SL 2009-342

53-738

DEFENCE R&D DÉFENSE

Content

1. Challenges and context
2. Poly-Tracing project
3. Poly-Tracing & redundancy – C2 Ops
4. Poly-Tracing & redundancy – Cyber security
5. Poly-Tracing – Software analysis
6. Concluding remarks

1- Challenges and context

The Cx of our C2IS will continue to grow in the future

These C2IS are connected to networks such as Internet…

Debugging is much more harder (multi-core, multi-level, …)

Traditional security frameworks are not sufficient

Solution put forward aims to improve significantly the availability, reliability, performance & security of C2IS

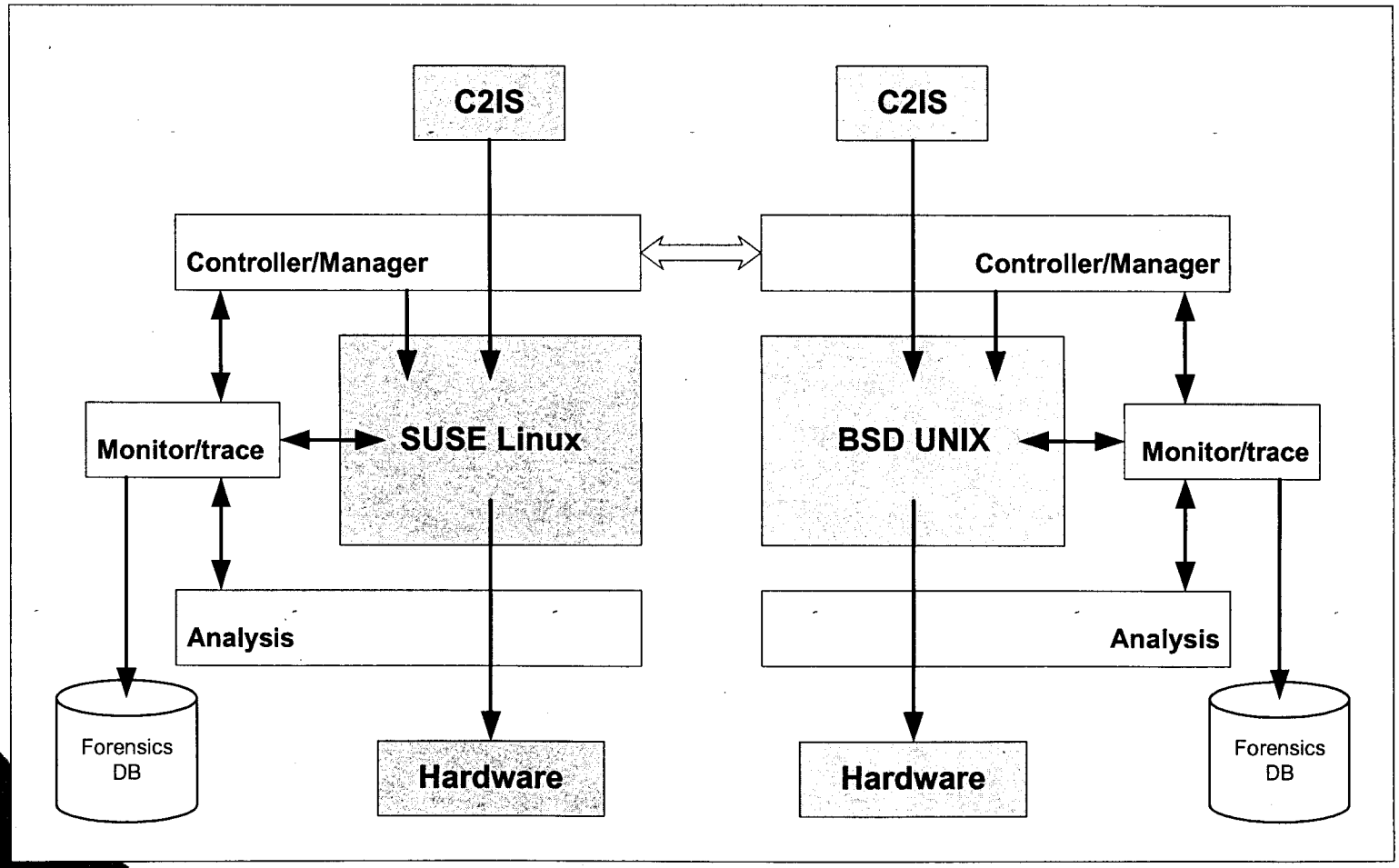
➔ R&D Project: **Poly-Tracing** (started last April)

