National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

A COLLATERAL EFFECTS ESTIMATE PROCESS FOR THE CANADIAN ARMED FORCES

Major Lee R.P. Bellemore

JCSP 46

Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 46

Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

A COLLATERAL EFFECTS ESTIMATE PROCESS FOR THE CANADIAN ARMED FORCES

By Major Lee R.P. Bellemore

Word Count: 5,062

Nombre de mots: 5.062

A COLLATERAL EFFECTS ESTIMATE PROCESS FOR THE CANADIAN ARMED FORCES

Introduction

The nature of warfare has evolved considerably over the last five decades as the implications of exponential development in information technologies have transformed nearly every aspect of global society. Western militaries have invested significantly in information technologies to optimize speed and precision of operations. The Director of Cyber Force Development within the Canadian Armed Forces (CAF) noted that what is "underpinning most of these incredible leaps in capability has been a reliance on cyberspace."[1] Indeed, land, air, maritime, and information operations all rely on cyberspace in order to develop, project, and manage military power. The requirement for holistic, full-spectrum planning is abundantly clear to ensure the most effective use of cyberspace along all lines of effort, regardless of the effect's domain of origin. Yet, the CAF's current joint targeting process does not incorporate the unique considerations necessary to understand targeting within cyberspace, but is anchored around munitions-based operations.

The CAF's Canadian Joint Operations Command (CJOC) has identified challenges in streamlining non-munitions-based planning into full-spectrum targeting. A key challenge faced by CJOC is accurately assessing the potential and consequential effects of non-munitions-based operations. In other words, they lack a functional assessment methodology for full-spectrum targeting. This paper will propose a Collateral Effects Estimate process for further development. In order to understand the requirements of a Canadian Collateral Effects Estimate it will be prudent to establish common

[1] Canada. Department of National Defence. JDN-2017-02 Cyber Operations, p. iii

taxonomy. The current Canadian joint targeting cycle will then be analysed in order to establish areas for development to bolster the assessment of non-munitions-based target sets. Areas in need of development will explored in further detail to determine the key planning considerations necessary to modernize the overall targeting cycle. Following an introduction to existing collateral effects assessment methodologies, this paper will prove that the CAF must adopt a holistic decision support model that includes considerations specific to cyberspace throughout the entire targeting process.

1. Definitions

The taxonomy of non-munitions-based operations is still under heavy debate across military, cyber, and informational communities. Current Canadian doctrine addresses the challenges posed by the lack of common taxonomy and provides multiple definitions from NATO, the *Tallinn Manual*, and the US Department of Defense by way of comparison.[2] The purpose of this paper, however, is not to defend or challenge existing taxonomy. Instead, the aim is to identify and recommend improvements to the Canadian joint targeting cycle as it relates to non-munitions-based targeting. Therefore, the following definitions will be highlighted in the interest of clarity for the discussion that follows:

1.1 'Munitions-' and 'non-munitions-based operations.' The CAF has chosen to use the terms 'munitions-based' and 'non-munitions-based' in place of 'kinetic' and 'non-kinetic' operations to delineate the means and ways of delivering effects from the physical characteristics of the effect itself.[3] Much of the research consulted in this paper uses 'munitions' and 'kinetic' operations interchangeably but readers should consider

[2] Canada. JDN-2017-02, p. 3-7
[3] Canada. Department of National Defence. CFJP 3-9 Joint Targeting (2014), p. V

their use limited to the means and ways an effect is delivered since non-munitions-based operations can still result in physical damage or harm.

1.2 'Damage' and 'Harm.' The *Tallinn Manual* discusses the misleading nature of the terms 'damage' and 'harm' as they apply to cyber operations. They assert that 'damage' also represents the loss of functionality of an object as consequence to cyber influence.[4] CAF doctrine has included this understanding of 'damage' and 'harm' and further asserts that a cyber attack that is successfully intercepted, and does not result in harm, would still be considered a cyber attack given the threat of harm or damage.[5]

1.3 'Unintended/Collateral Effects.' Again, there is not a common definition of collateral effects or unintended effects. The CAF's targeting doctrine defines collateral effects as those "resulting from a specific military action but occurring outside the target boundary."[6] They can result from munitions- and non-munitions-based operations and are usually expressed as second- and third-order effects. This paper will employ the terms 'unintended consequences' and 'collateral effects' more generally to include "overlaps between military, civilian, government, private, and corporate activities on shared networks in cyberspace…."[7]

1.4 'Collateral Effects Estimate.' The collateral effects estimate proposed in this paper refers to a decision support methodology to compliment the existing Canadian joint targeting cycle. It does not replace traditional collateral damage estimation. The commander's *effects assessment* is also a distinct step within the targeting cycle and is not replaced by the collateral effects estimate. The delineation between these steps and

---

[4] Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. 2013, p.110
[5] Canada. JDN-2017-02, p. 2-11
[6] Canada. CFJP 3-9 (2014), p. 1-9
[7] Canada. JDN-2017-02, p. 5-24

the overall collateral effects estimation process is a key focus of this paper and will be discussed in detail.

