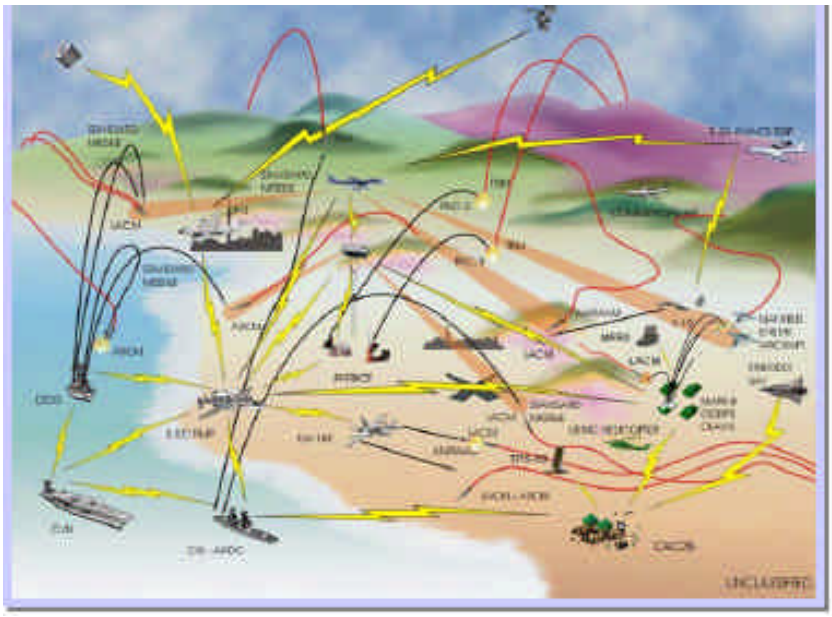
From Cyberspace to Battlespace

Speculations on Information Warfare and the Electronic Order of Battle in the Post-RMA Operational Environment



An Article

by

David Alexander

From **Military Technology** Magazine

Operations using the electromagnetic spectrum (the so-called fifth dimension of warfare) form a cornerstone of the Pentagon's transformation strategy to create a light, mobile, rapidly-deployable, digitally networked, high-technology military force with global reach by the year 2010. Information warfare (IW) operations are critical to the achievement of this objective, and dominance of the information sphere will prove of increasing necessity to achieve force-on-force superiority in the digitized battlespace that will define 21st century combined arms military engagements. In this regard it is correct to speak of a post-RMA (revolution in military affairs) operational environment, since global realities and technological developments have transcended the original RMA concept as originated at the end of the Gulf War.

If US DOD budgetary allocations for IW R&D are any indication of IW's importance to next-generation military operations, then increasing expenditures signal acknowledgment by the Pentagon of IW's importance to the defense sector. In FY97, for example an estimated USD544.4 million was requested by DOD for information systems and information technology research, development, testing and evaluation, out of an overall USD10.3 billion budget request, with some USD305 million earmarked for information security research, development, testing and evaluation. In FY98, the figure for such expenditures rose to USD 558 million. For the FY04 federal budget, sent to Congress on February 3 of this year, USD829 million was requested to improve information analysis and infrastructure protection, which includes approximately USD500 million to assess the nation's critical information infrastructure.

The IW budget requests from FY00 to FY04 of the Naval Information Warfare Activity (NIWA), which serves as program manager for the USN's offensive IW program, can be viewed as an indicator for the other service arms. Under Budget Item Z2263, for IW, appropriations requests rose from USD3,421 million to USD4,635 million between FY00 and FY02.

These skyrocketing funding levels reflect the expanded awareness in political and military circles that bytes have become as critical as bullets and bombs in defense and attack and that information operations of all kinds will become increasingly important both to homeland security and combined arms operations on the digital battlefield of the 21st century. In the approximate decade since the term "cyberspace" was coined, it too has moved from the realm of abstraction into the world of the concrete. Interactions and transactions in the digital realm of every imaginable type, and in all national sectors, have increased exponentially in the last decade, and will continue to rise. As former Secretary of Defense William Perry stated on the subject of RMA in 1996, "We live in an age that is driven by information. Technological breakthroughs ... are changing the face of war and how we prepare for war."

Of more recent coinage is the term information-based RMA (info-RMA or IRMA), referring to a similar revolution in information operations as they relate to the electronic order of battle (EOB). As Info-RMA, a December 2000 white paper by the Japan Defense Agency predicts, future warfare will be conducted by high-tech conventional attacks in concert with cyber attacks, in which the relative superiority of information awareness would give one side the decisive advantage in the battlespace. "In post-RMA combat, once caught by enemy sensors, a target could not escape the accurate attacks of precision guided munitions (PGMs). Therefore, battlefield awareness capability will decide the outcome of the battle," the report concludes. The distance from cyberspace to battlespace is now a short leap.

The U.S.-UK coalition War on Iraq (which is still in progress at the time of this writing) is an adumbration of this future battlfield as light, digitally enabled and highly mobile formations supported by combined arms information operations make rapid advances in theater. That this has happened when a fourth generation warfighting force takes on a second generation opponent is to be expected. In other respects, however, the digital battlefield has materialized along lines that few if any of the architects of the 21st century battleforce were able to surmise. One of these unforeseen consequences is the extension of the battlefield to the homeland, specifically to the continental U.S., a fact that has perhaps surprised Americans far more

than other nationalities due to a national mindset that wars are fought "over there" but not "here."

