Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

DRDC Support to Exercise Cyber Storm III

Lynne Genik
DRDC Centre forsecurity Science

Defence R&D Canada – Centre for Security Science
DRDC CSS TM 2011-24
October 2011

Canada

DRDC Support to Exercise Cyber Storm III

Lynne Genik, DRDC CSS

Defence R&D Canada – CSS

Technical Memorandum

October 2011

Principal Author

Lynne Genik, MSc
Operational Research Team, DRDC CSS

Reviewed by

Dr. Kathryn Perrett
Network Information Operations Section, DRDC Ottawa

Approved for release by

Dr. Mark Williamson
DRDC CSS Document Review Panel Chair

Abstract

This paper presents an overview of the DRDC command and control (C2) analysis support for Exercise Cyber Storm III, held in September 2010. It documents what was done, who was involved, challenges encountered, recommendations for improvement, and an indication of the overall effort required. After obtaining client support, DRDC teams were created for Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC), Government Operations Centre (GOC), the Canadian Forces Network Operations Centre (CFNOC), and the Royal Canadian Mounted Police (RCMP) National Operations Centre (NOC). Analysts prepared for the exercise by becoming familiar with exercise documentation and attending pre-exercise training and meetings. During the exercise, teams of one to three analysts observed exercise play at each operations centre, interviewed staff, and administered surveys. Following the exercise, DRDC letter reports synthesising information were delivered to clients. Key recommendations that result from providing C2 analysis for CSIII include: (1) for future exercises, DRDC should engage earlier to have ample time for preparation; (2) analysts and management must be educated on, and agree to, the commitment required to deliver this type of analysis; (3) the commanding officer of each operations centre should be engaged by DRDC prior to the exercise; (4) DRDC should deliver reports and briefings to clients within two to three weeks of the exercise for optimal impact; and (5) federal response plans related to cyber incidents are underdeveloped and require revision and harmonization. Despite several challenges, CSIII proved to be a worthwhile endeavour for both DRDC and the operations centres, helping to build strategic relationships and improve Canada's readiness for responding to major cyber incidents.

Résumé

Le présent document offre un aperçu du soutien analytique du commandement et contrôle (C2) fourni par RDDC lors de l'exercice *Cyber Storm III* qui s'est déroulé en septembre 2010. Il décrit ce qui s'est produit, qui était impliqué, les obstacles rencontrés, il fait des recommandations visant à améliorer l'exercice et donne une idée de l'effort global à effectuer pour y arriver. Après avoir obtenu le soutien du client, des équipes de RDDC ont été mises sur pied pour chacun des différents organismes : le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada, le Centre des opérations du gouvernement (COG), le Centre d'opérations des réseaux des Forces canadiennes (CORFC) et le Centre national des opérations (CNO) de la Gendarmerie royale du Canada (GRC). Les analystes se sont préparés à l'exercice en prenant connaissance des documents relatifs à l'exercice et en participant à des réunions et à de l'instruction préalable à l'exercice. Des équipes d'un à trois analystes étaient présentes dans chaque centre d'opérations lors du déroulement de l'exercice afin d'y faire des observations. Elles ont rencontré en entrevue des membres du personnel et effectué des sondages. Après l'exercice, des rapports sous forme de lettre de RDDC ont résumé les renseignements livrés aux clients. L'analyse du C2 lors de l'exercice CSIII comprenait notamment les recommandations clés suivantes : (1) lors de prochains exercices, RDDC devrait être engagée plus tôt afin d'avoir suffisamment de temps pour se préparer; (2) les analystes et les gestionnaires doivent être informés et convenir de l'engagement nécessaire pour réaliser ce genre d'analyse; (3) RDDC doit prendre contact avec les commandants de chaque centre d'opérations avant la tenue de l'exercice; (4) afin que les rapports et les briefings aient un effet optimal, RDDC doit les livrer aux clients dans un délai de deux à trois semaines après l'exercice; (5) les plans d'intervention fédéraux liés aux incidents cybernétiques sont insuffisamment développés et ont besoin d'être révisés et harmonisés. Malgré plusieurs défis à relever, l'exercice CSIII s'est révélé être une activité utile, à la fois pour RDDC et les centres d'opérations. Elle permet d'établir des relations stratégiques et d'améliorer l'état de préparation du Canada et ainsi pouvoir réagir aux incidents cybernétiques majeurs

Executive Summary

Genik, L.; DRDC CSS TM 2011-xxx; Defence R&D Canada – Centre for Security Science; June 2011.

Exercise Cyber Storm III (CSIII) was a multi-agency, functional cyber exercise, led by the Department of Homeland Security in the United States and Public Safety Canada's (PSC) National Exercise Division in Canada, which took place September 28-30, 2010. The intent of CSIII was to exercise and validate processes and procedures for cyber incident response, including several federal government response plans. CSIII was the first major cyber exercise to test the Government of Canada Information Technology Incident Management Plan (GC IT IMP). DRDC analysts were engaged one to two months prior to the exercise, and during the exercise teams of one to three analysts performed command and control (C2) analysis of the PSC Canadian Cyber Incident Response Centre (CCIRC), Government Operations Centre (GOC), Canadian Forces Network Operations Centre (CFNOC), and Royal Canadian Mounted Police (RCMP) National Operations Centre (NOC).

In preparation, analysts familiarized themselves with exercise and operations centre documentation and attended pre-exercise meetings and training. During the exercise, analysts observed operations centre staff, conducted interviews of staff, and administered surveys of exercise participants. Letter reports that included observations and recommendations were delivered to the Director General of the PSC Operations Directorate and the Commanding Officer of the CFNOC, and DRDC analysts contributed to the RCMP NOC evaluation team report. Some delays were encountered in delivering the final letter reports due to communication issues with the commanding officers of the operations centres. The level of effort required by analysts varied depending on the operations centre and the degree of activity during the exercise, the material analysed for the report (number of interviews, surveys, etc.), and the individual's contribution to reports. Most analysts expended approximately 7-20 days of effort in total on CSIII, generally on the higher end for those with more contributions to the reports. As the DRDC exercise lead and primary author for the PSC reports, the author expended on the order of 45 days related to the exercise.

The observations and recommendations provided to the Director General of the PSC Operations Directorate and the Commanding Officer of the CFNOC provided an objective, third party view of operations and a basis for evaluating plans and procedures. The DG PSC Operations Directorate and CFNOC CO were very interested in the results of the analysis. DRDC analysts reported that their exposure to the various operations centres was very beneficial to their understanding of cyber operations and the roles of the various departments. In the end, analysts came together in a short period of time and delivered quality reports to clients. Based on lessons learned within DRDC from CSIII, suggestions for improvements are provided in this document.

The DRDC analysis identified a number of challenges faced by operations centres during CSIII in areas such as roles, responsibilities, and resources; plans and SOPs; and situational awareness. Federal response plans related to cyber incidents are relatively immature and underdeveloped, and a review of the plans discussed in this document indicates that the plans are disjoint in some areas and require revision.

Sommaire

Genik, L.; DRDC CSS TM 2011-xxx; Defence R&D Canada – Centre for Security Science; June 2011.

L'exercice *Cyber Storm III* (CSIII) était un exercice cybernétique fonctionnel auquel participaient plusieurs organismes. L'exercice s'est déroulé du 28 au 30 septembre 2010. Du côté américain, il était dirigé par le département de la Sécurité intérieure et, au Canada, par la Division des exercices nationaux de Sécurité publique Canada (SPC). CSIII avait pour but de mettre en pratiquer et de valider les processus et les procédures d'intervention en cas d'incident cybernétique, y compris plusieurs plans d'intervention du gouvernement fédéral. CSIII a été le premier exercice cybernétique important à mettre à l'épreuve le Plan de gestion des incidents en matière de technologie de l'information du gouvernement du Canada (PGI TI GC). Les analystes de RDDC ont été engagés un à deux mois avant l'exercice; au cours de celui-ci, des équipes d'une à trois personnes ont fait l'analyse du commandement et contrôle (C2) du Centre canadien de réponse aux incidents cybernétiques (CCRIC) de SPC, du Centre des opérations du gouvernement (COG), du Centre d'opérations de réseau des Forces canadiennes (CORFC) et du Centre national des opérations (CNO) de la Gendarmerie royale du Canada (GRC).

En préparation à cette activité, les analystes ont pris connaissance des documents portant sur l'exercice et de ceux du Centre d'opérations; ils ont aussi participé à des réunions et à de l'instruction préparatoires à l'exercice. Au cours de l'exercice, les analystes ont observé les membres du personnel du Centre d'opérations, ils les ont rencontrés en entrevue et ils ont mené des sondages auprès des participants à l'exercice. Des rapports sous forme de lettres qui comprenaient des observations et des recommandations ont été envoyés au Directeur général de la Directions des opérations de la SPC et au commandant du CORFC. Les analystes de RDDC ont aussi apporté leur contribution au rapport de l'équipe d'évaluation du CNO de la GRC. Il y a eu certains retards dans la livraison des rapports sous forme de lettres finaux en raison de problèmes de communication avec les commandants des centres d'opérations. L'ampleur du travail des analystes variait en fonction de chacun des centres d'opérations et de son niveau de participation à l'exercice, du matériel faisant l'objet de l'analyse pour le rapport (nombre d'entrevues, de sondages, etc.) et de la contribution individuelle de chacun des analystes aux rapports. La plupart des analystes ont consacré entre 7 et 20 jours de travail à l'exercice CSIII, ceux ayant contribué davantage aux rapports travaillant généralement un plus grand nombre de jours. En tant que principal auteur des rapports de la SPC et chef de l'exercice pour RDDC, l'auteur a consacré environ 45 jours à cet exercice.

Élaborés selon le point de vue objectif d'une tierce partie, les rapports remis au directeur général (DG) de la Direction des opérations de SPC et au commandant (Cmdt) du CORFC contenaient des observations et des recommandations sur les opérations ainsi qu'une base d'évaluation des plans et procédures. Les résultats de l'analyse ont beaucoup intéressé le DG de la Direction des opérations de SPC et le Cmdt du CORFC. Les analystes de RDDC ont signalé que le fait d'avoir visité les différents centres d'opérations a eu un effet très bénéfique sur leur compréhension des opérations cybernétiques et des rôles des différents services. En fin de compte, les analystes se sont ralliés en peu de temps et ont livré des rapports de qualité aux clients. Compte tenu des leçons retenues de l'exercice CSIII par RDDC, le présent document contient des suggestions relatives à l'amélioration de cette activité.

L’analyse de RDDC contient un inventaire d’un certain nombre de défis auxquels ont été confrontés les centres d’opérations lors de l’exercice CSIII dans les domaines tels que les rôles, les responsabilités et les ressources, les plans et les IPO ainsi que la connaissance de la situation. Les plans d’intervention fédéraux portant sur les incidents cybernétiques sont encore relativement peu élaborés et insuffisamment développés et un examen des plans examinés dans le présent document révèle que ces plans sont disjoints dans certains domaines et nécessitent quelques révisions.

Table of contents

Acknowledgements

The author would like to thank all the DRDC staff who were involved with the support to Exercise Cyber Storm III.

1 Introduction

This document reports on the DRDC support provided for Exercise Cyber Storm III (CSIII) in performing command and control (C2) analysis of operations centres. The main purpose of the document is to capture what was done in support of CSIII, and to provide recommendations to improve future support efforts for similar exercises.

1.1 Exercise Cyber Storm III

Exercise Cyber Storm III (CSIII) took place September 28-30, 2010, as a distributed, multi-national, functional exercise led by the Department of Homeland Security. The Canadian portion of CSIII was led by the PSC National Exercise Division (NED).