2. The Canadian Joint Targeting Cycle

The CAF's established joint targeting cycle follows a six-step process that walks an objective from the original intent of a commander to post-execution assessment. This section will analyse the targeting cycle with special consideration to non-munitions-based targeting. It will become apparent that there are three distinct areas for improvement: 1) the target-system analysis, 2) the collateral damage estimate, and 3) the battle damage assessment. Further on, sections will discuss these areas in detail, in order to deliver recommendations.

2.1 – The First Step

The first step of the targeting process identifies the end state, mission, objectives, intent, priorities, and desired effects. Commanders provide their staff with guidance that drives the entire targeting process. This guidance typically includes the considerations of higher operational headquarters, military strategy, and/or national strategy in order to establish the ends, ways, and means available to conduct operations. As an orientation step, the specific considerations required for non-munitions-based weapons do not constitute a departure from those of munitions-base. Therefore, there would be no requirement to modify the first step of the targeting process.

2.2 – The Second Step

The second step, target development and prioritization, involves "the systematic examination of potential target systems […] to determine the necessary type and duration of action that must be exerted on each target and with which priorities, to create the

required effects consistent with the commander's objectives."[8] This step represents the bulk of effort within the targeting cycle and is full of subsequent steps, products, and validating, which will be the focus of this section. Intelligence direction commences the Target Development step, followed by a target-system analysis (TSA) and a targeted-audience analysis (TAA). The TSA identifies the importance of target-system components, elements, and nodes, while the TAA identifies socio-culture and cognitive dynamics of the operational environment, as well as the optimal method of influencing a target.[9] In other words, the combined analysis of the target-system and its associated audiences provides the basis of target identification.[10]

Within the cyber domain, there are unique characteristics of potential target-systems and audiences that require special consideration and articulation to commanders. It is therefore prudent to identify the interdependent nature of cyber and information effects across the spectrum of cyberspace. That is to say, that the relationship between a target-system and targeted-audiences is exponentially more complex than traditional physical relationships between the same entities. This is because of the interconnected and interdependent nature of the cyber target-system and its use by targeted (as well as collateral) audiences. To demonstrate this point, consider an integrated air defense system (IADS) along with its component parts (sensors, shooters, command and control (C2) systems, the operators, their force protection measures, and logistics) as a single target-system. For the purposes of this example, let's select the C2 component of the IADS as the optimal critical vulnerability. In this case, a munitions-based strike on a number of C2 nodes is determined to effectively disrupt the air defence coverage of an area necessary to

[8] Canada. CFJP 3-9 (2014), p. 4-4
[9] *Ibid*, p. 4-5.
[10] *Ibid*.

fulfill a larger military objective. The TAA for this physical strike determines little psychological impact beyond the operators of the IADS. From here, planners would conduct a collateral damage estimate around the C2 nodes considering the size of the target and the characteristics of the chosen munitions. However, a cyber option is also considered to deny the enemy access to their C2 systems, thereby creating the same effect more discretely, leveraging surprise.

The TSA of the IADS from the munitions-based perspective is complete in this example—the interdependencies of the IADS can be exploited by striking the C2 nodes. Consequently, there is considerable information lacking from the non-munitions-based perspective. A more heterogeneous analysis of that system needs to be conducted when considering the component parts of its information-technology (IT) and operational-technology (OT) infrastructure, acquired over multiple generations of military procurement.[11] The connectedness of these systems must be fully understood in order to predict potential cascading or unintended consequences beyond the intent of the target execution. The development of this cyber intelligence requires time and expertise unique to cyber operations. For instance, the software and network used by IADS hardware could be dual use and porous (connected to civilian, neutral, or even friendly systems via the internet, common programming). Herein lie the challenges with the CAF's current doctrine.

J2 (intelligence) personnel craft the TSA with a view to produce a target development nomination (TDN).[12] The operational imperative in the above example was denial or suppression of the IADS. Continuing the above example, the J2 identified the

[11] Max Smeets and JD Work. "Operational Decision-Making for Cyber Operations: In Search of a Model." The Cyber Defense Review. Spring 2020, p. 105
[12] Canada. CFJP 3-9 (2014), p. 4-6

C2 node as a TDN and submits it to the Canadian Forces Intelligence Command (CFINTCOM) for vetting and validation. In order for that target to be validated, it must meet all the objectives outlined by the commander, be legal, and directly contribute to strategic objectives.[13] As a military-built C2 node, the target is easily confirmed to be legal, inline with the commander's intent, and necessary to suppress enemy air defence. CFINTCOM returns the now validated target to planners in the form of the Joint Target List (JTL). J3 targeteers then analyse the JTL to verify that the targets are *technically suitable*.[14] Concurrently, J2 personnel commence target-intelligence production to determine physical and functional characteristics that inform subsequent weaponeering by subject matter experts (SMEs). For kinetic fires, the production of TSA, validation of TDNs, and creation of the JTL does not require input from J3 weaponeers beyond confirming the feasibility of striking the target—something that becomes inherently more obvious to J2 personnel with experience.[15] The dichotomy of effort seen here is effective in this case and supports the fundamental premise of the continental staff system. The cyber domain, however, requires significant analysis beyond the traditional norms of target development to include the integration of spatial, temporal, and force factors that impact intended and unintended consequences of target prosecution.[16] That is to say that the technical completeness of TSA and TAA within a cyber context will factor heavily on the collateral effects of a cyber operation. The risks in failing to account for these specific cyber considerations will be explored in detail during the CD portion of this paper.

