INFORMATION WARFARE IN THE 21ST CENTURY

By Mr Cisco Van Schaik

INTRODUCTION

"For to win one hundred victories in one hundred battles is not the acme of skill. To subdue an enemy without fighting is the acme of skill" - Sun Tzu

The post-Cold War era is characterized by a diffusion of power, geopolitical uncertainties, and technology-driven change. An information revolution is sweeping the world, forcing change as radical as that caused by development of the atomic bomb. Just as control of industrial technology was key to military and economic power during the past two centuries, control of information technology will be key to power in the 21st Century. To help us understand the changing nature of warfare, the four major types of world economies over time can be considered:

Hunter - Gatherer Economy. This was the first type of economy where man hunted and gathered from his immediate environment from a day to day basis in order to satisfy his basic needs.

Agricultural Economy. As man learned to till the soil, the hunter - gatherer economy gave way to the agricultural economy. This economy started the first great wave of change in history. It led to the first of today’s known societies. Agriculture enables communities to produce economic products, which in that age were also the cause of many conflicts. Conflict in this economy is closely linked to agricultural resources (i.e. the land).

Industrial Economy. This economy followed the Agriculture Economy. The economy changed the way wars were fought. Conventional weapons and weapons of mass destruction were introduced to destroy the enemies military / industrial complex in order to win the war. Strategic bombing and ballistic missiles were designed for use on a massive scale and small battlefield nuclear and chemical devices were added to the weapons arsenal.

Information Economy. By the early 1980s, third wave technologies and ideas began to impinge upon the industrial economy. The information economy, in both its technological and non-technological aspects, set in motion forces that challenge the design of many organisations and institutions. Quicker and more accurate dissemination of information to the lowest levels disrupts and erodes traditional hierarchies around which institutions are normally designed, calling for flatter and more flexible structures, also challenging traditional command & control frameworks by eroding middle tier management control. It diffuses and redistributes power and responsibility. Transparency and dynamic knowledge management through information systems becomes the critical success factors in the new global village.

As these information systems permeate our lives, we are crossing a new frontier - the Information Age. It will define the 21st century and influence all we do. Information Warfare has become central to the way nations fight wars, and will be critical to National Security operations in the 21st century. This means, of course, that today we must invest in our people, planning, equipment, and research so our ambitions can become reality, generating a wave of momentum that will carry us into the next millennium.

Information Warfare is not the exclusive domain of the Military, but intrinsically lies within their vital interests. Information technology advances will make dramatic changes in how this nation fights wars in the future. They will allow a commander's vision and view of the battle space to be shared at the lowest level. Because of this, every practitioner of the profession of arms has a responsibility to understand the impact of information warfare on their service.

The following are some of the possible scenarios of how information warfare might manifest itself in future:

Scenario 1. Information terrorists employed by a Nigerian drug cartel electronically blind early warning radar scopes all along Regional Task Force North (RTFN). Radar screens suddenly go fuzzy due to time / date activated viruses placed in computers before the time.

Scenario 2. As revenge for action by Government against the members of a extremist vigilante movement, a computer virus is surreptitiously placed in the South African banking systems, zeroing out the account balances of every member of the SANDF and SAPS creating widespread panic. Blackmail follows blatantly against a repetition.

Scenario3. Environmental extremists hack into and corrupt critical Eskom systems, thereby disrupting power supply drastically on a country wide basis, in retaliation to coal "strip mining" methods contracted by Eskom for fuelling their power stations.

Scenario 4. A disgruntled investor decides to crash the main system of the Johannesburg Stock Exchange (JSE) in response to losing money on the exchange. The result is a vacuum effect on the SA stock market as foreign investors remove their funds from SA companies and investment portfolios.

The Government wants to retaliate, but security advisors can't prove who did it or who to retaliate against. Although fictitious, these scenarios now sound more feasible than ever. Take note of the wide spectrum over which information warfare might be fought, impacting on all the power bases of the state.

AIM

The aim of this paper is "to define and discuss information warfare within the context of the global village and its impact on the national security of the RSA".

Before continuing, we must distinguish between information age warfare and information warfare. We make this distinction because much of the literature treats information warfare and advances in information technology synonymously. Information age warfare uses information technology as a tool to enhance our combat operations with unprecedented economies of time and force. Ultimately, information age warfare will affect all combat operations. In contrast, information warfare, the point of this paper, views information itself as a separate realm, potent weapon, and lucrative target. Information, as we will show below, is technology independent. Therefore, we can conclude that information age technology is turning a theoretical possibility into fact: directly manipulating the adversary's information. This is the driving force behind this paper.

CORNERSTONES OF INFORMATION WARFARE

Security Revolution. Information Warfare (IW) emerged as the hot, new topic of debate for security thinkers. At the highest levels of the Departments of Defense (DOD) and Safety & Security, IW is called the latest "revolution in security affairs. In South Africa (As in other countries around the globe), the DOD is posturing itself to fight these high-tech wars by creating Information Warfare Centres. But are we on the right track for preparing to fight these "information wars" of tomorrow?