The Department of Homeland Security's international objectives[1] included [1]:

1. Evaluating the Usual 5[2] formal information sharing protocols[3];

2. Assessing information sharing and intelligence sharing (classified, unclassified and proprietary) between communities of interest, including the ability to further share information with affected parties; and

3. Validating the Usual 5 public affairs protocols.

Although the "Usual 5" includes Canada, Canada did not participate in the international aspect of play.

Canadian national objectives as defined by PSC [1] included:

1. Exercising existing processes, procedures, plans, relationships and mechanisms in order to validate them during a cyber event/threat;

2. Exercising info-sharing protocols, including tear-line procedures, with a focus on sharing information at the appropriate classification level;

3. Validating coordination procedures/mechanisms across the constituency (Federal, Private Sector) including the federal/international linkages.

4. Validating decision making procedures for ADM EMC in response to a cyber incident; and

5. Assessing the implementation of specific corrective actions taken as a result of previous exercises (CSI and CSII).

From a Canadian perspective, CSIII was intended to validate the following plans and procedures:

[1] The US listed 12 international partners for the exercise http://www.dhs.gov/files/training/gc_1204738275985.shtm
[2] The "Usual 5" is the public safety/security terminology for what the military refers to as the "5 Eyes" nations, (Canada, the United States, the United Kingdom, Australia, and New Zealand)

- Federal Emergency Response Plan (FERP) [2],
- Cyber Triage Unit Standard Operating Procedures (SOPs) [3],
- Government of Canada (GC) Information Technology (IT) Incident Management Plan (IMP) [4],
- Assistant Deputy Minister (ADM) Emergency Management Committee (EMC) SOPs,
- International Watch and Warning Network (IWWN) SOPs, and
- Usual 5 SOPs.

As noted, the international aspect of CSIII was not played by Canadian federal government departments, so the latter two SOPs were not exercised. DRDC was not provided with a copy of the ADM SOPs.

Participating departments were originally intended to include:

- Public Safety Canada - Government Operations Centre (GOC), Canadian Cyber Incident Response Centre (CCIRC), Information Technology, Public Affairs;
- Department of National Defence (DND);
- Royal Canadian Mounted Police (RCMP);
- Canada Border Services Agency (CBSA);
- Canada Revenue Agency (CRA);
- Canadian Security Intelligence Service (CSIS);
- Communications Security Establishment Canada (CSEC);
- Transport Canada (TC);
- Human Resources and Skills Development Canada (HRSDC);
- Industry Canada (IC);
- Natural Resources Canada (NRCan);
- Treasury Board Secretariat (CIOC); and
- Department of Justice (DOJ).

However, these departments participated to varying degrees and some organizations, such as Industry Canada and the Integrated Threat Assessment Centre, withdrew their participation in advance of the exercise for reasons such as resource constraints.

Canadian exercise play officially began on Tuesday, September 28, 2010, at 0800 hours Eastern Daylight Time (EDT) and ended at approximately 1400 hours EDT on Thursday, September 30, 2010. Exercise play was approximately nine hours per day (0800-1700 hours EDT) for the first two days and six hours on the third.

The exercise storyline can be summarized as follows: an adversary launched the first and second phases of a coordinated, three-phase cyber attack against the Government of Canada. Phase 1 involved a web defacement attack and Phase 2 included both a malware attack and an attack on Government “Smart

Phone" Enterprise Servers (SPES). Phase 3 involved a *threatened* attack against the telecommunications controlling SCADA systems. The exercise injects were contained in a Master Sequence of Events List (MSEL) [5].

1.2 DRDC Involvement

Several months prior to the exercise, the Director General of DRDC CSS requested an assessment on potential DRDC support for Exercise Cyber Storm III. After attending an Exercise Design Team (EDT) meeting at the end of July (2010), the author proposed several options for support, depending on the appropriate availability of resources, namely:

1. Review previous lessons learned (LL)/after action report (AAR) documents, provide PSC NED with guidance for and/or assistance with developing evaluator forms, and/or provide observers/evaluators for departments;

2. Perform post-event assessment of evaluation forms and/or evaluation observations and/or assistance with the LL/AARs;

3. Review the scenarios and master sequence of events list (MSEL) for completeness and/or to ensure they are meeting exercise objectives and addressing comments/problems from previous Cyber Storm AARs;

4. Perform an independent command and control (C2) analysis of select operations centres.

Given the short time frame and the lead role of PSC NED in developing the exercise and performing the exercise AAR, the focus was decided to be on activities similar to those that DRDC performed for the Vancouver Olympic and Paralympic Winter Games 2010 (V2010) and the G8/G20 (held in June 2010) through the Major Events Coordinated Security Solutions (MECSS) project[4], that is, to provide a C2 analysis of individual operations centres (option 4). The intent was that DRDC would provide each operations centre with a C2 analysis that was independent of the overall exercise evaluation, and feed into the PSC NED evaluation as requested by the exercise lead at each operations centre.

1.3 Document Structure

The next section outlines the preparations that were undertaken for the exercise. Section 3 discusses the time commitment and tasks of the staff involved in the exercise. The analysis methodology is presented in section 4; section 5 highlights observation themes of the analysis and discusses federal response plans. Post-exercise activities are presented in section 6, followed by the conclusion.

[4] Numerous client letter reports were created during V2010 and G8/20; copies are held by DRDC CSS

2 Preparation

2.1 Clients and Buy-In

As identified in the Canada's Cyber Security Strategy, the Canadian Cyber Incident Response Centre (CCIRC) has the responsibility to "coordinate the national response to any cyber security incident" [6]. Among other things, CCIRC is the cyber response coordination point for the Government of Canada (GC), and is responsible for engaging the Cyber Triage Unit (CTU). The CTU consists of members from CCIRC as well as the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment Canada (CSEC), the Royal Canadian Mounted Police (RCMP), and the Department of National Defence (DND). Since these departments and agencies have key roles for cyber response, they were the initial client group considered for C2 analysis. However, given limited DRDC resources, pre-established relationships with members of DND, PSC, and the RCMP and the desire to continue to build relationships across these organizations, DRDC extended offers of support to the Public Safety Canada Operations Directorate – Government Operations Centre (GOC) and CCIRC, the DND Canadian Forces Network Operations Centre (CFNOC), and the RCMP National Operations Centre (NOC). These organizations are often hereafter referred to as the "clients".

Client buy-in was instigated at the operator level. Bill Casey, a Program Officer from the PSC Operations Directorate, was familiar with DRDC and had expressed an interest in discussing whether or not a DRDC scientific advisor (SA) would participate in CSIII[5]. Subsequently, the idea of C2 analysis support was informally discussed with Bill and with Luc Beaudoin, Chief of Cyber Operations at CCIRC and a former DRDC Ottawa engineer. A positive sentiment was received from these individuals. Following an EDT meeting, the offer of C2 analysis support was put forth by the author to representatives from the operations centres listed above. Subsequent meetings were arranged with each organization to discuss the proposal further. Senior management participated in these meetings, but the commanding officers of the respective operations centres were not directly involved in the discussions with DRDC. Generally the EDT members were the ones who coordinated the DRDC involvement.

Recommendation for improvement:

- *(Recommendation 1) While operator buy-in was essential, it would have been useful to briefly meet in advance of the exercise with the commanding officer of each operations centre to establish a relationship and ensure their buy-in. In the end, the commanders own the output reports and must ultimately decide whether or not to accept the analysis and recommendations contained therein.*

2.2 DRDC Teams

DRDC CSS initiated a reach-back request[6] to the DRDC labs for exercise support [7]. Based on the response, the author created support teams for the PSC Operations Directorate Government Operations Centre (GOC) and Canadian Cyber Incident Response Centre (CCIRC), the Canadian Forces Network Operations Centre (CFNOC), and the RCMP National Operations Centre (NOC). In order to maximize DRDC exposure to the exercise, analysts were drawn from five centres: DRDC CSS, Toronto, Corporate,

[5] A DRDC SA had been among the liaison staff at the GOC during V2010 and the G8/G20

[6] Reach-back requests originated with MECSS as a means of accessing expertise and support from DRDC labs

Ottawa, and Valcartier. It was considered crucial to have a team lead with exercise/operations C2 analysis experience, who could direct inexperienced analysts at each operations centre. Therefore, team leads with prior experience were sought. In addition, the teams were formed with at least one analyst with cyber expertise. It should be noted that some staff are better suited for this type of activity than others; ideally, analysts should be flexible, reliable, perceptive, and congenial. Therefore, having a sense of how analysts have performed in similar roles and/or personality traits and abilities is useful in selecting team members.

The DRDC teams were composed as follows, with area of expertise denoted in brackets after each team member's name:

1. PSC Operations Directorate:
    a. CCIRC
        i. DRDC Exercise Lead: Lynne Genik, Defence Scientist, DRDC CSS (C2/cyber)
        ii. Simona Verga, Defence Scientist, DRDC CSS (did not participate due to CCIRC feedback[7])
    b. GOC
        i. Lead: Wendy Sullivan-Kwantes, Group Leader, DRDC Toronto (C2)
        ii. Paul Béland, Thrust Coordinator, DRDC Corporate (cyber)
2. CFNOC
        i. Lead: David Smith, Defence Scientist, DRDC Toronto (C2)
        ii. Kathryn Perrett, Defence Scientist, DRDC Ottawa (cyber)
        iii. Fréderic Painchaud, Defence Scientist, DRDC Valcartier (cyber)
3. RCMP NOC
        i. Lead: Anthony Masys, Defence Scientist, DRDC CSS (C2)
        ii. Ian Chapman, Defence Scientist, DRDC CORA (cyber)

The DRDC analysts for the RCMP NOC served in a supporting role as part of the RCMP evaluation team, whereas the teams assigned to PSC and DND led an independent analysis. Since the RCMP support was coordinated through the RCMP team lead, Tony Masys, the author had little visibility into their approach.

[7] It was originally intended that two DRDC analysts would support CCIRC; however, CCIRC felt that one would be sufficient.

2.3 Exercise Meetings

The following table provides a schedule of exercise-related events requiring attendance by team members:

Date	Event	DRDC Attendance Required
August 31	DRDC meeting/conference call - Introduction to CSIII and DRDC support	All
September 1	CFNOC visit	Exercise lead and CFNOC team
September 7	GOC/CCIRC visit	Exercise lead and PSC team
September 9	EDT/SME meeting - review of MSEL	Exercise lead and at least one analyst from each team
September 10	DRDC preparatory meeting/conference call	All
Week of Sept 13	RCMP NOC visit	RCMP team
September 16	DRDC preparatory meeting/conference call	All
September 16	CSIII participant orientation (half day)	None – though in retrospect may have been helpful to witness player orientation
September 22	Controller/evaluator training (half day)	Exercise lead and at least one analyst from each team
September 23	DRDC preparatory conference call	All
September 27	DRDC analyst orientation	All
September 28-30	Exercise play	All
October 1	CSIII Hotwash	All welcome
October 5	DRDC debrief conference call	All

Some team members were not located in Ottawa and did not attend as many meetings as those staff located in Ottawa due to associated travel costs. As evidenced by the schedule above, the majority of meetings took place in the month preceding the exercise.

The visits to the operations centres were critical for pre-exercise knowledge gathering. In advance of the meetings, the operations centres were asked to provide answers to the following questions:

1. What are the exercise objectives for the operations centre?

2. What standard operating procedures (SOPs) will the operations centre be exercising? Are they documented? If so, can you please provide DRDC with copies?

3. Can you please provide an organizational chart or organizational structure document for the operations centre? What operations centre staff positions/groups would be most appropriate for analysts to focus on given limited DRDC resources?

4. Are there any priority areas/issues the operations centre would like DRDC analysts to be aware of?

5. Can you please confirm the operations centre hours related to the exercise? (For example, for V2010 some operations centres did briefings prior to/after exercise play.)