---

[13] *Ibid*.
[14] *Ibid*, p. 4-7
[15] Samuel Liles and Jacob Kambic, "Cyber Fratricide," 2014 gth International Conference on Cyber Conflict. P. Brangetto, M. Maybaum, J. Stinissen (Eds.) 2014, NATO CCD COE Publications, Tallinn
[16] Clara Maathuis, et al, "Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations." Milcom 2018 Track 3 – Cyber Security and Trusted Computing, p. 440

Target Development and Prioritization continues with the production of the Target Summary Sheet (TSS) and target lists. The TSS is produced by the J3 (operations) targeting officer and includes summaries of all targets as well as acts as a tracking document to follow where targets are along the process. The TSS is also used as a briefing tool "to enable senior commanders and legal advisers to judge the assessed military advantage of an intended engagement against the potential CD risk."[17] Here there is room for further non-munitions-based integration.

Both *JDN-2017-02 Cyber Operations* and *CFJP 3-9 Joint Targeting* only weigh military *advantage* against CD, without consideration of factors that could produce a military *disadvantage,* other than CD. Yet a significant number of researchers and academics from across the cyber and informational communities highlight the importance of considering how unintended consequences can lead to military disadvantages.[18] Further discussion on military disadvantage will follow in a later section, but it is prudent to note that the completeness of cyber targets on the TSS will be hindered without diligent consideration of adverse affects of cyber events on friendly, enemy, or other neutral third party systems. By extension, the quality of the TSS as a briefing mechanism to articulate cyber related risk to commanders is also questionable. Step 2: Target Development and Prioritization, concludes with the production of the Collateral Damage Estimate (CDE) and its inclusion onto the TSS.

2.3 – The Third Step

---

[17] Canada. CFJP 3.9 (2014), p. 4-7

[18] Clara Maathuis, et al, 2018; Clara Maathuis, et al., "Decision support model for effects estimation and proportionality assessment for targeting in cyber operations," Defence Technology, https://doi.org/10.1016/j.dt.2020.04.007; Natalie Vanatta and Brian David Johnson, "Threatcasting: a framework and process to model future operating environments," Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 2019, Vol. 16(I) 79-88

The third step to the Canadian joint targeting process is Capabilities Analysis. The purpose of this step is to economise the efforts of limited military resources to optimize desired effects, while concurrently minimizing CD.[19] Led by the J3 targeting officer, the step evaluates available capabilities against desired effects, building on Step 2, "to characterize the physical, functional, and behavioural vulnerability of the target as well as to confirm a connection to the [commander's] objectives and guidance."[20] As mentioned above, development of the complete cyber target-system is necessary to determine the risks and rewards to any cyber operation. The time required to achieve such development is dependent on the complexity of the targeted system, the desired effect, and the cyber capabilities available to the commander, consuming significant cyber intelligence resources. This raises concerns of potential friction between cyber planners and J2 staff, given the traditional TSA and TAA conducted by J2 personnel in step 2, versus the J6 SME-driven analysis of the same target-system in step 3.[21]

2.4 – The Fourth and Fifth Steps

The fourth step of the process involves the Commander's Decision and Force Allocation to fuse the capabilities analysis with available assets and engagement options.[22] With a decision made, the step concludes with the production of orders. The fifth step: Mission Planning and Force Execution, includes the targeting process' support to mission planning and execution, and is consistent across munitions- and non-munitions-based targets.[23]

2.5 – The Sixth Step

---

[19] Canada. CFJP 3-9 (2014), p. 4-11
[20] *Ibid*.
[21] Samuel Liles and Jacob Kambic, 2014
[22] Canada. CFJP 3.9 (2014), p. 4-11
[23] *Ibid*, p. 4-12

Assessment of effects realized, constitutes the sixth and final step of the targeting process.[24] Canada's joint targeting doctrine considers Step 6: Assessment as the combination of an effects assessment, a battle damage assessment (BDA), a weapons effectiveness assessment (WEA) and re-attack recommendations.[25] While identifying an effective Collateral Effects Estimate (CEE) is the aim of this paper, this should not be interchanged with the *effects assessment* portion of Step 6. According to Canadian doctrine, effects assessment relates to the requirements of commanders to review the evolving nature, and type of operations, along with the effects required, to achieve the end state.[26] BDA, on the other hand, is "the timely and accurate estimate of the damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective."[27] In other words, BDA is a measurement of effectiveness while the WEA assesses the technical performance and method used of specific weapons system (measurement of performance). For non-munitions-based weapons, the assessment of *damage* becomes problematic, not simply due to physical characteristics of 'damage,' but also due the latency or immediacy of second- and third-order effects produced by cyber and informational weapons. Over time, non-munitions-based operations can manifest inadvertently into second- and third-order effects, which influence enemy, neutral, as well as friendly systems. The spreading effect constitutes a spatial factor over time that needs to be monitored and assessed given the potential severity of adverse consequences or military disadvantages.[28] CAF's *Joint Doctrine Note*

