DRDC CSS LR 2013-056

Scientific Letter

PERSPECTIVES ON CYBER SECURITY IN THE CANADIAN SAFETY AND SECURITY PROGRAM (CSSP)

Purpose

To inform and make recommendations to the Director General of the DRDC Centre for Security Science, the Director General Emergency Management and Public Safety at Public Safety Canada and other senior decision makers, regarding CSSP science and technology (S&T) investments in Cyber security to focus outputs, optimize uptake and maximize impact on public safety outcomes of the Government of Canada.

Executive Summary

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 Understanding[1] (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;

[1] Memorandum of Understanding between the Department of Public Safety and Emergency Preparedness and the Department of National Defence for Collaboration in Science and technology related to Public Safety and National Security (13 July 2006) DND Identification Number: 2006043302

Introduction

The Government of Canada has published several documents through Public Safety Canada including the National Strategy for Critical Infrastructure (2009), Canada's Cyber Security Strategy (2010) and Action Plan[2] (2013) that provide overarching policy guidance for the large number of federal departments and agencies involved in achieving the desired Government outcomes. The Cyber Security Action Plan clearly identifies three pillars of Canada's strategy: 1) securing Government systems; 2) partnering to secure vital cyber systems outside the federal government; and, 3) helping Canadians be secure online.

In accordance with the 2006 MOU establishing the CSS, programs run by or through the Centre such as the CSSP 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. With that in mind, the CSS has consciously and deliberately avoided directly supporting the Cyber Security Strategy's Pillar 1 – securing Government systems – as this falls clearly within the purview of the following departments and agencies according to their mandates: the Treasury Board Secretariat (TBS) to provide strategic direction and leadership for information management and technology across the Government of Canada; the Communications Security Establishment Canada (CSEC) to provide guidance and services to the Government of Canada for protecting electronic systems and information and provide technical and operational assistance to federal law enforcement and security agencies; and, National Defence (CAF/DND) to provide military forces the ability to operationally use cyber-space while potentially denying its use to an adversary.

In recent testimony to the Standing Senate Committee on National Security and Defence[3] (SCONSAD) by BGen Loos, DG Cyber within the Chief of Force Development at National Defence, he stated "the top priority of DND and the CF is to defend its own systems. Our needs are quite different from those of most other government departments, particularly in that commanders must remain accountable for command and control and sensor systems upon which our military operations entirely rely." As a result of this National Defence priority and recognition of their different needs, the DRDC programs in direct support of the CAF/DND have and continue to focus their Cyber security efforts in this specialized military "domain".

Programs under other Government departments and agencies focusing S&T investments in support of ***Pillar 1*** receive significant funding, far and above what the CSS could contribute through the CSSP. Therefore, with Pillar 1 already well supported, the CSS adopted the position to not incrementally invest in these efforts but rather to focus efforts and investments supporting ***Pillar 2*** – 'partnering to secure vital cyber systems outside the federal government' and ***Pillar 3*** – 'helping Canadians be secure online', both of which have been clearly identified as priorities to the Government within Canada's Cyber Security Strategy, but at the time, enjoyed much less federal involvement and support.

That is not to say that the outputs of CSSP S&T investments remain isolated and withheld from those focused on Pillar 1. It is hoped that the outputs from science and technology investments directly supporting any one pillar can be leveraged, to the maximum extent possible, across all 3 pillars. The CSS will therefore share all results within the broader federal community and

[2] Action Plan 2010-2015 for Canada's Cyber Security Strategy, (2013) ISBN: 978-1-100-21895-3
[3] Testimony provided to SCONSAD 5 November 2012.

attempt to leverage outputs from other federal partners and rapidly transition them to appropriate public safety stakeholders.

With the foregoing in mind, the CSSP outcomes related to Cyber security are ***Intermediate Outcome 3*** which states "rapid and effective technology transition to ensure that new or innovative uses of science and technology" can be quickly brought to bear and ideally outpace potential advances in threats and ***Intermediate Outcome 4*** which is "the complex web of Canada's critical physical and cyber infrastructure remains resilient to disruptions ensuring that essential services remain in operation throughout Canada to support critical functions related to national security and public safety."

Cyber Security Pillar 2 - partnering to secure vital cyber systems outside the federal government.

"Canada's security and economic prosperity depend on the smooth functioning of systems outside the Government. Canada's private sector operates many of the systems, and is the custodian of sensitive information and industrial control systems, on which Canada's national security and public safety depend."[4] This recognition of the importance of cyber systems outside the federal government to national security and public safety is the driver behind Pillar 2 and the focus of the efforts of the CSS. Through the CSS Communities of Practice (CoPs), the CSS has not only been able to engage the broader Private Sector owners / operators of the national digital infrastructure (Communications and Information Technology Critical Infrastructure Sector) but also other critical infrastructure sectors that rely on the national digital infrastructure for their effective operation such as Energy and Utilities, Finance and Transportation.

