National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

RISK MANAGEMENT IN CAF JOINT TARGETING: TOWARDS ENTERPRISE RISK MANAGEMENT AND RISK GOVERNANCE

Major James Black

JCSP 46

Solo Flight

Disclaimer

PCEMI 46

Solo Flight

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

RISK MANAGEMENT IN CAF JOINT TARGETING: TOWARDS ENTERPRISE RISK MANAGEMENT AND RISK GOVERNANCE

By Major James Black

Word Count: 5,926

Nombre de mots : 5.926

RISK MANAGEMENT IN CAF JOINT TARGETING: TOWARDS ENTERPRISE RISK MANAGEMENT AND RISK GOVERNANCE

INTRODUCTION

This paper explores risk management as part of Canadian Armed Forces (CAF) joint targeting. While mitigation of risk is a stated aim of the CAF joint targeting process, there is little detail provided in terms of how risk is managed throughout the targeting process or across the targeting enterprise.[1] Where risk management is referenced, the doctrine focuses on risk resulting from the targeting process. Such a narrow view of risk foregoes a more comprehensive understanding in terms of how risk is assessed, communicated, and dealt with within the larger targeting enterprise. This creates potential for the misapplication of controls that maltreat complex risk as simple—ultimately undermining the philosophy of mission command, and creating unintended risk to the overall efficacy of targeting and operations. The purpose of this paper, therefore, is to enable the institutional leadership of the targeting enterprise by illuminating how risk is treated within it.

This paper will be structured into four parts. First, the concept of enterprise risk management (ERM) will be introduced and explained. Second, a brief introduction to the joint targeting process and the CAF targeting enterprise will be provided. Third, the CAF targeting enterprise will be evaluated with respect to ERM implementation. Lastly, this paper will conclude by reinforcing its thesis that a simplistic and linear view of risk management should give way to ERM and risk governance in order to ensure the efficacy of the targeting enterprise, and better align the targeting function with the philosophy of mission command. Fortunately, the CAF is well postured to achieve this shift given the ongoing development of the targeting enterprise.

---

[1] Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CJJP) 3-9 Targeting*, 1st Edition (Ottawa: Her Majesty the Queen as represented by the Minister of National Defence, 2014): 1-10.

In terms of scope, and in the interest of consistency and brevity, this paper will focus on deliberate targeting process vice that of dynamic targeting.[2] Such an approach is warranted given similarities between the processes despite differences in taxonomy and timelines. As explained by retired United States Airforce Colonel, Phillip Pratzner Jr., both processes can be reduced to four steps: 1) objectives and guidance; 2) planning; 3) execution; and 4) assessment.[3] He further argues that despite the steps of 'objectives and guidance' and 'planning' being less evident in dynamic targeting, they still equally apply. Specifically, while timelines are abbreviated, and there is increased need for flexibility, dynamic targeting is still driven by pre-established objectives, and is executed through pre-defined processes, largely resulting from deliberate planning related to targeting.[4] Additionally, all targets are engaged dynamically, even when identified and planned for within the deliberate targeting process.[5] Thus, with considerable overlap between the processes, considerations for risk management in deliberate targeting will have implications for dynamic targeting.[6]

---

[2] "*Deliberate targeting* is conducted against targets identified and located during the planning phase of operations, and intended to be prosecuted on either a scheduled or on-call basis. This method best ensures that the desired effects will contribute directly to strategic objectives, while avoiding or minimizing [collateral damage];" "*Dynamic targeting* is conducted against either known or unknown target of opportunity that have not been located during the planning phase of operations. These targets may be unplanned and/or unanticipated. Dynamic targeting is also a planned process but uses an expedited version of deliberate targeting procedures, to execute time-sensitive targets and other targets that need to be prosecuted quickly, due to their potentially fleeting nature, or critical importance." *CFJP 3-9*, 1-6.

[3] Phillip R. Pratzner, "The Current Targeting Process," in *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt and Frans P.B. Osinga (The Hague: T.M.C. Asser Press, 2016): 80.

[4] *Ibid*., 81.

[5] While the CAF treats dynamic and deliberate targeting separately in doctrine, the US acknowledges that the two processes are related in practice. Joint Chiefs of Staff (US), Joint Publication 3-60 Joint Targeting, 13 April 2007, II-13.

[6] While written from a Canadian perspective, given similarities in doctrine between Canada, the US, and NATO, this paper will be of interest to a wider audience than solely Canadian.

INTRODUCTION TO ENTERPRISE RISK MANAGEMENT

ERM as a concept was developed in the mid-1990s, and it saw waves of resurgence following the 9/11 attacks and the global financial crisis in 2008 given pressures to insulate firms from external market factors.[7] In short, ERM is "a systemic and integrated approach to manage all risks that an organization faces."[8] ERM, therefore, differs from specific risk management as the latter treats risk within a narrower context (e.g. financial risk related to a specific project). In a private sector context, ERM endeavors to ensure a company remains profitable given external, internal, or procedural risks. Thus, ERM is focused on managing uncertainty for the whole of an organization in order to maximize benefits from opportunities, while minimizing negative consequences resulting from threats.[9] Moving from a corporate context, concerned with maximizing profitability, the application to targeting is apparent. That is, where risk is fundamentally linked to uncertainty, the targeting process is aimed at managing said uncertainty to achieve objectives while minimizing the negative consequences of targeting activity.[10] Given increased demands for precision and humanity in Western warfare, it is no wonder political scientist, Christopher Coker, argues that targeting has become an exercise in risk management.[11]

---

[7] Yongrok Choi, Xiaoxia Ye, and Lu Zhao, "Optimizing Enterprise Risk Management: A Literature Review and Critical Analysis of the Work of Wu and Olson," *Annals of Operations Research* 237 (2016): 282.

[8] *Ibid.*

[9] *Ibid.*, 282-283.

[10] The linkage between uncertainty and risk is argued in the works of multidisciplinary scholars Marjolein van Asselt and Ortwin Renn, and sociologist Hauke Riesch. Marjolein van Asselt and Ortwin Renn, "Risk Governance," *Journal of Risk Research* 14, no. 4 (April 2011): 431-449; and Hauke Riesch, "Levels of Uncertainty," in *Handbook of Risk Theory*, Volume 2, edited by Sabien Roeser, Rafeaela Hillerbrance, Per Sandin, and Martin Peterson (New York: Springer, 2012): 97-99.

[11] Christopher Coker, "Targeting in Context," in *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt and Frans P.B. Osinga (The Hague: T.M.C. Asser Press, 2016): 9.

With respect to the component parts of ERM, Table 1 shows the leading ERM frameworks and their associated factors. While there are similarities between the frameworks, doctor of business administration, Sara Lundqvist argues, that there is little agreement on what constitutes ERM vice the management of specific risk.[12] According to Lundqvist, it is the third of her factors ('holistic organization of risk management') that serves as the true measure of ERM implementation. The other three of her factors remain relevant as preconditions for ERM, or as indicators of specific risk management, but it is the 'holistic' management of risk across an organization that serves as the defining benchmark of ERM.[13]

Table 1 - ERM Frameworks

COSO Framework (2004)	COSO Framework (2017)	ISO 31000 (2018)	Lundqvist Framework (2014)
• Internal Environment • Objective Setting • Risk Identification • Risk Response • Control Activities • Information and Communication • Monitoring	• Governance and Culture • Strategy and Objective-Setting • Performance • Review and Revision • Information, Communication, and Reporting	• Establish the Context • Communication and Consultation • Risk Assessment • Risk Treatment • Monitor and Review	• General Internal Environment and Objective Setting • General Control Activities and Information and Communication • Holistic Organization of Risk Management • Specific Risk Identification and Risk Assessment Activities

Sources: COSO, "Enterprise Risk Management: Integrating with Strategy and Performance - Executive Summary;" ISO, "ISO 31000 - Risk Management;" and Sara A. Lundqvist, "An Exploratory Study of Enterprise Risk Management: Pillars of ERM."

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework is the most widely adopted framework for ERM implementation; however, many firms have augmented or modified said framework given a lack of clarity

[12] Sara A. Lundqvist, "An Exploratory Study of Enterprise Risk Management: Pillars of ERM," *Journal of Accounting, Auditing & Finance* 29 no. 3 (2014): 394.

[13] Lundqvist, *"*An Exploratory Study of Enterprise Risk Management," 412.

and its "overly theoretical" guidelines.[14] In this tradition, The Treasury Board Secretariat (TBS) *Framework for the Management of Risk*, which applies to all Government of Canada (GC) departments, uses a modified International Organization for Standardization (ISO) 31000 framework. In GC parlance, such an approach is termed Integrated Risk Management (IRM) following the TBS guidelines.[15] A 2013 audit of IRM implementation for Public Safety Canada further elaborates that IRM includes functional integration, vertical integration, and horizontal integration of risk. Functional integration incorporates risk management practices directly into existing functions and decision-making processes. Vertical integration is the management of risk between different levels of hierarchy within an organization. Horizontal integration in concerned with the harmonization of risk management practices across an organization and between branches and programs. Horizontal integration is thus aimed at ensuring a common understanding and approach to risk between sub-organizations "which ultimately enables more informed and robust decision making."[16] In this way, horizontal integration is largely analogous to Lundqvist's 'holistic organization of risk management'.

