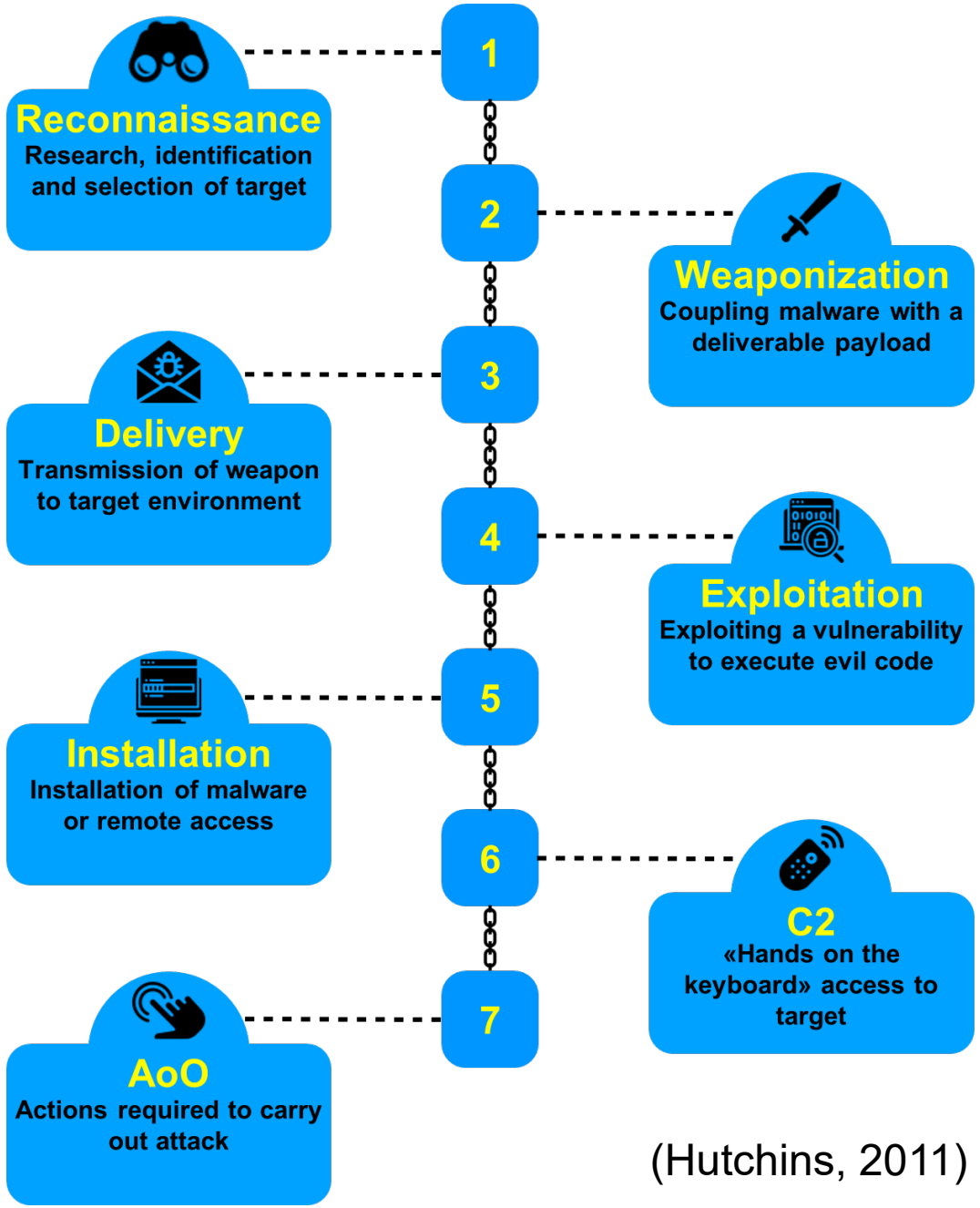
Attack trees + Kill Chain Analysis





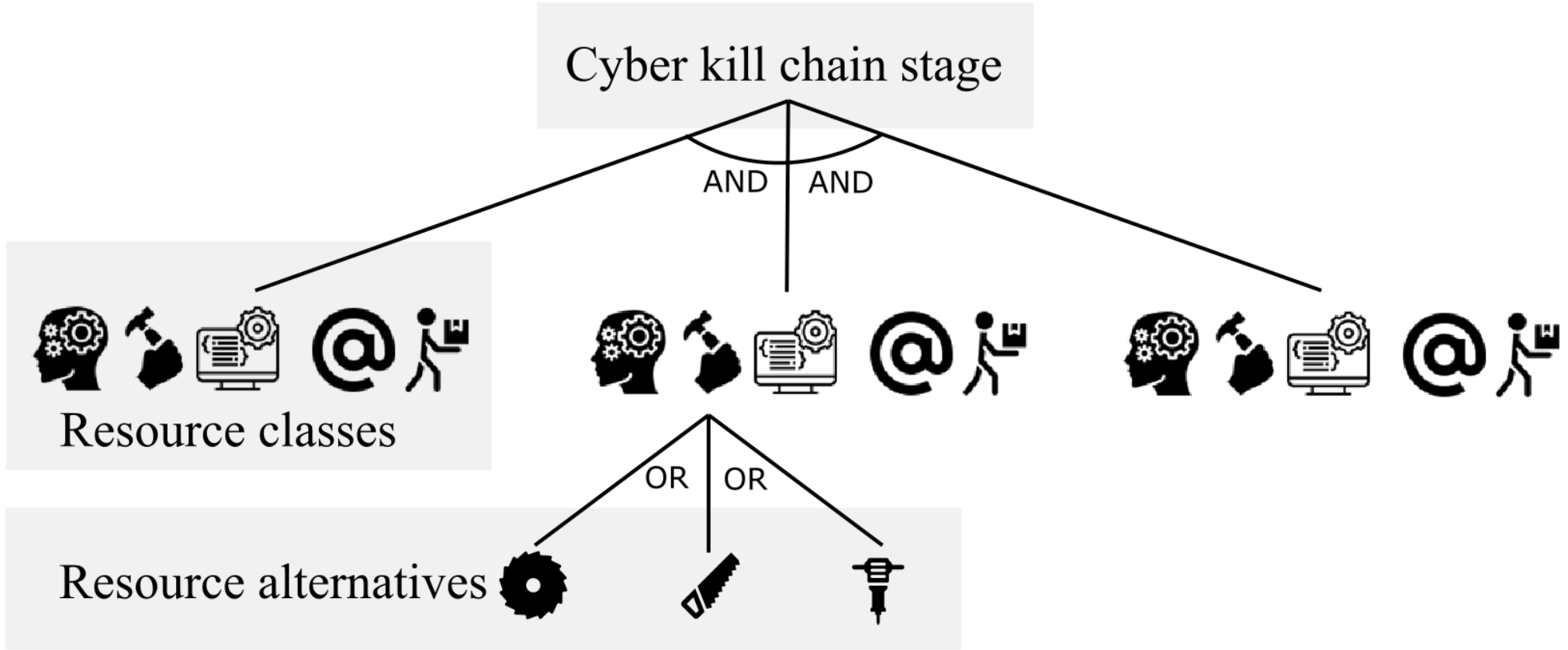


(Schneier, 1999)



(Hutchins, 2011)

LOCKHEED MARTIN



$$T = [(min\ cost = \sum_{\substack{\text{stage} \in \\ \text{kill chain}}} \sum_{i \in V} \alpha_i), (max\ cost = \sum_{\substack{\text{stage} \in \\ \text{kill chain}}} \sum_{i \in V} \beta_i)]$$

$$C = \prod_{\substack{\text{stage} \in \\ \text{kill chain}}} \prod_{R} \phi_j = \frac{\sum_{i \in R_j} c_i}{n}$$

Image source: Wikimedia commons

IRCM Info Attacker Profiles

Model info

Title: ECDIS update attack
Description:
Cost interval: [$0, $0]
Confidence: 1
Motivation: 0 hours - The attack is estimated to require a time investment of 0 hours
Technical skill level: None
Legal Limit: Legally - The attack can be realized with only legally available resources
Access level: External - The attack does not require any non-public access level
Probable attacker profiles: Script Kiddie, Hacktivist, Vandal, Petty Criminal, Mobster, Cyber Warrior, Terrorist, Internal - Hostile, Internal - Non-hostile,

Edit model info


Skill


Tangible


Logic


Logic-atomic


Behavioral

IRCM tool demo

Evaluation

Key findings

- Attacks are seldom free
- Cost modelling useful when there is a lack of incident data
- RCM most accurate with specific attacks
- Work-in-progress, promising feedbacks so far

Thanks!