DEFENCE R&D DÉFENSE

Defence Research and Development Canada

Cyber surveillance of information systems

Results from the current DRDC project, and way-ahead
(Tutorial/workshop)

Mario Couture
DRDC Valcartier (SoS/SAR)

March 8th, 2011

Contents

1. Definitions and work domains
2. Important facts
3. Cyber warfare – The need for new technologies
4. Current DRDC efforts – “Observe”
5. Next DRDC efforts – “Orient”
6. Concluding remarks

Definitions and work domains

Information system (IS):

- A "computerized system" allowing the *processing and sharing* of data and information
- With this *generic definition*, a cell phone can be considered as an IS

Surveillance of information systems:

- The use of specialised software systems (AV, HIDS, software tracers, etc.) for the *observation* and *analysis* of states and behaviours that are found within the IS
- Surveillance ➔ during operations, autonomous/manual, locally/remotely controlled
- The goal is to detect all anomalies in the IS and report/act appropriately

Work domains:

- DRDC Valcartier (SoS) ➔ *surveillance of hosts*
- DRDC Ottawa (NIO) ➔ surveillance of networks

} Collaborative work

AV: Antivirus
HIDS: Host intrusion detection system
IS: Information system

Important facts

Some important facts [**Charpentier & Lefebvre, 2010**]**:**

- Critical national infrastructures involve the use of increasingly complex ISs
- Fielded ISs will always contain unresolved design flaws & bugs (potential vulnerabilities)
- Nowadays bad hackers are very well organised and they have easy access to advanced hacking technologies (which are very cheap)
- The ability of current surveillance systems (AV, HIDS, …) to detect undesired software states and behaviours within hosts is dramatically limited: ~30% [Bell, 2010].

  – *The improvement of the dependability of ISs during operations is a complex problem*

  – *Sustained major iterative and incremental collaborative R&D efforts are needed*

The DRDC projects described today are examples of such DRDC efforts for DND

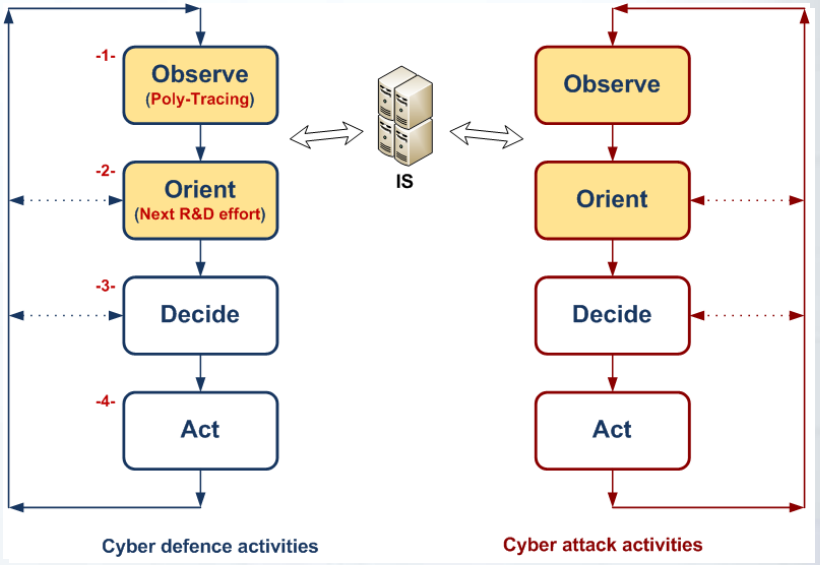
AV: Antivirus
HIDS: Host intrusion detection system
IS: Information system

Cyber warfare – The need for new technologies

Cyber warfare involves two well organised entities:
DND and ***bad hackers***

OODA Loop; in the case of *host surveillance*:
-Observe: observations deep within the IS
-Orient: fast/advanced analysis, adapted reporting
-Decide: automatic/manual decision processes
-Act: automatic/manual reactions and pro-actions

Some important needs:
-Better advanced techniques and models:
-for adaptive observation of hosts
-for adaptive data abstraction, fusion, analysis
-to lower the number of false positives
-Better reporting of:
-IS's health states
-detected undesired behaviours, states, anomalies
-Suggest to officers on duty the best courses of actions
-Very small overall "delta-t" (of the whole blue OODA Loop)



