Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Cyber Network Defence R&D Activities

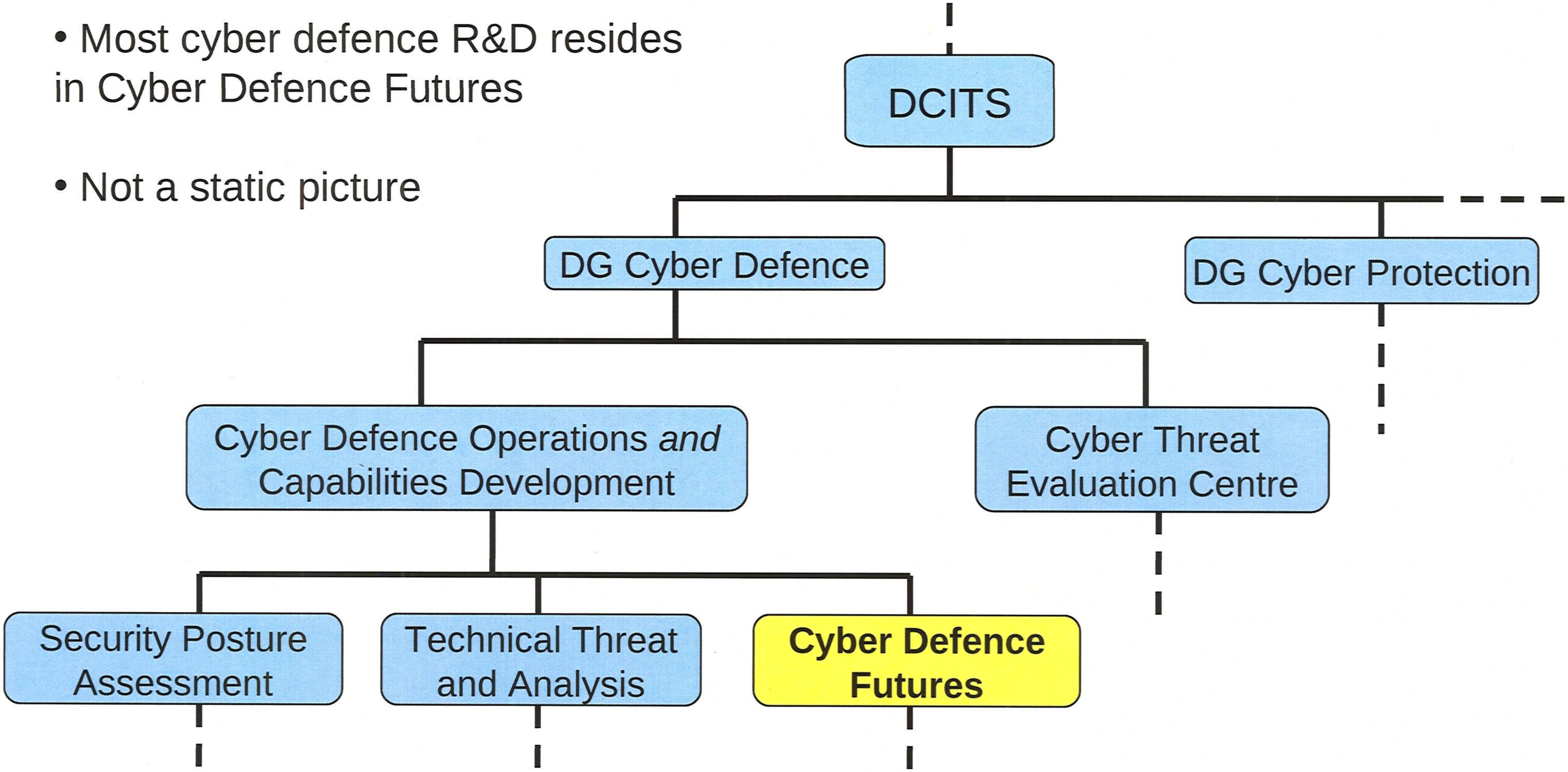
5IARC 2010

[redacted] CSEC N3C

CND R&D CSEC

- Most cyber defence R&D resides in Cyber Defence Futures

- Not a static picture



- DCITS
  - DG Cyber Defence
    - Cyber Defence Operations *and* Capabilities Development
      - Security Posture Assessment
      - Technical Threat and Analysis
      - **Cyber Defence Futures**
    - Cyber Threat Evaluation Centre
  - DG Cyber Protection

Current Focus

- Current operations are passive
  - Photonic Prism (aka P2)
    - Slipstream
    - Popquiz
    - Email attachment scanning (via Pony Express)
    - Snort
  - Host based intrusion detection
- Soon deploying dynamic defence
  - COTS hardware platform

N3 Research

- N3 is mostly a consumer of research
  - Given our resources this is an appropriate model
- Very much relationship based
  - SIGINT
  - R23
  - Defence Research and Development Canada (DRDC)
  - Royal Military College of Canada (RMC)
  - Communications Research Centre (CRC)
- Integrees
  - DRDC
  - CRC

