



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada

Cyber C2 governance wargame methodologies

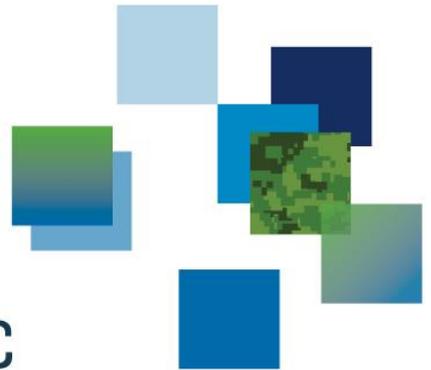
Patricia Moorhead

Melanie Bernier

Centre for Operational Research and Analysis

21st ICCRTS

6-8 September 2016



DRDC | RDDC

Canada 

Outline

- Background
- Study aims
- High level assessment for cyber C2 structure
- Wargame design
- Wargame evaluation
- Lessons observed

Background

- The Canadian Armed Forces (CAF) are adapting to meet challenges that come with operating in cyberspace such as an evolving set of threats, new capabilities, and rapid decision making.
- To ensure agility in the cyber domain, the CAF has established two initiatives:
 1. to adjust the governance structure for cyber force command and control (C2); and
 2. to introduce a new comprehensive operational framework for Defensive Cyber Operations (DCO).
- These initiatives will result in re-alignment of current authorities, responsibilities, and accountabilities (ARAs), the reorganisation and/or the creation of new organisations within the CAF, and new decision making processes.

Study aims

- The CAF identified four options for the C2 structure and three options for a new DCO framework.
- For both sets of options, the CAF wished to assess:
 - ❖ the clarity and simplicity of the associated ARAs;
 - ❖ the degree of unity of command and unity of effort;
 - ❖ the degree of responsiveness, agility, and flexibility;
 - ❖ the effectiveness of integration, deconfliction, and synchronisation of cyber operations;
 - ❖ the ease of interoperability with partners and Allies; and
 - ❖ the implementation effort and scale of investment.
- The options were to be assessed individually, as well as compared/contrasted with each other to determine their relative merits.
- A combination of high level assessment (HLA) and wargaming approaches was used to meet these objectives.
 - ❖ In the case of the C2 structure, a HLA was used to reduce the options from four to the two most viable prior to the wargame.

High level assessment criteria for the C2 structure options

Main Criteria Categories	High Level Analysis Criteria	Description
Clear roles and responsibilities	Chain of command	A clear, hierarchical command structure. Bypassing levels of command in either direction is only justified in exceptional circumstances.
	Unity of command	A single, clearly identified commander will be appointed. This commander has the authority to direct and control the committed resources, and is responsible and accountable for success or failure.
	Organizational coherence	The extent to which the C2 structure components fit with each other and with the external environment.
Balance between expectation and capacity	Implementation effort	The extent to which a change in organizational culture is required and the expected level of resistance to that change.
	Scale of investment	The extent to which additional person-years are needed to support the structure.
Interoperability	Multi-disciplinary approach	The level of collaboration and interoperability with all relevant partners (OGDs, Allies, research/commercial orgs, etc.).
Adaptability	Transformability	The ability to evolve and/or adjust with changes to the strategic environment.
	Agility	The ability to shift cyber resources in response to rapidly changing circumstances. The ability of commanders to make responsive decisions to cyber events and demands.

High level assessment results for the C2 structure options

- A total of 21 questions were developed for the HLA criteria with each question utilising a 5-point Likert-style response scale.
- Subject matter experts scored the options and the raw scores were then converted to ranks with ties allowed.
- The data was analysed using the Multi-criteria Analysis and Ranking Consensus Unified System (MARCUS) which determines a group consensus ranking based on a set of input rankings from multiple assessors and criteria weights.

