11th ICCRTS

COALITION COMMAND AND CONTROL IN THE NETWORKED ERA

Some aspects on cyber war faring in information arena and cognitive domain

Information Operations/Assurance

Roland Heickerö, PhD
Adjunct Professor
Deputy Research Director

Swedish Defence Research Agency, FOI
Division of Defence Analysis
Gullfossgatan 6, Kista
SE-164 90 Stockholm
Sweden
Phone: +46 8 5550 38 25
Mobile: +46 (0)70 208 06 86
E-mail: roland.heickero@foi.se

Abstract

Knowledge of war fighting in the digital battlefield is becoming more important due to the introduction of network centric warfare concepts. The key to success in cyberspace is to understand the prerequisites for conducting operations in the information arena and cognitive domain. Hence, for the Swedish Armed Forces (SAF), it is vital to develop useful theories, methods and strategies that give the ability to deal with new types of threats in cyberspace and their consequences.

The purpose of this study is to discuss theories and methods for modern warfare within the information arena and cognitive domain respectively, in line with the transformation to the digital battlefield. Initially the paper discusses the term “cyber warfare” and its relation to information arena and cognitive domain. Then, the effects of cyber warfare within the arena as well as the domain are shown in the form of an effect-matrix. The matrix could be used as a tool in order to develop practical methods for information operations (InfoOps) in a structured way related to capabilities such as electronic warfare (EW), computer network operations (CNO) and psychological operations (PsyOps). In following paper one example is shown that describe jamming of UAV communication links based on the matrix.

Some aspects on cyber war faring in information arena and cognitive domain

1. Introduction

1.1 General background

The prerequisites for information warfare in cyberspace are changing. The introduction of Network Based Defence[1] (NBD) shifts the focus from platform protection[2] to network defence. In a network centric approach, it will be important to protect vital nodes and links as well as information systems and the information that is produced, stored and used. Consequently, the need will grow over time to integrate different capabilities such as electronic warfare (EW) with computer network operations (CNO). The future of war fighting will be determined on digital battlefield within the information arena[3] and cognitive domain. Significant for conflicts in cyberspace is asymmetry, where a weaker combatant could inflict serious damage on an apparently stronger adversary. Thus, a combatant combatant could, at low cost, hit the digital environment with major consequences as a result. Neither military nor civilian systems are totally protected from attacks due to the fact that the information systems, techniques and equipments that are used are often integrated with each other.

In general, the transformation increases the need for knowledge of asymmetrical warfighting in the digital sphere. More specifically, a better understanding of how different adversaries could use EW and CNO capabilities in order to influence information arena and cognitive domain must be developed. Hence, for the Swedish Armed Forces (SAF), it is vital to develop useful theories, methods and strategies that give the ability to deal with new types of threats in cyberspace and their consequences.

1.2 Purpose and disposition

The purpose of this paper is to discuss theories and methods for modern warfighting within information arena and cognitive domain which can be adapted to meet the new demands faced by the Swedish Armed Forces.

Initially the paper discusses the term “cyber warfare” and its relation to information arena and cognitive domain. Then, the effects of cyber warfare within the arena as well as the domain are shown in form of a matrix exemplified by jamming UAV communication. Finally, some conclusions are drawn.

The effect-matrix could be used as a tool in order to develop practical methods for information operation (InfoOps) in a structured way related to capabilities such as electronic warfare (EW), computer network operations (CNO) and psychological operations (PsyOps). A simple example is shown on how to use the matrix. This is an area of interest for future studies.

[1] Network Based Defence concept is the Swedish acronym for Network Centric Warfare - NCW

[2] By protecting the ”network” the single platform will also be protected. There is no clash of interest between the parts.

[3] In Swedish doctrine the term ”information arena” is used instead of ”information domain” in comparison to American and English definitions used in NCW concept. In section 3 the term is discussed more in detail.

