NCW: THE DOUBLE-EDGED SWORD

SANJAY PODUVAL

> *What we are seeing, in moving from the Industrial Age to the Information Age, is what amounts to a new theory of war: power comes from a different place, it is used in different ways, it achieves different effects than it did before. During the Industrial Age, power came from mass. Now power tends to come from information, access, and speed. We have come to call that new theory of war network-centric warfare. It is not only about networks, but also about how wars are fought—how power is developed.*
>
> — Arthur K. Cebrowski

> *The conflicts of the 20th century are being replaced by hybrid wars and asymmetric contests in which there is no clear-cut distinction between soldiers and civilians and between organised violence, terror, crime and war.*
>
> — Alan Dupont

Warfare today is more complex than ever before. There is a blurring between peace and conflict, caused by the revolution in information technology. The revolution has enabled high speed dissemination of information over wide geographical areas almost simultaneously through dedicated networks. This was clearly seen in the conflicts in Kosovo and the Gulf, 2003, when the world woke up to the reality of Network-Centric Warfare (NCW) and the

* Wing Commander **Sanjay Poduval** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

multiplicative effects of information superiority that it provided. NCW, in some measure, has reduced the tyranny of distances, speeded up operations and has the potential to provide a seamless picture across the battlespace. However, this is by no means a silver bullet. It does have a flip side which was clearly brought out by the well coordinated 9/11 attack on the World Trade Centre. NCW has not truly met its match in the conventional sense; it is clearly dominated by the United States. This has led to wars of the present being more covert, with the adversaries leveraging the strengths of Information Technology (IT) against the proponents. As a result, most states today are perpetually at war; a war of a different nature, not against tangible elements but against bits and bytes. This information war is split between the offensive and the defensive. The advantage more often than not lies with the attacker who can choose the time and place of the attack. The blurring of offence and defence reflects another feature of the dual nature of NCW; it tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal. This makes it difficult, if not impossible, for a government to assign responsibility to any single agency—e.g., military, police, or intelligence—to be in charge of responding. The wars over the net or netwars refer to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organisation and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an 'inter-netted' manner, without a precise central command. Thus, information age netwar differs from the traditional modes of conflict and crime in which the protagonists prefer formal, stand-alone, hierarchical organisations, doctrines, and strategies.[1] Conflicts of the present century are being replaced by hybrid wars and asymmetric conflicts in which there is no clear-cut distinction between soldiers and civilians and between organised

[1] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND, 2001).

violence, terror, crime and war. In view of the above, the aim of this paper is to discuss the merits and demerits of NCW.

THE DUAL NATURE

In the military in the past 20 years, many astounding technological advancements in radars, directed energy, communication, space exploitation, miniaturisation, data processing, etc have taken place, which have not only influenced every aspect of our lives but have also altered the means of waging wars. Warfare can now be more efficient and effective. The integration of all these factors has essentially led to Network-Centric Warfare (NCW). Networking is a mechanism which improves operational tempo by accelerating the Observation-Orientation phases of Boyd's Observation-Orientation-Decision-Action (OODA) loop. The audacious second attempt on April 7, 2003, to decapitate the Iraqi leadership amply demonstrates this. The strike was especially noteworthy for the way it saw information on the whereabouts of the Iraqi dictator, which emerged at very short notice, transmitted rapidly to Allied air planners and then to the B-1B bomber aircraft. It took just 12 minutes for the crew to disengage from a previously assigned task and release their weapons on the new target.[2] The Iraqi leadership, however, escaped the attack, which implies that they too got wind of the impending attack equally fast.

The increasing dependence of societies and military forces on advanced information networks creates new vulnerabilities through means such as computer network attacks and directed energy weapons. The inherent implication here is that the universal nature of networked systems is in itself one of the key vulnerabilities. Provision of digital wireless connectivity between combat platforms is a major technical challenge which cannot be understated. While civilian networking of computers can largely rely on cabled links, be they copper or optical fibres, with wireless connectivity as an adjunct, in a military environment centred on moving platforms and field deployed bases, wireless connectivity is the central means of carrying

[2] "What Went Right?," *Jane's Defence Weekly*, April 30, 2003, http://www.oft.osd.mil/library/library_files/article_63_Jane.doc.

information and the area most vulnerable to interference.

Therefore, it is not surprising that anti-establishment forces, weaker forces and non-state actors have taken to the digital revolution with alarming alacrity. The low cost of entry (for example, a laptop connected to the Internet) and the ability to operate anonymously are factors responsible for asymmetrical operations from potential adversaries. A communication channel that broadcasts relevant and authentic data can also transmit irrelevant and false data. Network-centric deception supports any operation which has objectives that are a function of communication networks, irrespective of whether these are adversarial or friendly. In other words, if an adversary relies on communication networks to obtain, process, and analyse the Common Operational Picture (COP), the same can also be skewed or altered.

The fact that military networks and civilian networks are intertwined provides another set of vulnerabilities which must be addressed.

