eSecurity portfolio

Overview, analysis of value added, and way ahead

Doug Hales
D Hales Consulting Inc.

Rodney Howes
Eric Cooper
Margaret Porter-Greene
Andrew Vallerand

DRDC Centre for Security Science

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2014-R113
November 2014

eSecurity portfolio

Overview, analysis of value added, and way ahead

Doug Hales
D Hales Consulting Inc.

Rodney Howes
Eric Cooper
Margaret Porter-Greene
Andrew Vallerand

DRDC Centre for Security Science

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2014-R113
November 2014

IMPORTANT INFORMATIVE STATEMENTS

The eSecurity Community of Practice is supported by the Canadian Safety and Security Program which is led by Defence Research and Development Canada's Centre for Security Science, in partnership with Public Safety Canada.

Canadian Safety and Security Program is a federally-funded program to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence.

Template in use: SR Advanced Template(PO)_EN_V.02.00_271114.dot

Abstract

The Centre for Security Science's eSecurity Community of Practice was created 5 years ago to give increased visibility and focus to a growing threat to public safety and security. With the establishment of an associated eSecurity portfolio, the cyber security projects were grouped facilitating management and fostering program coherence. This report traces the origins of the eSecurity portfolio and provides an overview of past and planned investment. It provides a consolidated listing of reports generated and a discussion of plans and priorities for the Way Ahead. It breaks ground by providing a comprehensive self-evaluation, an attempt to analyze the value added. Forty projects were examined using a five point assessment framework developed and applied recently to evaluate Chemical, Biological, Radiological and Nuclear (CBRN) Research and Technology Initiative projects. The results of the analysis suggest that the majority of eSecurity projects have indeed added value. They also indicate that the eSecurity program focus is shifting from knowledge generation to technology transition and support to operations, reflecting priorities of the Canadian Safety and Security Program.

Significance to defence and security

This report provides context and detail enabling stakeholders and eSecurity community members to appreciate the breadth and depth of the portfolio and consolidates and recaps deliverables enabling stakeholders to exploit past research and development efforts and to position themselves to propose new projects. It documents the second application of an evaluation framework previously developed

Résumé

La communauté de pratique de la sécurité électronique du Centre des sciences pour la sécurité a été créée il y a cinq ans afin d'offrir une visibilité accrue et de se concentrer sur une menace croissante à la sécurité publique. Avec l'établissement d'un portefeuille connexe de sécurité électronique, des projets de cybersécurité ont été regroupés afin de faciliter la gestion et de favoriser la cohérence des programmes. Le présent rapport décrit les origines du portefeuille de sécurité électronique, en plus de donner un aperçu des investissements passés et prévus. Il fournit une liste consolidée de rapports déjà produits et un examen des plans et des priorités concernant la voie à suivre. Les travaux sont amorcés en donnant une autoévaluation complète, une tentative d'analyser la valeur ajoutée. Quarante projets ont été examinés à l'aide d'un cadre d'évaluation en cinq points élaboré et récemment appliqué pour évaluer les projets d'initiatives de recherche et de technologie chimique, biologique, radiologique et nucléaire (CBRN). Les résultats de l'analyse suggèrent que la majorité des projets liés à la sécurité électronique ont en effet une valeur ajoutée. Ils indiquent également que la cible du programme de sécurité électronique passe du développement des connaissances à la transition technologique et l'appui aux opérations conformément aux priorités du Programme canadien de sûreté et de sécurité.

Importance pour la défense et la sécurité

Ce rapport précise le contexte et les détails permettant aux intervenants et aux membres de la communauté de la sécurité électronique de mesurer l'ampleur et la profondeur du portefeuille, en plus de consolider et de récapituler les produits livrables pour que les intervenants puissent tirer profit des efforts de recherche et de développement et qu'ils soient en mesure de proposer de nouveaux projets. Il décrit la deuxième application d'un cadre d'évaluation antérieur.

Table of contents

List of figures

[1] Note: during CSS renewal and harmonization formal Call for Proposals was not held thus the decreased project funding.

List of tables

1 Introduction

This section provides some background information relating to the origins of the Centre for Security Science (CCS), the development of Canada's Cyber Security Strategy (CCSS), and the establishment of the eSecurity portfolio.

1.1 CSS' background

CSS' origins can be traced back to the attacks on the World Trade Center on September 11th, 2001. As part of the federal government's Public Security Anti-Terrorism (PSAT) initiative, the Chemical, Biological, Radiological and Nuclear (CBRN) Research and Technology Initiative (CRTI) was launched in May, 2002. It represented the federal science & technology (S&T) community's response to 9/11, and intent to further collaboration and offer science solutions to CBRN terrorist threats. In 2006, following a formal evaluation, the Public Safety and Security S&T Program (PSTP) was introduced reflecting both the success of the CRTI model and a broadening perception of the security environment.

The CSS was established as a joint endeavor between the Department of National Defence (DND) and Public Safety Canada (PS) as a Defence Research and Development Canada (DRDC) Centre and new *mission areas* were added. These included Critical Infrastructure Protection (CIP); Surveillance, Intelligence & Interdiction (SII); and Emergency Management & Systems Interoperability (EMSI). CSS assumed responsibility for overseeing both the CRTI and PSTP. The Canadian Police Research Centre (CPRC) merged with CSS in 2007 and the merger expanded CSS' scope introducing and integrating police, fire and emergency medical services to federal S&T initiatives and reinforced links to the first responder community. The resultant Canadian Safety and Security Program (CSSP) is mandated "to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology (S&T) with policy, operations and intelligence"[2].

[2] Defence Research and Development Canada, http://www.drdc-rddc.gc.ca/en/science-tech/safety-security.page accessed 18 August 2014.

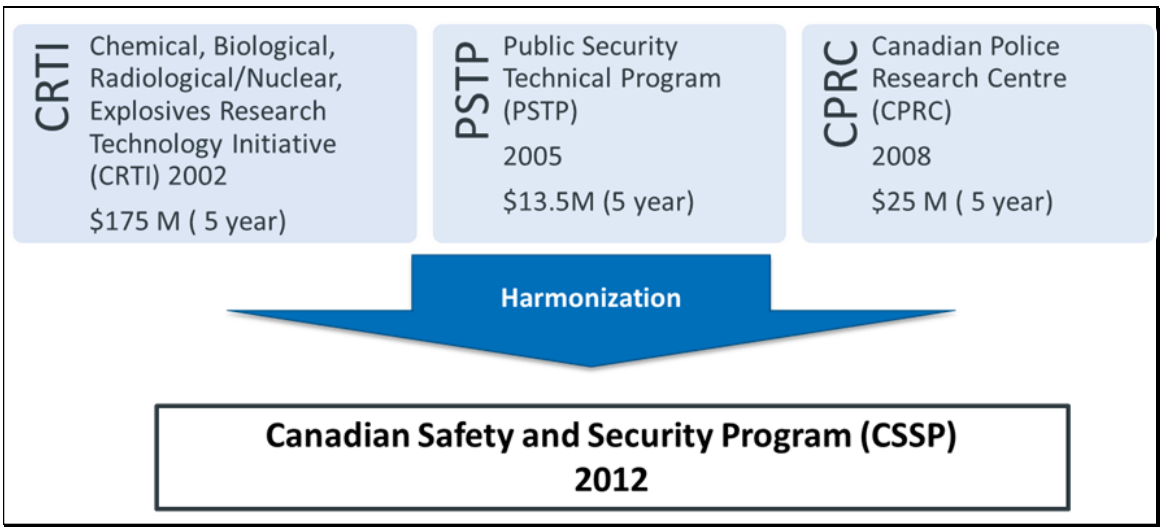


Figure 1: *CSSP harmonization.*

Elements of CRTI and PSTP were retained when the program was reviewed and refreshed in 2012 i.e., after a second 5 year term; specifically, the emphasis on leveraging science and technology and on partnerships. The Canadian Safety and Security Program (CSSP) both amalgamated prior mandates and provided for flexibility in investment distribution and program management.[3] Given the increasing pervasiveness and societal dependence on computers and telecommunication, it was natural for electronic security (eSecurity) to be increasingly identified as public safety and security concern.

1.2 Canada's cyber security strategy

The *National Strategy for Critical Infrastructure* (NSCI), published in 2009, defined critical infrastructure ("processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and effective functioning of government"[4]), distinguished ten critical infrastructure sectors (energy and utilities, finance, food, transportation, government, information and communication technology, health, water, safety and manufacturing) and described the fundamental concepts and principles underpinning the national strategy.

Canada's Cyber Security Strategy (CCSS) was published a year later.[5] It acknowledged Canadians' increasing dependence on information and networks, discussed threats and societal vulnerabilities, and underscored the importance of cyber security. The CCSS is built on three pillars:

[3] It is noteworthy that CSS and the CSSP is funded independently rather than deriving funds directly from DND.

[4] Public Safety Canada, Action Plan for Critical Infrastructure, Government of Canada, 2009 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/index-eng.aspx acessed 18 August 2014

[5] Public Safety Canada, Canada's Cyber Security Strategy, Government of Canada, 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx accessed 13 February 14

- Pillar 1: securing Government systems,
- Pillar 2: partnering to secure cyber systems outside the federal Government, and
- Pillar 3: helping Canadians to be secure online.

The CCSS establishes an overarching framework, i.e., a theoretical schema for developing relationships between goals, activities and actors.

1.3 eSecurity portfolio

As shown in Figure 2, the PSTP reflected an expansion in scope complementing the CRTI. Electronic security, eSecurity, was initially distinguished as an element of Critical Infrastructure Protection (CIP) one of the PSTP Mission Areas, as a target for threats now directed through the digital world (Table 1*)*.

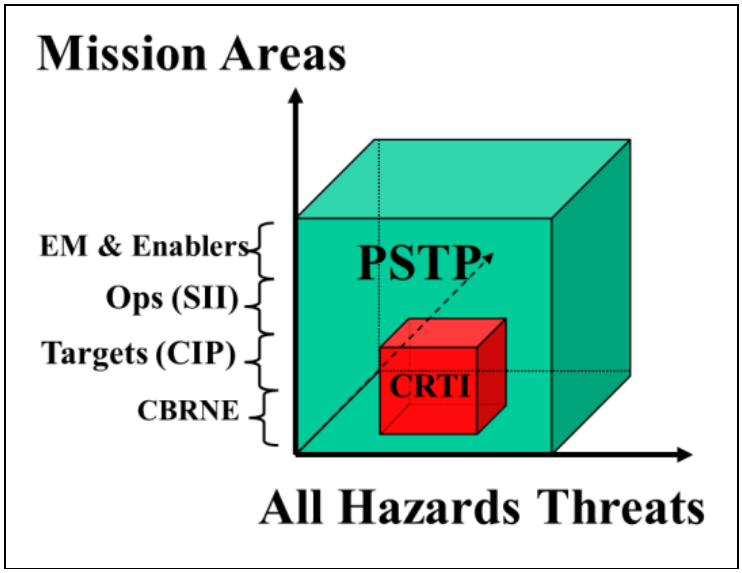


Figure 2: *CRTI & PSTP expansion.*

Table 1: *PSTP pillars.*

Defeat CBRNE Threat	**Critical Infrastructure Protection**
• Defeat Chemical • Defeat Biological • Defeat Radiological Nuclear • Defeat Explosives: (co-leads)	• Critical Infrastructure Vulnerability, Resiliency & Interdependencies • **e-Security (Cyber)**

Surveillance, Intelligence & Interdiction	**Emergency Management & Systems Interoperability**
• Biometrics for National Security • First Responder, Policing and Officer Safety • Border and Transportation Security liked to WG • Forensics	• Risk and Vulnerability Assessment • Emergency Management Systems Interoperability • Psycho-Social

With the introduction of the CSSP, eSecurity developed into a CSSP thrust/business line with its own Portfolio Manager (PM) and Community of Practice (CoP). The focus of CSSP, as with the prior CRTI and PSTP programs, remains horizontal i.e., multi-departmental, cross-jurisdictional and interdisciplinary. By direction and design CSS eschews infringing on areas that have been assigned by law or practice to other Government departments, boards or agencies. Further, it was decided that the CSS should avoid incremental investments in S&T initiatives which are progressing and receiving funding through other programs. Insofar as possible the CSSP, and eSecurity, should focus on addressing operational gaps by complementing these programs and leveraging the outputs of these investments.

With this in mind CSS has steered clear of investing directly in supporting Pillar 1. Responsibility for *Securing Government Systems* rests with Treasury Board, Shared Services and the Communications Security Establishment Canada. CSS determined that it could exploit and strengthen its links to industry and academia and contribute more to Pillars 2 and 3. The eSecurity related portfolio of projects reflects this intent.

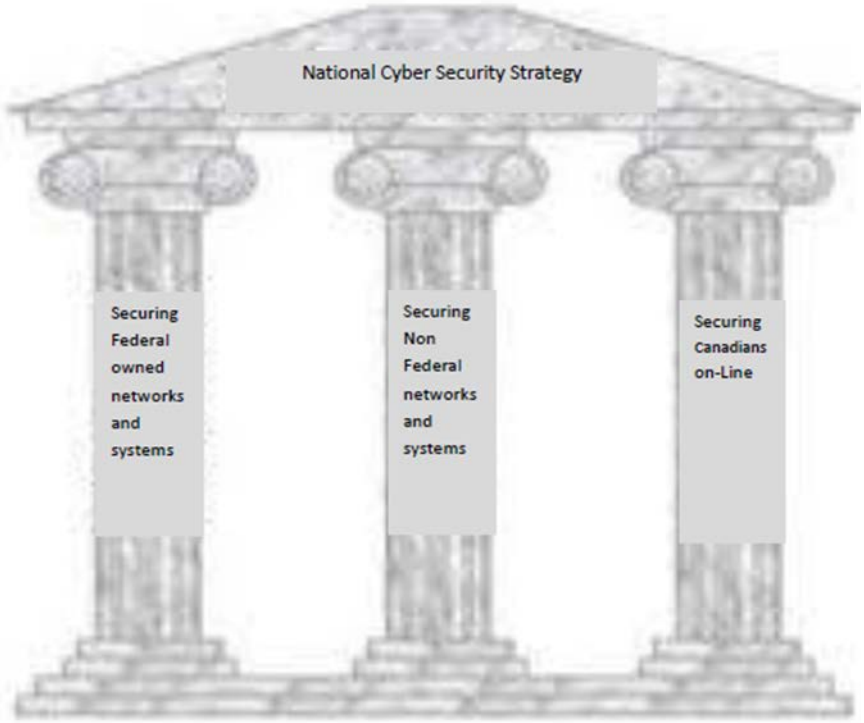


Figure 3: *Canada's cyber security strategy pillars1-2-3.*

2 Characterization frameworks

There are several perspectives through which the eSecurity portfolio can be assessed. Although there is some overlap; in general, each provides a unique and complementary view.

2.1 Investment

Inputs consisting of resources (financial and non-financial resources) are used to support portfolio activities, produce outputs, and create value. Measuring inputs provides a base for determining return on investment and, for horizontal initiatives, a sense of commitment. Generally it is easier to quantify inputs.

2.2 Program view

The first perspective provides a programmatic view. It can be used to characterize the eSecurity portfolio in terms of the CSSP delivery instruments:

- **Competitive Call for Proposals (CFP):**
  - Innovative ideas to address identified risks, vulnerabilities and capability gaps.
- **Targeted Investments (TI):**
  - TIs allow for direct funding of projects and activities proposed by portfolio managers that address critical gaps/investment priorities that are not being addressed adequately through the Call for Proposals (CFP) or other processes.
- **Community Development (CD):**
  - Action-oriented communities of practice build Canadian capability through technology acquisitions, studies, response capabilities, workshops and exercises.
- **Technology Acquisition (TA):**
  - TAs are funded through Vote 5 (Capital Expenditures) and the funds are transferred to the lead federal department through the supplementary estimates process. These acquisition projects are typically funded to a maximum of $200K and are completed within one fiscal year (FY).

2.3 CCSS logic model

Canada's Cyber Security Strategy (CCSS) was published in 2010.[6] It acknowledged the increasing dependence on information and networks, discussed threats and societal vulnerabilities, and underscored the importance of cyber security. Three pillars were identified and funding was provided to support realization of the CCSS. The three pillars included:

[6] Canada's Cyber Security Strategy, Public Safety, 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf accessed 13 December 2013

- Securing Government systems,
- Partnering to secure cyber systems outside the Federal Government, and
- Helping Canadians to be secure online.

A Logic Model (Figure 4) was subsequently developed by PS (with input from key stakeholders) to assist in aligning CCSS programs across departments and agencies and in assessing progress in implementing the CCSS. A Logic Model has been described as: a systematic and visual way to present the relationships between the resources an organization has to operate with, the activities the organization plans and the results the organization hopes to achieve"[7]. The CCSS Logic model reflects an attempt to articulate the CCSS and establish an analytical framework. This enables prime /lead responsibility for outcomes and activities and key supporting contributors to be identified. CCSS earmarked resources were apportioned accordingly. The model helps to draw attention to DRDC/CSS' role in implementation of the CCSS and specifically charges the Centre with responsibility to develop a focused S&T program and contribute to increasing Canada's cyber security related research & development capacity.

