Information Warfare
Part 1 A Fundamental Paradigm of Infowar

Originally published February, 2000

by Carlo Kopp

© 2000, 2005 Carlo Kopp

The turn of the millennium is a good time for reflection, and this is very much true for the issue of Information Warfare. Created as a paradigm during the early nineties, Infowar is today a fact of life, as much as many may still scoff at the idea.

Being tasked with producing a two part series on Infowar presented some interesting questions ? Would another dry technical analysis of offensive and defensive measures be appropriate ? Upon reflection I realised that the dry technical issues have mostly remained unchanged since Systems covered the subject two years ago.

A much bigger issue has arisen in recent years. It is rejection of the Infowar paradigm itself. Infowar sceptics/opponents/detractors seem to find endless reasons to deride and reject this ostensibly nineties phenomenon. I have seen assertions to the effect that "there is no such thing as Infowar", "Infowar is a transient fad", "Infowar lacks intellectual rigour", "Infowar is really Electronic Warfare", indeed this list of nonsensical assertions could be extended considerably.

Since I have little patience with fools, I hereby present a basic and fundamental paradigm of Information Warfare:

A Fundamental Paradigm of Information Warfare

To most of the public, Information Warfare (IW), and broader Information Operations (IO), conjure up the image of Middle Eastern terrorist types

paying vast amounts of cash to unkempt Eastern European crackers, who dig into the depths of the vast US DoD computer network, extracting vital secrets and compromising vital operations. Indeed, this Gibsonian image has captured the imagination of the media and Hollywood alike, and has become another one of the urban myths which are blindly accepted as a fundamental truth outside the inner circle of the professional IW theorists. Alas, Gibsonian cyberwar is but one facet of a much more complex reality.

In the most general sense, IW/IO are all operations which are conducted to exploit information to gain an advantage over an opponent, and to deny the opponent information which could be used to an advantage. To be pedantic, I would have preferred to see "information" replaced with "knowledge", insofar as in a more practical context "information = knowledge + garbage", if we look at much of what passes as "information" these days. A really vociferous defender of the established nomenclature can rightfully argue that Shannon's definition of "information" makes the established IW/IO nomenclature the proper one. The truth is that few people in my experience understand Shannon's theorems, let alone could place them into the context of IW/IO ! Muddled enough with issues of nomenclature ?

I am sure many IW/IO purists will no doubt lambast my frivolous treatment of nomenclature, however I think some frivolity doesn't hurt since it underscores the fact that too many formalisms can frequently obscure the deeper truths !

Exploring the taxonomy of IW/IO, we have Cyberwar, essentially involving the organised cracking of other people's systems, to spy, to deceive and alter, or to deny services. We also have the historically well established discipline of Propaganda, Psychological Operations or "Perception Management", essentially the use of information to confuse, deceive, mislead, destabilise and disrupt an opponent's population and armed forces. Then we have the Second Oldest Profession, the well proven art of intelligence/espionage and its sibling, the theory of deception, aimed at divining secrets from an opponent, inserting falsehoods into their perception of reality, and preventing the opponent from doing the same.

This however is only part of a much bigger picture. The well established discipline of Electronic Combat/Warfare (EC/EW), or Radio-Elektronnaya Borba (REB) in the nomenclature of the thankfully now departed Soviet Empire, deals with the jamming and destruction via hard kill of an opponent's radars and communications, and the prevention of an opponent from doing the same. Indeed there is much confusion in many parts of the EC/EW community, to this very day, with many using the terms EW and IW interchangeably. This is unfortunately a misleading simplification. Many of the fundamental paradigms in EC/EW are common to IW/IO, but this is because they are a subset of IW/IO.

The breadth of IW/IO as a discipline, its sheer complexity, and the overlapping of many if its constituent components has created many unfortunate side effects. One is that it has produced numerous opportunities for fringe players in all related disciplines to assert their paradigm as being central, thereby creating much fodder for IW/IO sceptics. Indeed, in many organisations the paradigm has produced distinct internal turf wars, as various players try to expand their respective internal fiefdoms to absorb as much of the paradigm as possible, and thus available budget. There is plenty of anecdotal evidence of this, much of which is best left unprinted.

Is there a fundamental underlying truth which we can distill from this babel of terminology, doctrine, strategy and technique ?

Perhaps the simplest way of defining what IW/IO is all about, is to say that any organised use or manipulation of information/knowledge which produces an advantage in a contest with an opponent, constitutes an aspect of IW/IO. Whether the use or manipulation is applied against the wetware in an opponent's head, or the software and hardware in an opponent's technological base, is a matter of instantiation.

My fellow IW/IO theorists will no doubt be yawning by now: "where's the punchline, Carlo ?".

