FREE to delegates at 2008 Singapore Air Show

January/February 2008
$7.95

STRIKE PUBLICATIONS

Defence today

DEFENCE CAPABILITIES & HOMELAND SECURITY

2008 Singapore Air Show issue

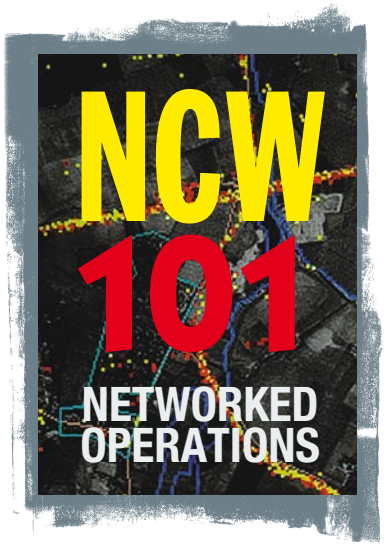
New trends in UAVs

Wedgetail update
AEW&C interview

F-22 stands up in Alaska

AIR7000
Link with US Navy BAMS

Print Post PP424022/00254
ISSN 14470446
64
9 771447 044001



Information warfare vs networks

NCW 101 Part 16

Dr Carlo Kopp

Networking capabilities are the 'plumbing' of any Network Centric Warfare (NCW) oriented warfighting system. Therefore, the application of Information Warfare (IW) techniques against networks can be highly profitable, if successful.

As with ISR systems, the traditional approach to discussing this problem is typically split into two separate discussions, one dealing with technical Electronic Warfare measures against network equipment, and another dealing with network penetration and 'cyberwar' style attacks. Again, as with ISR systems, this way of looking at the problem is increasingly problematic as increasing levels of integration in networked systems evolve. How do we best differentiate between the various ways a network can be attacked? Is an attack against the channel more profitable than an attack using 'cyberwar' techniques?

As with ISR systems, the more general approach to this problem is to look at the deceptive measures in the framework of the four canonical strategies of IW (refer previous two NCW101), and identify what the attack is targeting and how it does so. Repeating the model applied to ISR systems, we look at the victim networked system as a system, rather than its disparate parts.In exploring the problem of IW attacks against networks, it is useful to employ a functional model for a network. Happily, the OSI layered model and its IETF analogue are widely used for this purpose, refer Figure 1. In practical terms, the functions of the network protocols used to carry data across the network can be divided thus, using the more finely grained OSI model:

Application – programs running across the network.

Presentation – formatting and encryption of data used by applications.

Session – managing the state of the network session.

Transport – managing link traffic reliability (and flow).

Network – finding paths through the network and global addressing.

Data Link – immediate addressing of packets, some error control and management.

Physical – radio frequency, optical or cabled link waveforms and signalling.

When a networked application wishes to communicate over the network with another, the message it sends flows down this 'protocol stack' until it reaches the physical layer which uses hardware to effect the message transmission. At the receiving end, the message flows up the stack until it reaches the receiving networked application software. Flowing down the stack, the message is progressively encapsulated with packet header blocks, each containing layer specific directives required to effect the transmission. Flowing up the stack at the receiving end, these header blocks are stripped off, read and interpreted.

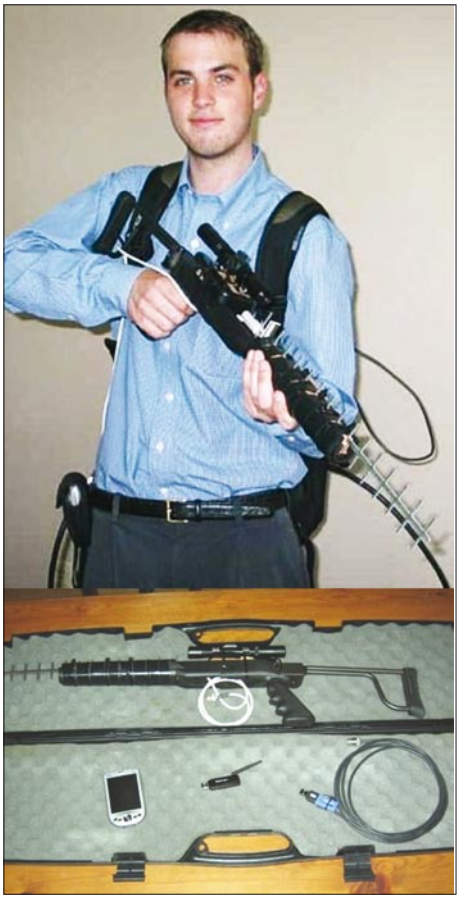
The simplest analogies are the 'onion skin' or 'Russian doll' models - the nugget of information embedded in the data of a message being transmitted between two networked applications is progressively wrapped up in layers of protocol data, sent across the channel, and then progressively unwrapped as the protocol data is stripped away.