[7] NATO Joint Analysis and Lessons Learned Centre, A framework for the Strategic Planning and Evaluation of Public Diplomacy, 2013, pg. 6, http://www.jallc.nato.int/newsmedia/docs/A%20Framework%20for%20the%20Strategic%20Planning%20and%20Evolution%20of%20Public%20Diplomacy.pdf accessed 18 August 2013

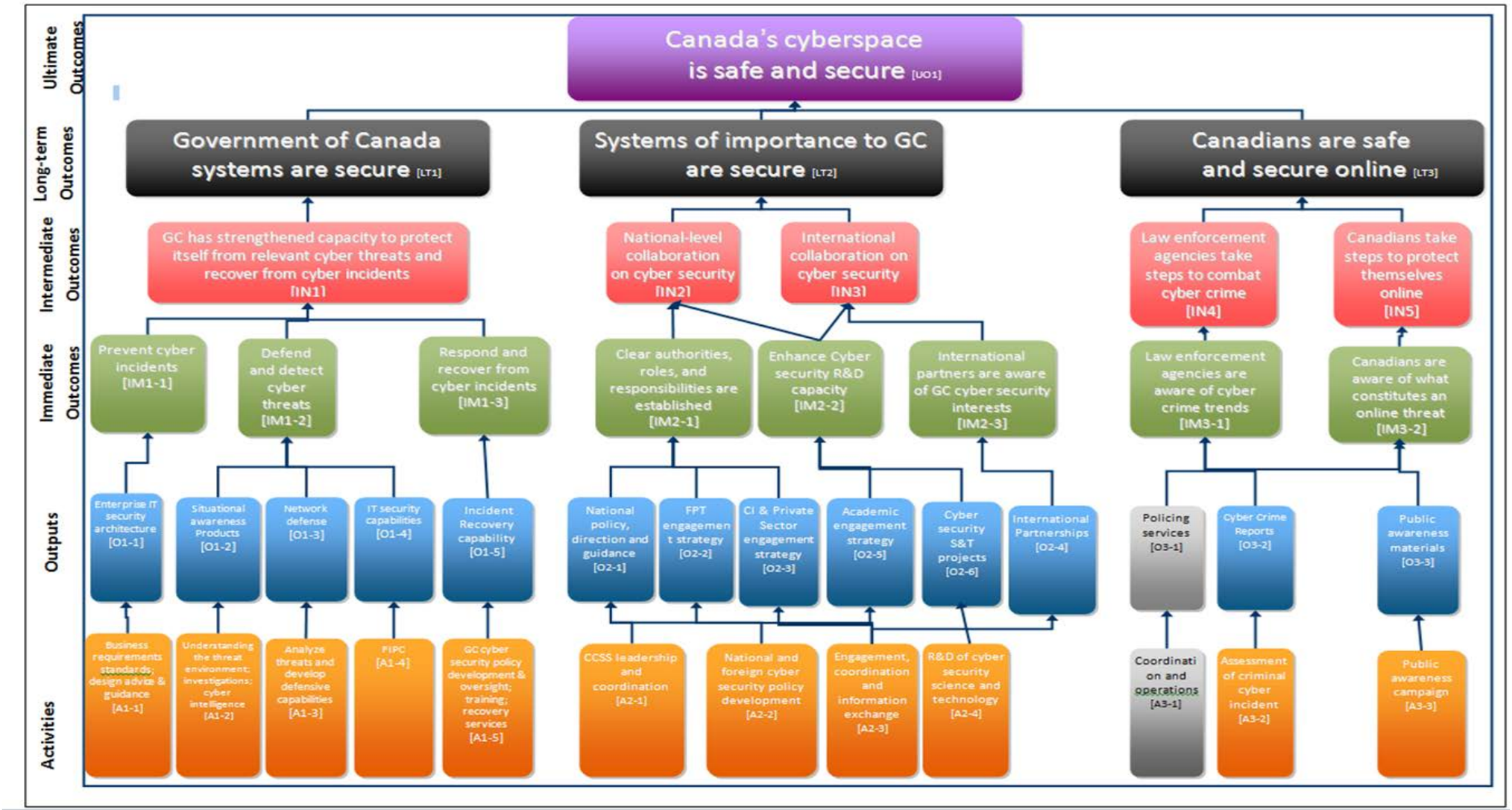


Figure 4: CCSS Logic Model.

2.4 Emergency management sectors

In addition to the three CCSS pillars, the Federal Government and Public Safety Canada have distinguished ten Critical Infrastructure Sectors:

- Energy and Utilities – electrical power, natural gas, oil production and supporting transmission systems;
- Finance – banking, securities, investments, integrity of the banking systems;
- Food – production, sales and use nodes, distribution systems;
- Transportation – roads, air, rail, and marine travel and transport;
- Government – public services and facilities, information and informational networks;
- Information and Communication Technology – telexcommunications, broadcasting;
- Health – Hospitals, healthcare services, and blood supply;
- Water – drinking and waste water management;
- Safety –hazardous substances, explosives, and nuclear waste; and
- Manufacturing – chemical and strategic manufacturers.

These 10 Critical Infrastructure Sectors are depicted below (Figure 5). In essence Pillar 2 (see Figure 3) has been rotated and dissected. These can also be related to the Emergency Response Functions identified in the Federal Emergency Response Plan (FERP).[8]

[8] Public Safety Canada, Federal Emergency Response Plan, January 2011, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf accessed 10 July 2014

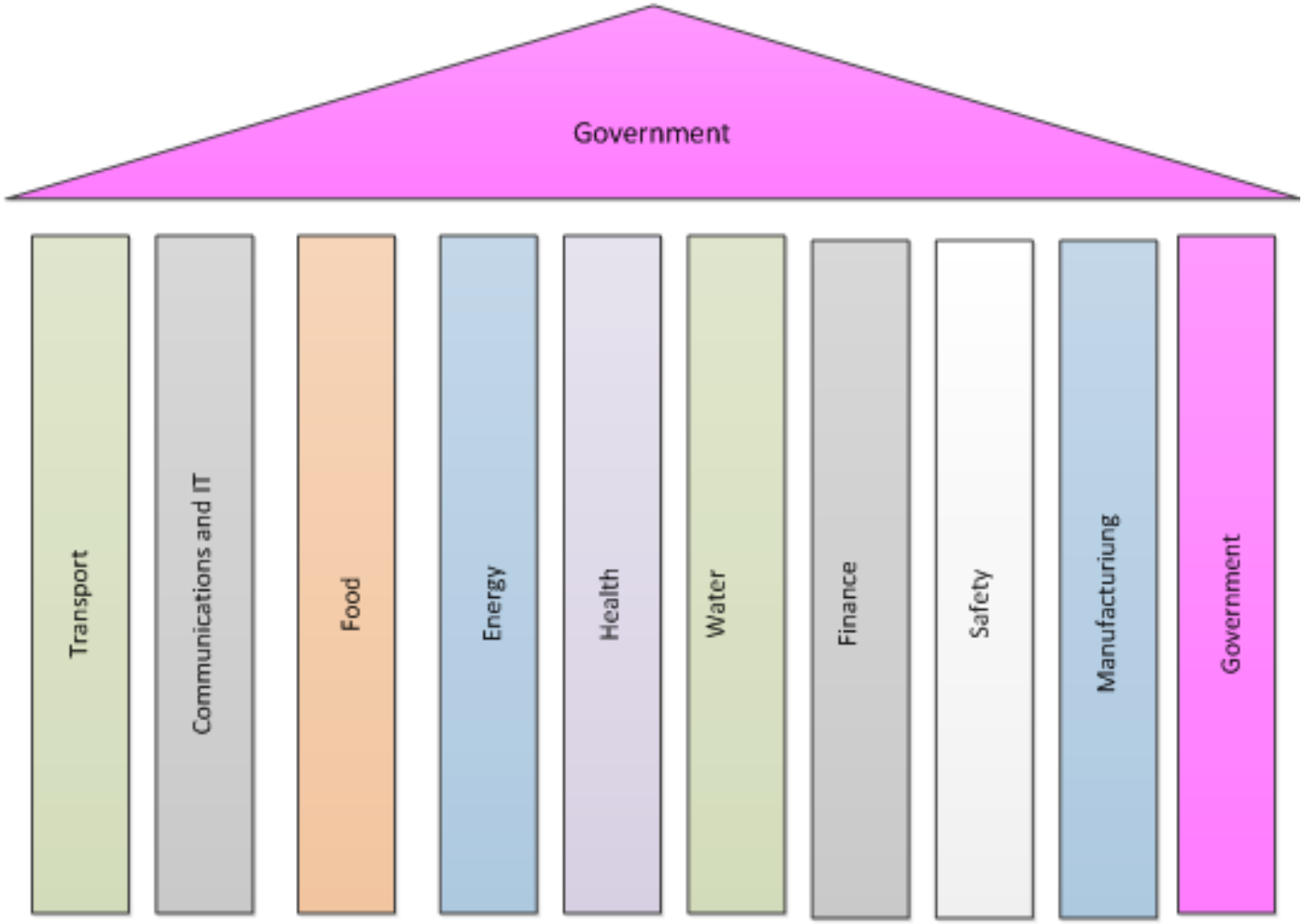


Figure 4: *Critical infrastructure sectors.*

3 Characterization analyses

3.1 Investment

The investment in eSecurity has grown steadily. In 2009 PSTP made provision for a dedicated Portfolio Manager. During the harmonization of the 3 CSS program to become CSSP Cyber Security remain a key priority. CSSP investment by year is illustrated below (Figure 6 and Figure 7). Projects may span more than one fiscal year; hence, the distinction drawn between expenditure commitments and fiscal year allocations. It is also important to note that CSSP projects are not funded completely by CSSP. Partner organizations co-invest in projects either with funding or, more, commonly, by allocating resources such as staff or laboratory time. Total investment i.e., CSSP + partners is captured in Figure 8. As shown, interest and investment in eSecurity and cyber-related projects increased significantly in 2013.

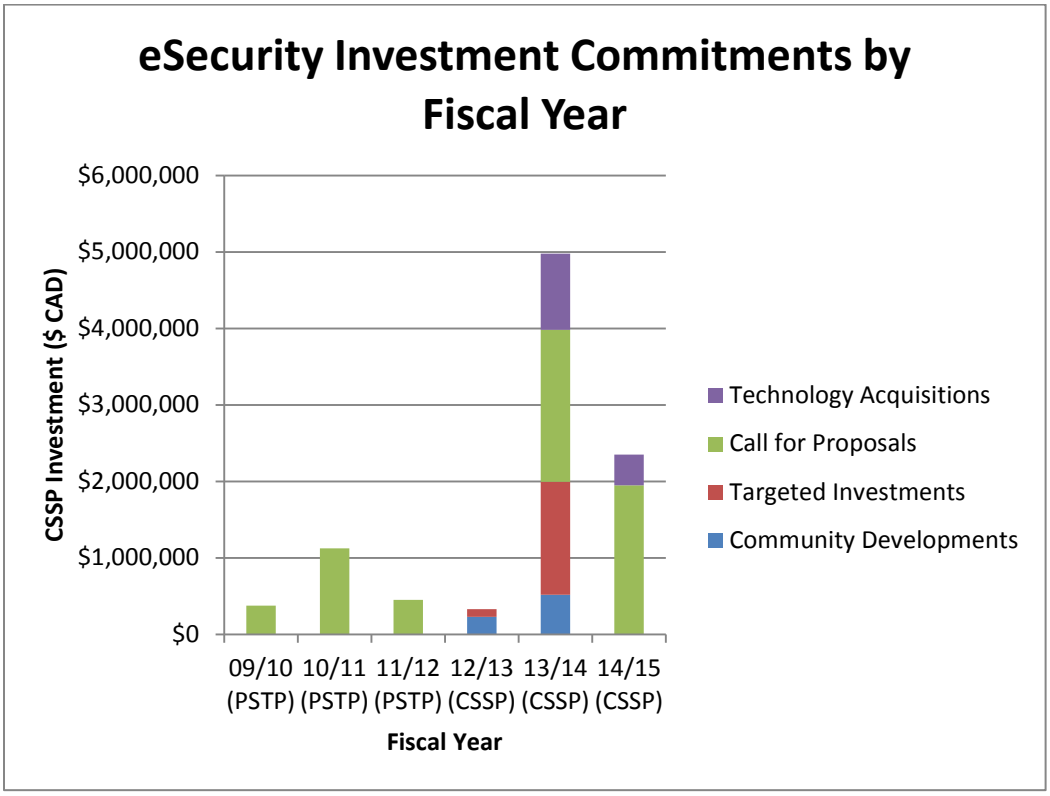


Figure 5: *Investment commitments by fiscal year*[9].

[9] Note: during CSS renewal and harmonization formal Call for Proposals was not held thus the decreased project funding.

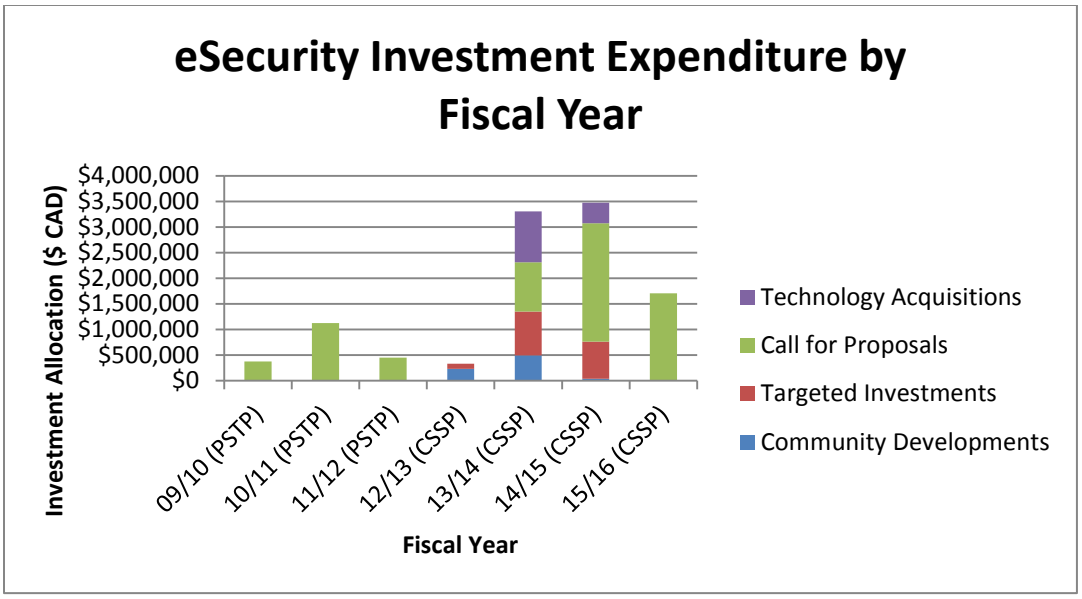


Figure 6: *CSSP investment allocation by fiscal year.*

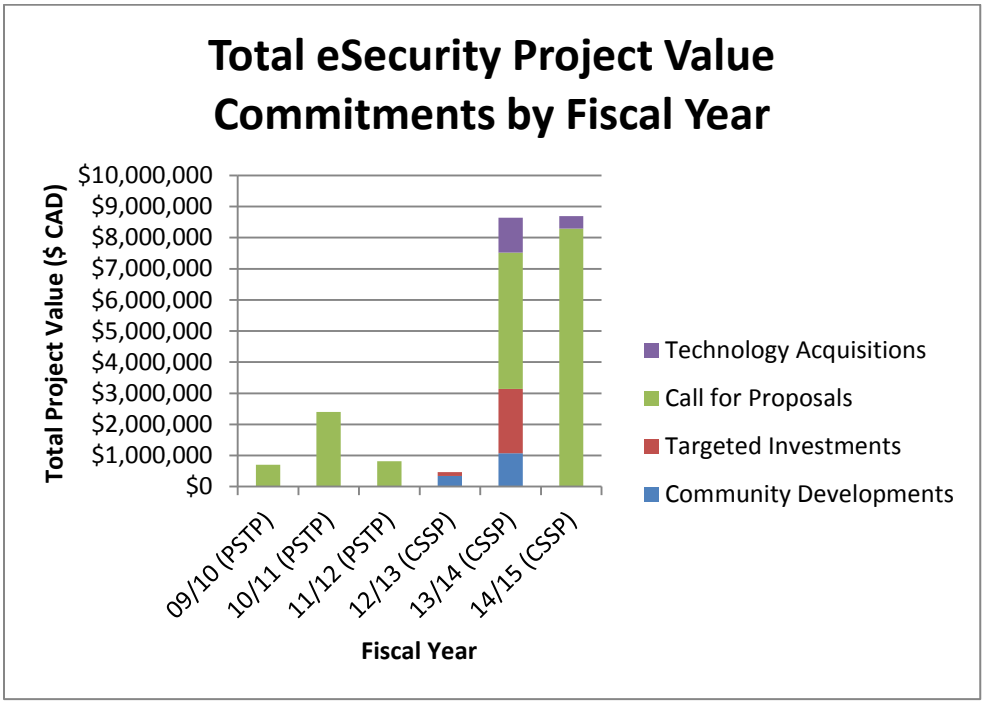


Figure 7: *Total project investment by fiscal year.*

Figure 6 and Figure 8 depict absolute growth. The CSSP itself has grown over time. Figure 9 illustrates relative growth i.e., the portion of PSTP and CSSP funding that has been allocated to eSecurity initiatives. As can be seen, relative growth has been uneven. Arguably this should be expected as events and/or proposals inform portfolio program allocations.