Deduction / conclusion. We also need to be aware that our technical dependencies represent potentially crippling vulnerabilities and it can therefore be stated that sophisticated, robust, multi-layered defenses for our military information functions may well be what separate us from joining the sorry league of military failures.

The emergence of an information-based society is changing the way we'll fight future wars, just as the move from the agrarian age to the industrial age forced a change in war fighting. Is IW our inevitable future in the technology age or it is a misguided attempt at phasing out traditional means of fighting?

Deduction / conclusion. One could rather deduce that Information, combined with modern information functions, has distinct characteristics that warrant it being considered a realm, just as land, sea, air, and space are realms.

Technological Revolution. The competition for information is as old as human conflict. It is virtually a defining characteristic of humanity. Nations, corporations, and individuals each seek to increase and protect their own store of information while trying to limit and penetrate the adversary's. Since around 1970, there have been extraordinary improvements in the technical means of collecting, storing, analysing, and transmitting information. Reams have been written about the impact of this technical revolution on the conduct of war, particularly since DESERT STORM. However, most of the literature focuses primarily on technical developments, not on how these developments impact doctrine.

Information Age. Because there is a technological revolution' sweeping through information systems and their integration into our daily lives leading to the term 'Information Age.' information-related technologies concentrate data, vastly increase the rate at which we process and transmit data, and intimately couple the results into virtually every aspect of our lives. The Information Age is also transforming all military operations by providing commanders with information unprecedented in quantity and quality. The commander with the advantage in observing the battlespace, analysing events, and distributing information possesses a powerful, if not decisive, lever over the adversary.

INFORMATION DEFINED

Perception and Interpretation. This definition is elementary, but pivotal. It is impossible to discuss information warfare meaningfully without rigorously defining the central concept: information. Information derives from phenomena. Phenomena, observable facts or events, are everything that happens around us. Phenomena must be perceived and interpreted to become information. Information, then, is the result of two things: perceived phenomena (data) and the instructions required interpreting that data and giving it meaning. This distinction is important and easily encompassed by a familiar paradox: If a tree falls, but no one was around to hear it, did it make a noise? The falling tree caused pressure waves in the atmosphere, a phenomenon. Noise, the information denoting a falling tree, occurs when someone's ear detects the pressure waves, creating data, and the brain's instructions manipulate that data into the sound recognisable as a falling tree. Within that person's context, there is no falling tree until the person hears (or sees) it.

Phenomena become information through observation and analysis. Therefore, information is an abstraction of phenomena. Information is the result of our perceptions and interpretations, regardless of the means. As falling trees make clear, to define information requires only two characteristics:

Information: data and instructions.

Distinct from Technology. Note that the definition for information is absolutely distinct from technology. However, what we can do with information, and how fast we can do it, is very dependent on technology. Technology dramatically enhances our observational means, expands and concentrates data storage, and accelerates instruction processing. We use the following term to encompass the technology-dependent elements associated with information:

Information Function: any activity involving the acquisition, transmission, storage, or transformation of information

For example, the system that tells a machine to stamp eighty hubcaps is performing an information function. The sheet metal press stamping those hubcaps is not.

MILITARY INFORMATION FUNCTIONS

Quality information is the counter to the fog of war. As mentioned earlier, the commander with better information holds a powerful advantage over his adversary. Military operations make special demands on information functions in seeking to give the commander an information advantage.

Surveillance and reconnaissance are our powers of observation. Intelligence and weather analysis are the bases for orienting observations. We use those bases to formulate operational orders, which command and control operations execute and monitor in directing the conflict. Precision navigation enhances mission performance. Together, these are the kinds of military information functions that enhance all military operations. Collectively, we use the term military information functions to describe force enhancing information functions.

Military Information Function: any information function supporting and enhancing the employment of military forces.

This definition serves to delineate militarily important information functions from the total universe of information functions.

INFORMATION WARFARE DEFINED

At the grand strategy level, nations seek to acquire, exploit, and protect information in support of their objectives. This exploitation and protection can occur in the economic, political, or military arenas. Knowledge of the adversary's information is a means to enhance our own capabilities, degrade or counteract enemy capabilities, and protect our own assets, including our own information. This is not new. The struggle to discover and exploit information started the first time one group of people tried to gain advantage over another.

Information warfare consists of targeting the enemy's information and information functions, while protecting our own, with the intent of degrading his will or capability to fight. Drawing on the definitions of information and information functions, we define information warfare as:

Information Warfare: any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own information functions.

Assertions. This definition is the basis for the following assertions:

* Information warfare is any attack against an information function, regardless of the means. Bombing a telephone switching facility is information warfare. So is destroying the switching facility's software. Information warfare is any action to protect our information functions, regardless of the means. Hardening and defending the switching facility against air attack is information warfare. So is using an anti-virus program to protect the facility's software.
* Information warfare is a means, not an end, in precisely the same manner that air warfare is a means, not an end. We may use information warfare as a means to conduct strategic attack and interdiction, for example, just as we may use air warfare to conduct strategic attack and interdiction.
* Militaries have always tried to gain or affect the information required for an adversary to effectively employ forces. Past strategies typically relied on measures such as feints and deception to influence decisions by affecting the decision-maker's perceptions. Because these strategies influenced information through the perception process, they attacked the enemy's information indirectly.