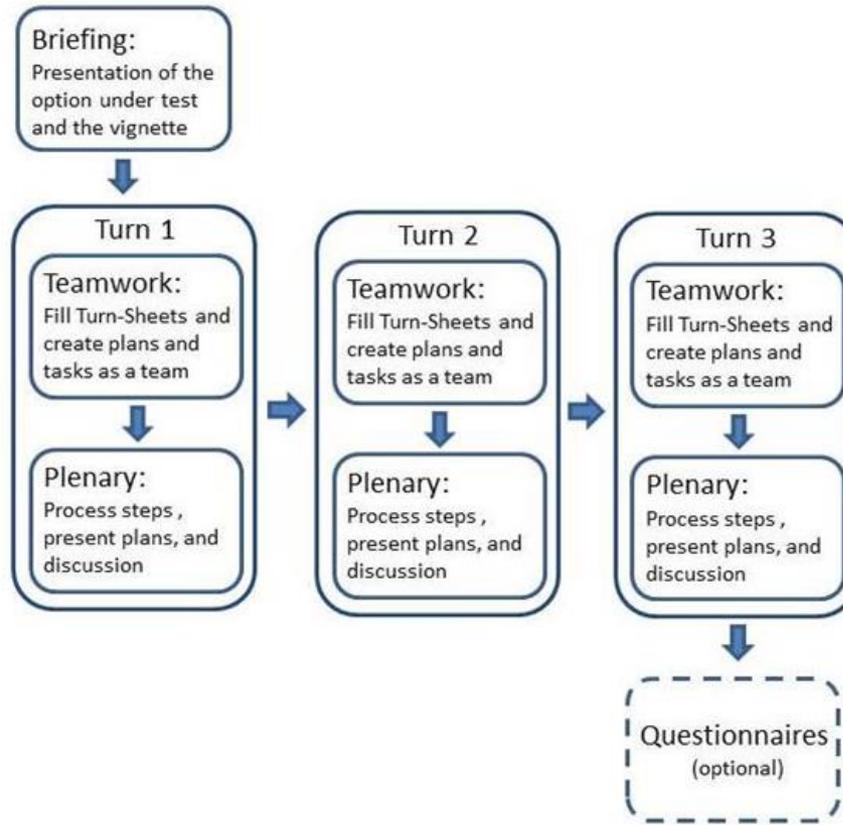
Main Criteria Category	Status quo	Minor change	Moderate change	Major change
Clear roles and responsibilities	4 th	3 rd	1 st	1 st
Interoperability	4 th	3 rd	2 nd	1 st
Adaptability	4 th	3 rd	2 nd	1 st
Balance between expectation and capacity	1 st	2 nd	4 th	3 rd

Wargame design concepts

- The wargame design used a hybrid of two game methodologies: the Concept Development Assessment Game (CDAG) and the Matrix Game.
- The CDAG, developed by NATO ACT and the Netherland's TNO, is a table-top game that focuses on challenge and discussion of conceptual documents, and assesses them within an operational context.
 - ❖ Each run consists of four phases: briefing, teamwork, plenary, and questionnaires.
- The Matrix Game, developed by Australia's DTSG, provides a structured framework to organise discussion and draw out participants' expert knowledge, concentrating on strategic planning issues, interagency interaction, and processes.
 - ❖ Each turn consists of three phases: scenario & injects, team planning, and plenary.

Wargame design hybrid model

- The game design was a hybrid of the CDAG and the Matrix Game where each run of the CDAG had a series of turns within it.



DCO framework game: run matrix and turn sheet

DCO Wargame					
Three Options: Op1 to Op3			Three Vignettes: V1 to V3		
	Day 1	Day 2	Day 3	Day 4	Day 5
AM	Orientation	Run 2: Op1 and V2	Run 4: Op2 and V1	Run 6: Op2 and V3	Run 8: Op3 and V3
PM	Run 1: Op1 and V1	Run 3: Op1 and V3	Run 5: Op2 and V2	Run 7: Op3 and V2	After Action Review

Category	Questions
Tasks	What are your tasks in this situation?
Decisions	What decisions should you/your organisation make? Who needs to be involved in the decision making? What are the DCO C2 relationships (supported/supporting relationships)? Who needs to be aware of the decisions made?
Expected decisions of other teams	What decisions/actions would you expect of other organisations? Who needs to be involved in the decision making? Who needs to be aware of the decisions made?
Desired effects and requirements	What are the desired effects of these decisions? What resources or enablers would be required? What information/communication links would be required?

