CYBER RAPID REACTION TEAM

French COMCYBER perspectives
SUMMARY

• National policy
• Capabilities in place/dev
• Budget assortment
• Organization of teams
• Exemple of deployment / use of capabilities
• Tools used
FRANCE’S POLICY ABOUT GIC

• CRRT ~ GIC = « Groupe d’Intervention Cyber »

• Concepts:
  – Different teams from each Service
  – Different alerting time to react
  – Different perimeter of action
  – Minimum level of qualification & equipment

• 2 ways of going:
  – within incident response process
  – planned on a specified perimeter
SOME CAPABILITIES

• Today:
  – To collect: any takings for background forensics analysis
  – To orient: first technical analysis, ops/user context
  – To apply: designed CND measures

• Tomorrow:
  – To increase the reactivity of response process, by both improving:
    • Tools: to perform onsite deeper investigations
    • Skills and standardization of teams: to enhance reliability
BUDGET...

• No specific budget but...
  – Included in COMCYBER’s global budget
  – Can be budgeted with military operations
  – Equipment costs supported by different staffs
ORGANIZATION OF TEAMS

- Manning: 1/2/0 to 2/4/0
  - 1 manager (1 deputy)
  - 2 to 5 analysts in network, services, system or threat intel

- CRRT leader has local control on the CND operation
  - Coordinates local network/services admins, users, units, and local command
  - Accordingly to MILCERT’s technical goals, guidelines & limitations
  - Deconfliction with local current ops as needed
EXEMPLES OF RECENT DEPLOYMENTS

• Incident response
  – Mainly on National Territory
  – 4 at the same time, in different places

• Planned
  – In various kinetic operations
  – 2 to 3 weeks
TOOLS

• Classical stuff
  – Storage
  – Forensics copy devices & software
  – High performance laptops
  – Secured comms
  – TAPs
  – Antimalware platform

• Tomorrow
  – Tactical box:
    • Indexing calculus
    • Analysis tools
    • Threat knowledge bases
  Long term?
    • Who knows what...
THANK YOU FOR ATTENDING

Questions ?