Iranian Journal Examines Electronic Warfare

Unclassified

Document ID: FTS19990202001199

Version Number: 01 Region: Near East/South Asia, The Americas, West Europe Sub-Region: South Asia, North America, West Europe Country: Iran, United States, Germany Topic: PROLIFERATION, TECHNOLOGY, MILITARY

Source-Date: 12/22/1998 Iranian Journal Examines Electronic Warfare LD0202172499 Tehran Saff in Persian No 224 22 Dec 98-20 Jan 99 pp 27, 29

[Report taken from Nashriyeh-e Siasi Nezami (Political Military Periodical), which is not further identified: "Electronics To Determine Fate of Future Wars"]

[FBIS Translated Text]

World military theorists believe that in the 21st Century, electronics assault on the enemy's vital communications network will replace bloody battles. The US Army has already begun to prepare itself urgently for electronics warfare. Indeed, at the moment situations are being developed that will enable the military gurus to boast of victory even before a single shot is fired. Major Feruli Buned Meyer [name as published] of the German armed forces Department of Research and Training says that the wars of the 21st Century will be exercises in hitting the enemy communications and computer systems rather than hitting the enemy personnel and weapons hardware. Bernhardt Mende [name as published], chief of the Joint Staff of the German Air Force, also believes that an advanced information and technological package can inject fear in the enemy mind and deter him from ever thinking of an invasion. In the age of information technology, soldiers and tanks will no longer determine the fate of wars; rather, the last word will be spoken by highly specialized computers and their highly intelligent operators. That is the finding of the latest research by world military research institutes. At the moment very complicated and advanced information technology equipment exists which has a very high degree of efficiency in warfare. What is more, every day these pieces of equipment are further modernized. Among these we can refer to communication and information gathering satellites, pilotless planes, and the digital system. They can all be deployed to gather intelligence and send messages to combat units at the fastest imaginable pace. They enable every army to achieve wider vision, faster reaction, and stronger combat capability. Digital assaults are guided by the slogans such as "Create more nuisance for the enemy," or "Confuse the enemy."

In future wars the target is to infiltrate the enemy computer network and disable it. One way to do so is to contaminate the enemy computer system with viruses. Today, a virus will do to the enemy what conventional weapons used to do in the previous wars. In addition to virus contamination, today technologically advanced armies of the world also make expert use of jamming devices to disrupt communication satellites and equipment and to confuse or even misguide the enemy defenses on the air, on land, or at sea and occupy their attention with imaginary targets. Once you confuse the enemy communication network you can also disrupt the work of the enemy command and decisionmaking center. Even worse, today when you disable a country's military high command through disruption of communications you will, in effect, disrupt all the affairs of that country. Sidney Dean, one of the writers of the Information for Detroit, believes that computer information networks are undoubtedly among the most vulnerable parts of every industrialized country's economic and military infrastructure. In the age of information technology the enemy spies, saboteurs, terrorists, and Mafia gangs, staying at a safe distance and without putting themselves at risk, will try to assault and destroy international computer networks belonging to the multinational corporations. No public sector computer systems of any country will remain immune to such attacks. If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronics assaults, then they will disintegrate within a few years.

What is worse, in the information technology warfare there is no longer any distinction between civilians and combatants.

American military experts, having carried out hundreds of research projects and organized computerized test exercises, have come to the conclusion that the enemy forces, using computer viruses, will be able to disable computer networks of communication centers, power houses, banks, and other vital services. That way they can direct their effective attack at the heart of the American society. John Deutch, former Director of America's espionage outfit, the Central Intelligence Agency, says that the electron is a very sensitive and dangerous weapon. He says the American experts have so far identified a large number of countries that have been able to develop theoretical as well as practical expertise on the making and using of information technology as an offensive weapon. The former CIA director, giving testimony to members of the committees in the American Senate, admitted that even groups like the Lebanese Hezbollah were able to attack America's submarine information centers. Such a capability would obviously endanger that country's national security and disrupt its economy. Today the Internet is at the disposal of everybody in the world who is interested in having access to it.

