Overt Information Operations During Peacetime

Selma Tekir

Izmir Institute of Technology, Izmir, Turkey

selmatekir@iyte.edu.tr

Abstract: Information superiority is the most critical asset in war making. It directly addresses the perception of the opponent and in the long term the will of him to act. Sun Tzu's classical text states this fact by the concept of deception as the basis of all warfare. The success in warfare then is dependent on being aware of what's happening, accurately realizing the context. This is the intelligence function in broad terms and mostly open source intelligence as it provides the context.

Competitive intelligence is based mainly on open sources and day by day the open source share in the intelligence product is increasing. Present diversified open sources & services represent a methodology shift in war. The two preceding ways have been overt physical acts against military targets in wartime and covert information operations conducted throughout peacetime against even nonmilitary targets respectively. The present methodology must be overt (open) information operations during peacetime. This coincides with a metaphor change as well. It proposes a transformation from a war metaphor into a game metaphor in which there are some playing rules. In fact, the existence of such rules helps in drawing the boundary of the field of competitive intelligence and thus making it a profession.

Game metaphor is safer to adopt than war as it's easier to take responsibility in public disclosure scenarios in this case. By following this metaphor, you continue to stay in the boundary of legitimate competition. In other terms, you make a conscious preference in terms of war intensities by choosing to avoid the more intense war forms limited conflict, and actual warfare respectively. Finally, this preference is in accordance with the fundamental point of the Sun Tzu's entire argument: The vision of victory without fighting.

To summarize, open source domination in the competitive intelligence lays the ground for the game metaphor that represents a transformation in warfare. The apparent outcome is overt information operations during peacetime. It emerges as the most important tool to fight against deception, thus success in information warfare in the contemporary world.

Keywords/Key Phrases: Information warfare, information operations, competitive intelligence, open sources, ethics.

1. Introduction

Information superiority is the most critical asset in war making. It directly addresses the perception of the opponent and in the long term the will of him to act. The Army’s Field Manual 3.0, Operations, (2001) as cited by (Thomas, 2003) describes the attainment of information superiority as capable of putting disparity in the enemy commander’s mind between reality and his perception of reality. This definition identifies information superiority as a capability to cause a deviation from reality.

Deviation from reality brings about lack of plausability and persuasiveness, which results in loss in the public support and isolation. Thus, as Sun Tzu stated "deception is the basis of all warfare" (Zi and Mair, 2009).

The army doctrine (DoD, 2001) defines information superiority as “the operational advantage derived from the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.” This second definition highlights reciprocal intelligence processes.

Information superiority is outcome of a continuous, dependable intelligence process along with a counter-intelligence perspective. In the Notional Information Operations Model that is presented in the Information Operations Primer (Department of the Army, 2006), the friendly intelligence process is termed as “Information Management” while the adversarial one is described by Intelligence, Surveillance and Reconnaissance (Figure 1).

