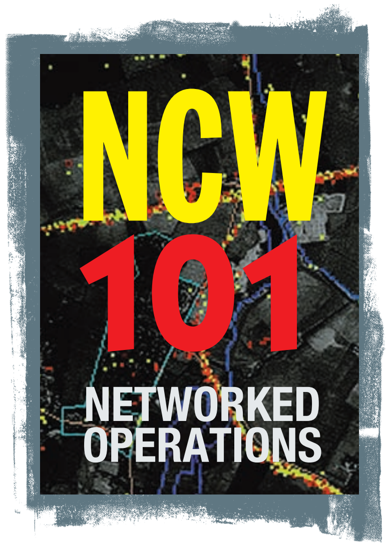
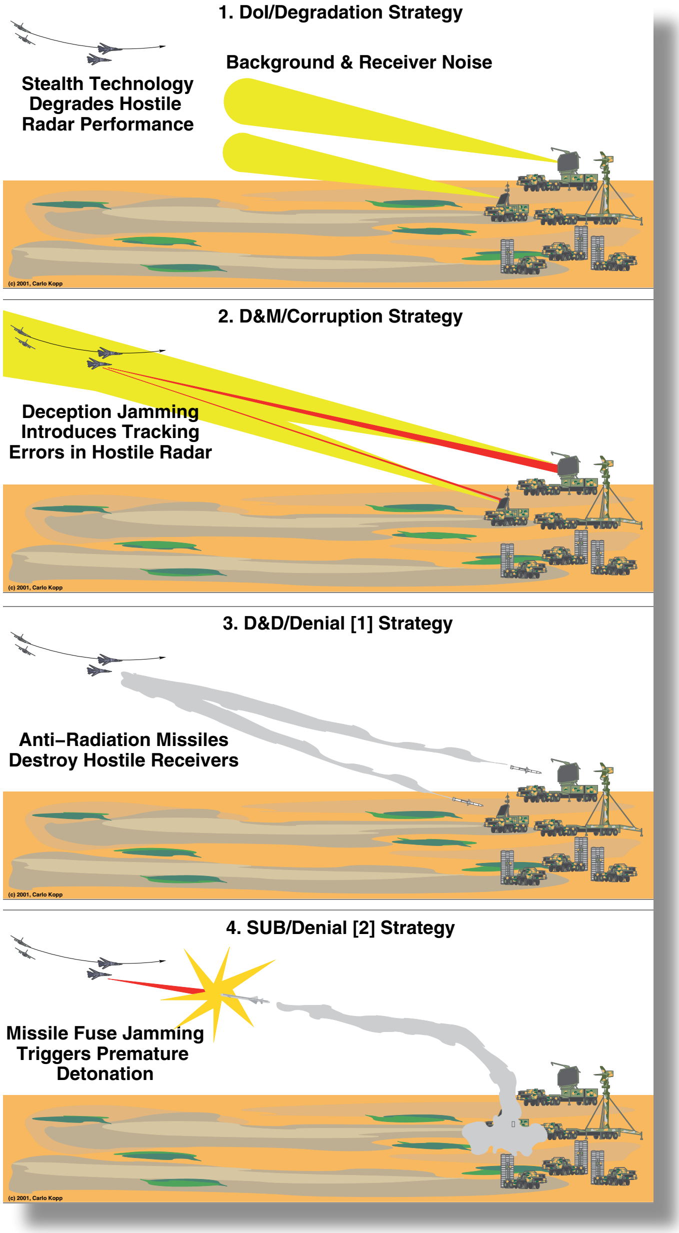


Fundamentals of Information Warfare

NCW 101 Part 14

Dr Carlo Kopp

Network Centric Warfare (NCW) is about gathering, processing and distributing information to accelerate the Observation Orientation Decision Action (OODA) loop. Reliant on the technology of digital computing and networks, NCW is inextricably intertwined with Information Warfare, which impacts every single aspect of a networked military system.


1. DoI/Degradation Strategy
Background & Receiver Noise
Stealth Technology Degrades Hostile Radar Performance
(c) 2001, Carlo Kopp
2. D&M/Corruption Strategy
Deception Jamming Introduces Tracking Errors in Hostile Radar
(c) 2001, Carlo Kopp
3. D&D/Denial [1] Strategy
Anti–Radiation Missiles Destroy Hostile Receivers
(c) 2001, Carlo Kopp
4. SUB/Denial [2] Strategy
Missile Fuse Jamming Triggers Premature Detonation
(c) 2001, Carlo Kopp

What is Information Warfare?