6. What hotwash(es)[8] is (are) the operations centre participating in? Dates/times?

7. Does the operations centre have lessons learned documents from previous Cyber Storm exercises that we can have access to?

The questions and answers were discussed in detail during the visits, overviews and tours of the operations centres were provided, and analysts were introduced to and had discussions with operations centre staff (typically those in supervisory roles).

Recommendations for improvement:

- *(R2) It would have been beneficial for staff to spend time observing operations centres in advance of the exercise in order to have a better sense of typical activities and how DRDC resources could be used most effectively. If this had been the case for CCIRC, DRDC may have advocated for two analysts to observe during the exercise, rather than agreeing to one.*
- *(R3) It may be more effective to have teams, in particular, team leads, in the same city as the operation centres so that they can more easily attend exercise-related events and meet with operations centre staff. Otherwise, DRDC should be prepared to pay associated travel costs.*

2.4 Exercise-Related Documentation

Exercise-related documentation to prepare analysts was provided through a portal populated by PSC NED as well as by individual operations centres.

2.4.1 CSIII Exercise Portal

Cyber Storm I, II, and III exercise-related documents are hosted on a PSC NED Cyber Storm portal. For Cyber Storm III, documents included the master sequence of events list (MSEL), EDT minutes, information on scenarios, player orientation information, exercise plans, etc. Portal accounts had to be requested from PSC NED. The author received portal access in early August soon after joining the EDT team, but the remaining team members were not granted portal access until mid-September, after submitting requests for accounts at the end of August. As a result, they did not have access to all of the exercise documentation and had to rely on the DRDC exercise lead to manually distribute documents in the meantime.

Recommendation for improvement:

- *(R4) The DRDC exercise lead should engage in exercise planning and begin preparations for DRDC support a minimum of three to four months prior to the exercise, in order to facilitate meetings and travel plans and so that issues such as access to the portal do not become time-critical.*

[8] This refers to the gathering of participants and planners shortly after the exercise to discuss what went well and what needs improvement.

2.4.2 Documentation Provided by Operations Centres

In advance of the exercise, the PSC Operations Directorate provided the following documents:

- Federal Emergency Response Plan (FERP) [2];
- Cyber Triage Unit Standard Operating Procedures (CTU SOPs) [3];
- Government of Canada information Technology Incident Management Plan (GC IT IMP) [4];
- Government Operations Centre Incident Report Criteria [8].
- Emergency Management and National Security Capability Improvement Process [9];
- PSC Operations Directorate organizational chart.

The FERP, GC IT IMP and CTU SOPs were three of the five plans/procedures that were intended to be validated by the exercise. The remaining two documents were the ADM EMC SOPs, which were outside the scope of the analysis, and the International Watch and Warning Network SOPs, which were not exercised since Canada did not participate in international play for CSIII.

The CFNOC provided:

- PowerPoint overview of the operations squadron [10];
- After-action reports from Exercise Trillium Guardian [11], Operation Cadence [12], and Olympic exercise-related material [13] and emails;

- A CD of plans and procedures. The content was too extensive to send via email, so a copy was sent by mail. Unfortunately, it did not arrive until the Friday prior to the start of the exercise, so there was very limited time remaining to review the plans and procedures in advance of the exercise (although analysts did review it). This is another example of an issue that could have been avoided had DRDC engaged earlier.

2.4.3 Exercise Event Timeline

The Master Sequence of Events Lists (MSEL) was the master document for exercise play, and contained a description of each exercise "inject" (information provided to players to generate action), such as the date/time, the mode of the inject (for example, email, phone, etc.), sent to/from, a description, and the expected action. For CSIII, the MSEL was an Excel spreadsheet with 188 injects [5]. Based on the MSEL, Simona Verga, a defence scientist with DRDC CSS, created visual timelines for the three events. Analysts were expected to be familiar with the scenario/event timelines, and this visual timeline provided a useful, quick visual reference.

2.5 Coordination with Operations Centres

After the initial meetings with the operations centres, it was the responsibility of the team leads to coordinate with their operations centre. There was some confusion between the CFNOC and the DRDC team, which resulted in a number of exercise-related emails being sent to a DREnet account that could not be accessed during the exercise, unbeknownst to both the sender and recipient.

Recommendation for improvement:

- *(R5) Teams should establish (1) clear points of contact and (2) plans for the exchange of information during the exercise with operations centres in advance of the exercise.*

2.6 Information Gathering Tools

Tools for gathering information about the exercise included semi-structured interviews and surveys. The interview questions and surveys were prepared in advance of the exercise.

2.6.1 Interview Questions

The following were the standard questions asked of interviewees:

1. What is your normal position and how long have you been in that position? Can you provide your contact information?

2. What was your role during Cyber Storm III? What were your responsibilities during the exercise?

3. How would characterize your understanding of cyber issues in the context of your position?

4. Overall, how well do you feel that your operations centre handled the cyber incidents that were part of the exercise?

5. What areas stand out as successful?

6. What areas stand out as challenging?

7. What supporting documents were available and were they effective? What, if anything, is not documented that you would like to see documented?

8. Did you notice any issues with handling of information (for example, appropriate classification of information)?

9. What would you change? How would you make things function better?

Since the interviews were semi-structured, the flexibility allowed for additional questions to be asked based on what the interviewee said.

2.6.2 Survey Design

PSC NED developed a participant survey (Annex A) that focused on an evaluation of the exercise. The DRDC exercise lead and David Smith, the CFNOC team lead, reviewed the survey for questions of interest to the DRDC analysis, and determined they were mainly the latter ones (questions 14-18). A separate DRDC survey was created based on previous V2010 and G8/G20 surveys, and focused more on the functioning of the operations centre and the participants' ability to perform their roles (Annex B). It was later noticed that the strongly agree/disagree columns were opposite for the PSC and DRDC surveys

(that is, in the PSC survey strongly agree was on the left of the scale and strongly disagree on the right, and for the DRDC survey it was the opposite).

Recommendation for improvement:

- *(R6) If multiple surveys are used, provide consistency between scales if possible to avoid any confusion.*

2.7 CSIII Ethics Protocol

The Cyber Storm III Ethics Protocol (Annex C) was prepared under the lead of David Smith, CFNOC team lead, using a template from the G8/G20, and was reviewed by the DRDC Toronto Human Research Ethics Committee. He provided a brief on the ethics protocol during the DRDC team orientation to the exercise.

During a later presentation on research misconduct [14], the Chief Scientist of DGMPR identified "unethical treatment of research subjects" as an area of research misconduct, with "absent or inadequate informed consent of human subjects", and the "failure to maintain confidentiality of human data without specific consent from the subject" as common problems. In light of this, the recommendation below is provided.

Recommendation for improvement:

- *(R7) Emphasis should be placed on the ethics protocol to ensure that all analysts clearly understand the protocol, its implications, and their responsibilities. Team members should each be provided with a copy of the ethics protocol and it should be reviewed in detail with the team.*

3 Tasks and Time Commitment

3.1 Time Commitment

The author asked analysts for feedback on the amount of time spent on CSIII activities. The response generally reflected the amount of preparation, exercise observation, and post-exercise analysis and report-writing time. The largest differentiator in time was related to the effort required for report writing; on one end, the team with the RCMP had completed their responsibilities and provided contributions to the RCMP report by the end of the exercise, while on the other, the PSC team leads had a significant amount of information from exercise activity - 60 plus pages of notes per team lead not including interviews, notes from approximately 30 interviews and 30 (x2) surveys - to process following the exercise. Most analysts reported spending in the vicinity of 7-20 days on activities related to the exercise; however, the DRDC exercise lead spent a total of approximately 45 days on the exercise.

Analysts reported that they felt their participation in CSIII was beneficial and provided valuable insight into cyber operations within the Government of Canada.

Recommendations for improvement:

- *(R8) All staff, but in particular the exercise and team leads, must have time to dedicate to this activity. This involves much more than showing up during the exercise, and includes a commitment to attend meetings and activities, to read and prepare in advance of the exercise, to communicate with the clients and team, and to follow through with delivering a client report and briefing in a timely manner.*
- *(R9) Management must be educated on the commitment required. The time necessary to lead this type of project and for analysts to provide C2 analysis support must be communicated and understood. Time requirements may be variable for different teams and will depend on factors like the number of pre-exercise meetings, extent of operations centre activity during the exercise, number and length of interviews performed, and survey analysis.*

3.2 DRDC Exercise Lead Tasks

The DRDC exercise lead was responsible for the formulation of the support proposal, constructing teams, and overall leading the exercise support. A summary of DRDC exercise lead tasks are as follows:

- Attend EDT meetings;
- Scientific lead on scope of exercise support and internal DRDC discussions;
- Create and market DRDC proposal to clients;
- Solicit DRDC analysts (discussions, briefings, etc.);
- Provide background and task description for reach-back request;
- Create teams for each operations centre;
- Communicate with clients, coordinate and attend operations centre visits;

- Team logistics – portal access, meeting attendance, travel, overtime, etc.;
- Prepare and lead DRDC team preparatory conference calls and orientation day;
- Conduct DRDC team debrief;
- Review team reports;
- Obtain sign-off on reports;

As the DRDC exercise lead for support to CSIII as well as the PSC Operations Directorate lead, the author spent approximately 45 days over a number of months on preparation, exercise attendance, communication with the DRDC teams and clients, and post-exercise analysis, report-writing and briefing preparation.

3.3 Team Lead Tasks

Team leads were responsible for leading the analysts within their respective teams, and coordinating with the staff of the operations centre. Tasks carried out by team leads included:

- Solicit DRDC analysts;
- Attend preparatory meetings including operations centre visits;
- Communicate and coordinate with respective operations centre;
- Communicate information and plans with team members;
- Observe exercise play, interview participants during and after exercise, distribute/collect surveys;
- Attend hotwash;
- Coordinate post-exercise team meetings;
- Lead survey analysis, review and verify data and calculations, interpret results;
- Analyse information and coordinate writing of client report;
- Ensure delivery of report to client in timely manner;
- Create client presentation and coordinate client briefing.

The team leads for the RCMP, CFNOC, and GOC reported time expenditures of 7-17 days for CSIII. These numbers may not be indicative of team lead time requirements for future efforts (that is, they may be on the low side) for the following reasons:

- Due to the relatively short lead-up time to the exercise, team leads may not have had a lot of time to invest in preparation given other work commitments;
- Travel limitations prevented two team leads (located outside of Ottawa) from attending a number of the meetings in advance of the exercise;
- The team leads were not primary authors of the reports (for various reasons such as team played a supporting role, unplanned leave of absence, etc.);
- Formal briefings were not given to commanders following the exercise.

3.4 Analyst Tasks

In their CSIII duties, analysts were expected to:

- Become familiar with operations centre staff, organizational structure, standard operating procedures, lessons learned documents, CSIII exercise objectives/documents, etc. This required pre-reading and a visit to the operations centre for most analysts;
- Participate in CSIII/DRDC orientation activities as required;
- Observe participants during play at the respective operations centres;
- Interview exercise participants during/after exercise;
- Distribute/analyze surveys; and
- Contribute to/write the final report. Draft reports were requested within two weeks of the exercise.

3.5 Administrative Support Tasks

Administrative support tasks included:

- Coordinating the reach-back request [7];
- Creating the tasking orders [15];
- Processing the travel claims.

This support was provided by DRDC CSS staff. A total of approximately 11 days of effort was reported for these activities.

A maximum of six hours per person of overtime was approved in advance of the exercise. The PSC team members were the only ones that worked overtime during the exercise.

4 C2 Analysis Methodology

The focus of the teams was to observe information sharing and command and control relationships for the operations centres, while also feeding into PSC NED's exercise evaluation through designated points of contact. Since the author was at the PSC Operations Directorate during the exercise, some of the additional detail in this section is provided from that perspective.