A common example is an ADSL broadband connection, where the ADSL modem/router device performs the Physical and Datalink layer functions over the telephone wires, but also part of the routing function associated with the Network layer. The computers at either end perform the functions of the upper layers in the stack. A more specific military example is the carriage of TCP/IP Internet Protocol traffic over the JTIDS/MIDS networking channel, where the JTIDS terminals and channel play an analogous role to the ADSL modem/router in the broadband connection.

Many of the four canonical strategies can be employed against more than one of the seven layers in the OSI model. The complexity of modern networked systems creates many such opportunities, and architects of such systems must be mindful of this.

Eavesdropping and geolocating an opponent's network terminals is now a common practice in the signals intelligence and electronic reconnaissance game. Depicted (above) an Israeli G550 Shavit ELINT aircraft, and an IAI Heron UAV (right).

The Defcon 2004 hacker conference saw the debut of the 'BlueSniper' gun, built by John Hering, James Burgess and Kevin Mahaffey. This device allows an eavesdropper to capture Bluetooth traffic from mobile phone headsets, Blackberries, PDAs, computers and other devices from well over a one kilometre distance. A construction guide for an improved variant is also available at http://www.tomsguide.com/us/how-to-bluesniper-pt1,review-408.html . Numerous examples of 'Bluetooth sniffer' software tools are available free on the Internet, refer http://bluetooth-pentest.narod.ru/ .



Passive Degradation Attacks

Degradation attacks are intended to bury the signal in noise, hiding it from an opponent. All forms of camouflage and concealment fall into this category, as does Low Probability of Intercept (LPI) and crypto technology. Such attacks primarily target the physics of an opponent's sensor or mathematics of their processing to reduce the visibility of the signal against the background, or the target's interpretation of the data stream.

Probably the simplest example of this style of attack is the use of an LPI spread spectrum radio waveform, designed specifically to appear like background noise or interference to any receiver which is not privy to the specific pseudo-random codes used to generate the spread spectrum waveform. An opponent's signals intercept receiver simply fails to see that a network transmission is in progress. A more sophisticated receiver may see that something is going on, but will not be capable of unravelling the encoding to extract the data link layer packets carrying the traffic.

Encryption of the data traffic, whereby the traffic is encoded in a manner resembling a stream of random symbols, represents another form of Passive Degradation attack. While the opponent can see that messages are being sent, the data inside those messages is opaque unless the opponent has access to the crypto keys and knowledge of the encryption algorithm being used.

A well designed networking system which employs both LPI transmission technology and robust, secure encryption, will present an opponent with two layers of Passive Degradation to overcome – finding and decoding the traffic in the ethers, and penetrating the encryption to see what the traffic actually is and what it contains.

The value of Passive Degradation is however greater than might be initially apparent. So far this discussion has focused on the information content being carried in the transmitted traffic. There is however other information available to an opponent which is 'implicit' in the transmission – that information is the physical location of the transmitter and the type of transmission equipment, both of which can be used to geolocate, identify and target the system or platform using the networking channel. If the opponent can determine that the signal is being produced by an LET capable JTIDS/ Link-16 terminal travelling at a specific speed and altitude, then the opponent may be able to identify the type of platform, its intent, and gain enough location information to effect a physical rather than electronic attack against the platform.

If the LPI waveform being used is clever enough, relative to an opponent's eavesdropping and geolocating capabilities, then this otherwise valuable 'implicit information' is denied wholly.

The growing popularity of 'covert' datalink technology, exemplified by the Intra-Flight Datalink Technology used in some stealth aircraft, shows that there is a good appreciation at least in US circles of the value of Passive Degradation in military environments.

