

**10<sup>th</sup> International Command and Control Research and Technology  
Symposium**

**The Future of Command and Control**

**An Operational Framework for Battle in Network Space**

**Final Paper #173**

**Topic area: Information Operations / Information Assurance**

LCol Rob Knight  
Deputy Commander  
Canadian Forces Information Operations Group HQ  
3545 Leitrim Road  
Ottawa  
K1A-0K4

Tel: 613-995-0151  
FAX: 613-945-0199  
[Knight.RDL@forces.gc.ca](mailto:Knight.RDL@forces.gc.ca)

Dr. Mark McIntyre  
Head, Network Information Operations  
Defence R&D Canada – Ottawa  
3701 Carling Ave  
Ottawa, ON

Tel: 613-993-9963  
FAX: 613-993-9940  
[mark.mcintyre@drdc-rddc.gc.ca](mailto:mark.mcintyre@drdc-rddc.gc.ca)

POC: Mark McIntyre

# **An Operational Framework for Battle in Network Space**

LCol Rob Knight  
Deputy Commander  
Canadian Forces Information Operations Group HQ

Dr. Mark McIntyre  
Head, Network Information Operations  
Defence R&D Canada – Ottawa

*“Thus, what is of supreme importance in war is to attack the enemy’s strategy”<sup>1</sup>*

-Sun Tzu

## **Abstract**

In modern network enabled operations, information networks are becoming so critical to the efficient and effective execution of military missions that failures in the network may lead directly to mission failures. The purpose of this paper is to make the case that the network is actually a space within which military art must be practiced. Forces must be able to sustain, protect and defend themselves in the network environment just as they have always done in physical environments such as land, sea and air. To this end we provide an initial overview of both network-enabled operations and information operations and attempt to draw direct analogies between protection and defence in physical space and cyberspace. We then show in some detail how Leonhard’s principles of war apply to the network environment. We hope to lay a conceptual framework for battle in network space with a focus on a keystone requirement for an intuitive, operational network awareness view for military decision makers.

## **1. Introduction**

“It was a time of major technological changes – with improvements in tanks, planes, and electronic warfare – leaning to new doctrines that would optimize their use (e.g., blitzkrieg). Those who recognized that this was an interwar period thought through the conceptual problems of the day and achieved striking success in the opening phases of World War II – most notably, the Germans.”<sup>2</sup>

The purpose of this paper is to give forewarning that the modern computer network has grown in sophistication to such an extent that it is tied to our everyday world in the same manner as the ground under our feet. Indeed, once the conceptual problems of today are thought through, the advocates of cyberspace will eventually bring the battle to us. The intent is to reflect upon these ideas and provide structure to the current approach of, “defend as well as one can afford to and be prepared to adapt and recover as quickly as possible if the defenses fail.”<sup>3</sup> It is very interesting that this quote, made in a

Rand Corporation: “Strategic Appraisal: The Changing Role of Information in Warfare”, in 1999, presupposes the ability to adapt, recover and defend in a cyber environment.

This paper has been written as a concept document to discuss the emerging subject of battle in network space. In the past, much work has been directed at the use of network technologies to enhance military mission effectiveness in conventional battlespaces. Within the air, land, sea and space arenas, networks are seen as principal enablers for improved, team focused decision making among warfighters at the tactical, operational and strategic levels. Indeed, information networks have become so important that many modern military tacticians, commanders and logisticians would be crippled without them and many modern military capabilities would be degraded. However, the heavy reliance of modern western forces on networks, and network applications, together with the information processing and sharing they enable, brings with it new vulnerabilities. This is especially true when the networks are heavily based on widely understood, commercially available hardware and software, or when network services are purchased from commercial suppliers. Because of these vulnerabilities, networks have become a new space in which warfighters must operate.

In the paper, we discuss information operations in the context of Waltz’ three-tier model of physical, information and perception effects. From this, we focus on the second tier – information. Clearly the Network is the chief enabler to this conceptual tier and thus is a key enabler for the foundation of information operations as a whole. In the context of Network Centric Warfare (NCW), as discussed in the work by CCRP,<sup>4</sup> we will draw out the difference between networks as enablers to human performance designed to enhance conventional physical battle and the network as a space in which battle is conducted. With this as introduction, we will then provide an argument that the network environment is a battlespace within which maneuverist concepts can and should be applied. Ultimately, we make the case that there is an urgent need for an intuitive, operational “Network Picture” upon which sense, act and shield decisions can be made for networks and where aspects of network battle can be modeled and war-gamed. To provide a clear and intuitive military argument, the paper uses the framework of a main defensive battle for a major land formation and applies this metaphorically to network space. As such, the thread of the argument moves through the structures of the defence and discusses the need for a potent counter penetration capability as well as making the argument that the defender must be able to manoeuvre within the Global Information Grid (GIG). Overarching all of this is the requirement for an extensive integrated Computer Network Intelligence, Surveillance and Reconnaissance (CN ISR), a capability that will be defined in this paper. Essentially, the end state is the net-enabled network.

In Section 2, we set the scene for discussion through a brief overview of Network Enabled Operations the term used in Canada for concepts referred to as NCW the US and Network-Enabled Capability in the UK. In Section 3, we continue with a discussion of Information Operations at the human and physical levels before focusing on information operations at the information level. In this section we draw analogies between protection and defence of physical space and protection and defence of information and information processing resources on the network. Through these analogies, we begin the argument

that the network needs to be viewed as a separate space in which battle is fought. The heart of the paper begins in Section 4 where Leonhard's principles of war are presented and then, in Section 5, this is discussed in detail in the context of network battle.

## **2. Network Enabled Operations**

The term network conjures up different inference for different people. For many, the term network is inherently a human concept that describes the cognitive and social interactions among groups of human beings. For others, networks are inherently physical and describe such things as energy or water distribution systems or transportation infrastructures for physical goods. Most recently the term network is used by many to refer to the hardware and software that make up the information processing and distribution systems that enable information sharing at the local, metropolitan and the wide area levels, both nationally and internationally [16].

The term Network-Centric Warfare (NCW) is frequently used in modern military literature to denote the synergy and effectiveness gained by interconnecting decision makers at all levels. The term implies a collaborative, shared information environment achieved through the deployment of a robust, responsive and secure information networks. These net-enabled command and control structures support spatially distributed military Commanders with a more effective framework for command, planning and decision-making in combat. The substantial increases in information transactions allow for the collection and distribution of intelligence supporting improved C4 ISR and therefore situational awareness. Finally, information velocity has increased to the point where what was done in hours can be done in minutes or seconds. In the UK, these ideas are embodied in the concept of Network Enabled Capability (NEC) while Network Enabled Operations (NEOps) is used in Canada. In this paper we will use the term NEOps.

Many of the best examples of NEOps come from the improved effectiveness and survivability that can be achieved in a strike mission through multi-platform cooperative engagement and precision strike with over-the-horizon targeting. In these examples, information networks are enablers for tactical decision-making in the traditional end-game of tactical strike. However, information networks are also critical enablers in collaborative decision-making at the operational and strategic levels as well as in just-in-time sustainment operations. Furthermore, as we have discussed, information networks are an essential component in the collection, process, analysis and distribution of information in support of the situational awareness for all human decision making.<sup>5</sup> The pivotal role of the 'human network' in military decision-making and the subordinate role that information networks play in enabling human networks, demand that the concept of waging war within these networks be seriously considered. In the next section we introduce information operations and how they can be applied at these levels.

### 3. Information Operations

For many, warfare is associated with the use of physical force to accomplish some physical effect. However, the physical effects of war are most often planned as a means to larger goals that are psychological, social or cultural in nature. The term “information operations” was coined to refer to operations at the physical, information and human level that complement or replace traditional military physical effectors in pursuit of the same outcomes. This is clearly seen from the Chinese perspective, which concludes, “the main tasks of IO are disrupting the enemy’s cognitive and trust system.”<sup>6</sup>

The Canadian definition of information operations, which is similar to the US definition, focuses on the achievement of national objectives by affecting the quality of information upon which decision-makers base their decisions.