4.1 Direct Observation

Analysts were deployed to the operations centres during the course of the exercise. The analysts observed activities (in some cases, such as at the CFNOC, real-world in additional to exercise activities), spoke to players about unfolding events when there were opportunities, and attended operations centre briefings and exercise-related meetings when possible. For example, teams at the PSC Operations Directorate and CFNOC attended operations centre briefings (such as the daily briefings) and PSC analysts attended Management Team and ADM EMC meetings.

Given real-world events involving the RCMP, the NOC activity was performed at the back-up location so the exercise would not interfere. In retrospect, the NOC may not have been the best place for analysts to observe exercise activity, since most of the activity occurred at the technical level and the NOC was not involved to a large degree; however, this was an RCMP decision. Given the low level of exercise activity involving the NOC, the DRDC analysts were sent home early during the exercise.

The CFNOC participated in one of the three exercise scenarios and most of their activity occurred early in the exercise. Analysts reported some difficulty in tracking incoming information since they were often unaware of when information was coming in or how it was moving around. The analysts had sufficient time to complete interviews by the end of the exercise. One analyst took 46 pages of notebook-sized notes during the exercise, including interviews.

CCIRC participated in all three exercise scenarios, and were very busy until the end of the exercise. The author and the GOC team lead than took more than 60 pages of hand-written notes each over the course of the exercise, not including interviews. These notes, including details of the events and participants, provided a very useful reference during post-exercise discussions and the writing of the report. As mentioned, only one analyst observed exercise play at CCIRC, which meant that a lot of activity could not be observed since many players were acting simultaneously in different physical locations. Two analysts seemed sufficient for observation of the GOC.

Determining the most appropriate placement of analysts/observers in advance of the exercise is generally done in conjunction with operations centre staff and requires a basic understanding of how information flows and decisions are made within an operations centre. Once analysts have a good understanding of information flows from initial vantage points, there may be value in moving around "with" information and as problem areas are identified.

Recommendations for improvement:

- *(R10) Efforts should be made to ensure that there are an adequate number of analysts/observers placed at effective vantage points within each operations centre.*

4.2 Exercise Email

Analysts at PSC and the CFNOC had copies of some of the email distributed as part of the exercise. An analyst at the CFNOC had access to the CFNOC inject emails. The analyst at CCIRC had access to a PSC email account with auto-forwarded exercise emails from the Cyber Duty Officer, containing CCIRC products, such as Cyber Flashes. PSC analysts were also on a GOC exercise distribution list and received GOC exercise products, such as Situation Reports. These emails were archived for later use, and proved useful references for operations centre products and the time of distribution.

Recommendations for improvement:

- *(R11) While it may be unrealistic for analysts to track all exercise emails, certain emails, such as those containing operations centre products (for example, situation reports), are pertinent for the post-exercise analysis of events. Therefore, it is useful to have analysts on appropriate exercise participant distribution lists.*

4.3 Staff Interviews

Semi-structured interviews were performed with operations centre staff, using the questions provided in section 2.6. Most exercise participants from the PSC Operations Directorate and the CFNOC were interviewed by DRDC analysts. However, at PSC it was not possible to interview all participants during the exercise given that some staff members were too busy. Therefore, some of the PSC interviews were completed after the exercise. Interviews ranged from approximately 10 minutes to an hour, depending on the involvement of the interviewee in the exercise and how much they had to say. Several interviews, specifically those of the Management Team from other departments, were conducted by phone.

Interviews are a very useful data collection tool since they provide a confidential forum for players to provide their views, their version of how events played out, their rationale for actions, as well as their suggestions for areas for improvement.

4.4 Survey Completion

Players were asked to complete two hard copy surveys towards the end of the exercise, a PSC NED Participant Feedback survey focusing on the exercise (Annex A) and a DRDC survey focusing on command and control and information sharing issues (Annex B). Players were able to complete the DRDC survey anonymously if they so chose.

The CFNOC team had very few surveys returned to them so a survey analysis was not included in their report, and the RCMP did not use the DRDC survey. Twenty nine surveys were completed by PSC exercise participants, ranging from operations staff and liaison officers to the Director General.

There was discussion during the DRDC team debrief about distributing surveys by email, but several team members reported that this hadn't work well in the past. The pros to using paper surveys include the ease of distribution and collection of the surveys within the operations centre. This becomes more challenging with email, especially in operations centres where (1) participants come from outside and do not have access to their personal email accounts to complete surveys and (2) analysts do not have access to their accounts to distribute surveys and track survey response. A web-based survey may resolve some of these issues; however the development of such a tool would require some effort.

Recommendations for improvement:

- *(R12) Team leads must ensure that most, if not all, exercise participants complete and return the survey forms before the end of (preferably), or shortly after, the exercise.*

- *(R13) If multiple surveys are distributed, sufficient distinction should be made to the players between surveys and their uses.*

- *(R14) Participants should be reminded of their right to anonymity.*

- *The pros and cons of paper versus electronic surveys should be considered.*

5 Observations and Analysis

5.1 Exercise Constraints

Despite the Exercise Development Team's best intentions to simulate realistic cyber events and elicit of realistic response, a number of issues were observed during CSIII [16], such as:

- CSIII was created as an international exercise, but Canada did not participate in the international play. However, exercise activity generated in other participating countries, such as the US, occasionally filtered into Canada. This often created confusion since it was not clear to players whether or not they should be acting on this information;

- The private sector did not participate in CSIII in Canada. In similar real-life situations the private sector would have been heavily engaged. Private sector companies participated in the US play[9], and this created some confusion when the companies also had offices in Canada.

- It was not always clear which departments were playing, which caused confusion. Some departments that would normally be involved in the unfolding of events in real-world situations, such as Industry Canada, did not actively participate during CSIII. This led to gaps in expertise and roles and responsibilities;

- In many cases, normal points of contact were substituted with different players or were simulated. This caused disruption and time delays, in particular on the first day of the exercise, and in some cases a degradation in the realism of the exercise;

- Exercise controllers were not always present at meetings in order to prevent players from going in directions that were not intended. For example, when international information was received, players were initially unsure as to whether or not they were intended to act on it;

- In some cases technical details were lacking so players did not have enough information to determine the appropriate course of action;

- Real events took priority and there were times when exercise events had to be put on hold. This caused delays in the sharing of information;

- A number of players reported not having had an opportunity to read the exercise material, not having had training for the exercise, and/or not having had an exercise briefing. Those individuals generally reported that they felt poorly prepared for the exercise.

5.2 Observation Themes

The PSC Operations Directorate [16, 17] and CFNOC [18] letter reports detail the findings of DRDC observations and analysis. The final analysis results for the PSC Operations Directorate were grouped into categories of:

[9] The US reported 60 private sector companies in CSIII http://www.dhs.gov/files/training/gc_1204738275985.shtm

1. Roles, responsibilities, and resources;

2. Plans and SOPs;

3. Situational awareness.

Within each of these areas, a number of observations were made. Along with each observation, recommendations for improvement were provided to the client. Many of the observations in the CFNOC report also fit into these categories. In the author's experience, these are common challenges within operations centres. Often particular roles and responsibilities may be unclear and/or personnel are inadequately trained. This may be related to a lack of clear documentation regarding roles and responsibilities, plans and standard operating procedures. While shared situational awareness is a goal for operations centres, it can be very difficult to achieve, particularly during high-paced events.

5.3 Survey Analysis

The responses of 29 surveys were analysed for the PSC Operations Directorate. This was a fairly time-consuming activity and technologists from DRDC Toronto were enlisted to assist with the analysis. Responses were first transferred from the paper surveys into an Excel spreadsheet for analysis. The numerical responses were analysed and the text responses to questions were grouped. Respondents were assigned to one of four categories based on their role: (1) CCIRC; (2) GOC; (3) SARA and Plans and Logistics; or (4) Other, which included staff from organizations/divisions that did not fall into one of the first three (such as liaison officers and the DG).

A sample of how the results were presented in the report is shown in the table below. The strongly disagree and strongly agree responses were combined with the disagree/agree responses respectively to give one percentage. The total number of responses was listed under "count".

List number and question here

Response	CCIRC	GOC	SARA + P&L	Other	Overall
N/A	%	%	%	%	%
Disagree	%	%	%	%	%
Neutral	%	%	%	%	%
Agree	%	%	%	%	%
Count	#	#	#	#	#

Table 1. Sample survey response table

A paragraph discussing the table results was provided for each question. Text responses were summarized, and the actual text comments and responses were included in an annex of the letter report, with potential identifying information removed.

The surveys provided insightful information into the views of the participants and provided quantitative and qualitative feedback. In particular, the survey results highlighted interesting differences of opinions between the various groups within the PSC Operations Directorate. This often supported observations made by analysts during the exercise.

5.4 Federal Plans and Standard Operating Procedures

A review of federal plans and standard operating procedures [16] identified a lack of consistency between the various plans, as well as inadequate definitions for what constitutes an "emergency" cyber incident. The plans are discussed in more detail below.

5.4.1 Federal Emergency Response Plan (FERP)

The purpose of the Federal Emergency Response Plan (FERP) [2] is to harmonize emergency response efforts between the federal government, provincial/territorial governments, the private sectors, and non-governmental organizations. It outlines a high-level structure and functions for the Federal Emergency Response Management System in general terms. The FERP begins with the statement: "Most emergencies in Canada are local in nature and are managed at the municipal or provincial/territorial level". This may be the case with many physical emergencies, such as floods and wildfires. However, given the interconnectedness of networks, speed of events, and lack of cyber response teams at lower levels of government, this will not necessarily be true of cyber incidents. The FERP seems to be designed for physical emergencies that escalate from the local level to the provincial and federal levels and, while cyber is mentioned as part of the all-hazards threat and risk environment, there are no distinctions made for cyber incidents.

An emergency as defined in the FERP is: "A present or imminent incident requiring the prompt coordination of actions, persons or property in order to protect the health, safety or welfare of people, or to limit damage to property or to the environment." Given this definition, it's challenging to know when a cyber incident becomes an "emergency". The FERP also lists "Industry" (Industry Canada) as the minister with the primary responsibility for emergency support functions pertaining to telecommunications. This is likely due to the historical development of telecommunications along with established relationships and agreements through groups like IC's Canadian Telecom Cyber Protection. However, CCIRC has the responsibility to coordinate the national response to cyber security incidents; this is not addressed within the FERP.

Recommendations for improvement:

- *(R15) The FERP must be revisited in order to clarify and reflect the unique aspects of cyber incidents.*
- *(R16) All federal departments should familiarize themselves with the contents of the FERP.*

5.4.2 Government of Canada Information Technology Incident Management Plan (GC IT IMP)

The Government of Canada Information Technology Incident Management Plan (GC IT IMP) [4] is the government's first plan related to cyber incident management, and CSIII was the first major cyber exercise to test it government-wide[10]. The plan establishes a baseline governance model, but lacks process and guidance detail and leaves much open to interpretation. It appears to have been developed with a large-scale incident in mind, as opposed to more common incidents that are less severe.

The GC IT IMP was developed with some fundamental assumptions that may not be in accordance with reality, such as "all departments within the GC will collaborate and contribute accordingly" and "all departments are familiar with the contents of the FERP". In the section on risk, the plan states that departments will perform internal risk analyses and share them with CCIRC, CCIRC will share departmental risk analyses with the CTU, and the CTU will perform a GC-wide analysis of an incident's potential or actual impact. This assumes that departments are capable of performing cyber risk analyses and that they will share those analyses with CCIRC, which may not be an accurate assumption. In addition, the GC-wide analysis role of the CTU as outlined in the GC IT IMP is not addressed by the CTU SOPs.