With consideration for the frameworks discussed above, ERM theory, and more general risk theory, the CAF targeting enterprise will be evaluated in terms of 'holistic' risk management. Particular attention will be paid to barriers to risk identification, assessment, communication, responsibilities, controls, and decision making, all through

---

[14] *Ibid*.

[15] Treasury Board of Canada Secretariat (TBS), "Guide to Integrated Risk Management: A Recommended Approach for Developing a Corporate Risk Profile," Government of Canada, last modified May 12, 2016, https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/guide-integrated-risk-management.html.

[16] Public Safety Canada, "Public Safety Canada Internal Audit of Integrated Risk Management," RDIMS# 893596, September 2013, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dt-ntgrtd-rsk-mngmnt/dt-ntgrtd-rsk-mngmnt-eng.pdf.

the lens of functional, vertical, and horizontal integration. As will be explained, the CAF targeting enterprise is most significantly lagging in terms of horizontal integration due to risk being traditionally managed through vertical and functional integration within the targeting process itself. This lack of holistic risk management reflects the emphasis on specific risk management and a lack of ERM implementation; however, the creation of the CAF targeting enterprise has the potential to address some of these shortcomings. Before expanding on this, a brief introduction to joint targeting is warranted.

INTRODUCTION TO CAF JOINT TARGETING

What is Joint Targeting?

The CAF Joint Targeting doctrine defines targeting as the "process of selecting and prioritizing targets and matching the appropriate response to them, taking into account operational requirements and capabilities."[17] Thus, targeting is first and foremost a process, and this process, broken into the six steps of the joint targeting cycle, is re-produced in Figure 1.

[17] Defence Terminology Bank, record 5514, as quoted in *CFJP 3-9*, 1-1.

Figure 1 -- The Joint Deliberate Targeting Cycle
Source: *CJFP 3-9*, 4-3.

The doctrine goes on to explain that targeting is effects focused, makes use of the most suitable munitions or non-munitions-based means, and is aimed at achieving the desired objectives or end state.[18] From the doctrine, "targeting undertaken by the CAF is a full-spectrum, effects-based, inherently joint, and where necessary, multinational activity, guided by the Government of Canada (GC) aims and priorities."[19] While this paper assumes a basic familiarity with the joint targeting cycle, a more detailed explanation can be found in Annex B.

The joint targeting cycle in Figure 1 reflects a relatively linear (albeit iterative), 'systematic', and rational process, whereby effects are planned and delivered against adversary systems in order to achieve specific objectives.[20] The process can be described as scientific in that it is repeatable, observable, measurable, and largely based on the laws of physics.[21] However, as Pratzner explains, the targeting process is equal parts 'art' in

---

[18] *CFJP 3-9*, 1-1.
[19] *Ibid*.
[20] The CAF joint targeting doctrine lists 'systematic' as one of the key principles of targeting. *Ibid*., 1-5.
[21] Pratzner, "The Current Targeting Process," 88.

that it employs a "cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity and judgement."[22] Targeting tradecraft competencies rely on both the 'art' and 'science', and Pratzner includes these competencies as having a direct influence on the quality of planning related to targeting.[23]

The creation of the CAF targeting enterprise is aimed at professionalizing and institutionalizing targeting to reinforce these competencies, and build on what have been largely *ad-hoc* targeting capabilities on operations. Thus, the following will serve to introduce the CAF targeting enterprise and will further ground the targeting doctrine into more complex realities.

Targeting in the CAF Context

Recent CAF operations, such as *Operation Mobile* and *Operation Impact*, saw the CAF contribute to allied and coalition operations through the application of joint targeting.[24] These recent operations echo the CAF's targeting experience in Afghanistan and Kosovo, and have informed, and in the case of *Operation Impact*, reflected the Chief of Defence Staff's (CDS) renewed emphasis on joint targeting. Within this context, the CAF targeting enterprise was born. The CAF joint targeting doctrine was published in

[22] *Ibid*., 87.
[23] *Ibid*., 82.
[24] In the case of Operation Mobile, in 2011, the CAF conducted joint targeting in Libya in support of the United States' (US) Operation Odyssey Dawn and the North Atlantic Treaty Organization (NATO) Operation Unified Protector. Under Operation Impact, from 2014 to present, the CAF conducted or contributed to joint targeting of Daesh in Iraq and Syria as part of the Coalition-led Operation Inherent Resolve. Government of Canada, "Operation MOBILE," last modified January 22, 2014, https://www.canada.ca/en/department-national-defence/services/operations/military-operations/recently-completed/operation-mobile.html; and Government of Canada, "Operation IMPACT," last modified 10 December, 2018, https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html.

2014, and the Joint Targeting Intelligence Centre (JTIC) was officially unveiled in 2018.[25] These two examples reflect the ongoing work within the CAF to mature its targeting capability.

The stand-up of the JTIC represented an important milestone in institutionalizing and repatriating CAF joint targeting from what was traditionally a deployed and *ad-hoc* capability. As the first Director of the JTIC, Lieutenant-Colonel Kristopher Purdy, explains:

> "Traditionally, we had to deploy to do all this. …The way intelligence was organized in Canada didn't centralize mutually-supportive capabilities required for target discovery and development. For example, you'd have your all-source analysts sitting in one place, your geospatial intelligence folks in another. And they would only come together when deployed. Now we've brought these single-source intelligences together in a single centre in Canada. It's fusion at its finest."[26]

In addition to the JTIC, there has been additional investment by way of the formalization of roles, boards, and processes, such as the Director Strategic Effects and Targeting (DSET) and the Strategic Effects Management Board (SEMB).[27] Such investment also reflects the CDS's stated intent. As part of the press release tied to the unveiling of the JTIC, he offered the following:

> "We [the CAF] need to bring targeting concretely and permanently in the Armed Forces. …It's not just the process of getting effects on a target or an outcome. There's more to it. Militaries around the world, including ours, will abandon current planning processes that are slow, that are counterintuitive, that require too much staff work and have an inefficient link between intelligence and operational doctrine."[28]

---

[25] Dawnieca Palma, "The Joint Targeting Intelligence Centre: Bringing Innovation into Intelligence," *The Maple Leaf*, last modified November 14, 2018, https://ml-fd.caf-fac.ca/en/2018/11/21578.

[26] *Ibid.*

[27] "Director Strategic Effects & Targeting (DSET) is responsible to oversee CAF targeting policies and governance processes to include the CAF Joint Targeting Coordination Board (JTCB), CAF Strategic Targeting Board (STB) and Strategic Effects Management Board (SEMB). The SEMB is the culmination of various Boards-Bureaus-Coordination-Cells-Working Groups (B2C2WG) that is meant to inform the L1s and CDS on future Targeting, Collection & Effects Priorities. The SEMB is held quarterly and is meant to look out 18 months to focus CAF priorities. The CDS is the final authority for SEMB decisions/priority setting." Lieutenant-colonel Germain Poirier, E-mail to the author, April 23, 2020.

[28] Palma, "The Joint Targeting Intelligence Centre."

The CDS's comments reflect the growing allure of joint targeting. Given the 'fiendishly complex' nature of the modern battlefield, and a 'philosophy' of effects-based-operations, targeting, with its focus on consequence management, has a particular appeal.[29] Likewise, its full-spectrum nature, its iterative and responsive cycle, and its integration of operations and intelligence, all aimed at achieving operational and strategic objectives, makes it well suited for the contemporary operating environment characterized as increasingly volatile, uncertain, complex, and ambiguous.[30]

While disciples of joint targeting are quick to profess its virtues of flexibility, timeliness, and operational relevancy, it is not without its challenges—foremost are challenges of complexity. Figure 2, reproduced from the US Joint Targeting School Student Guide, shows the dizzying array of organizations involved in joint targeting for a theatre of operations. While it is provided here for demonstrative purposes, the *complicated* hierarchy shown does not represent the truly *complex* way in which these organization interact on a functional basis.

---

[29] Coker, "Targeting in Context," 19.

[30] A full-spectrum approach to targeting incorporates an integrated application of munitions and non-munitions-based capabilities to achieve desired effects and objectives, *CFJP 3-9*, *op. cit.*, 3-1. The linkage between targeting and managing risk is alluded to when linking counter-terrorism efforts with risk reduction strategies in several texts. See Yee-Kuang Heng and Kenneth McDonagh, *Risk, Global Governance and Security: The Other War on Terror* (New York: Routledge, 2009); and Louise Amoore and Merieke de Goede (eds.), *Risk and the War on Terror* (New York: Routledge, 2008).

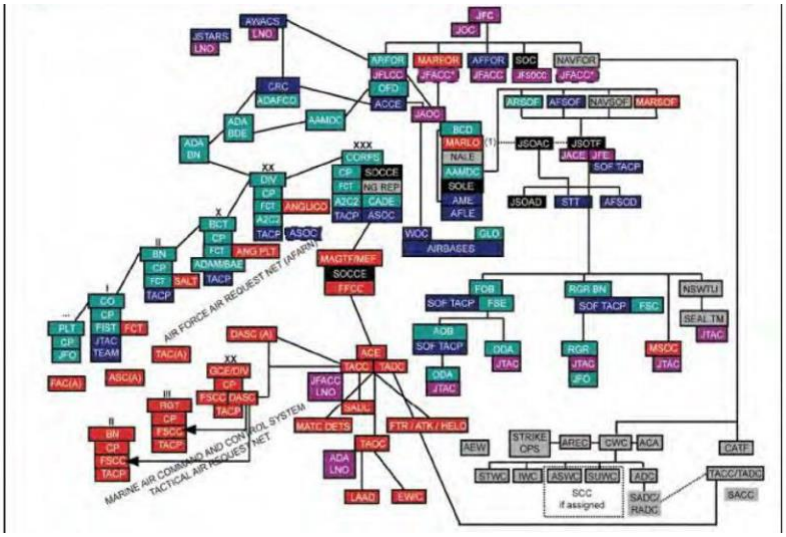


Figure 2 -- Theatre Air Ground System
Source: Joint Targeting School (US), *Joint Targeting School Student Guide* (Dam Neck, Virginia: 1 Mar 2017): 206.