*IO is defined as: actions taken in support of national objectives that influence an adversary’s decision makers by affecting other’s information and/or information systems while exploiting and protecting one’s own information and/or information systems and those of our friends and allies.*<sup>7</sup>

Such influence can be achieved in many ways at different levels of decision-making through either direct manipulation of information or by indirectly influencing the way in which it is processed or perceived. Figure 1 illustrates the full spectrum of information operations in a three-layer model as described in Ed Waltz’ book: “Information Warfare Principles and Operations.”<sup>8</sup>

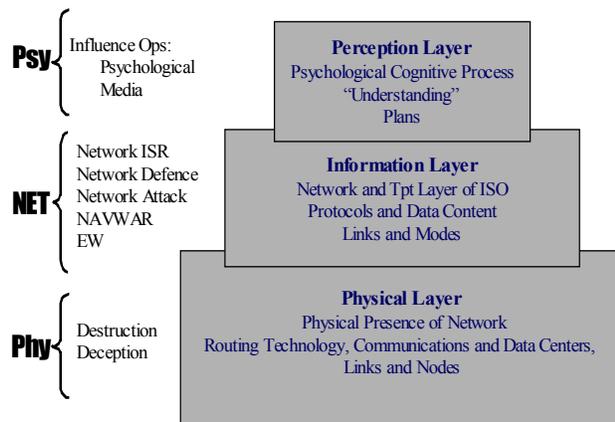


Figure 1: An Operational Model for Information Operations

In the following three subsections, we discuss information operations at the human and physical layers before focusing on information operations at the information layer, which is the main topic of this paper.

### 3.1 Physical-Layer Information Operations

A good example of information operations at the physical layer is stealth. Through careful design, military platforms such as aircraft, ships or tanks can be made less susceptible to detection using passive or active techniques, based on radio-frequency, acoustic or optical emissions. Through signature management techniques, military platforms can reduce the likelihood of detection by sensors' suites, thereby reducing the likelihood that they will register on the opponent's situational awareness picture. The intent of stealth is a physical masking of the platforms signature. This physical form of IO protects the platform from ever entering the decision cycle of an adversary.

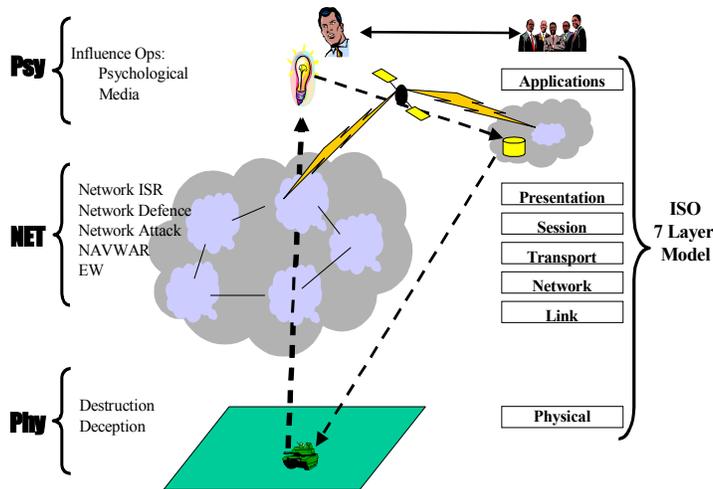


Figure 2: Mapping Information Operations to The Seven-Layer Model of Networks

### 3.2 Human-Level Information Operations

The formation and sustainment of effective teams or coalitions is fundamental in warfare at all levels of decision-making, from tactical, to operational, to the strategic. Non-physical actions, directed towards either individuals or groups, which influence either how they perceive or how they deal with information, is considered information operations at the human level. The Media, “CNN effect”, and direct Psychological Operations are the most obvious; however, commercial contractor organizations and even the work of NGOs can have great influence. Although information operations at the human level is not the focus of this paper, we must remain mindful of the fact that physical and information networks exist to support teams of human decision-makers, or human networks. The primacy of support to these human networks must often be considered when making effective information operations decisions at the physical and information layers.

### 3.3 Network Information Operations

A fundamental component of communications and networking is the point-to-point link between two humans. Two common examples of this are face-to-face conversations and the public switched telephone system over which voice and/or data can be passed between two end points. In these examples, a physical layer communication channel exists between the two end-points once a circuit is established. For face-to-face conversations, the channel is acoustic in open air while an established circuit in the telephone network can consist of a variety of wired or wireless links. However, modern packet-switched networks, such as the Internet, facilitate more sophisticated information sharing over large geographical areas by introducing a number of information layers between the physical communication channel and the end-users. The focus of this paper is to define how Network Enabled Operations concepts can be applied to these information networks.

The introduction of the middle layers of the model shown in Figure 2 has resulted in unprecedented flexibility and spatial coverage to the information sharing process compared with circuit-switched systems. However, with this flexibility comes a degree of uncertainty in the flow of information packets across a network. In diagrams that illustrate networks, this uncertainty is often represented in the form of a network cloud as illustrated in Figure 2. The use of the cloud indicates that information packets can be passed between the two end points within specified tolerances for packet capacity, latency or other qualities of service for packet delivery. Figure 2 illustrates a large network comprised of five smaller networks connected in some known topology and linked to a geographically separate network via a wireless bridge such as a satellite link.

While the topology of the network cloud in Figure 2 is usually unknown to those who require the network services it provides, the network is constructed based on open-standard network, transport and application protocols and software with a large and evolving set of well-known vulnerabilities. These vulnerabilities, together with the fact that the network “clouds” are openly accessible to many who may harbour malicious intent, demonstrates the seriousness of information security.

To draw an analogy between traditional warfare in physical space and war in network space, we must first discuss a typical military scenario where a force is tasked to protect and defend a physical enclave or safe haven. In Figure 3, a battlespace is depicted where a “High-Value Force” must be protected or defended. An important aspect of force protection and defence is to first identify the boundaries of the area that must be protected and then determine the likely avenues of approach. Based on an understanding of the terrain, ground cover and enemy intent, observation units are deployed to monitor movement through these areas. Additionally, other protection and defensive devices such as obstacles, minefields, or blocking forces can be deployed along the boundary of the enclave. Proactive defence of the enclave by military forces also involves deployment of reconnaissance teams outside the boundaries of the physical space to be protected. Figure 3 provides a perspective of this against the background of a map. The purpose of these tactical forward elements is to detect, localize and identify potentially hostile

activity before it becomes a problem. These tactical elements may deal with minor hostile activities themselves or may provide targeting information for a standoff attack if required. These analogies also apply to protection and defence of networks.

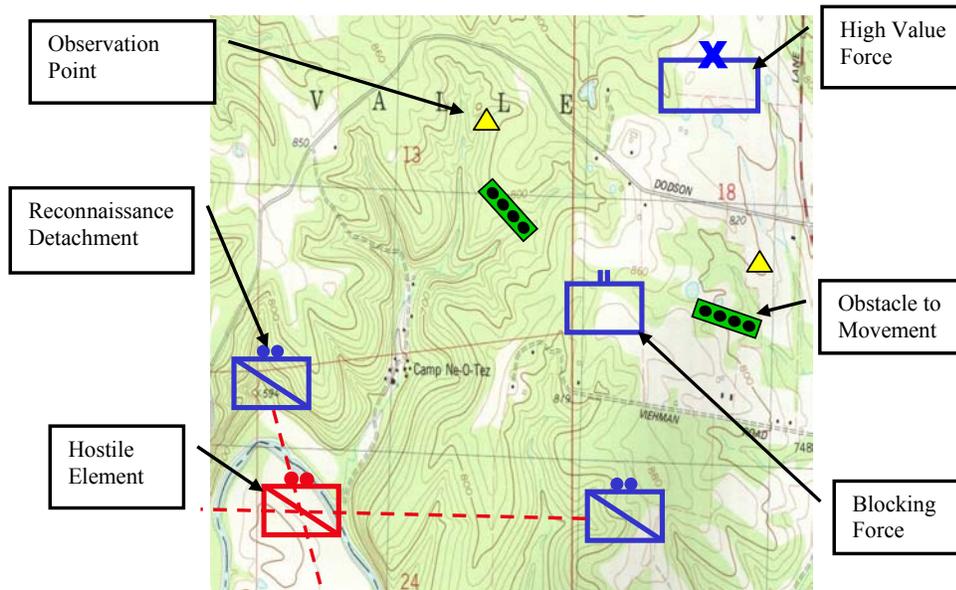


Figure 3: Protection and Defence in Physical Space

Analogous to the way armed forces routinely deal with security of physical spaces, Figure 4 illustrates a number of commonly employed practices for protection and defence in network space. The arrows labelled “avenues of approach” are the access points where a known local-area network accesses wide-area networks. Identical to our analogy of protecting enclaves in physical space, it is necessary to understand the likely avenues of approach to the protected network. In a network, it is at these points where network boundary control devices, such as firewalls and guards, are best employed. Moreover, secure network enclaves are designed so that all traffic destined for, or originating from, points outside of the trusted enclave pass through controlled access points.