To say that this should have been obvious in hindsight is probably Monday morning quarterbacking; nevertheless the proliferation of digital networks and exponentially increasing interactions in cyberspace in the private sector, and increased interconnectedness of many former private sector elements to the military sector, seem to have made it inevitable that this materialize, or that nonstate transnational actors, such as Al Qaeda and other terrorist groups, would view information attack as one of the asymmetric strategies available to them. In short, digital information networks present us with the metaphor of microchip as Achilles heel. In the words of ADM William Studeman (Ret.), former Deputy Director of Intelligence for the USN, "Massive networking makes the United States the world's most vulnerable target for information warfare." In this light the so-called electronic Pearl Harbor warned against in early IW position papers can be said to have at least in part materialized with the devastating terrorist attacks of September 11th, 2001.

This observer, having been caught close to Ground Zero on 911, has no doubt that the attack on the World Trade Center towers represented an intentional attack on a major U.S. strategic information target. Within a short time after the first hijacked jetliner struck the 110-story North Tower, most cellular phones, including my own, went dead. Bank ATM networks, the New York Stock Exchange's computers, television and radio broadcasting infrastructure, electronic control infrastructure for subway and surface transit and conventional land-line communications infrastructure were also compromised. The World Trade Center housed major telecommunications switching nodes and computer systems affecting Wall Street trading, and thus the global marketplace.

Similar damage was done to the Pentagon in what this observer hypothesizes based in part on forensic evidence relating to the sophistication of Al Qaeda's pre-strike planning, might have been a deliberate attempt to compromise the National Military Command Center (NMCC), which is a global nexus of U.S. command and control. The NMCC, whose upper and lower levels are located on the Pentagon's third and second floors, respectively, and which include such facilities as the Current Actions Center (CAC), Emergency Conference Room (ECR), the JCS Conference Room (known popularly as "The Tank"), and which also houses the Crisis Management Automated Data Processing System, is perhaps the main strategic operational hub of the U.S. As such it could well be considered a "center of gravity" for information attack

in the classic Clausewitzian sense as well as a strategic information target in the same sense as was the WTC. In other words, the 911 attacks might be considered as brute "denial of service" attacks on a massive scale, ones in which information infrastructure was subjected to a conventional rather than a cyber-based attack.

While the IW components of the 911 attacks have been overshadowed by the immense physical destruction and loss of life caused by the attacks, these IW components incontestably played into the terrorists' strategy, and can thus be seen as asymmetric attacks on the United States critical information infrastructure. In their aftermath Al Qaeda's threats of specifically targeting the U.S. banking system leave no doubt about terrorists' grasp of the concept of IW as a viable form of asymmetric warfare. More aptly, it has been estimated that of the some one hundred nations said to possess an information attack capability against the U.S., some fifty of those nations have already done so in the form of hacker break-ins of government and private sector information networks. One such break-in, now declassified, occurred in 1994, during which classified files were downloaded from Rome Laboratory's records database (Rome Laboratory is a civilian R&D facility administered by the USAF, located at Grifiss AFB).

Of course asymmetric attack is not the sole province of terrorists. IW operations were integral to the “shock and awe” campaign that preceded the ground phase of the War on Iraq and have continued throughout. These operations were intended to suppress Iraqi C^3I and to thereby degrade or destroy the ability of opposition force military commanders to effectively coordinate their forces in the field in defense and attack. Electronic warfare (EW) operations, now doctrinally a subset of IW operations, were also used in these paroxysmic opening hours of the war as part of the counter-C^3I mission. Psychological operations (psyops), another subset of IW operations, were also conducted, including leafleting and media broadcasts to the Iraqi populace.

The fiber optic infrastructure used for Iraqi military communications was attacked with the first wave of coordinated TLAM and ATGM strikes on Baghdad. Iraq's Chinese-built Tiger Song fiber-optic network, linking air-defense radars, comprised in part of American-made technology obtained with a waiver from the Clinton administration, was a primary target of the CENTCOM air tasking order and TOT lists, and continued disruption of this key command and control infrastructure has been an ongoing priority. Iraq's fiber optic network has been a long-term subject of strategic interdiction planning. It was first struck during the joint U.S.-UK Desert Fox air campaign

of December, 1998, whose mission objectives were "to strike military and security targets in Iraq that contribute to Iraq's ability to produce, store, maintain and deliver weapons of mass destruction." It was again the target of coalition air strikes in a raid in August, 2002, when coalition smart munitions again struck the center at al-Nukhaib, a major Iraqi C^2 node. Notable in the attack were the use of what is said to have been PGMs tailored to the destruction of fiber-optic nodes.

During the opening phase of the War on Iraq, conventional electrical and land-line-based communications networks, as opposed to fiber-optic nets, were targeted as well. Here, as in the opening phases of the 1991 Desert Wind phase of the Gulf War, TLAMs equipped with the Kit-2S antielectrical package were also deployed against Iraqi targets. The Kit-2S package makes use of rope chaff, a silicon-based filament impregnated with particulate carbon, in order to disrupt the transmission of electrically based streams across wire-based transmission systems. In the opening phase of Desert Wind, some twenty-eight electrical targets were selected in an operation code-named "Poobah's Party," derived from the callsign of the USAF general responsible for EW operations against Iraq. Attacks on the so-called AT&T building, a twelve-story communications switching facility in downtown Baghdad, through which more than half of all Iraqi military C^2 transmissions were routed, made it a priority target of the first strike, and the only building targeted by two coalition aircraft simultaneously.

Unconfirmed reports also have it that high power microwave (HPM) munitions (so-called e-bombs) were deployed during the current shock and awe campaign in Iraq. In 2000 British researchers at Matra-BAE Dynamics developed non-explosive artillery ordnance producing EMP-life effects over a span of several miles. Subsequent development has resulted in TLAM- and artillery-deliverable variants, the latter capable of being fired from both 155 mm howitzers and MLRS. Other variants could be equipped with penetrator warheads for interdiction and destruction of deep underground facilities (DUFs) such as buried command bunkers.