Likewise, although the joint targeting cycle is explained in doctrine as a relatively linear process, Appendix 1 to Annex B shows a more detailed process flow chart with its associated sub-processes, management boards, working groups, and inputs and outputs. While seemingly more *complicated* than the cycle represented in Figure 1, it still does not truly represent the *complexity* of the system when one considers other stakeholders (such as inter-agency partners, allies, and other partner nations), tangential and concurrent national and coalition process, the complexity of adversary target systems within a complex operating environment, and the non-linear fashion in which the cycle occurs in practice. With respect to this last statement, the aforementioned student guide actually shows the assessment step as spanning all five of the other steps of the targeting cycle given the ubiquitous and constant nature of the feedback from assessment.[31] Likewise, the insights gained through intelligence, as part of target development, will inform most other steps of the cycle. Thus, there is considerable overlap and concurrency with the

[31] Joint Targeting School (US), *Joint Targeting School Student Guide* (Dam Neck, Virginia: 1 Mar 2017): 194.

steps in practice. Lastly, the process shown in the annex does not begin to incorporate the processes which run in parallel and influence targeting such as joint intelligence, surveillance, and reconnaissance (ISR) management, airspace management, operational planning processes, information operations, the intelligence cycle, etc. Thus, where issues do occur within the targeting process, it is often a function of complex realities rubbing against a contrived and conceptually linear process. The danger is in the potential maltreatment of complex risk through simple controls, examples of which will be provided in the following sections.

INTEGRATION OF RISK MANAGEMENT IN CAF TARGETING

Vertical and Functional Integration of Risk Within Targeting

US targeting doctrine explains that risk, inherent in all military operations, is a command function.[32] CAF doctrine similarly asserts that risk management is a commander's responsibility.[33] Not surprisingly then, the targeting process has developed to enable commanders to exercise their duties in this respect. This traditional approach to understanding risk as a command responsibility has created a bias towards the functional and vertical integration of specific risk related to targeting outcomes.

Vertical integration of risk is best exemplified by the authorities, responsibilities, and accountabilities (ARAs) delineated as part of the targeting process. Initial direction and guidance is issued by the commander and will include objectives and targeting priorities. Such direction will account for risk to achieving the overarching mission, as

---

[32] *Ibid.*, 98.

[33] Joint Doctrine Branch, *Risk Management for CF Operations*, B-GJ-005-502/FP-000, November 2007, 1-1.

well as specific risk related to targeting activity. The commander will also impose risk controls, such as criteria for who can act as a Target Validation Authority (TVA) or Target Engagement Authority (TEA), depending on the nature of the target, type of engagement (i.e. munitions or non-munitions), the estimated collateral damage, or any other specific criteria as a form of risk control.[34] For example, the commander may wish to delegate or retain TEA based on the confidence of the intelligence, or the fact that the target is in a built-up area. At the operational level, these controls may be inherited from the strategic level by way of the Strategic Targeting Directive (STD). Ultimately, it is through the delegation of authorities, and the implementation of controls, that vertical integration is achieved.

Functional integration of risk is embedded throughout the targeting process itself. This is evident in the way risk is identified, assessed, controlled and ultimately managed. Beginning with Step 2 of the targeting cycle, specific risk is identified and assessed as part of target development. Target development is aimed at understanding the physical and functional characteristics of a target, related to its respective target system, in order to recommend effects in accordance with stated targeting objectives (given in Step 1).[35] *CJCSI 3370.01B, Target Development Standards*, details the standards to be applied in

[34] Target Engagement Authority (TEA) is the authority delegated to approve the prosecution of a target. "The appropriate approval authority will be specified in the relevant operation-specific targeting directives." The commander, usually designated the TEA, also presides over the joint targeting coordination board. Target Validation Authority (TVA) is the authority delegated to validate a target in order to "…confirm that future prosecution would meet all the objectives and criteria outlined in planning, …be legal …and directly contribute to the strategic objectives and success of the CDS's mission." Both TVA and TEA may be delegated to the same position/individual, but not necessarily. *CJFP 3-9*, 1-9, 3-2, and 4-6.

[35] *Ibid*., 4-6.

Step 2, and in this way standardizes risk assessment and the communication thereof.[36] As part of intermediate target development, required components of the target include its functional characterization, a statement of expectations, the significance of the target, critical elements of the target, concerns with respect to intelligence to be gained or lost, and collateral concerns, among others.[37] These required components, therefore, force a comprehensive analysis of the target in order to support subsequent decision making (as part of Step 4 of the process) related to engaging the target and the associated risks identified as part of collateral concerns.[38] In this way, collateral concerns are the primary considerations related to risk of undesirable consequences. This specific risk is subsequently refined and further assessed through Collateral Damage Estimation Methodology (CDEM) as part of advanced target development (see Annex B) whereby an estimation of the anticipated collateral damage is determined and mitigated to the greatest extent possible through weaponeering.[39]

In addition to the specific risk of collateral damage, there is also more generalized risk related to the uncertainty surrounding the target. More specifically, there may be uncertainty with respect to the target's function (i.e. what role it serves), its significance (i.e. how important or critical it is to the target system and adversary), the expected

---

[36] *CJCSI 3370.01B* has been recently superseded by *CJCSI 3370.01C*; however, the latter is not publicly available. Thus, this paper uses details from *CJCSI 3370.01B* throughout. *CJCSI 3370.01B, Target Development Standards* (Washington: Joint Staff, 6 May 2016).

[37] *Ibid.,* B-13 and D-A-1.

[38] It is worth noting that while *CJCSI 3370.01B* is primarily focused on identifying physical collateral objects (such as civilian facilities) within a generically prescribed collateral effects radius (CER), it also allows for collateral considerations related to second and third order effects. *Ibid*., D-C-9.

[39] Weaponeering: "The process of determining the type, quantity and point of application of a weapon to achieve a desired effect, considering the target's characteristics, the weapon's accuracy and reliability, and the probability of success. DTB, record 47939 quoted in *CJFP 3-9,* GL-8; CDEM is explained in further detail at *Ibid.,* 4-9.

effects (i.e. how engaging the target will effect the target system and for how long), and the resulting intelligence to be gained or lost (i.e. how effecting the target will either support or negate future intelligence collection opportunities). *CJCSI 3370.01B*, therefore, also requires a confidence level be ascribed to each aspect of the target (e.g. a target's function could be assessed with *moderate* confidence, while the magnitude and duration of the desired effect could be assessed with *low* confidence).[40] This confidence level, and the use of probability language in supporting intelligence, reflects the inherent uncertainty in assessing risk associated with future activity. As Multi-disciplinary scholars, Marjolein van Asselt and Ortwin Renn, explain:

> "Those assessing or appraising risks pertaining to future events or consequences are necessarily confronted with uncertainty… There are no future facts, …and if the future would be either predetermined or independent of present human activities, the term 'risk' makes no sense whatsoever."[41]

When one considers that decision making has to account for uncertainty related to several aspects of the target, and the resulting compound probabilities, clarity in expressing uncertainty is of vital importance.[42]

---

[40] *CJCSI 3370.01B*, D-A-1.

[41] van Asselt and Renn, "Risk Governance," 437.

[42] See A.P. Dempster, "Introduction to Probability, Evidence, and Judgement," in *Decision Making: Descriptive, Normative, and Prescriptive Interactions*, edited by David E. Bell, Howard Raiffa, and Amos Tversky (New York: Cambridge University Press, 1988): 288-290. Standardized language concerning probability and confidence levels are in accordance with intelligence community (IC) guidelines, such as that of the Office of the Director of National Intelligence (ODNI), thus enabling clear communication of risk. A number of studies, however, have concluded that numerical representation better supports understanding of uncertainty vice purely qualitative expressions of probability. See Nicolai Bodemer and Wolfgang Gaissmaier, "Risk Communication in Health," in *Handbook of Risk Theory*, Volume 2, edited by Sabien Roeser, Rafeaela Hillerbrance, Per Sandin, and Martin Peterson (New York: Springer, 2012): 631-635; and Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Lanham, Maryland: University Press of America, 2004): 145.

Horizontal Integration of Risk within Targeting

While traditional approaches to targeting have typically reinforced vertical and functional integration of risk management, the various boards and working groups serve as a limited example of horizontal integration. A cross-section of functional expertise will be present at the different targeting working groups and targeting boards (see Annex B). These battle-rhythm events, and the informal meetings and correspondence that occur around them, serve to integrate functional expertise (e.g. intelligence, legal, public affairs, etc.), and risk specific to those functions (e.g. legal risk).[43] Given that this expertise resides in the commander's staff, with the ultimate aim of supporting their decision making, one could argue that these battle-rhythm events serve as examples of vertical and functional integration. However, when one appreciates that these experts can leverage larger expert communities (such as the larger Intelligence Community [IC], or the Office of the Judge Advocate General), a case can be made that they also represent horizontal integration.

