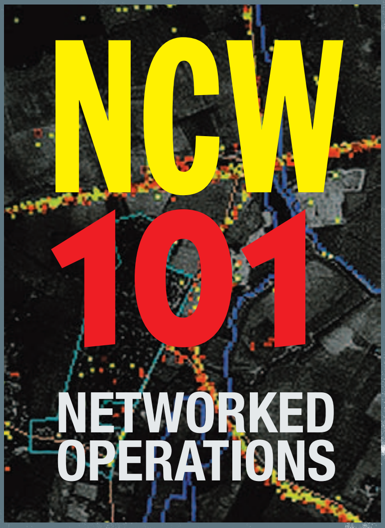


# Network Centric Warfare Fundamentals

Part 1

Dr Carlo Kopp

*“Network Centric Warfare (NCW) is now the defining paradigm in sharp end military operations and force structure development. NCW is by its nature complex, both in technological and operational terms, but there are few publications, textbooks, training courses or other media aimed at the uninitiated. The upper tier technical literature dealing with NCW topics is largely inaccessible, mainly because it assumes a high level of prerequisite knowledge in systems engineering, communications theory, network theory and operations modelling. Last year, the editorial team at DefenceToday asked the simple question: ‘how can this gap between operators and niche technical experts best be bridged?’ Our answer is ‘NCW101’, an ongoing series of tutorials that will explore NCW in plain language, and step-by-step lead readers to a better understanding of what networking is, how it works, what it can deliver, and what obstacles may arise. The author of this series has been integrating and designing computer networks, and hardware/software for such systems since 1985, and is an active researcher in wireless secure networking, and the theory underpinning NCW. DefenceToday is pleased to present this the first part of the NCW101 series.”*

*John Armstrong,*
*Managing Editor*

## Information and Why it Matters

Information is crucial to the functioning of all systems, biological or man-made, for the simple reason that information facilitates economy of effort. Knowing something usually provides opportunities to do it more efficiently or faster. Therefore, information has value attached to it; how much value depends largely on what that piece of information allows you to do.

In the pursuit of war, information has always been critical, and this was true of conflicts predating the Roman and Greek eras. Knowing or not knowing an opponent’s location, strength, capabilities, condition, reserves and intent has more than often been the decisive cause of victory or defeat. Many wars have started simply because of misperceptions of an opponent’s strength or weakness.

The advent of mechanised warfare during the 20th Century increased the importance of information. Large, fast moving formations on land, at sea and in the air deliver enormous firepower, with increasing precision using smart weapons. Knowing the strength and location of own forces and those of an opponent became vital to all types of military operations.

To find targets and kill them the mechanised military machine had to be fed with a stream of information. The capacity of mechanised forces to manoeuvre rapidly produced enormous pressures for timely information flow.

When defining ‘information’ the term is interpreted in different ways, and many NCW theorists have unique interpretations. At the most fundamental level of mathematical information theory, the measure of information is its unpredictability. If you know what a message contains beforehand, it has zero information content. If everything in the message is new, it has high information content. In a fundamental sense, how much information exists in any message depends on the prior knowledge of the observer.

To illustrate this, consider a situation where the observer is presented with a batch of reconnaissance photographs of a site of interest, each taken one day apart. Observing the first of these it has a high information content, absorbing the whole image and everything in it. If the image taken a day later is identical, it has no information content to an observer, other than the knowledge that no change has occurred. If the image includes a trench dug overnight, or enemy encampment, then the information content in the image lies in the changes observed, not the image itself.

A common mistake found in many discussions of information in warfighting is the idea that digital data is information. Digital data usually contains some information, but how much depends on the observer, and the content of the data. A mailbox full of identifiable ‘spam’ will have no information content to most observers as it is predictable rubbish.

This brings us to the issue of what kinds of information matter in military operations.

*Sensor operators onboard platforms used in the AWACS/AEW&C/ISR roles are the frontline troops in network centric operations: filtering, analysing and redirecting information when and where it is needed. (USAF)*

At the most basic level we are interested in the following:

1. The identity of entities in the battlespace: who or what are they; and are they friendly, neutral or hostile? This is because the consequences of mistaken identity in war are always dire, and well documented historically.
2. The location, direction of movement and speed of entities in the battlespace: are they approaching or retreating, where are they going, and how fast is this happening? Without knowing this information it is difficult, if not impossible, to pursue or avoid an engagement, depending on your intent.
3. The condition or intent of entities in the battlespace: are they armed and ready for a fight, are they aiming to engage, are they aiming to escape an engagement?
4. Command directives and instructions: issued from superiors, or being issued to subordinates. The faster moving and larger formations become in combat, the more critical it becomes to achieve coordination and synchronisation.