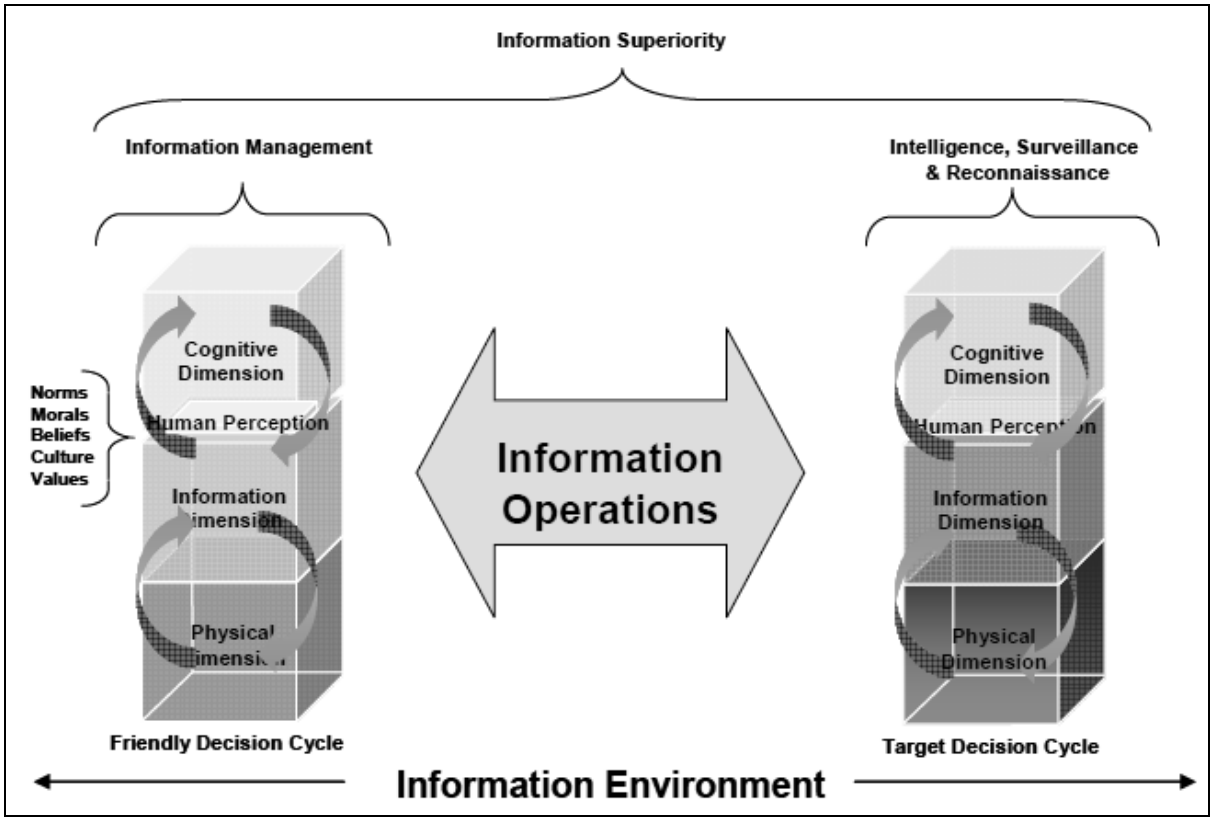

Figure 1: A Notional Information Operations Model (Department of the Army, 2006).

Both sides being a part of an information environment have different perceptions of a single reality, referred to as the situation. In order to achieve the goal of information superiority, information operations are conducted in the environment. Complete and correct assessment of the situation is called situational awareness and it's the high-level product of the information superiority reference model (Perry et al. 2004). The model is composed of three domains with associated functionalities (apparent in Figure 1):

- Physical domain-Ground truth (Entities, systems, intentions, plans, and physical activities.).
- Information domain-Collection and analysis capabilities.
- Cognitive domain-Decisionmaking, taking action.

Situational awareness requires accurately realizing the context. Open Sources Information (OSI) can be used in this manner as it contributes the understanding of the problem, tells the current situation and the context. Evaluation of the OSI in the first place for the intelligence collection provides a good

background and helps the effective and efficient tasking of the other, more difficult collection disciplines saving much of the resources.

Having recognized this potential, competitive intelligence is based mainly on open sources and day by day the open source share in the intelligence product is increasing. Present diversified open sources & services represent a methodology shift in war. The two preceding ways have been overt physical acts against military targets in wartime and covert information operations conducted throughout peacetime against even nonmilitary targets respectively (Waltz, 1998). The present methodology, owing to existing open sources, must be overt (open) information operations during peacetime. In order to clarify the implications of the proposed methodology, it's useful to consult the information warfare and information operations definitions.

The formal U.S. DoD information warfare definition is as follows (Waltz, 1998): Information warfare includes actions taken to preserve the integrity of one's own information system from exploitation, corruption, or disruption, while at the same time exploiting, corrupting, or destroying an adversary's information system and the process achieving an information advantage in the application of force.

The U.S. DoD defines information operations as the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making (Department of the Army, 2006).

The formal U.S. DoD definition of information warfare covers three different information operations namely defense, offense, and information dominance and no precedence assignment was introduced. It's also apparent in the definition of "Information operations", influencing decision-making was not recognized as the core functionality.

The issue of organizing these three information operations; identifying the boundaries, responsibility areas, resource tasking, and the communication and coordination process is helpful in defining an information warfare framework. A partial initialization of such a framework can be found in Libicki (2009).

Overt (open) information operations during peacetime methodology highlights the information dominance as the definitive component of the information operations as it puts an emphasis on information operations that support decision-making. Open source intelligence (OSINT) presents new opportunities in this area.

A second aspect of the proposed paradigm shift is the change in the treatment of war. Traditionally war can only be inferred to mean a "crisis or conflict" situation. This fact can be observed in the JP 1-02 definition of information warfare (DoD, 2001):

"Information operations conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."