The analogy to the blocking force shown in Figure 3, is the Computer Incident Response Team (CIRT) shown in Figure 4 and it is typically tasked to monitor traffic at the network access points. The teams are responsible for detecting and dealing with any incursions into the protected network. In a similar fashion, Figure 4 shows Computer Network: Intelligence, Surveillance and Reconnaissance (CN ISR) teams. As with the reconnaissance detachments in Figure 3, the CN ISR teams are deployed outside the boundaries of the enclave being protected. In the case of the network, these teams may be software agents rather than human teams but having the same purpose. The CN ISR agents would be tasked with detecting and identifying potential malicious activity before

it became a problem for the CIRT at the network boundary. Also shown in Figure 4 is a potentially hostile agent within the controlled boundaries of the network - representing either successful penetration of the enclave or the “insider threat”. Insider threat appears to be a much more serious consideration in Network space than in the traditional physical space. One reason for this is that the insider is often a malicious software program and not necessarily a malicious human being.

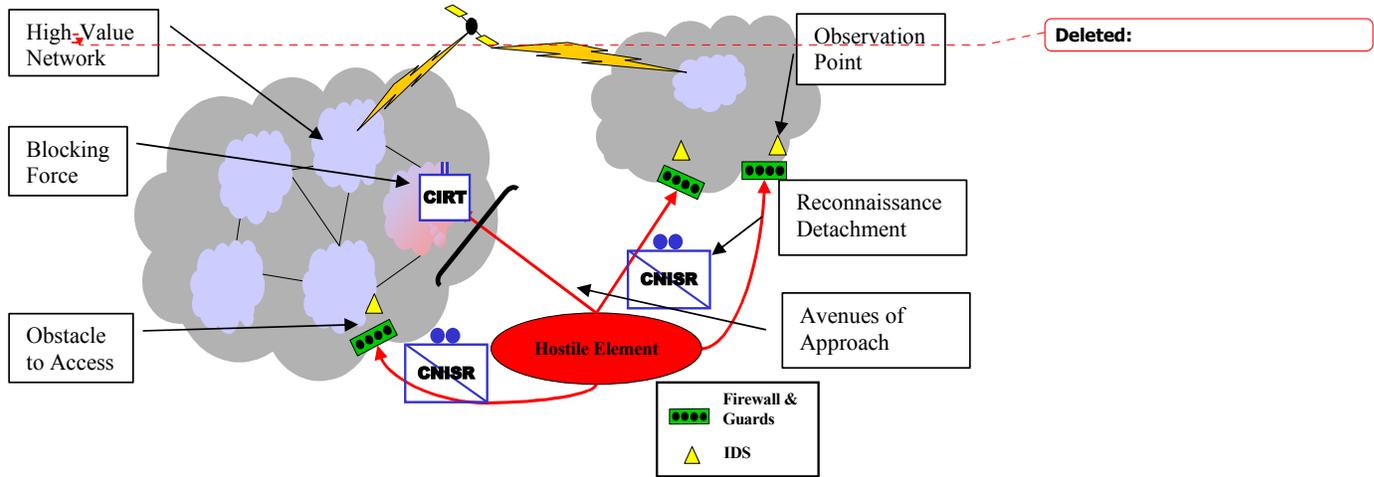


Figure 4: Protection and Defence in Network Space

#### 4. Leonhard’s Principles of War for the Information Age

To aid us in the development of the argument that the cyber ‘environment’ actually is a ‘space’ within which battle can take place, it is necessary to demonstrate the principals of modern warfare can be applied. To form this argument, we will use Leonhard’s principals of war for the information age, which exemplifies three overriding laws of conflict, or warfare: The Law of Humanity, the Law of Economy and the Law of Duality. [14]

First is the Law of Humanity, which states that all conflict is essentially a clash between human wills and is not necessarily a measure of the might of machines or doctrine. There are many examples where a powerful opponent was beaten by an underdog winning the hearts and minds or crushing popular support; US/Vietnam, Soviet/Afghanistan, French/Algeria are recent additions. However, this strategic approach has been used since the time of Genghis Khan and further back to Sun Tsu. Contemporary theorists have repeatedly observed that power does not exist in the absence of relationships: power is a relation among people, not an attribute [of a person] or a position.<sup>9</sup>

The Second Law, the Law of Economy, is the most intuitive for most military thinkers as it deals with the effective and efficient use of resources. However, one must

not only look at the material and human resources; it is just as important to consider both time and information as key aspects of economy. It will be these later two aspects that are most impacted upon in the cyber environment. In the military realm, those who master information technology have the potential to multiply lethality and mobility as well as provide leaner logistic tails for their armed forces. This means that that they can trade in ‘mass’ for quality and come out way ahead.<sup>10</sup>

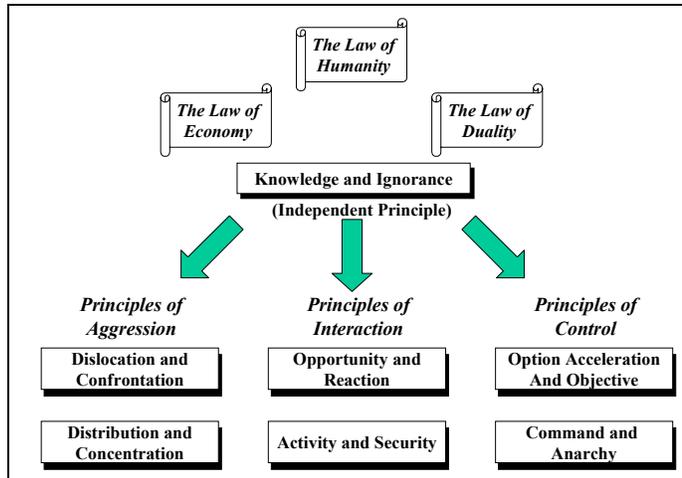


Figure 5. Leonhard’s Principles of War for the Information Age<sup>11</sup>

The Third Law, and least intuitive of the concepts, is the Law of Duality. This law provides for the “cat and mouse” game that is forever present in conflict. Duality essentially provides the solution to the contest between the ‘attritionist’ and ‘maneuverist’ camps of thought. Attritionist theory pits strength against strength in symmetry while the maneuverist uses asymmetry to apply strength against weakness. The difficulty with these camps is that it is not possible to purely conduct only one of these doctrinal approaches in real battle. Simply, the solution is that asymmetry cannot exist without symmetry. The concept is linked as for ‘light and dark’ – one means nothing without its opposite. Thus, this law states that conflict must have a dual nature whereby the conditions set by any one strength also provides for the circumvention of that strength thus providing tactical or operational opportunity. Obviously, the solution is neither forgoing all strength nor is it practicable to be strong everywhere. Further, when exploiting enemy weaknesses the question must always be asked, what happens when my own asymmetric stratagem meets its like? – the answer, of course is symmetry. The genius of military operational art is finding the balance between the duality of dislocation and confrontation?<sup>12</sup>

### 5. Leonhard’s Seven Principles Applied to Cyber Space

The Seven Principles that are formed from these three Laws are deconstructed as shown on Figure 5. It is noteworthy that the first and foremost of these principles,

Knowledge and Ignorance, is highly esoteric and a highly human oriented principle. From the Laws and this first principle, the six subordinate principals form three groups: Aggression, Interaction and Control. It is also noteworthy that there is always a duality shown in each of the principals. This provide the necessary contention between strength and circumvention, or between the symmetric and the asymmetric. To establish that these principles are active in the cyber environment, a metaphor to the Land Environment will be used to demonstrate cyberspace as a battlespace. The “metaphor” is used since it appears to be the most popular tool to describe cyberspace. Most notably among the figurative images are the human immune system (viruses), the Wild West with the concept of individual sovereignty, and the Medieval World with the enclaves, firewalls, guards and other cyber fortifications.<sup>13</sup> This paper attempts to capitalize on the practice of using figurative language by using the Main Defensive Battle to describe the emerging space defined by computer network interconnections and integration.

