INFORMATION WARFARE

Neil Munro, Washington Technology
Phone 703 684-8004.
NMunro@access.digex.net

Information warfare is the next big thing in the military.

It is emerging from the marriage of computerized weapons and a world wired for 500 cable channels.

Definitions are vague; One can view information warfare are a distinct arm of warfare or as a new perspective - a lens - to understand revolutionary changes in warfare.

Whatever it is, it's so big that the White House has been drawn in.

It has even won high-level attention from Congress; Here's a quote from Newt Gingrich; "Over the next 30-50 years, information warfare will be the kind of 'development definer' that the internal combustion engine and the radio were between 1880 and 1917. It will be an art of warfighting that is dramatically different than merely disrupting the opponent's command and control structure.

Like Alvin Toffler's 'Third Wave,' information warfare means a scale of change comparable to the shift from hunter-gathering to the Roman Army or from the Roman Army to the blitzkrieg and any vision of information warfare less monumental will be inadequate."

ORIGINS

The origins of Information Warfare lies in WWII, where both Axis and Allies relentlessly exploited the electromagnetic spectrum for advantage. The allies won that one - due in no small part to their skills jamming German radars and decrypting German's Enigma encryption devices.

The WWII experience led to the creation of two area of expertise - electronic warfare and electronic intelligence.

Electronic intelligence is the extraction of useful information from the ether and enemy cryptography, and is practiced by the NSA and all the services.

Electronic warfare is the effort to seize control of part of the spectrum for a short time, in order to jam an enemy missile, track an enemy aircraft and deceive an enemy leader.

EW and Elint were further developed during the Korean and Vietnam wars, where additional doctrinal variations appeared.

These included C3CM and SEAD. Command, Control and Communications Countermeasures is intended to wreck the command and control of enemy air defense networks. The Suppression of Enemy Air Defenses doctrine combines C3CM, EW and with physical attacks to suppress the radar-guided

THE GULF WAR

All these SEAD, C3CM, EW and ELINT skills were clearly demonstrated during the Gulf war, the Iraqi military's nervous system was very quickly crashed, allowing only the most limited communications between Saddam and his frontline troops.

But these doctrines were extended during the Iraq war to crash the Iraqi government's nervous system, partly to allow regional groups such as the Kurds and Marsh Arabs revolt against Baghdad. For example, the power grid, the telephone system, the bridges were wrecked, sharply limiting the hold of the Iraqi government over its own people.

These efforts were joined by open and covert psychological warfare efforts against Iraqi soldiers and civilians. for example, the CIA ran covert radio stations targeting Iraqi civilians, while the U.S. operated an open radio-based psyops campaign against Iraqi troops.

The combination of the physical attacks and the psyops campaigns seem to have had a great impact. Iraqi soldiers deserted or surrendered, and iraqi civilians revolted or stayed at home.

But the Iraqi government did not stay completely passive. It sought to foment international physops campaigns intended to weaken Arab support for the U.S.-led effort. With diplomatic promise and hostage-taking, it also tried to stoke internal splits in the United States over the value of the impending war, which caused several U.S. soldiers to go AWOL and made the Senate's vote for war a close-run thing.

Meanwhile, independent hackers rummaged through U.S. info-networks, seeking amusing and interesting data. There is no evidence that Iraqi tried to use these networks to collect data or inflict damage.

POST-GULF WAR

The Gulf war catalyzed U.S. thinking about information warfare.

Drawing upon years of analysis and study by people such as Tom Rona - the obstetrician of information warfare - Paul Strassmann and various analysts at SAIC in McLean, Va., DoD officials drew up a classified information war policy directive in late 1992.

I don't know the definition of info-war in the secret directive, but I don't have any reason to believe it differs from the version included in the Defense Secretary Perry's 1994 Report to the President and Congress which says;

"Information warfare is a mean to not only better integrate C4I, but also to address the comparative effectiveness of a potential adversary's C4I. It consists of he actions taken to preserve the integrity of one's own information systems from

exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information system, and, in the process, achieve information advantage in the application of force. Thus, Information Warfare is an aggregation of and better integration of C4, C4 countermeasures, information systems security and security countermeasures, and intelligence."