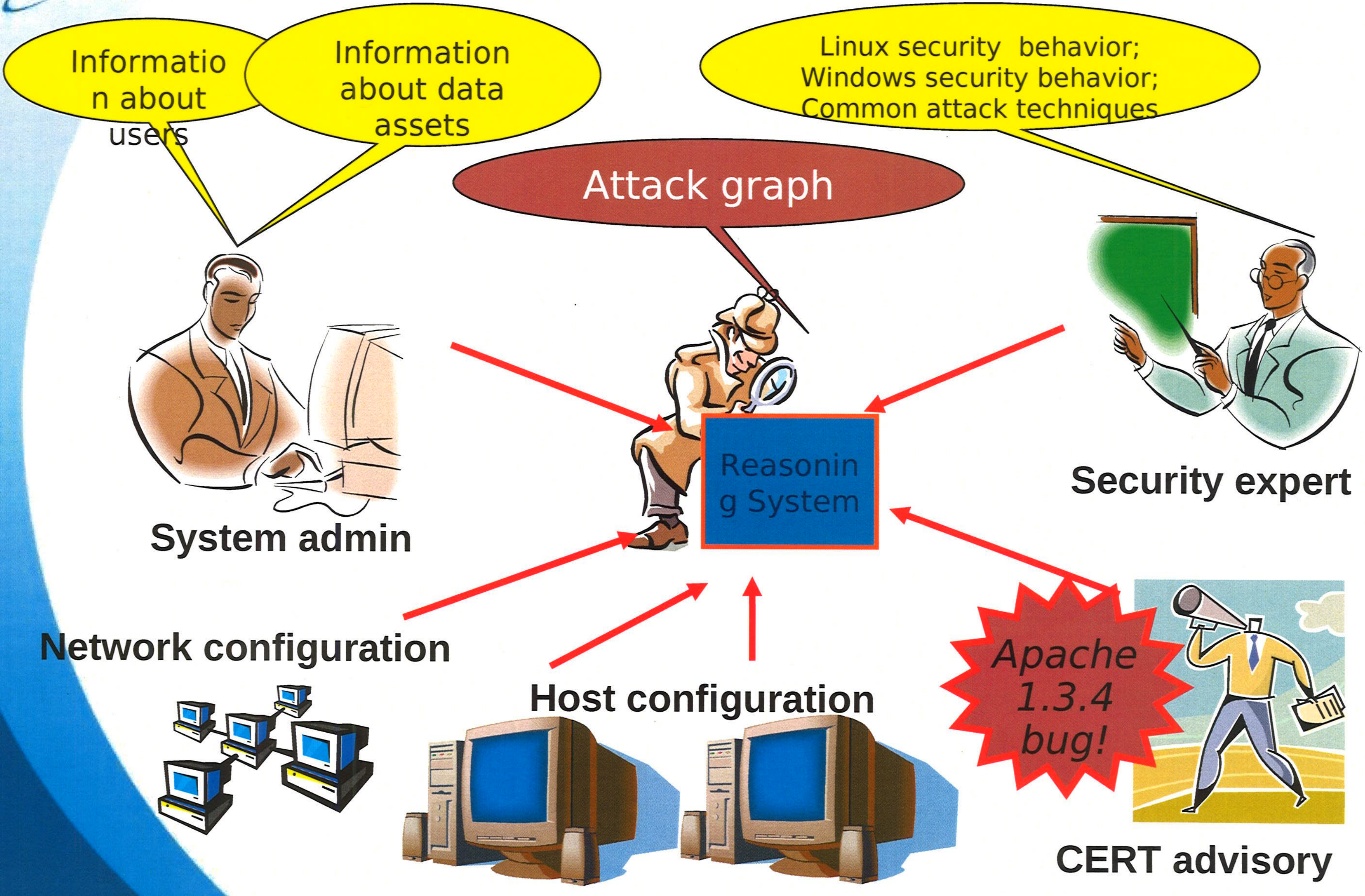
External Partners

- R23
- SIGINT
- *DRDC*
- *RMC*
- CRC

Defence Research and Development Canada (DRDC)

- MulVal + AssetRank
- Joint Network Defence and Management Systems (JNDMS)
- ARMOUR

MulVAL



Informatio
n about
users

Information
about data
assets

Linux security behavior;
Windows security behavior;
Common attack techniques

Attack graph

Reasonin
g System

System admin

Security expert

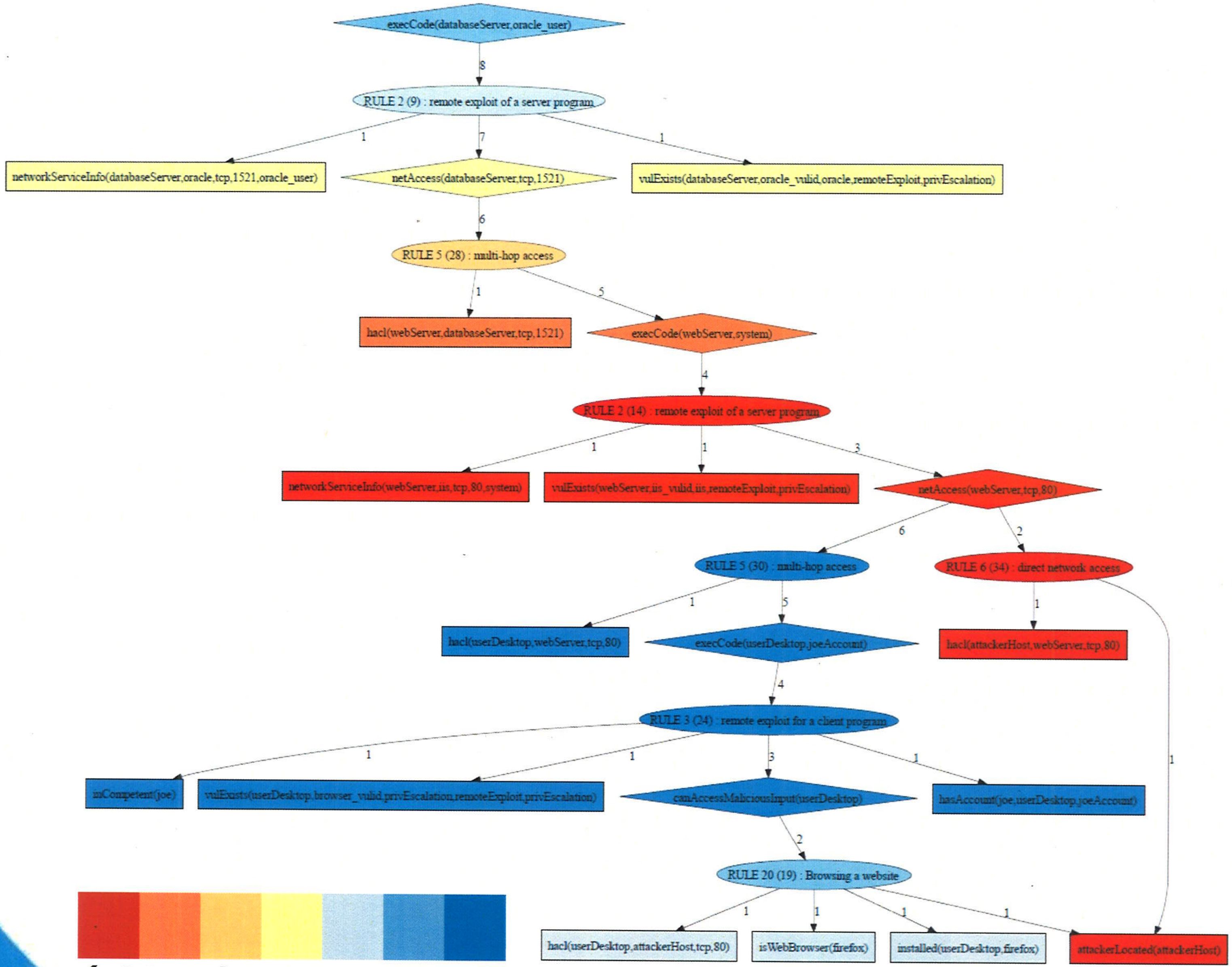
Network configuration

Host configuration

Apache
1.3.4
bug!