2. The principles of Cyber warfare

2.1 Definitions

In American and English military vocabulary, cyber warfare is a part of information warfare which belongs within Information Operations[4] (InfoOps). In Sweden the concept is mainly related to CNO and partly to EW. There is a difference compared to traditional warfare in the physical arenas (domains) such as land, air, maritime and space because cyber warfare takes place in a digital environment; the *information arena*, which is created by humans. However any effects that may occur as a result of an action happen in the physical arenas. Also, the methods and procedures used to conduct warfare may differ between the digital and physical environments.

Parks and Duggan [1] define cyber warfare as

"Cyber warfare is a sub-set of information warfare that involves action taken in the cyber world. The cyber world is any virtual reality contained within collection of computers and networks."

Moreover, they also believe that there are different "cyber worlds", and that the most important are the Internet and other related networks which share media with Internet. For instance, these could be wireless communication systems such as WLAN and 3G including the services and applications that are used.

Park & Duggan also state that cyber warfare is to some extent similar to submarine warfare as well as the actions of SOF[5]. There is a likeness in terms of behaviour and the intention to conduct surprise attacks against an opponent, to mislead, manipulate and distort information, as well as to corrupt communications and to destroy equipment of various kinds. In comparison to more traditional methods of physical destruction, your own forces do not necessarily have to be moved from one area to another in order to attack; instead you can stay in same place but hit different points of the opponent's networks and systems. An overall goal of cyber warfare is to influence the weakest part of the chain, that part with the greatest vulnerability. Here, there is an analogy with theories of centres of gravity [2] in networks which allow attacks on vital nodes and links.

Some assumptions for cyber war are:

- the information arena is the battleground for the digital war. The arena is global with a great variety [3] of behaviours. Information can flow without restriction. This means that the arena is accessible for attacks/influence by more or less all actors regardless of resources, i.e. it requires very small means to harm/disrupt/mislead an opponent. A relatively small cost brings also out that the barriers for an adversary to influence the arena by different means and methods will be reduced.

[4] Information operations deal with methods for using different capabilities such as CNO, EW, PsyOps, Information security, etc. in order to influence an opponent to act in a direction that is in favour of your own. The concept also considers the protection of your own information resources and the defence of the information arena.

[5] SOF – Special Operation Forces

- asymmetry is a characteristic. An inequality of resources in physical world will not necessary be a hindrance in digital arena.

- a cyber attack must give an effect in the real world either directly or indirectly, such as manipulation, disruption or destruction of sensors, equipments, systems and information of different kinds. Through deception it is possible to influence decision-makers on strategic, tactical and operative levels.

- a successful digital attack will influence cognitive, perceptive and emotional processes of the receiving part i.e. his/her apprehensions and actions.

- an objective is to achieve Dominant Battlefield Awareness (DBA), meaning a superior collective understanding of the situation[4].

- the basis of a successful operation is founded on combinatorial methodology and value chains [5] as a way of using different capabilities such as EW and CNO, in order to influence an opponent in a direction that is in line with your intentions.

- there is no clear and distinct rules for behaviours in digital world as long it does not oppose laws of nature, bandwidth capacity in the ether etc. The reason is the fact that the world is artificial and created by humans and therefore it could also change. Moreover, software does not always perform well because of inbuilt bugs in the systems etc. [6].

- in cyberspace the expected effect will not always be achieved because the prerequisites for success are not clearly defined. It may be hard to distinguish between deliberate and unintentional effects. At the same time the artificial environment is somewhat in control of the person that created it [7].

- tools for information warfare could be used both for attack and protection; techniques are available for scanning vulnerabilities within the own network as well as the adversaries. Other methods, for instance, are intrusion detectors that seek for special activities and incidents in the communication flow.

- the attacking and protecting parties control only a small area of cyberspace and often only their own hardware and software. If you manage to control your opponents HW and SW then you also control their freedom of action.

- the distances to the target is irrelevant, an infological attack could be initiated in one side of the globe and achieve an effect on the other side [8]. In contrast electronic warfare, which also is a part of cyber warfare, is to some extent more dependent on the distance to an object for its effect due to laws of nature such as radio wave propagation. But even for EW the distances could be huge and reach many thousands of miles.