Similarly, in the international law provided in the Geneva Convention and the additional protocols "armed conflict" characterizes a war incident (Haslam, 2000). However, here the aim is to avoid more intense war forms like limited conflict and actual warfare and to stay within the boundary of legitimate competition. This viewpoint can be considered in relation to the "before going to war" (jus ad bellum) criteria of Arquilla (1999) as it does not recommend progressing into the stage of waging war. Moreover, the idea reinforces the discipline of competitive intelligence.

2. Competitive Intelligence

Competitive intelligence is the result of a trend to incorporate intelligence methodology and tools into private businesses. The trend was triggered by accelerated economic competition around the world that increased demand for better decision-making. Another factor is related to the high-cost of diversified and sophisticated tools through technology that the burden on the government budget has become not withstandable making the privatization a plausible choice.

The adoption of intelligence cycle by the business sector revealed the legal and ethical concerns. Particularly, the collection phase has come into question, OSINT has become the basis.

The ethics of information dominance (intelligence) is just a subset of the ethics of information operations. Within this work, the focus is on this particular subset. The broader area of "the ethics of cyberwarfare" is addressed in (Dipert, 2011).

There are apparently two metaphors in the competitive intelligence world, war and game respectively. War is inherited from the government intelligence and game is the new introduced one for the business sector. Adopting war metaphor, you continue to stay in the old world seeing the main collection effort as espionage. You admit to do whatever is required as long as the final aim is to defeat the opponent. This is not an appropriate vision and/or mission for a competitive intelligence professional.

The metaphor of a game sees competition in business as an exciting game, in which each competitor strives to achieve excellence, satisfy customers, and succeed as a result. The motive in this type of game is not to drive out the competition, but to work hard, play by the rules of the game, and do one's best in order to succeed (Trevino and Weaver, 1997).

Today, the nature of intelligence has changed dramatically. The information operations are not evaluated within the frame of an armed conflict. They do not have to accompany an armed conflict. Globalization is dominant, global corporations are everywhere. Their interests are not restricted with national or even continental boundaries. Information warfare has been started to be evaluated within the context of organizational decision making.

This status was also supported by the three consecutive streams in Prescott (1999). The stated streams give the history of the intelligence field. The first is described as Sun Zi's The Art of War, which articulates the philosophical framework for war making and intelligence. The second stream of intelligence puts national security concerns as a policy issue. The third stream places the business organization at center stage, which results in a systematic orientation towards business intelligence.

Warfare in the organizational context targets the perception, decision-making performance, operational effectiveness, and ultimately the will of the organizations.

In an adversarial competition or conflict, organization warfare seeks to understand and then change a target organization's behavior to achieve the goals of the attacker; generally these goals include deterrence, dissuasion, deception, disruption, degradation, or total defeat of the targeted organization Particularly the adversary's unity of command and purpose is targeted while preserving your own. In corporate competition, an organization may employ many of the principles and technical methods, herein, to ethically collect, analyze, and understand an adversary to employ ethical methods to influence the market and its competitor. The organization may also employ these methods to detect and deter an adversary's unethical efforts at manipulation (Kott, 2006).

The planner must consider the legality of organization influence operations and the potential collateral effects on civil populations to remain compliant with directly relevant international legal protocols (Geneva Conventions has a protection focus on civilian population, individual civilians or civilian objects).

In the organizational warfare, in targeting an organization for impact, there are two complementary approaches: Targeting the critical nodes of the organization, and focusing on the entire organization as a social entity. The former one puts an emphasis on individuals while the latter on the whole structure. People component deserves special attention as it is the one that transforms a business into a corporate asset.

As the competitive environment with globalization could be characterized by the game metaphor rather than the war metaphor (the traditional metaphor usually used for characterizing competition), it is increasingly important to include ethics in the corporation's strategy and potentially implement it in a way that achieves a competitive advantage for the company and adds value to the stakeholders (Azmi, 2006).

Contrary to the belief, game metaphor is not weaker than the war counterpart. Even using legitimate means one can acquire and process the required information. It's also advantageous to mutually agree on some set of rules as it also restricts the diversity of means available for the opposing parties. Thus, there is a decreased uncertainty in the competition.

Another concern is related to the characteristics of the digital environment. In the digital environment, the footprints cannot be concealed. Now or later it has high potential to be revealed. Being aware of this fact, staying in accordance with the rules of the game, one preserves his organizational reputation. Organizational reputation and its associated assets are of high importance.