CERT advisory

Mulval + AssetRank ➔ Mulasses


execCode(databaseServer,oracle_user)
8
RULE 2 (9) : remote exploit of a server program
1
7
1
networkServiceInfo(databaseServer,oracle,tcp,1521,oracle_user)
netAccess(databaseServer,tcp,1521)
vulExists(databaseServer,oracle_vulid,oracle,remoteExploit,privEscalation)
6
RULE 5 (28) : multi-hop access
1
5
hacl(webServer,databaseServer,tcp,1521)
execCode(webServer,system)
4
RULE 2 (14) : remote exploit of a server program
1
1
3
networkServiceInfo(webServer,iis,tcp,80,system)
vulExists(webServer,iis_vulid,iis,remoteExploit,privEscalation)
netAccess(webServer,tcp,80)
6
2
RULE 5 (30) : multi-hop access
RULE 6 (34) : direct network access
1
5
1
hacl(userDesktop,webServer,tcp,80)
execCode(userDesktop,joeAccount)
hacl(attackerHost,webServer,tcp,80)
4
RULE 3 (24) : remote exploit for a client program
1
1
3
1
1
inCompetent(joe)
vulExists(userDesktop,browser_vulid,privEscalation,remoteExploit,privEscalation)
canAccessMaliciousInput(userDesktop)
hasAccount(joe,userDesktop,joeAccount)
2
RULE 20 (19) : Browsing a website
1
1
1
1
hacl(userDesktop,attackerHost,tcp,80)
isWebBrowser(firefox)
installed(userDesktop,firefox)
attackerLocated(attackerHost)

← More dangerous

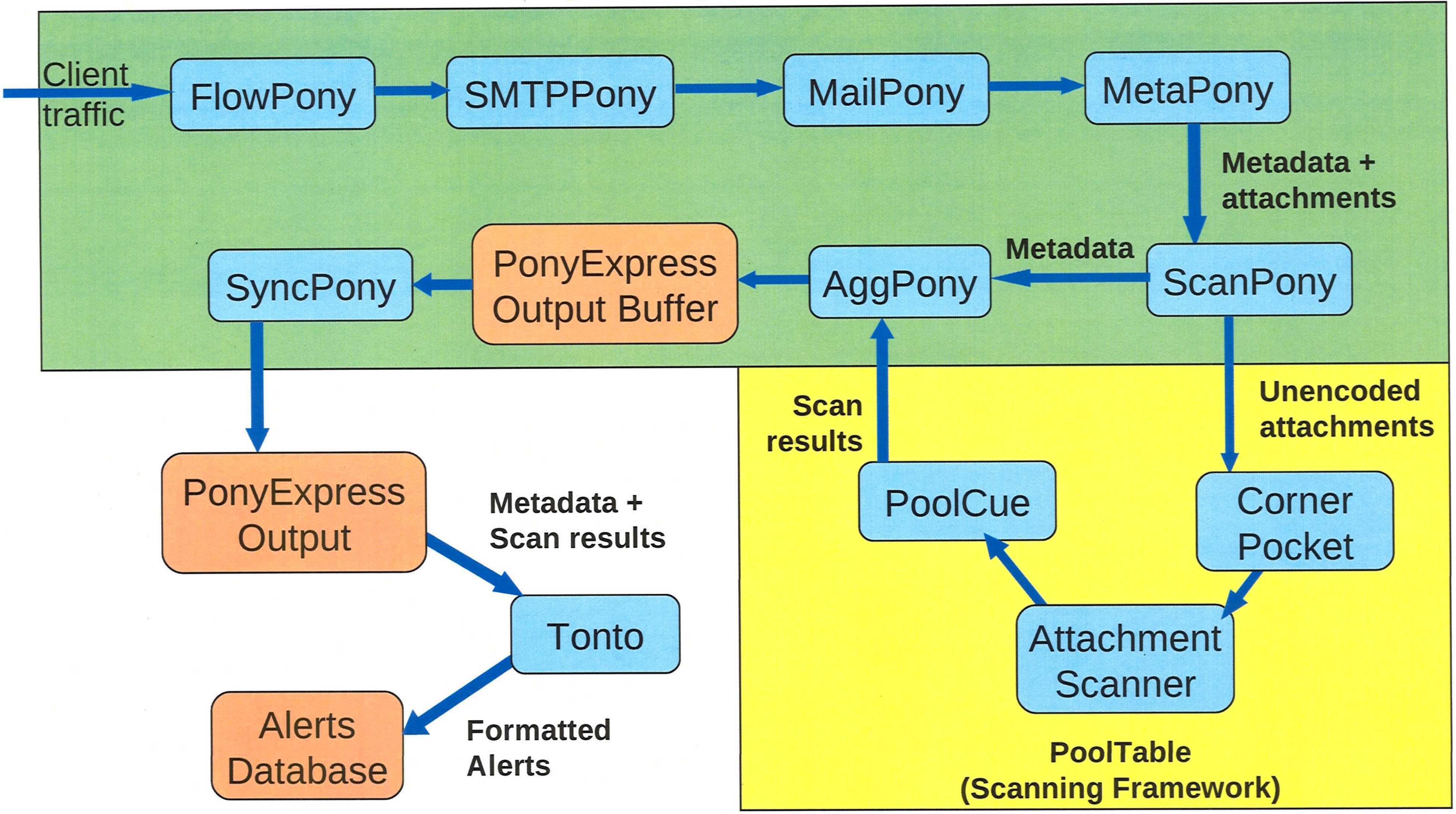
Royal Military College

- Support ~ 1 grad student per year
- Sliding Window Anomaly Detection (SWAD)
  - Models normal traffic
  - Applies the concept of hidden Markov model (HMM)
  - Used to detect covert channels

CND Development

- Mix of internal development and external collaboration
- Current CND projects
  - Some Pony Express
  - Software modules for COTS hardware (dynamic defence)
  - Streaming 10 Gb/s sensor (P2)
  - Analyst data mining tools

Pony Express



Ponies of the PonyExpress

- **FlowPony** (flowp)
  - TCP Session reconstruction
- **SMTPPony** (smtpp)
  - SMTP Parsing & Header Extraction
- **MailPony** (mailp)
  - RFC822 E-mail Parsing & MIME Attachment Extraction
- **MetaPony** (metap)
  - Evaluation & Scoring of Parsed Metadata
- **ScanPony** (scanp)
  - Analysis Pre-Processing & Scan Dispatching
- **AggPony** (aggp)
  - Scan Result Aggregation
- **SyncPony** (syncp)
  - Transfers buffered output from local disk to the SAN

Ongoing Sensor Development (Photonic Prism)

- Integration of in-house and external partner anomaly detection tools and signature based detection
  - Sliptstream
  - Popquiz
  - 8Ball
  - Snort
- Updating our sensors for multiple 10 Gb/s sources
- Moving to full streaming with full capture
- Data analysis
  - Improved analyst interface that fuse data from many sources
  - Custom GUI (based on Eclipse framework)

Ongoing Sensor Development (Photonic Prism)

