C2 AND THE PRIMACY OF INFORMATION

HENGAMEH IRANDOUST
Defence Research & Development Canada
Hengameh.Irandoust@drdc-rddc.gc.ca

1. Introduction

During the past three decades, western armies have been confronted with the complex reality of Command and Control (C2) in modern warfare, where decisions must be made based on incomplete and uncertain information, and actions planned and executed, sometimes under severe time constraints, against a resourceful and adaptive adversary in a contested and congested environment.

Often characterized as a four-stage decision loop that moves from observation and monitoring to decision-making and action execution, C2 has evolved to account for new operational concepts introduced by military strategists in an attempt to effectively deal with the challenges of the new threat environment, while keeping the cost of operations at a reasonable level. The key to this efficiency goal seems to have been an increased use of information in general, and of intelligence, in particular.

For the sake of clarity, let us provide some definitions. Information is any signal, sign, symbol or sequence of symbols that conveys a meaning for a particular audience. Intelligence, a particular type of information, is privileged and/or protected information [17] that has been actively looked for and acquired to be used for the benefit of an individual, group, organization, or nation.

The growing prominence of information/intelligence in new warfare concepts is based on the rapid development of information platforms and networks in recent years, which have made large amounts of data available for military intelligence, and at the same time, created a new operational domain, where information can be used as an effector, or produced as an effect, to achieve strategic objectives.

This paper aims to open the discussion on the way information/intelligence is reshaping C2, its benefits and its challenges. To that end, it explains the C2 decision cycle (Section 2), and discusses (Sections 3-5) several aspects of C2 that are being redefined as information/intelligence increasingly enables and drives the C2 decision-making process.

2. The C2 Decision Cycle

C2 is generally represented by the *Observe*, *Orient*, *Decide*, and *Act* (OODA) Loop (Figure 1), or four classes of information processing functions, which are [2]:

1. Information acquisition
2. Information analysis
3. Decision and action selection
4. Action implementation

Typically, in operations, the C2 decision cycle unfolds as follows: information is acquired, processed, and analyzed by the command team to achieve awareness relatively to an *Area of Interest* (AOI) and the actors operating therein. Based on this information, decisions are made and courses of actions developed, with consideration of opposing forces' intent, capabilities and vulnerabilities, own capabilities, probability of success or failure of possible actions, and their predicted effects and outcomes. Actions are then planned and coordinated, and resources allocated. Finally, actions are implemented to produce the desired effects and their outcomes monitored, leading to a new phase of observation and situation assessment.

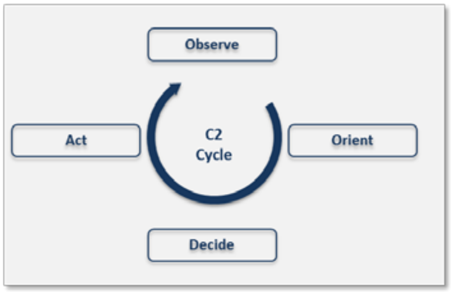

Figure 1: The OODA Loop

The decision making cycle can occur along three different decision making levels and timelines, referred to as *Strategic*, *Operational* and *Tactical* C2, with each level contributing to the achievement of the higher level objectives. Strategic C2 is concerned with decisions and plans that have a very broad scope and are elaborated considering long-term economic, political, cultural, and social factors. At the operational level, the objective is to accomplish a particular mission over a timeframe of days to weeks. Such operations are planned according to a standard staged procedure, referred to as the *Operational Planning Procedure* (OPP) [5]. Finally, at the tactical level, the mission timeframe is generally anything from minutes to hours, and the decision making process is often based on doctrine and established Tactics, Techniques, and Procedures (TTPs) learned through training, exercises and previous operations.