[24] *Ibid.*
[25] Canada. CFJP 3-9 (2014), p. 4-2
[26] *Ibid*, 4-14
[27] *Ibid.*
[28] Clara Maathuis et al., 2018, p. 440

Cyber Operations addresses this gap in fusing non-munitions- and munitions-based BDA, calling for further research and development on the final page.[29]

To conclude the section on the existing targeting process, it is important to note that the CAF's joint targeting cycle provides commanders with decision support in the prosecution of known targets. From the commander's perspective, the process must effectively manage the prioritization of all the effects-assets available to the commander, either munitions- or non-munitions-based. It is therefore prudent to identify weaknesses within the process and make the necessary adjustments to optimize decision-making. Through the examination of the current process there were three distinct points of entry identified to enhance the development and prosecution of non-munitions-based targets: 1) cyber and information driven TSA, 2) non-munitions CDE, and 3) non-munitions BDA. Each of these areas will be explored in further detail.

3 – Enhancing Target-System Analysis

The ongoing discourse around non-munitions-based targeting has been fluid, often debating basic principles such as definitions, scale and scope of unintended effects, and the outright demarcation from kinetic taxonomy. Many within the cyber community argue that the risks from unintended consequences of cyber or informational operations have been exaggerated. According to Bertoli and Marvel, "the non-intuitive and highly complex nature of the cyberspace domain has resulted in an overinflated perception of the risk associated with the employment of cyberspace capabilities."[30] They conclude that

[29] Canada. JDN-2017-02, p. 5-10
[30] Giorgio Bertoli and Lisa Marvel, "Cyberspace Operations Collateral Damage – Reality or Misconception," Cyber Defence Review (Fall 2017): https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1588897/cyberspace-operations-collateral-damage-reality-or-misconception/, p. 61

non-munitions-based weapons can be controlled "in their function and behaviour,"[31] much in the same manner as the explosive yields of munitions. Therefore, they recommend that munitions- and non-munitions-based targeting should follow the same processes. However, as the authors of the *Tallinn Manual* point out, the various modalities of non-munitions-based operations can range from offensive cyber operations (OCO) with destructive effects to influence activities with disruptive effects to policy and international law.[32] The Canadian Armed Forces (CAF) regards the combination of physical and psychological effects as a deliberate and comprehensive planning and targeting effort to ensure that "the effects of physical activities [do not] undermine those of influence activities generated through information operations."[33] While there is always potential to exaggerate second- and third-order effects resulting from non-munitions engagements, the CAF agrees in its doctrine that the unintended consequences of non-munitions-based operations can be vast and risk imposing military disadvantages.

The CAF employs extensive control measures to minimize the risks of friendly fire during operations. Established and refined over time, these measures include procedural, technical, geographical, temporal, and organizational constraints and restraints. However, the same control measures typically do not apply to the cyber domain. For example, geographical boundaries delineate the fires and effects of one force from another, thereby reducing the chance of cross-boundary fires and fratricide. Since physical targets occupy physical space, the fires of one force can be restricted to the

---

[31] *Ibid*, p. 56
[32] Paul A.L. Ducheine, "Non-kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting," in *Targeting: the Challenges of Modern Warfare*, eds. Paul A.L. Ducheine, Michael N. Schmitt, and Frans P.B. Osinga (The Hague: T.M.C. Asser Press, 2016), pp. 204-227
[33] Canada. Department of National Defence, B-GL-300-001/FP-001 *Land Operations* (Ottawa: DND Canada, 2008), pp. 4-24

geographical area surrounding that physical target. Upon prosecution of the target, the first-order kinetic effects are contained inside that area. However, the cyber target-system supporting that same physical target is not automatically contained within the same geographical space. If the physical target's email server, for instance, is assessed as the point of entry for a cyber attack, then the physical location of that server becomes a consideration as does all the connected nodes (enemy, friendly, and neutral). That server may very well be physically located in another area operations, state, and/or jurisdiction. In such a case, that server may be the subject of another operation where its continued functionality may be critical to data extraction, for example. The disruption of that server by the attacking force would thereby jeopardize the overall mission effectiveness of the other operation. This inherent risk to cyber operations has been identified as 'cyber friendly fire,'[34] 'cyber fratricide,'[35] and 'military disadvantage'[36] by various researchers.