Cyber C2 structure game: run matrix and turn sheet

Cyber C2 Wargame			
Two Options: Op A and Op B		Six Use Cases: UC1 to UC6	
	Day 1	Day 2	Day 3
AM	Orientation	Run 2: Op A and UC2	Run 7: Op B and UC1
		Run 3: Op A and UC3	Run 8: Op B and UC2
			Run 9: Op B and UC3
			Run 10: Op B and UC4
PM	Run 1: Op A and UC1	Run 4: Op A and UC4	Run 11: Op B and UC5
		Run 5: Op A and UC5	After Action Review
		Run 6: Op A and UC6	

Category	Questions
Force Employment	<p>Provide examples of strategic/operational level FE decisions that need to be made and who should have the ARAs to make them.</p> <p>Do you see any issues/concerns with the proposed Options and ARAs that are relevant to FE in this situation?</p> <p>Do you see any benefits of the proposed Options and ARAs that are relevant to FE in this situation?</p>
Force Generation, Force Development, Force Management, and Human Resources	<p>Based on the FE discussion where do you see the ARAs lying for: FG; FD; FM; and HR?</p> <p>Do you see any issues/concerns with the proposed Options and ARAs that are relevant to FG/FD/FM/HR in this situation?</p> <p>Do you see any benefits of the proposed Options and ARAs that are relevant to FG/FD/FM/HR in this situation?</p>

Data collection & analysis techniques

- A combination of qualitative and quantitative data collection methods was used to capture the participants' data during the wargames. These included:
 - ❖ Observations collected by the defence scientists;
 - ❖ Participants' judgements and insights collected within the turn sheets;
 - ❖ Participants' questionnaires for wargame assessment and option comparison; and
 - ❖ After Action Review conducted by the players at the end of the wargame.
- The technique used consisted of consolidating the data, removing duplicates and then drawing out overarching themes. The themes were used to categorise the data and form a framework in which to organise the recommendations for implementation in development of the operational plans.
- The operational results are not currently releasable. A summary of the option comparison results can be found in the conference paper. We will focus on the wargame evaluation here.

Wargame evaluation

- The focus of the wargame evaluation was to assess how well the game design and its execution enabled/supported the game objectives, and to capture any lessons that can help improve future games.
- The evaluation questionnaire consisted mostly of Likert scale-based questions with some comment-based questions.
- The Likert scale-based questions were analysed based on the observed patterns in the scores, as well as the median and mode scores as measures of central tendency.

Note: As the DCO framework wargame was executed first, the results of this game were used to improve the design of the cyber C2 structure wargame.

Wargame evaluation – qualitative analysis results (1/2)

Theme	DCO game comments	Cyber C2 game comments
Read-ahead package and introductory briefs	<ul style="list-style-type: none"> • Include overarching strategic and policy documents in the read-ahead package. • Include a glossary of cyber terms with specific definitions. • Include fewer details for the scenario background and more details on the vignettes. 	<ul style="list-style-type: none"> • Send the information package on methodology and associated templates ahead of scheduled wargame to participants. • Each organisation should provide their documents that define their ARAs.
Options and Vignettes	<ul style="list-style-type: none"> • More focus can be given to defining touchpoints throughout the decision making process, to clarify roles and expectations. • Include some case studies (e.g. issues handled in the past) to demonstrate why the status quo must change. 	<ul style="list-style-type: none"> • The use cases were far more effective for discussion of FE. They did not include sufficient detail to deal with FG, FD, FM or HR (e.g. use cases framed in experimentation, collective and individual training would help to frame these issues).

Wargame evaluation – qualitative analysis results (2/2)

Theme	DCO game comments	Cyber C2 game comments
Plenary Discussions	<ul style="list-style-type: none"> • The break-out sessions could be better moderated. • Electronic capture of data would be better than pen/paper based. • Focussing the discussion more around the agreed upon criteria would help shape thought processes through all options/vignettes. 	<ul style="list-style-type: none"> • Keep the format, but create a limit (time and number of times) a participant can speak to the group. • A better draft of the ARAs for each option would have been preferred. It was mostly focused on authorities and not enough on responsibilities and accountabilities. Such a document would have offered a better basis for discussions.
Other	<ul style="list-style-type: none"> • All stakeholders could be involved from the beginning of the study, not just at the wargame. • Avoid timings that overlap with summer leave periods and break the wargame into shorter sessions to limit the number of consecutive days away from the office. 	<ul style="list-style-type: none"> • An organisational expert should have attended the wargame.