Most common discussions of information in warfighting divide it into Intelligence, Surveillance and Reconnaissance data, command and control data, and logistical and support data. These are valid divisions in terms of the source or use of the information contained, but all ultimately fall into the four categories above.

In an ideal world we have ‘perfect information’: we know everything that needs to be known about a game in progress; indeed this is a common assumption made by mathematicians working with game theory. Reality is inherently messy, and this is reflected in the popular notion of ‘fog of war’, which encapsulates the blindness experienced by a commander who is constrained by uncertainty and a lack of valid, current information. Making decisions in a fast moving and complex battlespace, without a clear picture of the situation, differs little from trying to navigate shoals in a fog, or fly an instrument approach visually.

Confronted with a lack of valid information, a commander has three options. If he is a risk taker, he can opt to roll the dice, forge ahead and more than often lose the engagement and possibly his command. If the commander is prudent, he will move slowly and cautiously, and cover every move with strong reserves. If the commander is weak, he is apt to collapse into paralysis and do nothing. Military history is replete with case studies of all three behaviours.

Modern Western military thinking emphasises the idea of ‘information superiority’ whereby a commander is always provided with a decisive advantage in the amount of information he has available over his opponent. The opening hours of the Desert Storm campaign in 1992 present the most stark case study – with the Coalition forces annihilating Saddam’s air defences, the latter literally stabbing blinding into the dark. The enormous assymetric advantage held by the Coalition in information gathering assets has much to do with this now classical military debacle.

Having ‘information superiority’ is not a panacea in war. Knowing something but being powerless to deal with it due to a shortage of combat assets, or inappropriate combat assets, literally throws away any advantage having that information might offer. Networking is itself only a mechanism to accelerate the distribution of gathered and processed information; it cannot gather and process information as one might be led to believe by some NCW proponents. In practical terms, networking is not a substitute for information gathering and processing assets, and it is definitely not a substitute for real combat assets. What networking is, when combined with information gathering and processing assets, is a means of enhancing an existing combat capability.

One misguided view, which has been strongly asserted in the public debate on NCW in Commonwealth nations but not the United States, is that the addition of networking justifies large reductions in combat asset capabilities and numbers. This is simply nonsense. To defeat an opponent a force must have superiority in information, in addition to superiority in combat assets. While smaller and weaker players may often win individual engagements due to subterfuge and cunning, their opponents usually learn quickly and the advantage is not sustained.

Time is a critical factor in combat. Battles, indeed wars, are most often won by commanders who are able to concentrate and apply more firepower faster than their opponents. The old saying about winning by being ‘first-est with the most-est’ is fundamentally true - and in many respects the idea underpinning all modern manoeuvre warfare technique.

In practice, time is an issue both for the distribution of information in combat and the movement of firepower. Where there is enough firepower to achieve an advantage in concentration of fire, a shortage of timely information can impose a decisive limit on combat effect. However, an abundance or over-abundance of timely information is useless without timely application of firepower - assuming the firepower exists and can be applied.

What networking provides is a high-speed digital wireless pipe to rapidly move information between assets or systems gathering it, and commanders and combat assets who are to use it. For it to be useful, information needs to be gathered and processed quickly enough, and combat assets replenished or moved quickly enough.

The reason information and the timeliness of that information are so critically linked is because the modern battlespace is a rapidly changing environment. To have an accurate picture of a rapidly changing situation, snapshots need to be taken quickly enough to capture every change. In fact, the mathematical basis for this is Nyquist’s sampling theorem, which dictates taking snapshots at at least twice the fastest rate of change in the picture observed. Otherwise, a change may occur between snapshots and inevitably be missed, and the observer is blind to it having occurred at all.

Much of the drive to mechanisation in modern war is about moving around fast enough to defeat an opponent’s information gathering and processing apparatus; and should this fail, fast enough to stay ahead of the opponent’s countering deployment of forces. The idea implicit in networking combat forces is thus to move information around fast enough to defeat a fast moving opponent’s attempts to circumvent information gathering and processing efforts.

NCW articles today often talk about the ‘sensor-to-shooter interval’ or ‘shortening the kill chain’. This is technical jargon, which encapsulates the idea of minimising the time between the detection of a target and its engagement in combat. It presupposes that information gathering assets are able to detect the target, and that combat assets are able to kill it.