➔ Highly qualified participants

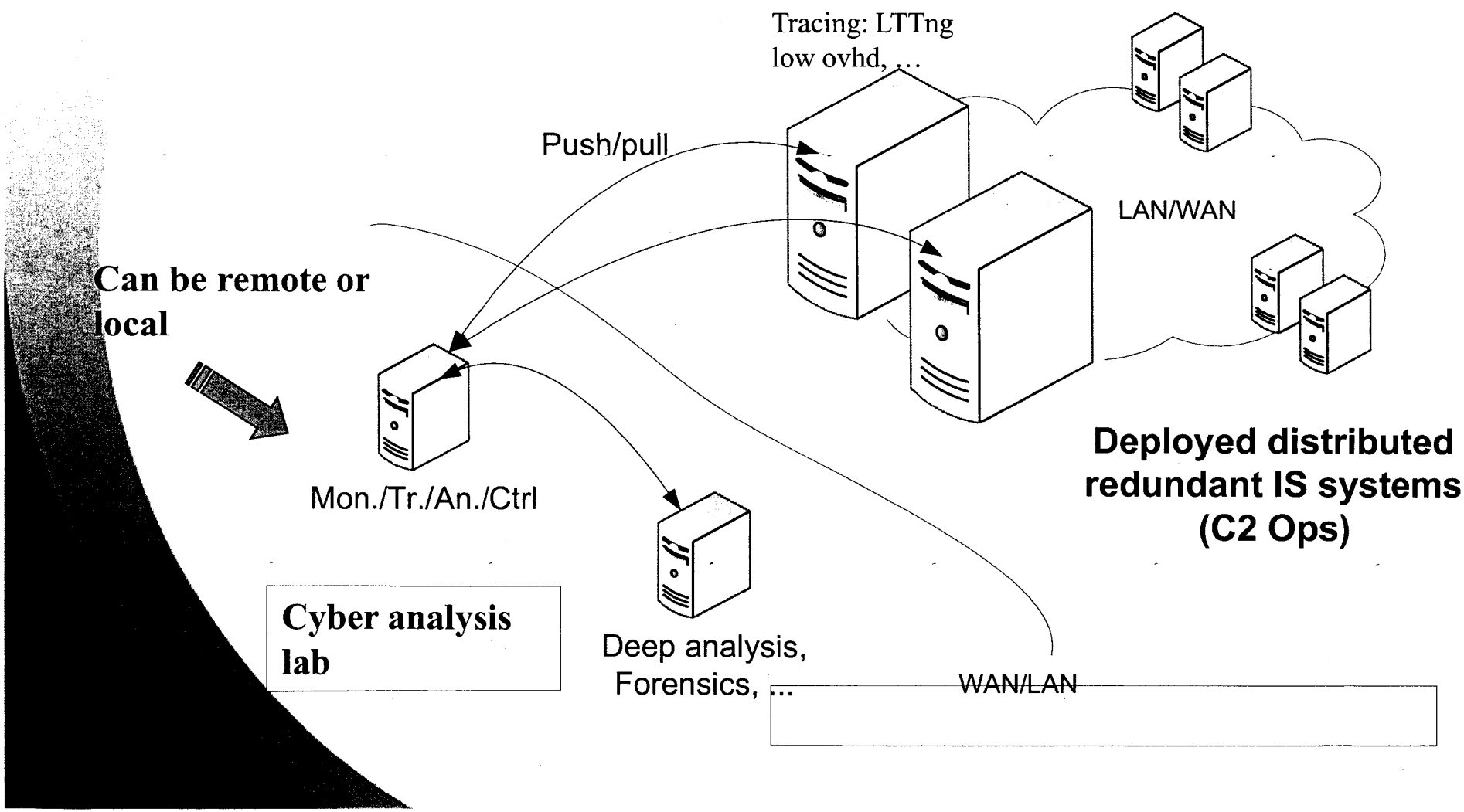
➔ 3-to-1 leverage: **NSERC** + **Ericsson** + **DRDC**