### **5.1 Knowledge and Ignorance:**

The first principle to consider is Knowledge and Ignorance. Essentially, this principle states that knowledge is expensive and ignorance is free. However, what is the real value of collecting, processing and analyzing the last 50, 20 or 10% of the information? Is this value actually worth what it costs the decision-maker? Is it necessary for the decision making process?<sup>14</sup> Knowledge gained within a conflict is understood to cost both material and men but it also costs time, and in the cyber environment, time is very expensive! In Industrial Age warfare of the 19<sup>th</sup> and 20<sup>th</sup> centuries, ignorance of the battlespace was common, typified as friction by Clausewitz. The current observation is that this has been replaced by entropy.<sup>15</sup> In our current world, there is so much information at the command level that containing it and organizing it in one human mind is a feat. The myriad of information elements acts entropy-like and takes time and energy to consolidate. The essence of this principle is to minimize one’s own entropy while fostering it for the enemy.

To combat this information fatigue the soldier on the battlefield asks the age-old questions:

“Where am I?  
Where are my buddies?  
Where is the enemy?”<sup>16</sup>

In modern, physical NEOps the first of these questions has been answered by a topographical map with satellite-enabled geopositioning to within a few meters on the globe. In network space, this same situational awareness, or map, is less spatial than it is logical in nature. Such network maps define network interconnectivity and logical space, which is then displayed in Network Operations Centers (NOCs). This is not as advanced as its spatial counterpart; however, there is much R&D work being done to develop intelligent and intuitive modeling and visualization tools that will work in near real-time for situational awareness of cyberspace.<sup>17</sup> The second and third questions relate to the difficulty of not only understanding the ‘map’ but also understanding the players or actors on the map. ‘Where are my buddies’, is a matter of increasing the collaboration of

friendly actors in reporting both activity and architecture. ‘Where is the enemy’, states the requirement for precision sensing and corroboration of activity on both our own networks as well CN ISR on the ‘approaches’ to our networks through the GIG. Clearly, if the information system is to be of operational use eventually it must interact with the GIG. Even the secret information systems must use this transport system.<sup>18</sup> This realization brings us to the discussion of the main defensive battle of cyberspace and Leonhard’s remaining principles. Just as the principle of Knowledge and Ignorance is central to Leonhard’s model and the subordinate principals, the concept of CN ISR is central to the remainder of this argument.

## 5.2 Distribution and Concentration

The opposing concepts of Distribution and Concentration work together in battle to insure sufficient power is brought to bear with significant purpose. Spatial distribution and concentration are influenced significantly by the law of economy and the situational awareness information available to the Commander about both his own and his opponent’s forces. Temporal distribution is essentially the concept of pre-emption, meaning time is not taken to mass as much power but the timing of the attack is used to provide strategic advantage such as surprise.

Distribution and concentration of force in a classic defensive construct are commonly conceptualized as depth, achieved by providing the enemy with a progressive number or increasingly complex obstacles. Strength without depth provides a Magniot Line model where the an opponents strength can be probed and assessed for weakness over time and then completely dislocated by an attack that renders that strength impotent, thus the Ardennes. Figure 4 is a network depiction of such a defensive situation and unfortunately, the most common form of defence used in network space.

To gain access, the ha-ttacker uses probes, just as an enemy would approach a physical defensive line; however, since there is no delaying force set outside of our networks, the enemy is free to probe over time. Once the enemy wishes to make a move, the network environment allows rapid massing of effects to distract the targeted organization (nation state, business, criminal...) into reacting. This serves to confuse the defender who can only confront portions of the attacks. This leaves the aggressor open to act with impunity in other more important areas of interest. This is a classic example of functional dislocation and has been labelled “Cyber Swarming”.<sup>19</sup>

The proper defence for such a situation is the same as it is for the physical battlespace – a defence in depth! Like a physical defence in depth, a properly prepared network defence should have relatively light defence at the periphery to keep out the common or unsophisticated attack. Then, further within the Network, the more sophisticated attacker can be dealt with using more skilled people and sophisticated methods. The most survivable organization is the one that is best able to mass effects or absorb attacks with little real impact on the operation of the network.<sup>20</sup>

As Figure 4 depicts, the network has its own minefields and observation posts. In physical battle these minefields do not serve the purpose of destroying the enemy in themselves, but work to delay or break the momentum of the enemy advance. The network firewall serves this same purpose as these obstacle fields; however, instead of hindering the spatially oriented 'advance' of the enemy, it delays the enemy's access. In both cases there is no question the obstacle will be breached but it is a matter of when.

So, if they are going to breach anyway, why bother with the obstacle? Because the time the attacker takes at the obstacle will provide a window of opportunity for the defence to detect and act. Therefore, an obstacle without some sort of observation or monitoring serves only as a nuisance and contributes little to the defensive posture. In network space, the Intrusion Detection Systems (IDS) serve as the observation on the obstacle. Moreover, a human firewall must also be considered. A system or network can, and should, be decomposed into sub-systems or safe havens and then, when an attack is imminent, defensive measures can be emplaced such as we have on the network periphery.<sup>21</sup> Such a situation is depicted in Figure 7 and allows for progressively more difficult obstacles to be set before the attacker. Since only the more sophisticated attackers make it through the periphery, the highly skilled Computer Incident Response Teams (CIRT) or the blocking force, can economize effort and can be brought to bear on only what is necessary. Thus the din of the 'swarm' is held back at progressively more difficult lines of defence. However, there is also the presupposition that a cyber ISR function exists to provide a clear picture or top-sight necessary to shape the attacks and continue the canalization of the opponent.

### **5.3 Dislocation and Confrontation**

Once the opponent has been channelled by our depth, what is to be done with him? – how is this situation reversed? The answer to these questions is found in our next principle: Dislocation and Confrontation. This is truly the central concept of maneuverist theory. This is the art of rendering an enemy's strength irrelevant. Once the enemy's strength has been set aside, the friendly force is free to attack through weakness to bring about defeat. Confrontation. This can be achieved through four main methods. Functional Dislocation – creating a dilemma; Positional Dislocation – manoeuvre; Temporal Dislocation – surprise; or Moral Dislocation – attack will.<sup>22</sup>

We have already broached this concept while discussing cyber swarming attacks on our network. The enemy's attempt to create a dilemma for us at our periphery we have dealt with by using depth. Now it is time for us to reverse the tables and provide our own dislocation. Before we continue, it is useful to make reference to our physical battle space and ask the question: how is this accomplished? One answer is the Killing Zone (KZ). In physical battle the KZ is used as a positional dislocation of the enemy. In this tactic, the enemy is permitted to advance and believe that he is gaining advantage but the advance is by design and is being slowed and finally blocked by friendly forces. Then at the point when the enemy is halted and therefore vulnerable, a counter stroke is launched using pre-planned tactics on favourable ground – the enemy is out manoeuvred.