Cyber friendly fire is defined as "the intentional offensive or defensive cyber/electronic actions intended to protect cyber systems against enemy forces or to attack enemy cyber systems, which unintentionally harms the mission effectiveness of friendly or neutral forces."[37] Cyber fratricide has been defined as occurring "when agents in one friendly domain negatively impact the actions of agents of another friendly because of the blurry boundaries inherent to cyber conflict."[38] The third term, military disadvantage, is defined "as unintended effects that do not contribute to achieving military objectives and impact allies, friendly, neutral, even the target or conducting

[34] Thomas E. Carroll, Frank L. Greitzer, and Adam D. Roberts, "Security informatics research challenges for mitigating cyber friendly fire." *Security Informatics*, 3:13 (2014): http://www.security-informatics.com/content/3/1/13, p. 2
[35] Samuel Liles and Jacob Kambic, 2014, p. 332
[36] Clara Maathuis et al., 2018, p. 438
[37] Thomas E. Carroll et al., 2014, p. 2
[38] Liles and Kambic, 2014, p. 332

actors."[39] In comparing the three terms, 'military disadvantage' breaks from the confines of cyber operations and is applicable across the entire spectrum of targeting to include munitions-based, influence, informational, and cyber targeting.

The concept of military disadvantage, as defined above, is absent in current Canadian doctrine. Yet, *JDN-2014-02 Cyber Operations* implicitly references the central theme of military disadvantage as it relates to the cyber domain:

> It is entirely possible that cyber operations will have been taking place for some time, possibly years, before conventional forces are deployed. As such, commanders and staff must recognize that these cyber operations may be dependent on infrastructure and networks associated with, or even located within, physical target sets that must be deconflicted and thoroughly understood such that the gain/loss balance can be determined to avoid fratricide.[40]

However, the CAF does not have a methodology or model within the joint targeting process to ensure that commanders and staff recognize the holistic associations of networks and infrastructure. Since target sets are developed during Step 2 of the targeting process, it is here where commanders and staff must make these recognitions.

Maathuis et al. conducted extensive interviews with military commanders and cyber practitioners to determine the information requirements to enable the decision-making processes of non-munitions-based targeting. Firstly, they discovered that a poor understanding of the nature of cyber operations leads to avoidance. Secondly, they discovered that commanders are required to understand risks associated with non-munitions-based operations in terms of spatial, temporal, and force comprehension.[41]

Spatial scale factors relate to the spreading nature of cyber and informational effects. These are not meant to be articulated as second- or third-order effects, but analyse

---

[39] Clara Maathuis et al., 2018, p. 438
[40] Canada. JDN-2014-02, 2014, p. 5-16
[41] Clara Maathuis et al., 2018, p. 440

the national, regional, and global reach of potential non-munitions-based weapons given the network and IT infrastructure of a target, as seen in Table I.[42] Temporal scale factors (Table II) relate to the duration over which effects manifest and take place. While the explosion of munitions and subsequent first-order effects are relatively instant, the return on an influence activity or OCO could occur over periods of time ranging from tenths of a second to several years.[43] Force factors (Table III) represent the severity and probability of unintended consequences and can be assigned measurable metrics.[44] The determination of these factors occurs throughout the targeting process, but begins during TSA.

TABLE I. SPATIAL SCALE FACTORS (SPREADING)

Target (T)	Network of Target (NT)	National (N)	Regional (R)	Global (G)

TABLE II. TEMPORAL SCALE FACTORS (DURATION)

Short Term (ST)	Medium Term (MT)	Long Term (LT)
0 – 1h 1h – 1 day	1 day – 1 week 1 week – 1 month	1 month – 6 months 6 months – 1 year 1 year – 3 years

TABLE III. PROBABILITY

Probability	Value
No (N)	0%
Low (L)	0 – 25%
Moderate (M)	25 – 50%
High (H)	50 – 75%
Very high (VH)	75 – 100%

Source: Maathuis et al. (2018)

Maathuis et al. provide a methodology for determining the spatial, temporal, and force factors. The methodology was developed to be complementary to the American targeting process and can thus be transferred to the Canadian joint targeting cycle. The researchers conclude that target development requires three additional forms of cyber system analysis: 1) system architecture (to include structure, components, functions and

[42] *Ibid.*
[43] *Ibid.*
[44] *Ibid.*

behaviour; and connections, dependencies, and connectivity), 2) hardware architecture, and 3) software architecture.[45] Once the target set has been developed, a specific target effects assessment needs to follow to weigh spatial, temporal, and force factors against military advantage (intended effects adversely affecting the enemy), collateral damage (unintended effects adversely affecting civilian populations), and military disadvantage (unintended effects adversely affecting mission effectiveness), as depicted in Tables IV and V.[46]

TABLE IV. MILITARY ADVANTAGE ON EACH LEVEL OF WARFARE

Battlefield / Level	Strategic	Operational	Tactical
Land / Sea / Air / Space / Cyber			

TABLE V. MILITARY (DIS)ADVANTAGE IN CYBER OPERATIONS

Type	On Target	Duration	Spreading	Severity	Probability

Source: Maathuis et al. (2018)

Step 3: Capabilities Analysis is meant to "maximize the efficiency of forces through application of sufficient force to create the desired effects [military advantage] while minimizing CD, duplication of effort and wasted resources [military disadvantage]."[47] While the development of target sets rests with the J2 staff during Step 2, the weighing of military advantage, collateral damage, and military disadvantage falls to the responsibility of the J3 targeting officer. Consequently, the J3 targeting officer must be enabled by J6 cyber and J3 information operators to weigh the type of military advantage/disadvantage, objects of a target-system, spatial, temporal, and force factors. This is a significant area for development within Canadian doctrine since "military advantage is [currently] assessed by military commanders and their staff based on

