2010

TECHNOLOGY INVESTMENT FUND (TIF) PROJECT PROPOSAL

1. Basic Information		
Project Title: C4ISR Host-Based Cyber Situation Awareness		**Date:** June 2010
Principal Investigator: Mario Couture **Center:** DRDC Valcartier	**E-mail:** mario.couture@drdc-rddc.gc.ca **Partner Grp:** PG-5 C4ISR **Thrust:** Drop down for PG 0 to 2 15b-Communications and Computer Network Oper **Primary S&T Expertise:** 01 - Command and Control	**Telephone:** 418-844-4000 4285 **Fax:** 418-844-4538
Project Team Members: 1. Mr. Patrick Maupin 2. Defence Scientist To Be Hired In 2010/2011 3. Prof. A. Hamou-Lhadj 4. Prof. M. Dagenais 5. Prof. M. McGuffin 6. Mr. Jie Cai (Dnd/Navy Advisor) 7. Mr. Reginald Sawilla (Drdc Ottawa Scientific Advisor)	**Affiliation:** 1. Drdc Valcartier (Sad) 2. Drdc Valcartier (Sds) 3. Concordia University 4. Polytechnique Montréal 5. École De Technologie Supérieure 6. Dnd/Navy (Felex Project) 7. Drdc Ottawa (Nio)	**Fiscal Year:** 11/12 start

Abstract (Suitable for Publication, 150 words maximum): With the constant increase in cyber threat sophistication, the protection offered by traditional means (antivirus, …) has constantly decreased over the past 10 years; their efficiency is now ranging between 20% and 30% [1, 2]. Since command and control information systems (C2IS) are operated in hostile environments, this limitation must be addressed, with top priority given to the detection of stealthy malicious activities that can silently compromise military decision capabilities. The proposed research aims to provide operational officers with the host-based situation awareness (H-SA) needed for establishing trust in C2IS. This can be achieved through the use of innovative approaches and techniques to detect anomalies and describe current health states of critical hosts. H-SA will be made available: 1- locally on officers' computer screens in near real-time; 2- remotely through secure network requests; and 3- on-disc for later deep in-laboratory analyses. This research will significantly improve reactive and proactive computer network defence (CND).

2. General Description of Proposed Project (2 pg maximum)

2.1 Background information and problem.

The use of networked information systems (IS) to support military operations has become more pervasive in the last decade. It defines the cyber warfare within which military units must *electronically* defend themselves to protect those decisional capabilities that rely on networked computing devices. In this cyber landscape, adversaries are now using advanced technologies to conduct sophisticated cyber attacks (Advanced Persistent Threat; APT [1]) against governmental infrastructures [2, 4, 5, 6] which may result in harmful consequences in a much quicker and stealthier way than for traditional conflicts. Maintaining IS dependability, survivability, and trustworthiness in this context is highly problematic. The time scales of cyber attacks range from milliseconds to decades, weapons take the form of insidious malicious software such as botnets and other forms of denial of service coordinated attacks [3, 7, 4]. The Strategic Capability Roadmap document asked for the capability to "provide sufficient warning of threats to allow pre-emptive action at the tactical level" and to "provide information on adversarial intent and possible courses of action". These are not yet available [7]; operational commanders do not have coherent technical situation awareness of ISs to contribute to the CND decision-making process in a timely and comprehensive fashion [8]. The proposed research aims to explore, design, and prototype new techniques and approaches to significantly *improve the situation awareness of C2ISs* ***during operations***, *provide sufficient warning*, and i*nitiate appropriate and timely proactive measures to mitigate the threat*. A second TIF project is proposed by Mr. Charland (DRDC Valcartier). It focuses on "***in-laboratory post-mortem analysis*** *of cyber attack traces and effects*" (malware analysis). While there are few common traits, both projects require different expertise that could not be adequately put to use in a unified team, hence the two propositions. The results will be shared whenever pertinent between the two projects.

2.2 Purpose.

The purpose of this research is to push further DRDC competencies and capabilities in *on-line software cyber surveillance* by designing and demonstrating the **next generation host-based cyber surveillance system** (**ng-CS2**) as specified by DND: "design, develop, generate and sustain effective cyber operations capabilities" [11], improve proactive CND [6], and maintain cyber superiority. The ng-CS2 will support new approaches to produce, on a continual basis, **host-based situation awareness (H-SA)** containing updated accurate health states of ISs, details of early detected anomalies, and associated levels of system trust. H-SA will be made available locally in quasi real-time on officers' computer screens (*site-awareness level*); graphical on-screen H-SA representations will be well adapted for intense operations, for both novices and experts. The same H-SA will also be made available remotely through secure network requests (feeding national-level CND operations; *enterprise-wide-awareness level*). Finally, H-SA will be continually saved on disc in specialised databases during operations for later in-laboratory deep analyses such as cyber forensics, malware analysis, and continual system improvement. The ng-CS2 will be designed with scalability and flexibility in mind, enabling the addition of newly available leading-edge components to face unforeseen threats, and to preserve DND's cyber superiority.

2.3 Scientific and technical objectives.

The main scientific objectives of this research are intimately related to the new approaches that are put forward to improve software surveillance to the level of host-base situation awareness (H-SA) [1, 5, 12]. The objectives are the following. **(Obj. 1)** The transformation of security systems (antivirus, firewalls, intrusion detection systems, advanced software tracers, etc.) into an adaptive entity that will collect and merge raw data that originate from many different sources within the IS, allowing on-request focus on any components of the IS at runtime. **(Obj. 2)** The highly efficient continual reduction (abstraction) of this generated huge volume of raw data into more manageable software behaviour objects without loss of relevant information. **(Obj. 3)** The highly efficient analysis of these abstracted objects to produce, on a continual basis, elements of the H-SA: health states, detected anomalies, and levels of system trust. Closer examinations of the H-SA content should allow characterising service degradation, malicious activities and intents, and identifying potential responsive courses of action early in the contamination process [63, 80]. New techniques from software trace abstraction and analysis and multisensor data fusion will, for the first time, make combined use of: (a) approaches currently utilized (i.e., signature-based malware detection), (b) new holistic approaches that consider IS health states and deviations from normalcy (**anomalies**), (c) new architectural patterns that improve cyber security [13, 14], and (d) a new knowledge base defining a healthy IS [19, 21]. This combination aims to make possible the early detection (with a low false alarm rate) of most types of known and unknown threats [33, 15, 16, 17] during operations, before system failures happen [18]. **(Obj. 4)** New techniques will be explored to make all the components of the ng-CS2 work as a single synergistic entity that can self-adapt and self-optimise with respect to evolving operational situations. **(Obj. 5)** New on-screen visualisation techniques will be designed to illustrate the content of H-SA with easy and quick to understand interactive graphical pictures. New specialised databases will also allow the highly efficient on-disc saving and searching of H-SA for immediate utilisation and for later in-laboratory deep analyses (saving the appropriate data for court-grade cyber forensics and malware analysis).

2.4 Approaches and methodology.

Important preliminary studies [7, 13, 14, 19, 21, 22, 20, 30] were conducted prior to this research and helped identify new approaches for addressing the problems described earlier. These approaches are: **(appr. 1)** transform current host-based security systems into a responsive adaptive entity allowing on-demand focus on specific IS components [5, 19]; **(appr. 2)** conduct holistic surveillance of IS [5, 4, 19, 20]; **(appr. 3)** produce H-SA based on the analysis of IS health states, anomalies, and signature-based surveillance [5, 14, 19]; **(appr. 4)** use new knowledge bases [21] and new architectural patterns [13, 14] (involving both redundancy, diversity, and data reconciliation [12]) to improve the pace, precision, completeness of analyses, and rate of false positives [16]; **(appr. 5)** make the whole ng-CS2 feedback-directed, self-optimising and self-adapting [19, 30, 61]; and **(appr. 6)** adaptively deliver H-SA locally (on-screen picturing), remotely (on-request secure network transfers), and to repository (highly efficient on-disc storage and searching) [20, 30].