The fact that military networks and civilian networks are intertwined provides another set of vulnerabilities which must be addressed, for example, during Operation Iraqi Freedom, US and Coalition forces reportedly did not execute any computer network attacks against Iraqi systems, even though comprehensive Information Operations (IO) plans were prepared in advance. It is widely speculated that the IO plans against the Iraqi financial services were rejected because Iraq's banking network is connected to the financial communications network also located in Europe. Consequently, according to Pentagon sources, an information operations attack directed at Iraq might also have brought down banks and ATM machines located in parts of Europe.[3] This vulnerability has tremendous ramifications for the mischievous intents of anyone who wishes to take advantage of the situation.

The present information revolution is posing new security problems that could prove more severe for open societies than for closed ones. As we

[3] Charles Smith, "US Information Warriors Wrestle with New Weapons," NewsMax.com, March 13, 2003, http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml .

become economically stronger, our dependence on other countries and on connectivity and computation would only increase and we could become more vulnerable to information warfare. Integration in the world economy, with its criss-crossing networks, enlarges the risk. The prospect of a disruption of the national economy due to attacks on the domestic information infrastructure could tilt the ambivalence of a nation in a distinctly negative direction, thus, emboldening a militarily inferior enemy.

As we become economically stronger, our dependence on other countries and on connectivity and computation would only increase and we could become more vulnerable to information warfare.

Greater dependence on information technology in military systems could imply greater susceptibility to information warfare during operations. The Revolution in Military Affairs (RMA) places a bull's eye on the Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) that is critical to it. In the extreme, the ability to project power and to strike at will, would be undermined if an otherwise weaker enemy interfered with the links that network forces, fuse sensor data, and permit joint warfare. Even if the military establishment secures its own dedicated links and nodes, effective information warfare attacks on public telecommunications network, on which nearly all routine military traffic flows, could create havoc in a crisis and cripple a campaign.

THE PROS: THE 'RIGHT' EDGE OF THE SWORD

Operation Enduring Freedom (2001–02)

The network-centric capabilities of the US Central Command (US CENTCOM) elements during the conduct of Operation Enduring Freedom in Afghanistan proved vital in the battle against the Taliban and Al Qaeda forces. The operations were conducted in the mountainous, landlocked country which presented an extremely challenging environment. The long sought goal of networking weapons and sensor platforms came to fruition in the austere environment where both the needs and the advantages of NCW were readily apparent.

The Special Operations Forces (SOF) on the ground were networked with aircraft capable of delivering Precision Guided Munitions (PGMs). This combination proved extremely effective. However, networking the sensors and the shooters in real-time was only part of the requirement. Taliban and Al Qaeda targets during Operation Enduring Freedom were often fleeting, and weapons platforms had to be updated very quickly while in the air. The B-2 bombers (flying from bases in Missouri), and B-1 bombers (flying from other bases far from the theatre of operations), required the capability to change mission tasking en route to the target areas in Afghanistan. Carrier-based aircraft needed a similar capability to deal with the dynamic nature of their targets. Unmanned Aerial Vehicles (UAVs) were successfully used for this purpose to a greater degree than ever before. The ability to pass information gathered by Predator and Global Hawk UAVs to ground commanders in Afghanistan enabled near-real-time battlefield situational awareness. Satellite communications and related technologies enabled this networking capability to a degree not previously achievable.

Operation Iraqi Freedom (2003)

The impressive network-centric capabilities of US forces were clearly evident during the conduct of Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF). Many significant improvements in these capabilities were apparent by the time OIF began in March 2003. Network-centric capabilities provided, without question, a major contribution to the decisive victory of Coalition forces in Iraq.

Network-centric capabilities evident in US forces during OIF included not only technology and systems that enabled effective conduct of Network-Centric Operations (NCO), but innovative new concepts for the employment of technology and an enhanced understanding of the human side of the NCW equation as well—highly trained, motivated soldiers, sailors, airmen, and marines fighting as part of an integrated, networked joint force. Most of the groundwork for the information network and other network-centric capabilities that empowered the forces during OIF was actually completed during OEF. Technology enabled the rapid sharing of information at all levels with a capability to move intelligence rapidly from the sensor to either the decision-maker or directly to the shooter. The communications, C2, and ISR systems were hooked up to, and interoperable with, the Global Information Grid (GIG), and were adaptable to circumstances on the battlefield.[4]

Modern technology and new operational concepts enable networked units and individual platforms to operate together in ways not possible just a few years ago.

Therefore, as is evident, modern technology and new operational concepts enable networked units and individual platforms to operate together in ways not possible just a few years ago. NCW is characterised by the ability of geographically dispersed forces to attain a high level of shared battlespace awareness that is exploited to achieve strategic, operational, and tactical objectives in accordance with the aim. This linking of people, platforms, weapons, sensors, and decision-aids into a single network creates a whole that is clearly greater than the sum of its parts. The results are networked forces that operate with increased speed and synchronisation and are capable of achieving massed effects, in many situations, without the physical massing of forces required in the past. This increased speed and synchronisation directly impacts operations across the battlespace, from support areas through combat zones. NCW enhances the ability of a force to combine into a seamless, joint, coalition war-fighting force. As information moves down to the lower echelons, so does decision-making. Thus, smaller joint force packages can possess more flexibility and agility and are able to wield greater combat power than before. NCW generates new and extraordinary levels of operational effectiveness. It enables and

[4] "The Implementation of Network-Centric Warfare," http://www.au.af.mil/au/awc/awcgate/transformation/oft_implementation_ncw.pdf

leverages new military capabilities while allowing the use of traditional capabilities with more speed and precision.