[45] *Ibid.*
[46] *Ibid*, pp. 440-442
[47] Canada. CFJP 3-9 (2014), p. 4-11

feeling, background, experience, common sense using the information about the target, without relying on a specific assessment methodology."[48] Moreover, cyberspace is cross-domain and therefore impacts all warfare levels across all other domains, often exceeding the expertise of those determining military advantage. Maathuis et al. provide a methodology for systematically analysing military advantage and disadvantage of cyber operations within a pan-domain context as seen in Tables IV and V. As part of Capabilities Analysis, military advantages must be identified and analysed by J3 operators. The initial assessment of advantages is required prior to determining disadvantages and collateral damage necessary for weighing risk.

4 – Collateral Damage/Effects Estimate

As discussed during the introduction, the taxonomy of 'harm' and 'damage' has been a source of confusion in appropriately determining collateral impacts to civilian populations and property. It is, therefore, prudent to introduce the nascent term 'Collateral Effects Estimate' (CEE) to demarcate the physical metrics of traditional CDE from the considerably more complex process of measuring intended and unintended effects of non-munitions-based weapons. As mentioned above, the spreading risks of cyber and informational weapons necessitate in-depth analysis of the system, hardware, and software architectures of a targeted system. This begins with TSA and TAA, but continues throughout the capabilities analysis, commander's decision, CDE, execution, and assessment phases of the targeting cycle. Given the target development (J2) of an object within a complex-cyber system (J6), and its potential military advantages (Commander) and emerging disadvantages (J3/J6), CDE represent the point of convergence of understanding the full nature or potential of a non-munitions-based strike.

[48] Clara Maathuis et al., 2018, p. 441

Following their interviews and research, Maathuis et al. determined that an effects assessment methodology for Cyber Operations must meet the following requirements:

a) Be structured, adaptable and illustrative;
b) Be compatible, familiar or designed in a similar way as the methodologies used in kinetic Military Operations
c) Consider time, space and force dimension; and
d) Be evaluated on realistic Cyber Operations scenarios.[49]

These requirements are necessary to effectively articulate to commanders with limited technical competence the full range of risks and benefits of complex non-munitions-based operations. However, the CAF does not have a formalized CEE process. The ad hoc doctrine notes are not entirely compatible within the current targeting cycle nor do they consider time, space, force factors. This is representative of the status of formalized CEE across NATO and other liberal democratic militaries.[50] However, the methodology proposed by Maathuis et al. offers the CAF a framework that can be adapted to the current targeting cycle by injecting critical cyber and informational considerations into TSA, TAA, and CEE processes along with the formalization of military advantage and disadvantage analyses. This must include an assessment of the potential efficiency, effectiveness and performance as seen in Table VI. This assessment is not only required to accurately articulate risk to commanders, but can be developed and further used to conduct non-munitions-based BDA after delivery. Once all the variables have been identified and assessed, a formalized CEE can take place (Table VII). Though originally proposed in cognitive terms in 2018, Maathuis et al. have since developed modeling software for their methodology and have tested the CEE process against two realistic

[49] *Ibid*, p. 439
[50] Erwin Orye and Olad M. Maennel. "Recommendations for enhancing the results of cyber effects," NATO CCD COE Publication, Tallinn. 2019.

cyber scenarios.[51] They published their results in the April 2020 issue of *Defence Technology* titled, "Decision support model for effects estimation and proportionality assessment for targeting in cyber operations."

TABLE VI. EFFICIENCY, EFFECTIVENESS AND PERFORMANCE IN CYBER OPERATIONS

Name Indicator	Level Of
Efficiency	Low
Effectiveness	Medium
Performance	High

TABLE VII. COLLATERAL DAMAGE IN CYBER OPERATIONS

Type	On Asset	Duration	Spreading	Severity	Probability

Source: Maathuis et al. (2018)

The software employs 'fuzzy logic' to weigh military advantage against CD and military disadvantage using spatial, temporal, and force factors associated with targeted systems across all levels of warfare and domains. To test the efficacy of the software, they also employed four targeting decision experts to manually conduct CEE. The first test produced a 75% similarity between the software and its human counterparts. The second test resulted in 100% consensus between the system and the experts. The software produces expressions of risk in decimal integers between 0 and 1. In other words, fuzzy logic enables the system to make non-binary determinations of risk given the host of data input from TSA, TAA, military advantage, CD, and military disadvantage. For example, the military advantage to an operation could be assessed as 0.52 with CD at 0.48. The resulting proportionality decision would sit around 0.52. According the decision authorities put in place, that final score determines if an operation is proportional or not.[52] Figure 1 illustrates the sum of fuzzy logic's CEE from one of the two cyber scenarios.