- an adversary could act anonymously which makes it difficult to identify both the person or organisation behind the attack and the intentions [9].

- an influence on the information arena could have judicial implications, as responsibility may be hard to prove [10].

3. Cyber warfare and its relation to information arena, the physical arena and cognitive domain

3.1 General

The battleground for digital warfare is the information arena[6] (domain), as mentioned above. According to Gartska [11] the arena is the place where information[7] lives; it is created, manipulated and shared with others. It is also the basis for achieving DBA against an opponent. This is why the arena has to be protected and defended with different means and methods.

There are a number of definitions of arenas[8] as well as domains[9] and their internal relation, respectively. In general, an arena is a limited area in space in contrast to a domain which is more related to functions. There could be some uncertainties when using the terms. There is a risk that the terms could be confused with each other. The terms are also used in same way to describe similar characteristics. There is a lack of stringency in terminology.

In the MNIOE[10] White paper [12] the arena is defined as "… *the (virtual and physical) space in which information is received, processed and conveyed. It consists of the information itself and Information Systems"*.

3.2 Internal relations between the arenas and cognitive domain

The information arena lives in symbiosis with both the physical arena and the cognitive domain. Compared to the information arena, the cognitive domain is the place where consciousness originates and characteristics and capabilities such as leadership, moral, doctrines, tactics etc are created and developed.

In order to produce information the *cognitive*[11] and *perceptive*[12] processes have to be involved. But *emotional*[13] processes are also needed. The reason is that more or less all human senses are used in the process of analysing and interpreting information. It is difficult to separate single components from others. For instance, in a case of deception in psychological operations the goal is to mislead as many parts of human apprehensions as possible. The receptivity of an individual to be influences such as misleading and

---

[6] Within the American NCW-concept "information domain" is commonly used, compared to Sweden where the term "information arena" is used instead. Basically the definitions are more or less the same in terms of content. A more detailed description of differences and similarities is done in *Heickerö, R* (2005). Olika perspektiv på informationsarenan. FOI Memo 1605.

[7] *Information* is data which been processed to some sort of content and meaning for a user. It was the American mathematician C.E Shannon in 1940s who defined information in terms of non predictability.

[8] A Wikipedia defintion on *Arena* is: " … a circular or oval public place (similar to a classic amphitheatre), with the function to show theatre, music or sports. It is based on a large open space, with all sides surrounded by seats for audience".

[9] A Wikipedia definition on *Domain* is: "… from french *domaine* landed property or estate, from latin *dominium* (with the same meaning)".

[10] MNIOE – the Multinational Information Operations Experiment Group. A Nato working group describing development of capabilities in Information Operation context

[11] Cognition is a collection of different mental (thought) processes. (*Source*: Wikipedia).

[12] Perception is a psychological concept formation describing processes which are active to interpret sensory impression to meaningful information, consciousness as well as unconsciousness (*Source*: Wikipedia).

[13] Emotion is a psycho-physiological condition for an organism to carry through some kind of actions (*Source:* Wikipedia)

manipulating messages varies between individuals and with time. Through training, an individuals readiness to handle different kinds of (misleading-) information could be developed.