The plan claims to identify the senior management committees that are engaged when triggers are met. First of all, the trigger criteria are so general that they could apply to many cyber incidents (for example, descriptions include qualifiers such as "affect more than one department", and "affect common services"). Given this, the criteria are likely too vague to provide effective assistance in helping departments decide when to report an incident to CCIRC. Secondly, the management team is defined as the "executive-level team that provides strategic guidance to the GOC and CCIRC". The team is comprised of representatives "described in the FERP" as well as a Treasury Board Chief Information Officer Branch representative. However, when one refers to the FERP, representatives from the Department of Justice and the PSC Associate DG of Communications are specified, with the rest of the management team composed of "primary department representatives" as determined by the DG Operations Directorate in consultation with the Federal Coordinating Officer. Nowhere are the specific organizations, the appropriate branches of organizations, or proper levels of representative defined. Furthermore, details of the roles of the management team are not defined beyond high level statements such as that above (that is, providing strategic guidance). In reality, inclusion in the team and roles appear to be largely at the discretion of the DG PSC Operations Directorate. The management team was convened during Cyber Storm III for the first time in the history of the IMP, with a new DG who relied on the GC IT IMP for guidance.

Recommendation for improvement:

- *(R17) The GC IT IMP should be updated under the consultation of key cyber response departments. In particular, it is recommended that the plan define practical thresholds for cyber incidents.*
- *(R18) It is recommended that specific Terms of Reference be developed for the Management Team, including a list of the appropriate representatives to be included in the Management Team.*

[10] The GC IT IMP was tested during Vancouver Olympic preparatory Exercises Silver and Gold in 2009, but in a very limited capacity.

5.4.3 Cyber Triage Unit (CTU) Standard Operating Procedures (SOPs)

The Cyber Triage Unit (CTU) Standard Operating Procedures (SOPs) [3] pre-date the FERP and GC IT IMP. The SOPs provide the operational framework for cyber incidents that require an initial assessment in order to determine the primary organizations affected and the supporting roles of other departments. However, the GC IT IMP defines a number of roles for the CTU that are not consistent with the SOPs, such as impact analysis and GC-wide analysis of risk.

The CTU met twice during CSIII, although the RCMP did not participate in all of the meetings. Apparently this was the result of contention over the role of DND within the CTU. The GC IT IMP lists DND as a "proposed member under discussion"; however, DND is not listed as a member in the SOPs.

Recommendation for improvement:

- *(R19) The CTU SOPs and membership should be routinely (on the order of every two years) reviewed and updated to clarify roles and responsibilities. The expectations outlined in the GC IT IMP should be discussed, and revisions to the CTU SOPs and/or GC IT IMP made accordingly.*

6 Post Exercise

6.1 Exercise Hotwash

Several DRDC analysts attended the PSC NED exercise hotwash and reported back to the entire team. The hotwash was an opportunity for departments to report on key observations from their experience during CSIII.

6.2 DRDC Team Debrief

A DRDC team debrief was held the week following the exercise. A summary of the discussion is provided in Annex D. The team debrief is important in order to get feedback on what worked and what could have been done better from the analysts' perspective. Many of the issues have been identified in this document, along with recommendations for improvement.

6.3 Client Reports and Briefings

The reports produced for each operations centre differed. It was left to each team to decide on the structure and content of their report(s).

The DRDC support team to the RCMP submitted their comments to the RCMP evaluation team before the end of the exercise, which became a part of the RCMP report. The RCMP report was not shared with the DRDC analysis team.

Two Protected B DRDC letter reports were produced for the PSC Operations Directorate. An initial report was delivered within two weeks of the exercise followed by final report draft two months later[11]. The differences between the reports were fairly substantial since the latter included more detail of the findings presented in the initial report, an analysis of response plans and SOPs, and survey results. A briefing for the Director General (DG) of the PSC Operations Directorate was scheduled and the delivery of the final report was intended to occur after receiving feedback during the briefing. However, after several postponements the briefing did not occur. However, the DG held a meeting within the directorate to discuss the recommendations from the report and plan a way forward.

The CFNOC team produced one Protected B DRDC letter report, initially in draft form for comment. Communication challenges within the team resulted in a delay in the production of the draft report and there was a delay in delivering the final version to the CFNOC due to several unsuccessful attempts to obtain feedback from the commanding officer (CO). At the end of the exercise, the CO expressed a high interested in the DRDC findings during an informal discussion with the team lead and had discussed using them in a briefing note to his superiors. The CFNOC team lead offered to provide a later briefing to the CO; however, a formal briefing on the analysis results did not occur.

[11] Note that the reports were delivered by hand given the lack of a common Protected B network on which to share them.

The experience with both the PSC Operations Directorate and CFNOC demonstrate the importance of delivering reports and briefings to the clients soon after the exercise, while issues are at the forefront for commanders. There appears to be a window of opportunity following exercises to get the commander's attention; however, as time moves on, other issues seem to take priority. Delays providing feedback also likely have a negative effect on the reputation of DRDC to deliver promptly, and may affect the relationship between DRDC and the operations centres.

Clients were given ownership of the reports and their distribution, and were told that the reports would have very limited exposure within DRDC. This was based on the model used with client letter eports during the Major Events Coordinated Security Solutions Vancouver 2010 Olympics project. The reports were reviewed within CSS and were not shared with section heads of participating staff without the explicit consent of the client.

Recommendation for improvement:

- *(R20) Teams should work together immediately following the exercise to coordinate observations and report-writing roles (including on the weekend if team members have come from out of town, in which case management must be prepared to pay overtime). This was done for V2010 exercises and proved to be an efficient first step in delivering a timely initial report.*
- *(R21) In order to maximize impact, initial (or "quick-look") client letter reports should be delivered within two weeks of the exercise and team leads must take responsibility for ensuring this by allotting the necessary time following the exercise to dedicate to report writing.*
- *(R22) Team leads should provide an in-person presentation of key observations and recommendations to the commander of the operations centre within two to three weeks of the exercise.*
- *(R23) Client reports should go through the DRP process of the home lab of the lead author. Staff should be able to share their acquired knowledge within their section, in particular with their section heads.*
- *(R24) If DRDC is involved in Cyber Storm IV, former (CSIII) clients should be consulted for approval to distribute the CSIII letter reports among the relevant CSIV support teams.*

6.4 Security-Related Issues

Top Secret Special Access security clearances are required for staff working at the CFNOC. However, for the exercise, the CFNOC agreed to accommodate the supporting DRDC analysts, all of whom had Secret security clearances. This meant that all team members had to be escorted throughout the CFNOC.

Secret security clearances were sufficient for the PSC Operations Directorate and the RCMP NOC.

The PSC Operations Directorate and CFNOC reports were designated as Protected B, therefore had to be encrypted on the DWAN with the public key infrastructure (PKI). However, not all team members had PKI keys, which posed challenges.

Recommendations for improvement:

- *(R25) DRDC analysts with clearances appropriate to the level of the operations centre should be sought.*

  (R26) All analysts should have PKI-enabled DWAN in advance of the exercise. Analysts should arrange for computer/Internet access during the exercise with their respective operations centres.

7 Conclusion

This report outlines the DRDC support effort for Exercise Cyber Storm III. It provides a reference for what was done, challenges encountered and 26 recommendations for improvement for future exercise support. Preparation work began with the buy-in of clients and the creation of teams of analysts from five DRDC centres for CCIRC, the GOC, the CFNOC, and the RCMP NOC. Analysts were educated on the exercise, operations centres, and their roles and responsibilities. During the exercise analysts observed operations centre staff, conducted interviews, and administered surveys. The analysis of this material, combined with previously-provided documentation (plans, etc.), provided the basis for the reports. Letter reports of observations and recommendations were provided to the DG PSC Operations Directorate and the CO CFNOC, and analysts contributed to the RCMP evaluation team report.

While CSIII was a worthwhile endeavour for DRDC, several key recommendations for improvement for future exercise support resulted from our involvement:

- DRDC should engage earlier in order ensure that analysts are adequately prepared and to avoid unnecessary time constraints during preparations;
- Analysts and management must be educated on and committed to fulfilling their roles and responsibilities for exercise support;
- The commanding officers of operations centres should be engaged by DRDC in advance of the exercise to ensure their support;
- In order to have optimal impact, reports and briefings should be provided to clients within two to three weeks following the exercise. It is recommended that analysts meet immediately following the exercise to synthesize their observations for the report.

CSIII represents the first time that the GC IT IMP was exercised on a large scale. This plan is an important step in the preparedness for cyber incident response, but the exercise revealed that the GC IT IMP and other federal plans and SOPs require further development with respect to cyber incidents. Furthermore, the plans require harmonization.

Overall, Exercise Cyber Storm III provided value to DRDC and the operations centres, providing a forum for building strategic relationships, educating analysts and operators, and improving Canada's readiness for responding to major cyber incidents.

8 References

[1] *Cyber Storm III Briefing regarding Chief Information Officer Council (CIOC) Involvement*, PowerPoint Presentation, National Exercise Division, Public Safety Canada, June 23, 2010

[2] *Federal Emergency Response Plan*, Government of Canada, December 2009

[3] *Standard Operating Procedures Cyber Triage Unit*. Revised 13 March 2006

[4] *Government of Canada Information Technology Incident Management Plan*, Government of Canada, 2009

[5] *Cyber Storm III Canadian MSEL v5,* Excel Spreadsheet, Public Safety Canada National Exercise Division (available on the Cyber Storm III portal)

[6] *Canada's Cyber Security Strategy*, Public Safety Canada, ISBN: 978-1-100-16934-7, available from http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx

[7] Major Dave Jones, *Ex Cyber Storm III ReachBack Request 10-25*, Email sent to DRDC lab Deputy Director Generals and Senior Military Officers, Attachment "REACH BACK REQUEST: STAFF CHECK FOR SUPPORT TO EX CYBER STORM III/ PERSONNEL", 3 pages, August 5, 2011

[8] *Incident Report Criteria*, Government Operations Centre, Draft, August 31, 2010

[9] *Emergency Management and National Security Capability Improvement Process*, Cyber Storm II CImP, version 3

[10] *Operations (A) Squadron*, Canadian Forces Network Operations Centre, presentation to DRDC scientists September 2010, 32 pages

[11] Clarke, Sgt D.W., EX Trillium Guardian 12 May 2010 After Action Report (AAR) CFNOC, May 18, 2010, 2 pages

[12] CFNOC After Action Report Op Cadence June 2010, 2 page table

[13] Op Podium – Ex Silver – AAR – Lessons Learned, Excel Spreadsheet, 1 page

[14] Farley, Kelly, Chief Scientist DGMPRA, *Research Misconduct*, presentation to DRDC CSS, April 28, 2011

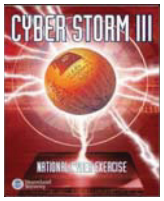
[15] Major Dave Jones, *Cyber Storm III Tasking Order*, Email sent to DRDC lab Deputy Director Generals and Senior Military Officers, Attachment "Tasking Order 04 DRDC Support to Exercise Cyber Storm III, 6 pages, September 9, 2011

[16] Genik, L., Sullivan-Kwantes, W., Beland, P., Lam, Q., Maceda, E., Hendriks, T., *Analysis of the Public Safety Canada Operations Directorate during Exercise Cyber Storm III*, DRDC CSS Letter Report, Protected B, April 2011, 37 pages

[17] Genik, L., Sullivan-Kwantes, W., Beland, P., *Initial Analysis of the Public Safety operations Directorate during Exercise Cyber Storm III* (September 28-30, 2010), DRDC CSS Letter Report, Protected B, October 14, 2010, 8 pages

[18] Perrett, K., Smith, D., Painchaud, F. *EX Cyber Storm III: Analysts' Report on Canadian Forces Network Operations Centre (CFNOC) Operations*, Protected B, November 2010, 7 pages

Annex A PSC NED Participant Feedback Survey



CS III Participant Feedback
September 28 – 30, 2010

Please return the completed questionnaire to the Controller/Evaluator before leaving. All identifying information with the exception of organization is optional.