Tom Rona's version is broader, and places greater emphasis on peacetime info-war. Moreover, Rona emphasizes a vision of info-war that combines military-oriented info-war with peacetime political and cultural struggles.

Andrews' secret directive was followed by an JCS publication which used two new terms that reflected Pentagon think.

The first term was "Information Differential," that is, the superior access to and ability to employ information the strategic, operational and tactical situation which advanced U.S. technologies provide our forces."

The second term was "the informational instrument of national security strategy; public affairs, psychological operations, and public diplomacy. This information effort is crucial to the success of any contemporary military operation, because it involves the support of the American people, allies, and friendly nations and the morale of the opposing side."

The JCS also approved "Memorandum of Policy No. 30; Command and Control Warfare."

MOP 30 is the military's first cut at Information Warfare, and reflects the military's recognition that information warfare is much broader than the military's overview.

MOP 30 directs the CinCs to include in their staff a team of experts that will work together in peacetime and wartime to coordinate each commands's use of EW, Pysops, Physical Attack, Operational Security (OpSec) and Deception.

So, MOP 30 effectively directs Central Command to prepared integrated Info War plans for use against Iraq and other local enemies. The nature of such plans is clearly classified, but a few elements can be sketched.

- A plan to collapse the Iraqi air defense and surveillance networks.
- A scheme to wreck and manipulate Iraqi communications links.
- A propaganda campaign to undermine the Iraqi government's domestic and international credibility

The C3I info-war document that gave birth to the military's MOP 30 also directed agencies such as the NSA, the Defense Information Systems Agency, the DIA, the Defense Mapping Agency etc., to prepare for information warfare.

For these agencies, the main task was to boost the Pentagon's defensive capabilities. Yes, the NSA and the DIA are seeking to gather data on enemy vulnerabilities, but they are also trying to lean how an enemy might conduct info-war against the U.S. phone networks, the power grid, as well as the Pentagon's DISA-managed communications networks.

After all, the Pentagon is relying more and more on civilian information technology, services and providers.

For example, the Air Force relies on civilian package-delivery firms - and therefore their largely unprotected computer networks - to transfer spare part between frontline units and rear-area maintenance centers.

DISA uses commercial satcom providers to relay lower-priority data between combat units and support centers, including logistics, payroll and personnel data, and also uses commercial computer networks to process that data.

Pentagon reserve forces depend heavily on commercial computer systems and civilian phone networks to manage their mobilization in a crisis.

The interaction of civilian and military info-networks is getting more complex;

The Pentagon's GPS network is needed to guide and coordinate the military's combat units, missiles, ships and aircraft. It is also being used by a growing number of civilian firms - effectively reducing the military's ability to limit use of GPS by foreign militaries.

The NSA's eavesdropping task is being made more difficult by the proliferation of easy-to-use but hard-to-crack commercial crypto. The NSA's network-protection task is being made more difficult by the proliferation of computer-cracking tools and expertise through the Internet.

INFO-ASSURANCE

All of which means that the Pentagon has to be concerned that its commercial rear-end is very exposed to information-warfare attacks. The nascent effort to protect DoD and the nation's information networks has produced the term "Information Assurance."

Because Information Assurance is defense-oriented, it has proved somewhat easier for the government to digest - which explains why the term was chosen as the title of the new Presidential policy working its way through the system.

The draft presidential policy is mostly classified and may never be completed.

Many agencies are jumping on the bandwagon, including ARPA, which has already started a new information assurance technology effort aimed at protecting nationwide info-networks.

We'll see if this draft policy ever emerges into the light of day.

The Clipper controversy hints at the political controversy likely should he defensive-minded Info-war policy be approved. But the political
problems facing the offensive portion are even greater.