While the above serves as a somewhat limited example of horizontal integration of risk management, these battle-rhythm events still focus on managing specific risk within a pre-established process. What is lacking is a more comprehensive horizontal integration of risk from an enterprise level. Explained another way, sociologist Hauke Riesch proposes a five-level model of uncertainty: 1) uncertainty about the outcome; 2) uncertainty about the parameters of a model for predicting probability; 3) uncertainty about the model; 4) uncertainty about acknowledged inadequacies and our implicitly made assumptions; and 5) uncertainty about unknown inadequacies (i.e. 'unknown

[43] *CJFP 3-9*, 6-4 to 6-7.

unknowns').[44] Thus, the examples provided above are predominantly level one and two uncertainties related to risk. What is lacking is horizontal integration related to risk associated with uncertainty about the model (understood as the targeting process and its constituent components), its inadequacies, and mechanisms to adapt to unforeseen circumstances.

The need for better horizontal integration is evident by the way risk is inherited and integrated with inter-agency and coalition partners. A recent example is Canada's endorsement of the Safe School Declaration.[45] Guideline 4 for the application of the SSD reads:

> While the use of a school or university by the fighting forces of parties to armed conflict in support of their military effort may, depending on the circumstances, have the effect of turning it into a military objective subject to attack, parties to armed conflict should consider all feasible alternative measures before attacking them, including, unless circumstances do not permit, warning the enemy in advance that an attack will be forthcoming unless it ceases its use.[46]

This specific guideline reflects the aim of the SSD which is to afford schools protection beyond the law of armed conflict (LOAC) given their importance in the protection of children and in conflict resolution.[47] There are also implication for how Canada treats a school that is either dual-use, or is solely occupied by belligerents, and therefore is

---

[44] Hauke Riesch, "Levels of Uncertainty," 97-99.

[45] Global Affairs Canada, "Canada Endorses Safe Schools Declaration - News Release," *Government of Canada*, last modified, February 21, 2017. https://www.canada.ca/en/global-affairs/news/2017/02/canada_endorses_safeschoolsdeclaration.html.

[46] Global Coalition to Protect Education from Attacks, "Guidelines for Protecting Schools and Universities from Military use During Armed Conflict," December 2014, http://protectingeducation.org/sites/default/files/documents/guidelines_en.pdf.

[47] Conflict resolution in this sense is also meant to include post-war reconstruction and peace-building initiatives. It is also worth noting that the SSD represents policy coherence with respect to Canada's position on child soldiers reflected in the Vancouver Principles. Government of Canada, "Vancouver Principles: On Peacekeeping and the Prevention of the Recruitment and use of Child Soldiers," November 15, 2017, https://www.international.gc.ca/world-monde/assets/pdfs/issues_development-enjeux_developpement/human_rights-droits_homme/principles-vancouver-principes-english.pdf.

functionally characterized as something other than a school.[48] With the Department of National Defence (DND) being included with Global Affairs Canada in the press release, one can infer DND was consulted with respect to the policy implications of SSD. What is less clear is what consideration was given to the impact the SSD would have on specific targeting policy, doctrine, and operations, especially given that the US is not one of the 103 signatories of the declaration.[49] While the CAF ceased its airstrikes in Iraq and Syria in 2016, direct and indirect support to targeting continued, and the JTIC continues support to *Operation Inherent Resolve*.[50] Thus, these national differences towards targeting in a coalition context, and the resultant risk to national policy and targeting efficacy, deserves consideration.

The national differences in the application of SSD also highlights the role of culture in risk management. Social influence and organizational culture have a significant effect on decision making and perceptions of risk.[51] These differences must be considered to ensure national participation in coalition targeting reflects Canadian interests and obligations. Thus, CAF doctrine devotes an exclusive (albeit short) chapter to targeting in multinational operations where it delineates lead-nation and contributing-

---

[48] "An object that is normally a civilian object, depending on the circumstances, can be considered a military objective. Such objects are referred to as a 'dual use' object. Although the term is commonly used in targeting publications, dual use is not a term of law. An object is either a military objective or it is not." *CFJP 3-9*, 2-5.

[49] Global Coalition to Protect Education from Attacks, "Safe Schools Declaration Endorsements," Last updated April 3, 2020, https://ssd.protectingeducation.org/endorsement/.

[50] Library of Parliament, "Canada's Military Role In Iraq," *HillNotes*, last updated July 25, 2019, https://hillnotes.ca/2019/07/25/canadas-military-role-in-iraq/; Stewart Bell and Andrew Russell, "Exclusive: Coalition Forces in Syria, Iraq Targeted Three Canadians, Secret Document Says," *Global News*, last updated May 29, 2018, https://globalnews.ca/news/4232306/exclusive-coalition-forces-in-syria-iraq-targeted-three-canadians-secret-document-says/; and Jessica Desjardins, "CAF Reaches an ISR Milestone," *The Maple Leaf*, last updated March 6, 2020, https://ml-fd.caf-fac.ca/en/2019/06/30226.

[51] Dan M. Kahan, "Cultural Cognition as a Conception of the Cultural Theory of Risk," in *Handbook of Risk Theory*, Volume 2, edited by Sabien Roeser, Rafaela Hillerbrand, Per Sandin, and Martin Peterson (New York: Springer, 2012): 725-760.

nation targeting responsibilities.[52] What the doctrine does not address is the nuanced approach to risk management between national targeting processes. Given that doctrine is deliberately generalized, this is not meant as a critique, but again highlights that risk must be managed at the enterprise level.[53] The national differences towards IC vetting serves as an example in this respect. From *CJCSI 3370.01B*:

> Target vetting mitigates risk to the [Joint Force Commander] by tasking IC members to provide their assessment of the target characterization in the [Electronic Target Folder] and effectively distributing some risk of engaging the target with the IC. Target vetting is a valuable mechanism to mitigate risk, however it is not required to engage a target, and may not be a realistic expectation for every joint target list (JTL) and restricted target list (RTL) target. Target vetting should be completed for higher risk targets (e.g., dual-use targets, targets with complex characterizations, and targets in urban areas), in balance with lower risk targets (e.g., adversary units).[54]

Thus, the US treats target vetting as a selective risk control based on the assessed risk of the target itself. In juxtaposition, Canadian doctrine requires all national targets be vetted and validated before submission to the coalition for duplicate vetting and validation.[55] With a timeline of 10 working days for IC vetting, the trade-off is latency in the targeting process, which itself presents risk due to increased uncertainty of the parameters of the target, as well as more generalized risk to the efficacy of the targeting enterprise.[56] Thus, by attempting to manage specific risk though rigid controls, risk trade-offs are not considered, and complex and mutable risk is maltreated as simple risk. If we consider IC vetting as a mechanism to mitigate risk to the commander in their decision to validate a

---

[52] *CJFP 3-9*, 3-9, 6-3, and 6-4.

[53] The generalized nature of doctrine at the joint operational level (compared to an environment- specific tactical level) is explained in the CAF capstone publication on doctrine. It explains that doctrine espouses the "fundamental principles by which military forces guide their actions in support of objectives. It is authoritative but requires judgment in application." Thus, it differs from standard operating procedures or tactics, techniques, and procedures as being *relatively* more generalized, conceptual, and abstract. Canadian Forces Experimentation Centre, *CFJP -01 - Canadian Military Doctrine*, 1st Edition (Ottawa: Her Majesty the Queen as represented by the Minister of National Defence, 2009): 1-1 to 1-3.

[54] *CJCSI 3370.01B*, B-12.

[55] *CJFP 3-9*, 6-3.

[56] *CJCSI 3370.01B*, E-A-1.

target, that commander should be similarly empowered to refuse target vetting in favour of risk trade-offs.

With the JTIC conducting intermediate target development in support of CAF on expeditionary operations, and with some of those operations in support of coalition operations, there is potential for the JTIC to nominate a target for coalition approval and engagement. Similar to Canada's approach to vetting, there may be a bias towards rigidly applying risk controls in order to ensure targeting efforts remain aligned with Canadian interests and obligations. If we accept that risk management is a command function, the implementation of risk controls must be careful not to maltreat complex risk as simple, and must provide suitable flexibility to enable the commander in this role. An example of this maltreatment could include placing rigid constraints on the types of targets authorized for development vice validation (see Appendix 1 to Annex B). Understanding that target development plays an important role in informing the rest of the cycle, and that it is the primary mechanism for risk identification and assessment, artificially constraining the types of targets authorized for development may contribute to risk blind spots and artificially limit optionality. A similar example of maltreatment could be to rigidly require a specific number of intelligence sources for validation vice risk controls related to intelligence confidence levels (described above). A minimum number of intelligence sources does not directly relate to the confidence level associated with a target's functional characterization. For example, multiple sources of reliable human intelligence may represent greater uncertainty, and be assessed at a lower confidence level, than a single piece of signals intelligence.[57] Thus, such a risk control,

[57] For the purpose of our discussion, 'different sources' refers to reports of different provenance vice different intelligence disciplines.

similar to those that ensure positive identification (PID) during a dynamic engagement, may not be appropriate for deliberate targeting. Again, respecting that risk management is a command function, the commander must be enabled to make risk decisions without controls potentially maltreating risk and constraining those decisions prematurely.