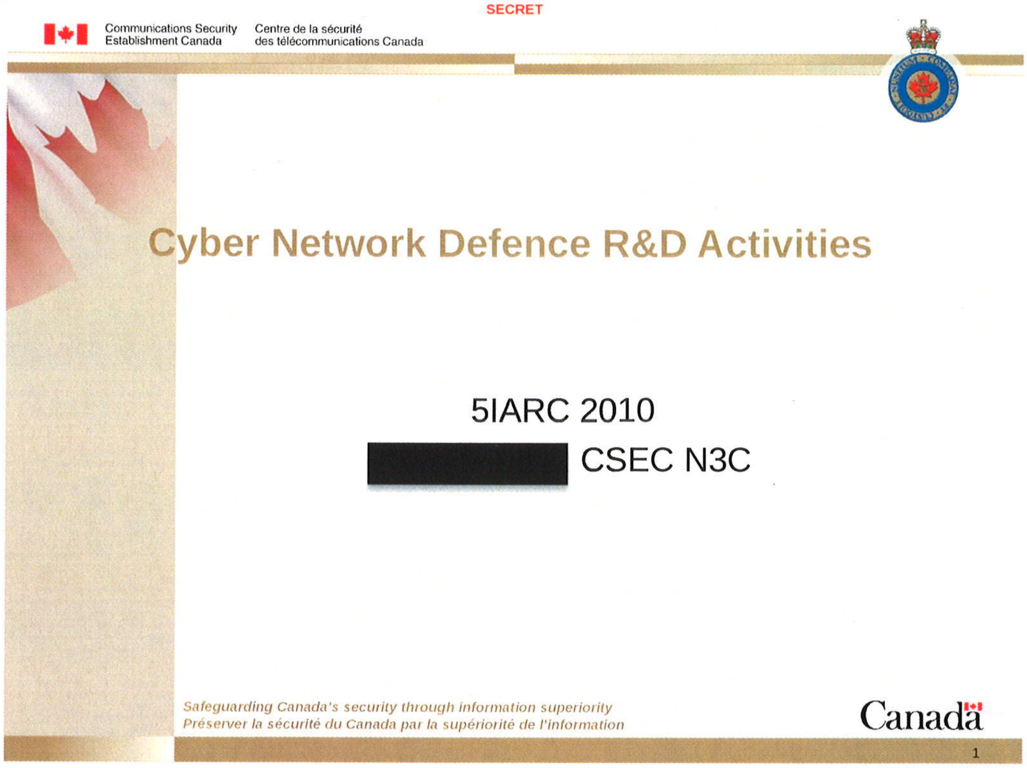
- Improved Analytics
  - Better facilities for collaboration
  - Near real time access to anomaly data
  - Improved alert/pcap performance
  - Knowledge database

Software modules on COTS Hardware (Dynamic Defence)

- Internal but close collaboration with NSA
- ~~Active~~ Dynamic defence (inline device)
- Modules for based device
  - miniSSL (passive)
  - SSLfuzzer
  - DNS
  - Data Extractor
  - Synflood
- Legal and policy work ongoing

Challenges

- Lots of standard development work to do
- Resources to pull through available research
- Length of Research Activities
- Translating classified requirements to an unclassified domain
- Properly engaging Industry and Academia
- Focusing external partners on R&D that is most valuable to us
- Policy



SECRET

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

Cyber Network Defence R&D Activities

5IARC 2010

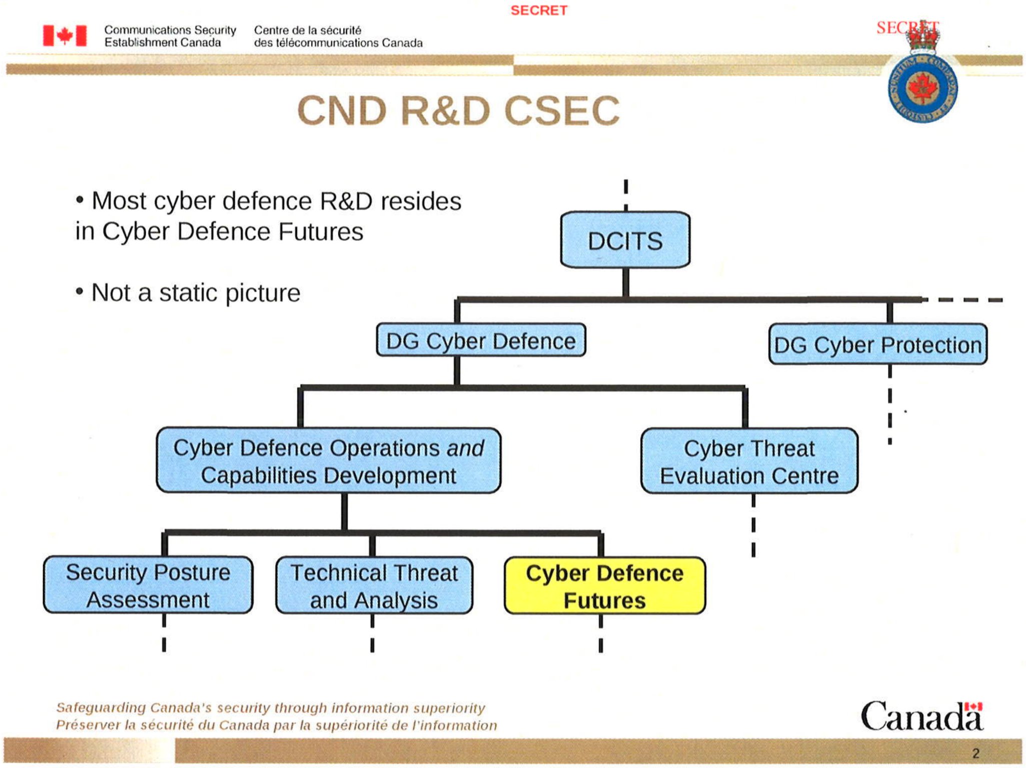
[redacted] CSEC N3C

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

1

Within the Cyber Protection Branch there is an Architecture and Engineering Directorate where most of the Research and Development Activities takes place.



SECRET

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

SECRET

CND R&D CSEC

- Most cyber defence R&D resides in Cyber Defence Futures
- Not a static picture

DCITS

DG Cyber Defence

DG Cyber Protection

Cyber Defence Operations *and* Capabilities Development

Cyber Threat Evaluation Centre

Security Posture Assessment

Technical Threat and Analysis

Cyber Defence Futures

Safeguarding Canada's security through information superiority

Préserver la sécurité du Canada par la supériorité de l'information

Canadä

2

The purpose of my talk is to characterize the R&D within CND at CSEC. I can not give a complete picture.

This is just to provide some context of where cyber defence research resides with CSEC.

This is a recent *partial* picture.