2- Poly-Tracing project – Vision

WBE 1: **Monitor, trace, analyze & control systems**
WBE 2: **Add redundancy and diversity in architectures**



2- Poly-Tracing project – A typical configuration



2- Poly-Tracing project – R&D threads

WBE 1: Monitoring/Tracing of multi-core systems

1- Adaptive fault probing (LTTng, LTTV in Eclipse)
2- Multi-level, multi-core distributed traces synchronisation
3- Trace abstraction, analysis and correlation
4- Automated fault identification
5- System health monitoring and corrective measure activation
6- Trace directed modelling

WBE 2: Software redundancy for cyber attack resistance

1- Conduct the review of current works and literature (state of the art)
2- Define a theoretical framework allowing the formal conception, validation and development of redundant architectures in function of specified constraints
3- Design and validate a redundant information system that is optimized for cyber attack resistance

3- Poly-Tracing & redundancy – C2 Ops

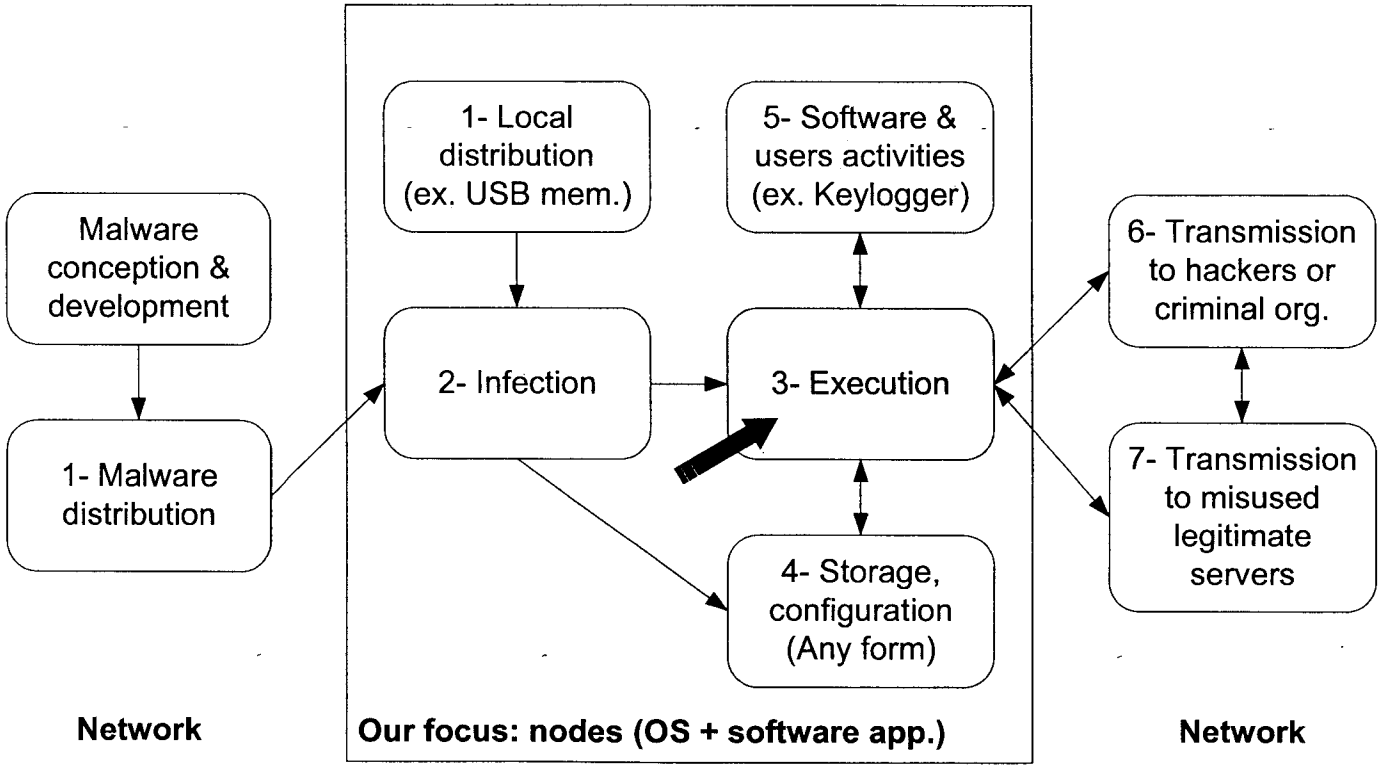
Online, in operations:

- Feedback-directed diagnostic & control
  - Control tracing probes (focus & resolution)
  - Comparison/analysis of abstracted execution traces
  - Activate corrective measures

- Redundancy & diversity – A security layer on top of the traditional security framework

4- Poly-Tracing & redundancy – Cyber security

Stages of typical cyber attacks



5- Poly-Tracing – Software analysis

Offline, in laboratory (combined with other types of analysis)**:**

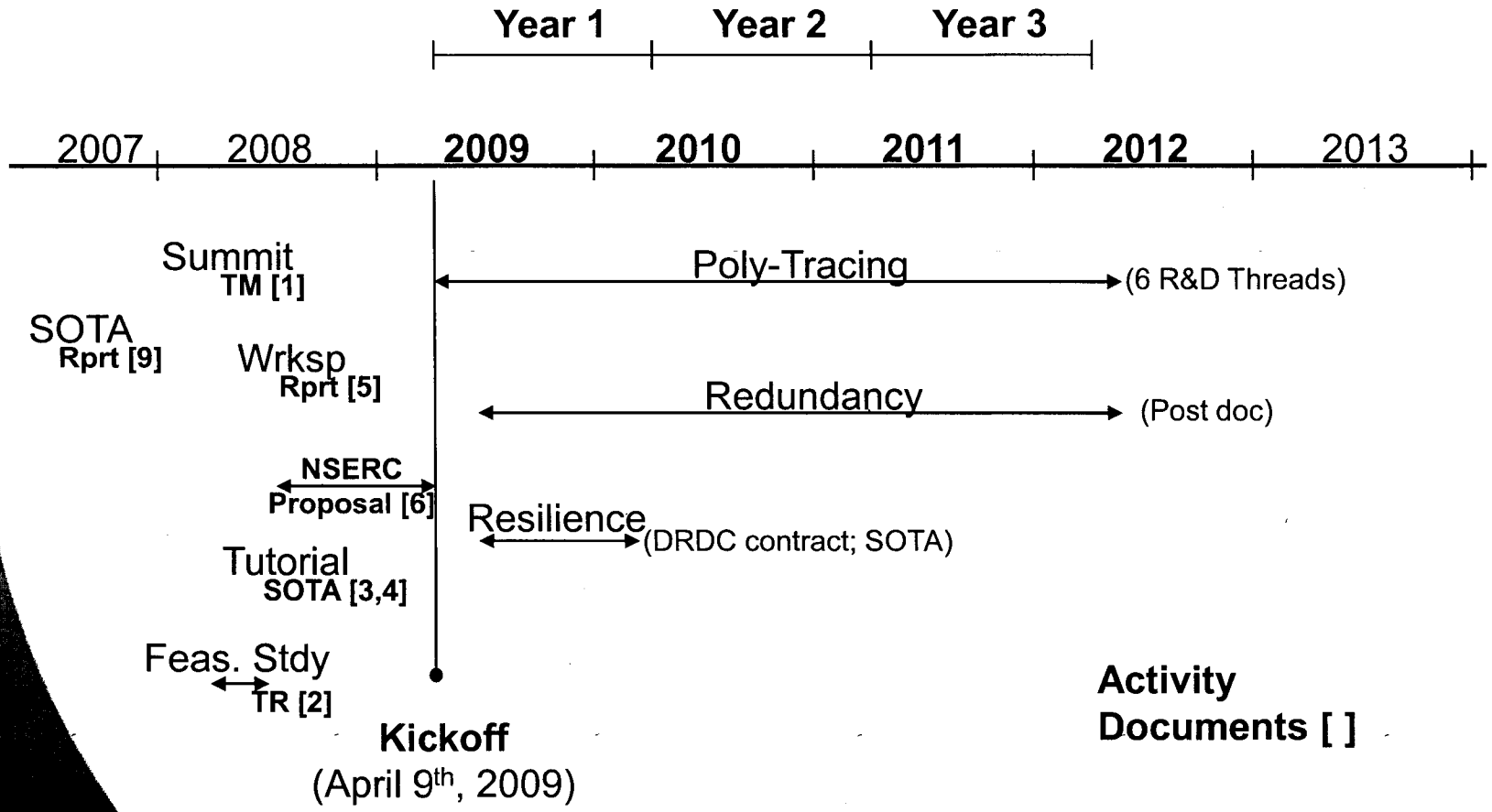
- Software debugging (distributed, n-core and n-level systems)
- Analysis of software & malware (in a sand box)
  - Behaviour analysis
  - Impact analysis (in the user space and kernel space)
- Forensic analysis

6- Concluding remarks

- **Demonstrations will be held at the end of the project**
  ~ Spring 2011 & Autumn 2012
- **Your input & participation is welcome**
  - **Classified or not**
  - **No cost**, the project is already financed

Mario Couture or Robert Charpentier
(418) 844-4000 (4285)
Mario.Couture@drdc-rddc.gc.ca
Robert.Charpentier@drdc-rddc.gc.ca

Poly-Tracing project – Activities



References