3. Intelligence as Decision Enabler

Access to critical information, through sensing, observation and intelligence products, is an important determinant of both decision quality and decision speed in the C2 cycle. In warfare, *information superiority* can provide significant military advantage. Thus, over the years, the notion of C2 has been gradually replaced by a series of derivative concepts (e.g., C2I, C4ISR, C4ISTAR) resulting from the combination of Command & Control with a number of enabling information provision functions: [Communications] [Computers] [Intelligence] [Surveillance][i] [Target Acquisition][ii] [Reconnaissance][iii].

Among these, *intelligence* refers to information of high interest that can be obtained directly, but which is generally derived from the fusion and analysis of information collected from a range of different sources following what is referred to as the *Intelligence Cycle*. This product can inform C2 decision-making in different ways. In tactical C2, intelligence is generally used offline to build the threat models and feed the TTPs, whereas, in operational C2, the *Intelligence Preparation of the Battlespace* (IPB) is triggered early in the Initiation stage of the OPP and remains active throughout the operations [4]. Thus, there are several levels of intelligence that feed different decision making levels.

The relationship between the *C2* and *I* cycles, can be described as follows (Figure 2): the output of the intelligence cycle feeds the C2 *Orient* process: it supports situation understanding, and informs the subsequent decision-making and action planning (how and when adversary's capabilities should be engaged / countered). In turn, the information deficiencies for situation analysis and decision making experienced during operations provide directions for information collection within the next intelligence cycle.

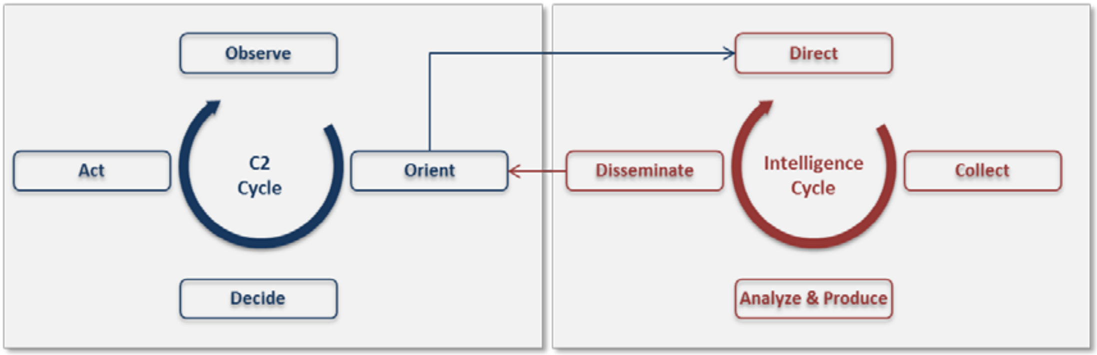

Figure 2: The C2I Process

The fact is that modern operations seem to be characterized by an ever-increasing reliance on intelligence, defined as privileged information [17] that has been sought and acquired for a specific purpose. The importance of leveraging information and intelligence capabilities in support of operations is repeatedly emphasized by defence strategies [1, 15]: 'The ability to collect, understand and disseminate relevant information and intelligence has become fundamental to the military's ability to succeed on operations [1].'

This vision has been fuelled in recent years by the availability of advanced information capabilities, such as surveillance aircraft, remotely piloted systems, space-based surveillance assets, and social/information networks, which can provide massive data while allowing remote monitoring and control. Intelligence thus produced would provide commanders with *prior* insight into the objectives, intentions, capabilities, and limitations of all actors within a given area of interest, and therefore allow them to gain the initiative, *i.e.*, deny the adversary the ability to act and force it to react.

However, although this intelligence-based operational model can be highly effective, there are still some major obstacles to the exploitation and dissemination of information, as discussed below (Sections 3.1 and 3.2).

3.1. Information Exploitation Challenges

The volume, ubiquity and speed of information that characterize the present era, have the potential to greatly facilitate the acquisition and exploitation of information for military objectives.