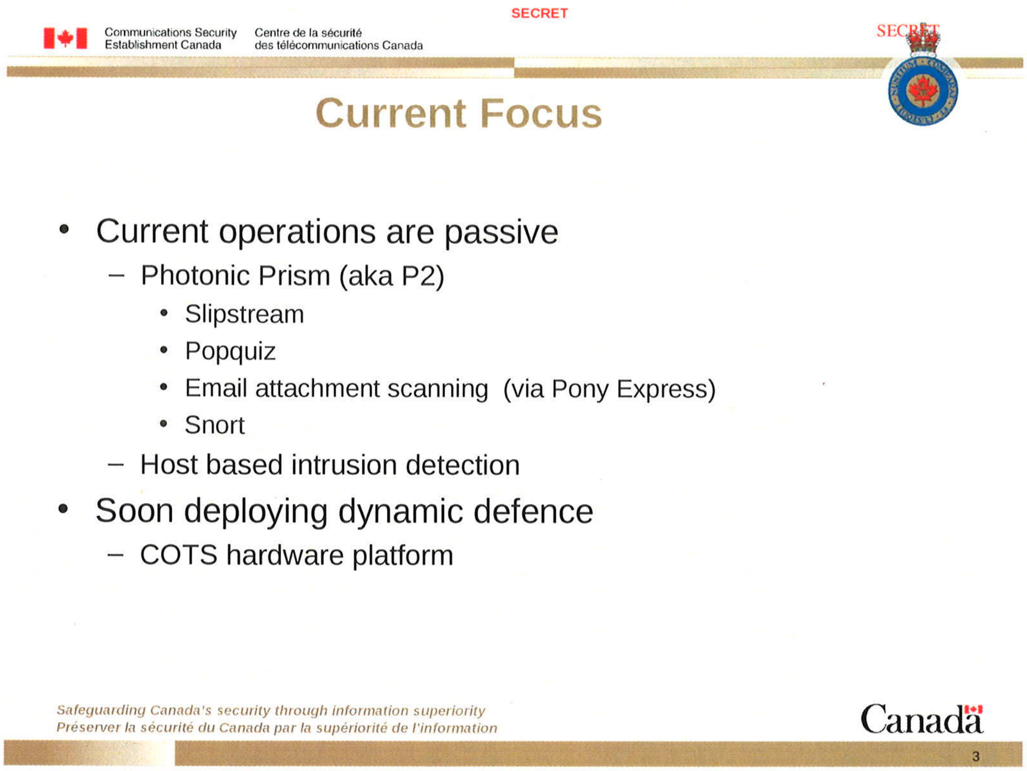
It is not static however, the org chart is evolving.

CTEC is very new and still defining its role.

Some future changes:

It is anticipated that **Cyber Defence Operations** and **Capabilities Development** will be become 2 separate directorates.

Cyber defence futures will be split into 2 sections. Eventually those sections will for the start of the Capabilities Development directorate.



SECRET

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

SECRET

Current Focus

- Current operations are passive
  - Photonic Prism (aka P2)
    - Slipstream
    - Popquiz
    - Email attachment scanning (via Pony Express)
    - Snort
  - Host based intrusion detection
- Soon deploying dynamic defence
  - COTS hardware platform

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

3

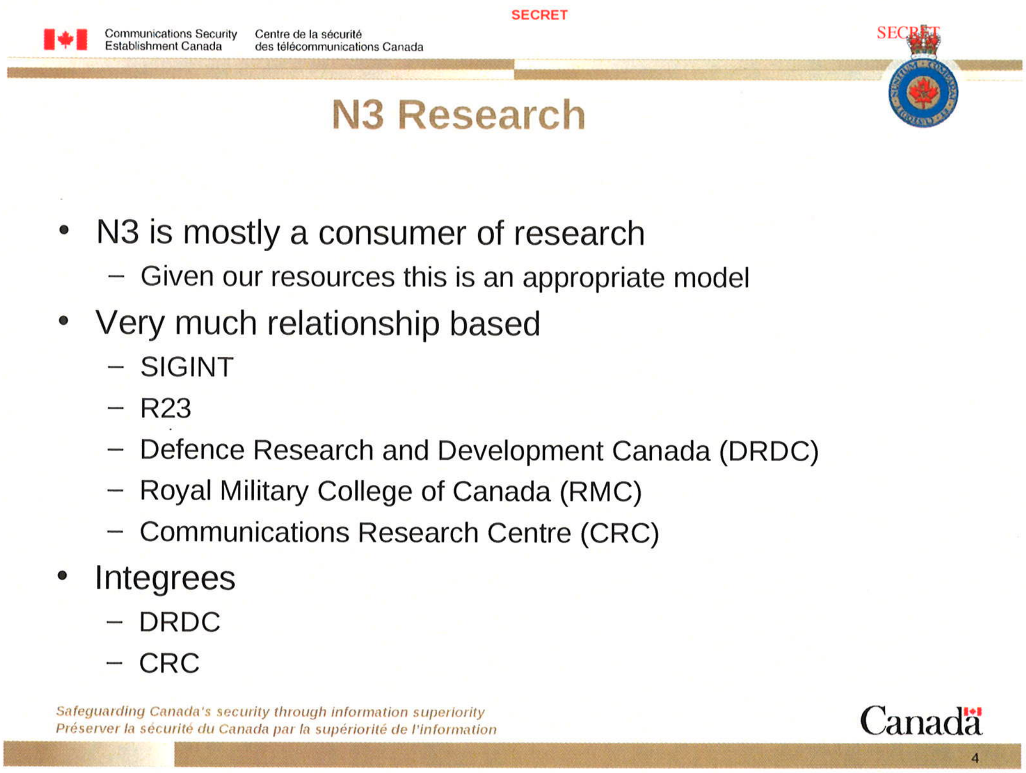
At the moment most of our efforts are on incremental improvements on the current sensor.

Making it ready for > 10 Gb/s systems and beyond.

Our detection capabilities are based on 4 frameworks:

1. Slipstream
2. Popquiz
3. Pony Express
4. Snort

We should soon have our first dynamic defence deployment.