Name: _____ Telephone: _____

Position: _____ Organization: _____

E-mail: _____

Explanation of Scoring: If you strongly agree with the statement in the Assessment Factor column you would assign a score of 1. If you strongly disagree you would assign a score of 5. Scores 2 and 4 are assigned based on your degree of agreement or disagreement. A score of 3 is assigned if you neither agree nor disagree with the statement.

	Assessment Factor	Strongly Agree				Strongly Disagree	
1.	Sufficient information and training was provided in advance of the exercise regarding the scope of the exercise, administrative arrangements etc.	1	2	3	4	5	NA
2.	The exercise was well structured and organized.	1	2	3	4	5	NA
3.	The exercise scenario was plausible and realistic.	1	2	3	4	5	NA
4.	The pace of the exercise was about right.	1	2	3	4	5	NA
5.	I received sufficient information concerning the scenario to understand the context of the exercise.	1	2	3	4	5	NA
6.	My organization's role during the exercise was clear.	1	2	3	4	5	NA
7.	This exercise allowed my department/agency to practice and improve capabilities.	1	2	3	4	5	NA
8.	After this exercise, I believe my department/agency is better prepared to deal successfully with a cyber event.	1	2	3	4	5	NA
9.	The exercise met my expectations.	1	2	3	4	5	NA
10.	The exercise was a positive experience.	1	2	3	4	5	NA
11.	The exercise scenarios and play provoked realistic responses form my organization.	1	2	3	4	5	NA
12.	Coordination and information sharing between my department/agency and other participants was effective.	1	2	3	4	5	NA
13.	Existing plans, policies and guidelines were understood and	1	2	3	4	5	NA

	Assessment Factor	Strongly Agree					Strongly Disagree
	followed.						

14. What worked well?

15. What areas do you feel could be improved?

16. What were the key lessons learned from the exercise?

17. Are there any specific actions that you would recommend should be taken by your department/agency/organization, or by another department/agency/organization?

18. **Do you have any additional comments?**

Annex B DRDC Survey

Cyber Storm III Survey
September 2010

This questionnaire was designed by DRDC to obtain your feedback with regards to CSIII. While your participation is voluntary, you will be providing valuable input into the functioning of your operations centre. By completing and returning this survey, you are indicating your consent to participate. Your answers will be kept anonymous and only a compilation of everyone's feedback will be provided to your management/leadership. Please answer all questions **as completely as possible, to the best of your knowledge**.

1. What operations centre were you part of?

O	CCIRC	O	GOC	O	CFNOC	O	RCMP TPOF
O	Other – please specify:						

2. Which organization are you from?

O	PSC	O	CF	O	DND Civilian
O	RCMP Regular Member	O	RCMP Civilian Member	O	RCMP Public Servant
O	Other – please specify:				

3. What was your position at your given operations centre during the exercise?

4. Briefly describe the function/role that you had within your operations centre:

5. Please rate your agreement with the following statements as they relate to **your experiences during CSIII**. Please provide additional comments where possible.

Statement	strongly disagree	disagree	neither agree nor disagree	agree	strongly agree	N/A	Comments
a) I have had adequate training for my role (played during the exercise)	O	O	O	O	O	O	
b) My role and responsibilities were clear	O	O	O	O	O	O	
c) My workload was manageable	O	O	O	O	O	O	
d) I had sufficient situational awareness to perform my duties	O	O	O	O	O	O	
e) The Command and Control structure was effective	O	O	O	O	O	O	
f) I was able to work effectively with members of:							

i. other groups/sections in my organization	O	O	O	O	O	O	
ii. other Canadian departments/agencies	O	O	O	O	O	O	
iii. international agencies	O	O	O	O	O	O	

Continued on reverse side

Statement	strongly disagree	disagree	neither agree nor disagree	agree	strongly agree	N/A	Comments
g) Overall, I had access to all tools and equipment required for the execution of my tasks and function(s)	O	O	O	O	O	O	
h) Overall, I am confident that my ops centre fulfilled its roles and responsibilities	O	O	O	O	O	O	
i) The following plans or standard operating procedures were effective:							
i. The Federal Emergency Response Plan (FERP)	O	O	O	O	O	O	
ii. The Government of Canada (GC) Information Technology (IT) Incident Management Plan (IMP)	O	O	O	O	O	O	
iii. The Cyber Triage Unit Standard Operating Procedures	O	O	O	O	O	O	
j) I had the appropriate classified communications means available (networks, phones, faxes, etc.) when I needed them	O	O	O	O	O	O	
k) Senior leadership demonstrated an understanding of cyber issues	O	O	O	O	O	O	

6. Any additional comments, suggestions, or recommendations for improvement?

This is the end of the survey. Thank you very much for your time.

Annex C Exercise Cyber Storm III Ethics Protocol

Revised Protocol #L - 758
June 17, 2010

Revised Protocol: L - 758

Title: Operational Analysis of Exercise Cyber Storm III (CSIII) Command and Control Procedures.

Principal Investigator: Dr. David G. Smith, Human Systems Integration Section, Defence Research and Development Canada - Toronto

Co- Investigators: Lynne Genik, Defence Research and Development Canada - Centre for Security Science (CSS) – Ottawa; Wendy Sullivan-Kwantes, Adversarial Intent Section, Defence Research and Development Canada –Toronto; Dr. Anthony Masys, Defence Research and Development Canada CSS

Thrust Code: 33bd

Executive Summary

Defence Research and Development Canada (DRDC) has been engaged in various research activities aimed at improving command and control (C2), decision making, and collaboration in joint, interagency, multinational, and public (JIMP) environments. Review of the scientific literature, in the above specified context, identified factors that contribute to or act as barriers to successful information sharing as well as individual, organizational, technological and process factors that characterize information sharing. Based on these findings, DRDC Toronto created a customized questionnaire and set of interview questions that aim to describe and assess C2 functions as well as effective information sharing in any specific JIMP setting.

Exercise Cyber Storm III (CSIII), scheduled for 27 - 30 September 2010, is a multi-national cyber exercise involving the United States, Canada, the United Kingdom, Australia, and New Zealand. The exercises were designed to evaluate and ensure that Canada and allied countries are prepared to respond to a significant cyber attack. The agencies involved, including the Department of National Defence (DND), the Royal Canadian Mounted Police (RCMP), Public Safety Canada PSC), and several other organizations will be required to coordinate their efforts in order to respond to significant cyber threat(s).

A customized version of the JIMP questionnaire as well as a set of post-exercise interview questions will be utilized during and after the exercise to capture individual's feedback with regards to response to cyber attacks. The 12 question, 15 minute questionnaire has been combined with additional questions of direct relevance to cyber incidents. The immediate post-exercise interviews will consist of approximately ten questions and take approximately 15 minutes to complete.

Overall, our goals are: 1) to provide Canada and its allies with timely, adaptive, and easy-to-interpret feedback on their operational practices and plans as they affect countering cyber attacks; 2) to make continuous improvement to the questionnaire and interview questions so that they will be a useful re-usable instrument for studying information sharing issues during other major events.

There is minimal risk associated with this protocol.

Revised Protocol #L - 758
June 17, 2010

Revised Protocol: L - 758

Title: Operational Analysis of Exercise Cyber Storm III (CSIII) Command and Control Procedures.

Principal Investigator: Dr. David G. Smith, Human Systems Integration Section, Defence Research and Development Canada - Toronto

Co- Investigators: Lynne Genik, Defence Research and Development Canada - Centre for Security Science (CSS) – Ottawa; Wendy Sullivan-Kwantes, Adversarial Intent Section, Defence Research and Development Canada –Toronto; Anthony Masys, Defence Research and Development Canada CSS

Thrust Code: 33bd

List of Acronyms

CORA	Centre for Operations Research and Analysis
DRDC	Defence Research and Development Canada
CSS	Centre for Security Science
CF	Canadian Forces
JIMP	Joint, Interagency, Multinational, and Public
C2	Command and Control
RCMP	Royal Canadian Mounted Police
DND	Department of National Defence
S & T	Science and Technology
PSC	Public Safety Canada
OGD	Other Government Departments
DHS	Department of Homeland Security
CSIII	Cyber Storm III
NCSD	National Cyber Security Division
GSP	Government Security Policy
DAIP	Directorate of Access to Information and Privacy
IAW	In accordance with

Background

Defence Research and Development Canada (DRDC) has been engaged in various research activities aimed at improving command and control (C2), decision making, and collaboration in joint, interagency, multinational, and public (JIMP) environments. Review of the scientific literature, in the above specified context, identified factors that contribute to or act as barriers to successful information sharing as well as

individual, organizational, technological and process factors that characterize information sharing. Based on these findings, DRDC Toronto created a customized questionnaire and set of interview questions that aim to describe and assess C2 functions as well as effective information sharing in any specific JIMP setting.

Exercise Cyber Storm III (CSIII) is a three day functional exercise sponsored by the United States (U.S) Department of Homeland Security (DHS). It is the third in a series of international multi-national cyber incident consequence management exercises involving the United States, Canada, the United Kingdom, Australia, and New Zealand. Exercise Cyber Storm III (CSIII), scheduled for 27 – 30 September 2010, provides a forum in which federal departments and agencies can validate plans, capabilities and procedures while responding to a significant cyber event(s) affecting the National Interest.

To ensure that Canada and allied countries are prepared to respond to a significant cyber attack, the exercises were designed to gain an understanding of critical cyber security weaknesses and capabilities in the homeland security environment. In this context, cyber attacks can be physical attacks aimed to disrupt critical Infrastructure as well as attacks intended to degrade public confidence in the Federal Government and specific government operations by targeting critical IT infrastructure of specific Federal Government agencies. The agencies involved include the Department of National Defence (DND), the Royal Canadian Mounted Police (RCMP), Public Safety Canada (PSC) and several other organizations. Together they will be required to coordinate their effort, evaluate their techniques and communicate in order to respond to significant cyber threat(s).

DRDC Toronto Investigators will be deployed to provide analytical support to CSIII. Investigators will act as silent observers as well as administer a survey that incorporates elements of our questionnaire to confirm a functional, integrated command and coordination structure with effective information and intelligence sharing in support of the Canadian national security and emergency management framework for the exercise and to examine the processes, procedures, tools and organizational response to a simulated multi-sector coordinated attack through, and on, the global cyber infrastructure.

A customized version of the JIMP questionnaire (Annex B) as well as a set of post-exercise interview questions (Annex C) will be utilized during and after the exercise to capture security personnel's individual feedback with regards to cyber incidence response and their perspective with respect to achievement of exercise objectives. The 12 question, 15 minute questionnaire has been combined with additional questions of direct relevance to cyber incidents. The immediate post-exercise interviews will consist of approximately ten questions and take approximately 15 minutes to complete

Our primary goal is to conduct a preliminary analysis of the questionnaire responses as well as the post-exercise interviews as soon as possible after CSIII. We hope that the insight gained from using these forms of data collection will help to identify the opportunities or requirements that exist for improving information sharing and coordination amongst organizations, and to recommend how such improvements can be made in the future. Our secondary goal is to use the insight gained from CSIII to refine the questionnaire and interview questions for future exercises or operations.

Overall, our goals are: 1) to provide Canada and its allies with timely, adaptive, and easy-to-interpret feedback on their operational practices and plans as they affect countering cyber attacks; 2) to make continuous improvement to the questionnaire and interview questions so that they will be a useful re-usable instrument for studying information sharing issues during other major events;.