CONS: THE OTHER EDGE

After the 34-day War with Israel in 2006, Hezbollah was described by some Israeli officials as a well-equipped, networked force still capable of commanding its combat units after weeks of high-intensity fighting. Hezbollah's units were supported by a well-fortified terrestrial communications network supplemented by satellite telephone and broadcast services which included the Al-Manar television network. Hezbollah units also reportedly had the capability to attempt eavesdropping on Israeli cellular networks.[5] Hezbollah guerrillas were able to hack into Israeli radio communications during the conflict, an intelligence breakthrough that helped them thwart Israeli tank assaults. This gave the guerrillas a picture of Israeli movements, casualty reports and supply routes. It also allowed Hezbollah anti-tank units to effectively target advancing Israeli amour.[6] The same networks which were providing information advantage to the Israelis, aided their adversaries.

Hamas was also reportedly inspired by the way Hezbollah fought against Israel in Lebanon. The organisation is continuing to receive increasing support from Hezbollah in the form of weapons, funding, and training. Hezbollah is also reportedly sharing with Hamas operatives many of the lessons they learned from the recent military engagement with Israel.[7] Cells of people that are under central direction, allow the organisation to be highly flexible, elusive and adaptable.

Al Qaeda too is evolving and coming to terms with the newer commercially available communication systems. Their dispersed cells may become more coordinated and self-organising, with increased situational awareness, and the possible future capability of conducting their own network operations in

[5] Barbara Opall-Rome, "Combating the Hezbollah Network," *Defense News*, October 9, 2006, p. 6.

[6] Noah Shachtman, "Hez Hacked Israeli Radios", http://www.noahshachtman.com/archives/002785.html

[7] Alon Ben-David, "Hamas Boosts its Weapons Stocks," *Jane's Defence Weekly*, October 25,2006.

ways similar to the network operations of current military units.[8] Al Qaeda is transforming itself into a virtual organisation, while creating new links to local franchisees. It is these new local groups that are now carrying out terrorist attacks, rather than Al Qaeda itself, and these smaller, local groups are more difficult for the military to anticipate, locate, and engage.[9]

Cyber terrorism is the biggest threat that India is likely to face because the network infrastructure of the country is vulnerable and may be attacked any time.

Another serious concern comprises the reports which state that Pakistani cyber criminals deface nearly 40-50 Indian websites every day. Nasscom surveys have pointed out that information security threats have created an unprecedented demand for qualified and experienced information security professionals but India is yet to comprehend this crucial issue.[10] Studies suggest that the slipshod attitudes of both the corporate sector and the government regarding cyber security impede any positive approach. Cyber terrorism is the biggest threat that India is likely to face because the network infrastructure of the country is vulnerable and may be attacked any time.[11] Asymmetric warfare, Counter-Insurgency (CI) or Counter-Terrorism (CT) operations, rather than conventional warfare, is the order of the day across the globe. An adversary will seek to wage asymmetric war and cripple the economic and energy infrastructure rather than engage military targets. Alternately, the adversary will launch cyber attacks to cripple the banking, railway or power grid systems. Today, the terrorist threat is real. Each terrorist network is part of a complex network of autonomous terrorist groups, thus, forming an international terrorist Internet. In India, there exists

[8] David Compert, "Battle-Wise: Gaining Advantage in Networked Warfare", Center for Technology and National Security Policy, National Defense University, January 2005, p. 15.

[9] "Business Lessons from Terrorists", World Economic Forum, January 21-25, 2004, [http://members.weforum.org/pdf/Session_Summaries2004/084e.pdf

[10] Amit Sinha, "Pakistani Hacking Onslaughts Makes India a Hapless Prey", http://www.littleabout.com/news/45008,pakistani-hacking-onslaught-india-hapless-prey.html

[11] "Cyber Terrorism Next Big Threat to India: Cyber Security Whizkid", http://www.thaindian.com/newsportal/sci-tech/cyber-terrorism-next-big-threat-to-india-cyber-security-whizkid-with-images_100279193.html, November 24, 2009

a nexus of terrorist and insurgent organisations which operate in Jammu and Kashmir, the northeast and the hinterland areas of Madhya Pradesh, Bihar, Andhra Pradesh, Chhattisgarh and Jharkhand which make extensive use of the Internet. These organisations have cyber savvy terrorists who use the worldwide web, e-mail and electronic bulletin boards and are involved in hacking of sensitive national websites.[12]

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 modern day 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. Therefore, the anti-establishment forces, weaker forces or the non-state actors have taken to digitisation with alarming speed. The ease of entry is a major factor responsible for asymmetrical operations from potential adversaries.