In the context of cyberwar, where an attacker has penetrated into an opponent's network, the use of protocols, traffic types and messaging which are not easily differentiated from legitimate traffic constitutes a Passive Degradation attack, as the attacker is in a sense camouflaging against the background.

Active Degradation Attacks

Traditional EW (Electronic Warfare) falls into the category of active degradation attacks, where noiselike or otherwise disruptive jamming signals are transmitted at a victim receiver to degrade its sensitivity or otherwise impair the signal transmission.

The most basic forms of Active Degradation attacks involve radio frequency jamming (COMJAM) of the radio modulation being used i.e. the Physical Layer in the transmission system. This jamming may involve unsophisticated brute force attacks, in which a noise-like signal is simply used to bury the real signal so that is cannot be demodulated, or it may involve more sophisticated attacks, for instance using techniques devised to disrupt frequency hopping datalinks. The latter typically involves the use of a jamming technique which targets a specific weakness or vulnerability in the radio modulation being used, with the intent of increasing the Bit Error Rate (BER) of the transmission.

A more sophisticated form of Active Degradation attack (which if severe enough amounts to a 'soft kill' Denial Attack), may arise where an attacker is able to penetrate into an opponent's network and generate bogus message traffic targeted at a specific victim computer, or indeed a specific victim interface and port number (ie TCP/IP). The protocol software attempting to extract intended packets containing real traffic has to contend with other bogus packets, which albeit easy to find and discard, ie filter, consumes computational effort and thus time, and may even cause real packets to be dropped forcing retransmissions. As a result the useful bandwidth of the channel has been degraded, which is exactly the intent of any degradation attack.

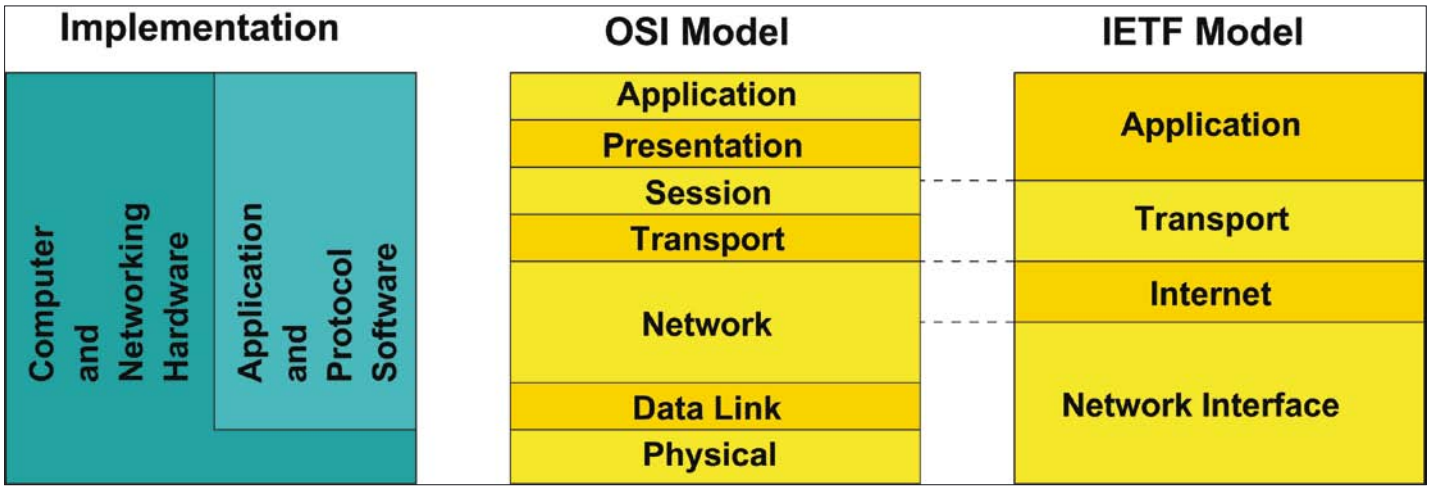


Figure 1 Functional models for networked systems.

Corruption Attacks

Corruption Attacks inherently involve some kind of deceptive or mimicking play by an attacker, intended to deceive the victim by making a target look to be something other than what it really is. If detection is inevitable, then confusing the enemy becomes a high priority.