The standard HPM package fits inside an outer casing which breaks open over the target, at which point the munition unfolds its radio transmitter aerials through which a high-powered electromagnetic pulse in the terawatt range is transmitted. This high-powered microwave (HPM) energy is emitted as sidelobe pulses rather than as a single beam in order to minimize backscatter which can compromise navigational and targeting systems of friendly aircraft. For the same reason HPM munitions are deployed by standoff systems rather than aerially delivered as proximity fuzed ATGMs.

While use of HPM munitions is currently the subject of speculation, U.S. Defense Secretary Donald H. Rumsfeld has uttered enigmatic pronouncements concerning their use. "Though the Pentagon prefers not to to use experimental weapons on the battlefield," said Rumsfeld, "the world intervenes from time to time."

Flux-compression generator (FCG) ordnance is a variant of weaponry producing EMP-like effects. These weapons are worrisome because relatively simple to manufacture; in fact one of the principal architects of such weapons has stated that any country or transnational group possessing 1940s technology could in theory manufacture FCGs. And FCG is essentially an explosive-packed tube nested within a slightly larger copper coil. Instants prior to the detonation of the chemical explosive, the coil is energized by a bank of capacitors, generating a powerful electromagnetic field. Because the explosive charge detonates from the rear forward, as the tube flares outward it touches the edge of the coil, thereby creating a moving short circuit, which in turn produces a ramping current in the megawatt range; enough raw electric power to black out a small city. The relative simplicity of the design of FCG ordnance makes its acquisition by terrorist groups seeking a devastating asymmetric IW weapon a cause for considerable concern.

Weapons and forms of strategic attack such as those described above represent the more tangible manifestations of battlefield IW toward achieving rapid operational dominance and sustaining/maintaining OPTEMPO. Whether or not HPM or other EMP-like weapons have been deployed against Iraq, it is certain that as more facts become known it will be demonstrated that the offensive IW mission has proved a primary concern for coalition warplanners. But defensive IW operations are also sure to have been conducted. When USAF Major General Ken Minihan (Ret.) suggested in 1995 that IW be viewed as "the microchip as aimpoint," he added, "I want to defend it, and I want to attack it, and I want to do that in an integrated way."

Indeed, among the two most visible systems that can be considered defensive IW assets are AWACs and J-STARS, which, respectively, facilitate real-time identification and tracking of friendly and unfriendly assets in the air and on the ground (AWACs also possesses ground tracking capabilities). Likewise, offensive and defensive IW operations solely within the realm of cyberspace will almost certainly have played their part in the war. Information warriors working out of the DIA's Office of Information Defense, DISA, the USAF's Information Warfare Center, the USN's Space, Information Warfare, Command and Control Directorate, and other similar agencies, including the

FBI's Cyber Technology Section based at Quantico, Virginia on the domestic front, have been tasked with both offensive and defensive IW missions.

In battlelabs and warfare planning and development centers, the information warfare mission is the subject of increasing operational initiatives. All service branches have incorporated IW (or NCW for network centric warfare operations, a less common usage) into the electronic order of battle. White papers published by the USAF have recognized that domination of the information spectrum is as critical to present and future conflict as controlling air and space or occupying land had been in the past; this is typical of USN, US Army and USMC doctrine too. USAF doctrine now views information power, like airpower and space power, as an indispensable and synergistic component of aerospace power, and holds that, while traditional principles of warfare still apply, information has evolved beyond its traditional role.

Today, the USAF states, "information is itself both a weapon and a target," echoing the Minihan definition of "microchip as aimpoint" of earlier coinage. Information operations, using a variety of information in war (IIW) functions are seen as key enablers of battlespace awareness, affording commanders insight into the operational environment in which their forces are deployed and promoting more effective aerospace operations. Information operations, involving actions that affect adversary information and information systems while defending friendly information systems toward achieving and maintaining information superiority are a key element of joint command and control doctrine as well as a critical part of aerospace security.

Even a partial description of current IW initiatives in the defense sector would require a separate article, but a brief listing of some of the key programs in the accompanying sidebar should present a picture of the overall scope of information operations' critical role within the EOB of 21st century warfighting forces.

Politically, cyberwarfare and cyberdefense initiatives have been brought into focus by the last two U.S. presidential administrations. Several Clinton administration-sponsored bills on cyber-security were introduced to the 106th Congress. During his tenure at the Pentagon former Secretary of Defense William Cohen warned of the risks of asymmetric IW. The U.S. Executive Order on Critical Infrastructure Protection of October, 2001, which came in the wake of the 911 attacks, acknowledged that information technology has "changed the way business is transacted, government operates and national defense is conducted." It called for a broad range of initiatives to protect critical U.S. information infrastructures and to insure against their future disruption. Most recently, on February 14, 2003, the Bush administration

issued its National Strategy to Secure Cyberspace, calling, among other recommendations, for the creation of a comprehensive cyber-security defense system for critical information infrastructure in all national sectors.

Though slow to become integrated into the electronic order of battle, mastery of information operations in attack and defense toward the achievement of information dominance has become mission-critical for all service branches, as pointed out at the beginning of this article; indeed, we can now speak of an Info-RMA as a revolution in military affairs in its own right. Yet the seamless integration of IW into joint operations and the realization of a true system of systems architecture remain achievements for the future. At present loopholes in information security continue to pose serious vulnerabilities; the threat of information terrorism will not soon go away. On the homeland security front, the recent Bush administration plan lacks concrete, nuts-and-bolts solutions, and proposes too great a reliance upon cooperation by the private sector.