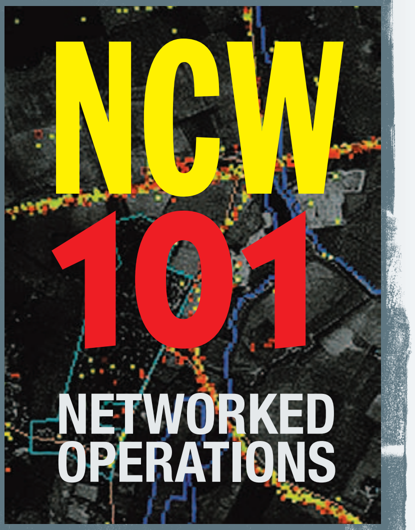
A key issue in contemporary networking development efforts is achieving higher speeds in wireless digital radio links used for networking. This is a direct byproduct of the need for timeliness. Over the last decade we have seen the advent of digitised sensors for Intelligence, Surveillance and Reconnaissance applications. Modern synthetic aperture high resolution mapping radars, and daylight or thermal imaging cameras, can now produce Megabytes of raw imagery data per second with ease. Most of the wireless digital radio links used today are products of 1970s technology, designed to carry small tightly formatted text messages - concentrated information packages containing carefully filtered information that can be directly used for engagements or targeting. Such links are simply inadequate when confronted with Megabyte sized lumps of raw digital data, such as reconnaissance images. Pumping imagery files of this size through low speed digital links can take minutes or tens of minutes to perform, time which is not available in a fast moving battlespace. As a result, there is much pressure today to deploy new link technologies such as JTRS (Joint Tactical Radio System) to replace legacy systems like JTIDS (Joint Tactical Information Distribution System)/Link-16.

Achieving very short sensor-to-shooter intervals is thus not a simple proposition. First, adequate combat assets must be available to provide a persistent presence in the area of interest. Second, adequate Intelligence, Surveillance and Reconnaissance assets must be available to provide coincident persistence in the area of interest. Third, sufficiently fast digital connections must be available to connect the ‘sensors’ to the ‘shooters’ and their command system.

In essence, the three pillars of any viable - rather than dysfunctional - system for Network Centric Warfare / Networked Enabled Operations are persistent firepower, persistent ISR and true networking of these assets. Cripple any of these three pillars by under-investment and the system will fail.

# NCW 101

## NETWORKED OPERATIONS



### INTELLIGENCE SURVEILLANCE RECONNAISSANCE

In building up a force structure suitable for NCW (or NEO), or indeed adapting an existing force structure, the starting point in investment must be assets for gathering information. Until these are deployed and matured in service, no amount of networking investment will matter.

In the broadest of terms information gathering assets (ISR) can be divided into three tiers, separated by the useful footprint of the asset.

At the upper tier are systems that can surveil large footprints in high detail, typically mapping geographical extents of tens to hundreds of miles. Such systems can cover a large fraction of a theatre of operations.