The last example highlighting the need for better horizontal integration is with the recent GC and DND direction on intelligence sharing and 'avoiding complicity in mistreatment by foreign entities'.[58] Relevant sections of the DND Directive state:

> 2. When there is a substantial risk that disclosing information to a foreign entity would result in the mistreatment of an individual, and officials are unable to determine if that risk can be mitigated through, for example, the use of caveats or assurances, the matter will be referred for decision to the Chief of the Defence Staff and the Deputy Minister.
> 3. If that substantial risk cannot be mitigated, information will not be disclosed to that foreign entity.
> 4. In any case when approval to disclose information is granted because the Chief of the Defence Staff and the Deputy Minister determine that the substantial risk can be mitigated, the basis for such a determination must be clearly documented.[59]

This directive is aimed at reducing risk to both that individual and the GC by placing controls on intelligence sharing where there is concern of possible mistreatment of that individual by a 'foreign entity'. The unintended consequence, however, is that all other things being equal (i.e. a valid military objective that complies with LOAC) the sharing

---

[58] The DND Ministerial Directive is issued under the auspices of the *Avoiding Complicity in Mistreatment by Foreign Entities Act.* A portion of the enactment of Bill C-59, the Act places into statute responsibilities related to intelligence sharing and thus serves as a legal framework for ministerial direction to the same end. Minister of Justice, "Avoiding Complicity in Mistreatment by Foreign Entities Act," S.C. 2019, c. 13, s. 49.1, last amended on July 13, 2019, https://laws-lois.justice.gc.ca/PDF/A-18.8.pdf.

[59] "'Substantial risk' is a personal, present and foreseeable risk of mistreatment. In order to be 'substantial', the risk must be real and must be based on something more than mere theory or speculation. In most cases, the test of a substantial risk of mistreatment will be satisfied when it is more likely than not that there will be mistreatment; however, in some cases, particularly where the risk is of severe harm, the 'substantial risk' standard may be satisfied at a lower level of probability." Minister of National Defence, "Ministerial Direction to the Department of National Defence and the Canadian Armed Forces: Avoiding Complicity in Mistreatment by Foreign Entities," *Government of Canada,* November 24, 2017, https://www.canada.ca/en/department-national-defence/corporate/ministerial-directions/avoiding-complicity.html.

of intelligence where an individual may be captured, and subsequently mistreated, represents more institutional risk than were that individual be killed in an airstrike. Given that the counter-Daesh Coalition "…continues to work by, with and through regional partners to militarily defeat the Islamic State of Iraq and Syria…" and that in 2018 the "Coalition helped the [Iraqi Security Forces] focus clearance efforts, develop targets, and track the progress of operations," these concerns are grounded in reality.[60] In summary, a well-intentioned policy aimed at ensuring the humane treatment of individuals has created a risk regime whereby it represents less institutional risk to kill someone than it does to enable their capture (if there any concern with respect to how they will be treated) due to the relationship between uncertainty and risk.

ENTERPRISE RISK MANAGEMENT AND RISK GOVERNANCE FOR CAF TARGETING

While the above examples serve to highlight how complex risk can manifest and potentially be maltreated as simple risk through rigid controls, the ongoing creation of the targeting enterprise provides significant opportunity to address risk in a more comprehensive and horizontally integrated manner. The common thread in the examples above is that external organizations are involved. Thus, risk management must move beyond traditional mechanisms designed for largely internal and specific risk related to the targeting process. A shift to ERM and risk governance is needed.

While Lundqvist is critical of the appointment of a Chief Risk Officer (CRO) as the sole variable indicating ERM implementation, she does include it as a component of

[60] U.S. Central Command, "Combined Joint Task Force - Operation Inherent Resolve," last accessed April 21, 2020, https://www.centcom.mil/OPERATIONS-AND-EXERCISES/OPERATION-INHERENT-RESOLVE/.

'holistic organization of risk management'.[61] The designation of a CRO is similarly found in the other frameworks reproduced in Table 1, and a recent study by Poole College shows growth in the appointment of an executive level CRO in large organizations, public companies, and financial services entities across the US since 2009.[62] In the case of DND, the Assistant Deputy Minister (Review Services) fills this role; however, a 2017 internal audit concluded that IRM had not been adopted within the Department at a systemic level.[63] This is perhaps explained by the emphasis placed on risk management as a *command* responsibility, and a resulting bias towards vertical and functional integration of risk focused on operational outcomes. The creation of the CAF targeting enterprise provides an opportunity to establish focal points and mechanisms for horizontal risk integration related to targeting. Specifically, the creation of a DSET allows for the roles and responsibilities of a CRO to be embedded into that position, thus making them responsible for the risk management of the targeting enterprise on the CDS's behalf. Likewise, the SEMB provides a mechanism whereby risk to the targeting enterprise can be discussed and managed at the executive level, beyond the management of specific risks related to effects.

The creation of the JTIC also provides an opportunity for ERM implementation though its role as a *de facto* centre of excellence, focal point, and forcing function within the enterprise. Given its role in institutionalizing target development from what was an

---

[61] Lundqvist, "An Exploratory Study of Enterprise Risk Management," 397.

[62] Mark S. Beasley, Bruce C. Branson, and Bonnie V. Hancock, "2019 The State of Risk Oversight - An Overview of Enterprise Risk Management Practices," *AICPA and Poole College of Management, NC State* (Spring 2019): 17, https://erm.ncsu.edu/az/erm/i/chan/library/2019_Current_Report_on_State_of_Risk_Oversight.pdf.

[63] Assistant Deputy Minister (Review Services), "Review of Integrated Risk Management," *Department of National Defence,* November 2017, https://www.canada.ca/content/dam/dnd-mdn/migration/assets/FORCES_Internet/docs/en/about-reports-pubs-audit-eval/291p1850-3-012-eng.pdf.

ad hoc, deployed capability, the JTIC provides for continuity with external organizations (such as inter-agency partners and allies) and serves to force horizontal integration through the federated nature of intelligence and targeting in a multinational context. The continuity provided through the JTIC also presents opportunities for building trust within the CAF and with external partners. This is important given linkages between trust, risk, and co-operation. According to philosophers Philip Nickel and Krist Vaesen, trust both informs perceptions of risk of 'the other' and conversely is informed by assessments of risk posed by 'the other'. Similarly, high trust also reduces cognitive and affective interpersonal risk whereby mutually beneficial aims can be pursued in a cooperative manner.[64] Thus, the continuity provided by the JTIC has the potential to reinforce interpersonal and interorganizational linkages whereby risk is more effectively communicated and collaboratively managed.

Collaborative risk management is also important given the increasingly collaborative and federated nature of targeting. Like the CAF, allies are increasingly relying on reach-back organizations to provide targeting support to deployed elements.[65] Thus, the number of organizations, of varying nationalities, under different command and control relationships, adds complexity and increases the number of stakeholders in contemporary operational level targeting. Likewise, increased emphasis on non-munitions-based effects, such as those involving information and cyber, adds similar complexity through additional stakeholders as well as the introduction of level three and four uncertainties (uncertainty about the model, and uncertainty about acknowledged

---

[64] Philip J. Nickel and Krist Vaesen, "Risk and Trust," in *Handbook of Risk Theory*, Volume 2, edited by Sabien Roeser, Rafaela Hillerbrand, Per Sandin, and Martin Peterson (New York: Springer, 2012): 858.

[65] One such example is the creation of the Air Force Targeting Center at Langley Air Force Base, Virginia. Pratzner, "The Current Targeting Process,"84.

inadequacies and our implicitly made assumptions). Specifically, information and cyber warfare add to uncertainty over what constitutes an armed attack, uncertainty related to different orders of effect, blur the distinction between civilian and military targets and means of targeting, and challenge the joint targeting process' ability to incorporate these complexities. The Russian NotPetya cyberattack on Ukrainian equities in 2017 highlights some of these challenges amid massive spill-over of effects beyond the boundaries and intended target of Ukraine.[66]

The traditional approach to addressing some of these challenges would be to use existing processes and mechanisms to more tightly control risk; however, doing so would also carry on the tradition of mistreating complex risks as simple. Such an approach also presents risk to the efficacy of the targeting enterprise and undermines the philosophy of mission command. While Coker argues that targeting has become an exercise in risk management, one could argue that targeting always involved risk management.[67] The change comes in the form of increased controls due to a contemporary focus on minimizing undesirable consequences—requiring an unprecedented degree of precision and restraint in order to minimize risk to forces and risk of collateral damage. This subversion of command through increased control was the topic of a 2016 Cranfield University paper and is akin to the concept of the '1,000-mile screwdriver'. The report explains that due to compression of the operational level of warfare, "Command may be becoming obsolete, with authority now tending to reside within the Control or

---

[66] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired,* last updated August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[67] Coker, *op. cit.*, 9.

Management, Planning and Coordination functions rather that being vested in the Commander."[68] This dichotomy between mission command and general risk aversion is further expanded on by retired Major-General Daniel Gosselin. Writing in 2006, he observed that mission command had all but disappeared from the CAF. Gosselin attributed this trend to a generally risk adverse culture within the CAF and GC, which gave way to increasingly centralized decision making and centrally held authorities.[69] At the crux of the issue around targeting, he also remarked that "the typical reaction to complexity and uncertainty is to increase controls and to increase centralization of decision making."[70] Nowhere is this more true than in joint targeting, and while mission command has enjoyed a renaissance within the CAF, targeting professionals continue to operate in a rigid framework of highly prescribed processes. In light of the examples in the previous section, it also seems that the answer to increasing complexity is to increase controls, the dangers of which have been highlighted. Thus, how does the targeting enterprise effectively manage complex risk? Risk governance shows promise in this respect.