Information Warfare (Infowar, IW) is a broad term often abused and misrepresented, which encompasses the “use of information to gain an advantage in a competitive survival contest”, be it biological or social. Thus in warfare, being effectively a fusion of both of the latter, IW is central to most aspects of war.

IW is for all intents and purposes an umbrella term covering a wide range of issues, problems, techniques, strategies and practices. As such IW can be divided into a range of constituent areas.

Cyberwar is the use of hacking or penetration of an opponent’s computer systems and networks to gather information, contaminate information, or to effect denial of service attacks against an opponent’s computing and networking infrastructure. Cyberwar is often misrepresented as IW, mostly by proponents or advocates of Cyberwar.

Electronic Warfare (EW) is the use of a range of techniques intended to either deny the use or deceive an opponent’s electromagnetic sensors and communications, including wireless networks. Not unlike Cyberwar, many advocates of EW claim IW to be EW, again misrepresenting the scope of the problem.

Deception theory, as applied to intelligence operations, and propaganda of the military, political, ideological, religious or commercial ilk, is also deeply steeped in IW techniques, even if many adept practitioners remain unaware of this fundamental relationship.

Camouflage techniques intended to conceal military assets and infrastructure from the prying eyes – or sensors – of an opponent are another subdiscipline of IW.

This particular division of IW into categories, although not exhaustive, is based essentially on the area of application. A different division proposed by IW pioneer Winn Schwartau during the early 1990s is by the severity of the attack, with focus on applications in computing and networking. Schwartau’s model breaks down into four categories:

Class I IW - Compromising Personal or Corporate Privacy is the lowest grade of IW, and occurs when for instance an individual’s personal account is compromised and confidential information accessed, such as email read or phone calls charged to an account.

Class II IW - Industrial and Economic Espionage is the next step up, in which instance government or corporate computers are hacked into and information covertly stolen. Class II IW is on the rise, if recent allegations pertaining to the Euro-US trade negotiations are believed.

Class III IW - Info-Terrorism and Denial of Services. The intentional trashing of another party’s computer or network, or denial of service via other means is usually described as ‘info-terrorism’. Whether the offending party is a malicious hacker, a criminal extortionist, a genuine terrorist (who probably regards himself as a martyr to whatever cause), or a foreign government seeking to take down a system or systems, the end result falls into the same category.

Military IW - The use of all of the above combined with other military techniques in order to disrupt an opponent's military operations, government activity and economy qualifies as Military IW, which is the most destructive type, as it involves both soft and hard kill techniques.

Information Warfare as a research discipline is immature, the term itself being less than two decades old. As an area of practice, in human social systems it dates back to the beginning of organised societies. The label 'second oldest profession' applied to espionage speaks for itself.

It is important to consider that IW is biological in its nature and its origins. Microorganisms were deceiving each other and larger organisms to gain a survival advantage well before the advent of humans, primates or indeed even mammals. The fossil record and contemporary species of every genus display in one way or another manifold evolutionary adaptations to this effect. That species spanning insects to large predators display complicated camouflage, mimickry or behavioural adaptations intended to conceal from or deceive an opponent makes a compelling case study of the extent to which evolution has favoured IW as a survival technique.

In the context of networked military systems we are specifically interested in three facets of IW, these being Cyberwarfare and its impact inside networked systems, electronic warfare and its impact on both sensors and channels used in the networked system, and camouflage techniques in as how they impair the ability of a networked system to gather information.

The Four Canonical Strategies of Information Warfare

The formal identification and mathematical formulation of the Four Canonical Strategies of IW is a relatively recent development. In late 1999 Dr Andrew Borden, a retired US Air Force mathematician, identified the first three strategies and defined them in terms of Shannon's information theory, the basis of modern digital communications, and effects on the channel. Concurrently, this author was independently researching the same problem, and produced a definition of the four strategies, also in terms of Shannon's information theory. US theorists in mathematical IW usually refer to this model as the "Borden-Kopp Model of IW". It remains the only mathematically robust definition of fundamental effects in IW, and has become the basis for other mathematical modelling performed in the area.

The starting point from which we can appreciate the four strategies best is Shannon's notion of information and the idea of a "channel" carrying information.

