Cyber Rapid Reaction Team
National perspectives

Center for Cyber Security
Denmark
Thomas
• CFCS **building RRT (rapid reaction team) capability since 2014**.

• RRT now on standby to assist military and civilian partners
  - RRT team delegated authority with local military commander to investigate and remediate
  - cooperation with military partners to ensure quick access and knowhow of military network backbone
  - Incident response “light” vs full blown incident response
• On site analytical process

- RRT bus
- Network monitoring capabilities
- Forensic servers and imaging equipment
- Malware reversing platform

Onsite monitoring

New YARA rules, network signatures, IoCs

Identify malicious activity/compromises

Reverse malware, determine TTP

Forensic servers and imaging equipment
Examples of issues regarding capabilities, management and policy:

- **General observation** - **Preparation and execution**: large part of work is at-home preparation. But important to be able to adapt to unique on-site conditions when executing RRT.

- **Training to deploy more than one team simultaneously**
  - select team members getting basic military training to prepare to deploy in higher risk areas. National requirements?

- **Written own RRT “manual”** based on industry guides
  - fitting Danish context and related internal processes in CFCS

- **Legal framework**: determining what is allowed and not allowed
  - Not necessarily clear cut
  - possible national variations in legal frameworks underpinning RRT
  - working closely with legal department
• **Ensuring technical knowhow** through proper hiring and continuous training and learning
  - knowing what best practice looks like and working towards that
  - is there a lack of properly qualified applicants in national job market?

• **Building a team** that work together across specializations and personalities

• Determine need for **equipment and tools**: testing, maintenance
  - what do we need/want to do – e.g. capability to image 10 machines in what timespan? Full packet capture for how long in what sized network? Preparing for what eventualities?

• **Determining system ownership in advance** and delegating necessary **authority to act on information** gathered during an incident response
  - asking in advance who makes the tough decisions – e.g. closing an entire network disrupting “business as usual”?