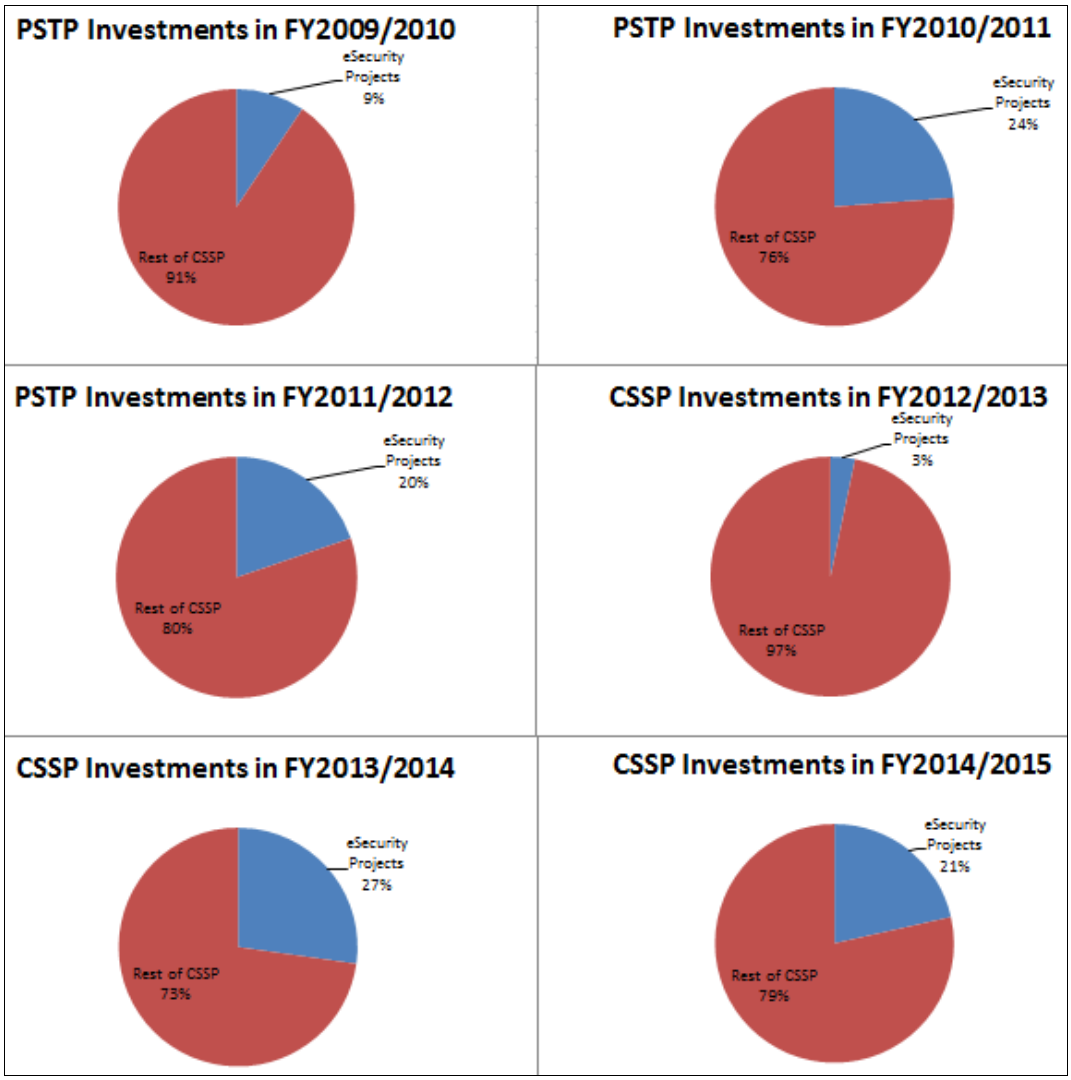


Figure 8: *Relative growth of the eSecurity portfolio.*

Cyber security will continue to be an investment priority for CSS reflecting in part the pervasiveness and reliance on information and communications technology. Cybercrime poses a threat to Canadians' prosperity and safety, when one has visibility and takes into account the enormous global scale of stolen credit cards, pre-paid cards, as well as goods that are contraband, counterfeit and illicit whites. The losses are in the billions[10] of dollars and Intelligence suggests that it is easier to steal just about anything digitally than physically. Documented cases of counterfeit ball bearings and counterfeit airbags (the latter dispersed shrapnel) attest to cyber related supply chain safety concerns. The recently completed CSSP Environment Scan also

[10] Norton. (2013). "2013 Norton Report." Symantec. http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.en_ca.pdf (accessed October 27, 2014). Canada's Cyber Security Strategy, Public Safety, 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf page 4 accessed October 27, 2014

concluded that "cyber security has quickly come to be regarded as a critically important dimension of national security". "Cyber-sabotage is a particularly acute concern given the critical infrastructure vulnerabilities" and "actors lacking the military capability to engage an adversary directly could conceivably employ cyber-attacks as an alternative".[11]

3.2 Project type

Whereas the PSTP was restricted to studies and, as noted previously, the CSSP has a number of investment options depending on the nature and scope of the project. These include Call for Proposals, Targeted Investments, Community Development, and Technology Acquisitions. Figure 10 depicts eSecurity investment by project type. The eSecurity portfolio reflects the CSSP move away from studies and towards a focus on outcomes. The FY 13/14 graphically illustrates how full advantage was taken of all investment vehicle options. It is early into FY 14/15 cycle so may be premature to draw conclusions and there are some drawbacks to representing the portfolio this way. For instance, it does not show that several of the recently approved projects are multiyear undertakings e.g., 2 of the 3 FY 13/14 TIs are two year projects. Figure 10 might be more accurately described as eSecurity Start-ups by type. Numerical comparisons are also problematic; in FY 14/15 related proposals were combined. In previous years, the 4 proposals were likely have been managed and tallied as separate projects. The lack of CDs reflects a CSSP reorientation described in more detail later.

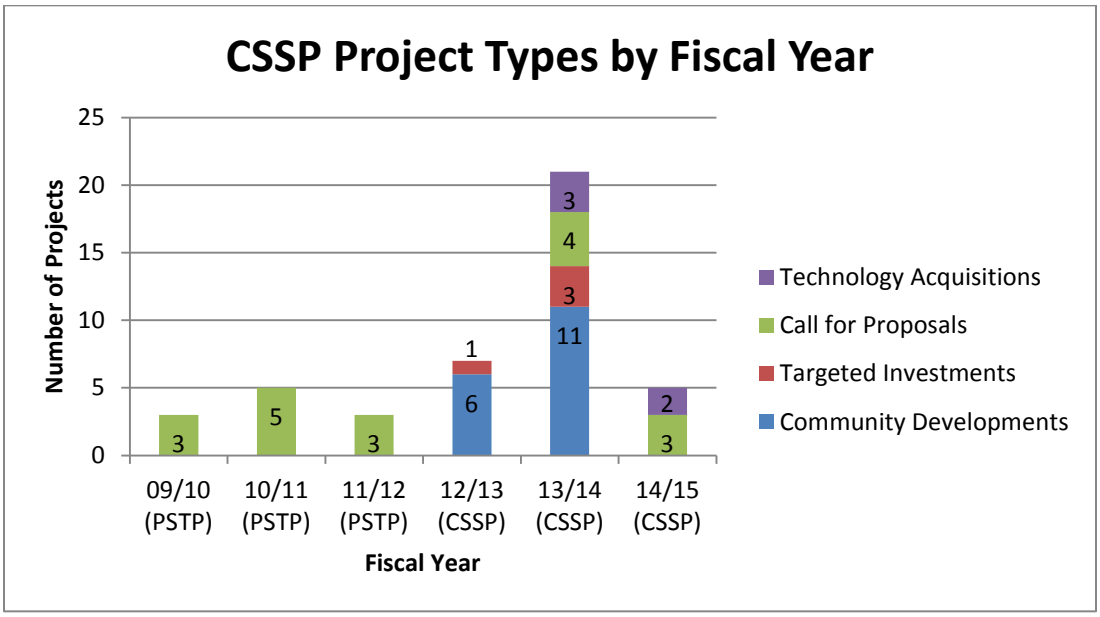


Figure 9: *eSecurity project types.*

3.3 Partnerships

Caution must also be exercised in interpreting the following graphs reflecting eSecurity project partnerships and community of practice demographics. Few projects were initiated in FY 11/12

[11] Centre for Security Science, CSSP Environmental Scan 2013, May 2014, pg 3,4.

(3) and in FY 12/13 (7) and participation was uneven as depicted in Figure 11. Details can be found in Annex B - Critical Infrastructure Sectors and Partners. A more equitable balance between government, industry and academia has been restored.

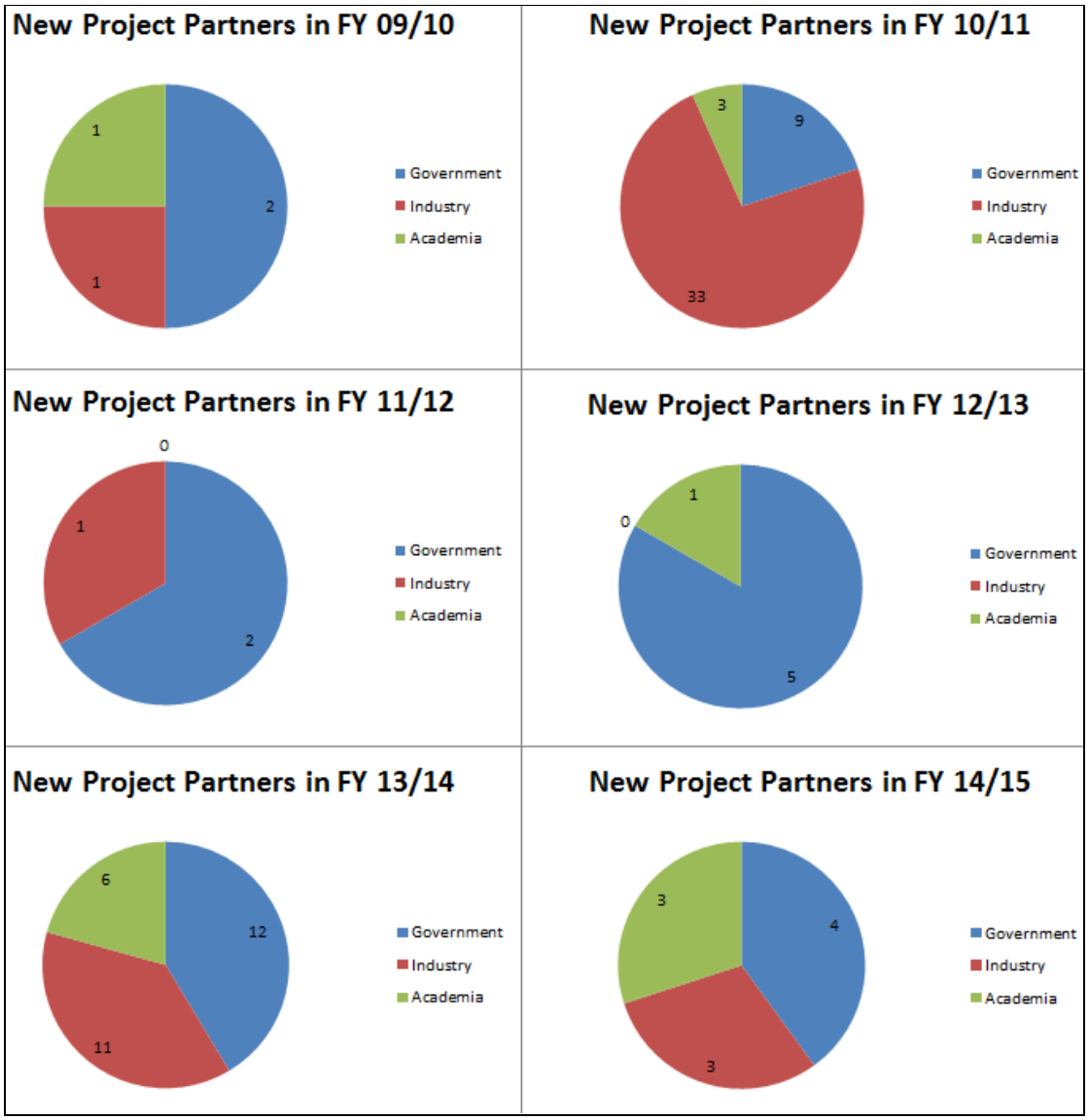


Figure 10: *eSecurity partnerships – pie chart.*

Presenting this information as a bar chart (Figure 12) provides insight into absolute numbers. FY 11/12 is an anomaly – a large number of community members participated in one project; thirty-five partners took part in PSTP 02-347eSec Study in Cyber Security and Threat Evaluation in SCADA Systems.

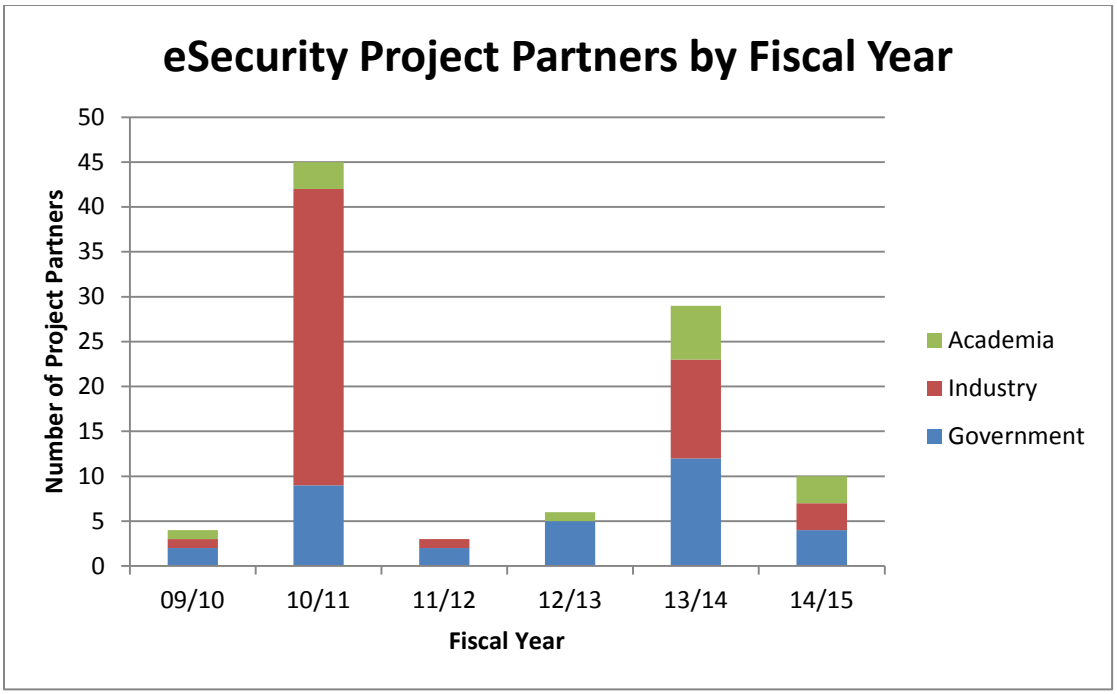


Figure 11: *eSecurity partnerships – bar chart.*

Figure 13 presents an aggregate view which provides a useful overarching perspective but conceals variances and makes it difficult to determine trends.

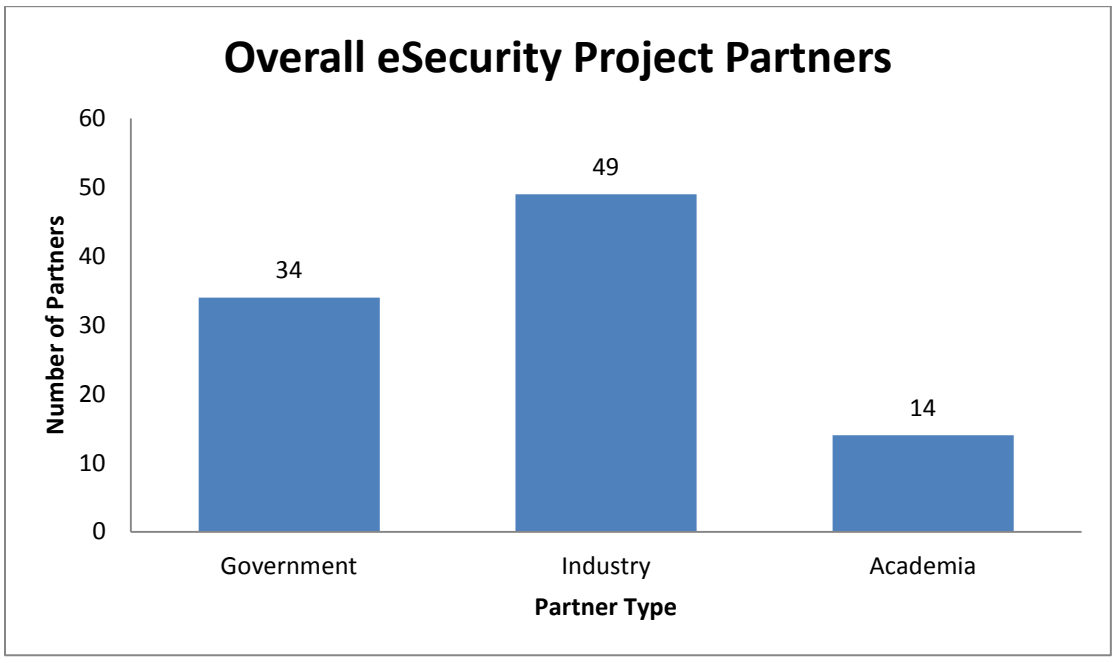


Figure 12: *eSecurity partners – aggregate view.*

3.4 Co-investment

The CSSP is founded on a philosophy of shared value. Figure 14 depicts co-investment by partners by fiscal year. As might be expected, the growth in co-investment parallels the growth in CSSP investment in the eSecurity portfolio. The data presents no surprises but offers confirmation of engagement and commitment by partners.