What is the Network KZ? Figure 6 provides a conceptualization of just this. In this construct honeynet<sup>i</sup> technology is used to provide a ‘pocket’ within which the attacker can seem to manoeuvre and exploit perceived successes. Within the ‘pocket’ a highly sophisticated defence is being fought. The defence is comprised of a honeynet which shapes and channels the attackers’ efforts. First, the defender is able to monitor functionality and traffic, and even conduct payload extraction. If the honeyed network is sophisticated enough, it would also be possible to correlate and analyze attack signatures in real time and learn attack profiles without being dealt any real damage. This in itself has incredible potential for trend analysis or early warning and prediction.<sup>23</sup>

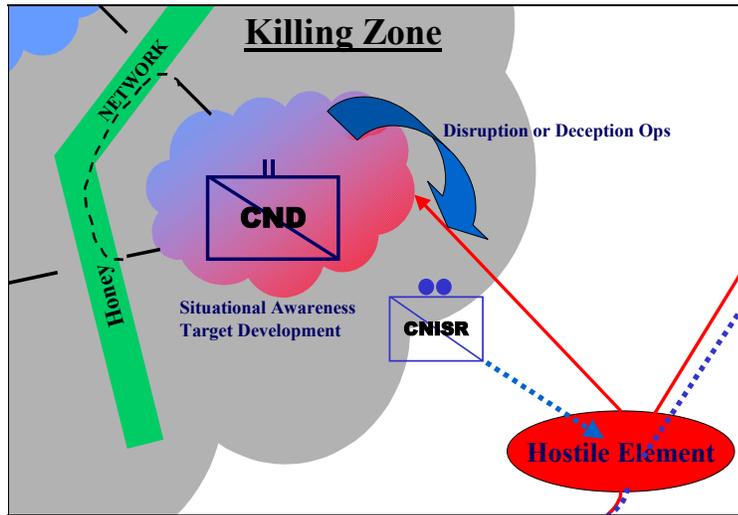


Figure 6. Cyber Killing Zone

Of course, to be realistic such a system would require the ability to be rapidly reconfigured, have real-time honeynet analysis and imaging, near real-time code reverse engineering, and its own covert hacking tools. Since such a capability is not realistic because of issues such as data overload, false positives and negatives, resource constraints or quantity of knowledgeable defenders to mention a few; other measures must be borrowed from the physical battlespace.<sup>24</sup> Essentially the cyber defender must be able slow down the aggressor or create a “sticky honeypot”<sup>25</sup> and be able to initiate

<sup>i</sup> A Honeynet is a network, placed behind a reverse firewall that captures all inbound and outbound data. The reverse firewall limits the amount of malicious traffic that can leave the Honeynet. This data is contained, captured, and controlled. Any type of system can be placed within the Honeynet, to include those systems that are currently employed on the network that the Honeynet is intended to protect. Standard production systems are used on the Honeynet, in order to give the hacker the look and feel of a real system. A Honeynet is a network that is intended to be compromised, to provide the system administrator with intelligence about vulnerabilities and compromises within the network.  
*John Levine, Richard LaBella, Henry Owen, Didier Contis, Brian Culver “The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks”, Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY June 2003, page 2.*

his own attacks on the opponent, either covertly or overtly, to delay or disrupt. Indeed, a diverse inventory of weapons that rely on different technologies and effects would appear to be particularly important.<sup>26</sup>

Such a defence can “even be taken one step farther. If an attacker knows your organization is using honeypots, but does not know which systems are honeypots and which systems are legitimate computers, they may be concerned about being caught by honeypots and decide not to attack your organizations. Thus the honeypot deters the attacker.”<sup>27</sup>

#### **5.4 Activity and Security**

Once inside the KZ, what prevents our opponent from breaking out of the pocket and running amok? Of course, the answer is found in the principle of Activity and Security. This concept is kin to concentration and distribution as it deals with economy; however, in this case, security can be described as any capabilities used for the purpose of force protection and therefore are unavailable for the true “activity” – advancing the Commander’s Plans for defeating the opponent. Again, the principle of Knowledge and Ignorance weighs heavily in this situation since the more knowledge you have about the state of the enemy, the more efficient the allotment of power between activity and security.<sup>28</sup>

The Security problem in Cyberwar is much more intrusive than one may consider on first look. Not only are hacking tools and Internet vulnerabilities of serious concern but there is also the problem of procuring secure hardware and software. “This becomes particularly difficult when trends in defence industry are forcing all defence firms to compete and diffuse their civilian and defence know-how and products globally to survive.”<sup>29</sup> Essentially this means that a single software product could contain modules of code created in the US, India, Singapore and France or perhaps other more distressing points on the globe. How do we provide security to such an environment?

The current cornerstone for cyber security is embedded in the system of Certification and Accreditation (C&A). This system, created by law enforcement principles, essentially compiles case files of proof that a crime, that has not yet been committed, is unlikely to be committed. This is then multiplied by the number of potential crimes that are currently being envisaged. The snapshot provided in the end requires an endless necessity for either money to be spent on mitigation or for the operational authority to accept some esoteric ‘residual risk’. Clearly defined best practices for security are important; however, the real need is a systematic intelligence preparation of the battle space (IPB) and a proper defensive framework constructed.

Borrowing from our defensive metaphor, there is a clear requirement for Cyber Rear Area Security. Such a security philosophy builds upon both the best practices from the C&A as well as the concepts of depth and safe havens discussed earlier. To ensure survivability, the network space must be severable. Once the network is penetrated it must be possible to reconfigure it such that the network defenders can exploit the severed

pocket. Now, at a heightened state of vigilance, the subdivided network safe havens can be protected in a defence in depth. To ensure the safety of the security posture there must be teams conducting rear area security as depicted in Figure 7. Network Vulnerability Analysis Teams (NVAT) provide the eyes and ears to determine the accuracy of the cyber map at any given time while a Red Team is engaged to keep the Information System Security Officers (ISSO) of the safe havens informed on their procedural and technical situation. Indeed, all of this forms part of the Cyber Rear Area Security net.

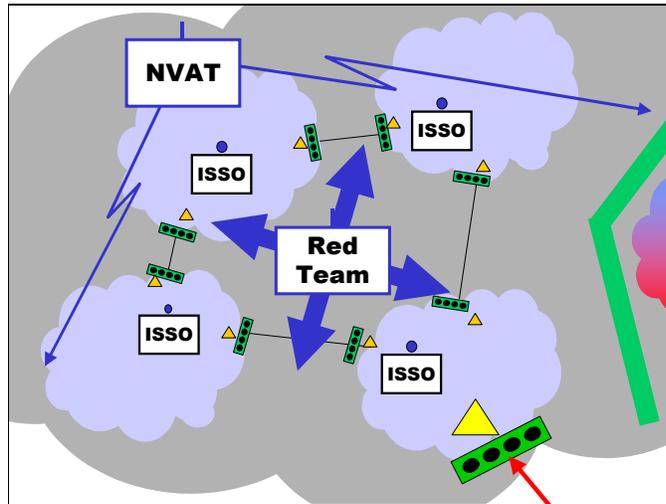


Figure 7. Cyber Rear Area Security

Within these safe havens, the ISSO is responsible for the monitoring and maintenance of security policies. Personnel and procedural security must be enforced and tools such as security compilers and run-time monitors must be engaged to ferret out blocks of dormant code that could contain trap doors or software weapons. If all of the best practices available to the security officer are in effect and done properly, it is almost impossible to “hack” into a system from the outside and even an insider would have great difficulty. One of the reasons for this is that the human in the loop provides inefficient and erratic behaviour therefore denying the hacker a predictable environment. Therefore, it is advisable to maintain a skilled and experienced team of ISSOs and planners to form a cyber battle staff.<sup>30</sup>

## 5.5 Opportunity and Reaction

With the opponent detained in the KZ, it is now necessary to address the true aim of the defensive battle – getting the upper hand! “In the past, armies [or commanders] have often relied upon the mystical notions of offensive operations or initiative as the best way to recapture opportunity. But classic concepts of initiative exist, and only have meaning, in the context of ignorance.”<sup>31</sup> Creating opportunity is the essence of what is referred to as freedom of action. The dual nature of such a principle provides that there is

a wrestling match between reacting to the enemy's actions and taking action to force the enemy reaction, thus creating opportunities for friendly forces to act with impunity. Earlier in this paper the attacker demonstrated this principle with the cyber swarming tactics used to attempt to confuse us, so that he would be free to pursue deeper penetrations.