But although huge amounts of information are available, their exploitation can be arduous, time-consuming and sometimes impossible. One of the biggest challenges in this area is that raw data is rarely accurate, current and reliable enough to be directly consumed. C2 operators often have to make rapid decisions based on inconsistent or conflictual data sensed and observed through different sources. Intelligence analysts, on the other hand, have to spend a lot of time verifying, cross-checking, and integrating pieces of information from different sources before anything meaningful and useful can be extracted.

The multitude and diversity of information sources can potentially reduce the uncertainty of collected data, however, fusion and integration of large amounts of heterogeneous data with variable levels of reliability remains a complex problem and algorithmic solutions cannot always yield accurate results. In this regard, structured and unstructured data pose different challenges. In the former case, the complexity of correlation and fusion is often due to data imperfection. This is principally due to the limitations of the physical systems that capture or communicate raw data (*e.g.*, sensors, computerized systems) and the adaptive/deceptive weapons/tactics used by the adversary.

The problem with unstructured data, in form of natural language (text documents, emails, social media posts, audio files) or image (pictures and videos) is often their inherent complexity and ambiguity. While some data may have a structure that is simple enough to be easily decoded by an automation-based system, the interpretation of such data will often require common sense knowledge, contextual information, and a kind of reasoning that is still exclusive to human beings.

With the advent of machine learning techniques and data analytics, artificial intelligence technologies are currently viewed as enabling technologies for information collection, analysis and exploitation. Yet, although such technologies have made breakthroughs in many aspects of modern life, their application to image or language processing has still many limitations, mainly because of the rigidity of the models used, and the failure of processing methods to account for interpretation levels (*e.g.*, semantic or pragmatic) that yield the real meaning of visual or textual discourse.

3.2. Information Sharing Challenges

During operations, the multiplication of information sources is enabled through the expansion of an operational force to assets from other environments and allied nations. Such assets can bring unique capabilities, and when geographically dispersed, significantly increase sensor and effector coverage. This enhances the C2 *Observe* phase, as it allows each unit to obtain information from other units that are better positioned to acquire it. It also improves the *Act* phase, as it augments and optimizes combat power and increases the reaction time.

The potential of information leverage in distributed operations saw, during the last decade of 20th century, the emergence of the Network-Centric Warfare (NCW) concept. The latter was based on the assumption that robust networking, information sharing, and collaboration among units can enable information superiority and effective coordinated action [7]. This principle is still central to military thinking, as illustrated by concepts such as *Joint ISR* - collect, analyse and share information among allies to maximum effect [3], *Integrated Air & Missile Defence* - leverage all forms of information to support detection, targeting and engagement [12], or *Joint Fires* - use different force components' combat power in coordinated action to produce desired effects on a target [9].

The effectiveness of distributed operations is, however, still challenged by a range of factors that can hinder the flow of information around the network within each of the different domains of net centric operations. Operational units belonging to different organizations/nations often suffer from lack of connectivity and interoperability among platforms and systems (*physical domain*); are alternately deprived from and overwhelmed by information coming from other units (*information domain*); are sometimes denied information on other units' capabilities (*social domain*); and finally, are unable to properly use received information because of the lack of contextual information that characterizes remote communication, and/or the lack of a common reference frame for information interpretation among different organizations/nations (*cognitive domain*).

Despite such obstacles, allied forces have greatly benefited from information sharing at all three decision-making levels and defence strategies continue to emphasize the importance of maximizing capability by integrating assets into a joint system-of-systems that will guarantee both information superiority and flexibility, and will provide combat power at an affordable cost.

4. Proactive versus Reactive Decision Making

The possibility of acquiring sufficient and accurate intelligence on the adversary and its vulnerabilities, or the assumption of it, has led to a new conception of C2, where commanders can plan high impact actions in advance and impose the operations tempo. In other words, decision-making becomes proactive.

Although the term *Effects-Based Operations* (EBO) is no longer used, the concept still forms the basis of military strategies that attempt to energize the C2 cycle. Introduced by the US Joint Forces Command, EBO consist in enabling superior decision-making by establishing desired strategic effects, based on the prior comprehension of the enemy's system [8], and then planning back to operational and tactical level actions that can possibly achieve those desired effects.