The so called Shannon-Weaver model of information is usually cited thus: 'The quantity which uniquely meets the natural requirements that one sets up for "information" turns out to be exactly that which is known in thermodynamics as entropy.'; 'Information is a measure of one's freedom of choice in selecting a message. The greater this freedom of choice, the greater the information, and the greater is the uncertainty that the message actually selected is some particular one. Greater freedom of choice, greater uncertainty, greater information go hand in hand.' (Sveiby 1994). Working through Shannon's theory, a level of detail superfluous for this discussion, leads us to Shannon's model of the channel.

The model has five key components: The 'information source' which generates messages containing information; The 'transmitter' which sends messages over the 'channel'; The 'channel' and associated 'noise source', this could be any number of physical channel types including copper or optical cable, radio link or acoustic channel; The 'receiver' which detects and demodulates messages received over the 'channel'; The 'destination' or 'information sink' which responds to messages by changing its internal state. It is implicitly assumed that messages sent by the 'information source' can be understood by the 'sink'. Refer Figure 2.

In Shannon's model, 'channel capacity' or the measure of how much information the channel can carry is of interest. The maths distill down to a very simple expression, as: Capacity = Bandwidth X Log2 (1 + Signal Power / Noise Power). Deceptively simple as this might be, it has profound implications for systems that transmit or gather information. Both bandwidth and signal power can be increased to improve the capacity of a channel, while noise or impairments to bandwidth and signal power diminish channel capacity.

An attacker has a number of options available to reduce or indeed eliminate the capacity produced by a channel – that channel being possibly a radio datalink or a sensor used to gather information. These options turn out to be the four canonical strategies.

> While IW may have a vast number of manifestations in social, technological or biological contexts, the deeper reality presents a huge advantage to a practitioner who understands the formal models, and is prepared to aggressively apply them to solving real world problems.

The first strategy is usually termed Degradation, and sometimes Denial, achieved by burying the signal flowing through the channel in noise and thus driving channel capacity down to zero. In simpler terms, the channel is prevented from carrying useful amounts of information by degrading it with noise.

There are two forms of this strategy. The first is the active form of degradation, exemplified by noise jamming in EW. The attacker basically injects noise into the channel to degrade capacity. The second form of this strategy is the passive form. It is characteristic of stealth, camouflage and spread spectrum Low Probability of Intercept (LPI) communications, where the power in the channel is driven to zero, driving capacity down to zero. In effect the message carrying information to the victim of the attack is made so faint it becomes buried in background noise.

An important consideration is that the passive form is covert, in the sense that the victim does not know an attack is under way. Conversely, if the active form is used, the victim knows an attack is under way.

The second strategy is usually termed Corruption, and some times Mimicry. This strategy involves the attacker using a signal that mimics the victim's signal so well that it cannot be distinguished from the real signal and is used instead. The result is that the victim accepts corrupted information – of the attacker's choice – rather than real information. Corruption is inherently covert as the victim will reject it otherwise.

Corruption is characteristic of a plethora of deception jamming techniques in EW, as well as being the dominant form of deception used in intelligence and propaganda operations, be they political or commercial, and in identity theft in Cyberwar. In biological systems it is exemplified by a vast number of organisms that mimic other species to scare away predators.

The third strategy is termed Denial, and sometimes Destruction. This strategy involves the simple expedient of damaging or destroying the victim's receiver or the transmission link, so its capacity is reduced to zero either temporarily or permanently. Whether an anti-radiation missile or smart bomb used against opposing radar or communications sites, a high power electromagnetic weapon, a hacking denial of service attack, or an organism squirting a noxious excretion into the eyes and nose of its victim, Denial always involves an overt and direct attack on the victim apparatus providing the channel.

The fourth strategy is the only one that does not directly impair the channel and is usually termed Denial via Subversion or simply Subversion. Attacks using subversion are such attacks that penetrate the internal functions of the victim to compel it to do something self destructive using its own resources to damage itself. The plethora of virus and worm programs present good examples, as do the wide range of biological examples where the victim organism is usually biochemically subverted to serve a parasite of some kind. Usually a Corruption attack is employed to penetrate defences and implant the self destructive directive.

Careful analysis of the behaviour of these strategies and extensive study of examples and case studies shows that even complicated multi-channel and multi-faceted deceptions can be broken down into a collection of more basic attacks, often mutually dependent but each comprising only one of the four canonical strategies. From a science perspective these strategies can be said to be atomic in the sense that they are simplest forms, from which all other more complex forms are constructed.