In the defensive posture, it is necessary for our forces to learn as much as possible from the attack signature by using software tools and backtracking technologies.<sup>32</sup> This means it is necessary to move out of our KZ – Honeynets and onto the GII to track down and deal with the perpetrators using the spectrum of influence available to the government. This spectrum includes activities such as adjusting system security policy, engaging law enforcement, covert network intrusions and military kinetic response.

The metaphor to the defensive battle now presents civilized cultures with a moral dilemma for the defence of cyberspace. As expected, such a defence requires vigilance and the appropriate oversight to include Rules of Engagement (ROE). Therefore, to conduct operations in cyberspace, it is necessary to prepare an intelligence preparation of the battlespace (IPB), determine the 'areas' of interest and then determine what effects are to be achieved within each 'area'. As network mapping becomes more detailed, and intuitive maps for cyberspace are perfected, it will be possible to 'Net Enable' the network with a combination of sensors and information technology. The next step is to select the weapon for the effect specified in the plan.

It is at this point the dilemma occurs, since network weapons effects, thus far, are not predictable. This is to say, there is no measurable error probabilities as there are for kinetic weapons. Indeed, there is very little understanding of what would be the second and third-order effects of: setting loose a malicious code, taking down a firewall or even conducting aggressive port scans. Once a network action is taken, a subsequent battlefield damage assessment (BDA) for the action has to be measurable in order for the nation-state to argue that the action was proportional to the attack.<sup>33</sup> This does not disprove the argument that cyberspace acts as a battle space, on the contrary. However, this does define a moral dislocation. "Threats to democracies' cyberspace endanger not only the citizens' quality of life but also their resolve."<sup>34</sup> Therefore, the ethical decision-maker is in a weakened position to the terrorist or less ethical decision-maker who can take advantage of opportunities created by such an attack. Therefore, it can be argued that the greatest limiter to the progress of cyber defence is political, because freedom of action is reduced since society does not have the will to act in this space.

The remedy to this is enacting the first principle of Knowledge and Ignorance and therefore Cyber ISR. Once battlefield visualization and situational awareness are defined, it is possible to conduct weapons effects simulations and therefore assessment of collateral damage. Precision, as exists in the physical battlespace, can eventually be developed. In physical space the notion of precision is viewed as the ability to eliminate the inverse relationship between range and accuracy through the use of information technology.<sup>35</sup> In cyberspace, information technology must be used to eliminate the inverse relationship between time and understanding. Where range and spatial proximity

is the major factor on the physical battlespace, time and logical proximity are the major factors in cyberspace. With the ability to do this, the dilemma is broken and decisive action is more achievable. Moreover, democratic powers should not be confined to responding in kind to cyber attacks, but employ them as a measured response within the spectrum of conflict.<sup>36</sup>

## 5.6 Option Acceleration and Objective

This Principle provides us a break from the rank and file of constructing a defensive position and facilitates a discussion of command philosophy. Essentially, Option Acceleration and Objective deals with the way in which one manages the end states for a conflict. Classical military operational planning processes demand that end states be delivered very early in the planning process to provide unity of action and coalition stability. This provides for rapid and focused action but does not allow for the necessary flexibility to act upon a high-payoff alternative end-states. Option acceleration is a knowledge-enabled construct that allows for rapid exploitation of opportunity, shattering the opponent's planning ability and inevitably creating panic or malaise. The greater the knowledge gap between the combatants, the faster option acceleration can progress.<sup>37</sup>

Smaller, lighter forms of attack have been used in swarm tactics in military history since the Roman Legion broke the Phalanx. These coordinated attacks require skill and information to execute. Indeed, if an aggressor can swarm the target and create confusion, or Clausewitzian fog, then the aggressor has the advantage and can quickly shift from a minor objective, such as destroying the opponent's force, to the more important goal of defeating the opponent economically or politically – thus option acceleration. Little analytical attention has been given to swarming, yet it can be seen as one of the most important modes of interaction in the information age.<sup>38</sup>

In the 13<sup>th</sup> Century, the “Mongol horde's” success relied almost entirely on learning exactly where their enemies were, while keeping their own whereabouts a secret until they attacked. This enabled them with far inferior numbers to overthrow the finest and largest armies of the known world. The Mongols emphasized decentralization and comparatively sophisticated communications techniques, while their enemies waited for orders from distant capitals. In an Option Acceleration approach to the battlespace, the Mongols forced massive enemy armies into a reactionary mode and then took the opportunity to directly attack the political centers of gravity. In the 20<sup>th</sup> Century, the US achieved the same feat against a numerically superior force during the opening of first Gulf War; however, it failed in the final stages of the war as the coalition was politically unable take action against the center of gravity in Baghdad – and therefore, a second Gulf War was required a decade later. Essentially, the dramatic asymmetric success of the Mongols is a lesson for us to focus on the defeat of the enemy and not to fixate on the immediate objectives involved in destroying his offensive capability.<sup>39</sup>

To deal with cyber swarming, the defensive construct that has been discussed in this paper attempts to use a balance of both objective and option acceleration. A defence

in depth design provides sequential objectives to occupy the opponent while attempting to achieve a superior information position. This in turn provides a competitive advantage characterized by decisively altering initial conditions, developing high rates of change and locking in friendly success while locking out alternative enemy strategies.<sup>40</sup> However, the speed at which attacks can be launched and altered works against us in the cyber environment. Also, there needs to be no central leader or command center in this environment; therefore, much of the system acts as a cellular or flat organizational construct. The military hierarchical Command and Control constructs are not necessarily the most conducive to dealing with such a lightning speed, hydra-headed threat.<sup>41</sup> This construct is also problematic in coalition environments “where participants have overlapping or sometimes different priorities, perspectives and constraints.”<sup>42</sup> Therefore, as with the Mongol threat of the 13<sup>th</sup> Century, the monolithic military structures of today must develop methods to deal with these new threats. The military must consider a mix of agent based, almost autonomic responses, to cyber threat signatures. Waiting for orders from parliamentary process or even the operational level HQ for a conflict in this space will result in similar results for modern network defenders as for those that opposed the Mongols. The hierarchy needs to be flattened in cyberspace.

## 5.7 Command and Anarchy

Moving from philosophy of command to its mechanics, the last principle pits the concept of Command against Anarchy. Command seeks success through unity of effort and authoritative direction while anarchy seeks success through skilful integration of effects. A balance between these transactional and transformational constructs is where any real future scenario must focus.<sup>43</sup> This means that the knowledge derived from a shared awareness combined with a confident understanding of the commanders’ intent, enable self-synchronizing behaviour, allows a smaller footprint, and increases effectiveness.<sup>44</sup>

NEOps cries out for a flattening of the command structure and the cyber environment is among the loudest of these voices. Work by the US Command and Control Research Project provide excellent examples where efficiency has been brought to bear on projects, like the Navy’s Co-operative Engagement Capability (CEC). This project improves the ability of the US Navy to conduct Air defence by allowing highly dispersed combat elements and sensors to be netted together with a high performance backplane. This in turn provides the increased information velocity necessary to support a fully integrated Common Operating Picture (COP).<sup>45</sup> However, the question must be asked: what happens when like capabilities are pitted against each other? The two highly integrated capabilities engage in a duel instead of the expected route. Given that each side has strength of resolve, in a duel the fastest to the trigger often has the advantage. This is very nearly the case in the cyber environment.