Another example of the double-edged nature of NCW is the use of the Global Positioning System (GPS) which is considered to be the enabler of NCW. The use of GPS guided munitions provided an asymmetric advantage to the Allied forces. They were able to precisely hit most of their targets at all times in all kinds of weather. Most of the expensive, cruise-type missiles in the US inventory such as the Tomahawk Conventional Air-Launched Cruise Missile (CALCM) and some land-attack versions of the Harpoon missile employ GPS for navigation purposes. The problem is that of GPS exploitation. Even during the Gulf War, it was reported that the Iraqis used commercial GPS equipment to assist in calibrating Scud launch sites. The real problem will come about when countries start dusting off their 50s and 60s technology cruise missiles and retrofit them with commercial GPS autopilots. Most of these weapons used combinations of inertial autopilot,

[12] Ibid.

radio command link and anti-ship radar homing guidance to attack either shipping or area land targets. In the latter instance, they were never taken seriously due their poor accuracy. However with GPS accuracies, they become very effective standoff weapons, a problem which could be extrapolated into the Indian context once the Indian Regional Navigation Satellite System (IRNSS) becomes operational. The September 11, 2001 terrorist attack on the US took a new turn on the destructive usage of GPS. Reports say that the US Federal Bureau of Investigation (FBI) is suspecting terrorists' use of GPS as their lethal weapon to precisely locate the ill-fated sites.[13] It is suspected that at least three of the 19 terrorists could have purchased a GPS device that year.[14]

The 9/11 planners and hijackers exploited the Internet to achieve their goals. Senior Al Qaeda coordinators involved in the suicide hijacking plot, such as notorious Al Qaeda training camp manager, Abu Zubaydah, exchanged thousands of encrypted messages, posting their operational plans on a password protected section of a website.[15] The extensive use of the Internet by the 9/11 hijackers and planners of attacks elsewhere illustrates how the Internet serves as a logistical tool for terrorist operatives.

Terrorist webmasters and militant extremists from dozens of countries are exploiting the anonymous, inexpensive, and easily accessible global reach of the Internet. Extremists are using the Internet media to recruit potential terrorist operatives, solicit funding for operations, train current terrorists with the latest in bomb-making knowhow, and plan operations against civilian targets worldwide. The success Al Qaeda and affiliated movements have had in exploiting the Internet as an operational centre illustrates that the Al Qaeda guerrilla movement has migrated from physical space to cyber space. With laptops, communication systems and the like,

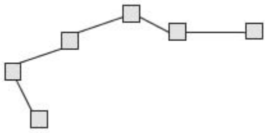
[13] Arik Hesseldahl, "After The Attacks, New Attention on GPS", Forbes.com, October 2, 2001. http://www.forbes.com/technology/2001/10/02/1002gps.html

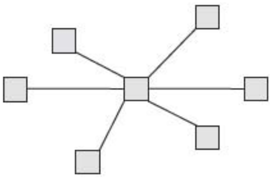
[14] Sue Kwon, "GPS Technology Could Help Taliban Fight U.S", KPIX Channel 5, U.S http://beta.kpix.com/news/local/2001/10/23/GPS_Technology_Could_Help_Taliban_Fight_U.S..html

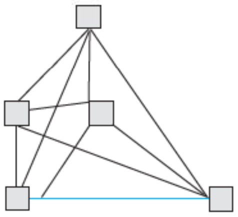
[15] "Anti-Defamation League, Jihad Online: Islamic Terrorists and the Internet" 9 (2002), http://www.adl.org/learn/internet/jihad_online.pdf

jihadists have sought to replicate the training, communication, planning, and preaching facilities they lost in Afghanistan with countless new locations on the Internet.[16]

THE FABRIC OF NETWORKS







The networks of these groups need to be analysed for a better appreciation of their operations and organisation. According to John Arquilla and David Ronfeldt, the network fabric is of three types; chain, hub and meshed.

- **The chain network** is typified by smuggling networks, where end-to-end exchanges (information, contraband, etc.) must travel back and forth between intermediary nodes. This is also a feature of a hierarchical network.
- **The hub, star or wheel network** as in a franchise or a cartel where a set of disparate actors is tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other.
- **The all-channel full-matrix or meshed network** is a collaborative network where every individual actor is able to communicate fully with all other nodes in the network.

Each node/point in the diagram can refer to an individual, a group or an organisation or even a state. The nodes maybe loosely or tightly coupled to the central agency. The loosely coupled ones take orders from the central agency and after that they are largely on their own. These loosely coupled ones, once let loose, will be difficult to recall. They may revert to the centre only in extreme cases. The tightly coupled ones are more integrated with the central agency and a greater control can be exercised over them.

[16] Steve Coll & Susan B. Glasser, "Terrorists Turn to the Web as Base of Operations", http://commlaw.cua.edu/articles/v15/Davis.pdf

Each type may be suited to different conditions and purposes, and all three may be found among netwar related adversaries e.g., the chain in smuggling operations; the hub at the core of terrorist and criminal syndicates; and the all-channel type among militant groups that are highly internetted and decentralised. There may also be hybrids of the three types, with different tasks being organised around different types of networks. For example, a netwar actor may have an all-channel council or directorate at its core but use hubs and chains for tactical operations.