SECRET

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

SECRET

N3 Research

- N3 is mostly a consumer of research
  - Given our resources this is an appropriate model
- Very much relationship based
  - SIGINT
  - R23
  - Defence Research and Development Canada (DRDC)
  - Royal Military College of Canada (RMC)
  - Communications Research Centre (CRC)
- Integrees
  - DRDC
  - CRC

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

4

It's difficult to speak about a research program that is virtual

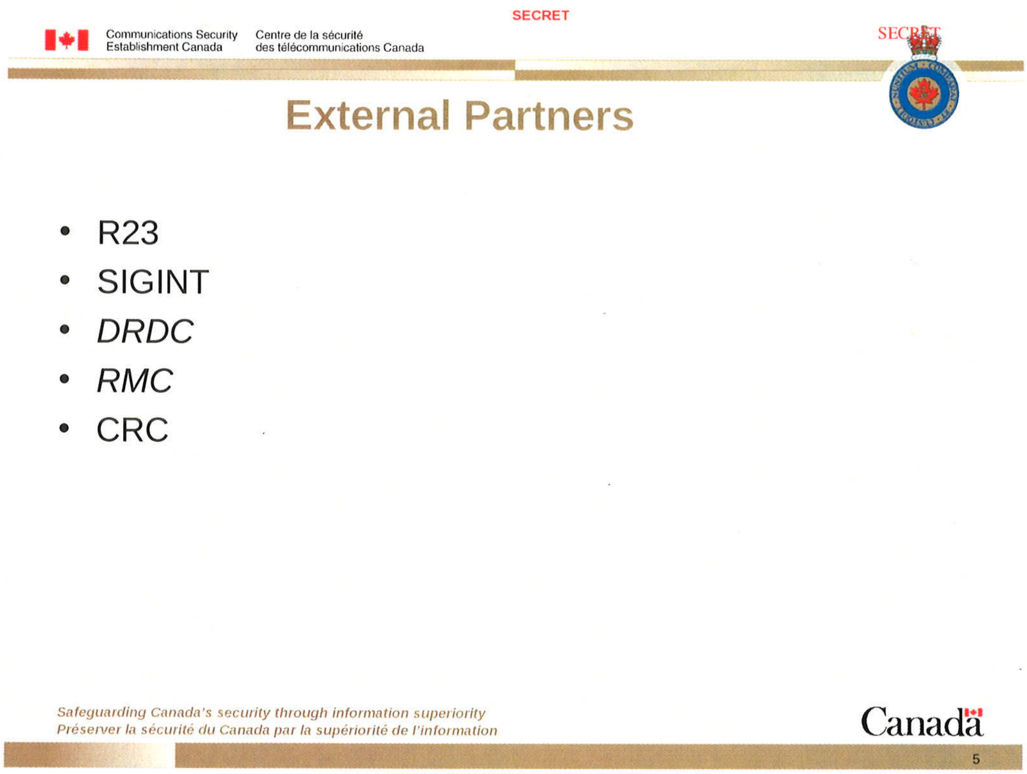
We are a small group (but growing) trying to look at a lot of data.

Given our size, our best return on investment would not come from using current resources for low level research.

It make more sense to leverage the R&D of some external partners. There is already a large body of work out there that we can benefit from before we need to push it ourselves. This means our R&D program is mostly a relationship based program.

In fact, this model has already proven to be extremely valuable via the success of popquiz developed by R23 and our email attachment scanner from GCHQ.

In between in-house and external is the use of integrees.



SECRET

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

SECRET

External Partners

- R23
- SIGINT
- *DRDC*
- *RMC*
- CRC

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

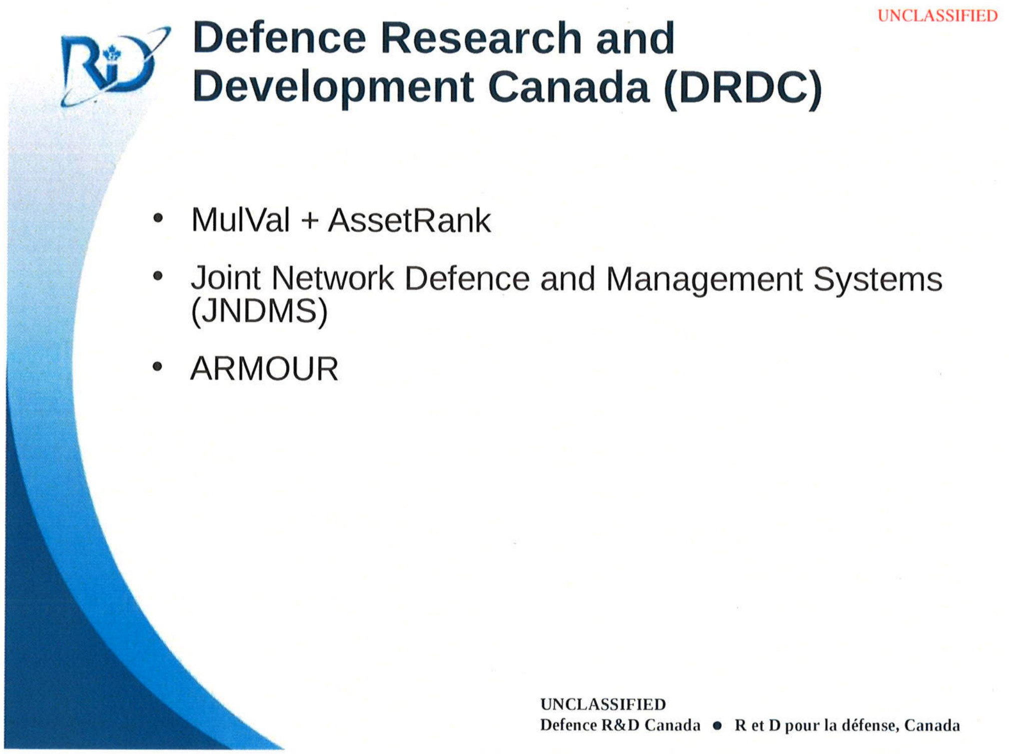
Canada

5

The next set of slides provides some overview of the research done by our external partners that we are following/tracking/consuming.

Some is in use (popquiz)
Some will shortly be in production (Popeyesear)
Many are "for the future"

Some chosen examples follow.



UNCLASSIFIED

Defence Research and Development Canada (DRDC)

- MulVal + AssetRank
- Joint Network Defence and Management Systems (JNDMS)
- ARMOUR