There are four main threads in this research. **(Thread 1) Reference models**. The listed approaches require the design of a new reference model [5, 19, 21]—the Linux knowledge base (LKB)—which will provide the information characterising a healthy IS to each element of the following set of chained processes (see Figure 1): *raw data generation*, *abstraction*, *fusion*, *analysis*, and *H-SA generation*. **(Thread 2) Raw data generation, abstraction, and fusion**. Concepts from trace abstraction [23, 25, 26, 27, 30] and multisensor data fusion [12, 28] will be extended and new techniques will be designed for the abstraction and fusion of the huge volume of raw data that is generated by the set of tracing and security systems (which will be made adaptive [19]), producing more manageable software behaviour abstractions for subsequent analyses, and avoiding the loss of relevant information (a major problem [27]). **(Thread 3) Data analysis, correlation, and H-SA generation**. New techniques inspired by the trace analysis [23, 24, 30], multisensor data fusion [12, 28], and statistics domains need to be designed to conduct complex analyses of these abstract objects and produce H-SA. Recently identified orthogonal conditions defining a healthy information system [19] and redundant-diverse architectural patterns improving cyber security [13, 14] will, for the first time, be utilised as a ground base in correlation analyses. The self-optimisation and self-adaptation of the whole ng-CS2 will also be studied with the goals to minimise the time duration of analyses, to optimise resource utilisation, and to lower the reaction time to cyber attacks (a major problem [4, 5, 6, 7, 61, 63]). **(Thread 4) Adaptive reporting and decision-support systems**. New interactive visualisation techniques (inspired by [69-79] and [52-54]) will be explored to lower the time needed to understand H-SA (for both novices and experts), and to ease IS control. A new specialised database will be designed to efficiently store and make available the huge amount of data (H-SA), both on-line and off-line. A model defining the content of H-SA (with respect to the operational needs and resources availability) will keep the volume of data at manageable levels.

2.5 Risk mitigation.

This project was defined according to an S&T methodology that produced state of the art reports and feasibility studies for this research [7, 13, 14, 19, 21, 22, 20, 30]. The main risks that were identified are related to the monitoring of IS executions to allow decisive analyses and comparisons of results despite the huge volume of data that must be quickly handled. Risks associated with software behaviour and health analysis will be significantly lowered by: 1- the utilisation of Linux-based software applications, for which the source code is freely available [31, 32, 33, 34] (the adaptation of the ng-CS2 to Microsoft operating systems (closed source code) will be done in a future DRDC project); 2- close contact with a large team of specialists from another DRDC S&T initiative at Polytechnique Montréal [29]; and 3- the participation of leading experts, DRDC Ottawa (NIO), DND/Navy engineers, and industrial partners (DND-SERC Program).

2a: <u>Rationale for Choice of External Partner</u> (1/4 page maximum)

The problem of continually producing and making available accurate H-SA during operations makes this research multifaceted. To lower risks, the hard to solve problems must be simultaneously addressed by members of a collaborative team having complementary expertises [5, 11]. Professor A. Hamou-Lhadj from Concordia University is a world leader in software trace abstraction, analysis and visualisation (three major problems addressed by this research). His knowledge in system self-adaptation, self-optimisation and correlation will also bring a significant contribution to this research. Professor M. Dagenais from Polytechnique Montréal is a world leader in the area of deep system analysis. His comprehensive knowledge of the Linux operating system and recent CPU technologies will be intensively put to contribution in the design of the LKB. He also leads Linux Trace Toolkit next generation (LTTng; [35, 36, 64-68]), which is one of the main stepping stones of this project. Professor M. McGuffin from École de technologie supérieure is a leading expert in complex data visualisation. His expertise makes him the perfect candidate for the design of the needed graphical interactive pictures describing complex concepts of H-SA. Mr. J. Cai from DND will provide (as a DND/Navy Advisor) the very important feedback this research needs to stay perfectly aligned with real military needs [60]. He will also start a Ph.D. in the context of this research. Lockheed Martin Canada (Mr. D. Knight) will also bring a significant contribution to this research (likely through a DND-NSERC Program). Close collaboration with Mr. Reginald Sawilla, a researcher in the application of graph theory to security problems and our Scientific Advisor from DRDC Ottawa (NIO), will ensure the interoperability of the ng-CS2 with other similar complementary national-level efforts ([8, 9, 10, 63, 80] and the Public Security Technical Program project Automated Risk Management System; ARMS).

3. Project Work Plan

Activity Phase	Description	Resources Needed (k$, PYs)	Milestones
Year 1: **Solution options exploration, analysis and prototyping activities**		**270 k$, 1.7 DRDC PY**	
1.1 Modelling (Figure 1)	- LKB (v1) - Architectural patterns and on-line reconfiguration strategies (v1) - Models for raw data abstraction, fusion and analysis (including correlation) (v1) - H-SA model (v1) - Meta-optimisation model (v1)	150 k$	**Month 6**: The collaborative env. and modelling tools are functional. Potential solution options have been acquired, and evaluated. **Month 12**: Version 1 of architectural patterns, models, knowledge bases completed (prototypes).

1.2 Design (Figure 1)	- Prototyping and experimentation environment (v1) - Techniques for raw data abstraction, fusion, and analysis (including correlation) (v1) - Techniques for meta-optimisation and scalability of the ng-CS2 (v1) - Techniques for adapted reporting and H-SA sharing (v1)	100 k$	**Month 6:** Potential solution options have been acquired, and evaluated. **Month 12:** Version 1 of prototyping env. and techniques completed (prototypes). Specification of the ng-CS2 (interoperability, scalability)
1.3 Experimentations	-Prototyping activities in each thread (prepare v2)	20 k$	**Month 12**: Prototyping activities on version 1 of the technologies completed & results documented for v2.
Decision point 1	*Solution options to be considered* *Integration of components*		***Month 12***.
Year 2: **Refined designs and integration of selected solution options, and prototyping activities**		**280 k$, 1.7 DRDC PY**	
2.1 Modelling (Figure 1)	- LKB (v2) - Architectural patterns and on-line reconfiguration strategies (v2) - Models for raw data abstraction, fusion and analysis (including correlation) (v2) - H-SA model (v2) - Meta-optimisation model (v2)	100 k$	**Month 24**: Version 2 of architectural patterns, models, knowledge bases completed (prototypes).
2.2 Design (Figure 1)	- Prototyping and experimentation environment (v2) - Techniques for raw data abstraction, fusion, and analysis (including correlation) (v2) - Techniques for meta-optimisation and scalability of the ng-CS2 (v2) - Techniques for adapted reporting and H-SA sharing (v2)	150 k$	**Month 24**: Version 2 of prototyping env. and techniques completed (prototypes). Integration of all ng-CS2 components according to the ng-CS2 specification.