All in all, however, information operations are now as much a part of the ground truth as ships, planes and tanks and a chief component of the electronic order of battle. IW is an integral part of the way 21st century military forces wage war and will continue to prove a key enabler for prevailing in all forms of future conflict.

SIDEBAR: U.S. IW PROGRAMS AND INITIATIVES

■ DARPA: The Information Awareness Office (IAO). IAO will imagine, develop, apply, integrate, demonstrate, and transition information technologies, components, and prototype closed-loop information systems that will counter asymmetric threats by achieving total information awareness that is useful for preemption, national security warning, and national security decision making.

■ DARPA: Tactical Technology office (TTO): The Ultralog program will create survivable command and control systems highly resistant to information attacks under the harsh, chaotic conditions of a major regional contingency (MRC) supported by directed adversary information warfare attack. Core architectures for Ultralog include: adaptive communications protocols, layered certificate and encryption-based data security, software that can recover heuristically from catastrophic information loss, high system fault tolerance and system scalability.

■ DARPA: Advanced Technology Office (ATO): The Composable High Assurance Trusted Systems (CHATS) program will focus on the development of the tools and technology that enable the core systems and network services to protect themselves from the introduction and execution of malicious code and other attack techniques and methods. WolfPack will hold enemy radar and other battlefield communications emitters at risk throughout the tactical battlespace while avoiding disruption of friendly military and protected commercial radio communications. Air-deployable, ground-based, close proximity, distributed, networked architecture will be used to obtain radio frequency spectrum dominance via a node based system to sense the radio frequency environment, ascertain the type and configuration of the threat and disable unfriendly communications and/or radar reception.

■DISA: Center for Information Systems Security (CISS): The center's goal is to create and manage a unified, fully integrated information systems security program for all Defense Information Infrastructure (DII) systems. CISS acts as the focal point for assuring availability, integrity and confidentiality of DII Automated Information Systems (AIS) information. Other DISA initiatives in

this sector include Global Combat Support System (GCSS), Information Assurance (IA) and the Defense Information System Network (DISN).

■SPAWAR (Space and Naval Warfare Systems Command): The Space and Naval Warfare Systems Command designs, acquires and supports systems which collect, coordinate, process, analyze and present complex information to the nation's leaders. It administers the Navy Marine Corps Intranet (NMCI). Integral to SPAWAR's knowledge base are the following disciplines: Advanced technology, space systems, information support systems, information and electronic warfare, command, control and communications, and command, control, communications, computing and intelligence, surveillance and reconnaissance (C^4ISR). IW initiatives will be directed toward the newly established Program Executive Office for Command, Control, Communications, Computing, Intelligence and Space (PEO C^4I & Space).

■USN: Naval Surface Warfare Center (Crane Division). The Surface Electronic Warfare Engineering System Department provides full spectrum engineering services to the Navy, Coast Guard, and Foreign Military Sales (FMS) customers for Surface Electronic Warfare (EW) systems. These services include development, design, test and evaluation, product engineering, production support, acquisition engineering, specialty engineering, and full fleet support for all Navy Surface EW systems. Also provided are engineering, logistics, and maintenance and repair support for the ALQ-99 Airborne Countermeasures System used in the Navy/Marine EA-6B and Air Force EF-111A aircraft and other EW systems used by USN, USMC, USAF and other customers.

■USN: Naval Air Warfare Center Weapons Division Information Warfare Division (IWD). Pursuing programs in support of Battle Force C2, Battle Force ISR and Battle Force NAV and their C^4ISR, IW and NCW subfunctions. These include the Sea Strike, Sea Shield, Sea Basing, Strike Land and Air Defense (SLAAD) and FORCEnet initiatives intended to facilitate fleet and force protection, littoral ASW, time critical strike, warfighter protection, autonomous operations and the information operations central to the successful completion of these missions. The IWD also undertakes the horizontal integration with and identification and exploitation of existing and emergent systems and technologies for integration into IW products, the development and deployment of comprehensive IW and planning system capabilities, and the acquisition of capability packages for DOD and non-DOD entities.

■USAF: Information Warfare Center: Development and acquisition of critical infrastructure in support of aerospace information operations,

