SL 2009-338 532729

DEFENCE R&D DÉFENSE

Cyber Threat Center (CTC) – The Vision

Content

1. Introduction
2. January 2009 deployment @ CFNOC
3. Overview of the vision
4. The Vision document
5. Conclusion

Cyber Threat Center (CTC) – The Vision

1- Introduction

Origin of this effort

2008 meeting: LCol Drapeau wanted to improve CFNOC's capabilities:

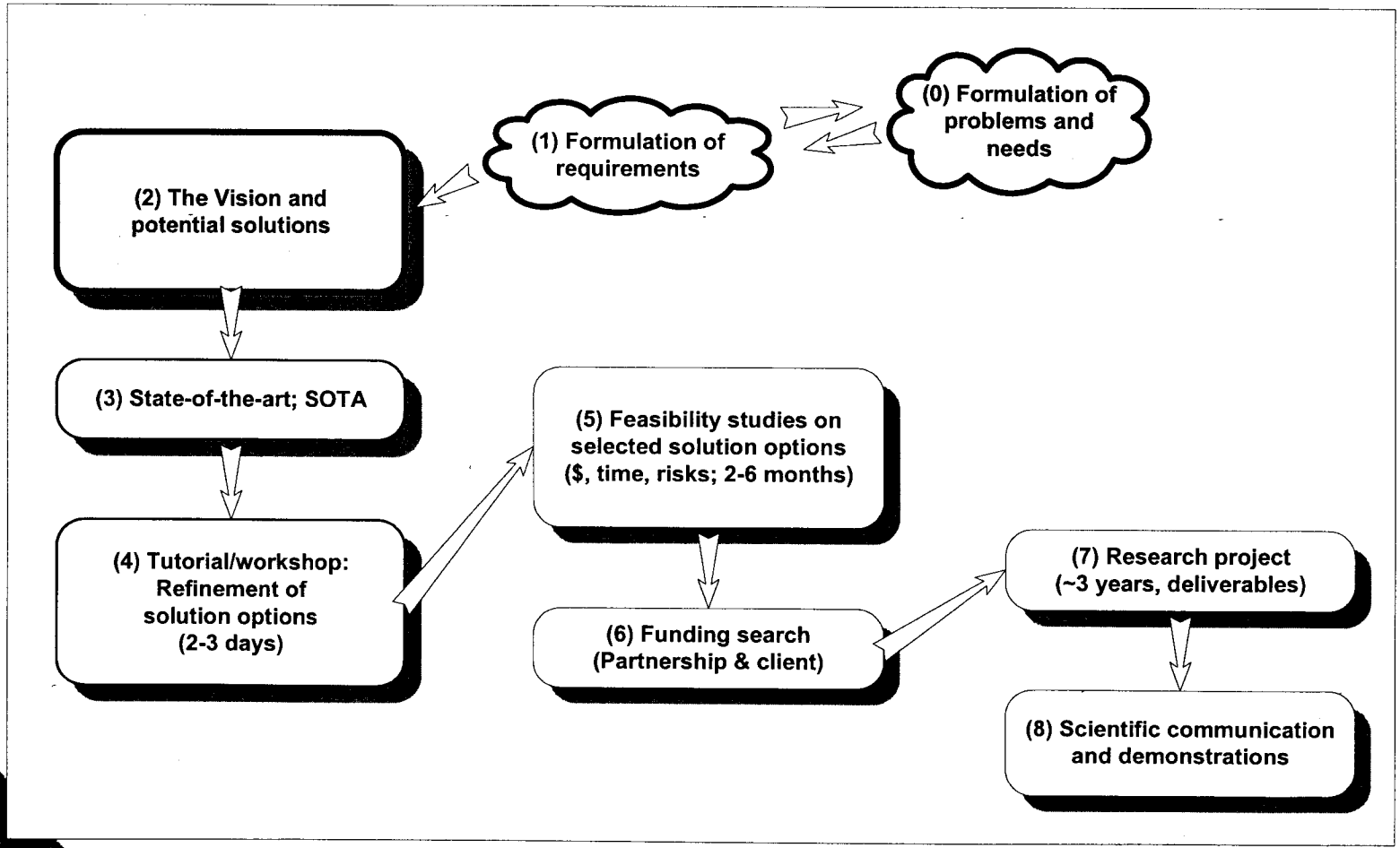
→ Protection against cyber attacks
→ Capture ID of attackers (and other relevant information)
→ Quick recovery after cyber attacks (& other activities)
→ Capture of evidences for near-legal cyber forensics analysis
→ Conduct both passive & proactive CND
→ Eventually, conduct CNE & CNA (GoC policies…)