[51] Clara Maathuis et al., 2020, p. 17
[52] *Ibid.*

This system should be tested within a Canadian context to determine the validity of the methodology as it relates to the CAF's joint targeting cycle. Its quantifiable metrics can more readily articulate risk to commanders in a reproducible, predictable, and illustrative manner.

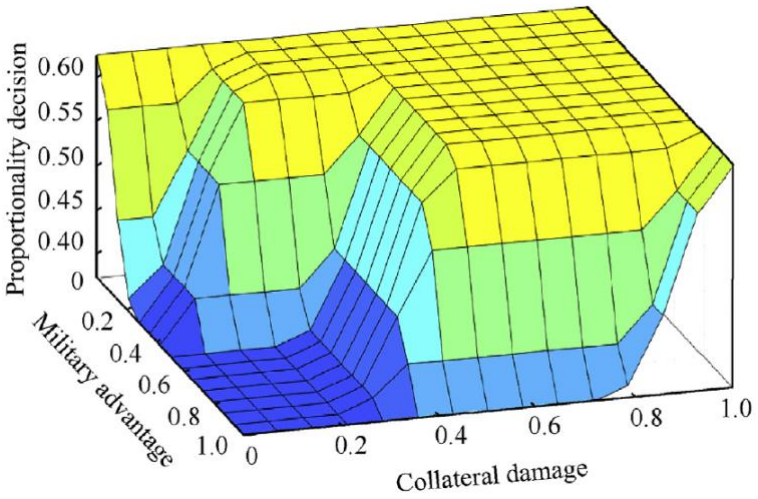

Fig. 1. Targeting decision in cyber operation model entire output surface.
Source: Maathuis et al. (2020)

5 – Battle Damage Assessment

The revelations emerging from the Stuxnet cyber operation have brought the challenges and requirements of non-munitions-based BDA into the spotlight.[53] CAF doctrine highlights that "although traditional assessment of military operations has been in terms of first-order battle damage, ongoing and recent military operations suggest that physical damage is often not the most operationally or strategically important."[54] While the discussion of this paper has been focused on the planning and preparatory requirements of non-munitions-based targeting, the need to be able to accurately measure effectiveness over prolonged timelines cannot be overstated.

[53] David Raymond, et al., "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons," 5th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2013.
[54] Canada. JDN-2017-02, p. 5-10

However, it is also necessary to keep the expression of measurements of effectiveness in terms understandable to commanders and staff.[55] Maathuis et al. suggest that their methodology for conducting CEE can also be used during the post-execution assessment phase.[56] As discussed earlier, the porosity of targeted IT systems can lead to unintended spreading of effects to neutral, friendly, or other enemy assets to include civilian infrastructures. It is therefore necessary to monitor and measure the ongoing spatial, temporal, and force factors following a non-munitions-based strike. Again, the spreading effect is indiscriminate of physical control measures and geography, highlighting the requirement for robust cyber and informational intelligence to continue well after a target has been prosecuted. This can further blur the lines between J2, J3, and J6 responsibilities within the current continental staff system.[57] However, since the proposed CEE methodology necessitates closer fusion between staffs, it is necessary to extend that relationship to the conclusion of the assessment phase. This will enable the continuous analysis of military advantages, CD, and disadvantage when second- and third-order effects begin to manifest across the cyber and informational domains. To that end, it is recommended that the CEE process as described in target development be used as an ongoing assessment tool throughout the entire targeting process.

Conclusion

The theatre of operations has expanded in the cyber and informational domains, bringing about "a radical shift in the nature of the wartime battlefield."[58] The CAF has called upon experts, researchers, and academics to help bridge the gap between the old

---

[55] *Ibid*, p. 5-22
[56] Clara Maathuis et al., 2018, p. 440
[57] Liles and Kambic, 2017, pp. 330-331
[58] N. Solce, "The battlefield of cyberspace: the inevitable new military branch-the cyber force," Alb. LJ Sci. & Tech, no. 18, 2008, p. 293

way of conducting kinetic operations with the emerging trends and considerations of the non-munitions-based domains. To that end, this paper analysed the CAF's targeting cycle and cyber operations doctrine to identify areas for development and modernization. The TSA/TAA, CEE and BDA processes are currently lacking specific considerations for non-munitions-based operations along IT systems and networks. By demarcating the non-munitions-based processes, target development would include cyber and informational intelligence to determine the spatial, temporal, and force factors involved in a target-system. With appropriately developed target sets, the targeting cycle must allow for the formal determination and analysis of military advantages, CD, and disadvantages within cyber and informational contexts.

The decision support model proposed by Maathuis et al. (2020) establishes a structured, illustrative, holistic, and tested digital process for CEE. As discussed, this process can be used for CEE during planning as well as assessing the efficacy of non-munitions-based operations after delivery. The adaption of this methodology will require further examination of the current continental staff system, upon which the targeting cycle is designed. Cyber and informational intelligence is required from the onset of target development and requires closer collaboration between J2, J3, and J6 personnel throughout every step of the targeting cycle. Lastly, the CAF needs to investigate cyber fratricide, cyber friendly fire, and military disadvantage in more depth. Professional military education in these themes is the best opportunity to establish cognitive associations between tactical cyber or informational activities and the potential geopolitical ramifications of influencing misunderstood target-systems.

