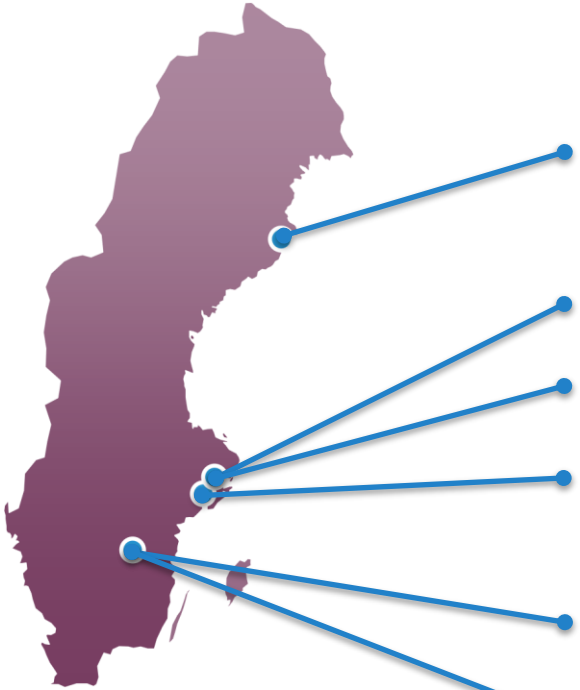
# Defensibility

CDIS Spring Conference, 21 May 2026

Ralf Alvarsson & Henrik Karlzén

# Swedish Defence Research Agency

FOI



CBRN Defence and Security

Defence Analysis

Defence Technology

Weapons, Protection and Security

Cyber Defence and C2 Technology

Electromagnetic Warfare

Research Support and Administration

FOI

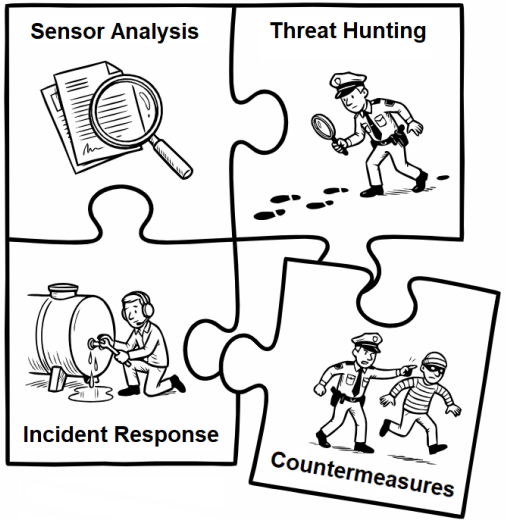
# The project

| Project parameter | Value |
|---|---|
| Timeframe | 2025-2027 |
| Project sponsor | Swedish Armed Forces: Research and Technology Development programme |
| Budget | 9 MSEK |
| Purpose | Provide a basis for evaluating whether a system is defensible |
| Goal | Determine guidelines for attributes that enable effective defence of cyber systems |
| Method | • Literature studies<br>• Interviews with operators<br>• Technical evaluation in Crate<br>• Collaborate with FMV, KTH |

# Project objectives

The topics that the project will focus on are:

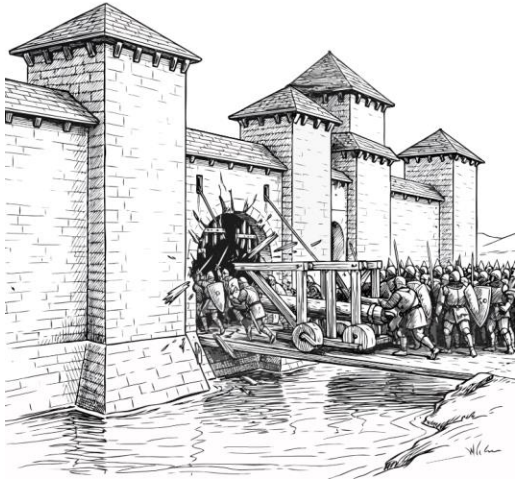
- Variables linked to defensibility
- Variables with the greatest defensive activities
- Which variables are enabling and which are reinforcing
- Technical solutions and processes that increase defensibility
- Does defensibility stand in opposition to protection
- Agreements or regulations that prevent or favor defensibility

