Cyber Advanced Analysis Lab

Needed capabilities as proposed by Robert in 2008:

1➔ Reverse engineering (& other related analysis)

2➔ Capture of legal evidences (Forensics)

3➔ Defensive measures integration (Honey potting)

4➔ Capture of knowledge & training

5➔ Threat & technology watch

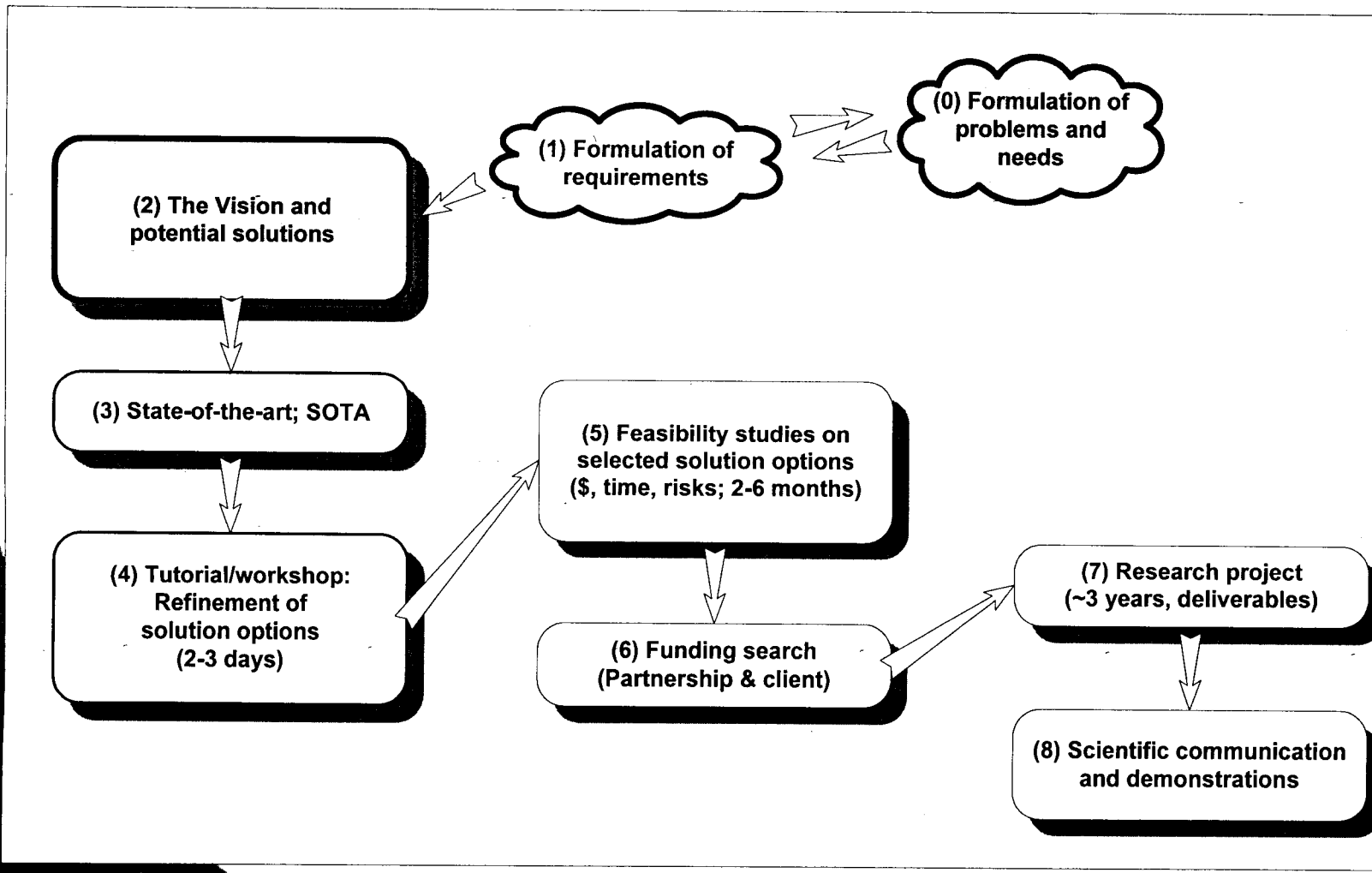
Cyber Advanced Analysis Lab

My mission: Capture & describe the vision of the lab

- **Learn CFNOC org & ops (AAT, NAT, CND Tp, WSS)**
- **Capture the vision (will be described in a classified report)**
- Use proven methodology & framework
- Ease the transition from this phase of the methodology to the next one (up to the TDP or other projects)

Cyber Advanced Analysis Lab

Used methodology:



Cyber Advanced Analysis Lab

Used framework: Zachman (modified for the CAAL)

And the IEEE Std 1362-1998: "Concept of Operations (ConOps) Document"