INFO-WAR PROBLEMS

Here a few questions for info-war advocates to answer;

- If info-war is so broad, how can it be defined narrowly enough to guide bureaucracies as they make policy, war plans and spending decisions?

- The value of deception was shown during the Gulf war when over-excited press reports played up the threat of a Marine Corps landing in Kuwait, tying down significant Iraqi forces in defense of beaches that were not to be attacked. Military officials did not lie to anyone about this supposed invasion, but they stood by when the media deceived itself and Iraqi listeners. That's OK by me - I wrote an article before the war broke out saying the invasion publicity was likely a deception campaign - but how can such a deception-policy be written in peacetime without generating cries of outrage from the Paladins of the first amendment and the public-spirited members of the fourth estate?

- How can the advantage and disadvantages of secrecy - ie surprise vs. technical flexibility - be balanced?

- Will the future of info-war be taken over by industrial-age bureaucracies such as the Air Force?

- How can the government integrate its open and covert pysops, public diplomacy and deception efforts with a democratic political culture that is leery of secrecy and government, and a capitalist system that fosters continual innovation via independent competing enertainment, news and cultural forces?

- How can the government prepare to eavesdrop upon or wreck international communications networks, wether it be the Internet or Iridium - many of which are being built or being operated by U.S. companies? What would AT&T demand in return for government's knowledge of its international networks? Is $500 million in the DTA be good enough?

In geo-politics, it's often easier to classify controversial policies or else just never write them down.

PROBLEM SOLVERS

The White House and the DoD are attacking these problems now.

The JCS headed by Adm. Owens is running info-war wargames, focussing mostly in very high-tech combat across a theater.

The Office of Net Assessment headed by Andy Marshall is preparing a report for John Deutch, the DepSecDef, on how to promote innovation in the U.S. military as the world undergoes an information-driven "Revolution in Military Affairs."

OSDC3I has its info-war group shrouded in secrecy.

The Air Force has its Information Warfare Center, the Army has TRADOC and the Navy has its SEW directorate.

Meanwhile foreign thinkers are at work. There is no reason to believe that foreign countries will not aggressively push these ideas - after all, other countries are poorer, and lack the Pentagon's armory of sensors and weapons so they need a comparative advantage.

In some ways, Information warfare is as easy to export as concept of a Panzer division.

Pentagon doctrine, rival ideas, can be read in open literature.

Ferriners can be clever - ask the Poles who managed to make the first inroads into the German Enigma machine. Ask the Indians software group in Bangelore which is one of two software centers in the world rated at level 5 by the SEI. Moreover, information-age technological skills learned by foreign students in the U.S. can be easily transferred to info-war applications.

Info-war promises a very high-payoff for a limited investment

There are many ways to wage info-war, whether it be in peace or crises, against armies or peoples.