The punchline is a very simple one:

The fundamental paradigm of IW/IO appears to be a basic evolutionary adaptation resulting from competition in the survival game. Whether it is the game of chemical deception played by a micro-organism against an immune system, or the use of camouflage and deception by prey and predator alike in every tier of the natural world, or whether it is some part of the complex structures we use to describe the modern IW/IO paradigm, the fundamental paradigm is essentially one and the same.

Therefore quibbling over definitions and demarkation boundaries, which characterises a large part of the public and not so public debate on the subject, is simply complicating a very simple and fundamental idea.

If we are to apply a classification scheme to the most basic strategies in IW/IO, they can be divided into four simple categories:

A) denial of information (DoI), ie concealment and camouflage, or stealth.

B) deception and mimicry (D&M), ie the insertion of intentionally misleading information.

C) disruption & destruction (D&D), ie the insertion of information which produces a dysfunction inside the opponent's system; alternately the outright destruction of the system.

D) subversion (SUB), ie insertion of information which triggers a self destructive process in the opponent's target system.

The latter D in D&D is not the same as DoI, insofar as the opponent is not denied knowledge of one's presence, but is denied the means of precise identification and engagement. A case of knowing the other player is there, but being blinded to his movements. SUB frequently requires the use of DoI, D&M or D&D to initiate the self destructive process, and is thus arguably a "two tier" strategy.

It takes little effort to isolate examples of each of these strategies in almost any domain where the IW/IO paradigm can be applied. I will instantiate this model with three domains - the insect world, electronic combat, and cyberwar:

In the insect world, these examples will do:

A) DoI - stick insects, variously camouflaged beetles, moths and other bugs, who do their best to blend into the background.

B) D&M - harmless insects which mimic the appearance of dangerous predators such as wasps, stinging ants or arachnids.

C) D&D - beetles, bugs and roaches which spray noxious fluids on predators, thereby blinding and numbing the predator's visual and olfactory senses, temporarily or permanently.

D) SUB - predatory insects which emit analogues of the mating pheromones of other species, or mimic the appearance of food, to lure prey. D&M is used to trigger a programmed response which leads to self destructive behaviour.

Moving a few tiers up the chain, to electronic combat in air warfare:

A) DoI - the stealth fighter which uses shape and absorbers to disappear from radar, and a cooled jet exhaust to hide from infra-red equipment.

B) D&M - the defensive jamming equipment on a fighter which emits signals similar to radar returns from a hostile radar, but including an erroneous position measurement.

C) D&D - the high power noise jamming equipment which blinds an opposing radar so it cannot see an approaching bomber, and/or disrupts the radio communications linking radars and weapons, or the

HPM or EMP weapon which toasts the radar and supporting computers and communications.

D) SUB - the use of deceptive signals which trigger the premature initiation of weapon fuses, such as proximity fuses on guided missiles.

Finally we look at cyberwar:

A) DoI - the use of encryption and concealment to prevent unwanted parties from reading or finding what they ought not to.

B) D&M - the use of various techniques for masking the identity of a penetrating party into a network or a system.

C) D&D - any denial of service attack, from "ping of death" to an EMP bomb.

D) SUB - logic bombs, viruses and other destructive programs which use system resources to damage the system itself.

We could continue instantiating this paradigm exhaustively, chewing through encyclopedias, catalogues of micro-organisms, stacks of biology texts, mountains of military history, or archives of information security bulletins.

It is interesting to note that these strategies are neither mutually exclusive, nor confined to either side of the predator/prey or offensive/defensive game. Some may be favoured more by particular predators or prey, but in principle either player can use any or all.

The generality of this model for a number of known and extant domains can be easily shown, and in the context of modern IW/IO, cyberwar and EC/EW are more than good enough to satisfy this.

Can we extend this model indefinitely and declare it to be a truly universal theorem ? In the sense of a rigourous mathematical proof, this is tricky, since it essentially requires that we prove that no other strategies can exist to achieve the same effects, across all possible domains. This is arguably an impossible task.

We can however exploit Shannon's information theory, and assuming a channel with a finite and bounded bandwidth, show that the first three strategies derive from very fundamental and simple models:

A) DoI amounts to making the signal sufficiently noise-like, that a receiver cannot discern its presence from that of the noise in the channel.

B) D&M amounts to mimicking a known signal so well, that a receiver cannot distinguish the phony signal from the real signal.

C) D&D amounts to injecting so much noise into the channel, that the receiver cannot demodulate the signal.

This is as basic a representation of these three models as is possible. Showing the fundamental nature of the fourth model, subversion (SUB), is a little trickier since it relates to system internal behaviour. The manipulation of a channel carrying information is a means to an end.