2.3 Experimentations	- Define goals and scenarios of the global experimentation - Prototyping activities in each thread (prepare global experimentation)	30 k$	**Month 24**: Prototyping activities on version 2 of the technologies completed & results documented for global experimentation. ng-CS2 scalability and interoperability tested. Ng-CS2 is feedback-directed.
Decision point 2	*Experimentations to be conducted* *Publications*		***Month 18.***
Year 3: **Final refinements and integration of solution options, global experimentations, and publications**		**200 k$, 1.7 DRDC PY**	
3.1 Modelling (Figure 1)	- Documentation and publication - LKB (v3) - Meta-optimisation (v3) - Architectural patterns and on-line reconfiguration strategies (v3) - Models for raw data abstraction, fusion and analysis (including correlation) (v3)	25 k$	**Month 36**: Version 3 of architectural patterns, models, knowledge bases completed (ng-CS2). Publications Documentations
3.2 Design (Figure 1)	- Documentation and publication - Techniques for raw data abstraction, fusion, and analysis (including correlation) (v3) - Techniques for meta-optimisation and scalability of the ng-CS2 (v3) - Techniques for adapted reporting and H-SA sharing (v3)	25 k$	**Month 36**: Version 3 of techniques completed (ng_cs2). ng-CS2 is self-optimising, self-adaptive. Publications Documentations
3.3 Experimentations	- Documentation and publication - Large experimentation involving all components of the ng-CS2 (as a whole self-optimising and self-adapting entity) - Show and characterise the effectiveness of models, knowledge bases, techniques, measures of performance.	150 k$	**Month 36**: Global experimentation done. Publications Documentations
Decision points	*At decision points, timelines will be reviewed according to eventual issues to be investigated. Scope will also be realigned according to previous findings. Decision points might also be used as GO/NO-GO milestones.*		

4. Assessment Criteria Min 1/4 page – Max 1/2 page of text each

Please describe your proposal in terms of:

1). Scientific Quality (Weight = 1)

2). Technical Plans & Methodology (Weight = 1)

3). Team Capabilities, Include Biographic Sketches

[Note that "Project Team Capabilities" is not rated directly, but is a factor in the criterion "Overall Proposal Scientific Merit" which has a weight=1. There is no section for the Applicant to comment on this criterion. Instead, the reviewer bases the assessment on information found in several sections of the proposal, such as the Description of Project, Team Capabilities, Project Work Plan, etc.]

4). Novelty / Breaking New Ground (Weight = 3)

5). Impact on the DRDC R&D Program; or,
Impact on OR&A Decision Support Capability (Weight = 1.5)

6). Defence Potential (Weight = 1.5)

1). Scientific Quality:

H-SA will result from the following **chained processes** (see Figure 1): *raw data acquisition*, *abstraction*, *fusion*, *analysis*, *H-SA generation,* plus feedback-directed optimisation. A global synergy is necessary among working ng-CS2 components to optimise its internal dynamics and make it more self-adaptive and self-optimising [19]. Based on the model defining a healthy IS [19, 21] and the use of redundancy and diversity in IS architecture [13, 14], advanced optimisation techniques will continually evaluate the results obtained by analysis for optimisation purposes. The best configuration options (of ng-CS2 components) will then be automatically selected for the next analyses, making possible feedback-directed optimisation (as introduced in [61]). As a result, multiple adaptive data sources (within the IS) will produce appropriate volumes of the most relevant raw data [1, 12] to be analysed by the most appropriate mechanisms in a timely manner. The design of the Linux knowledge base (LKB) represents an important challenge due to the high complexity and huge size of the Linux kernel. As shown in Figure 1, mechanisms pertaining to two different domains (trace abstraction and analysis and multisensory data fusion; two viable alternatives) will be concurrently used to maximise raw data volume reduction and subsequent analyses. Based on [14, 23-27, 30] and results from another DRDC project [29], new techniques will be designed to abstract and analyse the huge volume of data that is generated by the advanced software tracer (LTTng [35, 36, 64-68]). The Bass model [28, 38] will be extended to allow: 1- the fusion of these data with those originating from other security systems (such as host-based intrusion detection systems, antivirus, firewalls, etc.), 2- the analysis of host-based situations (health states), and 3- the analysis of detected anomalies. New correlation techniques (based on [14, 25, 42]) will use new architectural patterns (involving redundancy and diversity [13, 14]; an extended form of data reconciliation [12]) with the goal to effectively analyse and compare software behaviours, IS health states and anomalies on each redundant-diverse system. As an example, if the exact same input is provided to two instances of the same IS (each concurrently running on two operating systems that are technically different), the probability of a successful simultaneous cyber attack on these two parallel systems is very low because vulnerabilities are not the same for both systems [12-14]. In addition, leading-edge techniques based on Hidden Markov Models [42-45] and other techniques [47-51] will also be explored and pushed further to improve the timely detection of any kind of anomaly [15, 17, 39-41], lower the false alarm rate (a major problem [5, 42]), and identify potential courses of action [63, 80]. Finally, the time needed by an operator to understand and manipulate graphical pictures of H-SA (and manually control IS) will be lowered by new adapted human-machine interfaces and techniques based on others from similar domains [69-79, 52-54]. New techniques and specialised databases will be designed to efficiently store, retrieve, and share the content of H-SA during operations.

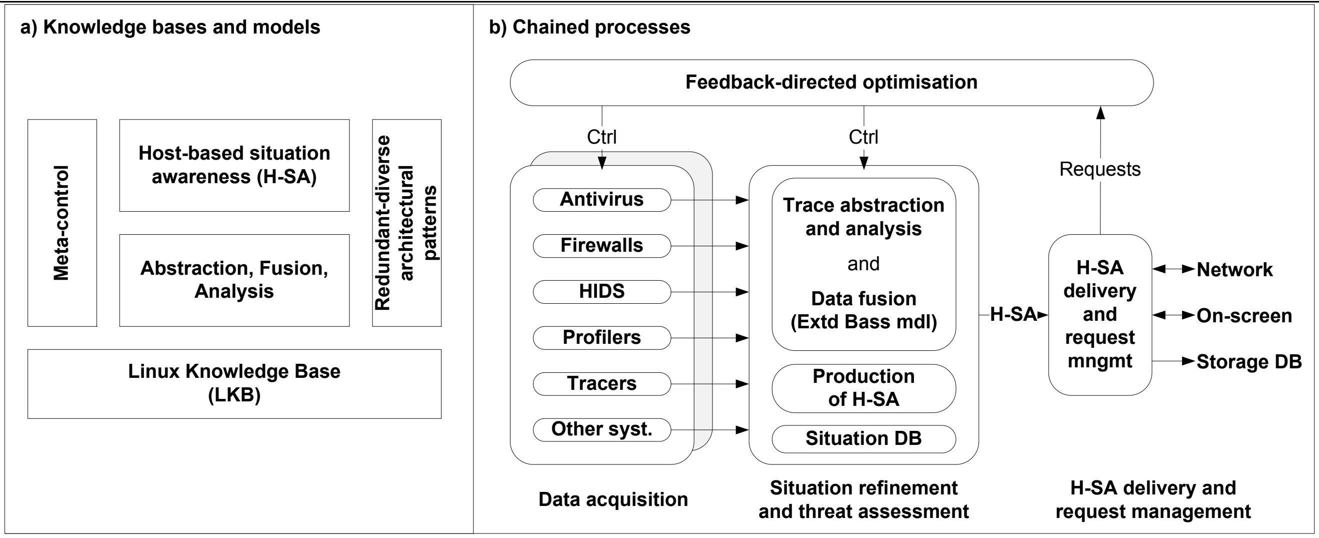
a) Knowledge bases and models
Meta-control
Host-based situation awareness (H-SA)
Abstraction, Fusion, Analysis
Redundant-diverse architectural patterns
Linux Knowledge Base (LKB)
b) Chained processes
Feedback-directed optimisation
Ctrl
Ctrl
Requests
Antivirus
Firewalls
HIDS
Profilers
Tracers
Other syst.
Trace abstraction and analysis
and
Data fusion (Extd Bass mdl)
Production of H-SA
Situation DB
H-SA
H-SA delivery and request mngmt
Network
On-screen
Storage DB
Data acquisition
Situation refinement and threat assessment
H-SA delivery and request management

Figure 1. (a) Interrelated ng-CS2 knowledge bases and models; (b) ng-CS2 chained processes.