Specific examples of initiatives in support of Pillar 2 include:

1. The establishment of the National Energy Infrastructure Test Centre (NEITC)[5]

   A National Energy Infrastructure Test Centre (NEITC) was established in response to identified emergent threats to Canada's critical infrastructure (CI). Supervisory Control and Data Acquisition (SCADA) systems have a broad range of commercial uses and are used widely in the Energy and Utilities Sector. However, it had been illustrated how SCADA systems could be 'hacked' and physical equipment controlled remotely. The establishment of a test bed followed by addition of complementary simulation capabilities has permitted members of the Energy and Utilities Critical Infrastructure Sector together with numerous Federal Department partners to participate in advanced multi threat scenario training workshops inside NEITC. During the workshops they receive hands-on cyber security training, are permitted to exercise and test deployed cyber security technologies, are informed of related research and development initiatives and other activities that directly support enhanced cyber security and reducing threats to their critical infrastructure.

[4] Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2013 (ISBN: 978-1-100-21895-3)

[5] Letter Report: Analysis of the Operational Value of the National Energy Infrastructure Test Center (NEITC) 14 Dec 2013 3780-1 (DSTPS) DRDC CSS LR 2013-048

2. The access and enhancements to SmartGrid Security facilities,

The CSS is providing support and increased access to Canadian stakeholders to two SmartGrid test environments, one a Smart microGrid test bed at the British Columbia Institute of Technology (BCIT) and the other focusing on the development of SmartGrids as well as control systems and automated systems to improve grid behavior at Hydro Quebec's Institut de Recherche d'Hydro-Québec (IREQ). Increased access has facilitated engagement of Canadian stakeholders from government, industry and academia in identifying and combatting cyber threats associated with the emerging evolution of electrical grinds into a smart electrical grid. Utilities have realized that their newer grids are no longer isolated and protected from attackers. While the 'attack surface' of grids will continue to increase, neighbouring utilities are increasingly interconnected via IT technology and Smart Grid specific Communications Technologies. There are immense challenges in ensuring that successful attacks on utilities in one jurisdiction do not spread to utilities in other jurisdictions quickly cascading from a local event to a national outage, while taking into account the related challenges and opportunities in the USA. Increasing access to these integrated test centers has facilitated collaboration across government initiatives, national partners and the private sector for testing, analyzing and training stakeholders in relation to cyber threats caused by the convergence of the electrical SmartGrid operations, technologies and IT Technology, in a national SmartGrid Security facility.

Cyber Security Pillar 3 - helping Canadians be secure online.

"The third pillar of *Canada's Cyber Security Strategy* focuses on providing Canadians with information to protect themselves and their families online, and on strengthening the ability of law enforcement agencies to combat cyber-crime."[6] Public Safety Canada has taken the lead on providing Canadians with information to protect themselves through their "Get Cyber Safe" initiative[7] and so the CSS has focused on strengthening the ability of law enforcement agencies to combat cyber-crime. Working with a number of federal departments and agencies as well as industry and academia, to develop cyber forensics in order to detect, classify and identify the source of cyber threats to Canadian interests and aid in their neutralization and possible prosecution of the perpetrators.

A specific example of an initiative in support of Pillar 3 is:

Partnering with the National Cyber-Forensics & Training Alliance (NCFTA) in Pittsburgh,

The CSS has acquired a seat at the NCFTA in Pittsburgh, Pennsylvania to facilitate engagement of Canadian stakeholders from government, industry and academia in identifying and combatting global cyber threats. The NCFTA provides a neutral collaborative venue where international partners from industry, law enforcement and academia come together to leverage cross-sector resources to more effectively analyze critical, real-time intelligence against emerging cyber threats. The actionable intelligence developed is used not only to detect and identify cyber persistent threats, but also to

[6] Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2013 (ISBN: 978-1-100-21895-3)

[7] http://www.getcybersafe.gc.ca/index-eng.aspx Accessed 03 March 2014.

mitigate and ultimately neutralize persistent global cyber threats, in an effort to protect intellectual assets, countries and citizens.

Conclusion

In conclusion, 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 will be investments specifically related to public safety and emergency preparedness, as per the existing MOU. 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 such as those related to Pillar 1 - securing Government systems - but rather leverage their outputs to achieve Government desired outcomes related to Pillar 2 - partnering to secure vital cyber systems outside the federal government and Pillar 3 – helping Canadians be secure online. With this in mind it, CSS recommends a five prong strategy for investment in cyber security, through its eSecurity efforts as follows:

1. Avoid incremental investment in S&T programs that are already progressing and receive significant funding from other government departments that have been assigned related cyber security mandates;
2. Leverage, to the maximum extent possible, the mature (high TRL) 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.

J.D. Graham,

Author

CAE IES

Original Signed By

R. Howes,

Author

DRDC CSS

Original Signed By

A.L. Vallerand,

Author

DRDC CSS

Original Signed By

Reviewed by:

Dr. A.L Vallerand

Director, DSTPS

DRDC CSS

Original Signed By

Distribution List

Info

Dr. Mark Williamson, A/DG DRDC CSS

Mr Pierre Trudel, A/DDG CSS

Mr Colin Murray, Dir DSTT

Dr Andrew Vallerand, DRDC CSS Dir DSTPS

Mr. Jack Pagotto, DRDC CSS A/Dir DK&STI

Mr. Pierre Meunier , DRDC CSS Section Head

eSec CoP
CIP CoP

Unclassified/controlled goods id: DMC-A