D) SUB at the simplest level amounts to the diversion of the thread of execution within a Turing machine, which maps on to the functional behaviour of the victim system. It amounts to surreptitiously flipping one or more specific bits on the tape, to alter the behaviour of the machine.

In the bounded context of IW/IO as defined above, we can quite comfortably accept the "four strategy" model as being the most basic structural paradigm which exists for the phenomenon. The abundance of examples in the biological world merely underscores the fundamental nature of IW/IO.

IW/IO sceptics/opponents/detractors should carefully consider their fundamental premise at this point in the argument - can you disprove the existence of IW/IO strategies as survival tools in a competitive universe, driven by the survival of the best adapted ?

A single counterexample would suffice to disprove their premise.

QED.

Why Information Warfare at the turn of the Millennium?

The next interesting question we can ask is why IW/IO now, if it has been such a great part of our established reality for so long ? Indeed this could be said to be the crux of many doubters' basic rejection of the paradigm.

The simplest answer is to point out that until recent times, the basic strategies of IW/IO were embedded, implicitly, within a great number of very diverse disciplines many of which had few obvious connections. All of this changed as we began the transition from smokestack industrial age economies to "digitised" information age, knowledge based economies.

For centuries, the knowledge required for the basic economic processes of wealth creation, and the art and science of war, were locked away in the heads of members of occupations, vocations, professions and guilds. If you wanted a sword you went to an armourer, if you wanted a loaf of bread, a

baker. Knowledge of processes was passed down, generation by generation, largely by word of mouth. Every once in a while some bright individual produced a new idea, which proliferated, and those who used it gained an economic or military advantage against other players.

The value of knowledge is that it ultimately provides for a recipe to perform a specific task or set of tasks, or to perform them more successfully. If these tasks pertain to wealth creation or warfare, both competitive and survival centred social activities, that knowledge carries within itself an inherent survival value. The more effective the knowledge is when applied to such competitive activities, the greater its value.

Gutenberg's printing press produced the technological foundation for the industrial age, since it allowed the dissemination of exact copies of pieces of knowledge to a wide audience. Ultimately, by purchasing a decent pile of engineering or process textbooks and digesting their contents, anybody could go out and manufacture whatever they chose to make. The industrial age postal system combined the time proven courier with the printed message to produce a robust means of accurately transmitting knowledge.

It is worth noting that one of the first large scale uses of the printing press was to wage the propaganda war between the reformation clerics and the Catholic church.

Economically and militarily valuable knowledge has always been a jealously guarded secret, and this justifiable paranoia about it not falling into the wrong hands became a major issue during both of the industrial age world wars. The complexity of some of the espionage and deception strategy plays during this period is quite remarkable. The industrial age boom in the West would have been impossible without printed textbooks, papers and replicated drawings. It is also significant that the Soviet revolutionaries used the press to great effect, as did Hitler and Mussolini who also exploited cinema and radio, the precursors of the modern electronic media.

The postwar development of genuine electronic media, followed by the development of the digital computer and its mass production, set the stage for the transition to the modern information age we live in. Combining the digital computer technology base with the well established technologies of analogue communications provided the basis for the modern digital communications network, and ultimately the Internet.

The fundamental change which arose with the proliferation of computing and digital technology is the speed with which knowledge (and garbage information as well) can be transmitted and processed. This is a pervasive paradigm . Whether we are replacing cheques and letters of credit with EFT protocols, FTP-ing production data between sites, emailing correspondence or research data, or datalinking target coordinates between bomber and

guided weapon, the digital technology base allows almost instantaneous and almost error free transmission of knowledge.

Many contemporary military theorists identify the greatest value of the digital revolution as being "coordination, speed and precision", in the context of destroying an opponent's forces. In the context of a modern economy, the same speed and precision characteristic of a well implemented digital system means that many processes can be greatly accelerated, and hitherto unseen levels of coordination between multiple players achieved. This is true of finance, stock markets, manufacturing, research and development. Therefore those economic players who master the digital environment can potentially acquire a huge competitive advantage over those who do not. This is especially true in commerce. Not surprisingly, extremist special interest groups, ultra-nationalists and proto-fascist parties have taken to the digital revolution with alarming alacrity.

Speed, coordination and precision are decisive advantages in the economic, military and political games, and the military term "force multiplier" describes the effects of well implemented "digitisation" upon an organisation very nicely. Such an organisation can produce results out of all proportion to its size, compared to its industrial age equivalent.

The possession of a digital infrastructure is one of the key determinants of military power and economic strength today. It should not be surprising that the Asian meltdown had little effect in Australia, the most digitised economy in the region.

The digital infrastructure is the enabling technology base for the current globalisation paradigm, and its proliferation is in no small part responsible for much of the economic restructuring in OECD nations.