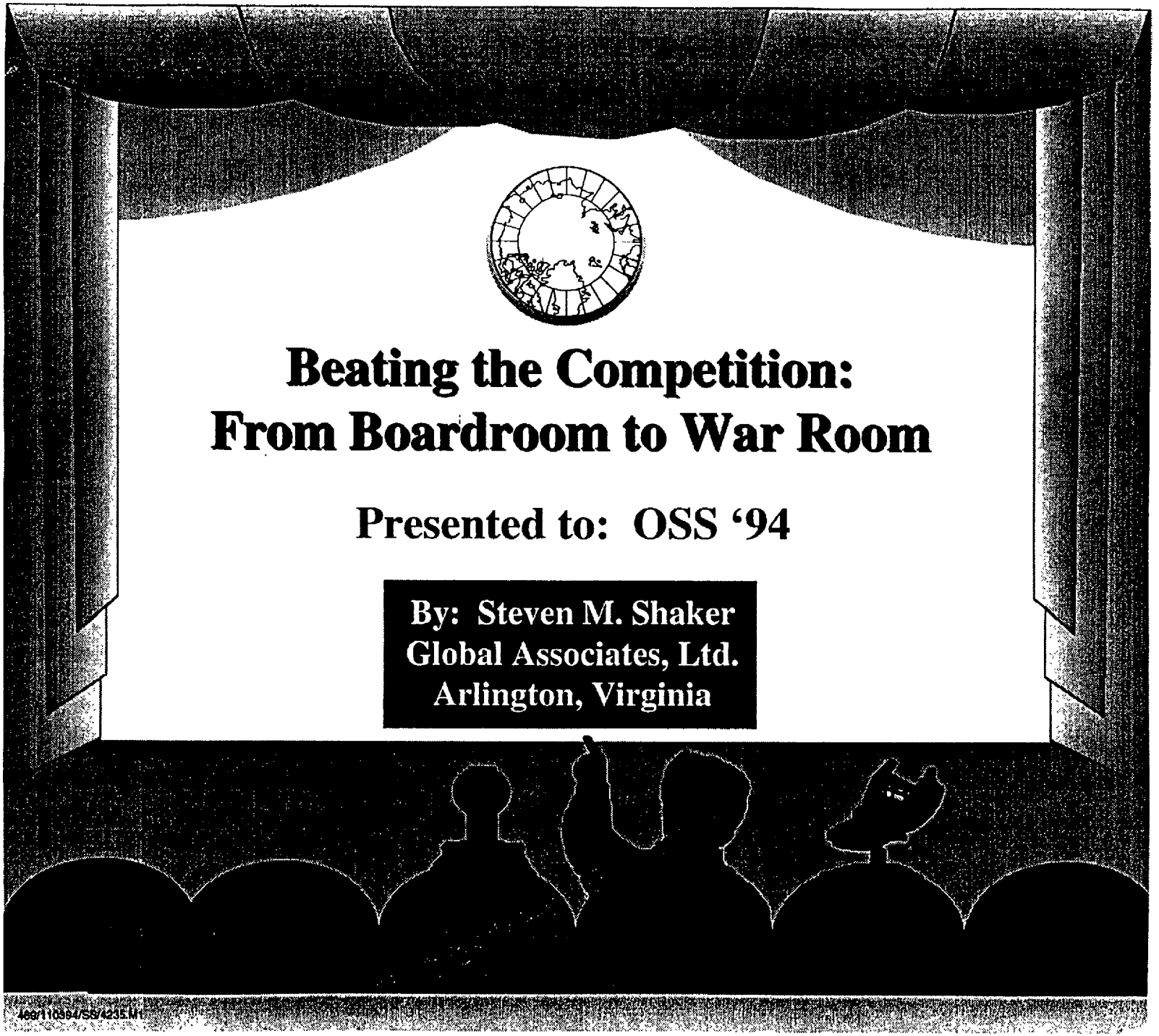
CONCLUSION

Let's try a little history here; In 1906, Adm. Jackie Fisher, the British Empire's "first Sea Lord," - surely the best title in military history - launched HMS Dreadnought, the first of a new generation of battleships that made the world's existing battleships - including the British Empire's many battleships - obsolete overnight.

This sudden technological change gave Imperial Germany a chance to a Navy to rival the Brits. After all, the odds were suddenly 0:1 Dreadnoughts instead of a few:many old warships.

But by braving his critics and leaping into the future before the Germans, Italians, Japanese or Americans launched their first Dreadnoughts, Fisher preserved the Empire's naval mastery until the next technological development - aircraft carriers - proved beyond the Empire's resources.

What will be the result of this vast U.S. and foreign group-grope? Ask me next year for an update.


Beating the Competition:
From Boardroom to War Room
Presented to: OSS '94
By: Steven M. Shaker
Global Associates, Ltd.
Arlington, Virginia

THIRD INTERNATIONAL SYMPOSIUM on NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1994 Volume II - Link Page

Previous	ASIDIC Perspectives, and Its Contributions to National Competitiveness, by Ms. Maureen Kelly, President, Association of Information and Dissemination Centers (PART THREE)
Next	Beating the Competition: From Boardroom to War Room, by Steven M. Shaker, Global Associates, Ltd.

Return to Electronic Index Page