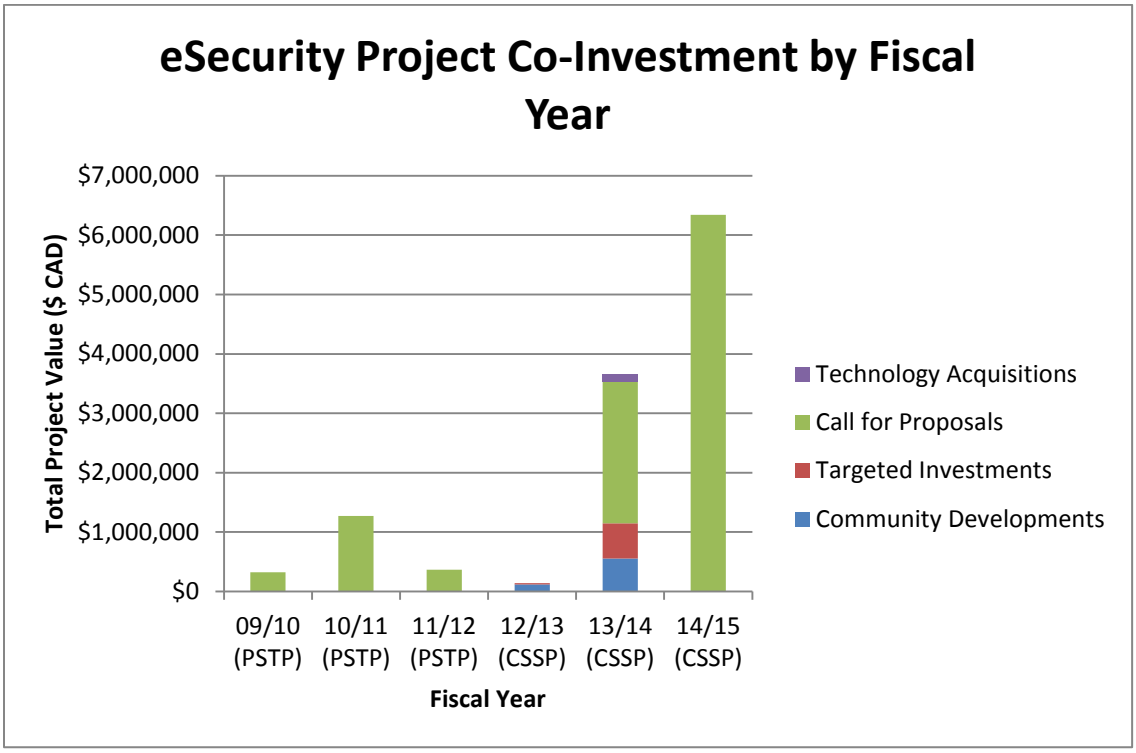


Figure 13: *eSecurity portfolio- Co-investment.*

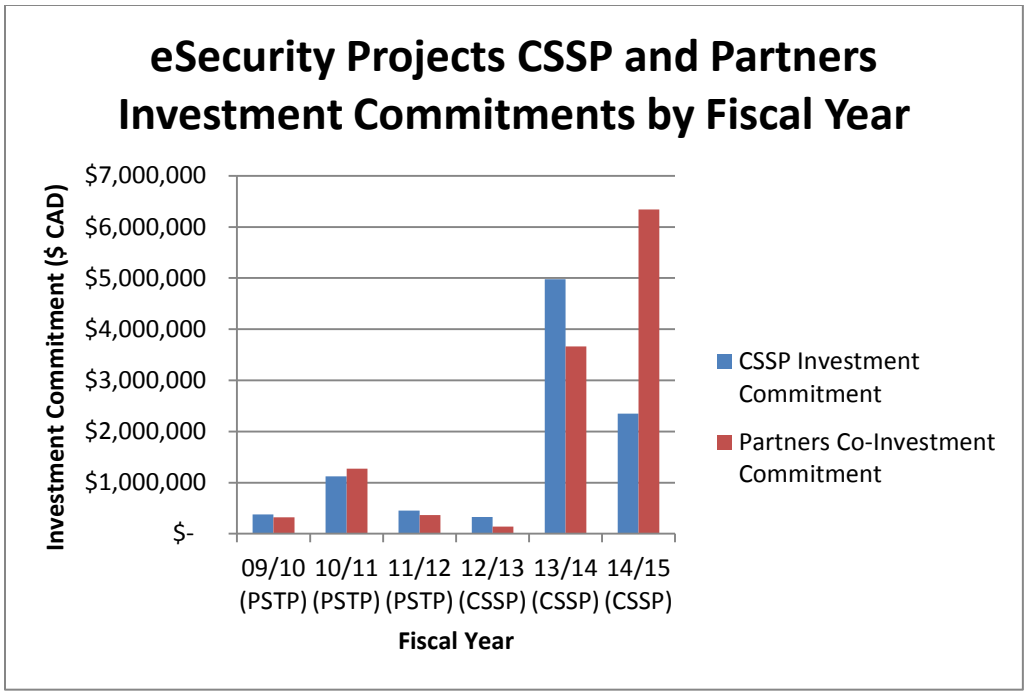


Figure 14: *eSecurity portfolio- comparing CSSP and partner investments.*

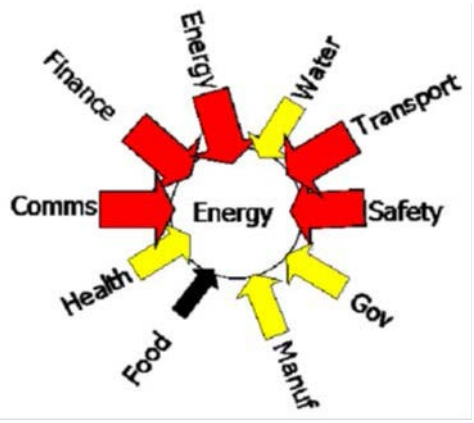
3.5 Investment by sectors

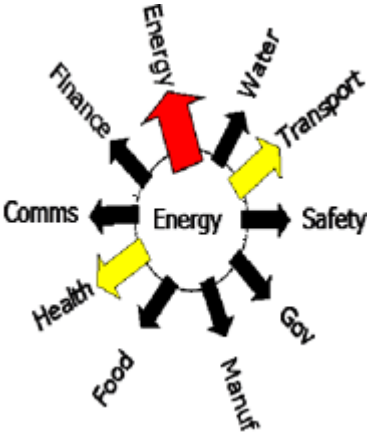
CSS' eSecurity program has made a conscious effort to focus on Pillar 2 and initially on the telecommunications, energy and finance sectors. In characterizing eSecurity investment, it was found that a number of projects focused on general rather than sector specific threat appreciation and awareness or development of analytical approaches and tools applicable across sectors.[12] A previous study into cyber reliance within key critical infrastructure (CI) sectors confirmed the importance of energy and utilities intra and interdependencies:

- Energy is a large consumer of data from other CI sectors and has the highest overall inbound dependency. Energy's *inbound/upstream*

• Energy Inbound Dependencies	Energy Outbound Dependencies

[12] Bell Canada. Cyber Dependencies within Canada's Key Infrastructure Sectors, Final Report Part 1, July 2007-availble upon request





- **Figure 16** requirements are heightened relative to other sectors by the high delivery-assurance standards mandated by clients and government.
- Energy is the largest consumer of its own information and data as a result of the tight supply chain linkages between different business entities involved in production and distribution.[13]

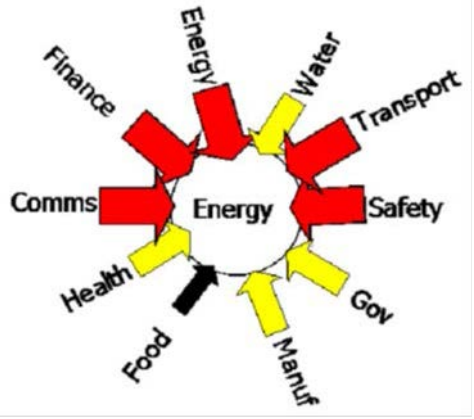
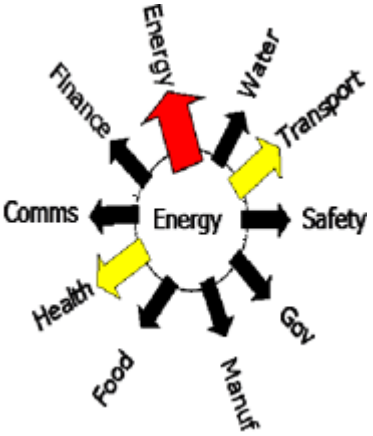
Energy Inbound Dependencies	Energy Outbound Dependencies
	

Figure 15: *Energy inbound and outbound dependencies.*

The report also noted that Communications and IT is "most dependent" on information flowing within the sector because this data exchange is essential to coordinating the delivery of services to clients.[14] Similarly data exchange is "core" to Finance sector.[15] In the case of the Finance sector, both inbound and *outbound/downstream*

Energy Inbound Dependencies	Energy Outbound Dependencies

[13] Ibid, pg. 33
[14] Ibid. pg. 34
[15] Ibid, pg. 33

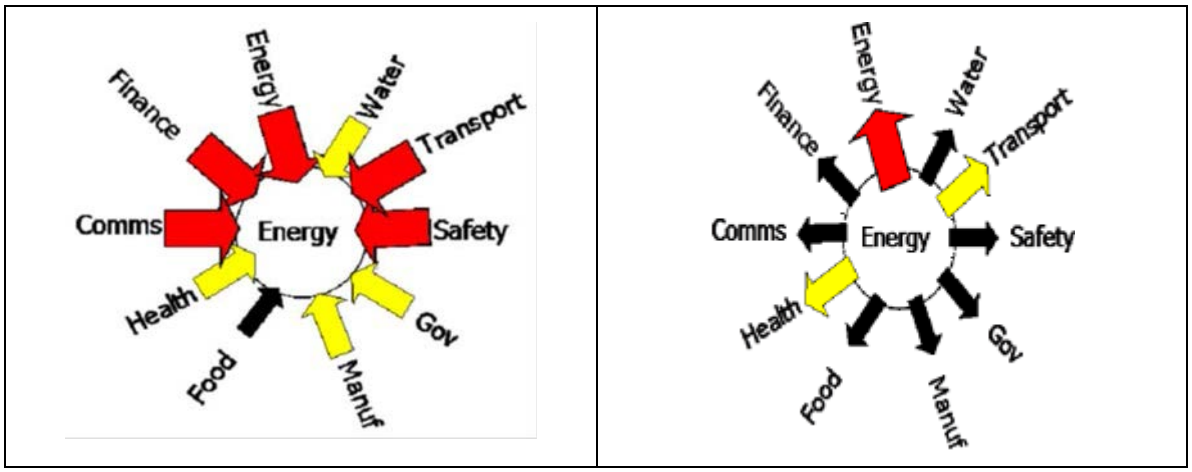


Figure 16 dependencies are critical:

- All sectors rely heavily upon data flows from Finance – either for conducting day-to-day business or for protecting sensitive competitive or personal information.[16]
- Finance has the highest *Outbound Contagion* of all sectors, indicating that an impact on the assurance of data and from the Finance sector would have the gravest impact to the Canadian economy as a whole.[17]

These three sectors provided obvious priority investment areas. All three rely heavily on cyber in large part because they provide services as opposed to goods which can be stockpiled or substituted.

A breakdown of portfolio investment by sectors is shown below.

[16] Ibid, pg. 33
[17] Ibid. pg. 43. The report introduced the concept of contagion – the potential for a physical or logic degradation or disruption to have a cascading impact on other sectors.

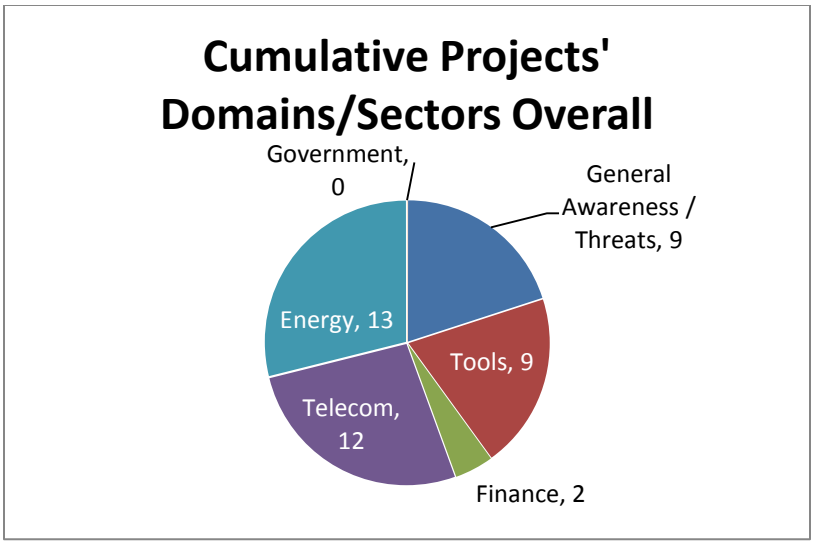


Figure 16: *eSecurity portfolio- investment by sector.*

Investment has been somewhat uneven which is not surprising given that it is driven in large part by demand and opportunity. Finance has invested heavily in in-sector data assurance and business continuity and is understandably risk averse. Hence it has taken more time and effort for CSS to establish credibility and a foothold. Familiarization with the CSSP promotes further interaction. The breakdown may be useful in determining if there is a requirement to target outreach programs.

4 Evaluation frameworks

4.1 Value framework

Assessing value is a challenging but critical undertaking. It links proposals, projects, outputs, and outcomes. CSS serves as both facilitator and enabler. Value in terms of public safety and security is achieved when project outputs are exploited, transitioned, institutionalized, and sustained i.e., when outputs inform and impact client, stakeholder or partner behaviour and/or programs.

CSS has developed a framework to describe and assess value.[18] It distinguishes between *potential* (available but not exploited and sustained) and *realized* value, and it offers an ontology for characterizing value into one of five types:

- **Knowledge/advice.** The aim is to advance understanding and to inform and improve operational policy, doctrine and procedures. Typically the output is a report;
- **Building the related community of practice.** In this case the aim is to promote information sharing, an exchange of best practices and increased collaboration. Workshops are a common means;
- **Maturing innovative concepts/technology.** Activities of this type support evolving and evaluating/testing and proving concepts and/or developing a prototype or raising its Technology Readiness Level (TRL);
- **Transitioning/exploiting innovative concepts/technology**. The aim is to support operationalization, commercialization and/or acceptance into service of concepts or technologies; and
- **Support to special operations or a major events.** In this case the aim is direct support to the planning for and conducting of a specific, upcoming operation or event.

In addition to *types of value*, the framework identifies 5 perspectives (criteria) which can be used to assess value and a scale (Good"; "Improve"; "Not so Good") for assessing impact. The criterion set titled measures of value includes:

- **Impact on operational capability or capacity.** The outputs would inform changes in doctrine or operational, plans and expand capability or increase capacity;
- **Stakeholder, operator or end user support**. Participation and acceptance of the approach and results e.g., recommendations and/or products;
- **Exploitation plan.** Evidence of a realistic blueprint for applying the knowledge gained. This might include identification of customers and/or plans for further development/maturation or commercialization;
- **Reporting and communication**. The significance of the activities and results have been reported and communicated effectively to the right stakeholders; and

[18] CSS TM 2013-013, September 2013 more complete description of the framework and case study is available. Greg Luoma and Andrew Vallerand. A Value Framework for Science and Technology Projects: A Case Study, DRDC http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p537917_A1b.pdf

- **Impact relative to investment**. His criterion relates Measure #1 to the level of effort to determine efficiency in turns of impact versus costs.

Each is described in more detail in the DRDC Technical Memorandum. While these measures are subjective, situational and time dependent, they provide a practical framework for evaluating projects.

The framework was applied to almost 100 CRTI projects to confirm its utility and benefits. An example is provided below:

Project #	Types of Value Created: 1) Advice, 2) Build CoP, 3) Mature Tech, 4) Transition, 5) Support to Ops	Value Assessment through some Measures of Impact (Good=Green, Improve=Yellow, Not so Good=Red)					Degree of Value: Realized (Green), Potential (Yellow), Lost (Red)	Notes: Summary of key Statement Actions/Activities to Increase Realized Value
		Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment		
CRTI 05-0092TA	3) Maturing technology	GOOD	GOOD	NEED TO IMPROVE	NOT SO GOOD	NEED TO IMPROVE	POTENTIAL	Need better communications of Value of results to potential users. Need commercialization plan/partner to realize full value

Figure 17: *Example of applying the value framework.*

4.2 Horizontal Performance Management Strategy (HPMS)

The HPMS distinguished specific indicators (see Table 2) and targets. An initial "report card" was prepared in winter, 2014, and another is due in the fall. As CSS' mandate and the eSecurity component goes beyond CCSS implementation responsibilities, and the funding received under CCSS auspices is being used to supplement the overall investment in the eSecurity program. The HPMS perspective may be narrow but nonetheless it provides an alternate evaluation framework and insight into CSS' contribution to CCSS realization.

Table 2: *Indicators for HPMS.*

Indicator	Baseline	Target
Growth – number of conferences and attendance, R&D seminars/ workshops hosted and participation levels.		
Coordination & Collaboration - number of project partners (government, national & international), personnel deployments/exchanges		
Sponsorship & Co-investment – number of project proposals and amount of matching funds	10% matching funds	(By FY 14/15) 33% matching funds
Exploitation - Percentage of partners who report that DRDC's R&D outputs (products) helped advance their cyber security innovation/problem-solving, percentage of collaborators who respond positively on the value of DRDC contributions, extent that Canadian papers on cyber security are cited by other researchers, successful cyber security Intellectual Property (IP) developed and transferred to partners (e.g., industry, OGDs, other orders of government		

5 Evaluation analyses

5.1 Applying the value framework

An effort was made to apply the ontology outlined to characterize the type of value eSecurity projects addressed. Project characterization can be found at Annex B – Value Added Framework Evaluation and Analysis and a portfolio perspective below (Figure 19 and Figure 20).