DND activities

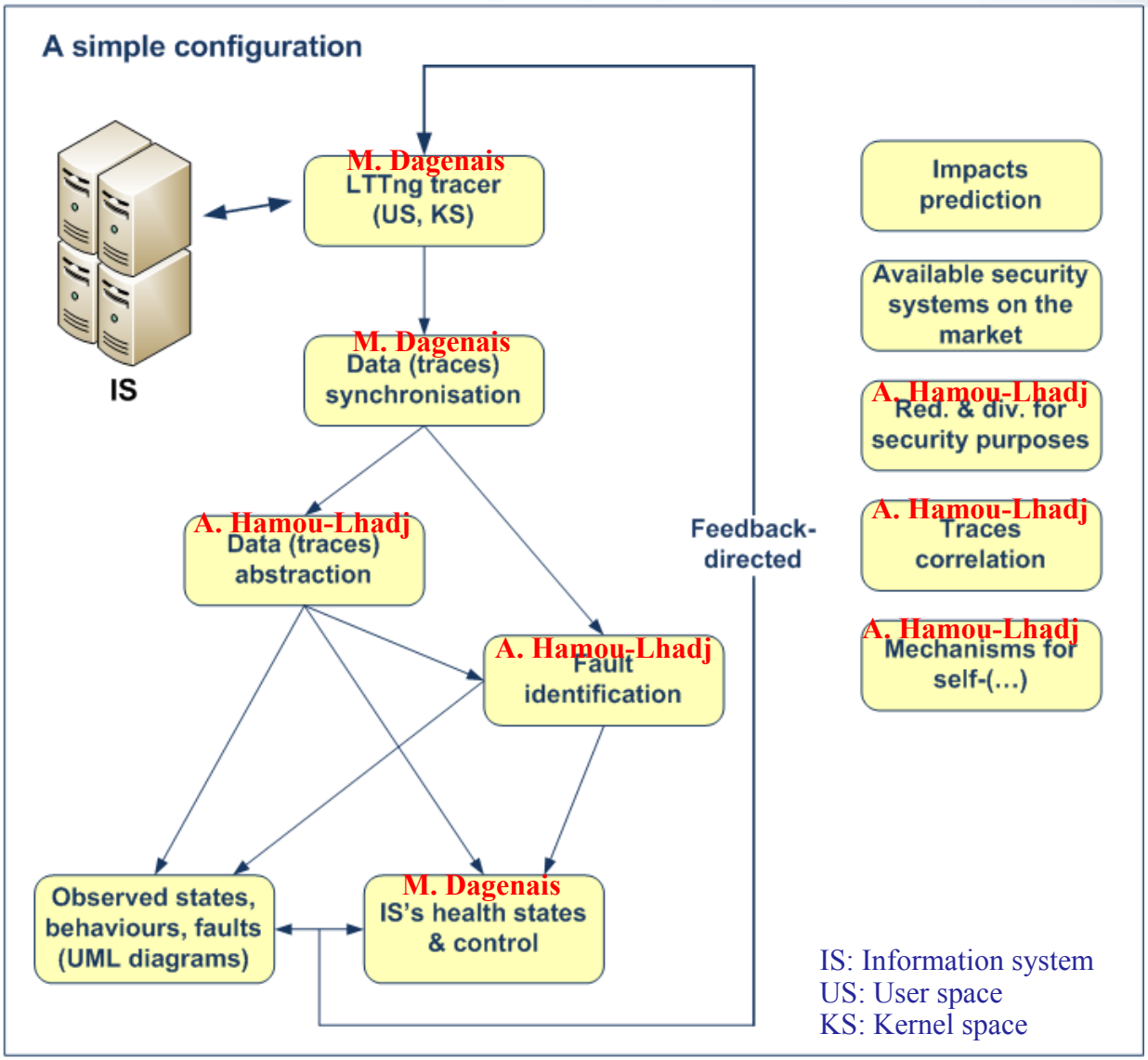
Bad hackers activities

-Well organised
-Easy access to hacking technology
-(…)