Along the same lines, *Targeting* systematically analyzes and prioritizes targets and matches appropriate lethal and nonlethal actions to those targets to create specific desired effects that achieve higher-level objectives [13]. Targeting optimizes military action by limiting its scope to specific targets (objects, installations, persons, and organizations) that are 'critical', 'high-value', and 'high-payoff'. By providing time and control, intelligence-based and proactive strategies allow commanders to maximize the desired effects while mitigating the undesired ones, such as engagement errors or collateral damages.

In Figure 3, the joint targeting cycle [4], summarized as DECIDE-DETECT-DELIVER-ASSESS, has been broken down into phases to show that prior to action execution, this offensive strategy is roughly the reverse process of classical Operational C2, which was initially conceptualized as a defensive one. By identifying the desired effects first and then back planning, *targeting* streamlines and rationalizes the decision cycle, based on previously acquired intelligence.

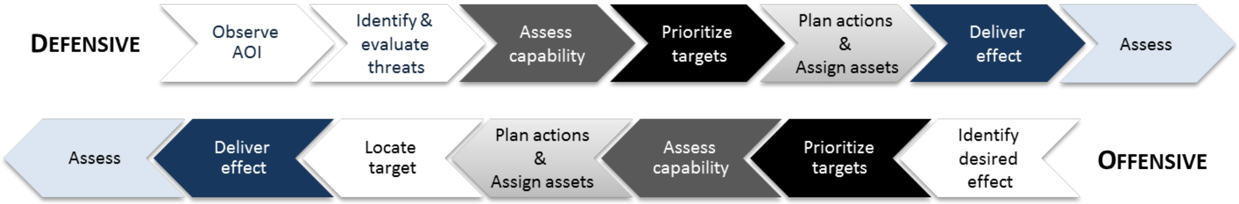

Figure 3: Defensive versus Offensive C2

In the future warfare environment, completely transformed by technological advances, this type of proactive ISR-based decision making is expected [16] to be punctuated with reactive phases, during which commanders will have to counter the unprecedented speed and reach of adversary operational tools within reduced decision timeframes.

5. Information as Effector

Over the past years, with the rapid development of defence technologies and the increasing pervasiveness of information and communication networks, the notion of battlespace, traditionally limited to air, land, and sea, has seen itself extended to new environments, such as space, cyberspace, the electromagnetic spectrum, and the whole public information domain. This has given way to a whole new range of operations and warfare concepts such as, *Psychological Ops, Influence Ops*, *Electronic Ops/Warfare*, *Cyber Ops/Warfare,* and *Information Ops/Warfare,* which often subsumes all the previous.

In the majority of these operations, information is not collected and exploited in support of a course of actions, but is itself the high value asset that should be acquired, protected, employed or propagated to achieve a specific strategic, operational or tactical objective. These new approaches to warfare have shown that 'deft use of information can offset the military advantages of well-trained personnel and highly capable equipment' [16].

Information can influence and manipulate specific groups or the general public opinion, subvert and corrupt existing information, or disrupt and degrade entire systems and infrastructures. Information capabilities can be used alone or in conjunction with other kinetic or non-kinetic targeting solutions [10] to generate a range of physical and psychological effects in support of global objectives.

In populated regions where most current operations take place, information can be easily propagated. Events can be immediately captured and relayed through social and news media, and subjected to 'reporting, scrutiny, and analysis by a global audience' [14]. Thus, all military action should be planned with consideration of its direct effects, as well as its desired or undesired informational ramifications.