Purpose of the Study

The purpose of administering the questionnaire and the immediate post-exercise interviews is to capture security personnel's individual feedback with regards to cyber incidence response, to ensure exercise objectives were achieved and to help determine if there are operational issues or constraints affecting information sharing and the organizations abilities to coordinate their efforts in order to respond to security threats.

Selection of Human Subjects

The team comprising each of the operations Centre's and security personnel will be interviewed. Team members include the DND, the RCMP, DHS, PSC and employees of Other Government Departments (OGDs) and possibly government contractors.

Methodology

Procedure

The questionnaires are specifically designed for each unique operational command centre and will be presented to individuals participating in CSIII. The questionnaire (Annex B) should take approximately 15 minutes to complete and will be administered during and after the exercise. Members within each of the Operational Centre's will be briefed on the purpose of the anonymous questionnaire and will be provided with hard copies to be filled out and returned after their shift. As this is an anonymous questionnaire, subjects will not be required to fill out a Voluntary Consent Form before completing the questionnaire.

In addition to the questionnaire, DRDC Investigators will conduct anonymous post-exercise interviews (Annex C) with key personnel within each location in order to document lessons learned, best practices and establish timelines of events during the exercise. There is minimal risk associated with these interviews and each participant interviewed will be read the below statement regarding confidentiality and verbal consent.

> "The following questions should take approximately 15-20 minutes to answer and were designed to obtain your feedback with regards to incidents that occurred during Exercise Cyber Storm III. Your answers will be kept anonymous and only the compilation of every one's feedback will be provided to exercise planners.
>
> The experimental data concerning you will not be revealed to anyone other than the DRDC Toronto Investigator(s) or external investigators from the sponsoring agency without your consent except as data unidentified as to source. Moreover, should it be required, you agree to allow the experimental data to be reviewed by an internal or external audit committee with the understanding that any summary information resulting from such a review will not identify you personally.
>
> You are free to refuse to participate and may withdraw your consent without prejudice or hard feelings at any time. Do you consent?"

Data Analysis

The data will be analysed by a) ranking responses to questions according to mean response; b) ranking mean deviations between responses to both questionnaires; c) correlation analysis to determine which questions are related to one another; d) data collected from interviews will be analyzed using content analysis.

Medical Screening

The experiments will require no medical screening.

Physician Coverage

The presence of a physician in the experiment room will not be necessary.

Roles and Qualifications of Team Members

The questionnaire will be overseen by DRDC Investigator(s). The interviews will be administered by DRDC Investigator(s) deployed to the operational centres. All of the data collected will then be analyzed during an intensive post-exercise session by the investigators identified in this protocol.

Withholding of Information

There will be minimal withholding of information in that participants will receive an information sheet (Annex A). The information sheet will allow us to keep with the allotted time of 15 minutes for the completion of the questionnaire and 15 minutes for the post-exercise interviews. A copy of the full protocol will be available to the participants should they choose to read it at a different time.

Confidentiality of Data

Experimental data will be protected under the Government Security Policy (GSP) at the appropriate designation and not be revealed to anyone other than the DRDC Toronto Investigator(s), external investigators from the sponsoring agency or contracted support without the participants' consent except as data unidentified as to source. Electronic experimental data collected will be transcribed and analyzed by DRDC Toronto Investigator(s), while contractor support, with appropriate security clearance, will transcribe and analyze hard copy forms of questionnaires. Participants' names will not be identified or attached in any manner to any publication arising from this study. Moreover, experimental data may be reviewed by an internal or external audit committee with the understanding that any summary information resulting from such a review will not identify me personally.

As a Government Institution, DRDC is committed to protecting participants' personal information. However, under the Access to Information Act, copies of research reports and research data (including the database pertaining to this project) held in Federal government files, may be disclosed. Prior to releasing the requested information, the Directorate of Access to Information and Privacy (DAIP) screens the data in accordance with the Privacy Act in order to ensure that individual identities (including indirect identification due to the collection of unique identifiers such as rank, occupation, and deployment information of military personnel) are not disclosed.

Risks and Benefits

Risks

This is a minimal risk study.

Benefits

Our primary goal is to provide feedback to the exercise planning team as to the effectiveness of their information sharing technologies, communication, coordination and procedures among DHS and other government agencies at the federal, state and local level as well as the public and private sectors in order to help them make improvements. Therefore, the results of the questionnaires and interviews will, likely, directly benefit all of these organizations involved.

The secondary goal of this task is to improve the questionnaire and interview questions so that they can be used to make ongoing recommendations for other major events which will benefit future users of this tool.

Potential Conflicts of Interest

All work related to administering the questionnaire will be done in-house using DRDC personnel. We are aware of no conflicts of interests.

Approximate Time Involvement

This task will require one session of approximately 15 minutes duration to administer the questionnaire and approximately 15 minutes duration to administer immediate post- exercise interviews.

Remuneration

There will be no remuneration for this task as it will be included as part of regular duties.

Annex A Protocol #L - 758 Operational Analysis of Exercise Cyber Storm III (CSIII) Command and Control Procedures – Information Sheet

Background	Defence Research and Development Canada (DRDC) has participated in various research activities aimed at improving command and control (C2), decision making, and collaboration in joint, interagency, multinational, and public (JIMP) environments. Several factors have been identified that contribute to or act as barriers to successful information sharing as well as individual, organizational, technological and process factors that characterize information sharing. DRDC Toronto has thus created a customized questionnaire and set of interview questions that aim to describe and assess command and control (C2) functions and effective information sharing in any specific JIMP setting.
Questionnaire / Survey	The anonymous questionnaire and post-exercise interview questions will be utilized during and after the exercise to capture participants' feedback with regards to cyber incident response. The questionnaires will be presented to individuals participating in CSIII and should take approximately 15 minutes to complete. Exercise participants will be briefed on the purpose of the questionnaire and will be provided with hard copies to be filled out and returned after their shift. DRDC Investigator(s) will also conduct anonymous post-exercise interviews with

	CSIII participants in each location in order to document lessons learned, best practices and establish timelines of events during the exercise.
Your Rights as a Participant	Your participation in the questionnaire and interview is completely voluntary. You may ask the DRDC Investigator(s) questions at any time. You may end your participation at any time, and are free to skip any questions that you do not wish to answer. If you do choose to complete the questionnaire and/or interview, we ask that you answer as honestly as possible so that our data accurately reflects your experience and the things that are important to you.
Confidentiality	Experimental data will be protected under the Government Security Policy (GSP) at the appropriate designation and not be revealed to anyone other than the DRDC Investigator(s), external investigators from the sponsoring agency or contracted support without the participants' consent except as data unidentified as to source. Electronic experimental data collected will be transcribed and analyzed by DRDC Investigator(s), while contractor support, with appropriate security clearance, will transcribe and analyze hard copy forms of questionnaires. Participants' names will not be identified or attached to any publication arising from this study. Moreover, experimental data may be reviewed by an internal or external audit committee with the understanding that any summary information resulting from such a review will not identify me personally. As a Government Institution, DRDC is committed to protecting participants' personal information. However, under the Access to Information Act, copies of research reports and research data (including the database pertaining to this project) held in Federal government files, may be disclosed. Prior to releasing the requested information, the Directorate of Access to Information and Privacy (DAIP) screens the data in accordance with the Privacy Act to ensure that individual identities (including indirect identification due to the collection of unique identifiers such as rank, occupation, and deployment information of military personnel) are not disclosed.
Benefits / Risks	There is minimal risk associated with these questionnaires and interviews. There are two goals; 1) to provide feedback to the exercise planning team as to the effectiveness of their information sharing technologies, communication, coordination and procedures among DHS and other government agencies at the federal, state and local level as well as the public and private sectors in order to help them make improvements, 2) to use the insight gained from this exercise to refine the questionnaire and interview questions for future exercises or operations.
Contact Information	Dr. David Smith Tel: (416) 635-2198 Email: david.smith@drdc-rddc.gc.ca DWAN: DAVID.SMITH15@forces.gc.ca You may also contact the Chair, HREC at DRDC Toronto Dr. Jack Landolt Tel: (416) 635-2120 CSN 7-0-634-2120 Email: jack.landolt@drdc-rddc.gc.ca

Annex B: Post Exercise Survey - General

Exercise Cyber Storm III (CSIII) - September 2010 - OVERALL ASSESSMENT QUESTIONNAIRE

This questionnaire was designed by the Knowledge Transfer Team to obtain your feedback with regards to cyber incidence response for Exercise Cyber Storm III. While your participation is voluntary, you will be providing valuable input into the planning of future events. By completing and returning this survey, you are indicating your consent to participate. Your answers will be kept anonymous and only a compilation of everyone's feedback will be provided to the Exercise planners. Please answer all questions **as completely as possible, to the best of your knowledge**.

1. Please rate your agreement with the following statements as they relate to **your experiences at Exercise Cyber Storm III (CSIII).** Please provide additional comments where possible.

	strongly disagree	disagree	neither agree nor disagree	agree	strongly agree	Comments
a. From my perspective, CSIII was successful	O	O	O	O	O	
b. From the security perspective, the event was well organized	O	O	O	O	O	Please explain:
c. From the administrative perspective, the event was well organized	O	O	O	O	O	Please explain:
d. My personal needs (transport, meals, accommodation, etc.) were adequately taken care of	O	O	O	O	O	
f. The training I received was adequate	O	O	O	O	O	
g. My role and responsibilities were clear	O	O	O	O	O	
h. The Command and Control structure was effective	O	O	O	O	O	
i. I was able to work effectively with members of other agencies, when necessary	O	O	O	O	O	
j. Overall, I am confident the Operational Centres fulfilled their roles and responsibilities	O	O	O	O	O	
k. Overall, I had access to all tools and equipment required for the execution of my tasks and function(s)	O	O	O	O	O	
l. Information sharing was adequate	O	O	O	O	O	

m. Shared situational awareness was achieved	O	O	O	O	O	
n. CONPLANS/MOUs/ GUIDING DOCUMENTS were readily available	O	O	O	O	O	
o. CONPLANS/MOUs/ GUIDING DOCUMENTS were effective	O	O	O	O	O	

2. Was your location required to respond to any incidents/events? yes O no O

If yes, please briefly describe each incident:

3. What have been the benefits and the challenges of the different agencies/organizations working together for this Exercise?

Benefits:	**Challenges:**

4. What things might improve future interagency collaboration?

5. Are there examples of collaboration between the different agencies that could be used as a model for similar operations? yes O no O

Please explain:

6. What worked and did not work during CSIII?

What worked:	What didn't work and suggested remedies:

7. Which Command Centre or Venue did you participate from?

O CCIRC O NOC O _____

O CFNOC O ??? ??? O Other – please specify: _____

O GOC O ???

8. Which organization are you from:

O RCMP O DND O Other – please specify: _____

O PSC

9. What was your position title at your given Operational Centre or Venue:

10. Have you participated in other major events or exercises? yes O no O
()

If yes, please note which ones:

11. Briefly describe the function/role that you or your group have within your Operational Centre or Venue:

12. Any additional comments?

This is the end of the survey. Thank you very much for your time.

Annex D DRDC Team Debrief Notes

DRDC CS III Debrief

Tue 5 Oct 2010 (13:00-14:30)

Attending: Lynne, Ian, Kathy, Simona, Paul (phone), Fred (phone), Wendy (phone)

The goal of the meeting was to discuss our experiences during CS III: what worked well, and what could be improved for next time. This document is structured to roughly follow the timeline of the discussion.