Additionally, staying in the boundary of ethics helps in forming an organizational culture that will return benefits in the long term. This can be explained by corporate ethics rather than business ethics. On the one hand, business ethics has an external emphasis. Business ethics considers the gap between the corporation's ethical behaviour and the market place's perception of the corporation's ethics in its business operations. Corporate ethics, on the other hand, has an internal emphasis and this could be well managed toward a unique competitive advantage as anything related to people (corporate ethics through people) is very difficult to imitate and this raises the chances of achieving a sustainable competitive advantage (Azmi, 2006). By the use of corporate ethics, an investment on people is made and it will always have returns of vital value.

Game metaphor has an important mission as well: To draw the ethical boundary of the competitive intelligence discipline. CI practitioners need to have the profession recognized by external stakeholders as being legitimate and ethical. As the adoption of ethical standards is a hallmark of a profession, it paves the way for the competitive intelligence profession (Fleisher and Blenkhorn, 2000).

3. Conclusion

Competitive intelligence originated from the government intelligence. It borrowed the war metaphor from the traditional intelligence viewpoint. Game metaphor is in accordance with the conditions of the global economic environment, corporate cultures, civil emphasis, open sources & services, and thus more appropriate today. The above stated conditions started to put a pressure on all intelligence organizations that must also share them. Consequently, competitive intelligence has high potential to change its originating source by causing new reflections on the concept of war which can bring about redefinitions of information warfare and related concepts.

An example evidence is related to public disclosure. Game metaphor is safer to adopt than war as it's easier to take responsibility in public disclosure scenarios in this case. By following this metaphor, you continue to stay in the boundary of legitimate competition. In other terms, you make a conscious preference in terms of war intensities by choosing to avoid the more intense war forms limited conflict,

and actual warfare respectively. Finally, this preference is in accordance with the fundamental point of the Sun Tzu's entire argument: The vision of victory without fighting (Zi and Mair, 2009).

To summarize, open source domination in the competitive intelligence lays the ground for the game metaphor that represents a transformation in warfare. The apparent outcome is overt information operations during peacetime. It emerges as the most important tool to fight against deception, thus success in information warfare in the contemporary world.

References

Arquilla, John. (1999) “Ethics and Information Warfare”, [online], RAND Corporation, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap13.pdf (accessed on 23/03/12).

Azmi, Rania A. (2006) “Business Ethics as Competitive Advantage for Companies in the Globalization Era”, [online], http://ssrn.com/abstract=1010073 (accessed on 31/01/12).

Department of the Army (2006) AY07, Information Operations Primer, Headquarters, Department of the Army, U.S. Army Printing Agency, Washington, D.C.

Dipert, R. R. (2010). "The Ethics of Cyberwarfare." **Journal of Military Ethics** Vol 9 Is 4, pp 384-410.

DoD (2001) Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, [online] http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed on 02/02/12).

Fleisher, Craig S., Blenkhorn, David L. (2000) **Managing Frontiers in Competitive Intelligence**, Quorum Books.

Haslam, Emily. (2000) “Information Warfare: Technological Changes and International Law”, **Journal of Conflict and Security Law**, Vol 5 No. 2, pp 157-175.

Kott, Alexander. (2006) **Information Warfare and Organizational Decision-Making**, Artech House Publishers.

Libicki, M. (2009) “Cyberdeterrence and Cyberwar”, [online], RAND Corporation, http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf (accessed on 22/03/12).

Perry, Walter L., David Signori and John E. Boon. (2004) “Exploring Information Superiority: A Methodology for Measuring the Quality of Information and Its Impact on Shared Awareness”, [online], RAND Corporation, http://www.rand.org/pubs/monograph_reports/MR1467 (accessed on 31/01/12).

Prescott, J. (1999) The Evolution of Competitive Intelligence, Designing a Process for Action, APMP, Spring.

Thomas, T.L. (2003) “Is the IW Paradigm Outdated? A Discussion of U.S. IW Theory”, **The Journal of Information Warfare**, Vol 2 Is 3, pp 109-116.

Treviño, Linda Hlebe, Weaver, Gary R. (1997) “Ethical issues in competitive intelligence practice: Consensus, conflicts, and challenges”, **Competitive Intelligence Review**, Spring Vol 8 Is 1, pp 61-72.

Waltz, Edward L. (1998) **Information Warfare Principles and Operations**, Artech House, Inc.

Zi, Sun Mair, Victor H. (2009) **Art of War: Sun Zi's Military Methods**, Columbia University Press, New York.