Deduction / conclusion from assertions. One can therefore see that the competition for information is as old as man's first conflict. It involves increasing and protecting our own store of information while limiting and penetrating the adversary's - targeting the enemy's information functions, while protecting ours, with the intent of degrading his will or capability to fight.

Added Vulnerability. However, modern means of performing information functions give information added vulnerability: direct access and manipulation. Modern technology now permits an adversary to change or create information without relying on observation and interpretation. Here is a short list of modem information system characteristics creating this vulnerability: concentrated storage, access speed, widespread information transmission, and the increased capacity for information systems to direct actions autonomously. Intelligent security measures can reduce, but not eliminate, this vulnerability; their absence makes it glaring.

Militaries are not inclined to trust their success to the fortunes of war. So we must direct our information warfare efforts to more than just targeting an adversary's information: we must also defend our own information, and all its operations. The Defense Force depends heavily upon military information functions, making them vulnerable to information warfare. The integrity of military information functions, as well as the information itself, bears heavily and directly on the success of military operations.

Deduction / conclusion. As the Defense Force and indeed other Government Departments becomes more technologically sophisticated, it therefore becomes more technologically dependent. We need therefore to use that technological sophistication to avail our selves of all the opportunities and threats that information, as a target, presents.

THE THREAT OF INFORMATION WARFARE

The Incompetent Threat. The incompetent threat is an amateur that by some means (perhaps by following a hacker recipe or by accident) manages to perform some action that exploits or exacerbates vulnerability.

The Hacker/Cracker. This threat implies a person with more technical knowledge who to some degree understands the processes used and has the intent to violate the security or defenses of a target to one degree or another.

Disgruntled Employee or Insider. The disgruntled employee threat is the ultimate inside threat: the individual who is inside the organisation and trusted.

Criminals. When examining the potential for information warfare activities, the potential for a criminal or non-governmental attack for economic purposes must be considered.

Political Dissidents. The increasing interconnectivity of information systems makes them a tempting target for political dissidents. Activities of interest to this group include spreading the basic message of their cause by a variety of means as well as inviting others to action.

Terrorists. By attacking those targets in a highly visible way, the terrorist hopes to cause the media to provide a great deal of publicity of the action, thereby further disseminating the message of fear and uncertainty.

Competitor Nations. The purpose behind such attacks could be an attempt to influence South African policy by isolated attacks; foreign espionage agents seeking to exploit information for economic, political or military intelligence purposes; the application of tactical counter measures intended to disrupt a specific SANDF military weapon or command system; or an attempt to render a major catastrophic blow to the RSA by crippling the National Information Infrastructure. The South African armament industry will be one of the prime targets where foreign competitors will conduct IW operations.

The Threat of IW in the Private Sector. The Private Sector and the large IT Vendors (Micro-Soft, Oracle, Novell, etc) all have their own Information System Security teams busy with R&D and ISS counter measures to neutralise the IW Threat. The Private Sector is already gearing up to put more effort and finance into defeating the IW Threat than was utilised against the Y2K problem. It will require great ingenuity and effort to defeat the Hacker-Clique, Hacking Freeware, Virus Incubators and Organised Crime. The principle of "it takes one to catch one" often prevails in the private sector, where hackers are recruited for their very skills in a defensive capacity.

Cyber Warfare. Global trends indicate a steady increase in incidents. One of the major problems in this arena is that Governments and Business are loath to report incidents of this nature to avoid public embarrassment. The recent year 2000 (y2k) phenomenon indicated just how sensitive our IT / IS environments are to "attack" and what the possible implications would be if left unattended.. It can also serve as a baseline / benchmark for the inherent risks we face from Cyber warriors, as well as the critical environments in this regard.

If the fact that one individual (Hacker, cracker) can cause major disruption without firing a shot with relative ease seems frightening, what about a dedicated bunch of doomsday fanatics…. Cyber warfare has the ability to displace more conventional warfare in terms of "non lethal" means. However, the trend seems to be a combination of both (i.e. precision ammunition, EW etc.) to achieve sure victory.

Multi-Nationals impose their own national ISS standards on their overseas branches and interests, eg British Standard 7799. They will in future have to comply to RSA ISS Standards and Legislature. They also belong to International ISS Forums/Response Groups, make use of the international Gartner and META research groups and are forming their own RSA forums.

The Low Technology side of Information Warfare. An example of a leader who defeated his enemies with Command, Control and Communications warfare (C3W) is Mongol leader Genghis Khan. According to Paul Linebarger in his book Psychological Warfare, Khan was widely known for leading hordes of savage horsemen across Russia and into Europe. While not totally unfounded, the Mongols' image of total, barbaric domination was greatly enhanced by Khan's use of psychological operations, deception, operational security, and targeting his adversaries' decision-making process. "Agents of influence" were sent in advance of his armies to do face-to-face psychological operations, telling of brutality and large numbers in the Mongol army.

Khan also used deception to create the illusion of invincible numbers by using rapid troop manoeuvre, making his army look larger than it really was. He had a network of horsemen called "arrow riders" to communicate quickly with his commanders, and he targeted enemy messengers to prevent enemy commanders from communicating with each other. All these actions caused a weakness in their enemy's psyche, and the Mongols were feared wherever they went.