There may also be hybrids of network and hierarchical forms of organisation. For example, traditional hierarchies may exist inside particular nodes in a network. Some actors may have a hierarchical organisation overall but use network designs for tactical operations; other actors may have an all-channel network design overall but use hierarchical teams for tactical operations. Again, many configurations are possible, and it may be difficult for an analyst to discern exactly which type characterises a particular network.

The all-channel model is becoming increasingly significant as a source of organisational collaborative power. The all-channel network has no central leadership and no key node whose removal might disrupt the entire organisation. Instead, the network is completely decentralised, allowing for initiative and autonomy at lower levels in the organisation which may at times appear to be operating without anyone in charge, and at other times, multi-headed. The all-channel network is one of the most difficult to maintain because it requires a strong communications capacity to maintain ties between nodes. Moreover, nodal autonomy results in a distributed, consensus style of decision-making which is necessarily dependent on back-and-forth communication. As such, this form of organisation has only recently become feasible on a greater scale with the dawn of the information age.[17]

APPRECIATING THE PROBLEM

Infowar is inevitably, as any survival contest is, split between the offensive and the defensive. The advantage more than not often lies with the

[17] Arquilla and Ronfeldt, n. 1.

initiator, who is like a needle in a haystack, making things difficult for the defender.

In a conflict, many nations today are more willing to drop a laser guided bomb through an opponent's window than penetrate his computer system. This is because they and the public at large have failed to grasp the fact that cracking into an adversary's computer, or putting a hacksaw through a fibre cable, is acting no differently than if they were shooting off a ballistic missile or lobbing a satchel of charge into a munitions depot. It is an act of war, but not appreciated in that sense.

A government which sponsors crackers to bust into another country's computing infrastructure is performing at a minimum the equivalent to a special operations commando penetration of its opponent's military basing or government buildings. This is equivalent to a large scale bombing raid or special commando operation and should evoke an equivalent response; but it does not. The underlying cause for this clearly irrational posture is that the gravity of the act is undervalued, and it is, therefore, dismissed as being of substantially lower importance than it really is. Until such an attack produces a truly dramatic, Pearl Harbour category disaster, it is unlikely that the message will get across.

This issue is further complicated by the boundaries between military and civil operations. Whereas legislation may eventually allow a nation's armed forces to respond in kind, or respond preemptively to an information attack, with a like information attack, or conventional counter-strike, civilian agencies and commercial players are unlikely to be afforded such latitude. For instance, a security guard at a bank may open gunfire on an armed intruder trying to force his entry into a bank; however, a bank's system programmer launching a denial of service against a criminal attempting to break into the bank's internal network is, at this time, legally problematic. More than likely, it would result in the criminal's Internet Service Provider (ISP) successfully suing the bank in question. The issue of legislation is indeed a thorny one, and one which will take some time to sort out. If conventional, precedent-based legal practices are to apply, many of these issues will have to wait for test cases to produce rulings. In the meantime, a good measure of paralysis will exist.

Rules of Engagement

The legal issues are closely related to the issue of Rules of Engagement (RoE), the fundamental constraints and protocols which are applied to any military operation. These have been in existence since the epic periods of the *Ramayana* and *Mahabharata*. In conventional wars, such as those fought in the Persian Gulf in 1991, or over Serbia in 1999, the conflicts were waged under some frequently complicated and often very restrictive RoE. In conventional wars, the RoE are very carefully crafted to reflect political and operational constraints. What can and cannot be attacked, and under which conditions it can be attacked, is carefully (or not so carefully in some instances) defined and set down as inviolate constraints to military personnel. The purpose is primarily to set boundaries for military operations, either in terms of geography or types of targets to be engaged. A typical RoE package today includes constraints from the Law of Armed Conflict (LOAC), which are mostly aimed at preventing the loss of innocent civilian lives, or the destruction of significant historical or cultural artefacts. While much debate continues as to the merits of many RoE packages and philosophies, it is a fact that responsible states would go to war with some kind of RoE. Defining a meaningful RoE package for infowar is not an easy task, and is yet to be properly resolved. History is witness that RoE has been violated in the past by the belligerents and heavyweights and will also be in the future. In this scenario of networked operations, establishing the RoE is very important because of the diffused and seamless nature of networks, and should be construed as guidelines.

In this scenario of networked operations, establishing the RoE is very important because of the diffused and seamless nature of networks, and should be construed as guidelines.

Consider the scenario in which an opponent's electricity grid or communications network is taken down. Both are target sets which evoke much argument in conventional targeting, since it can be argued that denial of both services can indirectly cause civilian casualties, and impose unreasonable hardship upon the population. Taking down an opponent's finance infrastructure or stock market, plunging it into an economic collapse, could produce similar effects. Will this constitute a violation of established protocols designed to protect civilians from unreasonable hardship? Wrecking of a nation's economy via a systematic information attack on its finance infrastructure could produce wider repercussions by damaging countries with mutual economic dependencies with the target nation. These are not very different from physically wrecking its economy by large scale air raids. All these are interesting questions which need to be understood and properly addressed.