As a result, the effectiveness of C2 is increasingly viewed in the judicious use of information and the ability to deliver effects across all domains through the application of the full range of military and non-military capabilities. The *multi-domain* character of C2 in modern warfare is best captured under the concept of *Hybrid Warfare*, where military capabilities are only one among many 'instruments of power' [11] that can be used to target adversary vulnerabilities. The impact of such hybrid strategies has been best demonstrated when used by state and non-state actors to overcome disparity in combat power, in what is referred to as *Irregular*, *Asymmetric* or *Unconventional Warfare*. The operational outcomes of such strategies are no longer described in terms of their physical manifestation, but in terms of linear and non-linear effects that they produce across 'the full spectrum of societal functions' [11].

Multi-effect decisions, generally made at the strategic level, are difficult ones, as they involve a large number of variables, and are based on predicted effects, which may be very uncertain. In this regard, decision-making and planning in the information domain carry a high level of risk, whether information is used as an effector or is the effect to be generated. In fact, the success of information operations depends not only on technological capabilities, but on deep knowledge and understanding of the inner workings of the political, economic, social, and cultural characteristics of the areas where effects are to be produced.

Finally, one of the main challenges in the information domain is to benefit from information capabilities to deliver effects, while denying adversaries those same advantages. Information technologies and networks are accessible to many actors and nations who can use them to inflict damage. This makes it very difficult for any actor to manoeuvre and take action in the information space without being exposed or targeted. As such, information capabilities both empower their users and make them vulnerable.

6. Conclusion

Major advances in information technologies, and the extension of the concept of operational domain to new and demanding environments, have transformed modern warfare and progressively changed the way C2 is conceived of. In this realm, C2 is increasingly required to be intelligence-based, proactive, predictive, precise, effective across multiple domains, and ultimately, efficient. The new C2 model is articulated around the acquisition, analysis, exploitation, dissemination, manipulation, production, and control of information.

This paper presented the above view and discussed its benefits and challenges at different decision making levels and in relation to different phases of the C2 decision cycle.

References

1. *Strong, Secure, Engaged*, Canada's Defence Policy, Minister of National Defence, 2017.
2. Parasuraman, R., Sheridan, T.B., and Wickens, C.D. A Model for Types and Levels of Human Interaction with Automation, IEEE Transactions on Systems, Man, and Cybernetics, 30, 2000, 286-297.
3. Joint Intelligence, Surveillance, Reconnaissance, https://www.nato.int/cps/en/natohq/topics_111830.htm
4. NATO Standard AJP-3.9, Allied Joint Doctrine for Joint Targeting, April 2016.

5. The Operational Planning Process Handbook, Canadian Land Force Command and Staff College, March 2010.
6. United States Army Field Manual: FM 3–0 Headquarters, Department of the Army *(14 June 2001).* FM 3–0, Operations*. Washington, DC*.
7. Garstka, J. & Alberts, D. (2004). Network-centric Operations Conceptual Framework. EBR Report.
8. Batschelet, A.W., Effects-based operations: A New Operational Model? US Army War College, 2002.
9. Joint Fire Support, https://www.army.mil/e2/c/downloads/361884.pdf, June 2010.
10. The Laws of Armed Conflict, http://www.genevacall.org/wp-content/uploads/dlm_uploads/2013/11/The-Law-of-Armed-Conflict.pdf
11. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, MCDC January 2017.
12. Weiss, G.F., Seeing 2020: America's New Vision for Integrated Air and Missile Defense, Joint Force Quarterly 76, 2014.
13. https://en.wikipedia.org/wiki/Targeting_(warfare)
14. Leonhard, R.R., Buchanan, T.H., Hillman, J.L., Nolen, J.M., and Galpin, T.J., A Concept for Command and Control, John Hopkins APL Technical Digest, Volume 29, Number 2, 2010.
15. National Strategy of the United States of America, Sharpening the American Military's Competitive Edge, 2018.
16. United States Army Training and Doctrine Command, The Operational Environment and the Changing Character of Future Warfare, smallwarsjournal.com.
17. Intelligence 101, http://www.intelligence101.com/information-vs-intelligence

[i] Persistent monitoring of an area/entity

[ii] Detection, identification, recognition and location of an entity to be engaged

[iii] Targeted information-gathering