Effort done so far in this direction

1- Nov.'08 @ Leitrim (LCol Drapeau, Major Lachine, Capt Messous)
2- Deployment of a DRDC Valcartier DS @ Leitrim (Jan. 2009)
3- Development of the CFNOC CTC vision
4- Writing of the Vision document

Cyber Threat Center (CTC) – The Vision

1- Introduction; Methodology



Cyber Threat Center (CTC) – The Vision

2- January 2009 deployment @ CFNOC

Goals

1- Understand the CFNOC organization & its teams
   - Mission, CC, operations, tools, information, int/ext collaborations, …

2- Get feedback from leading officers, analysts, technologists, …
   - Vision, tasks, current problems, needs, elements of solution, …

3- Start to integrate this information

Cyber Threat Center (CTC) – The Vision

2- January 2009 deployment @ CFNOC; Framework

		A	B	C	D	E	F
		The "What"	The "How"	The "Where" & "connectivity"	The "Who"	The "When"	The "Why"
1	**Scope (Contextual) (Planner)**	Important "objects" to CFNOC	Used "processes"	"Locations" in which the CFNOC will operate	"Living entities" important to CFNOC	"Events/cycles" significant to CFNOC	"Goals/mission" CFNOC
2	**Business mdl (Conceptual) (Owner)**	Conceptual or semantic model (CARE Lab)	Business process model (CARE Lab)	Business logistics (CARE Lab)	Work flow model (CARE Lab)	Master schedule (CARE Lab)	Business plan (CARE Lab)
3	**System mdl (Logical) (Designer)**	Logical model (CARE Lab)	Application architecture (CARE Lab)	Distributed system architecture (CARE Lab)	Human interface architecture	Processing structure (CARE Lab)	Business rule model (CARE Lab)
4	**Technology mdl (Physical) (Builder)**	Physical model (CARE Lab)	System design (CARE Lab)	Technology architecture (CARE Lab)	Presentation architecture (CARE Lab)	Control structure (CARE Lab)	Rule design (CARE Lab)
5	**Detailed representations (Sub-contractors)**	Objects definition (CARE Lab)	Program, process (CARE Lab)	Network architecture (CARE Lab)	Security architecture (CARE Lab)	Timing definition (CARE Lab)	Rule specification (CARE Lab)
6	**Functioning**	Object	Function, capability, strategy	Network	Organization units	Schedule	ConOps, strategy

Some errors must be corrected in this figure

Cyber Threat Center (CTC) – The Vision

2- January 2009 deployment @ CFNOC

Types of questions that were asked to CFNOC people:

- What is the **mission** of your team?
- Please describe your **tasks** @ CFNOC?
- Would you show me some current **security cases** & related documents
- What **tools** (hardware, software, information, others …) are you using?
- Are there any **problems** that limit your work (or impact deliverables)?
- What **needs** can you identify from your position?
- Do you have any **elements of solution** to suggest?

Cyber Threat Center (CTC) – The Vision

2- January 2009 deployment @ CFNOC

→The CFNOC CTC Vision: main points

- CFNOC CTC will be a **recognized cyber threat center**
  - Pool of well trained analysts (military and civilian people); continuity…
  - 24/7 mode of operation (where necessary)
  - IR: (1day;1st response)→(1 week; deeper an.)→(2 weeks; complete/deep an.)
  - Poll of external partners having complementary expertise

- **Focus and types of CNO**
  - Wired & wireless DND networks and activities (hardware, software & data)
  - **Passive CND**: IDS, IR, forensics analysis, malware & VA + remediation, technology/malware/Internet watch, blue/red teaming; quickly reproduce DND networks & simulate/test/PenTest, special ops & special deployments in theatres
  - **Proactive CND** (see Vision document)
  - And eventually **CNA** if GoC policies allow it