Towards Risk Governance in the CAF Targeting Enterprise

As highlighted above, there are significant aspects of targeting ERM that involve external stakeholders such as the wider GC apparatus and Canada's allies. In this respect,

---

[68] Lorraine Dodd, Geoff Markham, and Jeremy Hilton, "Has Command Authority Been Subverted to Control?" *Cranfield University, Defence Academy of UK* (2016): 10. http://internationalc2institute.org/s/paper_15.pdf.

[69] Daniel P. Gosselin, "The Loss of Mission Command for Canadian Expeditionary Operations: A Casualty of Modern Conflict?" in *The Operational Art: Canadian Perspectives - Leadership and Command*, edited by Allan English, (Kingston, ON: Canadian Defence Academy Press, 2006): 220-222.

[70] *Ibid*., 211.

relatively newer theory on risk governance shows promise in terms of potential applications for targeting. Where traditional ERM would identify risk from external organizations as threats and hazards to be addressed, risk governance places emphasis on stakeholder engagement and collaborative risk management.[71] Within the context of public policy, Marjolein van Asselt and Ortwin Renn argue that risk governance constitutes a paradigm shift from simple risk management to a set of principles to be applied to complex systems with their characteristically uncertain and ambiguous risk. They argue that the relevancy of risk governance has transcended that of risk management given distributed agency between a multitude of stakeholders related to public policy. They also differentiate between horizontal, vertical, and multi-level governance which is somewhat analogous to vertical and horizontal integration in IRM—the primary difference being direct control of sub-organizations in the case of IRM, and the need for collaboration and cooperation between external stakeholders in the case of risk governance. They conclude that with effective communication and inclusion of stakeholders, a more comprehensive and integrated approach to risk, and a continuous reflection on risk management practices, risk can be more effectively governed.[72]

In a similar vein, sociologist Catherine Wong also advocates for increased inclusion and stakeholder engagement, calling for collaborative problem solving. Wong argues that given the mutable nature of risk related to public policy, a collaborative risk governance framework is warranted:

---

[71] van Asselt and Renn, *"*Risk Governance," 439-443,

[72] *Ibid.*; see also Marijke A. Hermans, Tessa Fox, and Marjolein B.A. van Asselt, "Risk Governance," in *Handbook of Risk Theory*, Volume 2, edited by Sabien Roeser, Rafeaela Hillerbrance, Per Sandin, and Martin Peterson (New York: Springer, 2012): 1094-1112; and Catherine Mei Ling Wong, "The Mutable Nature of Risk and Acceptability: A Hybrid Risk Governance Framework," *Risk Analysis* 35, no. 11 (2015): 1969-1982.

> Risk problems are conceived as mutable entities and risk acceptability is at best temporary and incomplete. The risk governance framework, therefore, must have a reflexive component that constantly re-evaluates what the problems are, who the (new) stakeholders might be, and what their interests are. This approach favors adjustments and corrections as the project develops. Indeed, changes are not interpreted as dishonesty or unreliability, but an evolution/reconfiguration of the problem.[73]

Wong further highlights the utility of smart and responsive regulation in risk governance. She argues that "supportive mechanisms that enable and empower [industries] to set their own standards and achieve them, while maintaining state regulatory agencies' authority to impose sanctions" offers a means through which to address the mutable nature of risk.[74] Given the 2008 financial crisis, there are undoubtedly counter-arguments for self-regulation in the private sector; however, one must be careful not to conflate self-regulation for deregulation.[75] Additionally, the general concept of allowing those closest to the problem to collaboratively manage risk is sound, and with strict accountabilities inherent in the military chain of command, is more appetible within this context. Such a decentralized approach is also similar in nature to the command and control concept of 'Power to the Edge', put forward by David Alberts and Richard, and what retired General Stanley McChrystal termed 'empowered execution'— both aimed at achieving greater agility in the face of growing complexity.[76]

With the dangers of the potential maltreatment of complex risk through rigid and simple controls, and the challenges associated with holistically managing risk that

---

[73] Wong, "The Mutable Nature of Risk and Acceptability," 1973.

[74] *Ibid*., 1972.

[75] Brooksley Born, "Foreword: Deregulation: A Major Cause of the Financial Crisis," *Harvard Law & Policy Review* 5 (2011): 231-243.

[76] David S. Alberts, "Agility, Focus, and Convergence: The Future of Command and Control," *The International C2 Journal* 1, no. 1 (2007): 1-30; David S. Alberts and Richard E. Hayes, *Power to the Edge: Command… Control… in the Information Age* (Washington, DC: Department of Defence Command and Control Research Program, 2003); and Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin, 2015): 198.

increasingly involves external stakeholders, the targeting enterprise could benefit by embracing risk governance. Resisting the tendency to manage complexity and uncertainty through more centralized decision making and increased controls, risk governance could enable smart and responsive regulation while simultaneously promoting the philosophy of mission command within the targeting enterprise. With the institutionalization of the targeting function, the CAF is poised to effect this shift. Specifically, with accountabilities from the DSET up to the CDS, and authorities and responsibilities delegated down, the CAF targeting enterprise is poised to self-regulate through governance and oversight exercised by the DSET and supporting structures. Likewise, between both the DSET and JTIC, there exists focal points through which to engage with external organizations, and the benefits of relationships and trust have already been highlighted with respect to collaboration and cooperation.

Logically, the creation of the targeting *enterprise* has set the conditions for *enterprise* risk management. Key to success in this respect, however, is resisting the desire to manage risk through traditional mechanisms that reinforce vertical or functional integration of risk. Instead, the CAF must commit to holistically managing risk involving equities both internal and external to the CAF. Likewise, eschewing centralized controls and decision making, and allowing the targeting enterprise to manage risk in a more smart and responsive manner, through a degree of self-regulation, would better align the targeting function with the philosophy of mission command. Put another way, the targeting enterprise should be thought of as a framework for the exercise of mission command over the targeting function.

CONCLUSION

The preceding discussion served to highlight how risk manifests and is managed within the CAF targeting enterprise. An introduction to ERM and CAF joint targeting was provided in order to then highlight the challenges with managing and integrating risk as it relates to the CAF targeting enterprise. The nuanced application of effects offered through joint targeting requires a correspondingly nuanced and eloquent risk regime, capable of adapting to complexity. The ongoing creation of the CAF targeting enterprise serves as an inflection point whereby the CAF can continue to manage targeting risk through existing processes and controls, thereby maltreating complex risk as simple, or usher in a new approach in favour of ERM and risk governance. Given the growing complexities of targeting in the contemporary operating environment, the CAF would do well with the latter. As also discussed, the self-regulatory aspect of risk governance has the added benefit of aligning the targeting function with the philosophy of mission command. With the CAF recently releasing its Pan-Domain Force Employment Concept—that advocates for a 'targeting mindset', with emphasis on an 'outcomes-based approach', and alongside 'Whole of Nation' partners—the need for this shift is now.[77]

[77] Canadian Armed Force, *Pan-Domain Force Employment Concept: Prevailing in an Uncertain* World (Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2020): 30, and 51.

BIBLIOGRAPHY

Alberts, David S. "Agility, Focus, and Convergence: The Future of Command and Control." *The International C2 Journal* 1, no. 1 (2007): 1-30.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command… Control… in the Information Age*. Washington, DC: Department of Defence Command and Control Research Program, 2003.

Amoore, Louise and Merieke de Goede (eds.). *Risk and the War on Terror*. New York: Routledge, 2008.

Assistant Deputy Minister (Review Services). "Review of Integrated Risk Management." *Department of National Defence*. November 2017, https://www.canada.ca/content/dam/dnd-mdn/migration/assets/FORCES_Internet/docs/en/about-reports-pubs-audit-eval/291p1850-3-012-eng.pdf.

Beasley, Mark S., Bruce C. Branson, and Bonnie V. Hancock. "2019 The State of Risk Oversight - An Overview of Enterprise Risk Management Practices." *AICPA and Poole College of Management, NC State* (Spring 2019). https://erm.ncsu.edu/az/erm/i/chan/library/2019_Current_Report_on_State_of_Risk_Oversight.pdf.

Bell, Stewart and Andrew Russell. "Exclusive: Coalition Forces in Syria, Iraq Targeted Three Canadians, Secret Document Says." *Global News*. Last updated May 29, 2018, https://globalnews.ca/news/4232306/exclusive-coalition-forces-in-syria-iraq-targeted-three-canadians-secret-document-says/.

Bodemer, Nicolai and Wolfgang Gaissmaier. "Risk Communication in Health." In *Handbook of Risk Theor*y, Volume 2. Edited by Sabien Roeser, Rafeaela Hillerbrance, Per Sandin, and Martin Peterson, 621-660. New York: Springer, 2012.

Born, Brooksley. "Foreword: Deregulation: A Major Cause of the Financial Crisis." *Harvard Law & Policy Review* 5 (2011): 231-243.

Canadian Armed Force. *Pan-Domain Force Employment Concept: Prevailing in an Uncertain* World. Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2020.