If Genghis Kahn were alive today, he may have employed CNN's Peter Arnett instead of his agents of influence. He may have used Hollywood movie techniques to create propaganda films depicting the barbaric treatment enemies would face if they challenged the Mongols. He could have used satellite communications to talk with his commanders and electronic jamming to interfere with his enemies' communications. Conclusion : No matter what the technology, the effect would have been the same. Genghis Khan still would have controlled the information battle space.

Terrorism – Tools versus Tactics. Terrorists are adopting information technology as an indispensable command-and-control tool. Raids on terrorist hideouts, for example, are increasingly likely to result in the seizure of computers and other IT equipment. Instead of just finding a few hand written notebooks and address books, counter terrorism authorities are faced with dozens of CD-ROMs and hard drives. Likewise, terrorists' increasing use of advanced encryption tools often delays the process of finding key files and information.

Terrorists groups, such as the Osama bin Laden organisation, have yet to demonstrate that they value the relatively bloodless outcome of a cyber attack on a nation's critical infrastructure. But the threat remains real, according to Richard Clarke, national co-ordinator for security, infrastructure protection and counter terrorism at the National Security Council of the USA.

CRITICISMS & PERCEPTIONS

Debate. IW is a much-debated topic, and for every advocate there's also a critic. IW supporters say we're already under attack and, because of our reliance on technology, we have much to lose from our inactivity. IW critics see an unjustified obsession with technology that will divert money from more reliable, traditional capabilities. Indeed, there's a danger in relying solely on technology when conducting warfare. For example, a human intelligence asset is much less likely to be tricked by a decoy tank or aircraft than an intelligence analyst looking at satellite imagery. This is not to say we should ignore the new capabilities technology gives us today, but neither should we fixate on technology as a magical new way to employ forces. IW includes all operations where we attempt to influence a perception or behaviour using information, and this information doesn't have to be technology based. High-technology weapons and equipment can certainly support or augment traditional military operations, but they'll never replace them.

One of the most common misperceptions about IW is that it assumes conflict in a high-tech environment. How can we fight information wars with countries like Angola or the Democratic Republic of the Congo, who are still fighting in the industrial or agrarian age? Let us argue this and other issues in the form of thesis, antithesis, and a synthesis comprising deductions and conclusions from them respectively.

Thesis. We should not examine the merits of IW without examining its shortcomings. First and foremost, the potential impact of IW is directly proportional to the sophistication of one's adversary. The craftiest computer program will be useless against an enemy who communicates by beating on logs with sticks. Indeed, the Vietnam War and recent UN experience in Somalia illustrate how a determined, well-led force can overcome a technologically advanced opponent. The utility of IW increases in direct proportion to the adversary's reliance on information systems. Therefore, while information warfare systems will be an effective addition to our national arsenal, we must avoid considering IW a panacea for conducting engagements across the conflict spectrum.

Antithesis. While there are many nation-states in the world today that are clearly not as technologically advanced as others, we must keep in mind two points when examining the implications of information war.

The first point is that powerful information-age weapons (like modem-equipped computers, for instance) can be purchased in the commercial market for several hundred dollars. The technology is no longer limited or controlled by a select number of businesses or nation-states, and nearly everyone has access to a formidable IW capability.

The second point to consider is that the South Africa has become extremely dependent on computers, computer-based networks, and telecommunications equipment to manipulate and process a wide variety of information--financial data, medical data- bases, defense-related information, etc. Much of this information still travels on unprotected electronic networks that are subject to manipulation by anyone with the right equipment and a modicum of technical knowledge.

Take these two points together and you can therefore see why our dependence on information and information systems has exposed us to a number of organisations (both big and small) that possess the tools to exploit vulnerabilities we have yet to protect. In many cases, protecting ourselves may involve using DoD computers to conduct our own counter-information attacks against a wide variety of potential foes, from the lone hacker operating out of his room, to highly organised, well-financed crime syndicates. The point is, the capability to wage information warfare is not limited to advanced nation-states. Formidable IW weapons can already be purchased in the commercial market for a few hundred dollars, which gives lots of people and organisations the capability to attack us. We can therefore conclude that now that they have that capability, all they need is the motivation. The country that is the most "Technology reliant" also faces the biggest risk in terms of attacks by those with the ability and intent to do so.

Synthesis. These debates are valid, and each side has convincing arguments. What everyone agrees on is enormous growth in information technology gives us opportunities we never had before and we must adapt our doctrine and strategy to take advantage of them. IW is a new form of warfare resulting from changing technology, combined with an old strategy of war-fighting targeting our adversaries' decision-making process.

At this point we can only speculate how to best shape our force for the next 20 years. But it is crucial to remember IW is not the only way we will fight in the future, and because we don't have an unlimited budget we will have to make some very tough decisions in order to strike the right balance between a "mean & lean but modern" defense force.