It is one of the realities of nature that something of extreme complexity, such as strategic deceptions, can be broken down into an interconnected web of mutually dependent but essentially simple forms of attack.

What the four canonical strategies demonstrate is that the vast footprint of various IW techniques can all be broken down and modelled mathematically, or in simulations.

IW – The Practical versus the Theoretical

For decades, deception has been seen as an art and disciplines like EW as a science, albeit one containing a good measure of undisclosed black art. The deeper reality is that all of IW can be reduced to mathematical models and is thus science. Not surprisingly, the discipline of IW is now divided into two camps: one being theorists and practitioners with science backgrounds who prefer the mathematical approach to solving problems, and the other camp being those with humanities backgrounds who often reject the mathematical approach. Like many immature disciplines, the study of IW may take some time before it settles into maturity. Until then, publications on IW will continue to follow two often divergent tracks.

In looking at networked systems the fundamental theory of IW is valuable since it provides simple clearly defined criteria for validating, assessing and testing functional attributes.

A notional example might be an assessment of a new radio datalink technology, which is to be incorporated into a networked system.

Considering the first canonical strategy, the following questions could be asked:

How well does the datalink achieve the ideal aim of the passive form of degradation? Can this datalink be easily detected and identified?

How well does the datalink achieve the ideal aim of resisting attacks in the form of degradation? How well does it resist a narrowband or wideband noise jammer? How much channel capacity will it lose when being jammed in this manner.

Looking at the second canonical strategy, other questions emerge:

How good is this datalink at rejecting a deception jammer that might retransmit delayed copies of earlier messages, or might produce dummy messages? Can the datalink reject fabricated messages with no penalty in throughput performance?

Assessing in the context of the third canonical strategy can be trickier, insofar as the ability to evade attack by a smart weapon may be more a function of the platform carrying the datalink, than the datalink itself. A useful question that remains is whether the datalink equipment can resist attack by an electromagnetic weapon, such as a high power X-band phased array radar on a combat aircraft, or a microwave bomb. This is not unlike the question about the resistance of an electro-optical system to blinding by an opponent's laser.

The fourth strategy, Subversion, also presents good questions. Is the level of cryptographic security in the datalink such that hostile penetration can be ruled out? This is of course a trick question, as the cryptographic security problem, which strictly speaking falls under the second strategy, involves the rejection of mimicked messages. But are there any functional vulnerabilities in the datalink subsystem that may be triggered by a mimicked message, to the detriment of the system.

Whether designing datalink equipment or sensors, or assessing them for acquisition, the canonical strategies provide an intellectual framework for determining the vulnerability and susceptibility of the product to attack, and its integrity when under attack. The historical alternative of arbitrary checklists of performance parameters has one fundamental drawback – it is not inherently exhaustive. The four canonical strategies, being so fundamental, are exhaustive when the various permutations are considered relevant to compound attacks that the potential victim system may have to confront.

The forensic analysis of deception operations, either those being crafted or those being carried out by an opponent, also demonstrably benefits from the use of the canonical strategies as a tool.

While IW may have a vast number of manifestations in social, technological or biological contexts, the deeper reality (that all are driven by the same mathematics) presents a huge advantage to a practitioner who understands the formal models, and is prepared to aggressively apply them to solving real world problems.

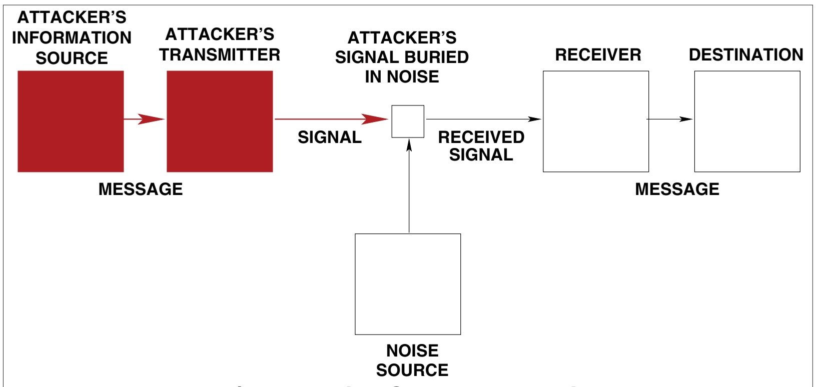
Further Reading:

http://www.csse.monash.edu.au/courseware/cse468/2006/subject-info.html

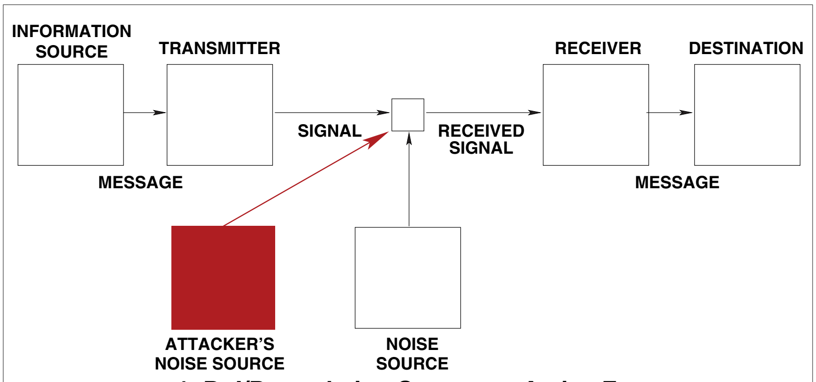
http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html

http://www.ausairpower.net/OSR-0200.html

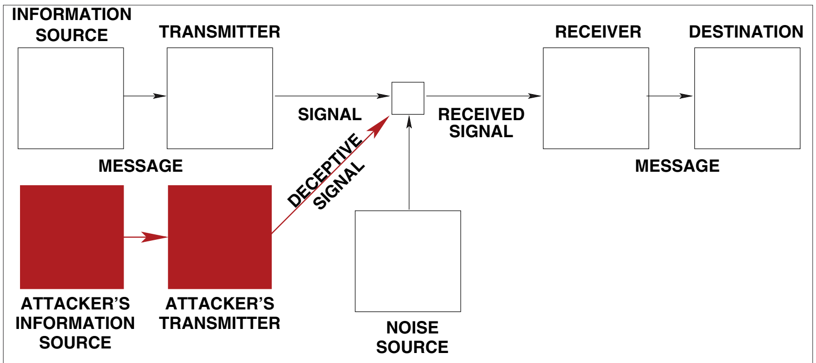
http://www.au.af.mil/info-ops/theory.htm#bordenkopp



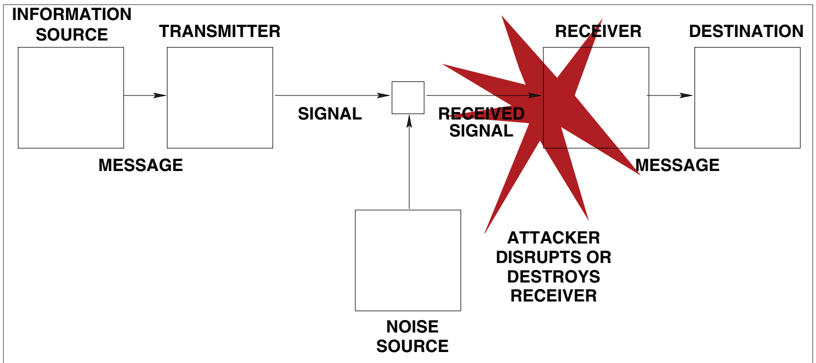
1. DoI/Degradation Strategy – Passive Form



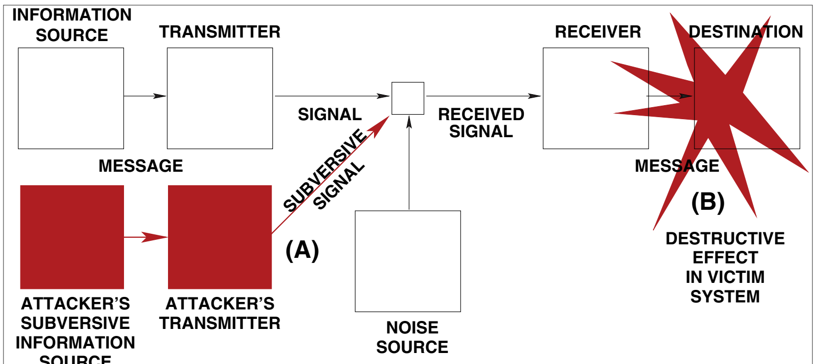
1. DoI/Degradation Strategy – Active Form



2. D&M/Corruption Strategy



3. D&D/Denial [1] Strategy



4. SUB/Denial [2] Strategy