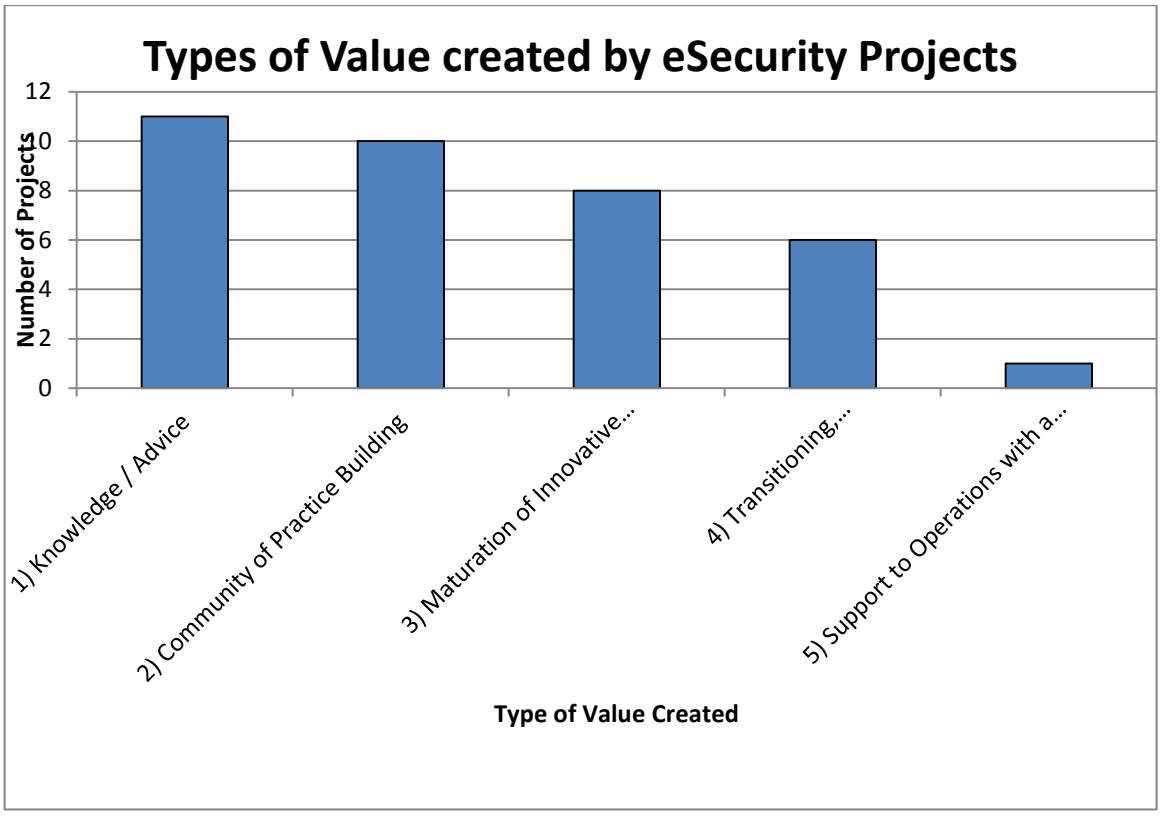


Figure 18: *eSecurity portfolio – types of value.*

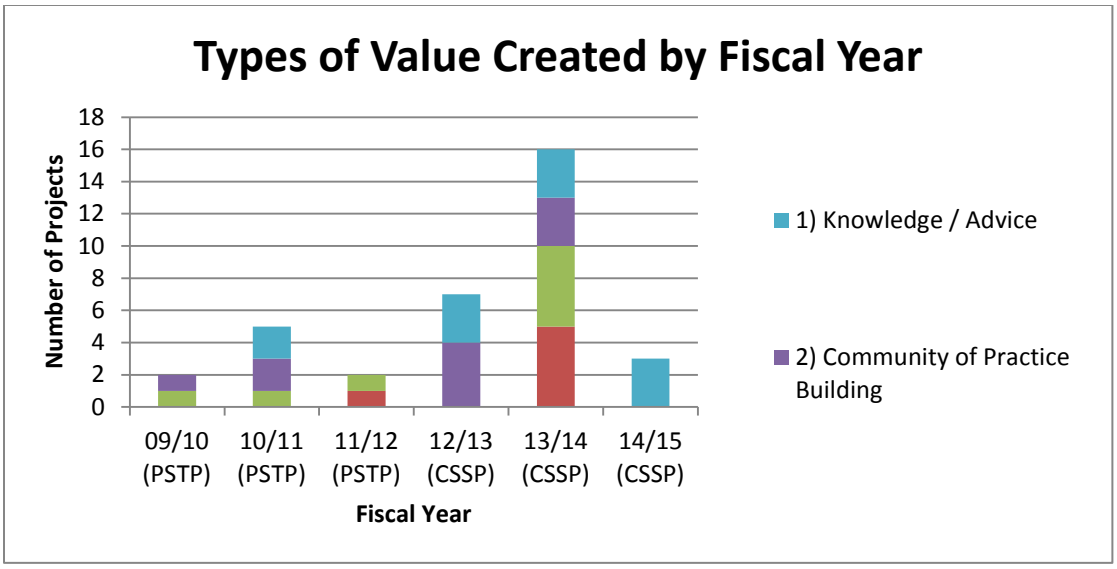


Figure 19: *eSecurity portfolio – types of value by fiscal year.*

As shown, although a majority of projects have focused on awareness (knowledge and advice). A reasonable balance has been achieved. Category 5, Support to Special Operations or Major Events, is by definition narrow and only one ESecurity project fell into this class. It is expected that the eSecurity mimics other CSS portfolios i.e., only a few projects are commissioned to support specific operations or events directly.

The aim of most of the eSecurity projects, particularly PSTP projects in the first few years, was to establish a knowledge baseline and define a community of practice. Later projects have involved maturation and exploitation of concepts and technologies. The charts do not illustrate horizontal linkages and developmental cycles. Type 1 knowledge capture and advice projects were used successfully in some instances to inform subsequent maturation and exploitation projects. For example, a survey of threats to SCADA systems led to follow-on projects culminating in the establishment and outfitting of a National Energy Infrastructure Test Centre (NEITC) and the conduct and operationalization of ICS Incident Response training.

Next measures of value criteria were applied and eSecurity projects evaluated. Again the evaluation of individual projects can be found at Annex B. Of the 45 evaluated 74% were considered to be good and a further 15% partially successful or needing improvement. 11% were judged to be not so good. These portfolio results are shown below in Figure 21.

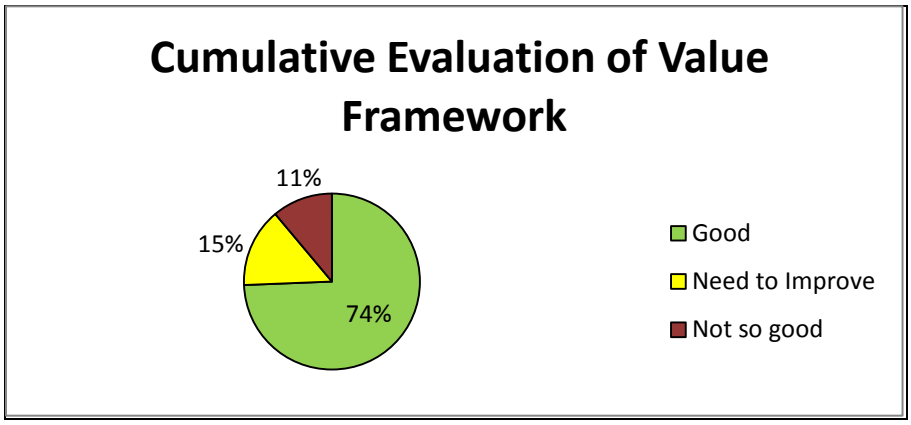


Figure 20: *Security portfolio – measures of value.*

The breakdown of evaluation by criteria (Figure 22) indicates that the most serious challenges to project success and value realization relate to exploitation and communication. This affirms intuition and aligns with the findings of the original study evaluating CRTI projects.[19] It should be noted in fairness that later projects have required brief descriptions of exploitation and communication plans as part of the bid and, once approved, are included in the project charter. Nonetheless determining how the knowledge gained will be employed to operational advantage, identifying and developing plans for employment, possible commercialization, and sustainment and follow on activity is and will remain difficult and demanding. Documenting and disseminating, reporting and communicating, the conclusions and recommendations reached following project completion is almost as important. In judging the results it should also be borne in mind that CSSP is seeking innovative solutions – often innovative solutions to "wicked problems" and some allowance must be made for "not so good" explorations.

[19] Luoma and Vallerand op cit. pp. 16-17.

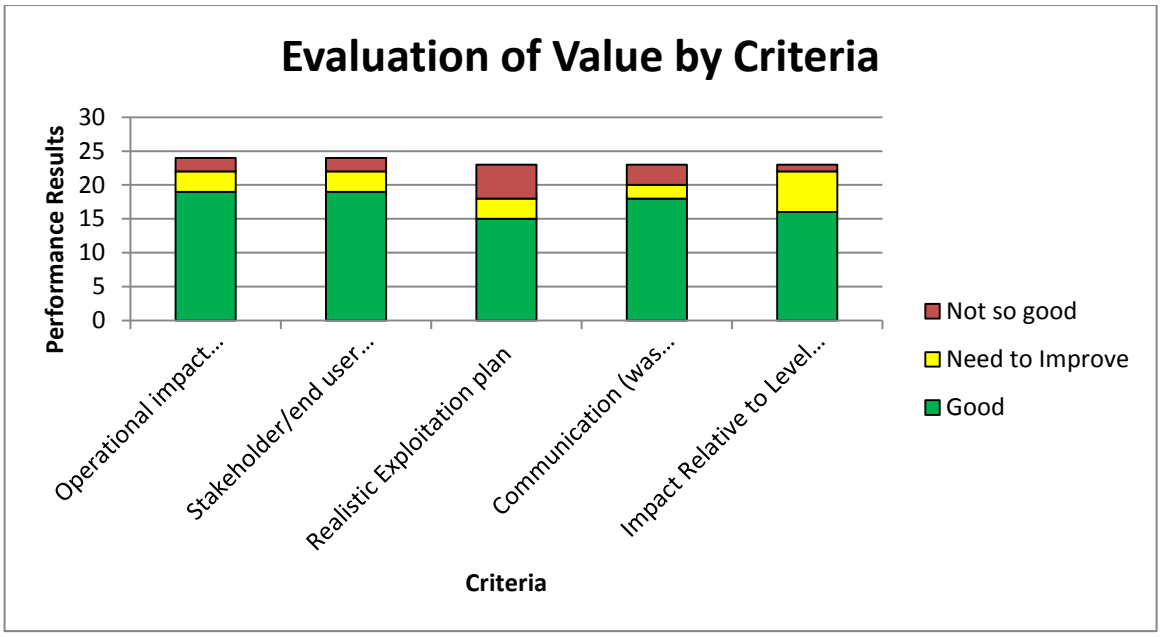


Figure 21: eSecurity measures of value by criteria.

Figure 23 portrays the overall project evaluation by fiscal year. Given the small set, caution must be exercised in extrapolating trends and/or drawing conclusions. Nonetheless it is noteworthy that in 3 of the 5 years there has been several "needs improvement" and "not so good" projects. Challenges relating to value realization are constant. FY 13/14 projects were assessed "good" but judgement may be a little premature. Arguably the economic climate should also be factored in in interpreting the results i.e., does government and/or industrial entrenchment constrain entrepreneurship and exploitation.

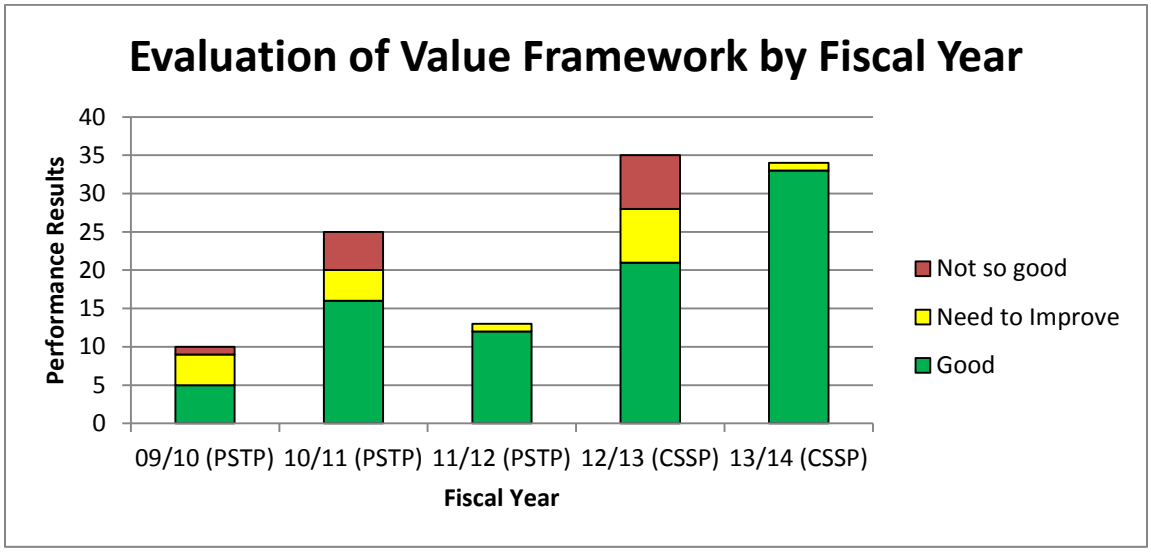


Figure 22: *eSecurity measures of value by fiscal year.*

5.2 Applying the Horizontal Performance Measurement Strategy (HPMS)

As noted previously, a HPMS was developed in 2013 which included an initial set of metrics to enable evaluation and support measurement and management of CCSS funded activities. CSS was commissioned to exploit CCSS funds to develop a focused S&T program. The initially proposed indicators related to this charge included growth, coordination and collaboration, sponsorship and co-investment, and exploitation. CCSS eSecurity funds have not been tagged; in practice, it is impractical if not impossible to distinguish between and to disaggregate CCSS and CSSP sponsored activities. As acknowledged in the initial performance report prepared investment, particularly S&T investment rarely produces immediate rewards and it is premature to judge results after a very limited period.

These HPMS indicators differ somewhat from the value framework and provide a complementary perspective. The first of these attempts to measure program growth in part through the number of conferences sponsored and attended and numbers of participations. While it may be useful to track the number of and attendees at conferences/workshops that are eSecurity portfolio-sponsored, it proved onerous and less meaningful to track participation by CSS staff at cyber security related events. In the latter case year-to-year variance is as likely to reflect changes in travel budgets and approval processes as interest and/or value. The second set of indicators, partnerships and co-investment, are more useful and valid measures of success, and are being monitored as are the third set which focus on programatics (number of projects) and inputs (CSSP investment and co-investment by partners). It is always challenging to measure outputs. The value framework provides a start. Most eSecurity projects have produced reports documenting the research and results and disseminating knowledge gains. A comprehensive list of these has been collated and is attached at Annex C – eSecurity Reports and Publications. A community survey appears to be the best way to assess exploitation and value. A questionnaire is being prepared and will be distributed to all partners this fall with a view to inclusion in the next/second report card. The number of citations serves as a useful proxy for judging acceptance and exploitation but has proved impossible to apply in practice not least because DRDC lacks the perquisite access and software to collect the data automatically.

6 Conclusions

6.1 Summary

In 2010 CSS formally added cyber security to its existing domains i.e., it has been 5 (going on 6 years) since the eSecurity portfolio was created. Hence it seemed an appropriate time to stand back and take stock. A concerted effort was made to collate and analyse project data. It confirms that the portfolio (CSSP investment and co-investment by partners) has grown, full advantage has been taken of investment options and a balance between government, industry and academic partners has been achieved. This investment has been distributed between promoting awareness, creating tools and supporting those sectors which depend heavily on cyber security e.g., Energy, Telecommunications and Finance. The framework developed by Luoma & Vallerand was then employed to assess the impact and value of the eSecurity portfolio. Analysis indicates that the focus has been largely exploratory with the aim of majority of projects knowledge generation and offering advice. Additionally reports have been inventoried and an assessment of projects conducted. While 74% the projects were considered "good", this review has confirmed the criticality of exploitation and communication planning.

6.2 Way head

6.2.1 CSP

A review of the selection process was conducted following last year's Call for Proposal and a number of changes have been instituted. These are described in detail the FY 15/16 guide.[20] Most e.g., tighter alignment with CSSP priorities, hosting a bidder's conference in conjunction with PWGSC, relaxation of the requirement to have partnerships agreed in time for synopsis submission, and restricting external reviewers to review of full proposals will be largely indiscernible to CSS partners. Major changes are planned to the CD investment option. Portfolio Managers have been mandated to conduct two workshops a year, one in the September/October timeframe and one in the February/March timeframe. Workshop objectives are to promote collaboration and contribute to defining CSSP priorities. They will provide an opportunity to engage communities of practice. A recent Conference Board of Canada observed that market orientation is important and "customer feedback is an important source of innovative ideas"[21].

6.2.2 Cyber technology landscape

Reliance on computers and connectivity continues to grow attracting threat actors. Cyber security will continue to draw attention and demand investment. CSS has a mandate to support public safety and security and a specific (CCSS) charge to develop a focused S&T program. A recent,

[20] Centre for Security Science, Call for Proposal (CFP): Bidder Guidebook – Call 003 2014/2015 https://buyandsell.gc.ca/cds/public/2014/08/11/3f4436c4100181f1c2fccf4aa9a0a03d/ABES.PROD.PW__SV.B059.E27860.ATTA001.PDF accessed 14 August 2014

[21] Amy Lui Abel, Sabra Brock and Amanda Popiela. Conference Board of Canada, Building the Foundation of an Innovative Culture, May 2014

internal and informal, review of the technology landscape was conducted to inform the FY 15/16 Call for Proposals. It identified a number of topical issues which pose specific S&T challenges:

- **Signature management and signature quality.** A signature is a distillation (usually a hash encoding) of a malicious pattern. Signatures are widely used, for example, to tersely identify cyber threats and, most widely, for the identification of viruses. The challenges identified aim to improve the quality, effectiveness and timeliness of signature-based techniques.
- **Anomaly detection and support discovery.** Anomaly detection refers to behaviour that does not conform to expected behaviour or usage patterns. From a cyber-security perspective, for example, anomalous traffic patterns in a network could suggest that a system has been penetrated and sensitive data is being infiltrated. The challenges identified target areas where anomaly detection and discovery could be materially improved.
- **Streaming and event driven analytics.** Streaming analytics refers to the inline analysis of data (e.g., I.P. packets, stock trades, currency trading, health monitoring) so as to rapidly and intelligently respond to evolving situations, potentially in near real time. There is a spectrum of algorithms, ranging from near real-time algorithms supporting almost instant response to adversarial situations; through to algorithms that take a longer-term, almost forensics-like, perspective. Identifying this algorithmic taxonomy is a research challenge in its own right.
- **Dynamic defence at the network edge and beyond.** A network edge is the location where the processing and enforcement of organizational policies commences. This hard problem focuses on developing dynamic defence techniques that can rapidly interdict network attacks, using both network and host-based capabilities.
- **Cloud (virtualization).** Cloud computing is the delivery of computing resources over a network. Cloud computing brings challenges pertaining to scale, security and privacy. Challenges arise from the evaluation, architecture and design of such systems. Furthermore, there are specific concerns about contagion of malware infections across virtual instances and into the underlying base image. Virtualization is a key technology underpinning Cloud computing.
- **Commercial Off- The Shelf (COTS) systems**. COTS products are those products that are commercially available, leased, licensed or sold and do not require specific maintenance/modification. COTS products tend to vary in quality, yet also evolve quicker and more usefully in response to broader market forces. The challenges once again pertain to evaluation, architecture and design of such systems as there is a need to scale evaluation capability and the potential to architect systems to mitigate threats arising from specific products. The supply chain is of particular concern with COTS products.
- **Enterprise-level metrics.** Such metrics allow questions that are fundamental to investment and deployment decisions to be answered e.g., “how secure is my organization?” and “how has my security posture improved through the last set of updates?” To properly manage systems, scientifically-based metrics and measures are required. Any underpinning “science of cyber security” will require a family of justified measures and metrics. Currently, there are no universally agreed upon methodologies to address the fundamental questions of how to quantify system security.
- **Mobility (including wireless).** Mobile devices are tending toward ubiquity and there is a strong desire to use capabilities available at home within the work place. Mobility raises

unique questions from a threat risk assessment (TRA) perspective and adds potential attack vectors due to the use of wireless and other over-the-air communication mechanisms. Challenges pertaining to evaluation, architecture and design once again arise though within a different context.