THE HUMAN FACTOR

Speed of Decisions. In the face of ever decreasing military budgets, decisions often come down to choosing between expensive, high-end systems or cheaper, time-proven equipment. Going back to the IW definition, these concepts focus on the actions taken to fight and defend, not the specific technology used. It really shouldn't matter what means we use to fight a war, as long as those means allow us to complete the decision-making process more quickly than our adversary. No matter if our adversaries are high-tech hackers or low-tech guerrilla fighters, human beings have the same basic wants, needs, and desires. Without a doubt, technology will play a significant role, and we must take advantage of it. But, it's just as important to understand our adversaries' cultural, ethnic, and religious beliefs as it is to be able to electronically attack their command, control, communication and computer (C4) nodes.

Information and Psychological Operations. Collecting information on our adversaries is essential, but we must also be able to understand how this information can be used to better understand our adversaries' intentions and exploit their weaknesses. For example, very few Soldiers have been educated in Information & psychological operations, yet it is one of the five elements of Command and Control they all must understand, especially in terms of the defensive stature of the DOD and of specific use during peace missions. An effective Information campaign is tailored to appeal to a specific target group based on our knowledge of their language and culture, and the same should be true with IW.

Knowing the Enemy. Human intelligence assets are being replaced by electronic sensors and data bases, and we risk losing the capability to understand what the enemy is thinking and what he intends to do. As Sun Tzu said, the only way to defeat the enemy is to know the enemy. We can only do this by studying the enemy. Technology allows us to collect and process information much more rapidly than ever before, but technology won't get us into the heads of the local population or leadership to let us know what they are thinking. Despite all we've heard about IW recently, there is a low-tech side to IW. No amount of technology will give us this broader understanding of humankind. The only way to truly know the enemy is to study their history, culture, and language. We can do this by providing opportunities for our personnel to attend schools that give a cultural awareness or regional orientation. We must maintain a large number of regional specialists and human intelligence assets. We ought to support foreign exchange programs and use our military-to-military contacts to better learn about other countries. We must not turn warfare into a computer simulation that discounts the intricacies of human behaviour, although there is no doubt IW is changing the way we will fight future wars.

ELEMENTS OF INFORMATION WARFARE

Traditional Approach. Recalling the definition, information warfare consists of activities that deny, exploit, corrupt, destroy, or protect information. Traditional means of conducting information warfare include the following:

* Psychological Operations use information to affect the enemy's reasoning.
* Electronic Warfare denies accurate information to the enemy.
* Military Deception misleads the enemy about our capabilities or intentions.
* Physical Destruction can do information warfare by affecting information system elements through the conversion of stored energy to destructive power. The means of physical attack range from conventional bombs to electromagnetic pulse weapons.
* Security Measures seek to keep the adversary from learning about our military capabilities and intentions.

Information Attacks. The Information Age has provided new and practical means to deny, exploit, corrupt, or destroy information, as well as the vulnerabilities to make those attacks possible. Military doctrine does not yet acknowledge or define these assaults on information, which we call Information Attack. Information Attack: directly corrupting information without visibly changing the physical entity within which it resides. Information attack, constrained by the definition of information, is limited to directly altering data or instructions. It is, therefore, just another means of conducting information warfare, one whose immediate effects do not include visible changes to the entity within which the information resides. That is to say, after being subjected to information attack, an information function is indistinguishable from its original state except through inspecting its data or instructions.

Indirect Information Warfare. Indirect information warfare affects information by creating phenomena, which the adversary will perceive, interpret, and act upon. Military deception, physical attack, and OPSEC traditionally achieved their ends indirectly. For example, the goal of deception is to cause the adversary to make incorrect decisions; deception does this by creating an apparent reality. Generally, this entails creating phenomena for the enemy to observer Success, however, depends on several conditional events: the adversary actually observes the phenomenon, thereby turning it into data; analyses it into the desired information; and acts upon the information in the desired manner.

Direct Information Warfare. Direct information warfare affects information through altering its components without relying on the adversary's powers of perception or interpretation. Information attack acts directly upon the adversary's information. Since nearly all modem information functions are themselves controlled by information, information attack may be directed against most information functions. Direct information warfare, the point of information attack, acts on the adversary's information without relying on the adversary's collection, analysis, or decision functions. It can short circuit the OODA loop through creating observations and skewing orientation, or decapitate it by imposing decisions and causing actions.

OODA LOOP INTERFERENCE

THE RELATIONSHIP BETWEEN INFORMATION WARFARE AND COMMAND & CONTROL WARFARE

The focus of information warfare is any information function, whether it is Command and Control (C2), a refinery's control system, or a telephone switching station. C2 represents only part of the universe of military information functions. As we have illustrated, information warfare not only attacks the C2 process, but it also attacks the enemy's combat power itself. Conversely, by definition, C2 warfare is not associated with reducing or nullifying the ability or desire of combat units to execute their orders. Tactical psychological operations and electronic countermeasures self-protection hinder the ability of units to execute orders. But they in no way affect commanders' ability to issue orders to those units, nor their ability to receive those orders. Most military policy on C2 Warfare is only a particular application of information warfare. For the military to concentrate only on C2 Warfare would be ignoring other legitimate target sets. Therefore, information warfare, and its attendant organising, training, and equipping issues, is essential to fully effective Command, control, communication, computer and Information / Intelligence (C4I2) warfare.