UNCLASSIFIED
Defence R&D Canada ● R et D pour la défense, Canada

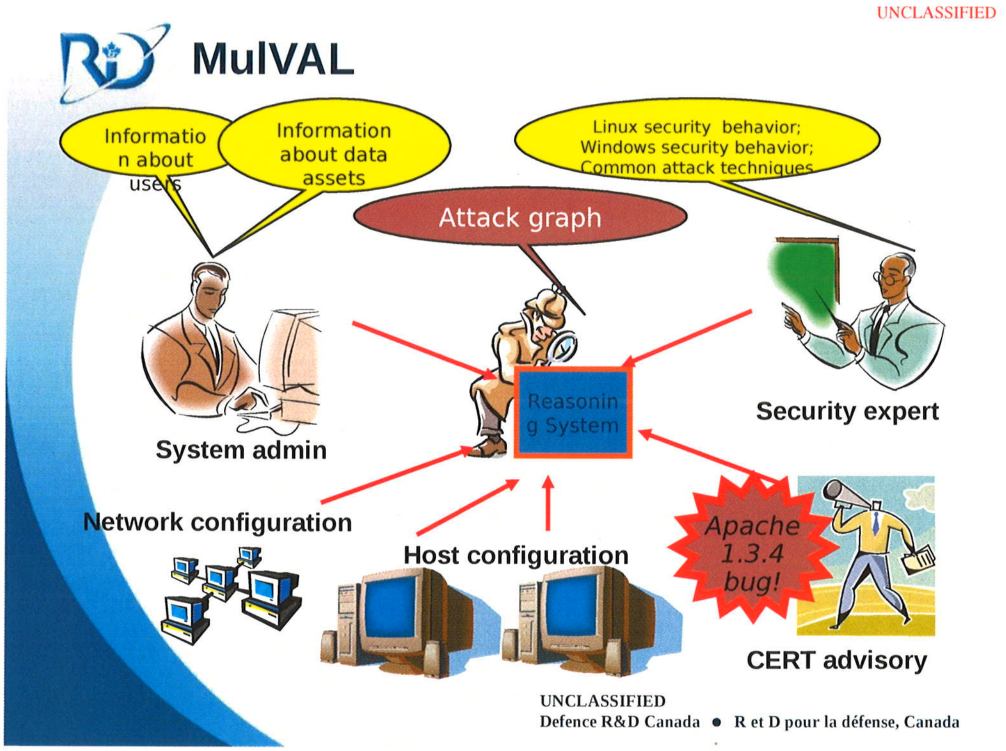
Defence Research and Development Canada is R&D arm of the Department of National Defence.

Within DRDC Ottawa is the Network Information Operations (NIO) section.

Within the Attack Detection and Analysis group, there are 3 projects of particular interest to us:

Mulasses, JNDMS and ARMOUR

DRDC also provides us a mechanism for working on NATO R&D projects as they already have a well established relationship with NATO.



UNCLASSIFIED

MulVAL

Informatio n about users

Information about data assets

Linux security behavior; Windows security behavior; Common attack techniques

Attack graph

Reasonin g System

System admin

Security expert

Network configuration

Host configuration

Apache 1.3.4 bug!

CERT advisory

UNCLASSIFIED
Defence R&D Canada ● R et D pour la défense, Canada

Network based vulnerability analysis project.

Pure logical based reasoning engine that generates attack graphs. These attack graphs can be huge. A system to prioritize them needed to be created.

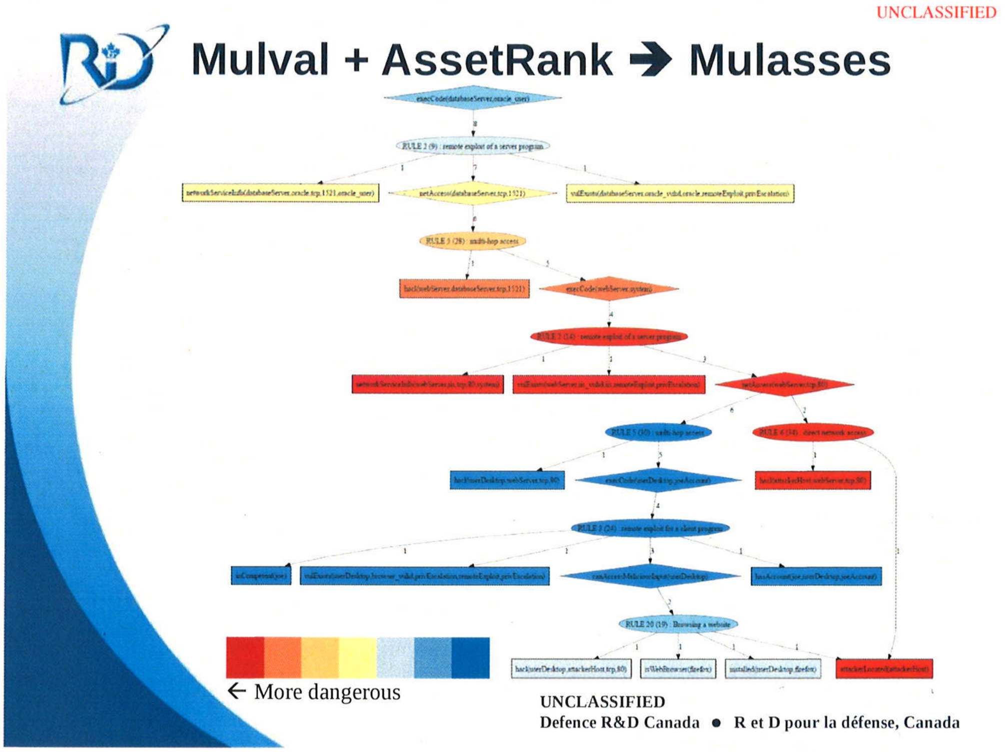
Based on Xinming (Simon) Ou PhD Dissertation from Princeton.

Simon is currently a professor at Kansa state University where he continues development of Mulval and related projects.

These are the 5 classes of input that go into MulVAL:

1. User and data asset information
2. Network configuration (hacls) – Basically describe which computers can talk and on which ports
3. Host configuration – software running on machines within the netwok
4. CERT (or other advisories) that contain information about vulnerabilites
5. Security expert information -- Logic to describe what can be accomplished on a computer given credentials

This input goes into a reasoning system (MulVal) which can then generate attack paths



UNCLASSIFIED

Mulval + AssetRank ➔ Mulasses

execCode(databaseServer,oracle_user)
RULE 2 (9) : remote exploit of a server program
networkServiceInfo(databaseServer,oracle,tcp,1521,oracle_user)
netAccess(databaseServer,tcp,1521)
vulExists(databaseServer,oracle_vuln,oracle,remoteExploit,privEscalation)
RULE 5 (28) : multi-hop access
hacl(webServer,databaseServer,tcp,1521)
execCode(webServer,system)
RULE 2 (14) : remote exploit of a server program
networkServiceInfo(webServer,iis,tcp,80,system)
vulExists(webServer,iis_vuln,iis,remoteExploit,privEscalation)
netAccess(webServer,tcp,80)
RULE 5 (30) : multi-hop access
RULE 6 (34) : direct network access
hacl(userDesktop,webServer,tcp,80)
execCode(userDesktop,joeAccount)
hacl(attackerHost,webServer,tcp,80)
RULE 3 (24) : remote exploit for a client program
inCompetent(joe)
vulExists(userDesktop,browser_vuln,privEscalation,remoteExploit,privEscalation)
canAccessMaliciousInput(userDesktop)
hasAccount(joe,userDesktop,joeAccount)
RULE 20 (19) : Browsing a website
hacl(userDesktop,attackerHost,tcp,80)
isWebBrowser(firefox)
installed(userDesktop,firefox)
attackerLocated(attackerHost)
← More dangerous

UNCLASSIFIED
Defence R&D Canada ● R et D pour la défense, Canada

Asset rank is an adaptation of the original Google page rank algorithm that can prioritize nodes of an attack graph (or any other logic based graph).

It is used to prioritize which network conditions (facts) are the most important to fix first in order to harden the network.