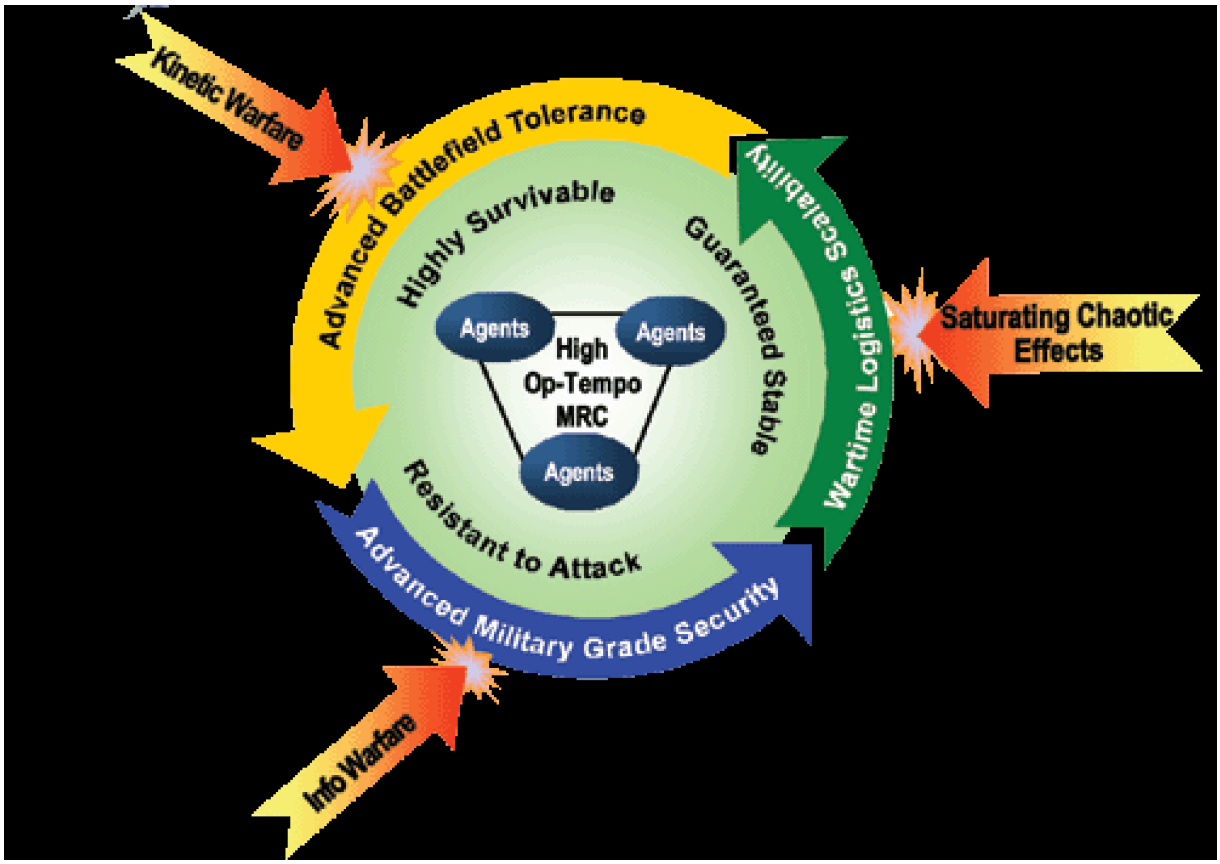
battlespace awareness and domination of the information spectrum. A specific program goal is technological engenderment of the single integrated air picture (SIAP) for battlespace awareness through integration of the Link-16 sensor-to-shooter network, incorporating data fusion from air, sea and ground assets such as E-3 AWACS, E-8 J-STARS, space based infrared system (SBIRS), AEGIS and land-based forces.

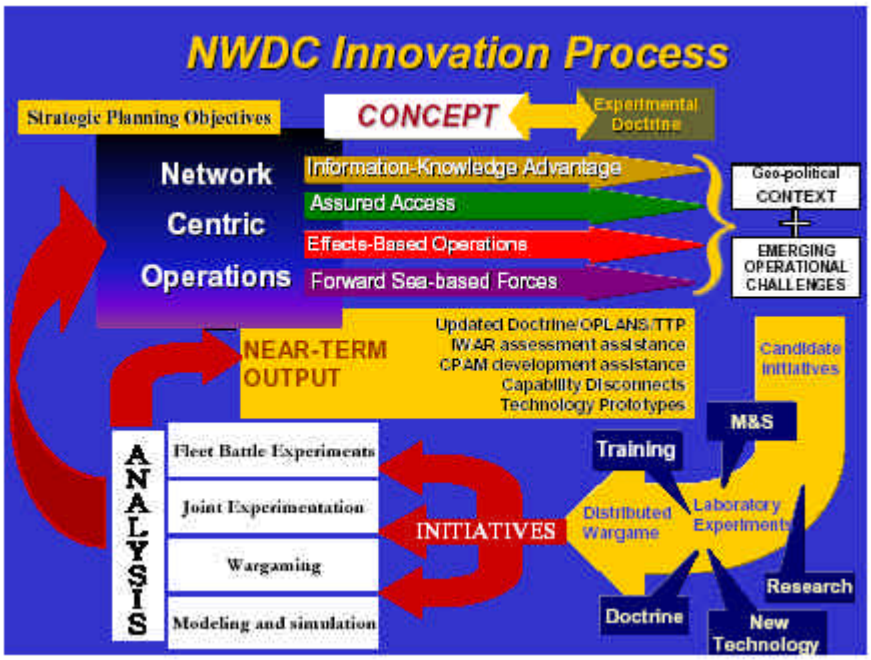
■USMC: Strategy 21: The United States Marine Corps' Strategy 21 incorporates information operations in support of MAGTFs and special purpose MAGTFS (SPMAGTFs), fleet antiterrorism security teams (FASTs), chemical biological incident response force (CBIRF) and C^3I functions associated with regional combatant commanders and joint forces commanders leading these and other forces. MITNOC-deployed support section teams serve as liaison between operating forces and IT bodies within USMC, USN and DISA. The Marine Intrusion Detection Analysis Section (MIDAS) is a computer incident response team. Development of the deployed security interdiction device (DSID) consisting of a suite of technologies to provide USMC operating forces with information security in the field. Sea Dragon is a program for concept-based battle experimentation conducted by the USMC Warfighting Lab (MCWL). Hunter Warrior wargaming has used advanced C^4ISR to succesfully pit small, light, digitally enabled forces forces of 7th Marines against far larger heavy mechanized formations.

■US Army: Army Vision is part of the Army concept of IW and NCW operations toward four core operational concepts under Joint Vision 2000. These are dominant maneuver, precision engagement, focused logistics and full dimensional protection, linked to two universal enablers: information superiority and technological superiority. These will be linked to a system of systems concept toward facilitation of C^4ISR modernization toward the fielding of the Force XXI Battle Command Brigade and Below ($FBCB^2$) and the First Digitized Corps by 2004. $FBCB^2$ will provide near real-time situational awareness to individual weapons, tactical vehicles and tactical operations centers (TOCs), generating position location reports and distributing these via the tactical Internet to friendly forces in the battlespace. This will leverage IO resources to provide individual land warriors with a collective picture of the battlespace, answering key questions such as "Where am I?" "Where are my buddies?" and "Where is the enemy?"