INFORMATION WARFARE WITHIN THE DEPARTMENT OF DEFENSE

Arms Of Service Perspective. The different services are best positioned to choose the best means for their ends. Each service has its own unique operational demands. After all, the Army is best qualified to decide which means are best suited for pursuing the goals Chief Joint Operation apportions to the Army.

As a result of its service-unique expertise, its own OODA loop requirements, logistics, etc., each service has information warfare concerns. In developing the doctrinal constructs required for information warfare, a central directorate co-ordinating and integrating the different arms of service requirements would not only be the most cost effective, but also serve to ensure force preparation and force employment doctrinal integration.

Centralised Perspective. On the other hand, CJ OPS has been appointed as the Controlling Authority for IW. An Information Warfare Control Board (IWCB) has been established by CMI (which is facilitating the initiation of the DoD’s IW effort on behalf of CJ OPS) under an SSO IW. Various Committees under the IWCB are being established and are based on 9 IW "Pillars" which all overlap or are intermingled. The number, type and mix of these "Pillars"/Committees is still to be finalised, but have been tentatively sub-divided as follows:

* Electronic Warfare
* Economic Warfare
* Infrastructural Warfare (Hard Steel on Target)
* Intelligence Based/OODA
* Psychological Warfare
* Hacker Warfare (Network Based)
* Cyber Warfare (Individual Based-Your PC/Your Password)
* Command and Control
* Training and Awareness

A decision on Offensive and Defensive IW has still to be made. ISS would appear to be the Defensive Component of IW. Both National and International Legal implications of IW have to be carefully considered.

An IW Battle Lab has been established under CMI/SSO IW, and the SSO IW has a budget for IW R&D and Projects. After a year of Research by IW Battle Lab/CSIR/Defensetek and deliberations of the committees the DoD will approach other Government instances to become part of the IW effort. SACSA has not yet been included but must come in at an early stage. Roles of the various DoD Divisions and their representation must also be considered and resolved.

IW THREAT CONFRONTING THE RSA

W = Widespread

L = Limited

PERSON / ORGANISATION

VALIDATED EXISTENCE

EXIST LIKELY BUT NOT VALIDATED

LIKELY BY 2005

LIKELY BEYOND 2005

Incompetent

Amateur hacker or poorly trained systems administrator and users.

W

-

L

L

Hacker

External/Internal technically qualified with intent to violate.

L

W

L

L

Disgruntled Employee

The ultimate threat as is within the organisation, trusted and has legal access.

W

-

L

L

Crook

Money only used 10% of the time and E -Commerce is increasing. Data manipulation for theft/fraud purposes on the increase. (Nigerian syndicates active with E Commerce fraud within the RSA.).

W

-

L

L

Organised Crime

Money only used 10% of the time and E Commerce is increasing. Data manipulation for theft/fraud purposes on the increase. (Nigerian syndicates active with E Commerce fraud within the RSA.).

W

-

L

L

Political Dissident

Propaganda, incitement to action or overloading /downing systems, eg E-Mail bombs to White House server or Mugabe Web-Site.

L

-

L

L

Terrorist Group

Propaganda, incitement to action; intimidation or maintaining climate of fear; downing of civil, police or military systems and espionage.

L

-

L

L

Foreign Espionage

Espionage, sabotage of systems for denial of service, disinformation and data manipulation, psyops, comms and data interception.

L

W

W

W

Tactical Counter

Measures

COTS IT solutions (firewalls, crypto, Anti-Virus s/ware, etc) readily available to nations as well as to political dissidents and terrorists but under control of technologically advanced nations wrt development, supply or inclusion of Malware. Includes defensive ability to protect own systems, as well as offensive capabilities to overcome adversary defenses. All other ISS measures to protect own systems must be included.

L

W

W

W

Orchestrated Tactical IW

Full spectrum of IW simultaneously launched against an adversary, this also being the main form of attack. Includes "Hard Steel on Target" attacks.

-

-

L

W

Major Strategic Disruption of RSA

Total isolation from rest world as well as total internal disruption (denial satellite and other comms, all trade and financial systems downed, all civil service and armed forces systems downed). Includes "Hard Steel on Target" attacks.

-

-

-

L

INFORMATION SYSTEM SECURITY - A INTERNATIONAL APPROACH

Beware of Myopic Vision in the Global Village. If knowledge is power and information is a force multiplier, security is the key to defense and commercial supremacy in the information age. Any kind of strength, whether military or economic, represents a target for adversaries or competitors. Information, however, is to modern civilization what fire was at the dawn of humankind: an unlimited asset that, if not controlled, quickly can be turned against its user. One problem people have in understanding information security is they often view it with blinders on. Frequently users think of security as protecting their own valuable interests – the "family jewels" of a company, conglomerate or government agency. Even macro-oriented thinkers usually consider security from no larger than a national perspective. However, even that’s no longer enough.

With today’s interconnected world built around reliance on the Internet and web-related technologies, it’s foolish to think of security in any terms other than international. No nation can protect its own secrets, its sensitive data or even its civilian infrastructure without considering how to safeguard against a parade of hostile information warriors or even a single international hacker. This is especially true in the defense arena. The countries constituting SADC must realize that virtually all future military mobilisations are likely to involve coalition operations. Accordingly, South Africa must cater for and gear its defense posture around this doctrine. (even NATO is reorganizing much of its force structure around information systems). This new approach opens up a host of new vulnerabilities, however, that could be exploited by an opportunistic adversary.