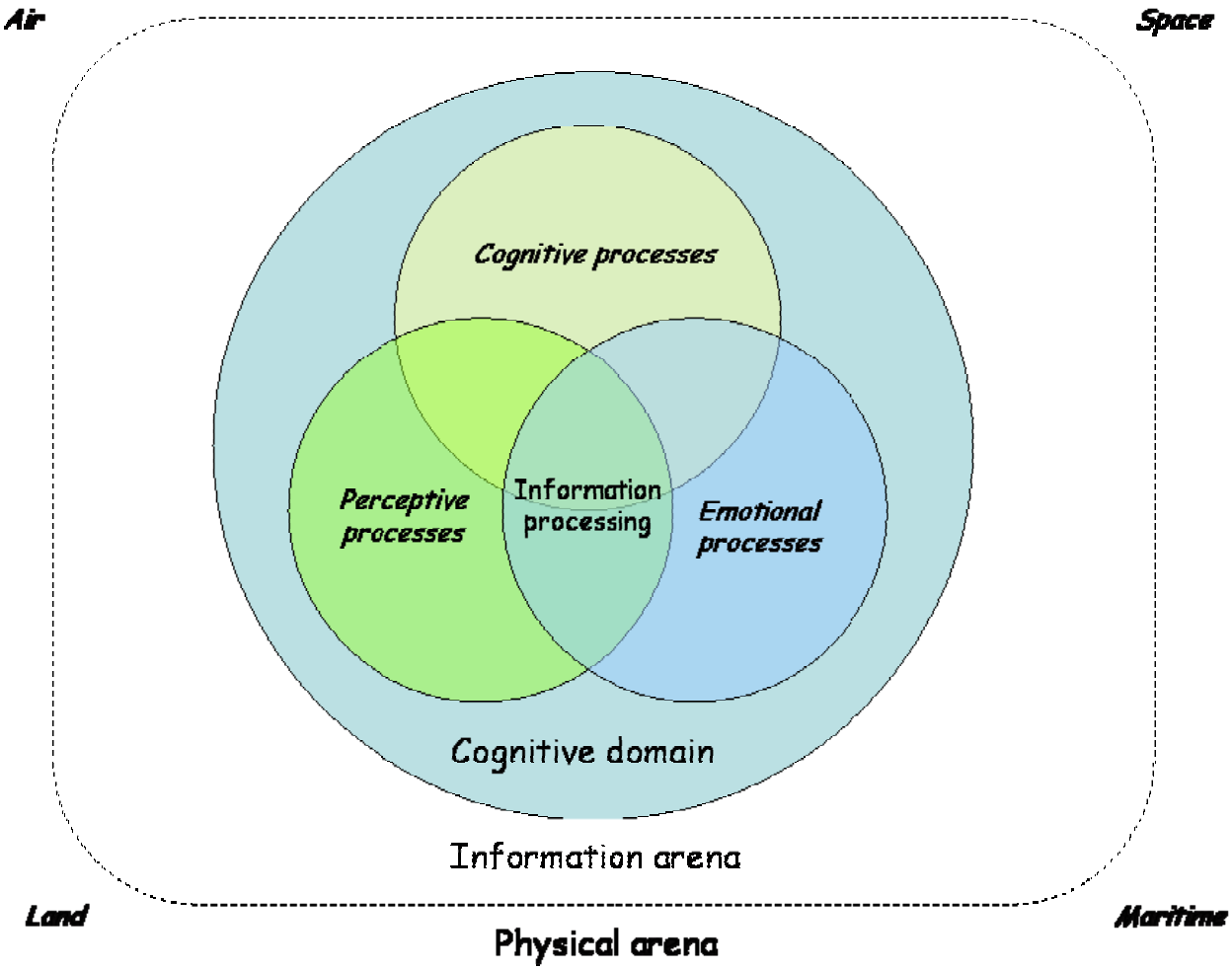

Figure 1. Relations between cognitive domain, information arena and physical arena

3.3 Effects of cyber attacks within information arena and cognitive domain

In a discussion about what should be concluded in the information arena it is also important to relate this to the effects that you would like to achieve or what factors that are in favour. Alberts [13] says that the purpose of the information arena is to:

- share information
- achieve increased consciousness
- achieve higher quality of information
- share situational awareness
- create self synchronisation and by that higher efficiency

Nunes [14] argues that there are three effects that may occur through information warfare (cyber warfare) and they are:

- **Physical effects**: physical destruction of information structure with the consequences that an operation cannot be fulfilled in a proper way because the information services could not be used fully (DOS-attacks[14]). A number of weapons and techniques could be used to knock out electronics; some of them are non-lethal EW weapons such as EMP[15] and RF[16].
- **Syntax effects**: the purpose is to attack the logic of the information system by delaying information and/or by developing "unpredictable" behaviours in information through, for instance, the introduction of viruses and trojans, and other hacking activities which include IT-weapons (CNO).
- **Semantic effects**: to destroy the trust in the system and information by manipulation, change of information and deception which may be harmful for the decision making process.