2). Technical Plans & Methodology:

In order to enable the detection of the threat early in the contamination process, we first need to enable more synergy between existing security mechanisms (firewalls, …) and, second to coordinate analysis and reactive measures at a higher level using feedback-directed optimisation (see Figure 1). The development of new techniques for the chained processes will integrate approaches put forward in this project, more particularly: the LKB [21], the set of orthogonal conditions defining a healthy IS [19], new architectural patterns [13, 14], and new advanced software tracing technologies (LTTng; [35, 36, 64-68]). This will be mostly done at Concordia University (CU) under Professor Hamou-Lhadj's supervision during the first half of the project. The design of the LKB will be done at Polytechnique Montréal (PM) under supervision of Professor Dagenais during the first year. The set of chained processes will be tested and optimised jointly by DRDC Valcartier and CU mainly in the second year of the project. As it would never be possible to simultaneously monitor all components of the C2IS (this would create a system overload), surveillance strategies will be defined, each one specifying which strategic probes in the IS need to be concurrently active. Levels of certainty will thus be needed to characterise H-SA [62]; the information needed to build a fully-accurate H-SA being unavoidably incompletely collected. Such trade-off studies (and false alarm management) will involve DRDC staff and both universities (CU and PM) and will go on for most of the second half of the project. The design of new visualisation techniques allowing adapted reporting of H-SA will be done at École de technologie supérieure (ETS) during the second half of the project. Since the Navy is currently adopting Linux aboard the Canadian Frigates, the naval environment is likely to become our **reference environment**. Formal discussions first occurred one year ago with the FELEX Project [60] (Mr. Jie Cai), which facilitated the linkage with Lockheed Martin Canada (LMC; the FELEX prime contractor) (Mr. D. Knight). Using this reference environment, H-SA will be demonstrated and critically reviewed by a group of representative users and system developers from LMC in the last year of the TIF project. It is not expected that the prototype produced by this research will be fielded in any operational environment, as coding standards and documentation in a TIF project are not adequate for operational software. Re-implementation of selected components for Linux (and for other types of operating systems such as Microsoft's) will have to be done in subsequent DRDC S&T projects.

3).Team Capabilities - Include Biographic Sketches:

Dr. A. Hamou-Lhadj (Concordia University). Dr. Abdelwahab Hamou-Lhadj is a world expert in the field of tracing and run-time monitoring of software systems. At Concordia University, he leads the Dynamic Analysis of Software Systems (DASS) research group, which investigates techniques and tools that facilitate the generation, modelling, handling, abstraction, and visualisation of large execution traces with the ultimate objective to help software engineers understand and analyze the behavioural aspects of software systems. He has authored several widely cited research papers published in the proceedings of renowned conferences, journals, and book series. Throughout his research career, he has worked with various companies including

Ericsson, Mitel Networks, QNX, and CAE.

Dr. M. Dagenais (Polytechnique Montréal). Michel Dagenais is professor at Polytechnique Montréal in the Computer and Software Engineering Department. He has been active in the area of system analysis tools for the past 15 years. He has, over the years, visited and collaborated with researchers at many of the largest industrial research centers at AT&T Bell Labs, Bell Northern Research, Sun, DEC, IBM, Ericsson and Google. The Linux Trace Toolkit, developed under the supervision of Michel Dagenais at Polytechnique Montréal, is used throughout the world and gained the cooperation of a large number of industrial contributors over the years such as Autodesk Media and Entertainment, Ericsson, Google, IBM, MontaVista, Red Hat, Sony and others. His group has made several original contributions to the Linux kernel related to tracing and to multi-processor performance.

Dr. M. McGuffin (École de technologie supérieure; ETS). Prof. McGuffin develops graphical user interfaces and interaction techniques for visualisation of scientific data and abstract information. He has worked at five different software companies developing graphical user interfaces, and obtained his Ph.D. from the University of Toronto. He has co-authored six papers describing novel popup widgets that enable a fast, gestural style of interaction; three other papers describing hybrid visualisations of trees and graphs that mix different visualisation styles together; and two other papers that have been cited over 90 times each. His 2009 paper at the IEEE InfoVis conference won an Honorable Mention. He has served on the program committee for IEEE InfoVis three years in a row (2008-2010). His team will design and implement prototype interactive visualisations for the project. McGuffin's lab is equipped with 3 multitouch surfaces and other input devices that would be available for the project and will prove useful.

Mr. Patrick Maupin (DRDC Valcartier). Group Leader for the Situation Analysis and Monitoring group, Patrick Maupin joined DRDC-Valcartier in 2001 as a Defence Scientist, specialising in pattern recognition and situation analysis. He is currently Project Manager and Scientific Authority for the ARP Project 13qd "Sensor Networks for Critical Assets Protection and Surveillance in Support of Air Expeditionary Wing Operations" (2008-2011) and the DIR Project 11hl10 "A Defense Initiative to Evaluate Situation Awareness for Coastal and Off-Shore Surveillance" (08/10). He is scientific team leader for the design of the Situation Analysis Module on the TDP 12pk "Self-healing Autonomous Sensing Network (SASNet) (07/10) and federal partner on the CRTI project "Data Fusion Solutions for Monitoring CBRNE Threats" (09/11). He is also co-investigator on three major academic projects (ARC Linkage, 08/20; MITACS, 07/09; and NSERC Strategic, 08/10), member of the NATO IST-079 RTG on "Decision Support in the Context of an Integrated Command and Control" and team member of the SECURINET and SASNet projects.

A DRDC - Valcartier defence scientist. A defence scientist will be hired in 2010-2011 (in the System of systems Section, Software Analysis and Robustness Group) to work full time on this TIF. This person will acquire the necessary expertise for the continuation of this work after the project ends.

Mr. Jie Cai (DND, Navy). Mr. Jie Cai holds B.Sc. and M.Eng. degrees in Mechanical Engineering. He also holds an M.Sc. degree in System Science from the University of Ottawa. After 11 years' work experience as a system and embedded software engineer at Nortel Telecommunication, he joined DND in 2008. He is now working in PMO HCM/FELEX.

Mr. Reginald Sawilla (DRDC Ottawa). Defence Scientist in the Attack Detection and Analysis group in the Network Information Operations (NIO) section. He is currently the scientific authority and project manager of the ARMOUR Automated Computer Network Defence Technical Demonstrator (TD) project; the federal lead for the Automated Risk Management System (ARMS) project of the Public Security Technical Program (PSTP); the lead for the Security Posture Assessment Demonstrator and Experimenter (SPADE); and scientific authority for an integration project with TrendMicro. He developed the AssetRank algorithm [80] for identifying critical nodes in AND/OR directed graphs, and an algorithm to compute courses of action that maximally disrupt communication between subcommunities in AND/OR directed graphs [63]. He has applied the algorithms to identify optimal ways to apply patches and connectivity changes to limit attackers' abilities to move in a network, and to prioritise spending areas for DND's Integrated Command and Control Outlook (IC2O) Working Group. He obtained an interdisciplinary M.Sc. degree in Pure Mathematics and Computer

Science (cryptography) at the University of Calgary in 2004, and is completing a Ph.D. degree in Computing at Queen's University (connectivity in AND/OR directed graphs).