All For One. Fragmented information security also raises other key issues. The NATO charter maintains an attack on one of its members is an attack on all. Yet no one has fully addressed this in relation to information operations in cyberspace. If one of NATO’s members suffers an attack on its information infrastructure from a foreign source, how should all the NATO allies respond? Is it credible to expect this type of unified response, especially in light of the potential ambiguities inherent in determining and defining a cyber attack? Members of SADC in the Southern African region should take note!

Now, however, the same type of credibility gap may be looming in information operations. To convince a budding adversary that individual information-security measures can stop a cyber attack strains the bounds of believability. The smorgasbord of security measures being implemented around the world will, by definition, create inequities that could be exploited by hostile information forces. The result is a greater likelihood of an information attack, rather than a deterrence effect.

This cyber attack needn’t come through a nation’s military system. Civilian government and economic infrastructures are targets enough. Crippling the infrastructure of even one NATO nation could blunt, or even stop, an alliance mobilisation or deployment. History has taught that enemies always seek to exploit their target’s weakest link. For the Free World, that might not be the country with the weakest military, but instead the country with the most porous information security. For example, any warehoused data accessible to international partners through databases can be corrupted while it’s in the recipients’ hands. A nation with poor security could be the Achilles’ heel to an alliance operation. Far from deterring attack, information systems instead may pose tempting targets to adversaries that respond with a Pavlovian reflex to weak security measures. The Internet already has become a de facto standard for anyone seeking to participate in the information revolution. From a procedural standpoint, however, a global organizational entity is necessary for functional management, as well as advocacy, of security standards.

IW – A Double Edged Sword. The defensive side of information warfare security measures aimed at protecting information-prevents an adversary from conducting successful information warfare against our information functions. Current security measures such as operational security and communication security are typical means of preventing, detecting, and subverting an adversary's indirect actions on our military information functions. In contrast, security measures such as Information System Security (ISS) encompass preventing, detecting, and subverting direct information actions on our information functions. Future security measures must evolve as information technology advances. Consequently, new-measures will likely take forms entirely different from today's security measures, rooted as they are in previous security requirements. As the simple examples in this paper illustrate, we must avoid falling victim to profound, debilitating effects of direct information warfare.

A NATIONAL APPROACH

One only has to consider the National Security Agency (NSA) of the United States of America to understand the importance of Information Assurance (IA) at national level. Neither the number of employees nor the size of the United States'

National Security Agency's budget are publicly disclosed. However, if the NSA was considered a corporation in terms of dollars spent, floor space occupied, and personnel employed, it would rank in the top 10 percent of the Fortune 500 companies. This is what they say on national level:

"The Information Age presents us with enormous challenges and opportunities. Our core competencies are the same technologies needed to exploit and protect information. However, we must reengineer our traditional approach to signals intelligence and information systems security if we are to remain relevant and play a leading role as key offensive and defensive components of a new national effort dedicated to a single goal -- information superiority for America. This strategic plan charts our course to achieve this noble end. No one will work harder as a single team -- we will think in new ways and strengthen our relationships with our customers and partners."

One can therefore deduce, that information Assurance (IA) missions provides the solutions, products and services, and conducts defensive information operations, to achieve information assurance for information infrastructures critical to national security interests.

In order to enable their customers to protect and defend cyber systems, the NSA develops, and supports a variety of products and services. They also conduct ongoing research to aid in the development of next generation solutions. Their IA solutions encompass a wide range of voice, data and video applications, extending across networked, tactical and satellite systems. IA solutions include the technologies, specifications and criteria, products, product configurations, tools, standards, operational doctrine and support activities needed to implement the protect, detect and report, and respond elements of cyber defense.

CONCLUSIONS

New Opportunities, New Threats. Thus the information revolution, startlingly fast as it is, shows no signs of slowing. As the Defense Force and indeed other Government Departments becomes more technologically sophisticated, it becomes more technologically dependent. We need therefore to use that technological sophistication to avail ourselves of all the opportunities that information, as a target, presents. We also need to be aware that our technical dependencies represent potentially crippling vulnerabilities. Sophisticated, robust, multi-layered defenses for our military information functions may well be what separate us from joining the sorry league of military failures. Information, combined with modern information functions, has distinct characteristics that warrant it being considered a realm, just as land, sea, air, and space are realms.

The competition for information is as old as man's first conflict. It involves increasing and protecting our own store of information while limiting and penetrating the adversary's. The recent explosion in information technologies is prompting the current discussion in and outside government on the topic of information warfare - targeting the enemy's information functions, while protecting ours, with the intent of degrading his will or capability to fight.