In addition to these specific topics, the review of the technology landscape identified several more generic, broader areas of interest. These included:

- **Science of cyber security.** Science is viewed as knowledge that results in accurate predictions or reliable outcomes. Successful progress on this capability gap will provide significant science-based foundations for developing cyber security techniques;
- **The internet of things.** The safety and security implications for resiliency of increasing pervasive connectivity have not been fully investigated and are not well understood;
- **Assessment and measurement (including visualization) techniques**. This reflects a broader interpretation of metrics and would extend S&T into presentational practices; and
- **"Big data".** There are a number of dimensions to explore relating to fusion and analysis of the massive amounts of available – structured and unstructured information. It is hypothesized that "big data" will enable the uncovering of previously unrecognized patterns and offer new insights into operating (security) environment.

In addition, interest has been expressed in international collaboration and a project focused on eCommerce and conduct of risk assessment of cyber-related vulnerabilities relating to cross-border supply chains. Less well defined at this point, although shared interest has been established, are potential studies into cyber security related training requirements and issues and into options and analysis of law enforcement cyber security forensics capability organizational models.

6.2.3 FY 14/15 CFP priorities

The immediate priorities, represented in the current Call for Proposals, reflect the technology landscape and are intended to build on the outcomes of past projects and extend the eSecurity portfolio. Two ongoing projects are noteworthy as they inform FY 15/16 priorities. CSSP-2013-TI-1044 has supported establishment of a National Energy Infrastructure Test Centre, specifically development and delivery of introductory, intermediate and advanced hands-on cyber security training and vulnerability assessment in energy and utilities sector. CSSP-2013-TI-1045 has provided a vehicle for partnership with the US-based National Cyber Forensics Training Centre (NCFTA) which is been used to help identify and evaluate options for countering cyber-crime and enhancing Canada's national cyber forensics capability.

Near term/immediate cyber security related investment priorities as articulated in the CFP include:

- Assess vulnerabilities and propose safeguards to enhance the cyber security of cross-border supply chains, including securing the exchange of electronic data, protecting cargo management and industrial control systems within transportation infrastructure and securing networks of sensors and screeners.;

- Projects to counter vulnerabilities in ‘eCargo’ resilience being impacted by contraband, counterfeit, illicit payment, services, etc. within worldwide transportation/border corridors;
- Analysis of cyber and physical security standards within CI sectors and the identification of areas of compatibility, misalignment, gaps, etc. between them, and recommendations for improvement;
- Projects that integrate and exploit new capabilities in direct support operations to support industrial control systems (ICS)/supervisory control and data acquisition (SCADA) security technologies and transition them to key critical infrastructure (CI) sector; and
- Vulnerability assessments and mechanisms to engage stakeholders (Electricity representatives from Energy & Public Utilities Sector) and propose safeguards for cyber security to improve SMART GRID Security.

6.3 Recommendations

It is recommended that:

- The value framework continued to be employed and refined, with an intent in the future to expand and broaden set of evaluators e.g., invite external in addition to internal assessments;
- HPMS criteria be reviewed and refreshed to reflect indicators that can both expose implementation progress and challenges without imposing an undue data collection cost. It is noteworthy that CSSP intends to engage mid-term outreach and survey to key stakeholders to determine if program investment and outputs have proven exploitable and how they have been contributed to positive outcomes and closing public safety and security capability gaps; and
- CSS continue to strengthen of the eSecurity Community of Practice. eSecurity poses unique challenges. Reliance on digital infrastructure has become pervasive and cyber security is a shared responsibility. The eSecurity CoP must keep up with rapidly changing technologies across a broad front and maintain close ties with other communities. There consideration should be given to forming sub-groups to focus on particular sector functions such as finance and banking or energy or emerging issues, such as social media and big data/predictive analytics.

This page intentionally left blank.

Annex A eSecurity investments by fiscal year

Number of CSSP Projects				
	Community Developments	Targeted Investments	Call for Proposals	Technology Acquisitions
09/10 (PSTP)			3	
10/11 (PSTP)			5	
11/12 (PSTP)			3	
12/13 (CSSP)	6	1		
13/14 (CSSP)	11	3	4	3
14/15 (CSSP)			3	2

CSSP eSecurity Investment Commitments				
	Community Developments	Targeted Investments	Call for Proposals	Technology Acquisitions
09/10 (PSTP)			$ 377,836	
10/11 (PSTP)			$ 1,123,500	
11/12 (PSTP)			$ 450,000	
12/13 (CSSP)	$ 231,000	$ 100,000		
13/14 (CSSP)	$ 520,000	$ 1,475,000	$ 1,988,700	$ 995,000
14/15 (CSSP)			$ 1,950,000	$ 400,000

Total eSecurity Project Value (including CSSP and in-kind)				
	Community Developments	Targeted Investments	Call for Proposals	Technology Acquisitions
09/10 (PSTP)			$ 701,461	
10/11 (PSTP)			$ 2,396,167	
11/12 (PSTP)			$ 813,000	
12/13 (CSSP)	$ 346,000	$ 125,000		
13/14 (CSSP)	$ 1,071,500	$ 2,068,000	$ 4,382,915	$ 1,120,000
14/15 (CSSP)			$ 8,293,040	$ 400,000

Total eSecurity Project Co-Investment				
	Community Developments	Targeted Investments	Call for Proposals	Technology Acquisitions
09/10 (PSTP)			$ 323,625	
10/11 (PSTP)			$ 1,272,667	
11/12 (PSTP)			$ 363,000	
12/13 (CSSP)	$ 115,000	$ 25,000	$ -	
13/14 (CSSP)	$ 551,500	$ 593,000	$ 2,394,215	$ 125,000
14/15 (CSSP)	$ -	$ -	$ 6,343,040	$ -

Annex B Critical infrastructure sectors and partners

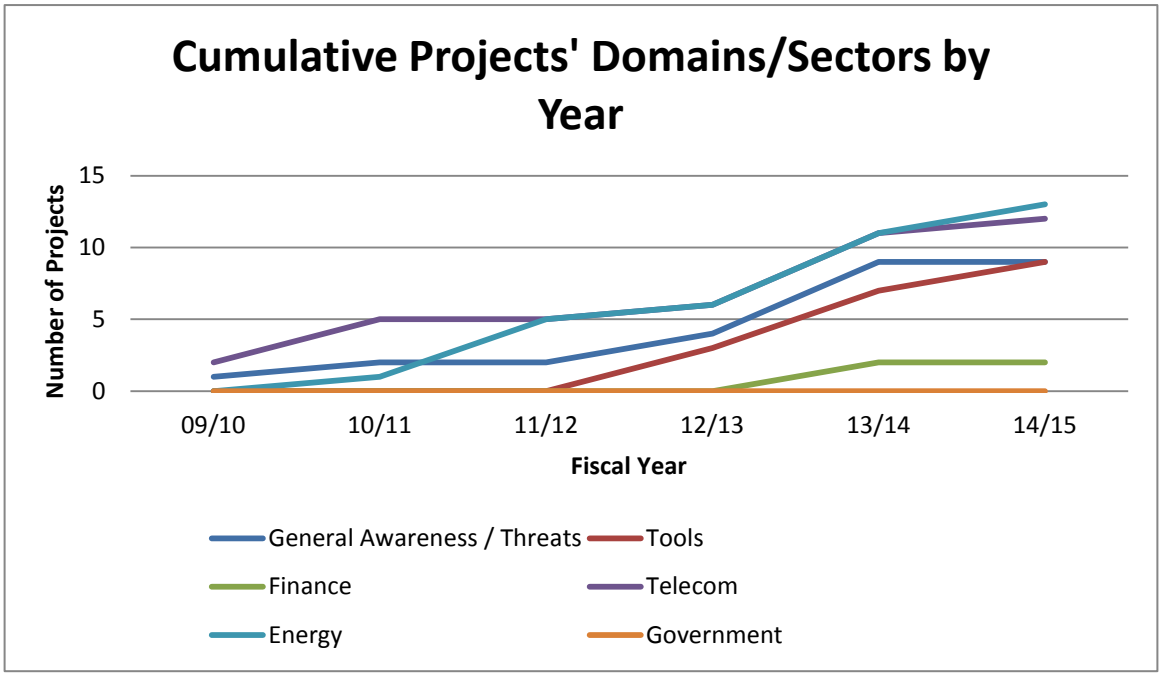
Fiscal Year	Long Title	Partner Organizations / User Community	Domain/Sector
09/10	Cyber Arms Study		General Awareness / Threats
09/10	Combating Robot Networks	RCMP, Bell Canada	Telecom
09/10	Automated Risk Assessment	DRDC, University of Ottawa, Bell Canada	Telecom
10/11	Study of Defined Radio for Spectrum Sensing in a Wireless Common Operating Picture	DND, CRC, ThinkRF	General Awareness / Threats
10/11	Watchdog Sensor Network with Multi-Stage RF Signal Identification and Cooperative Intrusion Detection	University of Western Ontario, Universite Laval	Telecom
10/11	Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity	Competition Bureau, NCFTA Canada	Telecom
10/11	Study in Cyber Security and Threat Evaluation in SCADA Systems	RCMP, Lofty Perch, Phirelight E-Business Solutions Inc, .Bruce Power, Liquid Max, Guidance Software, Tipping Point, Byrnes Security Siemens Canada, Telvent, Honeywell, Invensys Process System, Idaho National Laboratory, SRI International, Toronto Hydro, Abbotsford Water, Alliance Pipeline, Great Lakes St. Lawrence Seaway System, Pearson Airport, The Repository of Industrial Security Incidents. Industrial Defender, University of South Australia, Critical Intelligence Group, OSISoft, Cybernetic Corp.,Science Applications International Corp., Kenexis Corp., McAfee, Husky Energy. Sourcefire, Mu Security, The Logan Group, Digital Bond, Rockwell Automation, Elster Metering, Telus, Digital Stakeout	Energy
10/11	Ball Darknet Analysis (Network Traffic on Unallocated IP Space)	CSEC, Bell Canada	Telecom
11/12	SCADA Network Security in a Test Bed Environment/SCADA Testbed Data Analyzer	PS, Solana Networks	Energy

Fiscal Year	Long Title	Partner Organizations / User Community	Domain/Sector
11/12	Smart Grid Vulnerability Detection and Analysis		Energy
11/12	SCADA Testbed with Smart Grid	NRCan	Energy
11/12	SCADA Test Centre Control Room (Red & Blue Teams A/V Rooms)		Energy
12/13	Common CIP-Cyber Capability Gaps analysis/survey & Prioritization (Symposium)	CRTC	General Awareness / Threats
12/13	Cyber Architecture Analyses - Phase 1 Phase 2	NRCan	General Awareness / Threats
12/13	Cyber Situational Awareness Tools - Technology Survey	CSIS	Tools
12/13	2013 International Workshop on SCADA Industrial Energy and Utilities Control Systems Vulnerabilities and Solution	NRCan	Energy
12/13	Secure Communications for High Availability Environments	NRCan	Telecom
12/13	Tool Tech Operationalization - pre or post-Symposium	NRC	Tools
12/13	Cyber Intelligence Analysis Platform	RCMP, NRCan, École Polytechnique de Montréal	Tools
13/14	Data Centric Security Approaches for SCADA	Public Safety Canada	Energy
13/14	Privacy enhancing techniques for data exchange	TD Bank	Finance
13/14	Operationalize and deploy effective cyber investigation	Bell Canada- Corporate Security, PS Canada, RCMP	General Awareness / Threats

Fiscal Year	Long Title	Partner Organizations / User Community	Domain/Sector General Awareness / Threats
13/14	Canadian Cyber Information Exchange Initiative	NCFTA Canada, PS Canada, CRTC, RCMP, IC	
13/14	System Development of an Intelligent targeted search system	RCMP	Tools
13/14	Canadian Power Utility Network Security Smart Grid Workshop	BCIT	Energy
13/14	Upstream Cyber intelligence and analytics	PS Canada, Bell Canada – Corporate Security and Internet Protection Center (IPC), NRCan	Telecom
13/14	Internet intelligence aggregator and data mining for actionable intelligence products	CRTC	Tools
13/14	Traffic De-anonymizer	PSC, Dalhousie University	Tools
13/14	Fraud Information Sharing Analysis Capability Development	CSS	Finance
13/14	Canadian SCADA-Smart Grid Industry/Academia/Government Workshop	NrCan	Energy
13/14	Collaborative Identification and Localization of Wireless Security Threats and Intelligent Countermeasure Deployment	DRDC Ottawa, PS Canada, University of Western Ontario, University of Laval, Nutaq	Telecom
13/14	Cyber Defense Application: Automated Command and Control (C2) Signal Detection Using Machine Learning Techniques and Decoy Networks	Packet Forensics, CSIS	Telecom
13/14	Data Mining Algorithms for Advanced Persistent Cyber-Threat Detection	Manitoba Government, Department of Innovation, Energy and Mines (MERLIN), PWGSC, TRTech	Telecom

Fiscal Year	Long Title	Partner Organizations / User Community	Domain/Sector
13/14	Countering Security Threats using Natural Languages	NRC, MediaMiser, Thales, CSEC	General Awareness / Threats
13/14	Automating Technology Testing, Methodology Validation, Botnet-in-a-Box at the National Energy Infrastructure Test Centre (NEITC)	NRCan, RCMP, PS Canada, BCIT, Carleton University, École Polytechnique Montreal, Hydro Ottawa, Brookfield Renewables, Industrial Advisory Group	Energy
13/14	Canadian National Cyber Forensics Capability Pilot	CSIS, FINANCE Sector - Banks RCMP	General Awareness / Threats
13/14	CBSA Secure Data Exchange	CBSA, DRDC - Ottawa	Telecom
13/14	Emulation System in Process Control	NrCan	Energy
13/14	Threat Analysis and Monitoring System	CSIS	General Awareness / Threats
13/14	Automatic network intelligence search and detection system	RCMP	Tools
14/15	Behaviour Detection in Real time and Historical Data	PS Canada, Dalhousie University	Tools
14/15	Investigative Forensics Technologies for SCADA Networks	École Polytechnique de Montréal, PS Canada, Solana Networks, National Energy Infrastructure Test Center, Hydro-Quebec	Energy
14/15	SGCS-Can	BC Government Ministry of Energy, British Columbia Institute of Technology, Hydro-Québec's Research Institute (IREQ)	Energy
14/15	Network Traffic Conditioning Implementation	Public Safety Canada	Telecom
14/15	Perfect Jack – v2	RCMP – Federal Policing Operations - National security	Tools

	General Awareness / Threats	Tools	Finance	Telecom	Energy	Government
09/10	1	0	0	2	0	0
10/11	1	0	0	3	1	0
11/12	0	0	0	0	4	0
12/13	2	3	0	1	1	0
13/14	5	4	2	5	5	0
14/15	0	2	0	1	2	0
Total	**9**	**9**	**2**	**12**	**13**	**0**



Fiscal Year	Partner	Type
09/10	RCMP	Government
09/10	Bell Canada	Industry
09/10	DRDC	Government
09/10	University of Ottawa	Academia
10/11	DND	Government
10/11	CRC	Government
10/11	ThinkRF	Industry

Fiscal Year	Partner	Type
10/11	University of Western Ontario	Academia
10/11	Université Laval	Academia
10/11	Competition Bureau	Government
10/11	NCFTA Canada	Industry
10/11	Husky Energy	Industry
10/11	Elster Metering	Industry
10/11	Digital Stakeout	Industry
10/11	Telus	Industry
10/11	Sourcefire	Industry
10/11	Mu Security	Industry
10/11	The Logan Group	Industry
10/11	Digital Bond	Industry
10/11	Rockwell Automation	Industry
10/11	RCMP	Government
10/11	Alliance Pipeline	Industry
10/11	Great Lakes St Lawrence Seaway System	Government
10/11	Pearson Airport	Industry
10/11	The Repository of Industrial Security Incidents	Government
10/11	University of South Australia	Academia
10/11	Critical Infrastructure Group	Industry
10/11	OSISoft	Industry
10/11	Cybermetic Corp	Industry
10/11	Science Applications International Corp	Industry
10/11	Kenexis Corp	Industry
10/11	McAfee	Industry
10/11	Tipping Point	Industry
10/11	Bymes Security	Industry
10/11	Siemens Canada	Industry
10/11	Telvent	Industry
10/11	Honeywell	Industry
10/11	Invensys Process System	Industry

Fiscal Year	Partner	Type
10/11	Idaho National Laboratory	Industry
10/11	SRI International	Industry
10/11	Toronto Hydro	Government
10/11	Abbotsford Water	Government
10/11	Lofty Perch	Industry
10/11	Phirelight E-Business Solutions Inc.	Industry
10/11	Bruce Power	Industry
10/11	Liquid Max	Industry
10/11	Guidance Software	Industry
10/11	CSEC	Government
10/11	Bell Canada	Industry
11/12	Solana Networks	Industry
11/12	NRCan	Government
11/12	PS Canada	Government
12/13	École Polytechnique de Montréal	Academia
12/13	CRTC	Government
12/13	CSIS	Government
12/13	NRC	Government
12/13	NRCan	Government
12/13	RCMP	Government
13/14	BCIT	Academia
13/14	Carleton University	Academia
13/14	Dalhousie University	Academia
13/14	École Polytechnique de Montréal	Academia
13/14	University of Laval	Academia
13/14	University of Western Ontario	Academia
13/14	CBSA	Government
13/14	CRTC	Government
13/14	CSEC	Government
13/14	CSIS	Government
13/14	DRDC Ottawa	Government
13/14	IC	Government
13/14	Manitoba Government Department of Innovation, Energy and Mines (MERLIN)	Government
13/14	NCFTA Canada	Industry