Mr. Mario Couture (Principal investigator; DRDC Valcartier). Mr. Couture holds a B.Sc. degree in Physics and an M.Sc. degree in Physical Oceanography (modelling and simulation; M&S). After 8 years of M&S work at Fisheries and Oceans Canada, he completed a second M.Sc. in Electrical Engineering at Laval University (network quality of services; QoS). In 2002, he joined Defence R&D Canada – Valcartier as a defence scientist. He is now part of the Software Analysis and Robustness (SAR) Group (System of systems Section). He leads the 15ba applied research project "Tracing and monitoring of distributed multi-core information systems", which will end in 2012. Essentially, his work aims at designing new techniques (based on new approaches) that will significantly improve the surveillance of military information systems during operations, and the early detection of threats to these systems.

4). Novelty / Breaking New Ground:

Novelty in this research can be found in three main categories.
(1) Highly efficient techniques for trace abstraction, fusion, and analysis. Novel techniques, models, specialised databases, and knowledge bases will be developed to fully support all elements of the chain of processes (see Figure 1). For the first time, new techniques that will be derived from both the trace abstraction and analysis and the multisensory data fusion domains will be used together at runtime. The recently found set of three orthogonal conditions defining a healthy information system [19], the LKB [21], new redundant-diverse architectural patterns [13, 14], and new advanced software tracing technologies [35, 36, 64-68] will, for the first time, be integrated in analyses. The research will explore which parts or components of the system should be redundant, where diversity should be implemented, and how these patterns should be used and reconfigured at runtime to significantly improve cyber surveillance, protection, and reaction to cyber attacks.
(2) Continual production (and rendering) of H-SA during operations. Unprecedentedly, H-SA will give officers the information they need to establish the trust they can have in their IS. Also, new techniques and knowledge bases will, for the first time: 1- produce adapted on-screen H-SA interactive reports; 2- allow highly efficient on-disc H-SA saving, retrieving, and searching; and 3- make possible on-request secure networked H-SA transfers. These functionalities are not (or are rarely) available at this moment [8]. New visualisation techniques will be designed for cyber security purposes (based on [69-79] and [52-54]). New on-disc H-SA will also provide the mandatory information for court-grade cyber forensics and malware analyses.
(3) A functional knowledge base for the Linux operating system (the LKB). A solid foundation (the LKB) that fully supports the approaches put forward in this research will also provide the support the ng-CS2 components need all along the chain of processes. The LKB has no equivalent on the market [26].

5). Impact on the DRDC R&D Program:

There is a pressing need to improve cyber security not only for the DND/CF but for all government departments. By this key technology exploration on live detection of *stealth malicious malware and activities*, DRDC can expand its leading-edge expertise and offer a very rich project environment for its scientists, mostly in areas aiming at improving CND activities both during operations (cyber surveillance and protection) and in the laboratory (deep analyses like cyber forensics and malware analyses). DRDC Applied Research Programs (ARP) and Technology Demonstration Programs (TDP) are perfect DRDC vehicles for future developments of new ng-CS2 components, integrating new, more powerful techniques to address unforeseen increasingly complex cyber threats. The collaboration among participants will guarantee the transition of expertise currently residing with each of the external partners, and strongly encourage the definition of subsequent ARP and TDP collaborative projects. DRDC Valcartier will be in a better position to provide the continuous support DND needs to maintain its cyber superiority. This project complements (and is interrelated to) other DRDC Ottawa (NIO Section) similar S&T projects for the networks: **JNDMS** [9], **ARMOUR** [10], and **Net C2-ISAC** [8].

6). Defence Potential:

The recognition of the network environment as a battle space [11] means that Commanders and supporting staff must be continuously aware of the state of the information technologies (IT) and infrastructures supporting operations. At present, officers' awareness of IT health states and potential threats is very limited [8]. As a consequence, an information system may, during operations, experience an error (the result of a cyber attack) that may degenerate into a general service or system failure [18], without any forewarning. The proposed project aims to provide, on a continual basis, precise H-SA that includes details on detected anomalies and possible courses of action that can be triggered in response [63, 80]. H-SA is an essential asset because it will help diagnose and fix problems (locally and remotely) early in the contamination process, giving more time for automatic or manual proactive and reactive CND actions to be launched [6]. As mentioned in [11], "cyber-operations are an operational environment in their own right", "C4ISR enable cyber-operations like any other command". In this context, H-SA will significantly raise the knowledge officers have of the health state of DND's information systems during operations: this information is thus precious for CND C2 (**Command; Sense**). It will contribute to make the blue CND OODA loop (at both local and national levels) faster and more agile than the red OODA loop (**Act; Shield**). The efficient saving of H-SA on disc for later deep in-laboratory analyses and system improvements will, for the first time, contribute to preserve DND's cyber superiority by allowing the structured development and integration of new ng-CS2 components that take into account new technologies and unforeseen threats (**Sustain**). The work proposed in this research will provide direct support to address ADM(S&T) Hard problems HD5 (**Close capability gap**; "**Pro-active Computer Network Defence Acquisition Project # 266**") and HD12 ("**Enhance the Nation's Cyber Security"**). This research is also well aligned with important DRDC and DND projects: Halifax Class Modernisation/Frigate Life Extension Project (**FELEX**) [DND/Navy, Mr. Jie Cai]; **Net C2 ISAC** (CFNOC/DRDC Ottawa, Mr. Reginald Sawilla); and other DND classified projects (CFNOC, CSEC).

Annex – References

[1] MANDIANT. M-TRENDS; the advanced persistent threat. (http://www.mandiant.com; Accessed: May 2010), 2010.

[2] Maj. Gen. Beark. 8-slides presentation. National Surveillance Study. Chief Force Development. 2009.

[3] M. Couture and A. Gherbi. Cyber threat – Definitions and references. DRDC Valcartier TN 2009-239. Defence R&D Canada – Valcartier; May 2010.

[4] Bell Canada. Combating Robot Networks and Their Controllers: A Study for the Public Security and Technical Program (PSTP). Bell Canada, reference number cpq0229.1.36.4, 2010.

[5] J. Viega. The Myths of Security – What the Computer Security Industry Doesn't Want You to Know. O'Reilly, ISBN 978-0-596-52302-2, 2009.

[6] Treasury Board of Canada. Proactive Cyber Defence Project Report. Treasury Board of Canada Secretariat, Chief Information Officer Branch, Security and Identity Management. Draft document version 8, June 26th, 2008.

[7] R. Charpentier and J. H. Lefebvre. Le Développement de la force cybernétique canadienne. Presentation made at Institut militaire de Québec, DRDC Valcartier SL 2010-112, April 2010.

[8] Net C2 ISAC. Network Command and Control – Integrated Situation Awareness Capability. Project number CNO00009, (Documents: 1- Project Charter; 2- Statement of Operational Requirement; 3- Project Profile and Risk Assessment; 4- Options & PRICIE Analysis), March 2010.

[9] J. H. Lefebvre, M. Grégoire, L. Beaudouin, J. Treurniet. Joint Network Defence and Management System. Technical memorandum TM 2003-230, DRDC Ottawa, 2003.

[10] ARMOUR Project. Automated Computer Network Defence. Technical Demonstration Program 15BD, 2009.

[11] DRDC. Cyber Operations – Science and Technology (S&T) Strategy. Internal document, Issued on authority of ADM(S&T), ADM(IM), and CMP, September 2009.

[12] I. Corona, G. Giorgio, C. Mazzatiello, F. Roli, and C. Sansone. Information fusion for computer security: State of the art and open issues. An International Journal on Information Fusion. Special issue on Information Fusion in Computer Security. Volume 10, issue 4, 2009.

[13] A. Gherbi. Redundancy with Diversity Based Software Architecture for the Detection and Tolerance of Cyber Attacks. Technical DRDC Valcartier report, (Post Doc R&D work; supervision: R. Charpentier), submitted in July 2010.