The construct required to deal with this environment must be segmented in its approach so that a single bullet does not down the whole beast; Figure 7 illustrates this concept. The Network Operations Center (NOC) shown in this figure provides for the monitoring of system availability but also has a link to the NVAT, Red Teams and the

CIRTs. It also has linkage to the segmented safe havens in order to coordinate security efforts, provide system status and conduct required business continuity actions. This does not suggest that Command and Control be executed by one central all seeing NOC, this would result in a cyber Magnit Line. Each safe haven requires a smaller subordinate NOC to provide monitoring, patching, policy setting and local engineering. When fully deployed and inter-operating, the system functions much like the human immune system where the body contains infection, learns how to counter the disease, and then engineers antibodies or environmental conditions that halt the spread and then destroy the infection. However, a concerted attack, especially within the KZ, would require improved processing power, information storage, bandwidth and the application of advanced software technologies such as agent based - antibodies.<sup>46</sup> This form of agile and interoperable organizational structure, whose constituents are given enough autonomy to rapidly create effects and synchronize, is the future of Cyber Command and Control.<sup>47</sup>

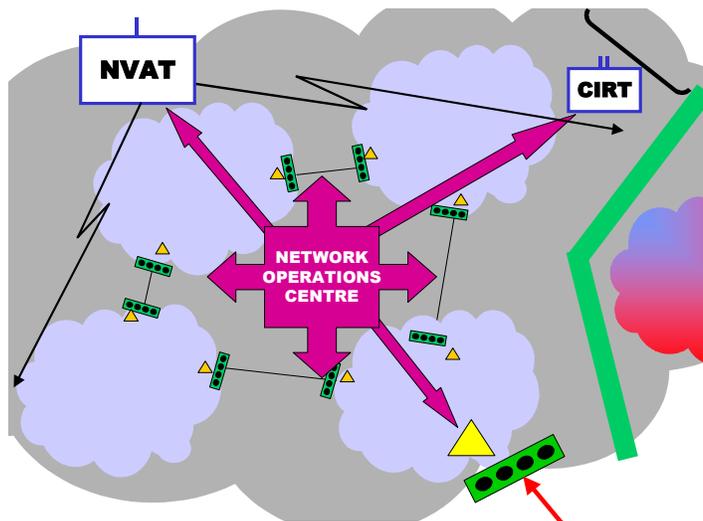


Figure 7. Network Operations

Any effective cyberspace protective strategy must take into account that no nation has effective sovereignty over cyberspace.<sup>48</sup> This makes the command and control issue very difficult for the cyber environment; however this is not a new concept. Within the reach of history it was once believed that maritime and air spaces could not be sovereign, yet through the development of technology and doctrinal practices these wilds were both tamed and currently the uncontrollable concept of ‘orbital space’ is well on its way to becoming sovereign. The ability to declare sovereignty does not lie in the total occupation of the environment but the ability to sense and act in that space with competence and conviction. Essentially, the first ingredient for sovereignty is the spatial awareness for which directed action can be taken. NEOps clearly is applicable to this problem set, especially since it generally involves seeking ‘top sight’ of one’s own and the opponent’s situation, while leaving that opponent in the dark.<sup>49</sup>

## 6. Summary and Conclusions

In this paper a conceptual framework for network battle is described with a focus on the cornerstone requirement for an intuitive operational network situational awareness picture or map. Such a map allows “net enabling” technologies to be brought to bear in logic space as opposed to physical space; however the same C2, planning and war gaming activities are necessary. We also describe the behaviour of both friendly and enemy actors upon such an infrastructure. It is argued that the network must be seen as a battlespace where cyber warfighters can ask the timeless questions: Where am I? Where are my buddies? Where is the enemy? Based on network situational awareness, the cyber-warfighter will have timely and accurate data from an array of pre-propositioned sensors fused on an operationally relevant network picture. With this in hand, the warfighter is able to make informed decisions about observable threat signatures and engage cyber adversaries with appropriate countermeasures based on rules of engagement supported by a much clearer understanding of their effects. Indeed, without truly “operationalizing” the network and providing a true battlespace awareness picture, we leave our enemies armed with an asymmetric advantage that will threaten our network-enabled capabilities.

The Military has a long history dealing with integrating new capabilities into Operational Art. Cyber activities are but one more complication to the Art of War and must be dealt with before those same complications deal with us. The objective should be to focus our military on cyber technology ensuring that network operations are coordinated so that they are consistent with national policy and the strategy of military commanders.<sup>50</sup> The strategic view must be that cyberspace is a developing battlespace in which many actors can engage. Historically, nation-states do not develop appropriate doctrine, techniques and tactics to contend with changing circumstances until they fail quite dramatically in the opening phases of conflict and only recover if they can quickly find effective countermeasures. It is noteworthy that historically, the underdog is more likely to be the father of ingenuity. “Revolution by the strong”<sup>51</sup> – is somewhat illogical, yet the need stares us in the face. The Roman legion, the Mongol Horse Riders, Bonaparte’s Levy en’ Mass, and the German Blitzkrieg all point out that we must deal with cyberspace before cyberspace deals with us.

### References:

- [1] Alberts, David S., John J. Garstka and Fredrick P. Stein. “Network Centric Warfare: Developing and Leveraging Information Superiority”. Library of Congress Cataloguing-in-Publication Data ( October 2004), 260 pages.
- [2] Alberts, David S. & Richard E. Hayes. “Power to the Edge”. Library of Congress, USA, June 2004, 236 pages.
- [3] Arquilla, John & David Ronfeldt. “The Advent of Netwar. IN ATHENA’S CAMP”. Rand Corporation, <http://www.rand.org/publications/MR/MR880>, 1997, 525 pages.

- [4] Ceborwski, Vice Admiral Aurther K & John Garstka, "Network-Centric Warfare: Its Origin and Future". US Naval Institute, 1997.
- [5] Clauswitz, Carl von. "On War". Ed & Trans. Michael Howard and Peter Paret. New Jersey: Princeton University Press, 1989.
- [6] Department of National Defence, Information Operations Policy for CF International Operations, [http://dcids.mil.ca/cosj3/ndcc/j3ioops/pages/policy\\_e.asp#info](http://dcids.mil.ca/cosj3/ndcc/j3ioops/pages/policy_e.asp#info), Canada, dated 2005-01-20.
- [7] French, Geoffrey S. "Rethinking Defensive Information Warfare". General Dynamics,
- [8] Command And Control Research And Technology Symposium, 2004, 13 pages.
- [9] Gershwin, Lawrence K. - National Intelligence Officer for Science and Technology. "Cyber Threat Trends and US Network Security". Statement for the Record to the Joint Economic Committee, 21 June 2001.
- [10] Houser, Dan. "Network Security : Submarine Warfare:", Information Security, Aug. 2003, pp 46-57
- [11] Johnson, Keith, "When a group of suspected Pakistani hackers broke into a U.S.-based computer system in June, they thought they had found a vulnerable network to use as an anonymous launching pad to attack Web sites across India", ZDNet News, URL: [http://news.zdnet.com/2100-9595\\_22-526520.html](http://news.zdnet.com/2100-9595_22-526520.html), 2005.
- [12] Khalilzad, Zalmay, John P. White and Andrew W. Marshal. "Strategic Appraisal: the Changing role of Information in Warfare". Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, 452 pages.
- [13] Leonhard, Robert. "The Art of Maneuver". Presidio Press, USA, 1991, 270 pages.
- [14] Leonhard, Robert R. "The Principles of War for the Information Age". Presidio Press, 1998, 262 pages.
- [15] Levine, John & Richard LaBella, Henry Owen, Didier Contis, Brian Culver. "The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks". Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY June 2003.
- [16] McIntyre, Mark and Sherri Flemming. "Network Centric Warfare for Dynamic Coalitions: Implications for Secure Interoperability", Proc. NATO IST Symposium, Quebec City, May 2001.
- [17] Molander, Rodger C., Andrew S Riddle, and Peter A Wilson. "Strategic Information Warfare: a New Face of War". US Army War College Quarterly, Autumn 1996. [Http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm](http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm).
- [18] Spitzner, Lance - Sun Microsystems. "The Honeynet Project: Trapping the Hackers". IEEE, Inc., 2004.
- [19] Spitzner, Lance - Sun Microsystems. "Honeypots: Simple, Cost-Effective Detection". <http://www.securityfocus.com/infocus/1690>, 2003.
- [20] Spitzner, Lance - Sun Microsystems. "Honeypots: Definitions and Value of Honeypots". <http://www.tracking-hackers.com>, 29 May, 2003.
- [21] Sun Tzu. "The Art of War". New York: Oxford University Press, 1971.