The other side of this coin is dealing with players who choose not to observe any RoE. For example, a clash with non-state actors or terrorist organisations or tin-pot dictators, with scant respect for international conventions, has been a source of concern. Players who fall into this category are unlikely to restrict their offensive information operations to target sets deemed legitimate under international law. Parking a surface-to-air missile launcher in the grounds of a hospital, or putting a civilian air raid shelter into the same facility as a military command post are both good examples of such behaviour.

Boundary Spanning Criminal Organisations

Boundary spanning/trans-national criminal organisations are empowered by the Information Technology (IT) form in the sense that it heightens their mobility, adaptability, and their ability to operate trans-nationally. These trans-national networks pose a problem for states operating in a conventional, inwardly focussed manner. For instance, drug cartels around the world draw power from their extended trans-national network resources, making it difficult for the governments to fight the cartels within the confines of their national boundaries. Thus, networking allows these organisations to easily operate across jurisdictions, evading national law enforcement agencies. Networks also make it more difficult to dismantle a criminal operation, given that there is less emphasis on a rigid, central leadership.

Despite these vast differences, all terrorist groups have one trait in common: they do not commit actions randomly or senselessly.

Media and Perception Management

The acquisition by terrorist groups of an offensive IO capability could represent a significant threat as the world becomes more dependent on information and communications flows. In addition to enabling networked forms of organisation, IT can also improve terrorist intelligence collection and analysis, as well as offensive information operations. The goals and motivation of terrorists vary widely from the fulfilment of some divinely inspired objective to issue-specific causes like education for girls. Despite these vast differences, all terrorist groups have one trait in common: they do not commit actions randomly or senselessly. Each wants maximum publicity to be generated by its actions. They seek to impress. They use the modern media as the principal conduit and, thus, the media 'unwittingly' form a vital part in the terrorists' calculus. Without media coverage, the impact of the act is wasted and could remain narrowly confined to its immediate vicinity.

The first group to successfully harness the power of the Internet was the Zapatista National Liberation Army (EZLN) or simply Zapatistas, an insurgent group. The Zapatista movement began as a seemingly traditional, hierarchical insurgency, but has transformed into an information-age conflict following setbacks in battles. The guerrillas switched tactics and began to exploit the network form, taking advantage of the Non-Governmental Organisations (NGOs) connections to mobilise global awareness and support for their reform movement, while putting pressure on the Mexican government. The Internet, which was in its infancy at the time, also became a key space for networking various groups from around the globe with the Zapatista movement. It made communication with the rest of Mexico and the world a high priority. The EZLN used technology, including cellular phones and the Internet, to generate international solidarity with sympathetic people and organisations. Its effective exploitation of the Internet in the beginning of the 1990s was subsequently emulated by other insurgent movements.

Getting a message out and receiving extensive news media exposure are important components of the terrorist strategy, which ultimately seeks to undermine the will of an opponent.

Terrorist groups seem to be adopting flexible, decentralised network structures as part of a shift away from formally organised, state-sponsored groups to privately financed, loose networks of individuals and sub-groups that may have strategic guidance but that, nonetheless, enjoy tactical independence. Past terrorist groups did incorporate autonomous cells, but they were largely coordinated in a non-networked manner. Newer terrorist movements such as Hamas, Hezbollah and Al Qaeda all employ less hierarchical, loosely interlinked organisational models. Rather than the rigid bureaucratic structures and nationalist agendas of the old terror groups, these new operatives are networked, relying on decentralised decision-making, with flexible ties between other individuals and radical groups sharing common values.

Given the importance of knowledge and soft power, it is not surprising that networked terrorists have also begun to leverage IT for perception management and propaganda to influence public opinion, recruit new members, and generate funding. Getting a message out and receiving extensive news media exposure are important components of the terrorist strategy, which ultimately seeks to undermine the will of an opponent. In addition to such traditional media as television or print, the Internet now offers terrorist groups an alternative way to reach out to the public, often with much more direct control over their message. The news media play an integral part in a terrorist act because they are the conduit for news of the violence to the general population. The 26/11 attack on Mumbai highlights this. As Bruce Hoffman has noted,

> Terrorism . . . may be seen as a violent act that is conceived specifically to attract attention and then, through the publicity it generates, to communicate a message.

Terrorists have improved their media management; in fact, some groups have even acquired their own television and radio stations to take direct control of the reporting of events. Hezbollah, through its television station, has broadcast footage of strikes carried out by its operatives and has a sophisticated media centre that regularly—and professionally—briefs foreign journalists. Hezbollah field units have even included specially designated cameramen to record dramatic video footage of Israeli casualties which are then aired in Lebanon and usually rebroadcast by Israeli television.

The Internet now expands the opportunities for publicity and exposure beyond the traditional limits of television and print media.

The Internet now expands the opportunities for publicity and exposure beyond the traditional limits of television and print media. Before the Internet, a bombing may have been accompanied by a phone call or fax to the Press by a terrorist group claiming responsibility. Now, bombings can be followed—should the terrorists so desire—by an immediate Press release from their own websites (at little cost).