Current DRDC efforts – "Observe"

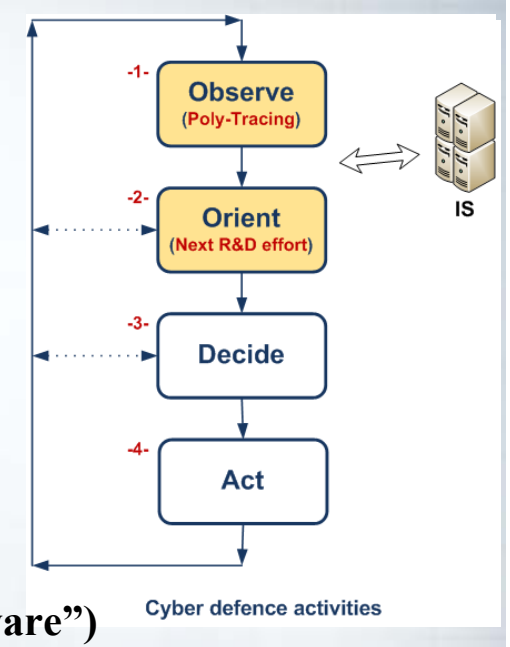
R&D threads in the Poly-Tracing project ("Observe")

- Automatic/manual deep monitoring of ISs
- Data synchronisation
- Data abstraction
- Automated fault identification
- Health monitoring and corrective measures
- Trace directed modelling
- Impacts prediction (of monitoring)
- Redundancy and diversity for security purposes
- Security systems currently available on the market



Self-(…): resilience, self-adaptation, self-healing, …

Next DRDC efforts – "Orient"



Based on Poly-Tracing results, push further R&D efforts to:

➔ **Improve significantly efficiency of the "Orient" activities**🡐

Some important needs:

- **New paradigm: consider the *health states of ISs***
- **Consider *all kinds of anomalies* in the IS (not limited to "known malware")**
- New highly-efficient **techniques** and **models** for:
  - Quasi real-time analyses, alarms management, elimination of false positives
  - Identification of COAs (automatic/manual, reactive/pro-active)
  - The resilience, self-adaptation, and self-healing of ISs (i.e. redun. & diversity in arch.)
- Integrate available efficient surveillance systems (AV, HIDS, …) from the market
- **Help officers on duty build and maintain HSA of ISs during operations**
- **Full interoperability with network surveillance systems (push/pull modes)**

➔**The next DRDC project is currently under definition**🡐

AV: Antivirus
HIDS: Host intrusion detection system
HSA: Host-based situation awareness
COA: Course of actions
IS: Information system

Concluding remarks (I)

Poly-Tracing & redundancy-diversity (on-going):

- A 3-year DND-NSERC project; 2.6 M$
- 3 partners: DRDC, Ericsson, NSERC
- 5 PhDs, more than 15 graduate students, Post-Docs
- At Valcartier: DSs, Post-Docs, DRDC contracts

Preliminary studies for the next DRDC project

- Additional 220 k$ (financial support: DRDC)

Next DRDC projects (will be submitted September 2011):

- Type: DND-NSERC project (academic and industrial orgs are very interested)
- Size: similar to Poly-Tracing

Concluding remarks (II)

Goals of this event:

- Inform attendees of recent technological advances in the domain of host surveillance (Poly-Tracing; “Observe”)
- Present elements of information of the future DRDC project (“Orient”)
- Important: *capture attendees’ feedback* (*only unclassified matter*):
  - Current operational and technological problems and needs
  - Current efforts to find new technological solutions
  - Recommendations for future DRDC projects

Please note that these projects are financially supported *by DRDC* (not DND)