- [22] The HoneyNet Project. "Know Your Enemy". Indianapolis, IN: Addison-Wesley, 2002.
- [23] Thomas, Timothy L. "Like adding Wings to the Tiger: Chinese Information War Theory and Practice". Foreign Military Office (USA), 12 June 2000.  
<http://call.army.mil/call/fmso/fmsopubs/issues/chinaiw.htm>
- [24] Waltz, E., "Information Warfare Principles and Operations", Artech House, August 1998, 350 pages.

End Notes:

- 
- <sup>1</sup> Sun Tzu, "The Art of War", New York: Oxford University Press, 1971, p.7
- <sup>2</sup> John Arquilla and David Ronfeld, "A New Epoch – and Spectrum – of Conflict, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 1.
- <sup>3</sup> Glenn C. Buchan, "Implications of Information Vulnerabilities for Military Operations, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 313.
- <sup>4</sup> Alberts, David S., John J. Garstka and Fredrick P. Stein. "Network Centric Warfare: Developing and Leveraging Information Superiority". Library of Congress Cataloguing-in-Publication Data (October 2004), page 88.
- <sup>5</sup> Alberts, David S., John J. Garstka and Fredrick P. Stein. "Network Centric Warfare: Developing and Leveraging Information Superiority". Library of Congress Cataloguing-in-Publication Data (October 2004), pages 133-155.
- <sup>6</sup> Timothy L. Thomas, "Like adding Wings to the Tiger: Chinese Information War Theory and Practice, (Foreign Military Office (USA), 12 June 2000.  
<http://call.army.mil/call/fmso/fmsopubs/issues/chinaiw.htm>
- <sup>7</sup> Department of National Defence, Information Operations Policy for CF International Operations, [http://dcids.mil.ca/cosj3/ndcc/j3ioops/pages/policy\\_e.asp#info](http://dcids.mil.ca/cosj3/ndcc/j3ioops/pages/policy_e.asp#info), Canada dated 2005-01-20. para 2.
- <sup>8</sup> Ed Waltz, "Information Warfare Principles and Operations", Artech House, Norwood (USA), 1998, p.148-152 & 239-243.
- <sup>9</sup> John Arquilla and David Ronfeld, "Preparing for Conflict in the Information Age, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 151.
- <sup>10</sup> David C. Gompert "Right Makes Might: Freedom and Power in the Information Age, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 48-60.
- <sup>11</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p252
- <sup>12</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p227-233.
- <sup>13</sup> Richard O. Hundley and Robert H. Anderson, "Emerging Chalange: Security and Safety in Cyberspace, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 242.

- 
- <sup>14</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p251-255.
- <sup>15</sup> John Arquilla and David Ronfeld, "A New Epoch – and Spectrum – of Conflict, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 156.
- <sup>16</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p36.
- <sup>17</sup> Robert H Anderson and Anthony C. Hearn, "An Exploration of Cyberspace R&D Investment Strategies For DARPA, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 156-164..
- <sup>18</sup> Bruce D. Berkowitz, "Warfare in the Information Age, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 189.
- <sup>19</sup> John Arquilla and David Ronfeld, "The Advent of Netwar, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 282.
- <sup>20</sup> Geoffrey S. French, "Rethinking Defensive Information Warfare", General Dynamics, Command And Control Research And Technology Symposium, 2004, page 4.
- <sup>21</sup> Robert H Anderson and Anthony C. Hearn, "An Exploration of Cyberspace R&D Investment Strategies For DARPA, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 161.
- <sup>22</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p64.
- <sup>23</sup> Lance Spitzner - Sun Microsystems, "The Honeynet Project: Trapping the Hackers", IEEE, Inc. [Website URL](#), 2004
- <sup>24</sup> Lance Spitzner - Sun Microsystems, "Honeypots: Simple, Cost-Effective Detection", <http://www.securityfocus.com/infocus/1690>, 2003
- <sup>25</sup> Lance Spitzner - Sun Microsystems, "Honeypots: Definitions and Value of Honeypots", <http://www.tracking-hackers.com>, 29 May, 2003.
- <sup>26</sup> Glenn C. Buchan "Implications of Information Vulnerabilities for Military Operations Age, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 304.
- <sup>27</sup> Lance Spitzner - Sun Microsystems, "Honeypots: Definitions and Value of Honeypots", <http://www.tracking-hackers.com>, 29 May, 2003.
- <sup>28</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p258.
- <sup>29</sup> Stephan J. Blank "Preparing for the Next War: Reflections on the Revolution in Military Affairs, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 1.
- <sup>30</sup> Glenn C. Buchan, " Implications of Information Vulnerabilities for Military Operations, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 291.
- <sup>31</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p258-259.

- 
- <sup>32</sup> Robert H Anderson and Anthony C. Hearn, "An Exploration of Cyberspace R&D Investment Strategies For DARPA, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 160.
- <sup>33</sup> Rodger C. Molander, Andrew S Riddle, and Peter A Wilson, "Strategic Information Warfare: a New Face of War", US Army War College Quarterly, Autumn 1996) [Http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm](http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm), p 4-7.
- <sup>34</sup> David C. Gompert "Right Makes Might: Freedom and Power in the Information Age, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 62.
- <sup>35</sup> David C. Gompert "Right Makes Might: Freedom and Power in the Information Age, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 60.
- <sup>36</sup> David C. Gompert "Right Makes Might: Freedom and Power in the Information Age, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 63.
- <sup>37</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p259
- <sup>38</sup> John Arquilla, David Ronfeldt and Michele Zanini "Networks, Netwar and Information Age Terrorism, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 82.
- <sup>39</sup> John Arquilla and David Ronfeldt, "Cyberwar is Coming!, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 34-40.
- <sup>40</sup> Vice Admiral Arthur K Cebrowski and John Garstka, "Network-Centric Warfare: Its Origin and Future", US Naval Institute, 1997, <http://WWW.usni.org/Proceedings/Articles98/PROcebrowski.htm>, page 13.
- <sup>41</sup> John Arquilla and David Ronfeldt, "The Advent of Netwar, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 275-281.
- <sup>42</sup> Alberts, David S. & Richard E. Hayes. "Power to the Edge". Library of Congress, USA, June 2004, pages 57.
- <sup>43</sup> Robert R. Leonhard, "The Principles of War for the Information Age", Presidio Press, 1998, p260
- <sup>44</sup> David S. Alberts, John J. Garstka and Fredrick P. Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority", Library of Congress Cataloging-in-Publication Data ( October 2004), 91
- <sup>45</sup> David S. Alberts, John J. Garstka and Fredrick P. Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority", Library of Congress Cataloging-in-Publication Data ( October 2004), 171.
- <sup>46</sup> Lawrence K. Gershwin - National Intelligence Officer for Science and Technology, "Cyber Threat Trends and US Network Security", Statement for the Record to the Joint Economic Committee, 21 June 2001.
- <sup>47</sup> Alberts, David S. & Richard E. Hayes. "Power to the Edge". Library of Congress, USA, June 2004, pages 56 & 203-210.

---

<sup>48</sup> Richard O. Hundley and Robert H. Anderson, "Emerging Chalange: Security and Safety in Cyberspace, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 239.

<sup>49</sup> David Ronfeldt and Armando Martinez, "A Comment on the Zapatista "Netwar": Security and Safety in Cyberspace, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 373.

<sup>50</sup> Bruce D. Berkowitz, "Warfare in the Information Age, IN ATHENA'S CAMP", [www.rand.org/publications/MR/MR880](http://www.rand.org/publications/MR/MR880), 1/14/2005, page 185.

<sup>51</sup> Jeremy Shapiro "Information and War: Is It A Revolution?, Strategic Appraisal: the Changing role of Information in Warfare", Rand Corporation, [www.rand.org/publications/MR/MR1016](http://www.rand.org/publications/MR/MR1016), 1999, page 139.