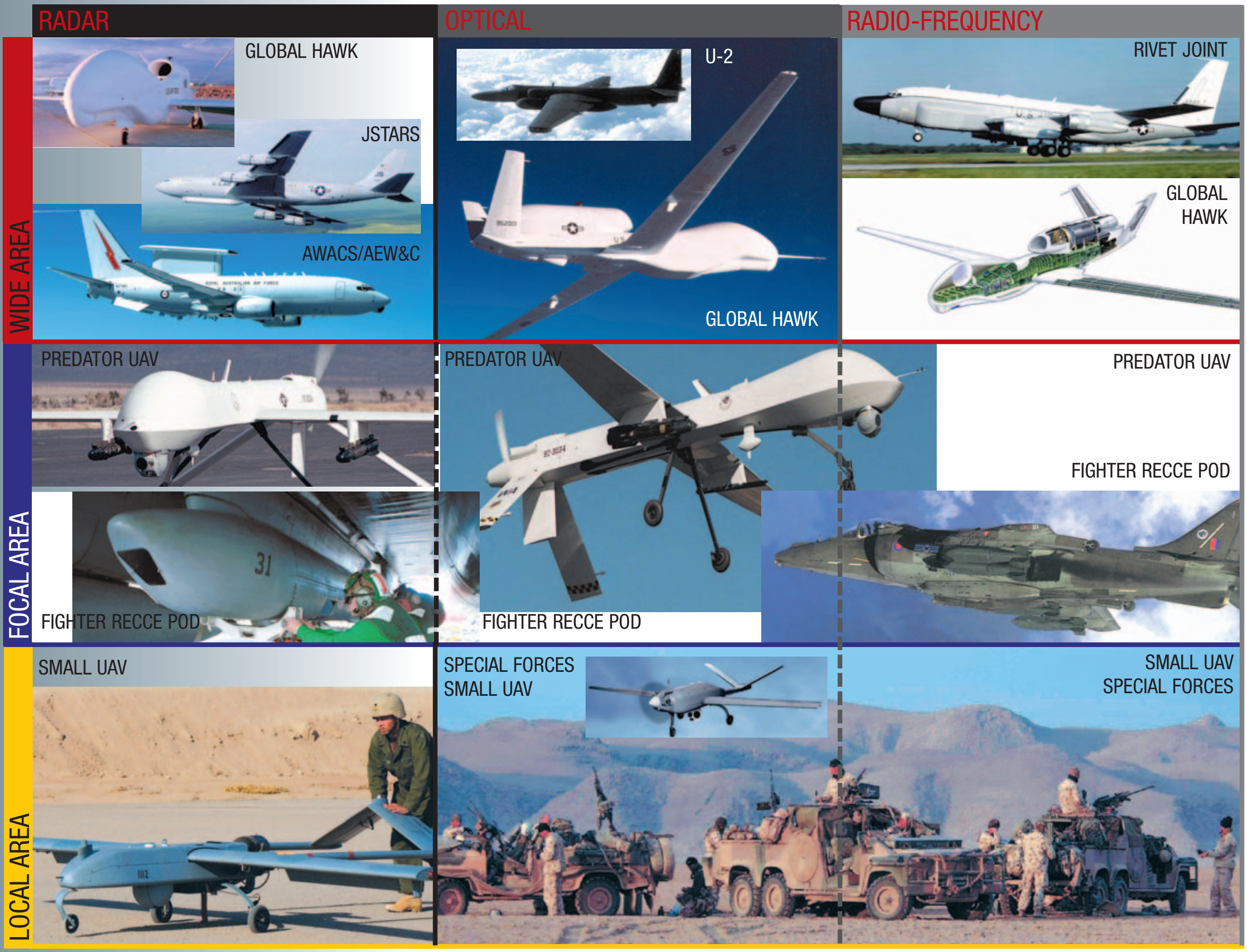
Examples include Airborne Early Warning & Control (AEW&C) aircraft such as the RAAF's new 'Wedgetail' fleet or E-3 AWACS and Over-the-Horizon radars such as JORN (Jindalee Operational Radar Network). These provide air surveillance and some surface surveillance. GMTI (Ground Moving Target Indicator) radar-equipped aircraft such as the E-8 JSTARS or E-10 MC2A, provide long range surveillance of moving ground vehicles or maritime targets. Passive surveillance systems such as the RC-135V/W Rivet Joint, which can detect and analyse radar and radio transmissions, plus high altitude manned and unmanned aircraft such as the U-2 and RQ-4 Global Hawk, or satellites, that can carry diverse sensor packages are assets that are expensive to acquire and operate, but nevertheless provide enormous capability.

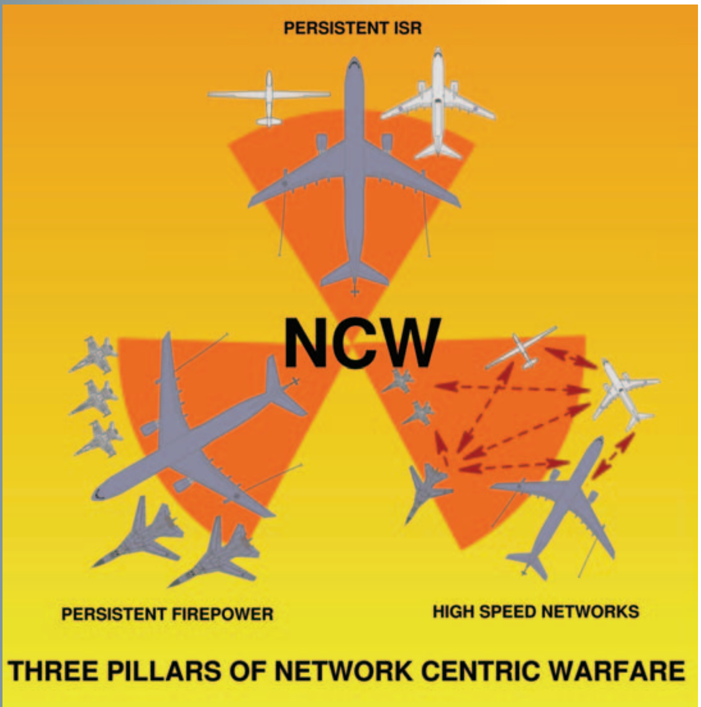
Lower tier assets include systems to surveil focal areas in high detail, typically mapping footprints of miles or less. While more affordable per unit than the larger systems, the smaller footprint requires unaffordable numbers of such systems to achieve strategic effect. In practice, they are used to supplement upper tier systems. Examples are mid-range UAVs such as the RQ-1 'Predator' series, and any of a wide range of sensor pods fitted to fighter aircraft, and in some instances helicopters.