Nunes also mentions that one reason for having ones own capabilities within the information arena is to speed up the decision process. Information is a "force multiplier" which could be added to other capabilities within the physical arena. Moreover, the distance for operations could be increased meaning that new targets can be attacked with other means compared to the traditional arena.

The information arena is also sensitive to directed attacks. Alberts [15] writes that new types of threats and (new) actors of different kinds such as single states, security services and also criminals and NGOs etc could behave antagonistically. The ability to remain anonymous as well as the ability to hide motives and intentions will increase over time.

A fruitful way to structure the different effects and relations to the physical arena, the information arena as well as cognitive domain could be by using following effect-matrix:

[14] DOS – Denial of Service
[15] Electromagnetic Pulse weapons
[16] RF-Radio Frequency

Means for information warfare/cyber war (EW, CNO, PsyOps, InfoSec)	Physical arena (land, air, maritime, space)	Information-arena	Cognitive domain (cognition, perception, emotion)
Physical effects	Interruption, destroy electronics and sensors, affect transmission and access links, derive robots, system failure	Interrupted communication, denial of services; DOS	Fragmented communication, decreased amount of information, reduced analysis capability
Syntax effects	Hacking, cracking virus, trojans, spam, interception, exploit, bugging illegal misuse of information system	Attack logic of system, delay and distortion of information, saturation	Mistrust against system
Semantic effects	Mass medial maneuvers, planted information, mutilation of sensor data	Deception and manipulation of information (disinformation)	Changed situation awareness, mistrust against and questioned of information, inability for decision making

Figure 2. Effect-matrix showing relationship between different types of effects within information warfare, arenas and domains

3.4 Using the effect-matrix: communication jamming

This very simple example describes the principles underlying the use of the effect-matrix.

The Swedish Armed Forces are engaged in an UN-led operation with a reconnaissance unit. The purpose is peace on for some time protecting. There have been disputes between rebel units controlling large rural areas in the region and a democratic government controlling major cities. The rebels' technical knowledge is of quite high standard. HUMINT reports indicate that the rebels are equipped with different types of weapons including communication jammers. They have also access to a number of anti aircraft guns.

The objective for the Swedish team is to conduct mobile reconnaissance over a specific area controlled by the rebels. The terrain is rocky and difficult to control. In order to achieve the objectives, the unit uses UAVs.

In this example the physical arena consists of sensors, links and nodes. Cameras acts as sensors mounted on the UAVs. The UAVs are connected by radio to a ground station. The ground station is responsible for remote UAV controlling as well as for processing data to produce information such as pictures, video clips and text. The information generated will continuously be sent forward to the battalion and brigade staff. Within the staff, analysts use

the information at tactical, operative and strategic levels in order to increase the situational awareness.

The rebels could either prevent or obstruct the reconnaissance work with different means and methods, for example through jamming or destruction of the UAVs. The simplest method is probably to jam the radio communication between the UAVs and the ground station and so hinder or reduce data transmission. The anti aircraft guns could also be used to shoot down the UAVs.