ILLUSTRATIONS: IMAGES AND GRAPHICS

Ultralog chart. Source: DARPA





Network Centric Operations Diagram. Source: USN

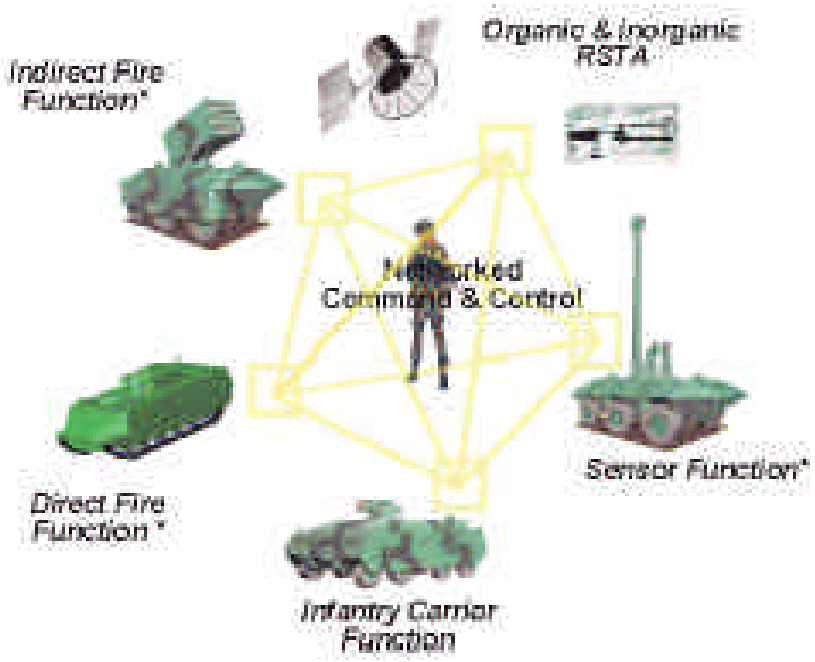


Figure C-1. Networked Command & Control