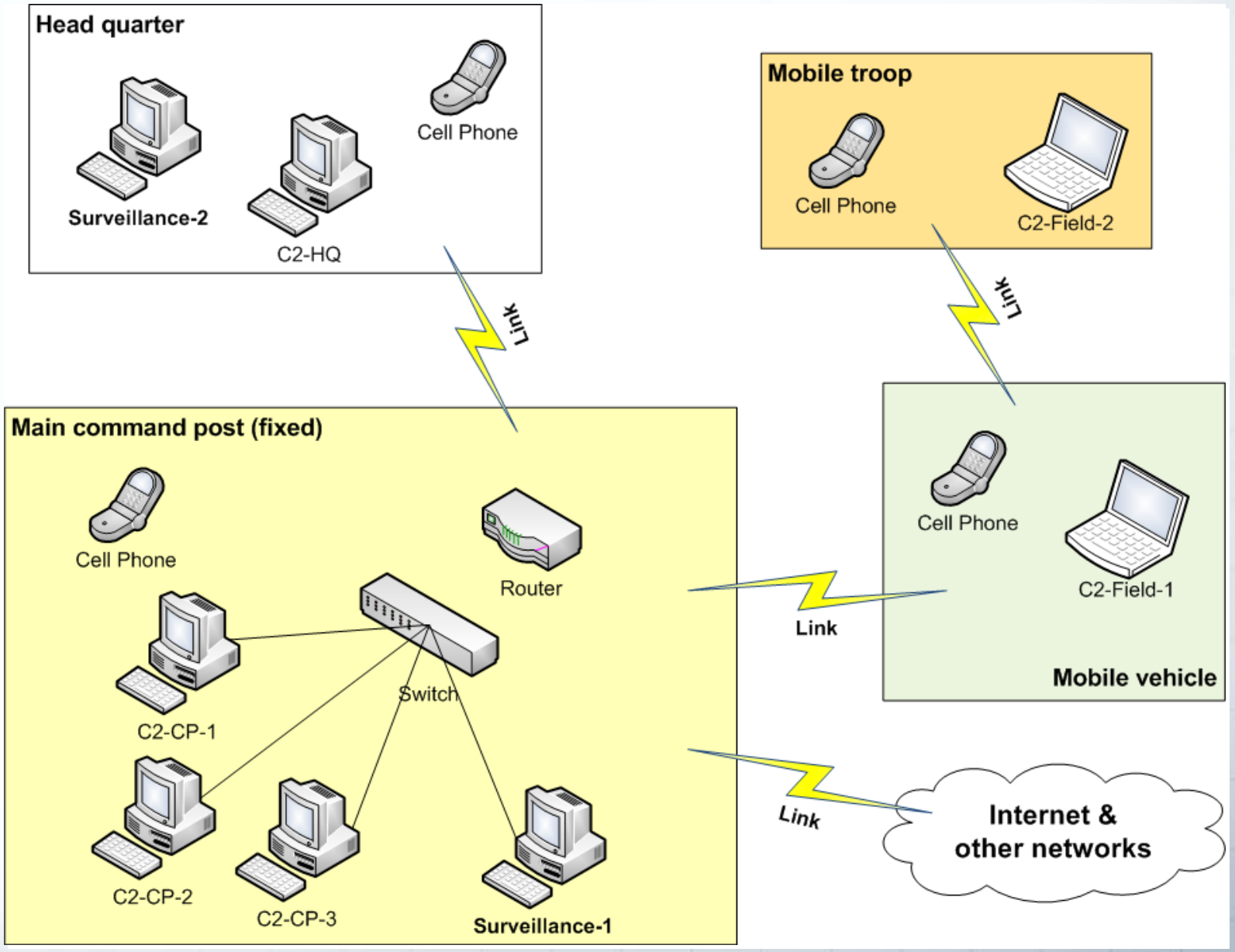
- Your feedback & recommendations will help better align future DRDC projects:
  - Address real DND technological problems (host surveillance)
  - Provide officers on duty with the tools they need to face new cyber threats
    - Malicious or not

Mario Couture

Mario.Couture@drdc-rddc.gc.ca

(418) 844-4000 4285

Extra slide


Head quarter
Surveillance-2
C2-HQ
Cell Phone
Mobile troop
Cell Phone
C2-Field-2
Link
Link
Main command post (fixed)
Cell Phone
Router
Switch
C2-CP-1
C2-CP-2
C2-CP-3
Surveillance-1
Link
Cell Phone
C2-Field-1
Mobile vehicle
Link
Internet &
other networks