BIBLIOGRAPHY

Arquilla, John and Ronfeldt, David. "Cyberwar is Coming!" in COMPARATIVE STRATEGY, Vol. 12, No. 2, Spring 1993, pp. 141–165

Bellovin, Steven M., Susan Landau, and Herbert S. Lin. "Limiting the undesired impact of cyber weapons: technical requirements and policy implications" *Journal of Cybersecurity,* 3(I) (2017): 59-88.

Bertoli, Giorgio, and Lisa Marvel, "Cyberspace Operations Collateral Damage – Reality or Misconception," *Cyber Defence Review* (Fall 2017): https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1588897/cyberspace-operations-collateral-damage-reality-or-misconception/

Brose, Robert. "Cyberwar, Netwar, and the Future of Cyberdefense." In 7th International Conference on Cyber Conflict: Architectures in Cyberspace, edited by M. Maybaum, A.M. Osula, and L. Lindström, 25-38. Tallin: NATO CCD COE Publications, 2015.

Canada. Department of National Defence. *CFJP 3-9 Targeting*. 1st Ed. B-GL-005-309/FP-001, 2014.

Canada. Department of National Defence. *Land Operations*. B-GL-300-001/FP-001, 2018.

Canada. Department of National Defence. *JDN 2017-02 Cyber Operations*, Ottawa: Canadian Forces Warfare Centre, 2017, p. 2-1

Carroll, Thomas E., Frank L. Greitzer, and Adam D. Roberts. "Security informatics research challenges for mitigating cyber friendly fire." *Security Informatics*, 3:13 (2014): http://www.security-informatics.com/content/3/1/13

Ducheine, Paul A.L. "Non-kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting," in *Targeting: the Challenges of Modern Warfare*, eds. Paul A.L. Ducheine, Michael N. Schmitt, and Frans P.B. Osinga (The Hague: T.M.C. Asser Press, 2016)

Ducheine, Paul A.L., Michael N. Schmitt, and Frans P.B. Osinga (Eds.). *Targeting: The Challenges of Modern Warfare*. The Hague: T.M.C. Asser Press, 2016.

Fanelli, Robert, and Gregory Conti. "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012.

Kostyuk, Nadiya, Scott Powell, and Matt Skach. "Determinants of the Cyber Escalation Ladder," *Cyber Defence Review* (Spring 2018): https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1588913/determinants-of-the-cyber-escalation-ladder/

Liles, Samuel, and Jacob Kamble. "Cyber Fratricide," 6th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2014.

Maathuis, Clara, Wolf Pieters, and Jan van den Berg. "Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations," MILCOM – IEEE Military Communications Conference, 2018.

Maathuis, Clara, Wolf Pieters, and Jan van den Berg. "Decision support model for effects estimation and proportionality assessment for targeting in cyber operations," Defence Technology, https://doi.org/10.1016/j.dt.2020.04.007;

Markov, J. (2010a). Before the gunfire, cyberattacks. New York Times. Retrieved May 5, 2014, from http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0

NATO. Allied Joint Doctrine for Information Operations. AJP-3.10, 2009.

NATO. Allied Joint Doctrine for Joint Targeting. AJP-3.9, 2008.

Nordquist, Keith B. "The New Matrix of War: Digital Dependence in Contested Environments." Air & Space Power Journal 32, no. 1 (Spring 2018): 109-117.

Orye, Erwin, and Olaf M. Maennel. "Recommendations for Enhancing the Results of Cyber Effects" 11th International Conference on Cyber Conflict, Tallinn: NATO CCD COE Publications, 2019.

Raymond, David, Gregory Conti, Tom Cross, and Robert Fanelli. "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons," 5th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2013.

Romanosky, Sasha, and Zachary Goldman. "Cyber Collateral Damage," *Complex Adaptive Systems*, Pub. 6., Conference Organized by Missouri University of Science and Technology. 2016.

Schmitt, Michael N., *Tallinn Manual 2.0 on the international law applicable to cyber operations.* NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2017.

Smeets, Max, and J.D. Work. "Operational Decision-Making for Cyber Operations: In Search of a Model," *Cyber Defense Review* (Spring 2020): https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-

View/Article/2121687/operational-decision-making-for-cyber-operations-in-search-of-a-model/

Solce, N. “The battlefield of cyberspace: the inevitable new military branch-the cyber force,” Alb. LJ Sci. & Tech, no. 18, 2008, p. 293

Vanatta, Natalie, and Brian David Johnson. “Threatcasting: a framework and process to model future operating environment,” *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* Vol 16(I) (2019): 79-88.

Warf, Barney, and Fekete Emily. “Relational Geographies of Cyberterrorism and Cyberwar.” Space and Polity 20, no. 2 (2016): 152

Weitz, Benjamin. *Updating the Law of Targeting for an Era of Cyberwarfare*, 40 U. Pa. J Int’l L. 735 (2019).