[1] Couture et al., 2008a. Monitoring and Tracing of Critical Software Systems - SOTA, DRDC Valcartier TM 2008-144, June 2008.

[2] Couture et al., 2008b. Tracing, Monitoring and Analysis of distributed Multi-core Information Systems - Selected Feasibility Studies, DRDC Valcartier TR 2008-300, November 2008.

[3] Dagenais et al., 2008a. State-Of-The-Art Tracing and Monitoring Multicore Execution, Polytechnique Montréal, November 2008.

[4] Dagenais et al., 2008b. State-Of-The-Art Tracing and Monitoring Multicore Execution. Tutorial given at Bell Centre Ottawa on November 2008 to 25 key people from DND

[5] Charpentier & Dagenais, 2008. Rapport d'atelier stratégique CRSNG, STPWS 364780-08, July 2008.

[6] Dagenais et al., 2008c. Tracing and Monitoring Tools for Distributed Multi-Core Systems, NSERC 90429374, July 2008.

[7] LCol Jackson DIM Secur, 2008. Support letter -Multicore Tracing Project, February 2008.

[8] Heikkila & Gulliksen, 2007. Multi-Core Computing in Embedded Applications, VDC Market Research, September 2007.

[9] Kienzle et al., 2007. Survivable Service-Oriented Computing Systems for Hostile Environments, McGill University, October 2007.