More recently a defacto third tier of systems has emerged, intended to provide coverage of very small footprints. These are typically sensor packages carried by small or man-portable UAVs, and sometimes light or general aviation aircraft or helicopters.

Sensor technologies can be broadly divided into three categories: radar, optical and passive radio-frequency.

Radar sensors are active devices, transmitting usually in the microwave frequency bands, which analyse energy back-scattered from terrain or targets to produce raw imagery or tracking data. A wide range of radar categories can be used for collecting information. Pulse Doppler and Air Moving Target Indicator radars are used to detect and track aircraft, ballistic and cruise missiles or helicopters. GMTI radars can detect and identify moving vehicles plus rotating antennas on stationary radar systems. Maritime Moving Target Indicator radars can detect and track shipping, while Inverse Synthetic Aperture radars can image the shape of vessel. Synthetic Aperture Radars can produce ground maps with resolutions down to inches, and Interferometric Synthetic Aperture Radars can do so and also measure terrain elevation, producing three dimensional ground maps. In addition, some specialised radars can





*Networked operations transcend traditional maritime, land and air operations enabling focused operations by separate but coordinated combat elements.*

*Multi-function sensors and coordinated information communicated to command centres are essential to effective ISR leading to decision-making and the application of military power. (Boeing)*

penetrate soil to shallow depths, to find structures, and others can penetrate foliage to detect hidden targets.

Radar has the tremendous advantage of being mostly capable of penetrating any weather including cloud, rain, fog or dust storms, day or night. During the invasion of Iraq, Saddam's forces attempted to move under the cover of a large dust storm, which hid them from optical sensors, but not the APY-3 radar on the JSTARS (Joint Surveillance  and Target Attack Radar System), resulting in massive casualties.

In the second category are electro-optical systems, passive devices that use reflected sunlight in the visible colour bands or thermal emissions in the infrared bands to image areas of interest. Such systems are mostly motion-stabilised telescopes, with the human eye replaced by an imaging chip. In fact some daylight reconnaissance systems use the very same chips used in high quality high definition TV broadcast cameras. Optical systems are usually divided by viewing angle achievable, the resolution of the image possible, and the visible or infrared colour bands they can record.

Two unique categories of electro-optical imager are infrared line-scanners, which image a swath of terrain beneath the aircraft or UAV carrying them, and hyperspectral imagers. The latter are capable of imaging terrain in hundreds of discrete visible or infrared colours, permitting very precise identification of targets. One US general was quoted commenting on how he could use a hyperspectral imager to pick a specific car painted with a specific factory paint from a complex image.

Optical sensors have enormous advantages in terms of identifying targets and capturing fine detail. Their principal limitation is an inability to penetrate cloud, fog, dust, haze and foliage, affording opponents opportunities to hide.

The third category of sensors are passive radio frequency receivers designed to detect and often 'geolocate' hostile radio and radar transmissions. Such receivers often have complex processing systems attached to analyse and identify the source of a transmission, permitting not only precise identification but also eavesdropping of radio and cellphone traffic. Over the last decade we have also seen increased numbers of systems capable of precisely measuring the location of a radar or radio emitter, exploiting interferometric antenna techniques and motion of the carrying aircraft.

As is the case with radar, electronic surveillance receivers can penetrate weather with ease, providing day/night all weather coverage. Their limitation is that they rely on an opponent actively transmitting a signal, which can be detected. A disciplined opponent or one who avoids transmissions altogether can frustrate such systems.

The big change seen over the past decade in sensors used to gather information is 'digitisation', or the provision of digital interfaces. This permits imagery or track data to be provided by the sensor directly in digital formats suitable for processing by computer or transmission over a digital network.