Fiscal Year	Partner	Type
13/14	NRC	Government
13/14	NRCan	Government
13/14	PS Canada	Government
13/14	PWGSC	Government
13/14	RCMP	Government
13/14	Bell Canada- Corporate Security and Internet Protection Center	Industry
13/14	Brookfield Renewables	Industry
13/14	Hydro Ottawa	Industry
13/14	Industrial Advisory Group	Industry
13/14	MediaMiser	Industry
13/14	Nutaq	Industry
13/14	Packet Forensics	Industry
13/14	TD Bank	Industry
13/14	Thales Systems Canada	Industry
13/14	TRTech	Industry
14/15	BCIT	Academia
14/15	Dalhousie University	Academia
14/15	École Polytechnique de Montréal	Academia
14/15	BC Government Ministry of Energy	Government
14/15	National Energy Infrastructure Test Center	Government
14/15	PS Canada	Government
14/15	RCMP	Government
14/15	Hydro-Québec	Industry
14/15	Hydro-Québec's Research Institute (IREQ)	Industry
14/15	Solana Networks	Industry

CSSP Project Partners				
	Government	Industry	Academia	
09/10	2	1	1	4
10/11	9	33	3	45
11/12	2	1	0	3
12/13	5	0	1	6
13/14	12	11	6	29
14/15	4	3	3	10
	34	49	14	

Annex C Value added framework evaluation and analysis

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
PSTP 08-0107eSec	Combating Robot Networks	2) Community of Practice Building	Good	Good	Good	Good	Good	* report was widely distributed internally and externally (Bell) and results informed future investments, Elevated threat knowledge in whole CoP
PSTP-08-0115eSec	Automated Risk Assessment	3) Maturation of Innovative Concept/Technology	Need to Improve	Need to Improve	Not so good	Need to Improve	Need to Improve	* this was a spinoff of DND project, exploitation weakness may have been a result of plan or partners choice of partners critical for transition

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
PSTP 02-305eSec	Study of Defined Radio for Spectrum Sensing in a Wireless Common Operating Picture	1) Knowledge / Advice	Not so good	Not so good	Not so good	Not so good	Need to Improve	* distribution limited to government limited stakeholder participation hence limited take-up
PSTP 02-325eSec	Watchdog Sensor Network with Multi-Stage RF Signal Identification and Cooperative Intrusion Detection	3) Maturation of Innovative Concept/Technology	Good	Good	Good	Good	Good	* Prescient * good report and effectively distributed. * generated follow-on work on technology with client Pull to exploit it
PSTP 02-345eSec	Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity	2) Community of Practice Building	Good	Good	Good	Good	Good	Good stakeholder take-up informed NCFTA Canada program Well received by eSecurity CoP

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
PSTP 02-347eSec	Study in Cyber Security and Threat Evaluation in SCADA Systems	2) Community of Practice Building	Good	Good	Good	Good	Good	Well supported by community, project had over 30 stakeholders! Established that the industrial control sector was susceptible to cyber threats still being distributed good stakeholder take-up
PSTP-02-359eSec	Bell Canada Darknet Analysis (Network Traffic on Unallocated IP Space)	1) Knowledge / Advice	Need to Improve	Need to Improve	Not so good	Good	Need to Improve	* consolidated information but did not provide new insights did not generate new knowledge

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
PSTP 03-423eSec	SCADA Network Security in a Test Bed Environment/SCADA Testbed Data Analyzer	3) Maturation of Innovative Concept/Technology	Good	Good	Good	Good	Good	* laid the groundwork for PS and NRCan to work together within the new NEITC concept (National Energy Infrastructure Test Centre)
PSTP 03-0431	SCADA Testbed with Smart Grid Technologies	4) Transitioning, operationalizing, or commercializing	Good	Good	Good	Need to Improve	Good	* although the report needed additional work the project contributed to institutionalizing NEITC as an operational capability
CSSP-2013-TI-1151	SCADA Test Centre Control Room (Red & Blue Teams A/V Rooms)	5) Support to Operations with a CONOPS or Special Ops or Major Events with Concept/Technology	Good	Good	-	-	Good	* equipment purchase for outfitting NEITC lab this is being used to support incident response training impacting Ops in user

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
								organizations
CSSP-2012-CD-1027	Common CIP-Cyber Capability Gaps analysis/survey & Prioritization (Symposium)	2) Community of Practice Building	Good	Good	Good	Good	Good	*Good report produced, has value to stakeholders, being implemented by NCFTA Canada *Some sensitivity WRT distribution
CSSP-2012-CD-1028	Cyber Architecture Analyses - Phase 1 Phase 2	2) Community of Practice Building	Good	Good	Good	Good	Good	* Support to portfolio, conops impacted on FY 14/15 investment planning *PPTs contributed to stakeholder engagement

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2012-CD-1029	Cyber Situational Awareness Tools - Technology Survey	1) Knowledge / Advice	Good	Good	Good	Good	Good	* solid report, award winning paper *helped developed onward focus of this area
CSSP-2012-CD-1030	2013 International Workshop on SCADA Industrial Energy and Utilities Control Systems Vulnerabilities and Solution	2) Community of Practice Building	Good	Good	Need to Improve	Not so good	Need to Improve	*report outstanding * some confusion over workshop focus
CSSP-2012-CD-1031	Secure Communications for High Availability Environments	1) Knowledge / Advice	Not so good	Not so good	Not so good	Not so good	Not so good	* money sent, and no reports received * indication project was cancelled

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2012-CD-1032	Tool Tech Operationalization - pre or post-Symposium	2) Community of Practice Building	Need to Improve	Good	Not so good	Good	Need to Improve	* first attempt at showcasing ESEC technologies, low TRL and arguably too abstract limiting community uptake
CSSP-2012-TI-1033	Cyber Intelligence Analysis Platform	1) Knowledge / Advice	Good	Need to Improve	Need to Improve	Good	Need to Improve	* early charters did not require an exploitation plan *no uptake
CSSP-2013-CD-1077	Data Centric Security Approaches for SCADA	-	Good	Good	Need to Improve	Good	-	
CSSP-2013-CD-1078	Privacy enhancing techniques for data exchange	2) Community of Practice Building	-	-	-	-	-	Deferred (banking partner incurred delays in contracting process)

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2013-CD-1079	Operationalize and deploy effective cyber investigation	3) Maturation of Innovative Concept/Technology	-	-	-	-	-	* awaiting report from Lead Department
CSSP-2013-CD-1080	Canadian Cyber Information Exchange Initiative	4) Transitioning, operationalizing, or commercializing	Good	Good	Good	Good	Good	*sensitivity restricts open distribution of reports
CSSP-2013-CD-1081	System Development of an Intelligent targeted search system	4) Transitioning, operationalizing, or commercializing	Good	Good	Good	Good	Good	* awaiting final report from Lead Department

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2013-CD-1082	Canadian Power Utility Network Security Smart Grid Workshop	2) Community of Practice Building	Good	Good	Good	Good	Good	*Internal Report * F/P, US, academic and industry partners participated * outstanding & enlightening workshop that learned forward with S&T concepts
CSSP-2013-CD-1083	Upstream Cyber intelligence and analytics	1) Knowledge / Advice	Good	Good	Good	Good	Good	* awaiting report from Liem Nguyen
CSSP-2013-CD-1084	Internet intelligence aggregator and data mining for actionable intelligence products	4) Transitioning, operationalizing, or commercializing	-	-	-	-	-	* awaiting report from Lead Department

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2013-CD-1085	Traffic De-anonymizer	3) Maturation of Innovative Concept/Technology	Good	Good	Good	Good	Good	Publication Pending
CSSP-2013-CD-1086	Fraud Information Sharing Analysis Capability Development	2) Community of Practice Building	Good	Good	Good	Good	Good	laid the framework for 2013-TI-1045
CSSP-2013-CP-1002	Collaborative Identification and Localization of Wireless Security Threats and Intelligent Countermeasure Deployment	3) Maturation of Innovative Concept/Technology						

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2013-CP-1006	Cyber Defense Application: Automated Command and Control (C2) Signal Detection Using Machine Learning Techniques and Decoy Networks	4) Transitioning, operationalizing, or commercializing						
CSSP-2013-CP-1008	Data Mining Algorithms for Advanced Persistent Cyber-Threat Detection	1) Knowledge / Advice						
CSSP-2013-CP-1031	Countering Security Threats using Natural Languages	1) Knowledge / Advice						

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2013-TI-1044	Automating Technology Testing, Methodology Validation, Botnet-in-a-Box at the National Energy Infrastructure Test Centre (NEITC)	3) Maturation of Innovative Concept/Technology						
CSSP-2013-TI-1045	Canadian National Cyber Forensics Capability Pilot	3) Maturation of Innovative Concept/Technology						
CSSP-2013-TI-1046	CBSA Secure Data Exchange	4) Transitioning, operationalizing, or commercializing						
CSSP-2014-CP-2008	Behaviour Detection in Real time and Historical Data	1) Knowledge / Advice						

CSSP #	Long Title	Types of Value Created (1-5)	Operational impact (degree)	Stakeholder/end user support (degree)	Realistic Exploitation plan	Communication (was advice or tech formally given & communicated)	Impact Relative to Level of Investment	Comments
CSSP-2014-CP-2009	Investigative Forensics Technologies for SCADA Networks	1) Knowledge / Advice						
CSSP-2014-CP-2010	SGCS-Can	1) Knowledge / Advice						

-	09/10 (PSTP)	10/11 (PSTP)	11/12 (PSTP)	12/13 (CSSP)	13/14 (CSSP)	Total
Good	5	16	12	21	15	69
Need to Improve	4	4	1	7	0	16
Not so good	1	5	0	7	0	13

	09/10 (PSTP)	10/11 (PSTP)	11/12 (PSTP)	12/13 (CSSP)	13/14 (CSSP)	14/15 (CSSP)	Total
1) Knowledge / Advice	1	5	0	5	4	3	18
2) Community of Practice Building	0	0	0	2	2	0	4
3) Maturation of Innovative Concept/Technology	1	0	1	0	5	0	7
4) Transitioning, operationalizing, or commercializing	0	0	1	0	4	0	5
5) Support to Operations with a CONOPS or Special Ops or Major Events with Concept/Technology	0	0	0	0	0	0	0

Annex D eSecurity reports and publications

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Cyber CoP participation in NEITC	N/A	N/A	National Energy Infrastructure Test Centre (NEITC) Concept and Development of an Entity to Assist in Cyber Protection of Industrial Control Systems within the Energy and Utilities Sector in Canada	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc149/p539278_A1b.pdf	Awareness of the vulnerability of SCADA and ICS networks increased dramatically following exposure of the 2010 Stuxnet virus which targeted Iran's nuclear facilities. This was the first publicly known attack on a programmable logic controller and highlighted the need for better testing and monitoring capabilities and more effective collaboration and training. Risk precludes using "live" systems; hence, an independent, complementary capability was needed. A requirement to integrate digital and physical components of SCADA and ICS systems and an opportunity to exploit emulation and simulation were identified. The concept of a "sandbox" used by software programmers to run untested code or untrusted programs in isolation was adopted. Several Federal partners collaborated to create an ICS test and training centre. This report summarizes key elements of the concept and development of the nascent National Energy Infrastructure Test Center (NEITC).

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Cyber Arms Study	PSTP-08-0115eSec	Study	Automated Risk Management System (ARMS for Cyber)	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc119/p536721_A1b.pdf	It is recognized that national preparedness requires foresight of the system-wide cascading impacts of a security event and the effect on operations. Such cascading effects have the result of magnifying the impact of a single event either by broadening the impact of the originating event or potentially triggering new events involving other infrastructure services. The question is how to make informed decisions about risk mitigation in the context of dynamic and interconnected systems and infrastructure. This is a challenging problem for existing risk models and modeling techniques as interconnections and dependencies change over time, the nature of each interconnection can be complex and interconnections between systems may exist at many levels. What is needed is a semi-intelligent risk management system that can both discover system interdependencies in an automated way and understand their impact in a risk management context. The use of the term semi-intelligent in this project reflects the fact that certain elements of the risk management problem will benefit from the use of heuristics and machine learning to collect and analyze information. It is also recognized, however, that there will always be the need for the involvement of the risk analyst to draw upon domain knowledge and personal experience. This research initiative will investigate tools and technologies from the fields of artificial intelligence and risk analysis to model cascading risk impacts to information, networks, and systems, caused by security events. Furthermore, the technologies examined will be evaluated based on their ability to model cascading risk impacts to information, networks, systems, and operations caused by security event scenarios.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Combating Robot Networks	PSTP 08-0107eSec	Study	Combating Robot Networks and Their Controllers: A STUDY FOR THE PUBLIC SECURITY AND TECHNICAL PROGRAM (PSTP)	Protected Document- limited distribution	Relevancy This report is written as a comprehensive reference 'how to' Combat Robot Networks and Advanced Persistent Threats on a national scale. It should serve as an excellent reference to anyone involved in cyber security and high-tech crime. It is of particular relevancy for police, intelligence & threat analysts, security architects, and policy makers. The chapters guide the reader through a deep-dive study into: • advanced Botnet tradecraft and Advanced Persistent Threats (APT); • quantitative evidence of ongoing attacks, the threat agents and prevailing uses of Botnets to support criminal activity against Canadian interests; • a discussion of the legal and privacy concerns related to information collection on Botnet activity and the issues related to proactive defence measures against Botnets; • effective architectural solutions to mitigate the risks posed by Botnets; • strategic business transformation roadmap for police, intelligence, defence and public safety agencies; and • advanced tools and techniques that can be used by Law Enforcement Agencies (LEA) to monitor Botnet activity and to gather evidence and actively pursue criminal activity using Botnets. Cyber Crime is big business "Cyber crime is now the most significant challenge facing law enforcement organizations in Canada" were the headlines of a nationwide survey, commissioned by the Canadian Association of Police Boards (CAPB) in 2008. Today, the tool of choice for these criminals is the robot network or botnet where home and office computers are hijacked, often without the knowledge of their owners, and programmed to serve a botnet controller for illegal purposes such as: espionage, fraud, identity theft, bulk email or spam and distributed denial of service attacks.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Study of Defined Radio for Spectrum Sensing in a Wireless Common Operating Picture	PSTP 02-305eSec	Study	PSTP2 e-Security Community of Practice Study No. 3 Final Report	Protected Document- limited distribution	The primary and fundamental objective of this project has been to provide the basis for an effective solution to the Government's wireless security problems because no other effective solution currently exists. Towards solving the Government's wireless security problem, this study has developed and demonstrated the emergent research and technology to provide intrusion detection capabilities for wireless and other radio frequency (RF) devices. It has specifically developed an efficient general-purpose high-performance low-cost SDR-based sensor solution that will satisfy the following public, government and military wireless security applications: • no-wireless policy enforcement; • real-time wireless signal intrusion detection (WSID); • technical security counter measures (TSCM); • real-time detection of signal initiated radio-controlled improvised explosive devices (RC IED).