Yet, it was only 20 years ago when Pentagon, which is the United States Department of Defense, developed Internet as a top secret equipment for control of nuclear wars. Now that it is accessible to everybody, the Internet has been turned into a kind of weapon for warfare managed by information technology. Indeed, the Internet is linked to all the important information centers, including 150,000 computers belonging to the US Army. So, America's enemies are able to inflict irreparable losses on the US Army through the use of the Internet. In the course of an information maneuver recently, the American information specialists, belonging to the Pentagon Defense Information Network, were able to see with their own eyes all the vulnerable areas of the US Army. During these maneuvers the offensive forces managed to infiltrate the army's computer networks in 80 percent of cases, while the US Army operators could only detect 4 percent of these intrusions. That kind of threat is very worrying for the information centers of the US Army. In an analysis of the current electronics warfare situation, the American daily, The Washington Post recently wrote that if the enemy forces succeeded in infiltrating the information network of the US Army, then the whole organization would collapse. It said in such a case that the American soldiers could not find food to eat nor could they be able to fire a single shot. As a matter of fact, the Pentagon is struck with a new fear. Washington has already spent several billion dollars on research work trying to find effective weapons and ways of safeguarding their computers against an enemy invasion. As one team continues work on finding ever newer offensive weapons, another team goes into action to find new defensive weapons against the new offensive ones.

So, the face of warfare is constantly changing, as it did during and after World War I with the invention of the tank. The invention of the tank was a major turning point in modern warfare. Very soon we may well witness that the invention of electronics introduced revolutionary changes in war technology. In June 1995, the first group of American officers trained in information warfare graduated from the National Defense Institute in Washington. Their area of expertise includes electronic warfare and attacks on the enemy computer brains and nerve centers. The crisis in Bosnia provided America with an opportunity to test its newly developed advanced electronic equipment in the field. American pilotless planes, flying over the enemy positions, were able to transmit very detailed and accurate pictures on the enemy troop formation and equipment. In some cases the faces of individual enemy soldiers could distinctly be seen. American military units stationed in Herzegovina were able for the first time to test and operate a secret Internet communication web. Through the same means they used to transmit secret information, aerial pictures, and logistics data to their command centers. [passage omitted on a brief recap of the above passages and adding that all this is only a small part of what is to come] Meanwhile, the German Army generals are anxiously watching America's efforts to equip its armed forces with ultra modern weapons.

They are uneasy about the strong possibility of the European armies, squeezed by financial shortages, being technologically dependent on America. Such dependency means that the European armies must buy their requirements in weapons from American arms manufacturers at exorbitant prices. On the other hand, there are other European military chiefs who look at various military events in Bosnia-Herzegovina in which the American units were involved and draw a different conclusion. They point out to the American infantry losses either from enemy snipers or landmines and conclude that perhaps American's overreliance on ultra modern technology is not as important as they originally imagined. In fact, a number of European military theorists believe that Europeans, because of being involved in more wars than the Americans, have accumulated valuable experiences which would come as a definite advantage.

Meanwhile, German military chiefs in Bonn bide their time, waiting to see what the future holds. In its research work the German Army's Department of Research and Training has concentrated its attention on creating a specialized military literature and to gather documents on the results of the American armed forces activities in high technology. "We must be victorious in the information warfare." This is the motto chosen by Helmut Wilman [name as published], commander of the Joint Chiefs of Staff of the German Ground Force.

Indeed, that is the motto which guides the activities of his colleagues in making plans for future electronics wars. Yet, in practice he lags behind Dennis Reimer, his American counterpart. The Commander of the Joint Chiefs Staff of the US Army can provide all the necessary wherewithal for each one of his soldiers who wants to enter the world of electronics warfare. He is in regular contact with his senior officers, making sure that they are well acquainted with computer technology. Bernhardt Mende, Commander of the Joint Chiefs of Staff of the German Air Force, admits that the mastery of communications technology is regarded as a strategic and operational point of strength. In conclusion, it must be admitted that in view of all the world military experts' timely access to information and then optimum use of the same information are among the most important factors ensuring victory in the present as well as future wars. In addition to strengthening the combat capability of their armed forces, almost all the countries in the world are also trying to develop the quality and quantity of their communications networks and satellite system at home and abroad.

Unclassified