[14] DRDC Valcartier Contract. Execution trace comparison and redundant and diverse architectures – Proof of concept and comprehensive analysis. DRDC Valcartier contract #01423, Scientific authority: M. Couture, 2010.

[15] S. Y. Lim and A. Jones. Network Anomaly Detection System: The State of the Art of Network Behaviour Analysis. International Conference on Convergence and Hybrid Information Technology, IEEE, 2008.

[16] F. Maggi, M. Mateucci, and S. Zanero. Detecting Intrusion through System Call Sequence and Argument Analysis. IEEE Transaction on Dependable and Secure Computing, ISSN: 1545-5971, (approximate date: 2006).

[17] P. Kabiri, A. A. Ghorbani. Research on Intrusion Detection and Response: A Survey. International Journal of Network Security, Vol. 1, No.2, pages 84–102, 2005.

[18] A. Avizienis, J.-C. Laprie, and B. Randell. Basic Concepts and Taxonomy of Dependable and Secure Computing. Technical Research Report TR 2004-47, Institute for Systems Research, 2004.

[19] A. Hamou-Lhadj. Software resilience, self-healing, and self-adaptation. DRDC Valcartier contract #92239, Scientific authority: M. Couture, January 2010.

[20] M. Couture, R. Charpentier, M. Dagenais, A. Hamou-Lhadj, A. Gherbi. Self-defence of Information Systems in Cyber-Space – A Critical Overview. In Proceedings of NATO IST-091 Symposium, 2010.

[21] DRDC Valcartier Contract. Knowledge base model for the Linux Kernel – State of the art and feasibility study. DRDC Valcartier contract #01009, Scientific authority: M. Couture, 2010.

[22] DRDC Valcartier Contract. Linux-based Security Systems – State of the art and analysis. DRDC Valcartier contract #01396, Scientific authority: M. Couture, 2010.

[23] A. Hamou-Lhadj. Techniques to Simplify the Analysis of Execution Traces for Program Comprehension. Ph.D. Dissertation, School of information Technology and Engineering (SITE), University of Ottawa, 2005.

[24] A. Hamou-Lhadj and T. Lethbridge. Measuring Various Properties of Execution Traces to Help Build Better Trace Analysis Tools. In Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems, IEEE CS, Shangai, China, pp. 559–568, 2005.

[25] A. Hamou-Lhadj and T. Lethbridge. Summarizing the Content of Large Traces to Facilitate the Understanding of the Behaviour of a Software System. In Proceedings of the IEEE International Conference on Program Comprehension, IEEE CS, Athens, Greece, pp. 181–190, 2006.

[26] H. Pirzadeh and A. Hamou-Lhadj. Software Visualization Techniques for the Representation and Exploration of Execution Traces. Submitted to IEEE Transactions on Visualization and Computer Graphics, 2010.

[27] A. Hamou-Lhadj and T. Lethbridge. Compression Techniques to Simplify the Analysis of Large Execution Traces. In Proceedings of the 10th IEEE International Workshop on Program Comprehension (IWPC), IEEE CS, Paris, France, pp. 159–168, 2002.

[28] T. Bass. Intrusion detection systems and multisensory data fusion. Communications of the ACM, 43 (4), 2000.

[29] M. Couture, M. Dagenais, D. Toupin, R. Charpentier, G. Matni, M. Desnoyers, P.-M. Fournier, 2008. Monitoring and tracing of critical software systems – State of the work and project definition. DRDC Valcartier TM 2008-144. Defence R&D Canada – Valcartier; June 2008.

[30] M. Couture, M. Dagenais, F. Prenoveau, B. Ktari, F. Lajeunesse-Robert. Tracing, monitoring and analysis of distributed multi-core systems – Selected feasibility studies. DRDC Valcartier TR 2008-300. Defence R&D Canada – Valcartier; April 2009.

[31] R. Carbone. Enterprise Linux Licenses – A comparison of licenses between Red Hat and Suse Enterprise Linux. DRDC Valcartier TN 2006-573. Defence R&D Canada – Valcartier; October 2006.

[32] R. Carbone, R. Charpentier. Life-Cycle Support for Information Systems Based on Free and Open Source Software. 11th ICCRTS (International Command and Control Research and Technology Symposium), 2006.

[33] R. Carbone. Free and open source software threat quantification. Defence R&D Canada – Valcartier, TM 2007-007. January 2008.

[34] R. Carbone. Operating system hardware reconfiguration – A case study for Linux. DRDC Valcartier TM 2006-595. Defence R&D Canada – Valcartier; November 2006.

[35] M. Desnoyers. Low-impact operating system tracing. Ph.D. thesis, École polytechnique de Montréal, 202 pages, 2009.

[36] Linux Trace Toolkit next generation - LTTng. http://lttng.org, [Accessed: May 2010].

[37] M. Sharif, K. Singh, W. Lee. Understanding Precision in Host Based Intrusion Detection – Formal Analysis and Practical models. Springer-Verlag, C. Kruegel, R. Lippman, and A. Clark (Ed.), Lecture Notes in Computer Science (LNCS) Vol. 4637: RAID 2007, pages 21–41, 2007.

[38] Marcelo N. Kapp, R. Sabourin, P. Maupin. A PSO-based framework for dynamic SVM model selection. GECCO 2009, pp. 1227–1234, 2009.

[39] Eulanda dos Santos, R. Sabourin, P. Maupin. Overfitting cautious selection of classifier ensembles with generic algorithms. Information Fusion 10(2): 150–162, 2009.

[40] Eulanda dos Santos, L. S. Oliviera, R. Sabourin, P. Maupin. Overfitting in the selection of classifier ensembles: A comparative study between PSO and GA. GECCO 2008: 1423–1424, 2008.

[41] Eulanda dos Santos, R. Sabourin, P. Maupin. Pareto analysis for the selection of classifier ensembles. GECCO 2008: 681-688, 2008.

[42] D. Gao, M. K. Reiter. Beyond Output Voting: Detecting Compromized Replicas Using HMM-Based Behavioral Distance. IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 2, 2009.

[43] W. Khreich, E. Granger, R. Sabourin, A. Miri. Combining Hidden Markov Models for Improved Anomaly Detection. Proceedings of the IEEE ICC, 2009.

[44] A. G. Tokhtabayev, V. Skormin. Non-Stationary Markov-Models and Anomaly Propagation Analysis in IDS. In Proceedings of the third IEEE International Symposium on Information Assurance and Security, 2007.

[45] J. Hu, X. Yu, H.-H. Chen. A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection. IEEE Network, 2009.

[46] I. Rish, M.Brodie, S. Ma, N.Odintsova, A. Beygelzimer, G.Grabarnik, K.Hernandez. Adaptive Diagnostic in Distributed Systems. IEEE Transaction on Neural Networks, (16) 5, 2005.

[47] U. Ahmed, A. Massood. Host Based Intrusion Detection Using RBF Neural Networks. IEEE International Conference on Emerging Technologies, 2009.

[48] M. Costa, M. Castro, L. Zhou, L. Zhang, M. Peinado. Bouncer: securing software by blocking bad input. In Proceedings of the ACM Symposium on Operating Systems Principles, pp. 117–130, 2007.

[49] G. Candea, E. Kiciman, S. Kawamoto, A. Fox. Autonomous recovery in componentized internet applications. In The Cluster Computing Journal, 2004.

[50] M. A. Sekeh, M. A. bin Maarof. Fuzzy Intrusion Detection System via Data Mining Technique With Sequences of System Calls. IEEE fifth International Conference on Information Assurance and Security, 2009.