A Corruption Attack is always targeted at the mechanism – be it machine or wetware – which provides for the recognition of a a signal or message.

There are a good number of jamming techniques in use which qualify as Corruption Attacks, and most involve the retransmission of a real signal with some time delay, or the creation of signals which are identical to the real item in type of modulation, packet structure, encryption technique etc, but contain bogus message payloads. A receiver or indeed even the protocol stack software cannot distinguish these from real traffic and is successfully deceived into demodulating or decoding/decapsulating the deceptive traffic.

Corruption Attacks are widely used as a supporting strategy in a compound attack, to enable for instance an Active Degradation or Denial Attack of some type to be carried out.

The whole domain of cyberwar hacking and 'identity theft' amounts to a range of Corruption Attack techniques, intended to deceive software and wetware so as to gain unauthorised access to an opponent's network or computer system. These are invariably compound attacks, as the Corruption Attack and resulting bogus identity of the attacker are tools employed to enable other mischief once the network's defences have been successfully penetrated. That mischief might be a Denial of Service attack, theft of data/information, or some form of Denial Through Subversion Attack. The precondition for all of these is penetration, and that can only be effected by a successful Corruption Attack, often at several levels of the victim system.

The US effort to introduce the capability to electronically penetrate opposing air defence networks to cause mayhem, using airborne platforms, is a good case study of a complete capability structured around the ability to perform repeatable Corruption Attacks against an opponent's radio frequency networks.

Denial Through Destruction Attacks

Smashing, crippling or bringing down an opponent's networked system is a denial through destruction attack, the aim of which is to temporarily or permanently remove that system from the battlespace. The term 'Denial of Service Attack' used in the cyberwar context is synonymous with a Denial Through Destruction Attack.

Denial through destruction attacks have become almost a subject of folklore in the cyberwar domain. Such attacks may be used independently, or may be used to support a more complex compound strategy.

Broadly we can divide Denial Through Destruction Attacks into the category of 'soft kill' and 'hard kill' attacks, the former where the system can eventually recover its full function, the latter where it is permanently damaged requiring repair, rebuilding or replacement.

If an attacker geolocates a network terminal and then puts a guided artillery round, smart bomb or missile into the site or platform carrying it, a classical 'hard kill' Denial Through Destruction Attack has been effected.

If an attacker geolocates a network terminal and uses an electromagnetic or microwave weapon against it, then a 'hard kill' or 'soft kill' attack will have occurred, the severity of the damage or downtime determining the latter.

If an attacker saturates a victim computer's network interface with a high volume flow of garbage traffic, preventing real traffic from being handled, or even crashing the victim system, then typically a 'soft kill' attack has been effected.

The common feature in all of these attacks, regardless of the means employed, is that the victim network or system has either been destroyed physically or electrically, or rendered inoperative by attacker induced software malfunction.

There have been a number of 'soft kill' attacks over the years reported against Internet Domain Name Server (DNS) hosts, which are the systems which translate Internet names (eg www.defence.gov.au) into specific IP addresses (e.g. 203.6.115.8). Regardless of the means used, a DNS server going down prevents computers from locating the addresses of any other machines, other than those recently accessed and locally cached in software buffers. Such attacks can temporarily cripple thousands of victim systems, by disabling a single point of failure system within the network. The form of a DNS server attack might be involve a deluge of bogus packets to deny useful bandwidth, but also penetration and corruption of the DNS database which holds the mappings between the DNS name entries and the addresses associated with each. The end result is much the same, in that all computers reliant on the DNS servers under attack are potentially crippled until the DNS service is restored.