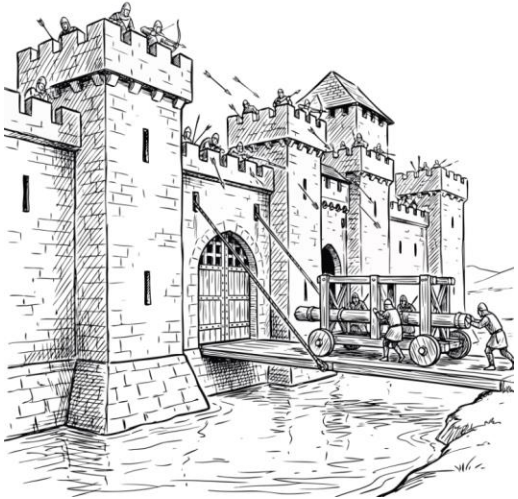



**Defensive Cyber Operations (DCO):**
Activities conducted in blue terrain

FOI

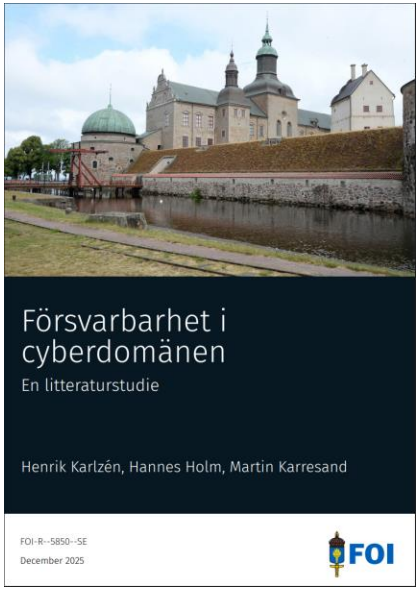
# Protective vs. Defensive





# Literature review (intro)

- Defensibility definitions:
  - The ability to defend, as provided by the right conditions.
  - Distinct from security.
  - A fairly new and rare term, now used by SwAF.
- Research questions
  - What tactics and techniques are used in the literature on protection/defence mechanisms?
  - How is defensibility affected by the mechanisms?




FOI

# Literature review (results)

- T&T used in the literature
  - 198 papers match the D3fend framework.
  - Detection (e.g. NTA) is the main focus (95% of papers).
  - This detection focus is similar to other research, e.g. on SOC AI use (dl.acm.org/doi/10.1145/3747587).
- Impact on defensibility
  - Only six papers make defensibility harder.
    - Mostly network isolation
    - One uses hardening (virtualization) between users
    - Not detection
  - Defenders are rarely mentioned, but sometimes when visualizing logs.

| Tactic | Technique |
|---|---|
| Model | Asset Inventory |
| | Network Mapping |
| | Operational Activity Mapping |
| | System Mapping |
| Harden | Agent Authentication |
| | Application Hardening |
| | Credential Hardening |
| | Message Hardening |
| | Platform Hardening |
| | Source Code Hardening |
| Detect | File Analysis |
| | Identifier Analysis |
| | Message Analysis |
| | Network Traffic Analysis |
| | Platform Monitoring |
| | Process Analysis |
| | User Behavior Analysis |
| Isolate | Access Mediation |
| | Access Policy Administration |
| | Content Filtering |
| | Execution Isolation |
| | Network Isolation |
| Deceive | Decoy Environment |
| | Decoy Object |
| Evict | Credential Eviction |
| | Object Eviction |
| | Process Eviction |
| Restore | Restore Access |
| | Restore Object |

FOI

# Secure compared to defend

| Secure | Defend |
|---|---|
| Encrypt data | Look at data |
| Obscure | Understand system |
| Whitelist software | Install defensive tools |
| Authenticate | Move freely |
| Segment and firewall | Use ports |
| Certify | Change |
| Uphold integrity | Plant disinformation |
| Log events | Surprise the attacker |
| Maintain secure state | Reach secure state |

Conjecture: ”It matters for defensibility if defenders can…”

FOI

# Evaluate conjectures (future work)

- “It matters for defensibility if defenders can…”
- Evaluation
  - Vary conditions e.g. documentation, CTI, logging, tools, mandates, attacker stealth, attack progression.
  - Check success rates in defence.
  - Let real defenders in to a cyber range environment.
  - Compare with defender interviews (published soon).

# Questions?