[51] R. Moskovitch, S. Pluderman, I. Gus, D. Stopel, C. Feher, Y. Parmet, Y. Shahar, Y. Elovici. Host-Based Intrusion Detection using Machine Learning. 2007 IEEE Interlligence and Security Informatics, 23-24 May 2007, New-Brunswick, NJ, USA, 2007.

[52] J. Xing, C. A. Manning. Complexity and Automation. Display of Air Traffic Control: Literature Review and Analysis. Final Report. Civil Aerospace Medical Institute, Federal Aviation Administration, Oklahoma City, OK (US) 73125, 20 pages, 2005.

[53] S. Rocco, D. Ferne Friedman-Berg, C. A. Manning. Application of Color to Reduce Complexity in Air Traffic Control. Technical Note number: DOT/FAA/CT-TN03/01, Federal Aviation Administration, Human Factors Division, Document is available to the public through the National Technical Information Service, Springfield, VA (US) 22161, 54 pages, 2002.

[54] M. Histon, J. Hansman. The Impact of Structure on Cognitive Complexity in Air Traffic Control. Report number: ICAT-2002-4, MIT International Center for Air Transportation, Department of Aeronautics & Astronautics, Massachusetts Institute of Technology, Cambridge, MA (US) 02139, 95 pages, 2002.

[55] M. Rehak, J. Tozicka, M. Pechocek, M. Prokopova, L. Foltyn. Autonomous Protection Mechanisms for Joint Networks in Coalition Operations. Integration of Knowledge Intensive Multi-Agent Systems, KISMAS 2007, 2007.

[56] A. Kanso, M. Toeroe, A. Hamou-Lhadj, F. Khendek. Generating AMF Configuration from Software Vendor Constraints and User Requirements. In Proceedings of the 4th International Conference on Availability, Reliability and Security (ARES'09), IEEE CS, Fukuoka, Japan, 2009.

[57] S. Antonatos, M. E. Locasto, S. Sidiroglou, A. D. Keromytis, E. Markatos. Defending Against Next Generation Attacks Through Network/Endpoint Collaboration and Interaction. In Proceedings of the 3rd European Conference on Computer Network Defense (EC2ND), 2007.

[58] J.-H. Cho, I.-R. Chen, P.-G. Feng. Effect of intrusion Detection on Failure Time of Mission-Oriented Mobile Group Systems in Mobile Networks. In Proceedings of the 14th IEEE Pacific Rim International Symposium on Dependable Computing, 2008.

[59] B. Pahlevanzadeh, A. Samsudin. Distributed Hierarchical IDS for MANET over AODV+. In Proceedings of the 2007 IEEE International Conference on Telecommunication and Malaysia International Conference on Communications, 14–17 May 2007.

[60] FELEX Project. Halifax Class Modernization/Frigate Life Extension Project (HCM/FELEX). DND contract number 2586 (448, 2697, 2778, 2783), 2010.

[61] J. C. Doyle, B. A. Francis, and A. R. Tannenbaum. Feedback Control Theory. Dover Publications inc, New York, ISBN 0-486-46933-6, 1992.

[62] X. Ou, S. R. Rajagopalan, and S. Sakthivelmurugan. An Empirical Approach to Modeling Uncertainty in Intrusion Analysis. Annual Computer Security Application Conference, ASAC '90, 7-11 December 2009, 2009.

[63] R. E. Sawilla. and C. N. Burrell. Course of action recommendations for practical network defence. DRDC Ottawa TM 2009-130. Defence R&D Canada – Ottawa; August 2009.

[64] P.-M. Fournier and M. R. Dagenais. Analyzing blocking to debug performance problems on multi-core systems. ACM SIGOPS Operating Systems Review, volume 44, number 2, 2010, pages 77-87.

[65] M. Desnoyers and M. Dagenais. LTTng : Tracing across execution layers, from the hypervisor to user-space. In Proceedings of the 2008 Linux Symposium, (Ottawa, Canada), July 2008.

[66] M. Desnoyers and M. Dagenais. LTTng, filling the gap between kernel instrumentation and a widely usable kernel tracer. In Proceedings of the 3rd Annual Linux Foundation Collaboration Summit, (San Francisco, California), 2009.

[67] E. Clement and M. Dagenais. Traces synchronization in distributed networks. Journal of Computer Systems, Networks, and Communications, vol. 2009, 2009.

[68] J.-H. Deschenes, M. Desnoyers, and M. Dagenais. Tracing Time Operating System State Determination. The Open Software Engineering Journal, vol. 2, pp. 40-44, 2008.

[69] S. K. Card, J. D. Mackinlay and B. Shneiderman. Readings in Information Visualization: Using Vision to Think. Morgan Kaufmann Publishers, 1999.

[70] J. J. Thomas and K. A. Cook. Illuminating the Path: The Research and Development Agenda for Visual Analytics. ISBN 0-7695-2323-4, 2005. http://nvac.pnl.gov/agenda.stm

[71] D. Holten, B. Cornelissen, J. J. van Wijk. Trace Visualization Using Hierarchical Edge Bundles and Massive Sequence Views. Proceedings of IEEE International Workshop on Visualizing Software for Understanding and Analysis (VISSOFT) 2007, pages 47-54, 2007.

[72] N. Henry, J.-D. Fekete, M. J. McGuffin. NodeTrix: A Hybrid Visualization of Social Networks. IEEE Transactions on Visualization and Computer Graphics (TVCG), 13(6), November/December 2007, pages 1302-1309, 2007.
[73] D. Beermann, T. Munzner, and G. Humphreys. Scalable, Robust Visualization of Large Trees. Proceedings of Eurographics / IEEE VGTC Symposium on Visualization (EuroVis) 2005, pages 37-44, 2005.
[74] K. Abdullah, C. Lee, G. Conti, J. A. Copeland, and J. Stasko. IDS RainStorm: Visualizing IDS Alarms. Proceedings IEEE Workshops on Visualization for Computer Security (Minneapolis, USA, 2005). IEEE Computer Society, 2005.
[75] J. Roberts. State of the Art: Coordinated & Multiple Views in Exploratory Visualization. International Conference on Coordinated and Multiple Views (CMV) 2007.
[76] A. Inselberg. The Plane with Parallel Coordinates. Visual Computer, 1985, 1, pages 69-91, 1985.
[77] N. Elmqvist, P. Dragicevic, J.-D. Fekete. Rolling the Dice: Multidimensional Visual Exploration using Scatterplot Matrix Navigation. IEEE Transactions on Visualization and Computer Graphics (TVCG), 14(6), pages 1141-1148, 2008.
[78] C. Ware. Designing with a 2 1/2D Attitude. Information Design Journal, 10(3), pages 255-262, 2001.
[79] M. J. McGuffin, I. Jurisica. Interaction Techniques for Selecting and Manipulating Subgraphs in Network Visualizations. IEEE Transactions on Visualization and Computer Graphics (TVCG), 15(6), November/December 2009, pages 937-944, 2009.
[80] Sawilla, R. E. and Ou, X. Identifying Critical Attack Assets in Dependency Attack Graphs. Proceedings of the 13th European Symposium on Research in Computer Security, 13, 18–34, 2008.