Canadian Forces Experimentation Centre, *Canadian Forces Joint Publication 01 - Canadian Military Doctrine*, 1st Edition. Ottawa: Her Majesty the Queen as represented by the Minister of National Defence, 2009.

Canadian Forces Warfare Centre. *Canadian Forces Joint Publication 3-9 Targeting*, 1st Edition. Ottawa: Her Majesty the Queen as represented by the Minister of National Defence, 2014.

Chairman of the Joint Chiefs Instruction (CJCSI) 3370.01B, Target Development Standards. Washington: Joint Staff, 6 May 2016. https://fas.org/irp/doddir/dod/cjcsi3370_01.pdf.

Choi, Yongrok, Xiaoxia Ye, and Lu Zhao, "Optimizing Enterprise Risk Management: A Literature Review and Critical Analysis of the Work of Wu and Olson," *Annals of Operations Research* 237 (2016): 281-300.

Coker, Christopher. "Targeting in Context." In *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt and Frans P.B. Osinga, 9-25. The Hague: T.M.C. Asser Press, 2016.

Committee of Sponsoring Organizations of the Treadway Commission. "Enterprise Risk Management: Integrating with Strategy and Performance - Executive Summary." June 2007, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

Dempster, A.P. "Introduction to Probability, Evidence, and Judgement." In *Decision Making: Descriptive, Normative, and Prescriptive Interactions.* Edited by David E. Bell, Howard Raiffa, and Amos Tversky, 284-292. New York: Cambridge University Press, 1988.

Desjardins, Jessica. "CAF Reaches an ISR Milestone." *The Maple Leaf.* Last updated March 6, 2020, https://ml-fd.caf-fac.ca/en/2019/06/30226.

Dodd, Lorraine, Geoff Markham, and Jeremy Hilton. "Has Command Authority Been Subverted to Control?" *Cranfield University, Defence Academy of UK.* 2016, http://internationalc2institute.org/s/paper_15.pdf.

Doyle, Brett. "The Whole-of-Nation and Whole-of-Government Approaches in Action." *Interagency Journal* 10, no. 1 (2019): 105-122.

Global Affairs Canada. "Canada Endorses Safe Schools Declaration - News Release." Government of Canada. Last modified, February 21, 2017. https://www.canada.ca/en/global-affairs/news/2017/02/canada_endorses_safeschoolsdeclaration.html.

Global Coalition to Protect Education from Attacks. "Guidelines for Protecting Schools and Universities from Military use During Armed Conflict." December 2014, http://protectingeducation.org/sites/default/files/documents/guidelines_en.pdf.

Global Coalition to Protect Education from Attacks. “Safe Schools Declaration Endorsements.” Last updated April 3, 2020, https://ssd.protectingeducation.org/endorsement/.

Greenberg, Andy. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired.* Last updated August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Gosselin, Daniel P. “The Loss of Mission Command for Canadian Expeditionary Operations: A Casualty of Modern Conflict?” In *The Operational Art: Canadian Perspectives - Leadership and Command.* Edited by Allan English, 193-228. Kingston, Ontario: Canadian Defence Academy Press, 2006.

Government of Canada. “Operation IMPACT.” Last modified December 10, 2018. https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html.

Government of Canada. “Operation MOBILE.” Last modified January 22, 2014. https://www.canada.ca/en/department-national-defence/services/operations/military-operations/recently-completed/operation-mobile.html.

Government of Canada. “Vancouver Principles: On Peacekeeping and the Prevention of the Recruitment and use of Child Soldiers.” November 15, 2017, https://www.international.gc.ca/world-monde/assets/pdfs/issues_development-enjeux_developpement/human_rights-droits_homme/principles-vancouver-principes-english.pdf.

Grabo, Cynthia. *Anticipating Surprise: Analysis for Strategic Warning*. Lanham, Maryland: University Press of America, 2004.

Greenberg, Andy. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired*. Last modified August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Heng, Yee-Kuang and Kenneth McDonagh. *Risk, Global Governance and Security: The Other War on Terror*. New York: Routledge, 2009.

Hermans, Marijke A., Tessa Fox, and Marjolein B.A. van Asselt. “Risk Governance.” In *Handbook of Risk Theory*, Volume 2. Edited by Sabien Roeser, Rafeaela Hillerbrance, Per Sandin, and Martin Peterson, 1094-1112. New York: Springer, 2012.

International Organization for Standardization. “ISO 31000 - Risk Management.” 2018, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

Joint Chiefs of Staff (US). *Joint Publication 3-60 Joint Targeting.* 13 April 2007.

Joint Doctrine Branch. *Risk Management for CF Operations*, B-GJ-005-502/FP-000. November 2007.

Joint Targeting School (US). *Joint Targeting School Student Guide*. Dam Neck, Virginia: 1 Mar 2017.

Kahan, Dan M. “Cultural Cognition as a Conception of the Cultural Theory of Risk.” In *Handbook of Risk Theory*, Volume 2, edited by Sabien Roeser, Rafaela Hillerbrand, Per Sandin, and Martin Peterson, 725-760. New York: Springer, 2012.

Library of Parliament. “Canada’s Military Role in Iraq.” *HillNotes*. Last updated July 25, 2019, https://hillnotes.ca/2019/07/25/canadas-military-role-in-iraq/.

Lundqvist, Sara A. "An Exploratory Study of Enterprise Risk Management: Pillars of ERM." *Journal of Accounting, Auditing & Finance* 29 no. 3 (2014): 393-429

McChrystal, Stanley. *Team of Teams: New Rules of Engagement for a Complex World*. New York: Penguin, 2015.

Minister of Justice. “Avoiding Complicity in Mistreatment by Foreign Entities Act.” S.C. 2019, c. 13, s. 49.1. Last amended on July 13, 2019, https://laws-lois.justice.gc.ca/PDF/A-18.8.pdf.

Minister of National Defence. “Ministerial Direction to the Department of National Defence and the Canadian Armed Forces: Avoiding Complicity in Mistreatment by Foreign Entities.” *Government of Canada.* November 24, 2017, https://www.canada.ca/en/department-national-defence/corporate/ministerial-directions/avoiding-complicity.html.

NATO Standardization Office. *Allied Joint Publication-3.9 Allied Joint Doctrine for Joint Targeting*, Edition A, Version 1. April 2016.

Nickel, Philip J. and Krist Vaesen. “Risk and Trust.” In *Handbook of Risk Theory*, Volume 2, edited by Sabien Roeser, Rafaela Hillerbrand, Per Sandin, and Martin Peterson, 833-856. New York: Springer, 2012.

Office of the Director of National Intelligence (ODNI), *Intelligence Community Directive 203 - Analytical Standards.* January 2, 2015. https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

Pratzner, Phillip R. "The Current Targeting Process." In *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt and Frans P.B. Osinga, 77-97. The Hague: T.M.C. Asser Press, 2016.

Public Safety Canada. "Public Safety Canada Internal Audit of Integrated Risk Management." RDIMS# 893596. September 2013. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dt-ntgrtd-rsk-mngmnt/dt-ntgrtd-rsk-mngmnt-eng.pdf.

Riesch, Hauke "Levels of Uncertainty." In *Handbook of Risk Theory*, Volume 1, edited by Sabien Roeser, Rafaela Hillerbrand, Per Sandin, and Martin Peterson, 87-110. New York: Springer, 2012.

Palma, Dawnieca. "The Joint Targeting Intelligence Centre: Brining Innovation into Intelligence." *The Maple Leaf.* Last modified November 14, 2018. https://ml-fd.caf-fac.ca/en/2018/11/21578.

Treasury Board of Canada Secretariat. "Guide to Integrated Risk Management: A Recommended Approach for Developing a Corporate Risk Profile." Government of Canada. Last modified May 12, 2016. https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/guide-integrated-risk-management.html.

United States Airforce. *Air Force Doctrine Document 2-1.9 - Targeting*. June 8, 2006.

United States Central Command "Combined Joint Task Force - Operation Inherent Resolve." Last accessed April 21, 2020, https://www.centcom.mil/OPERATIONS-AND-EXERCISES/OPERATION-INHERENT-RESOLVE/.

van Asselt, Marjolein B.A., and Ortwin Renn. "Risk Governance." *Journal of Risk Research* 14, no. 4 (April 2011): 431-449.

Wong, Catherine Mei Ling. "The Mutable Nature of Risk and Acceptability: A Hybrid Risk Governance Framework." *Risk Analysis* 35, no. 11 (2015): 1969-1982.

Yarger, H. Richard. "Toward a Theory of Strategy: Art Lykke and U.S. Army War College Strategy Model." In *U.S. Army War College Guide to National Security Issues - Volume I: Theory of War and Strategy.* 5th ed, edited by J. Boone Bartholomees, Jr., 45-51. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2012.