Until the 1990s, surveillance sensors typically provided output as blips on a screen to be interpreted by a human operator, while reconnaissance cameras and Synthetic Aperture Radars provided output on wet photographic film. The latter had to be flown to a processing lab, developed, printed to paper, and then couriered to the intended recipient, taking hours if not days to perform. Digitisation of such sensors has compressed timelines between gathering the image and presenting it to a user typically more than one hundredfold.

The issue of processing raw data gathered by sensors into a format suitable for use is central to the impact of 'digitisation'. For any image or situational picture produced by a sensor to be useful, it has to be presented in a viable format. This typically means attaching timestamps to identify when the picture was taken, and geographical coordinates to locate the target. Frequently, complex processing must be performed to permit easier detection and interpretation by human users.

Historically, photo-interpreters divined information from raw imagery collected by sensors. This skills set remains in high demand because while digital processing can make the task faster and easier the human mind is still required to make sense of what is in the picture. Human cognitive skills remain the most difficult to replicate in a computer, a situation that may persist for decades.

Automatic target recognition techniques are now maturing, after decades of less than entirely fruitful research. These systems typically involve the use of software, and sometimes specialised hardware, to identify characteristic shape features in an image, and thus sort targets from background clutter. Unfortunately, high 'false alarm rate' problems can arise, where the software may confuse a real target with something which exhibits similar shape features. The author recalls one millimetric radar based automatic recognition system he trialled, which consistently labelled cars as tanks, as both vehicles had a stepped shape profile. This is why humans will remain in the loop for some time yet, as human cognitive skills are vital to validating information - sorting false alarms from real targets. Current automated processing does a tremendous job of rapidly identifying large numbers of possible targets, but seldom provides the high level of integrity required to make a life-or-death decision.

The issue of integrity of information is thus critical, and one frequently glossed over or ignored by ardent NCW evangelists. Absolute certainty about the correctness of any piece of information used in combat is always difficult to achieve, especially when opponents make it difficult by concealment, decoys, camouflage and other forms of deception.

Usually, the best way to defeat deception is to use as many sources of raw data as possible, and compare these to identify consistencies and inconsistencies, to sort fact from non-fact. Again, humans are usually very good at doing this, as they can use experience and commonsense (technical context) to divine the truth. Only then is the output from sensors something that amounts to usable information.

The downside of human processing is its low speed, especially a problem when a vast number of possible targets need to be identified properly. Under pressure or fatigued, humans are also prone to make mistakes, even to the extent of punching keys out of order. As a result, the path from raw data to validated information is full of potential sources of errors, machine or man made.

Some of the most vociferous NCW evangelists have argued that systems should aim to minimise human intervention, assuming implicitly that humans are more error prone than machines. The latter is only true for highly repetitive and often simple operations; once the problem to be solved is cognitive, the tables are often turned.

Until we have artificial intelligence algorithms that can compete with human cognitive skills, much of the wish list of the ‘machine warrior’ advocates will remain ‘pie in the sky’ fantasy. As a result, the ‘information’ derived from highly automated sensor processing may often be suspect, and thus unusable without a high risk of killing something unintended.

Five decades ago advocates of artificial intelligence imagined that human cognitive skills could be replicated in the then coming decade, something that has not yet occurred. Such predictions have been repeated ever since, most often by individuals not performing artificial intelligence research! Until we see a breakthrough in fundamental artificial intelligence theory, which permits human-like cognitive skills in machine intelligences, we will not see the fully machine based network materialise as a viable system.

Computer scientists have used the slogan ‘garbage in, garbage out’ for decades to describe the capacity  of digital systems to replicate, process or transmit invalid data.

This is important in a networked system since it reflects the reality that erroneous data fed into the network can be propagated to large numbers of users in minutes or seconds, and thus compromise the integrity of the picture formed in the minds of these users. Whether the erroneous data is the result of hostile deception, or limitations in humans/sensors/processing, is immaterial.

NCW evangelists often assert that networking permits users, or automated systems, to rapidly amass data from various sources to facilitate elimination of errors or false targets. This is only true if the data or information so amassed is validated and known to be true. If errors exist in information or data sources used to validate new data of unknown validity, the effect can be to produce and further propagate additional errors. Consider a situation where a specific type of radar data processor, used in several different radars on different platforms, has a bug in a target identification algorithm. An operator may assume that having multiple tracks from multiple systems all saying the same thing makes it true.

The reality is that replicating the same mistake many times over does not make it into the truth, despite Third Reich Propaganda Minister Goebbels’ famous saying of 50 years ago.

Part 2 next issue ..
Data Links and Networks

NCW 101 NETWORKED OPERATIONS