Also, For Criterion 6) Only, Please Enter a Self Score (from A to D) here C
(see the Following Criteria Language Ladder (CLL))

SCORE	The project's technology:
A	Has some potential to impact defence/military operations
B	OR, has some potential for improvements in capabilities or protection
C	OR, has strong potential for significant improvements in capabilities or protection
D	AND is likely to precipitate a disruptive change in a number of defence and/or military practices

7). Describe the project's Contribution to the Defence S&T Strategy (Weight = 1.5)

The new techniques that will be developed in this project, combined with the central processing unit (CPU) power of current and future computing devices, gives rise to new CND capabilities that were not possible a decade ago. Because computers are pervasively used all over the DND, this technology opens the door to major advances against many of the challenges of the Defence S&T Strategy. Essentially, the ng-CS2 will provide continually updated H-SA, from which it will be possible to deduce a lot of unprecedented information on systems (i.e., health states, presence of anomalies, levels of service degradation, adversary activities and intents; **Challenge 1.1**). This information will help determine the trust officers can have in their systems, as well as inform the decision-making process during C2 operations (more particularly in CND C2) (**Challenges 1.1, 1.3**). Other connections with the S&T Strategy in relation to the human-machine interface and advanced interaction control mechanisms will significantly improve human systems integration (**Challenge 10.2**). The interoperability of the ng-CS2 (host-based analyses) with other national security systems (network-based analyses) [8, 9, 10] will bring a significant contribution to the resolution of national-level problems, early in the contamination process (**Challenges 1.5, 2.2**). The scientific literature clearly demonstrates that network and host-based surveillance systems complement each other [1]. They must be used together, in different decentralisation patterns, to be able to support Computer Network Operations (CNO) in any type of operational context [55–59]. Hence, it will be possible to install the ng-CS2 on most types of Linux-based information systems (i.e., C2IS, cell phones, specialised autonomous sensors, autonomous vehicles, etc.) (**Challenges 3.1, 5.1, 6.1**). Future DRDC S&T projects will have access to the knowledge and technologies issuing from this research, allowing adaptation of the ng-CS2 to other types of operating systems (such as Microsoft's). Finally, the ability to save on disc H-SA for later deep analyses will contribute to the optimisation of information systems (including CND systems for cyber surveillance and protection) according to the requirements of vulnerability, survivability, and maintainability (**Challenge 6.2**).

8). Describe the specifics and extent of Capability Development resulting from the proposed project (Weight = 1.5):

Given the exploratory nature of the proposed research, most of the innovations generated by this TIF project will be proofs-of-concept; R&D prototypes will have to be re-implemented to become operational technologies. The LKB is the most practical outcome that could be reused directly by the security community. However, close contact will be maintained with the Frigate Life Extension (FELEX) Project [60] that will be used as our **reference operational environment** and with Lockheed Martin Canada that is the prime FELEX contractor for the new C2IS. The choice of the internal and external project members, collaborative tools, and development methodologies (a combination of the iterative, incremental, and spiral approaches) was made in order to maximise the return on DRDC investment. Three defence scientists (DSs) from DRDC Valcartier will get a direct benefit from this research. They will be directly involved in all R&D and prototyping activities, favouring a continual acquisition and utilisation of technologies, expertise and knowledge, and establishing a strong basis with external partners for after-the-project continuation of this effort. Professor Hamou-Lhadj from Concordia University (deep and refined software trace abstraction, analysis, and visualisation), Professor Dagenais from Polytechnique Montréal (deep Linux-based system analysis and advanced Linux-based tracing tools), and Professor McGuffin from École de technologie supérieure (advanced visualisation techniques for adapted reporting) will be hiring graduate students to perform the research tasks under their supervision (i.e. highly-skilled personnel in cyber security available for future recruitment). Industrial and DND participants are: Lockheed Martin Canada (Mr. D. Knight) (likely through a DND/NSERC Program) and Mr. J. Cai from DND (engineer for the FELEX project [60]). Mr. R. Sawilla will be the DRDC Ottawa Scientific advisor (interoperability of the ng-CS2 with the JNDMS, ARMOUR, and Net C2 ISAC DRDC projects [8, 9, 10]).

5. External Referee Suggestions **(Please ensure Conflict of Interest is Avoided, and that proposed referee is available and agrees to participate)**

Salutation/First/Last/Affiliation	**Area of Expertise**	**Address / Phone / E-mail**
Dr / Rei / Safavi-Naini / University of Calgary	Cryptography: Information theoretic security, Provable security, Information security: Privacy Enhancing Systems, Rights Management, Network Security	Department of Computer Science, Room 636, ICT Building, 2500 University Drive, NW Calgary, AB, T2N 1N4, CANADA / +1 403 210 5492 / rei@ucalgary.ca
Dr / Ravin / Balakrishnan / University of Toronto	Software visualization, Human computer interaction, Usability analysis	Department of Computer Science University of Toronto 10 King's College Road, Room 3302 Toronto, On, Canada M5S 3G4 / (416) 978-5359 / ravin@dgp.toronto.edu
Dr / Shengdong / Zhao / National University of Singapore	Human-Computer Interaction	National University of Singapore / (+65) 6516-8413 / zhaosd@comp.nus.edu.sg
Dr / Kaleem / Siddiqi / McGill University	Visual shape analysis for computer vision, drawing on techniques from singularity theory, partial differential equations and graph theory, image processing and medical image analysis.	School of Computer Science, 3480 University Street, Montreal, Qc, Canada H3A 2A7 / +1-514-398-3371 / siddiqi@cim.mcgill.ca
Dr / Mohamed / Mejri / Laval University	Software Certification, Malware detection, Intrusion detection systems, Software security	Department of Computer Science and Software Engineering, Université Laval, Québec (QC), Canada, G1V 0A6 / (418) 656-2131 # 12816 / Mohamed.Mejri@ift.ulaval.ca

6. Financial Summary

Planning Year	Year 1	Year 2	Year 3	Total
A. FUNDING REQUESTED FROM TIF PROGRAM k$:				
R&D CONTRACTS	250	260	180	690
PROJECT O&M	20	20	20	60
TOTAL TIF k$	**270**	**280**	**200**	**750**
B. INTERNAL CONTRIBUTIONS				
SWE (X 2.4)	385	385	385	1155
O&M (NON TRAVEL)				
R&D EQUIPMENT	20	20	20	60
TRAVEL	10	10	10	30
TOTAL LAB CONTRIBUTION k$	**415**	**415**	**415**	**1245**
RATIO: INTERNAL CONTRIBUTION TO TIF FUNDING (divide part B total into part A total, express as %) [MINIMUM 70%]				**166**

7. Quad Chart

TECHNOLOGY INVESTMENT FUND (TIF) PROJECT PROPOSAL 2010

SIGN-OFF SHEET

Project Title: C4ISR Host-Based Cyber Situation Awareness

Comments:

This TIF proposal addresses one of the most difficult aspects of computer systems surveillance: the detection of anomalies on running, distributed software intensive systems in real-time, when those systems can be compromised by a targeted attack. This automated detection is required to trigger a pro-active reaction to mitigate the effect on the systems. While this project looks at the real-time detection of anomalies, Philippe Charland's proposed TIF looks at the forensic analysis, after an incident, of the malicious code. Both projects technically require vastly different expertise. Mr Charland's project works at the assembly level, one program at a time, after an incident, while Mr. Couture's considers the host machine as a whole during operations. It is therefore my recommendation to keep both project separated to maximize their productivity and their impact. I recommend commitment of the internal resources required for this project.

Section Head Signature: _Guy Turcotte, C/SdS_______________ Date: __________________

Comments:

This TIF will contribute to the Command and Control S&T Areas and the Software Protection and Counter Measures challenge. Considering that the CF are in the process of the creating a new CYBER environment, the domain of software system surveillance requires an augmentation of efforts to cope with the complexity and threat on software intensive systems, as these systems are the principal pillar of C4ISR related technologies.

I concur with the suggested Peer Reviewers.

Chief Scientist Signature: _____Christian Carrier______________ Date: _______________

Comments:

I approve commitment of the internal resources required for this project, and am satisfied that the resources being requested are consistent with requirements for the proposed research.

DG Signature: ______Guy Vézina________________ Date:__________________