Kathy felt that there were communication issues with the CFNOC exercise controllers that resulted in some confusion about the role of the DRDC evaluators with respect to exercise paperwork. Specifically, 50+ emails were sent to Kathy's DREnet account (to which she had no access during the exercise) that requested the end of day evaluation forms, input information for the HotWash report, etc. Most of the emails tracked the status of the CFNOC injects, information that would have been useful to have during the exercise. A future recommendation is that the DRDC evaluators meet with the operations centre Trusted Agents in advance to plan the sharing of information and establish a clear division of exercise duties. The evaluation team lead (Dave) should have been the primary point of contact, but this was apparently not clear to those at the white cell. Lynne agreed that there was some confusion with the communication with offsite controllers, noting that previous exercises have included onsite controllers.

On the topic of communication, Ian stated that the chat functionality was not working at RCMP (at least not initially). Paul was able to use chat at the GOC, and noted that the website had been updated with inject information. Ian indicated that some media person had the Canadian Post website up constantly at the RCMP. Those at CFNOC did not visit the Canadian Post website during the exercise. Paul found that being on the email distribution list was useful, as it helped to put events in context, yet a lot of emails went through the GOC. Lynne has received SITREPs and CyberFlashes, so she can go back and sort through those. Kathy has the inject emails for CFNOC and can forward these to her team members if desired.

Simona summarized her experiences with the Observer Program on the Tuesday of the exercise: Denis presented an overview before 9am and they were ushered into the MCSC to watch the controllers. The exercise website and information about the injects were available on the big screens. Simona described the atmosphere as "peaceful".

It was agreed that the individual player interviews were very helpful. Wendy stated that she managed to get most of the interviews she wanted. It was found that trying to interview people during the exercise was difficult or impossible in most cases, since the players were so busy.

It was observed that people from CCIRC were rarely seen at the GOC during the exercise. Wendy noted that if this had been a real event, they may have had more of a presence. Some of the evaluators found it difficult to position themselves without knowing in advance how the operations centres would organize themselves.

Lynne inquired about any difficulties experienced by the out-of-town travellers with regards to having opportunities for advanced visits. Fred indicated this was not really a problem for him, and that the conference calls seemed to work well.

Wendy regretted not having extra time at the end of the exercise, since she could not make it to the HotWash and debrief afterwards. Lynne had returned to PSC on the Friday and Monday after the exercise to continue with interviews. It was agreed that a buffer time for an after-exercise wrap-up would be helpful.

Wendy and Paul determined that it was useful having two people at the GOC so that they could split up. Lynne found that the physical set-up with cubicles and space limitations at CCIRC would present challenges in having more than one evaluator present. Kathy indicated that there was some difficulty with splitting up the team at CFNOC due to the need to be escorted everywhere (even to the washroom); having the appropriate security clearance would be helpful in future exercises.

There was some discussion about participation in future exercises. Lynne indicated there was interest in leveraging DRDC's experience with CS III for future exercise support at PSC. Dave is looking at a way to establish a pool of people at DRDC Toronto who can provide a "sustainable capability" in this area. There are also ongoing discussions at CSS as to how to provide this capability.

Wendy warned us that it can be challenging to find time to complete data analysis and write reports, in particular since everyone disperses after the exercise and must return to their other responsibilities. The example of the ongoing G8/G20 interviews was given. Lynne pointed out that our level of involvement depends mostly on our involvement in the exercise, i.e., Ian and Tony are mostly done, whereas Wendy and Lynne have to begin writing.

There was some confusion with the surveys. One problem was that the opinion scales (Agree/Disagree) ran in opposite directions in the DRDC survey compared with the Participant Feedback survey. Lynne felt that we did not distinguish enough between the two surveys. There was also some uncertainty about anonymity requirements for the exercise feedback form: Lynne had a discussion with Bill Casey and decided that, given the potential lack of clarity on ownership of the two surveys, names would be blocked before they were sent to Public Safety NED. Kathy noted that the CFNOC Participant Feedback forms have not been sent to PS yet, and Mark Renneberg should be contacted to ask where to send them (DRDC should keep a copy). Lynne recommends that, unless it was absolutely clear that CFNOC staff were putting their names of surveys to go to PS, that the names be stripped before sharing them with Mark or PSC.

The DRDC evaluation lead for each operations centre must now take the lead for writing a report, creating a presentation, and briefing the commander. Coordinating the sharing of notes was discussed among each group: Paul had sent his notes to Wendy; Lynne and Wendy were sharing their results with each other; Kathy had sent her notes via the DWAN to Fred and Dave, and Dave will be preparing an outline of the report this week. It appears that the RCMP evaluators are taking the lead on their own report. Groups should communicate internally to coordinate the completion of the reports. It is likely that they will be classified at the Protected B level, so assume this to be the case.

Ian asked if it would be beneficial to do surveys by email next time. Based on their previous experience, Lynne and Wendy did not think this would work well.

Ian raised the point that the Evaluation Objectives were too broad and vague, and that it would be helpful to see more specific questions (e.g., testing the implementation of Policy X). This would likely require more lead-in time before the exercise. According to Lynne, influencing the CyberStorm evaluation objectives would require getting involved with the National Evaluation planning team. However, this was deemed inadvisable for CSIII by CSS management, so our goal instead was to take the approach of evaluating the operations centre itself. To assist with exercise planning would require getting on the Exercise Development Team early on.

Lynne also pointed out that we had reviewed the CAIP on the Monday prior to the exercise to see what issues we should look for (Ian was at the RCMP operations centre and was not present for that meeting). The usefulness of gearing our assessments on specific factors like these also assumes that the operations centre works well to begin with; during an exercise, bigger issues can come to the forefront that may have been previously unknown (or hidden).

Kathy suggested that the next round of evaluators for CS IV (if not us) could potentially gain access to our final reports and use those for follow-up evaluation. It was pointed out that there is some risk that our reports could be "shelved" and not used. Kathy mused aloud that this should not be permitted, and that government departments should have a responsibility to the public to ensure their operations centres are open to evaluation and respond to the need for improvement.

Ian requested that, in future, evaluators be given exercise accounts on the department/agency systems and collect emails. This has the risk of creating a lot of email noise (Kathy pointed out hearing that there were 3000 exercise-related emails in the accounts of some the cells at CFNOC).

For the reports, we need to identify the broad problems and indicate where the issues lie: e.g., communication, briefing structure, definition of roles and responsibilities. Keep in mind that sometimes we must "soften the message" to avoid alienating the client. If possible, please provide a list including observation, consequences, and recommendations for improvement.

Action item: Please report to Lynne by email to advise her of an estimate on how much time you spent on CSIII, and whether you found your CS III participation to be useful. There needs to be a clear message to management to apprise them of how much time is required in supporting such an exercise: this includes the time spent on advanced preparation (including meetings) and that required afterwards for writing reports. Lynne would like to obtain this information from each evaluator: e.g., how many hours/days per week did you spend on CS III? If you have additional comments that you do not want to share with the group, please also bring these to Lynne's attention.

Although our participation with the RCMP may have not worked out as planned, PSC and CFNOC did appreciate our efforts.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

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.)

   Centre for Security Science
   Defence R&D Canada
   222 Nepean St. 11th Floor
   Ottawa, ON Canada K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

   UNCLASSIFIED

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.)

   DRDC Support to Exercise Cyber Storm III

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

   Genik, L.

5. DATE OF PUBLICATION (Month and year of publication of document.)

   October 2011

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

   58

6b. NO. OF REFS (Total cited in document.)

   18

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.)

   Technical Memorandum

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

   Centre for Security Science
   Defence R&D Canada
   222 Nepean St. 11th Floor
   Ottawa, ON Canada K1A 0K2

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.)

   31XC

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.)

   DRDC CSS TM 2011-24

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

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.)

This paper presents an overview of the DRDC command and control (C2) analysis support for Exercise Cyber Storm III, held in September 2010. It documents what was done, who was involved, challenges encountered, recommendations for improvement, and an indication of the overall effort required. After obtaining client support, DRDC teams were created for Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC), Government Operations Centre (GOC), the Canadian Forces Network Operations Centre (CFNOC), and the Royal Canadian Mounted Police (RCMP) National Operations Centre (NOC). Analysts prepared for the exercise by becoming familiar with exercise documentation and attending pre-exercise training and meetings. During the exercise, teams of one to three analysts observed exercise play at each operations centre, interviewed staff, and administered surveys. Following the exercise, DRDC letter reports synthesising information were delivered to clients. Key recommendations that result from providing C2 analysis for CSIII include: (1) for future exercises, DRDC should engage earlier to have ample time for preparation; (2) analysts and management must be educated on, and agree to, the commitment required to deliver this type of analysis; (3) the commanding officer of each operations centre should be engaged by DRDC prior to the exercise; (4) DRDC should deliver reports and briefings to clients within two to three weeks of the exercise for optimal impact; and (5) federal response plans related to cyber incidents are underdeveloped and require revision and harmonization. Despite several challenges, CSIII proved to be a worthwhile endeavour for both DRDC and the operations centres, helping to build strategic relationships and improve Canada's readiness for responding to major cyber incidents.

Le présent document offre un aperçu du soutien analytique du commandement et contrôle (C2) fourni par RDDC lors de l'exercice *Cyber Storm III* qui s'est déroulé en septembre 2010. Il décrit ce qui s'est produit, qui était impliqué, les obstacles rencontrés, il fait des recommandations visant à améliorer l'exercice et donne une idée de l'effort global à effectuer pour y arriver. Après avoir obtenu le soutien du client, des équipes de RDDC ont été mises sur pied pour chacun des différents organismes : le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada, le Centre des opérations du gouvernement (COG), le Centre d'opérations des réseaux des Forces canadiennes (CORFC) et le Centre national des opérations (CNO) de la Gendarmerie royale du Canada (GRC). Les analystes se sont préparés à l'exercice en prenant connaissance des documents relatifs à l'exercice et en participant à des réunions et à de l'instruction préalable à l'exercice. Des équipes d'un à trois analystes étaient présentes dans chaque centre d'opérations lors du déroulement de l'exercice afin d'y faire des observations. Elles ont rencontré en entrevue des membres du personnel et effectué des sondages. Après l'exercice, des rapports sous forme de lettre de RDDC ont résumé les renseignements livrés aux clients. L'analyse du C2 lors de l'exercice CSIII comprenait notamment les recommandations clés suivantes : (1) lors de prochains exercices, RDDC devrait être engagée plus tôt afin d'avoir suffisamment de temps pour se préparer; (2) les analystes et les gestionnaires doivent être informés et convenir de l'engagement nécessaire pour réaliser ce genre d'analyse; (3) RDDC doit prendre contact avec les commandants de chaque centre d'opérations avant la tenue de l'exercice; (4) afin que les rapports et les briefings aient un effet optimal, RDDC doit les livrer aux clients dans un délai de deux à trois semaines après l'exercice; (5) les plans d'intervention fédéraux liés aux incidents cybernétiques sont insuffisamment développés et ont besoin d'être révisés et harmonisés. Malgré plusieurs défis à relever, l'exercice CSIII s'est révélé être une activité utile, à la

fois pour RDDC et les centres d'opérations. Elle permet d'établir des relations stratégiques et d'améliorer l'état de préparation du Canada et ainsi pouvoir réagir aux incidents cybernétiques majeurs

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS

Exercise Cyber Storm III (CSIII); support to exercises; cyber security; cyber readiness; cyber incident; Public Safety Canada (PSC); Government Operations Centre (GOC); Canadian Cyber Incident Response Centre (CCIRC); Canadian Forces Network Operations Centre (CFNOC); Royal Canadian Mounted Police (RCMP) National Operations Centre (NOC); Federal Emergency Response Plan (FERP); Government of Canada Information Technology Incident Management Plan (GC IT IMP); Cyber Triage Unit Standard Operating Procedures (CTU SOP)