Attack graph:

Ellipse – AND nodes. True if all the dependencies are true.

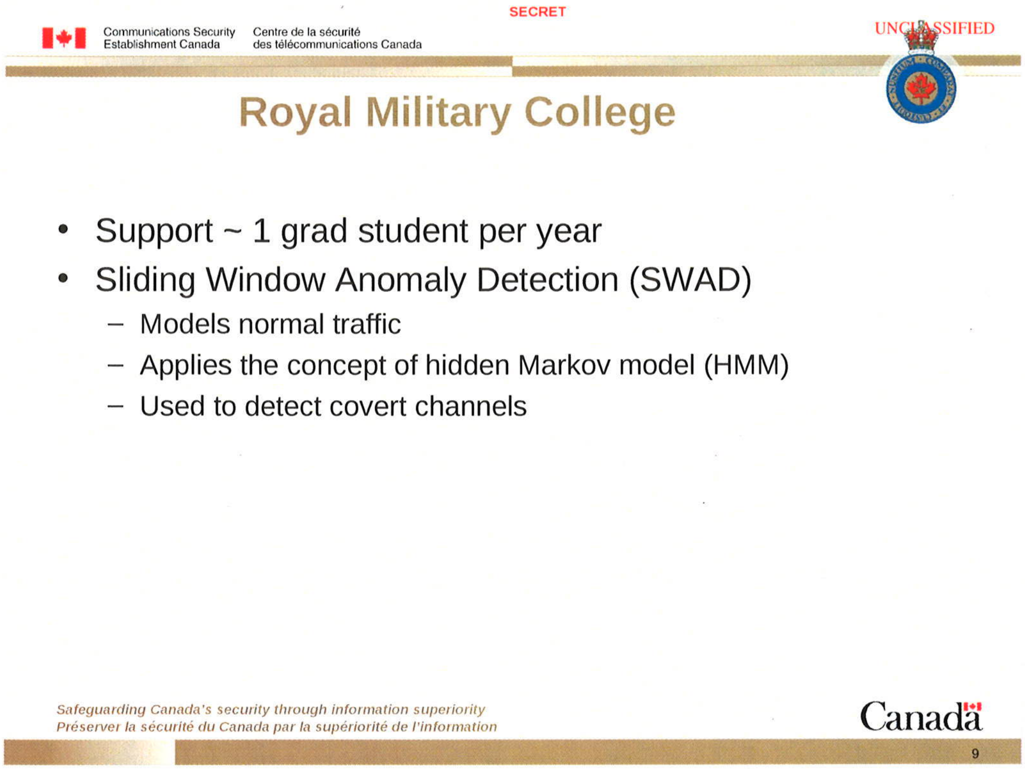
Diamond – OR nodes. True if any of the children nodes are true.

Box – facts: network/host configuration, installed/running software, vulnerabilities

Together Mulval + AssetRank ➔ Mulasses!

Mulasses output is a prioritized list of network configuration properties to be modified to harden the network.

This project has potential value in network vulnerability shop.



SECRET

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

UNCLASSIFIED

Royal Military College

- Support ~ 1 grad student per year
- Sliding Window Anomaly Detection (SWAD)
  - Models normal traffic
  - Applies the concept of hidden Markov model (HMM)
  - Used to detect covert channels

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

9

Hidden Markov model – State of the system is not visible to the observer, only the output. System is assumed to be a Markov process.

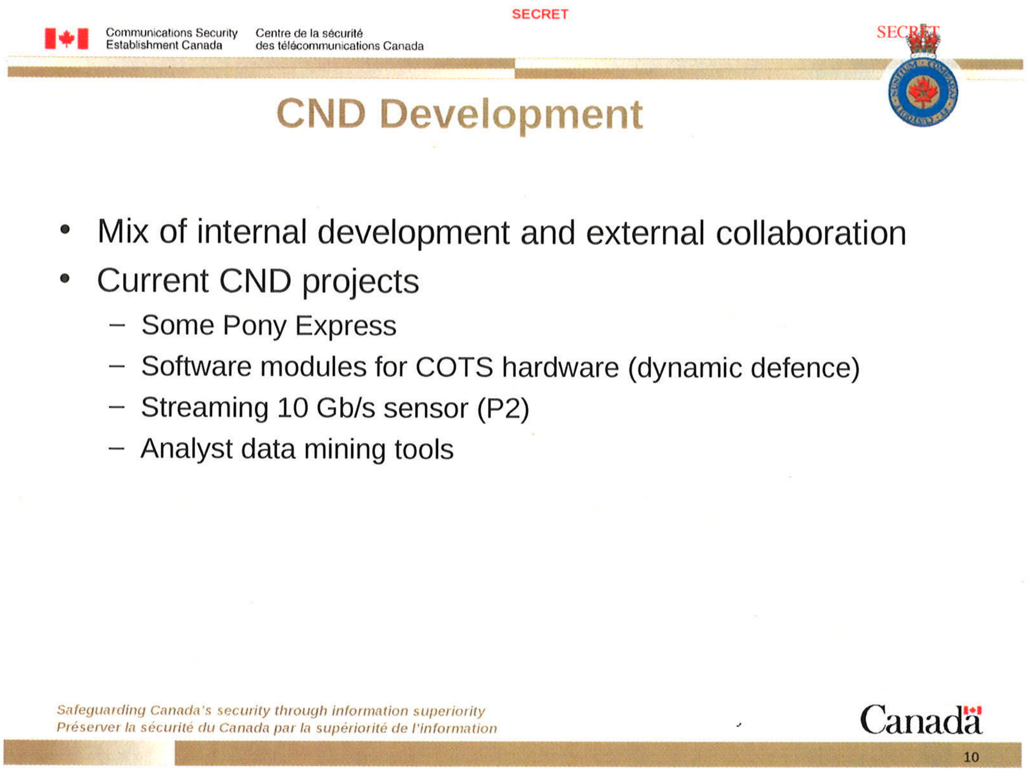
Markov process – A stochastic process with the Markov property

Markov property – random phenomenon depends only on the present state of the system, (i.e. does not depend on the past or future state).

Why we are interested. Detecting covert channels is our business. If it is successful, it may prove to be a very valuable tool.

Other benefits of RMC collaborations – People! Several RMC students have become CSEC employees. They are cleared, and have a education centred on our mutual interests.

The current phase of the SWAD project is to built a user interface that is analyst friendly. Much of the work to date has been proof of concept work.



SECRET

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

SECRET

CND Development

- Mix of internal development and external collaboration
- Current CND projects
  - Some Pony Express
  - Software modules for COTS hardware (dynamic defence)
  - Streaming 10 Gb/s sensor (P2)
  - Analyst data mining tools

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canadä

10

For the next couple of slides I will show some of our recent in-house development efforts.

We really do not have what I would characterize as "**research**" within Cyber Defence.

We do hope to get there.