If current trends continue the world will be divided into two major classes of nation, wealthy developed nations with large digital infrastructures, and poor industrial and agrarian economy nations with non-existent or weak digital infrastructures. In developed nations, wealth will concentrate in the hands of those who master the digital infrastructure, and those who cannot will become increasingly poorer. Mastering the digital revolution is no different from mastering the printed word, centuries ago. The rewards accrue to those who exploit the technology most effectively.

Every major paradigm in technology, and its associated changes in the patterns of wealth and military power, has spawned conflict. Indeed much of the Marxist paradigm of class warfare is predicated on this model. In a sense it is curious that the Sovs fell on their own sword, having never mastered the digital revolution.

The digital revolution is no different, with disaffected minorities in developed nations making themselves known. The Seattle WTO riots, the

proliferation of extremist websites, and the increasing popularity of ultra-nationalists like the Hansonites in Australia, and similar parties and groups in the EU and the US are all examples.

On an international scale, we see the growing influence of fundamentalist Muslim popular movements in the Islamic nations, and an increasingly hostile and disaffected Russia, China and to a lesser degree India. Of the three, only India has a decent foothold in the digital age, with China critically dependent upon commodity manufacturing for developed consumer markets, and Russia slowly disintegrating. Most South East Asian nations have also fallen foul of the digital revolution, indeed the rapid and massive withdrawal of investment capital during the Asian meltdown could not have been executed without the modern digital infrastructure.

The importance of IW/IO today is a simple consequence of the reality, that the digital infrastructure in the developed world processes, concentrates and carries the flow of knowledge which provides us with our decisive economic and military advantage against other players. The same effect, on a lesser scale, applies within developed nations, dividing those who accumulate wealth from those who cannot accumulate it.

The digital infrastructure is thus a lucrative target, in every sense, since it provides a single point of failure for the developed world's economic and military power base. It is also a capable weapon for penetrating our economic, military and political fabric, exploitable by foreign and domestic players with hostile agendas.

Consider an ostensibly benign medium like the Usenet news group. I have witnessed this medium being used for the propagation and dissemination of malicious conspiracy theories, racist propaganda, ultra-nationalist Russian and Serbian propaganda, neo-Stalinist propaganda and Stalinist re-interpretations of history, anti-Semitic propaganda, and plain military dis-information during the Serbian air war, all on the one newsgroup ! Whether we define the boundaries of warfare to be confined by classical Marxist "class warfare" between mutually opposed domestic groups, or nation states, black propaganda (ie fibbing) is a tool of warfare. The very same newsgroup which provided one of the key platforms used to demolish the mischievous Arnett/CNN Tailwind "nerve gas canard" was at the very same time being used as a propaganda platform by Russian ultra-nationalists and neo-Stalinists !

During this same period a major aerospace vendor was caught on the same newsgroup, when several corporate public affairs personnel using third party ISP addresses to conceal their identities, argued the merits of their products over a competitors' !

The highly effective use of a website and newsgroup advocacy by Australia's Hansonites during the peak of their popularity, two years ago,

underscores the value of the digital infrastructure as a political and propaganda tool, and thus an instrument of both intra-national and international warfare.

Not surprisingly the NATO website was subjected to a range of Serbian denial of service attacks during the Serbian air war, while the USAF were at the same time claimed to be hacking into Serbia's air defence network to insert misleading information. Equally it should come as no surprise that the Indonesian foreign affairs ministry website was hosting, during the peak of the Timor crisis, an almost comical package of nasty and untruthful anti-Australian excerpts from the ultra-nationalist Jakarta press. Comically inept to knowledgeable parties but nevertheless qualifying as black propaganda of the most classical kind.

Gibsonian cyberwar may have indeed captured the public imagination as the most critical aspect of the IW/IO paradigm, but if history teaches us anything, the use of new information distribution media to wage propaganda wars may be the area in which the greatest political and military impact is seen.

Arquilla and Ronfeldt defined the paradigm of "Netwar" to describe the emergence of diffuse, often trans-national, distributed forms of warfare, in which the players are largely hidden to avoid conventional attack, using the general populace to hide within. It is no coincidence that Netwar emerged strongly as an issue during the nineties (even if much of the basic paradigm has been central to terrorist and guerilla movements for most of this century). The digital infrastructure has been an enabler for Netwar, providing global and near instantaneous connectivity. Indeed global digital media such as the Iridium LEO constellation are a tremendous tool for exactly this kind of political or military play.

There can be no doubt that the digital revolution has brought about some very fundamental changes in today's world, the full impact of which we have yet to see. Part 2 will explore current issues in IW/IO.

$Revision: 1.1 $
Last Updated: Sun Apr 24 11:22:45 GMT 2005
Artwork and text © 2005 Carlo Kopp