Disruptive Attacks

If the ultimate goal of a terrorist is to influence his opponent's will to fight, IO offers additional means to exert influence beyond using simple physical attacks to cause terror. Netwar-oriented terrorists can also use IT to launch disruptive attacks—that is, electronic strikes that temporarily disable, but do not destroy, physical and/or virtual infrastructure. Disruptive attacks include "choking" computer systems through such tools as e-bombs[18], fax spamming, and hacking techniques to deface websites. These strikes are usually non-lethal in nature, although they can wreak havoc and cause significant economic damage. To date, disruptive strikes by terrorists have been relatively few and fairly unsophisticated—but they do seem to be increasing in frequency. For example, in 1996, the Liberation Tigers of Tamil Eelam (LTTE) launched an e-mail bomb attack against Sri Lankan

[18] An e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Today's Mujahideen have launched a cyber *jihad*, signalling that terrorists are also armed with a technical and strategic mastery of the Internet.

diplomatic missions. Using automated tools, the guerrilla organisation flooded Sri Lankan embassies with thousands of messages, thus, establishing a "virtual blockade." In 2000, a group of Pakistani hackers who call themselves the Muslim Online Syndicate (MOS) defaced more than 500 websites in India to protest the conflict in Kashmir. Pakistan's Lashkar-e-Tayyeba too claimed to have attacked Indian military websites in early 2000. E-attacks on Estonia[19] which shut down most of the country in May 2007, comprise another example of the same.

Disruptive rather than destructive actions take place for several reasons. Terrorists who rely on the Internet for perception management and communication purposes, may prefer not to take "the net" down, but rather to slow it down selectively. In addition, groups may want to rely on non-lethal cyber strikes to pressure governments without alienating their own constituent audiences. Terrorist groups may also follow the lead of criminal hackers and use the threat of disruptive attacks to blackmail and extort funds from private sector entities. In the early 1990s, hackers and criminals blackmailed brokerage houses and banks for several million British pounds. Money can also be stolen from individual users who visit terrorist websites.

Today's Mujahideen have launched a cyber *jihad*[20], signalling that terrorists are also armed with a technical and strategic mastery of the Internet. This knowledge enables terrorists to indoctrinate, recruit, and train new members for attacks, with little or no threat of discovery or capture. Al Qaeda and other terrorist groups are effectively using the Internet and an estimated 4,500 terrorist-related websites to advertise a global brand of terror to millions of sympathetic Web users.[21]

[19] "Estonia Hit by 'Moscow Cyber War", http://news.bbc.co.uk/2/hi/europe/6665145.stmm.

[20] Cyber *jihad* is a term coined to loosely describe (Islamic) extremist terrorists' use of the Internet as a communications, fund raising, recruitment, training, and planning tool in their battle against the enemy.

[21] Benjamin R. Davis, "Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for CyberGovernance", http://commlaw.cua.edu/articles/v15/Davis.pdf

MANAGING/MITIGATING THE PROBLEM

As far as security is concerned, there is no best firewall. The continuum lies between the two extremes: absolute security and absolute access. The closest to absolute security would be a machine unplugged from the network; power supply removed, locked in a safe, and placed at the bottom of the ocean. At the other extreme is a machine with absolute access which is extremely convenient to use: it's simply there, without questions, no authorisation and no passwords. Unfortunately, both are of no use. Every organisation needs to decide for itself where, between the two extremes of total security and total access, it needs to be. A policy needs to articulate this, and then define *how* that will be enforced.

Entities with vested interests are well on their way to acquire IT-based technologies and skills. It is, therefore, conceivable that the current groups will adopt more-offensive IT strategies in the future. New hacker/terrorist groups may also emerge to compound this problem. Some terrorist networks may have even become sophisticated enough to sustain and coordinate offensive campaigns in both the virtual and physical realms. We, therefore, need to be aware of, and develop, a policy to counter the dangers associated with exploitation of IT by elements with nefarious agenda.

The policies and tactics should be able to impede the speed with which the groups become "informationised" because groups facing a robust counter-terrorism campaign will have less time and resources to acquire new technologies.

- The first is to monitor changes in the use of IT by target groups, differentiating between organisational and offensive capabilities. The type of IT capabilities developed by each group, targeting its specific technological vulnerabilities, should be taken into account. Monitoring the shift in capabilities for each type of IT use and then examining trends in the aggregate can also help forecast future behaviour. Among the most significant trends to be carefully examined is the possible emergence of a new, and potentially dangerous, breed of terrorists—groups that are highly "informationised" along both the organisational and offensive axes. Evaluating how IT shapes their organisational processes and offensive activities will remain a critical component of the threat assessment. In this regard, a number of "signposts" should be identified and tracked. These could include monitoring the level of technical expertise of known leaders and their subordinates, frequency of disruptive attacks, type of IT equipment owned, and nature of relatively secure off-the-shelf information technologies purchased over a period of time.