Networked Command and Control. Sourc: US Army

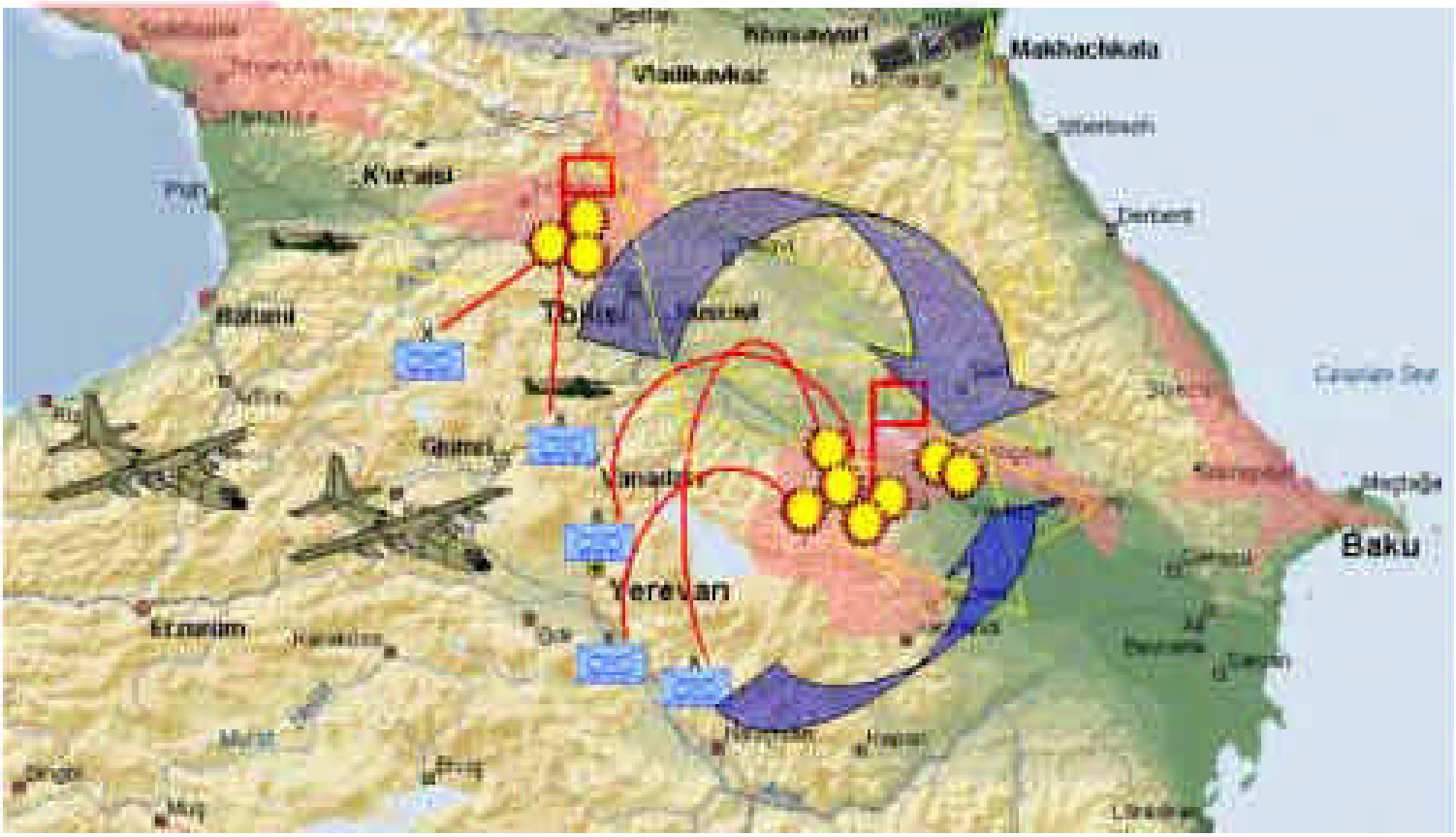
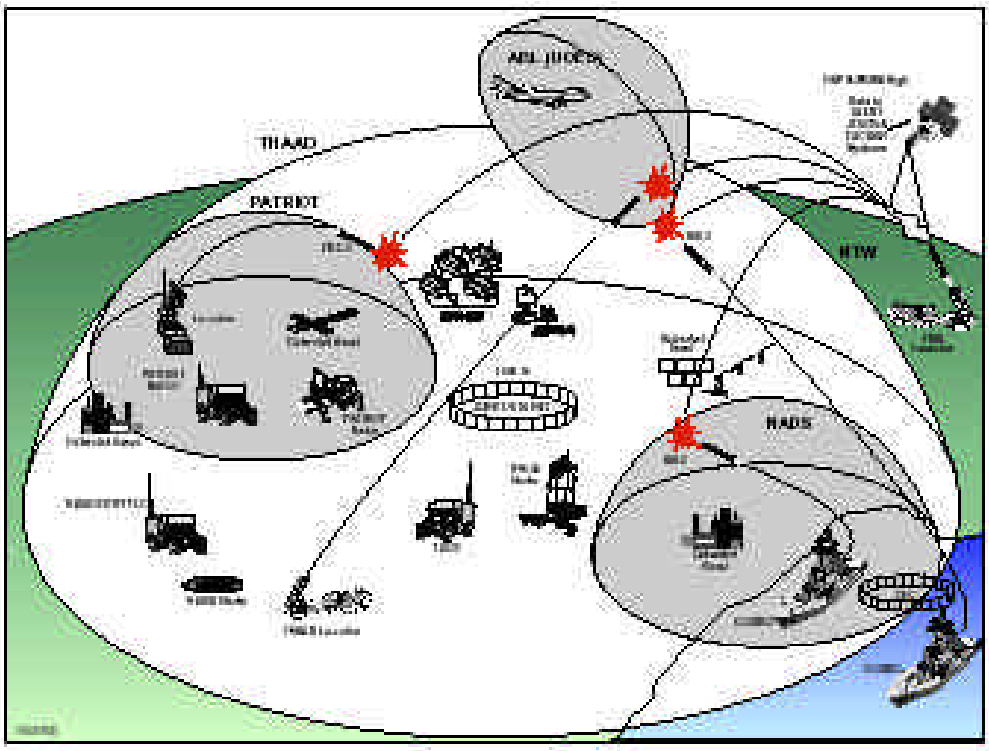
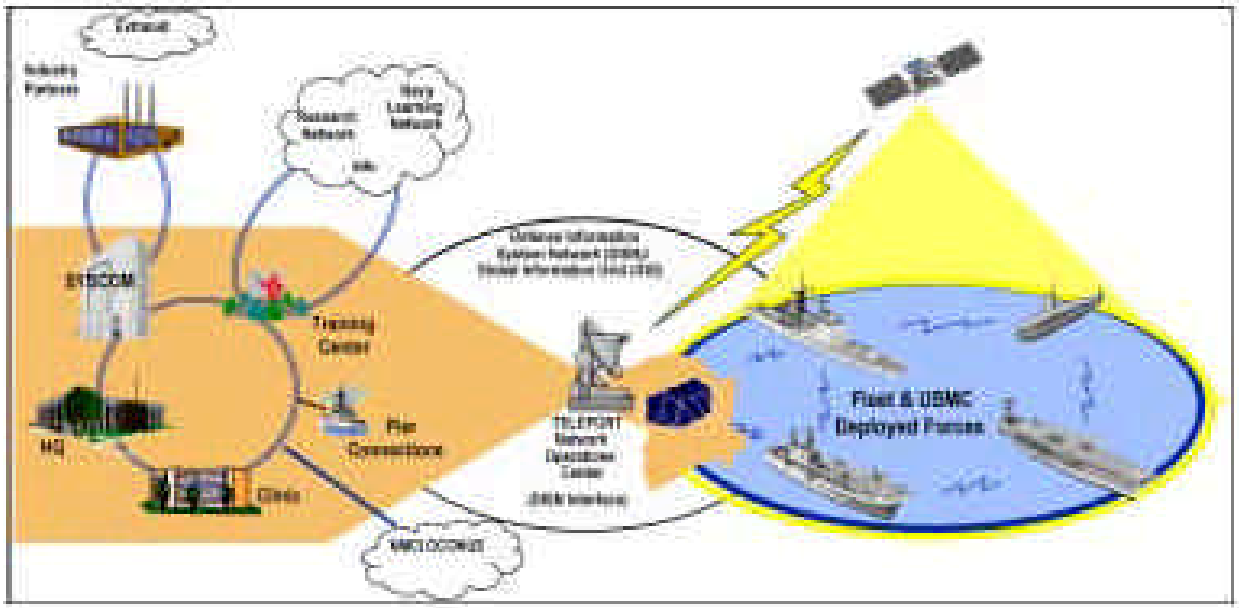