Wargame evaluation – quantitative analysis (1/2)

Question	Score Count DCO Game						Median Score	Score Count Cyber C2 Game						Median Score
	(0)	(1)	(2)	(3)	(4)	(5)	N=20	(0)	(1)	(2)	(3)	(4)	(5)	N=14
The introductory briefings on the first morning properly prepared you for wargame play.	2	0	0	0	4	14	5	2	0	0	1	4	7	5
You understood the methodology that was applied in the design of this wargame (i.e. the use of plenary discussions and individual data capture).	1	0	0	0	2	17	5	1	0	0	0	8	5	4
The Vignettes/Use Cases used for the wargame covered enough of the breadth of Cyber Operations to meet the game objectives.	3	1	0	1	12	3	4	1	1	0	1	5	6	4
The questions you answered in the turn sheets for each turn captured the right information needed to focus the plenary discussions.	1	0	2	1	7	9	4	1	1	1	1	5	5	4
The wargame design provided a structured way to assess the options.	1	0	0	0	4	15	5	1	0	1	0	7	5	4
You are satisfied that the wargame design used allowed the game's objectives to be met.	0	0	2	0	5	13	5	3	0	0	1	5	5	4
You are satisfied with the overall schedule and how it was executed.	0	0	0	0	6	14	5	1	0	0	1	3	9	5
You are satisfied with the room set up and the facilities used for the wargame.	1	1	2	1	7	8	4	1	0	0	0	2	11	5

- **Overall:** A majority of players had positive game experiences for both games.
- **Vignettes:** The set of vignettes for the DCO game did not sufficiently cover the breadth of DCO; the vignettes for the C2 game were more comprehensive.
- **Turn sheets:** Overall the results are favourable, although a minority saw significant room for improvement.
- **Read-in package:** The lack of a read-in package for the C2 game negatively affected players' assessment of the game design and understanding of the objectives.
- **Facilities:** Use of dedicated wargame facilities versus a conference room is preferred.

Wargame evaluation – quantitative analysis (2/2)

Questions found only in the DCO Game Questionnaire							
Question	Score Count						Median Score
	(0)	(1)	(2)	(3)	(4)	(5)	N=20
The information provided in the read-ahead package was well organized and easy to understand.	1	0	0	0	6	13	5
You have the right expertise to play your assigned role in the wargame.	1	1	1	0	11	6	4
There was enough time allocated to examine and discuss phase 1 for the options.	0	0	1	1	5	13	5
There was enough time allocated to examine and discuss phase 2 for the options.	0	0	1	2	6	11	5
There was enough time allocated to examine and discuss phase 3/4 for the options.	0	0	2	2	4	12	5
In general, there was enough time allocated to play each of the vignettes.	0	0	0	1	4	15	5
Questions found only in the Cyber C2 Game Questionnaire							
Question	Score Count						Median Score
	(0)	(1)	(2)	(3)	(4)	(5)	N=14
The training on the first morning on how to use the electronic data collection system was clear and properly prepared you for wargame play.	2	0	0	0	3	9	5
You are satisfied with electronic data collection system used to support the wargame.	1	0	0	0	2	11	5

- **Expertise:** While some DCO game players felt they did not have the right expertise, all players contributed valuable insights based on their diverse perspectives.
- **Schedule:** The fixed schedule for the DCO game was appropriate. A flexible schedule was used for the C2 game.
- **Facilities:** Use of electronic versus manual paper-based data capture is recommended.

Lessons observed

While overall the wargame design and execution were viewed positively by the game participants, there remains room for improvement. The lessons learned from each of these games will inform design and execution of future CDAGs, Matrix Games, or hybrid games.

- The importance of a read-in package for concept games cannot be understated.
- The individual vignettes have more significance in concept games than the larger overarching scenario.
- The turn sheets need to be brief, to the point, and aligned with player mindsets in order to make the best use of allocated time.
- Even for concept games (vice traditional player versus player games), electronic data capture is ideal.
- There is a lack of a mutually agreed upon lexicon for the cyberspace domain.



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada

DRDC | RDDC

SCIENCE, TECHNOLOGY AND KNOWLEDGE
FOR CANADA'S DEFENCE AND SECURITY

SCIENCE, TECHNOLOGIE ET SAVOIR
POUR LA DÉFENSE ET LA SÉCURITÉ DU CANADA