The situation could be described in following effect-matrix:

Communication jamming

	Physical arena (land, air)	Information-arena	Cognitive domain (cognition, perception, emotion)
Physical effects	Jamming radio communication links, destroy UAVs, achieve system failure	Interrupted communication, denial of services; DOS	Fragmented communication, decreased amount of data and information, reduced analysis capability
Syntax effects		Delay and distortion of information	Mistrust against and questioned of information
Semantic effects			Affect analysts/operators ability for decision making, decreased situation awareness

Figure 3. UAV radio jamming and the effects on the information arena and cognitive domain

From this matrix we can see the potential effects that jamming might have on the immediate mission (reconnaissance using the UAV) and hence the impact on the wider objectives for the SAF brigade in the area. In this case, mistrust in the information from the system might lead to poor situational awareness at all levels. This might in turn lead ground reconnaissance to confirm or deny information received, which might require more time and possibly a larger force. Such a mission might also expose the SAF personnel to higher risks (e.g. attack by rebels) and might also increase tensions in the area at a time when the purpose of the SAF force to reduce tension and promote peace.

We can also see from the matrix that one way to reduce the immediate risks to the UAV missions and hence to the SAF mission as a whole is to make the UAV communications less susceptible to jamming so that the information reaching the SAF is uncorrupted. Another way of reducing the risks would be to fly the UAVs out of range of the rebel guns, and that this in turn might lead to a requirement for more powerful imaging systems on the UAV.

From this example one can see that the matrix can be used to study the effects of cyber warfare on operations and hence to use this to select and prioritise countermeasures for use during the operation.

4. Conclusions and future studies

Knowledge of war fighting in the digital battlefield is becoming more important due to the introduction of network centric warfare concepts. The key to success in cyberspace is to understand the prerequisites for conducting operations in the information arena and cognitive domain and its effects. But digital warfare on the new battlefield is complex and involves a wide range of capabilities and behaviours. Hence, there is a need for theories, methods as well as definitions that describe the new situation and its circumstances. A viable way to structure different cyber warfare capabilities and relate them to the physical and information arenas as well as the cognitive domain is to use the effect-matrix.

The matrix could be used as a tool in order to develop practical methods for information operations involving mixed capabilities such as electronic warfare, computer network operations and psychological operations. For instance, it is possible to exemplify through case studies deception and jamming of information with EW and/or CNO and its effects on information arena as well as cognitive domain based on the effect-matrix. In the paper one very simple example has been described showing communication jamming of UAVs. In future studies the matrix could bee develop further involving a wide range of capabilities in different scenarios.

References

[1] Parks, R., Duggan, P. (2001). Principles of Cyber-warfare. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. United States Military Academy, West Point, NY, 5-6 June, 2001. ISBN 0-7803-9814-9

[2] Heickerö, R. (2005). Some thoughts on the Application of Military Theory to Information Operations and Network Centric Warfare. IO Sphere Journal. Fall 2005. Joint Information Operations Centre. San Antonio, CA, USA

[3] MNIOE White paper- Information Operations (Info Ops) in Future Coalition Operations. 2005, Version 1.6

[4] Gartska, J (2000) *Network centric Warfare: An Overview of Emerging Theory*. http.//www.mors.org/publications/phalanx7dec007feature.htm

[5] Heickerö, R. et al (2004). Telekrig i breddad hotbild. Underlagsrapport. FOI-R—1370--SE

[6] Parks, R., Duggan, P. (2001). Ibid.

[7] Parks, R., Duggan, P. (2001). Ibid.

[8] Nunes Viegas, PF (1999) *The impact of New Technologies in Military Arena: Information Warfare.* Conference paper: International Congress of Military Press, Lisbon 13-16 September 1999.

[9] Nunes Viegas, PF (1999) Ibid.

[10] Nunes Viegas, PF (1999) Ibid.

[11] Gartska, J (2000) *Network centric Warfare: An Overview of Emerging Theory*. http.//www.mors.org/publications/phalanx7dec007feature.htm

[12] MNIOE White paper- Information Operations (Info Ops) in Future Coalition Operations. 2005, Version 1.6

[13] Alberts (1996). The unintended Consequences of information Age technologies. NDU Press Book. www.ndu.edu/inss/books/uchome/html

[14] Nunes Viegas, PF (1999) Ibid.

[15] Alberts (1996). The unintended Consequences of information Age technologies. NDU Press Book. www.ndu.edu/inss/books/uchome/html