Figure C-2. Hypothetical Incident Using C4ISR

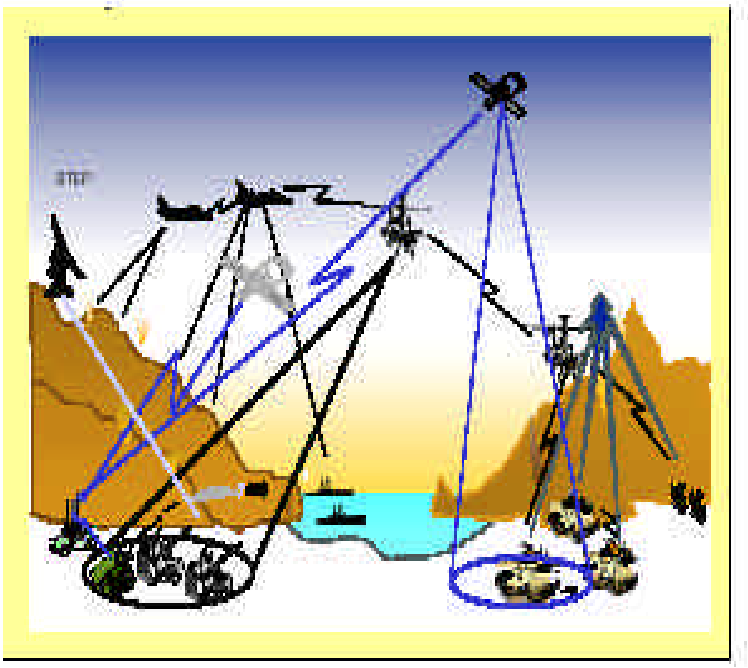
Hypothetical Incident Using C^4ISR. Source: DOD



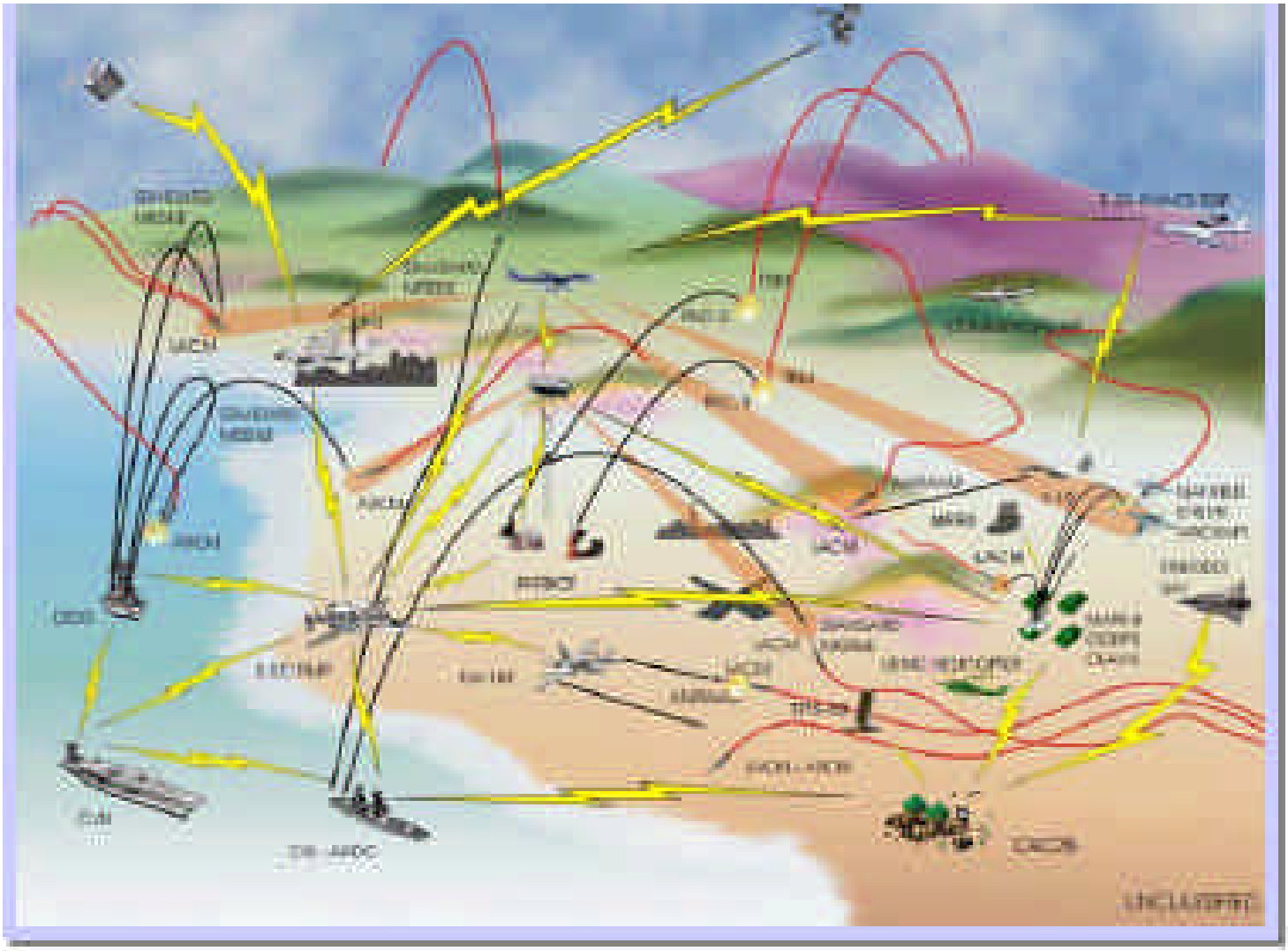
Network centric theater deployment Source: DOD



USN vision of information network during exercise. Source: USN



The US Army's vision for C^4ISR will digitize and link the battlespace. Source: DOD



A representation of the USN's Battle Force C^2 concept