Integrated IW as a Critical Success Factor. What everyone agrees on is enormous growth in information technology gives us opportunities we never had before and we must adapt our doctrine and strategy to take advantage of them. IW is a new form of warfare resulting from changing technology, combined with an old strategy of war-fighting targeting our adversaries' decision-making process. With the advances in information technology, the military must pursue information superiority just as they do air and space superiority. Only with these realms under control can they effectively employ all their combat assets. Military information functions are essential to combat operations. They are tools for achieving the Joint Force Commander's campaign objectives. Targeting the enemy's information functions keeps him from achieving his. The ultimate aim? Incorporating information warfare into the way the Defense force organises, trains, equips, and employs.

INTEGRATED INFORMATION OPERATIONS FRAMEWORK

Food for Thought. Information warfare is a concept that is only now beginning to make its way through governmental and military circles. The technology currently exists with which to conduct an IW campaign. Therefore national leaders must reflect on the implications of this new technology in order to develop coherent policy and rules of engagement. Many legal questions remain unaddressed. Intelligence agencies will have to evaluate the benefit of co-ordinated "hacking" and "phreaking" to obtain critical intelligence information while maintaining plausible denial of government involvement.. Military professionals will have to consider IW's impact on operations. They must plan how best to deliver strikes against an enemy command and control infrastructure and to preserve the integrity of their own info sphere. IW will no doubt become the subject of budgetary battles as departments / agencies vie to determine which will be top IW dog.

RECOMMENDATIONS

The Global Village (United Nations). The United Nations affords us the best opportunity for beginning to establish international-security standards. This organisation already has connectivity with all the world’s nations that’s necessary to implement global information-security rules. The UN could extend the scope of its current Security Council or establish a global-information-infrastructure security body akin to its International Telecommunications Union, which allocates bandwidth and establishes, related standards. A UN global information-security organisation would institute standards and provide guidance for security that would permit high-confidence electronic commerce. All the more reason for

South Africa to vie for a permanent seat in the UN Security Council in order to take a leading regional role.

The Regional Village (SADC). The globalisation of information security must be built around two thrusts. First, of course, is military security. The members of the Southern African Development Community (SADC) must agree on alliance-wide information-assurance standards for their own internal systems, not just those in the SADC infrastructure. Separate and distinct information measures won't prove to be an effective barrier to hostile cyberspace warriors. Second, and no less important is civilian-infrastructure security. This is especially vital as militaries increasingly rely on commercial information assets. Billions are transacted electronically every day, which is a tempting invitation to cyberspace criminals.

Our own Village (South Africa). The creation of a Information Assurance Security Framework, (IASF), developed in a collaborative effort by a Cyber Crime & Warfare Workgroup (CCWW) Sub-Committee of the new South African National Security Council. The aforementioned Sub-Committee to be chaired by the State Information Technology Agency (SITA), assisted by solution architects from the CSIR/Defensetek and SACSA. Other core members to be:

* NICOC/MISS laying down the basic security policy/guidelines.
* NIA (as Chief CI Functionary) monitoring adherence, issuing security clearances, investigating security breaches and espionage, sabotage, etc (in conjunction with SAPS).
* The South African Communications Security Agency (SACSA) being responsible for all Government crypto and the ISS National Council which is managed via the Joint Communications Security Council (JCSC) of which the DoD is a part.
* Representatives from the Governments international and security clusters respectively.
* Strategic RSA companies with requirements, component vendors, and commercial integrators, will guide their solution development.

SITA to ultimately enable all IT systems for National as well as Provincial Government. Their Information System Security mandate is as follows:

"To provide information technology, information systems and related service in a maintained Information Systems Security environment to, or on behalf of, participating departments and organs of the State and in regard to these services, act as an agent of the South African Government."

THEY WILL MANAGE THE ISS PROBLEM AS FOLLOWS:

DOD, NIA, SASS, SAPS, Presidents Office

Other Nat/Prov Depts

SITA

(Internal)

Risk Assessment, Policy, Training and Awareness

R & D and Architecture

SERT / Incident Response / DRP

Monitoring and Forensic Audits

Enterprise Systems Application Management

(CAAS, Main Frame, Networks)

The CCWW must find the right solution for environments ranging from outer space to the office or battlefield. Such a framework will provide top level guidance in addition to the specification of essential security features and assurances for Information security products.

Standards. The internationally recognised Common Criteria (CC), employs standardised terms to describe the security functionality and assurance of customer requirements and manufacturers' products. CC-based Protection Profiles specify what customers need at both the system and the component level to accomplish their mission. CC-based Security Targets describe how specific products meet customer requirements.

Mix and Match. Information Assurance solutions must take maximum advantage of commercial components, using own developed products and services to fill gaps in areas not satisfied by commercial offerings. Commercial-off-the-shelf (COTS) products include security products (e.g. a firewall) or security enabled or enhanced Information Technology (IT) products (e.g. an e-mail application or secure cellular phone).

The Will to Implement. Solutions must include technologies and tools necessary for a layered defense-in-depth strategy and tools for defensive / offensive information operations such as intrusion detection, automated data reduction and modelling/simulation tools. The technological means for effective information security are well within reach. What’s required is the will to implement them. Only through a co-ordinated international effort will the countries with the most to lose have an effective base for information security.

War should belong to the tragic past, to history: it should find no place on humanity's agenda for the future.

John Paul II (lived 1920), Polish pope.

Speech, Coventry (1982).