ABBREVIATIONS

BDA - Battle Damage Assessment

CDE - Collateral Damage Assessment

CDEM - Collateral Damage Assessment Methodology

CID - Combat Identification

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CJTF-OIR - Combined Joint Task Force - Operation Inherent Resolve

CTL - Candidate Target List

DND - Department of National Defence

DSET - Director Strategic Effects and Targeting

ERM - Enterprise Risk Management

GC - Government of Canada

IC - Intelligence Community

ISO - International Organization for Standardization

IOWG - Information Operations Working Group

IRM - Integrated Risk Management

JPTL - Joint Prioritized Target List

JTCB - Joint Target Coordination Board

JTL - Joint Target List

JTWG - Joint Targeting Working Group

MIDB - Military Intelligence Database

MOE - Measure of Effectiveness

MOP - Measure of Performance

OGD - Other Government Department

OTD (Op TD) - Operational Targeting Directive

PID - Positive Identification

ROE - Rules of Engagement

RTL - Restricted Target List

SEMB - Strategic Effects Management Board

STD (Strat TD) - Strategic Targeting Directive

TDWG - Target Development Working Group

TDNL - Target Development Nomination List

TEA - Target Engagement Authority

TSA - Target System Analysis

TSS – Target System Study

TVB - Target Validation Board

WEA - Weapons Effects Assessment

WoG - Whole of Government

THE JOINT TARGETING CYCLE

Figure 1 -- The Joint Deliberate Targeting Cycle
Source: *CJFP 3-9*, 4-3.

The CAF joint targeting cycle is closely aligned with both US and North Atlantic Treaty Organization (NATO) doctrine.[78] The cycle begins with the 'End State and Commander's Objectives'. The Commander's guidance at the operational level is nested in, and aligned with, strategic-level guidance. Such guidance includes relevant GC, DND, and CAF policy, the CAF Strategic Targeting Directive (STD), the CDS operation specific STD, and any other relevant orders or directives. Direction and guidance at the operational level will take into account strategic direction in order to link the ends of strategy to the tactical ways and means of targeting to achieve operational objectives.[79] Targeting direction at the operational level will normally be promulgated in an Operations specific targeting directive and/or as an annex to the operations order.[80]

---

[78] See Joint Chiefs of Staff (US), *Joint Publication 3-60 Joint Targeting*, 13 April 2007, II-13; United States Airforce, *Air Force Doctrine Document 2-1.9 - Targeting*, June 8, 2006; *and* NATO Standardization Office, *Allied Joint Publication-3.9 Allied Joint Doctrine for Joint Targeting*, Edition A, Version 1, April 2016, 2-2.

[79] For more on ends, ways, and means see H. Richard Yarger, "Toward a Theory of Strategy: Art Lykke and U.S. Army War College Strategy Model," in *U.S. Army War College Guide to National Security Issues - Volume I: Theory of War and Strategy*, 5th ed, edited by J. Boone Bartholomees, Jr. (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2012): 45-51.

[80] *CFJP 3-9*, 4-3.

Step 2, 'Target Development and Prioritization', is predominantly informed through the collection, processing, and production of intelligence in the form of Target Systems Analyses (TSAs), Target Packages, targeting materials (such as imagery and graphics), and supporting intelligence related to the function or physical description of the target. It is aimed at understanding the target and target system to inform priorities and effects in order to achieve the objectives laid out in Step 1. This step also includes target vetting and validation whereby the underlying intelligence is confirmed in the case of the former, and the target is validated as meeting all legal constraints and operational criteria in the case of the latter. Should the target pass validation, it will undergo collateral damage estimation methodology (CDEM) whereby the physical effects of attack will be estimated in order to assess, and where possible, control for collateral damage to civilian infrastructure and persons. Of note, the US *Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3370.01*, which details target development standards, has been adopted by the CAF. [81]

Step 3, 'Capabilities Analysis', is aimed at the judicious allocation of resources through matched force capabilities (such as delivery mechanisms and munitions) to desired effects, while minimizing collateral damage, duplication of effort, and risk to one's own forces. This step will result in recommendations brought forward to the commander in terms of how to effect targets, in what priority, and through what means.[82]

Step 4, 'Commander's Decision and Force Allocation', is the process of approving the "…[matched] prioritized targets with the available resources and

---

[81] *Ibid*., 4-4 to 4-10.
[82] *Ibid*., 4-11.

supporting intelligence, surveillance and reconnaissance assets… ."[83] This step will result in tasking orders for executing components and forces (i.e. those assigned to effect specific targets).[84]

Step 5, 'Mission Planning and Force Execution', includes the steps required to plan for and deliver effects onto a specific target.[85] As Phillip Pratzner explains:

> There are no magical solutions to ensure execution mistakes do not occur, for Von Clausewitz's concepts of the 'fog of war' and 'friction' are as prescient today as in his time. War and conflict carry risks that cannon be eliminated, but often can be mitigated.[86]

Thus, execution can also include the allocation of intelligence, surveillance, and reconnaissance (ISR) prior, during, and after a strike in order to mitigate risk, contribute to flexibility and understanding during the delivery of effects, as well as inform the assessment phase.[87]

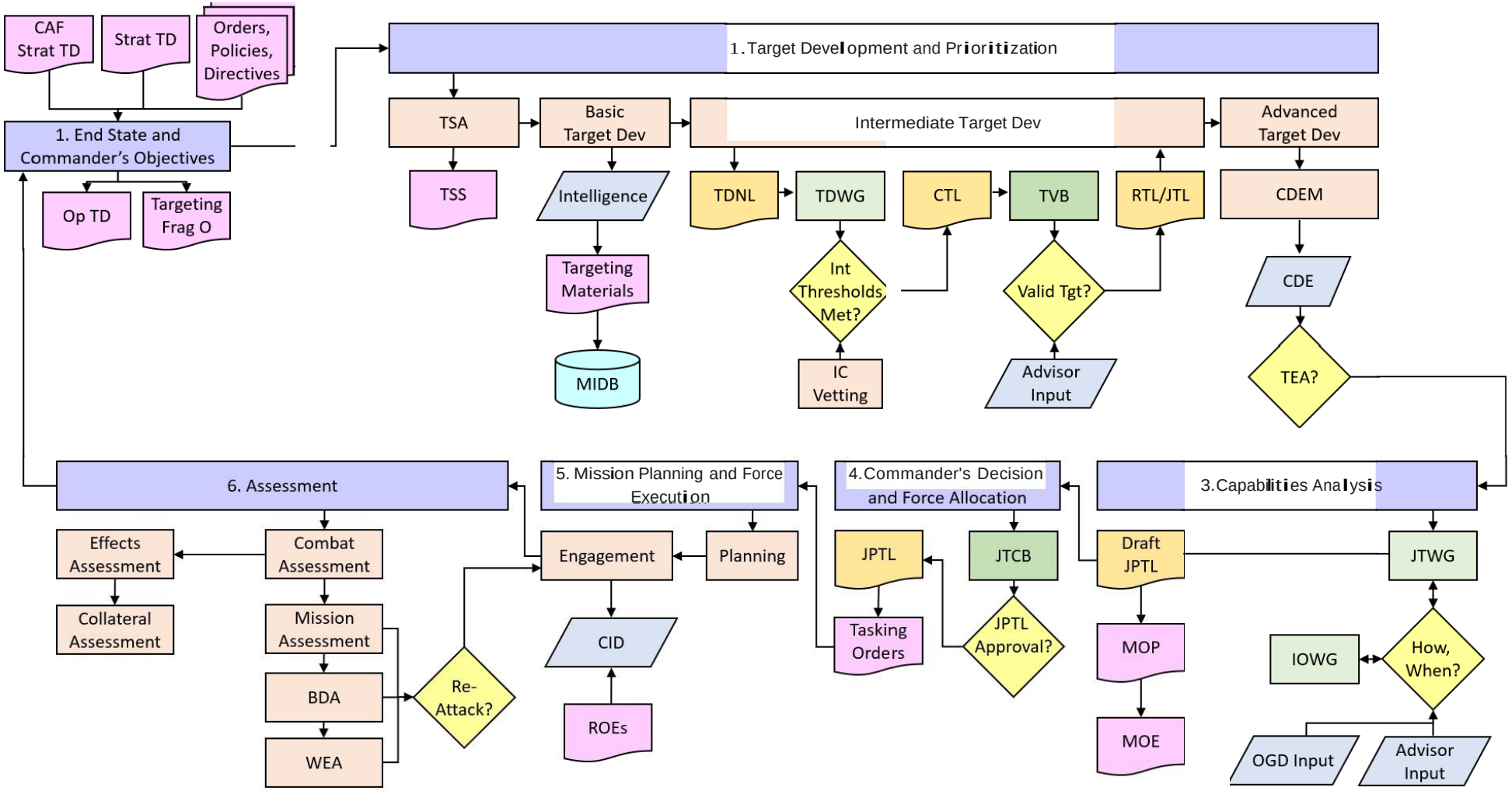
Finally, Step 6, 'Assessment', includes the measurement and judgement of performance and effectiveness related to effects on the target, the target system, and operational objectives. Measures of performance (MoP) help determine whether an attack had the desired result (e.g. destroying an ammunition production facility) through Battle Damage Assessment (BDA) (as part of what is termed 'combat assessment') and could result in a recommendation for re-attack. A measure of effectiveness (MoE), meanwhile, will inform whether the destruction of said facility supported the objective to which it was linked (e.g. disrupting an adversary's sustainment chain).[88] The output of this step should feedback into decision making related to earlier steps, and should also

---

[83] *Ibid*.
[84] *Ibid*.
[85] *Ibid*., 4-12.
[86] Pratzner, "The Current Targeting Process," 85.
[87] *Ibid*.
[88] *CJFP 3-9*, 4-12 - 4-13.

directly inform subsequent commander's guidance and direction at Step I, thus completing the cycle.

THE JOINT TARGETING PROCESS



Source: Adapted from CFJP 3-9, *Joint Targeting*, and the author's experience.
*Note: abbreviations used on this flow chart can be found in 'Annex A- Abbreviations'.