- **CFNOC CTC Vision** integrates people, SOTA tools, information, knowledge, expertise, processes, even working spaces, …

Cyber Threat Center (CTC) – The Vision

2- January 2009 deployment @ CFNOC

➔Needs: main points (1/2)

- Confirm **CFNOC's mission** in function of:
  current and future GoC policies (current work; M. Bergeron)
- Liaise with other **governmental orgs** (is there a National cyber protection endeavor?)
  Ex: 76 Comm Sqn
- Identify needed **external partners** and define **collaboration processes**
  Ex: CSEC, RMC, DRDC, RCMP, many other important orgs
- Strong **support** from high-level management
  1) Mission definition; 2) $ & H.R. to build/maintain the CFNOC CTC
- **Keep up to date** internal processes, equipment, information, infrastructure
  Security tools (hardw/softw), information (tech. spec.), working space, …
- **Capture & keep up to date** (in a central repository) the knowledge @ CFNOC
  Make it available to appropriate people with appropriate permissions
- Improved means to **share the situation awareness internally**

Cyber Threat Center (CTC) – The Vision

2- January 2009 deployment @ CFNOC

➔Needs: main points (2/2)

- CFNOC needs an appropriate number of **qualified people** (Mil./Civ.)
  Minimum knowledge & ability in Computer sciences
- **Strategic training plan** (and means) are needed as well
  Strategic because: consider people, operations, constraints, …
- Keep **newly posted people** more than 2 or 3 years (4 years minimum)
  Hire civilians and involve reservists (insure continuity of CTC services)
- Security cases attributed to people (notion of **responsibility**, commitment, …)
- A **strategy** for the building, maintenance and evolution of the CFNOC CTC
  ➔Passive CND: the current activities (see the Vision document)
  ➔Proactive CND: a new kind of activities (see the Vision document)
  - CNA: if GoC policies allow it

Cyber Threat Center (CTC) – The Vision

5 envisioned capabilities

Struct.: 1st, 2nd, 3rd line

RE & Related advanced analyses

Internet, Malware & Techno Watch

Integrated capabilities

Passive & Proactive CND

Capture & Legal evidences analyses

Full description in the Vision document …

Capture of knowledge & Strategic training

Cyber Threat Center (CTC) – The Vision

4- The Vision document (DRDC TM 2009-61): TOC

1- CFNOC's mission(s)

2- Proposed strategy for the development of the CFNOC CTC

- ➔Short-term: Passive CND
- ➔Mid-term: Proactive CND
- Long-term: CNE & CNA if GoC policies allow it

3- Description of needed capabilities

1- **RE and similar advanced analysis**
2- **Capture of evidences and cyber forensics analysis**
3- **Passive and proactive defensive measures**
4- **Capture of knowledge and strategic training**
5- **Threat, technology and Internet watch**

4- Concrete development plan

A 4-phase S&T project (TDP ??); aims to implement the strategy (2)

Cyber Threat Center (CTC) – The Vision

5- Conclusion

We have the vision, so what is next?

1- **Identify & describe current (and future) capability gaps**

Consider evolution of CFNOC's mission & GoC policies

2- **Prioritize solution options** (from the Vision document & others)

3- **Identify a strategy for building & maintaining the CFNOC CTC**

Consider selected options & proposed strategy

Consider constraints (availability of resources, GoC policies, …)

Identify & involve potential partners

4- **Prioritize actions**

High-level management, CFNOC and its partners

Cyber Threat Center (CTC) – The Vision

Many documents were consulted:

- **CFNOC**: CONOPS (CFNOC, NAT, AAT, CND-Troops, …), past & current security cases
- **NIST:** (many good documents to be utilized @ CFNOC)
- **Government of USA**: DoD, Homeland Security, recommendations for President, others…
- **GoC**: Treasury board of Canada (Proactive cyber defence)
- **Security organizations**: SOPHOS, McAfee, Symantek, Cigital, Kapersky, IBM, ESDA, Gartner, VisionGain, C-SAFE, …
- **Books & papers**: Cyber forensics, RE, cyber threats, vulnerability, security tools, cyber attack tools, …
- Others

➔The complete list will be available in the Vision document