- The second is to target the information flow. Since network designs are inherently information intensive, efforts should target the information flows of identified groups. Intercepting and monitoring information exchanges should remain a top priority. The agency responsible for national security in our country should develop and design systems to decode encryption software, tap cellular transmissions, etc. This, besides being a useful addition to signals intelligence, should be leveraged beyond passive monitoring to active disruption of such communications or planting misleading information. This could breed mistrust and compromise the integrity and relevance of the network itself, eliminating their key competitive advantage.
- The third step should be to deter IT-based offensive IO through better infrastructure protection. Changing/plugging the vulnerability of critical infrastructures can significantly alter a terrorist's IT calculus. If infrastructures, such as those that manage air traffic control were to become relatively more vulnerable, they would become more attractive as targets. They could be struck from a distance, generating as much—if not more—destruction as would have been caused by the use of traditional weapons. We should identify specific vulnerabilities to expected threats and develop security techniques that mitigate each. Counter-terrorist agencies may also want to consider the option of employing a large number of ethical hackers and leveraging their knowledge for defensive and possibly even retaliatory purposes.
- Fourth, to counter the wars over the net, we will need to adopt organisational designs and strategies like those of the adversaries. This

does not mean mirroring them but rather learning to draw on the same design principles of network forms. These principles depend to some extent upon technological innovation, on a willingness to innovate organisationally and doctrinally, and on building new mechanisms for inter-agency and multi-jurisdictional cooperation—essentially beating them at their own game.

The information revolution has ensured that conflicts will increasingly depend on information and communications matters.

Some Safe Practices: Looking at the types of attacks that are common, there are a few practices that can help prevent security disasters, and help control the damage in the event that preventive measures are not successful in warding off an attack.

- ***Have back-ups.*** Operational requirements should dictate the back-up policy, and this should be closely coordinated with a disaster recovery plan that will enable one to carry out proceedings from another location in case the original one has been attacked.
- ***Don't put data where it doesn't need to be.*** This will prevent unauthorised access to information, reducing the severity of a break-in
- ***Avoid systems with single points of failure.*** Any security system that can be intruded into by breaking through any one component isn't really very strong. Ensure a degree of redundancy as it could prevent a minor security breach from becoming a catastrophe.
- ***Stay current with relevant operating system patches.*** Exploiting old bugs is one of the most common (and most effective!) means of breaking into systems. The latest patches must be uploaded to overcome existing bugs.
- ***Security advisories.*** Watch for relevant security advisories from CERT and similar agencies. Personnel should be trained and should be familiar with security practices. They should keep themselves abreast with the latest developments and keep track of the various problems that arise.

CONCLUSION

Practically all ruses and stratagems of war are variations or developments of a few simple tricks like manipulation of beliefs, actions based on altered perceptions exploitation of the benefits from these actions *et al*. These have been practised by man through the ages. These deception concepts are now being employed within networks in order to deceive or condition a target's perception about the intent or purpose of actions.

The information revolution has ensured that conflicts will increasingly depend on information and communications matters. More than ever before, conflicts will revolve around "knowledge" and the use of "soft power." Adversaries will emphasise "information operations" and "perception management"—that is, media-oriented measures that aim to attract rather than coerce, and that affects how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries. Psychological disruption may become as important a goal as physical destruction. Thus, major transformations are coming in the type of adversaries, in the nature of threats they may pose, and in how wars will be waged. Information age threats are likely to be more diffused, dispersed, multi-dimensional, and ambiguous when compared to traditional threats.

As terrorist groups evolve towards loose, ad-hoc networks that form and dissipate unpredictably, counter-terrorism forces should also adopt a more flexible approach that crosses bureaucratic boundaries to accomplish the mission at hand. While it will be difficult for the military and government to do away with their hierarchies entirely, there is nevertheless much room for them to develop a more robust and dynamic organisational network than they currently have—a change that may offset some, if not all, of the advantages now accruing mostly to networked groups with vested interests.

In the era of information warfare, net wars, cyber warfare and nuclear backdrop, C4ISR systems should have physical and electronic security, survivability and adequate redundancy so that C4ISR and NCO systems are protected against deliberate or inadvertent, unauthorised acquisition;

disclosure, manipulation, loss or modification of sensitive information. The military is already keenly aware – both that it will have little ability to control the flow of information to and from the theatre and that the media will monitor every action of a soldier minutely. In a media intense environment, politicians and the public have become very unforgiving of even minor mistakes and transgressions by military forces. Events with minor operational effects often have disproportionately large effects on public opinion and, therefore, policy and outcomes. As a result, even the smallest aspect of military operations must now be planned with greater sensitivity to the public perception of the conflict. New techniques that allow manipulation of video images and sound recordings have created an even greater technical ability for potential opponents to conduct sophisticated psychological operations. The ability to influence such perceptions may mean the difference between victory and defeat. Governments no longer have the ability to control the flow of information to the public or their soldiers, in both peace and war-time. The biggest obstacle in the coming years will continue to be the technological illiteracy of those outside the computing community, and the closely related problem of poor appreciation of the implications of the digital revolution in the social, political and economic settings.

Even the smallest aspect of military operations must now be planned with greater sensitivity to the public perception of the conflict.