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Watchdog Sensor Network with Multi-Stage RF Signal Identification and Cooperative Intrusion Detection	PSTP 02-325eSec	Study	Watchdog Sensor Network with Multi-Stage RF Signal Identification and Cooperative Intrusion Detection	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc119/p536603_A1b.pdf	The study report begins with an overview of existing wireless standards and signal sensing/identification technologies in the first section. The time/frequency/protocol features of each standard wireless signal are summarized. Our intent is to discover all inherent signal features for the development of multistage RF signal sensing/identification and cooperative intrusion detection. In section 2, the proposed multi-stage signal existence detection and identification techniques for watchdog sensor network are investigated for standard compatible wireless signals. To extend the study to non-standard signals, section 3 investigates blind transmission parameter detection for arbitrary communication signals, which are commonly used in military applications. In the final section, intrusion detection and physical layer authentication in mobile Ad Hoc networks and wireless sensor networks (WSNs) have been investigated.
Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity	PSTP 02-345eSec	Study	The Dark Space Project Analysis of the Darknet Space for Predictive Indicators of Cyber Threat	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc125/p537638_A1b.pdf Limited Distribution	Cyberspace is best understood as a complex global ecosystem subject to technical and social drivers. The research carried out by this study suggests that current approaches to cyber security are ill-suited to detecting or anticipating threats, which increasingly rely on hybrid socio-technical vectors. Securing national cyberspace requires a paradigm shift toward a common operating picture of cyberspace. The project undertook research and experimental work along several axes critical to establishing a common operating picture of cyberspace. The principal outputs are grouped under the following three categories: i) research into the practical and ethical dimensions of a behaviour based model of detecting and anticipating cyber threats; ii) a reference architecture for implementing the objectives of the national cyber security strategy; and, iii) testing and validating methodological approaches to detecting advanced cyber threats on the basis of “live” data obtained from operational sources that had been stripped of PII.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Study in Cyber Security and Threat Evaluation in SCADA Systems	PSTP 02-347eSec	Study	Study on Cyber Security and Threat valuation in SCADA Systems	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc118/p536585_A1b.pd	This report summarizes the finding of study PSTP 02-0347eSec Study on cyber Security and Threat Evaluation in SCADA Systems. The primary objective of the study was to support the e-Security Community of Practice by leading a study to fill the knowledge gap concerning the current cyber-threat environment affecting SCADA systems. This work is intended to enhance the resilience of Canada's critical infrastructure by providing direction to research and development programs and recommending best security practices. This primary objective is supported by the following complementary objectives: 1. To establish trusted relationships with private sector critical infrastructure SCADA operators; 2. To enable the production of research reports on the current cyber-threat environment to SCADA systems; 3. To contribute to the development of a cyber-threat management system for continued situational awareness; and 4. To contribute to the development of best practices for the security of SCADA systems. The report is divided into five parts: 1. Task 1 Milestone “Assess State of the Art for SCADA Security” 2. Task 2 Milestone “Development of a Cyber Threat and Vulnerability Guideline” 3. Task 3 Milestone “Define the Scope and Capabilities of a Cyber-Threat and Vulnerability Management System” 4. Task 4 Milestone “Produce a Best Practices Security Manual or Guide” 5. Final conclusions, strategic advisory note, capabilities road map, study fact sheet, and quad chart
Ball Darknet Analysis (Network Traffic on Unallocated IP	PSTP-02-359eSec	Study	THE CANADIAN CYBER SECURITY SITUATION IN 2011 PSTP-02-359eSec-Z19	Available upon request	The recommended solution begins with upstream security services that ‘clean the pipe’ of toxic content at a safe distance; before reaching the enterprise network perimeter. Next-generation secure networks will be based upon the Reference Architecture17 and should include the deployment of multi-source collation, data Fusion and analysis capability using real-time global cyber threat intelligence.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Space)			The Dark Space Project	Publication Pending	
SCADA Network Security in a Test Bed Environment/SCADA Testbed Data Analyzer	PSTP 03-423eSec	Study	SCADA NETWORK SECURITY IN A TEST BED ENVIRONMENT Best Practices Guide: Securing WLAN and Cellular Infrastructure In Industrial Control Systems	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc122/p537220_A1b.pdf Posting Coming to Canadian Cyber Incident Response Centre (CCIRC) http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/index-eng.aspx?t=cbr-scrt	This project calls for the establishment of a SCADA network security test bed within the Public Safety Canada CCIRC (Canadian Cyber Incident Response Centre) secure lab facility. The test bed is to be used for assessment, testing and evaluation of SCADA network architectures, vulnerabilities, and defence mechanisms as well as development of best practices for securing such networks. A key project objective is to build greater capacity among Canadian government, industry and academia in the area of SCADA network security.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
SCADA Testbed with Smart Grid	PSTP 03-0431	Study	SCADA TEST-BED WITH SMART GRID TECHNOLOGIES	Available upon request	Many of Canada's Critical Infrastructure components, particularly in the energy sector, rely on Supervisory Control and Data Acquisition (SCADA) systems to monitor and control vital physical processes. As interdependencies between national critical infrastructure elements continue to expand, the connectivity among control systems also evolves. With the advent of the Internet, many SCADA systems have migrated to be web-accessible for reasons of ease of use and efficiency. Such accessibility, however, makes SCADA networks more vulnerable to sophisticated cyber attacks. With the emergence of new and more sophisticated cyber threats, some of which specifically target SCADA systems, there is a clear need to develop a test environment in which cyber threats can be simulated, weaknesses identified, and security best practices and strategies developed to address such threats. Such an environment would also permit control system operators to perform testing of critical equipment prior to deployment, thereby isolating critical SCADA systems vulnerabilities. The newly built SCADA Test-bed, developed in partnership with the Centre for Security Science (CSS), Natural Resources Canada (NRCan), and the Royal Canadian Mounted Police (RCMP), would simulate various architectures and technologies being used by Canadian Infrastructure owners/operators with the objective of addressing the growing cybersecurity threats. The Test-bed would also research and develop standardized security technology evaluations. Specifically, the project objectives are to: • Set up a control system environment that reproduces the key features and characteristics of real life SCADA networks deployed across the Electricity and Oil & Gas sectors; • Serve as a hands-on training and exercise laboratory, where front line operators and cyber security analysts can receive specialized training that will help to improve the security and resilience of their own SCADA networks; and • Serve as a security research facility focused on the development, testing and

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
					deployment of security technologies adapted to meet the stringent needs required by operational SCADA networks.
SCADA Test Centre Control Room (Red & Blue Teams A/V		Study			

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Rooms)					
Common CIP-Cyber Capability Gaps analysis/survey & Prioritization (Symposium)	CSSP-2012-CD-1027	Work-shop	A Software Framework for Spam Campaign Detection and Analysis	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc153/p539103_A1b.pdf	Every infrastructure is susceptible to abuse; email systems are not an exception. Spam, defined by Spamhaus [7] as “unsolicited bulk email” (UBE)[8], has become one of the biggest sources of email systems exploitation. Studies have shown that the number of spam emails is astonishing. For instance, according to Symantec Intelligence Report, the global ratio of spam in email traffic is 64.1% or 1 in 1.56 emails is spam [9]. Spam has affected almost all users around the world and wasted lots of storage space and network bandwidth. In addition, it has become a major tool for criminals to conduct illegal activities on the internet, such as stealing sensitive information, selling counterfeit goods, distributing malware and child pornography, etc.Despite the damages caused by spam, it is difficult for investigators and law enforcement agencies to track spammers and stop their malicious activities. This is mainly due to the astronomical amount of spam data, which makes its analysis by humans almost impossible. In addition, the strategies that are used by spammers to obfuscate the content of spam messages are various and in constant evolution, which make the investigation task even harder. Thus, it is absolutely necessary to perform an analysis of the information available on spam to determine its relative value for investigation. A vast range of studies have been conducted by security researchers on spam to mitigate its effect. However, it is still a cat-and-mouse game, where spammers continue to discover new techniques to evade anti-spam methods. Moreover, most existing work on spam has focused on detecting spam from large corpus email messages. Advanced forensic analysis of spam for the purpose of cyber crime investigation is still missing in the literature. In this report, we propose a new methodology and tool for forensic spam analysis that can be used by investigators to enforce Canada’s Anti-Spam Legislation[10].

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Cyber Architecture Analyses	CSSP-2012-CD-1028	Study	PERSPECTIVES ON CYBER SECURITY IN THE CANADIAN SAFETY AND SECURITY PROGRAM (CSSP)	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc152/p539279_A1b.pdf	Given the parallel program formulation activities for DRDC programs in direct support of the CAF/DND and those in support of the CSSP, while there may be opportunities to leverage investments in S&T to improve Cyber security across national defence and public safety, the CSS's primary focus, in accordance with the 2006 Memorandum of Understanding1 (MOU) establishing it, will be investments related to public safety and emergency preparedness. In addition, the CSS will avoid infringing on areas that have been assigned by law or Government direction to another department, board or agency of the Government of Canada but rather leverage their outputs to achieve Government desired outcomes. With this in mind it is recommended that, with respect to investment in Cyber security, the CSS should: 1. Avoid incremental investment in S&T programs that are already progressing and receive significant funding through other departments or agencies assigned adjacent cyber security mandates; 2. Leverage, to the maximum extent possible, the mature (high TRL) S&T outputs of other programs for Public Safety stakeholders; 3. Fund S&T projects in cross-cutting initiatives that enable government, industry and academia to work together to mature innovative concepts or technologies for rapid implementation; 4. Fund S&T projects that identify operational gaps and pilot programs that provide hard evidence/data to drive transition and operationalization. 5. Fund S&T projects that transition components of existing dual-purpose mature technology to the public safety domain;

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Cyber Situational Awareness Tools - Technology Survey	CSSP-2012-CD-1029	Workshop	Network Address Translation (NAT) Behaviour: Final report	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc151/p539336_A1b.pdf	Network Address Translation (NAT) is the mechanism, which is used to modify a packet's IP address information while it is in transit across a network routing device. Because NAT can hide a computer's or evens a network's IP address, identifying the presence of NAT in network traffic is an important task for network management and security. The aim of this work is to identify the presence of NAT in the network traffic by utilizing different approaches and evaluate the performance of these approaches under different network environments represented by the availability of different data fields. To this end, passive fingerprinting and data mining based approaches are used and evaluated under different test conditions. In these experiments, not only packet header and flow based features are employed without using source and destination IP addresses, source and destination port numbers and payload information, but also payload information is analyzed to understand how much performance gain is reached if it is available. Last but not least; experiments are also performed to identify NAT devices in encrypted as well as non-encrypted traffic.
Cyber Intelligence Analysis Platform	CSSP-2012-TI-1033	S&T Transition	Cyber Intelligence Analysis Platform Final Report	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc153/p800109_A1b.pdf	This is the final report for the research and development project between the Royal Canadian Mounted Police (RCMP) and l'École Polytechnique de Montréal. The principal objective for this project was to produce a "blue-print" for a Cyber Intelligence Analysis Platform (CIAP), which has advanced capabilities to study sophisticated cyber threats in a secure environment. In this report, a "how to guide" detailing all the key steps to build a CIAP that automates the execution and analysis of complex malware samples is presented. The CIAP follows the design implemented at l'École Polytechnique de Montréal's SecSI Cyber Security Laboratory, which has been used to emulate and study real world botnets at scale in an isolated environment. In particular, the SecSI's cluster has generated a 3000 node Waledac botnet, which enable researchers to understand its complex command and control infrastructure used operate it.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Tool Tech Operationalization - pre or post-Symposium	CSSP-2012-CD-1032	Study	Quantum random bit generation using energy fluctuations in stimulated Raman scattering	Available on request through PUBMED http://www.ncbi.nlm.nih.gov/pubmed/24514488 783 APPLIED RESEARCH\	Random binary keys (RBKs) are a critical resource in modern cyber security systems. They are used to convert plain text messages into secure ciphers for transmission over open channels. The rapid growth in the scale and speed of digital networks has resulted in an increased need for high quality RBKs in high volume to facilitate secure information transfer in applications where privacy is paramount. RBK generation methods based on classical processes or computer algorithms may be compromised if an adversary determines the algorithm used and then predicts the value of future keys. Quantum random bit generators (QRBGs) can create keys with guaranteed security because they use fundamentally random outcomes from measurements on suitable quantum systems. Here we summarize our QRBG research results; we measured pulse energy fluctuations in Stokes light from spontaneously initiated stimulated Raman scattering (SISRS) and converted the measurements to truly random, unbiased binary sequences. The principal results of our research are summarized as follows: 1. SISRS can be used to amplify broadband vacuum fluctuations of the electromagnetic field to levels which are easily measured using fast, inexpensive photodiodes. 2. Random fluctuations can be measured in the pulse energy of Stokes pulses generated using SISRS. 3. Measured Stokes pulse energies can be converted to high-quality RBKs which pass standard tests of randomness.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Canadian Cyber Information Exchange Initiative	CSSP-2013-CD-1080	Study	Deployment of the Canadian Cyber Information Exchange Platform	Publication pending / draft available on request	Nowadays, organizations are targeted with more sophisticated cyber attacks than ever before. Indeed, recent events demonstrated that individuals, corporations and governmental organizations could be subjected, at the speed of light and in full anonymity, to amplified, large-scale, debilitating, intimidating and disrupting attacks that might lead to severe privacy/security and economic consequences, and even to the endangerment and loss of human lives. These attacks might be carried out by a spectrum of individuals such as criminals, cyber-terrorists, terrorists and foreign government spies. Moreover, as the closest approximation of perfect anarchy, the Internet becomes an attractive tool to terrorists for spreading messages, recruiting supporters, planning and coordinating attacks. In this context, there is a desideratum for generating near-real-time cyber threat intelligence that can be used for the detection, analysis, mitigation, prevention and attribution of such cyber attacks. In addition, it is of paramount importance to share the generated cyber threat intelligence among security organizations, government agencies, Internet Service Providers (ISPs), law enforcement agencies, academia and research institutions in order to fight cyber attacks and develop essential counter-measures.
Canadian Power Utility Network Security Smart Grid Workshop	CSSP-2013-CD-1082	Study	Report on Smart Grid Security Workshop	Internal Report- available upon request	In this report, we discuss the Smart Grid Workshop, organized by BCIT, Group for Advanced Information Technology on January 21st, 2014. This event was made possible by funding from the Canadian Safety and Security Program (CSSP) which is led by Defense Research and Development Canada (DRDC). We summarize the talks presented in the morning, outcomes from the afternoon discussion panels and the results of the survey showing what the attendees identified as the priority areas that need to be further researched, addressed and implemented to ensure Critical Infrastructure Security in the Smart Grid sector.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Upstream Cyber Intelligence and Analytics	CSSP-2013-CD-1083		Cyber Threat Analysis Report	Limited Distribution	
Traffic De-anonymizer	CSSP-2013-CD-1085	Study	FINAL PROJECT REPORT: Traffic De-Anonymizer	Publication Pending	Proxies are used commonly on today's Internet. On one hand, end users can choose to use proxies for keeping their privacy and ubiquitous systems can use it for intercepting the traffic for purposes such as caching. On the other hand, attackers can use such technologies to anonymize their malicious behaviours. Thus, the prevalence of proxies and the different applications and users connected through a proxy has implications in terms of the different behaviours seen on the network. This is important for defense applications since it can facilitate the assessment of security threats. Thus, systems that can identify infected computers behind a proxy based on their behaviour represent a first step in taking the appropriate actions, for example, when a botnet client is identified. The objective of this research includes identifying proxies and the computers behind them based on their behavior from the traffic log files of a computer, which is on the network that is outside of the proxy. This is what we mean by traffic de-anonymizer. To achieve this: (i) we employ a mixture of log files to represent real-life proxy behavior, and (ii) we design and develop a data driven machine learning based approach to provide recommendations for the automatic identification of computers behind an anonymous proxy. Our results show that we are able to achieve our objectives with a promising performance even though the problem is very challenging.

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
Automatic Technology Testing, Methodology Validations, Botnet in a Box	CSSP_2013-TI-1044		National Energy Infrastructure Test Centre (NEITC) – ICS Incident Response Training Initial Observations on Building Resiliency	Publication Pending	
Canadian National Cyber Forensics Capability	CSSP-2013-TI-1045		Perspectives on Recent Efforts to battle Cyber Crime: - CSSP-2013-TI-1045-Z09 CSS/NCFTA Partnership – Concept of Operations CSSP-2013-1045-Z13 CSS-NCFTA Collaborative Partnership Progress Report#2014-1 CSSP-2014-TI-1045-Z17 Centre for Security Science	Available upon request	

Project Title	CSSP #	Project Type	Publication Title	Link to Publication	Abstract/Executive Summary/Introduction
			(CSS)/National Cyber Forensics Training Alliance (NCFTA) Collaborative Partnership Workshop – Stakeholder Expectations and Interests CSSP-2013-TI-1045-Z20		

Bibliography

Abel, Amy Lui, Sabra Brock and Amanda Popiela. Conference Board of Canada, Building the Foundation of an Innovative Culture: Human Capital's Role in Making it Happen, May 2014

Bell Canada. Cyber Dependencies within Canada's Key Infrastructure Sectors, Final Report Part 1, 6 July 2007

Centre for Security Science, From Concept to Capability:Collaborative Science and Technology for Public Safety and Security, 2011 http://publications.gc.ca/collections/collection_2012/dn-nd/D2-277-2011-eng.pdf accessed 18 August 2014

Centre for Security Science, CSSP Environmental Scan 2013, May 2014

Centre for Security Science, Call for Proposal (CFP): Bidder Guidebook – Call 003 2014/2015 https://buyandsell.gc.ca/cds/public/2014/08/11/3f4436c4100181f1c2fccf4aa9a0a03d/ABES.PROD.PW__SV.B059.E27860.ATTA001.PDF accessed 14 August 2014

Graham, J.D., R. Howes and A.L. Vallerand. Perspectives on Cyber Security in the Canadian Safety and Security Program, Centre for Security Science, DRDC CSS LR 2013-056, 2014

Luoma, Greg and Andrew Vallerand. A Value Framework for Science and Technology: a Case Study, DRDC TM 2013-013, September 2013, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p537917_A1b.pdf

NATO Joint Analysis and Lessons Learned Centre, A framework for the Strategic Planning and Evaluation of Public Diplomacy, 2013, http://www.jallc.nato.int/newsmedia/docs/A%20Framework%20for%20the%20Strategic%20Planning%20and%20Evolution%20of%20Public%20Diplomacy.pdf accessed 18 August 2013

Public Safety Canada, Action Plan for Critical Infrastructure, Government of Canada, 2009 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/index-eng.aspx

Public Safety Canada, Canada's Cyber Security Strategy, Government of Canada, 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Public Safety Canada, Measuring the Performance of Canada's Cyber Security Strategy, October 2012

Public Safety Canada, Federal Emergency Response Plan, January 2011, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf

http://publications.gc.ca/collections/collection_2012/dn-nd/D2-277-2011-eng.pdf

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

CBRN	Chemical, Biological, Radiological and Nuclear
CCSS	Canada's Cyber Security Strategy
CD	Community Development
CFP	Call for Proposal
CIP	Critical Infrastructure Protection
CoP	Community of Practice
COTS	Commercial Off The Shelf
CPRC	Canadian Police Research Centre
CRTI	CBRN Research and Technology Initiative
CCSS	Canada's Cyber Security Strategy
CSS	Centre for Security Science
CSSP	Canadian Safety and Security Program
DND	Department of National Defence
DRDC	Defence Research and Development Canada
DSTKIM	Director Science and Technology Knowledge and Information Management
EMSI	Emergency Management & Systems Interoperability
FERP	Federal Emergency Response Plan
HPMS	Horizontal Performance Measurement Strategy
NCFTA	National Cyber Forensic Training Alliance
NEITC	National Energy Infrastructure Test Centre
NRCan	Natural Resources Canada
NSCI	National Strategy for Critical Infrastructure
R&D	Research & Development
PSTP	Public Safety and Security S&T Program
PS	Public Safety Canada
PSAT	Public Security Anti-Terrorism
PWGSC	Public Works and Government Services Canada
RCMP	Royal Canada Mounted Police
SII	Surveillance, Intelligence & Interdiction

TA	Technology Acquisition
TI	Targeted Investment
TRA	Threat Risk Assessment
TRL	Technology Readiness Level

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean Street, 11th Floor
Ottawa, Ontario K1A 0K2
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2012

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

eSecurity portfolio : Overview, analysis of value added, and way ahead

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Hales D.; Howes R.; Cooper E.; Porter-Greene M.; Vallerand A.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
November 2014	92	0

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean Street, 11th Floor
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2014-R113	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

---

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Cyber Security; Programme Evaluation, eSecurity