Denial Through Subversion

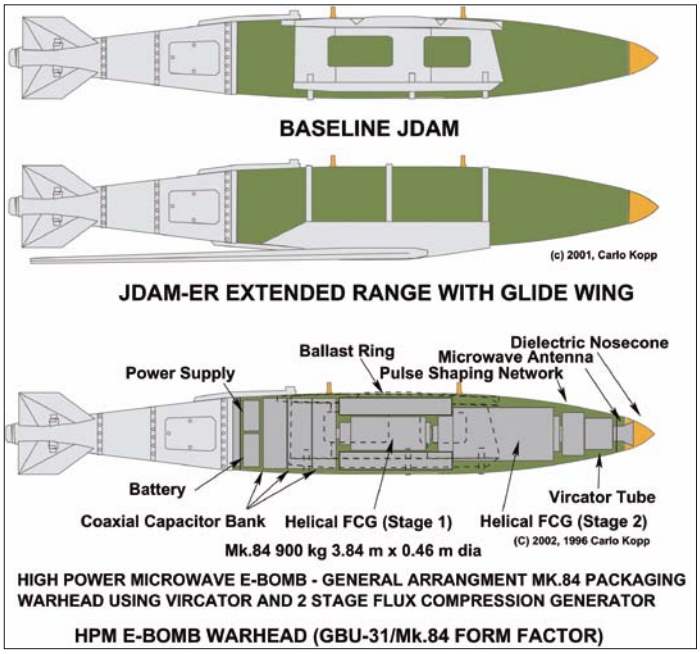
Subversion attacks, which involve implanting a self destructive instruction into a victim system, are common in biological systems and computer networks, and have become theme of almost 'urban myth' proportions in the popular, Hollywood and media cultural perceptions of Information Warfare. Alas, such attacks are not mythological, and continue to occur with considerable frequency in the cyberwar domain.

Subversion Attacks are usually employed in a compound strategy, whereby a Corruption Attack is used to penetrate defences and permit the Subversion Attack to take place.

An example might be an attacker who gains access via a radio frequency network, by using

High power jamming equipment suitable for the disruption or degradation of datalink channels used in military networks is now widely available in the open market. This Russian SPN-4 mobile jamming system is specifically built to disrupt microwave emitters such as airborne radars (Rosoboronexport).

EC-130H Compass Call communications jammer. The US Air Force claimed some years ago to have the capability to penetrate and internally disrupt the operation of opposing radio networks used in air defence systems. This is a classical compound strategy involving a Corruption Attack and a Denial through Subversion Attack.



The latest technology to emerge for Denial Through Destruction Attacks are microwave weapons, such as this High Power Microwave E-bomb, capable of electrically destroying a wide range of targets (Author).

the same equipment as the victim but with stolen authentication data and encryption keys, and who then proceeds to penetrate a key computer or group of computers on the network, and using stolen authentication for a highly privileged user, proceeds to bring the system down. The latter might simply be effected by commanding a shutdown, or more likely, by effecting deletion of key software applications, critical user data files, or even deletion of the operating system installation itself.

Virus, worm and trojan horse attacks, and the various forms of logic bomb, are classed into this category of attack. These are characteristically aimed at user desktop systems, large multiuser systems, web and file servers, and other host processing equipment or the software packages being run.

Less visible but potentially more damaging in military networks are Subversion Attacks aimed at network management systems used to configure large numbers of network terminals or routers from a single point. If an attacker can successfully penetrate into a management terminal or computer, the opportunity exists to reconfigure large numbers of network terminals or traffic routing devices in a manner which impairs traffic delivery, addressing or even operation. As a result the network loses the capacity to carry traffic, until each of these terminals or routers is reconfigured properly. The latter may require that a technician or network administrator physically access devices to reconfigure them from the local hardware interface, as network access may not be possible any more.

Assessing the Big Picture

The ubiquity of networks and associated computer systems across the civil and military infrastructure, and the increasing use of radio frequency networks such as JTIDS/MIDS, and in the future, JTRS, creates a myriad of opportunities for attackers. These range from 'classical' electronic warfare techniques applied against the data links employed, to a range of cyberwar techniques aimed at the networks and computers attached to them. A single chink in the digital armour may be enough for a smart opponent to produce a disproportionate effect, especially during combat operations. If a network used for air defence and cruise missile defence is brought down as an attack is being launched with aircraft and/or missiles, the battle is likely to be wholly lost in a matter of minutes.

Future warriors must come to grips with this reality – the vast power afforded by networked systems also creates an enormous, deep and pervasive single point of failure, the only comparable example elsewhere being the Navstar GPS system. A half century ago an operator needed to only grapple with jamming of radio frequency voice and teletype channels, and deceptive messaging and eavesdropping. As the Allied effort with Ultra/Engima demonstrated, even at that level of technology disproportionate effects could be produced. Modern digital networks offer vastly more potential for disproportionate effects to be produced.

Future warriors will need to be much smarter to survive in the complex digital jungle of a networked world.