	A	B	C	D	E	F
	The "What"	**The "How"**	**The "Where" & "connectivity"**	**The "Who"**	**The "When"**	**The "W**
Scope Contextual) (Planner)	Important "objects" to CFNOC	"Processes" the CFNOC will perform	"Locations" in which the CFNOC will operate	"Living entities" important to CFNOC	"Events/cycles" significant to CFNOC	"Goals/mi CFNC
usiness mdl Conceptual) (Owner)	Conceptual or semantic model (CAAL)	Business process model (CAAL)	Business logistics (CAAL)	Work flow model (CAAL)	Master schedule (CAAL)	Business (CAA
ystem mdl (Logical) Designer)	Logical model (CAAL)	Application architecture (CAAL)	Distributed system architecture (CAAL)	Human interface architecture	Processing structure (CAAL)	Business mode (CAA
hnology mdl Physical) (Builder)	Physical model (CAAL)	System design (CAAL)	Technology architecture (CAAL)	Presentation architecture (CAAL)	Control structure (CAAL)	Rule de (CAA
Detailed resentations -contractors)	Objects definition (CAAL)	Program, process (CAAL)	Network architecture (CAAL)	Security architecture (CAAL)	Timing definition (CAAL)	Rule speci (CAA
unctioning XYZ Lab	Object	Function, capability, strategy	Network	Organization units	Schedule	ConOps, s

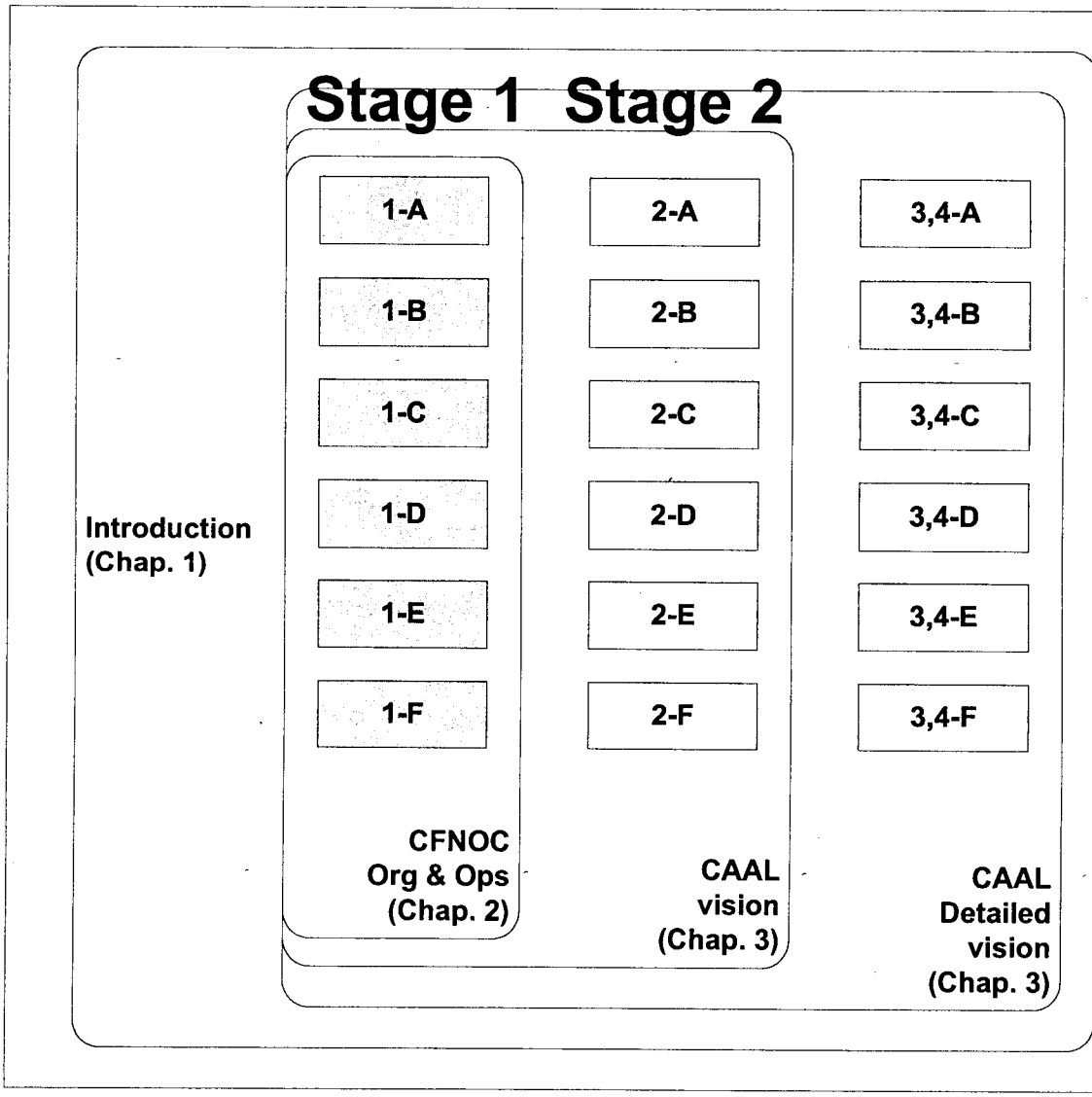
Cyber Advanced Analysis Lab

Deployment:

- 2 stages

Redaction:

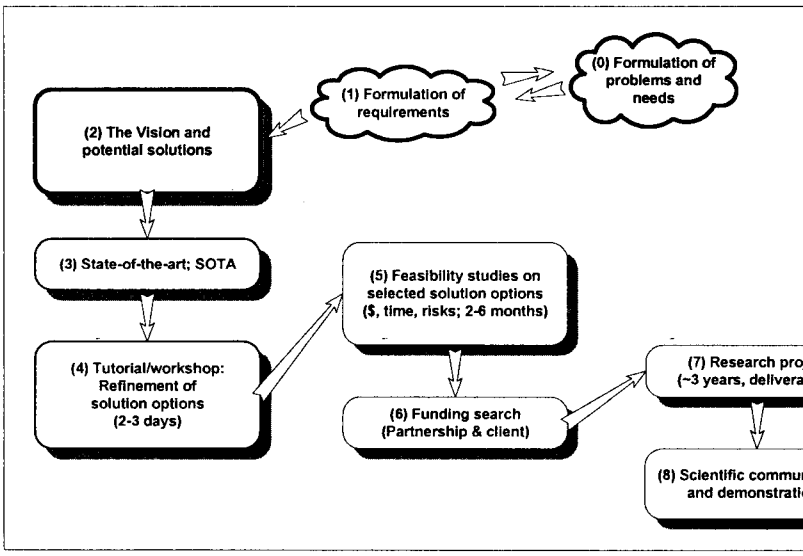
- 3 chapters

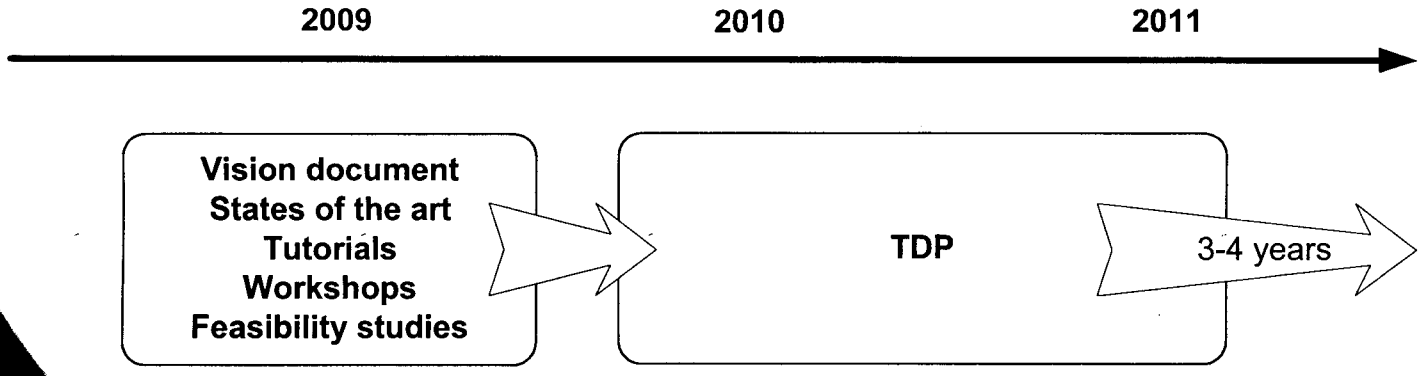


Cyber Advanced Analysis Lab

Planning:

According to the used methodology:





Cyber Advanced Analysis Lab

The Five needed capabilities vs used methodology phases:

		Capability 1 RE & other related analysis	Capability 2 Capture legal evid. (Forensics)	Capability 3 Defensive measures (Hon. Pot.)	Capability 4 Knowledge capture & training	Capabili Threat tech wa
Vision document						
States of the art		Done	Partly done	S. Knight (RMC)	Being done by TBS	Partly d
Tutorials & workshops		Planned	Planned			
Feasibility studies		Many were done	Planned			
in TDP treads		DRDC Val	TBD NCFTA	TBD RMC	TBD, TBS, DRDC Val	TBD, EV DRDC

Cyber Advanced Analysis Lab

- **End-result of this work:**
  - A high-level description of CAAL:
    - vision, mission, implementation plan, etc.
- **Schedule:**
  - Steps 1,2: January 12th to 16th: deployment at CFNOC
  - Redaction: January 16th to March 1st
    - March: "usable" document (to be reviewed for publication)
    - June: Publication (classified)