The information war-V

Infor. Tech.
The Nation
6.12.01

Shahwar Junaid

Due to lack of knowledge and in-depth research analysts in Pakistan tend to avoid discussion of changes in the nature of the global information environment. These changes have taken place as a result of swift technological development, an increase in the interdisciplinary use of information technology as well as a revival of interest in the impact of information on power structures in modern society. Power fascinates not just politicians and academicians but the military and the financial communities as well. Both of the latter use the most modern applications of information technology in their work. Many countries have full-fledged institutions, at par with regular forces, dealing with information technology applications for various purposes, including information warfare.

In August 2001 a US Navy spy plane flew over mainland China. It was intercepted and damaged by a Chinese fighter jet. Thereafter it was forced to land on Chinese territory and detained there. Initially the Pentagon defended the flight of the aircraft over China as a routine surveillance. Later military officials revealed that the aircraft, fitted with sophisticated data recording devices, was on a mission that went beyond surveillance and could be said to be in the realm of information warfare. Aircraft such as the USN EP-3 can get closer to intelligence targets than satellite or land station equipment can. Thereby they position themselves in "antenna alleys"or the so-called side lobes of the communication systems of adversaries, areas where microwave and other signals traverse the air and might be intercepted. This is why even domestic aircraft and helicopters are not allowed to circle over government buildings. The airspace over parts of many US cities was closed after September 11, 2001.

Information warfare is no longer simple use and manipulation of media content aimed at psychological control of populations, or even the mere hacking of computer and communication systems to gain information about opponents. At this time information warfare involves the systematic use of several types of technology and a number of disciplines. The pooling of information from a variety of sources is expected to allow a country, such as the United States or Britain, or a security organization, to out-think an enemy. In full spectrum information operations a combination of psychological, electronic and covert warfare techniques are closely coordinated with general military strategy using traditional and modern military weapons, international diplomacy and public information activities. Action plans are based on analyses of data collected.

In simple language, the analysis and subsequent manipulation of data should allow a country, such as the United States or Britain, or a security organization such as NATO, to map out what the enemy, whosoever that might be, is thinking and take steps to neutralize the enemy's plans and ability to execute plans before action can take place. This may be done by delivering information designed to push the enemy to take certain, predetermined courses of action that would make the enemy's elimination, or neutralization, easier. For instance, the threat of the use of limited nuclear strikes in Afghanistan was expected to terrify the population and fighting forces fleeing strongholds where defences had been built. Similarly, the threat of the use of suffocation bombs in the mountains and subterranean hideouts was also an attempt to create panic and trick fighters into leaving familiar ground.

– The threat of the use of limited nuclear strikes in Afghanistan was expected to terrify the population and fighting forces into fleeing strongholds where defences had been built. Similarly, the threat of the use of suffocation bombs in the mountains and subterranean hideouts was also an attempt to create panic and trick fighters into leaving familiar ground.

– As we acquire knowledge of the tools of state policy that are used to control populations questions arise about the need for international standards and the regulation of Information Warfare as a tool of aggression.

The US Department of Defence describes this "neutralization through diversion" phase of information warfare as the process of compelling an adversary to take a particular course of action voluntarily, by providing incorrect or misleading information, rather than imposing a direct, physical (military) defeat. In the case of Afghanistan the use of such tactics (threat of nuclear strikes and suffocation bombs) did not take into account the fact that devastated populations in such terribly underdeveloped areas simply cannot imagine a more terrible fate than the one they are already facing as a result of cold, hunger and war and their most committed fighters cannot imagine a fate worse than surrender. This means that despite the best efforts of information strategists and the enormous amount of data available to them, there remains a wide gap between their understanding of the situation and the understanding of the same situation by their adversaries.

Disinformation, one of the tools of information warfare, is supposed to be created and made available after an analysis of the adversary's thought processes, based on the data collected. There are dry runs of such techniques during peacetime. Such dry runs and experiments are supposed to help in the preparation of methodology for use during times of war and crisis. To illustrate the point let us use a simple experimental model based on everyday life: an article in a generally well-regarded glossy magazine may, for instance, discuss the importance of taking mineral and other food supplements. This may be done without mentioning that in some cases a number of mineral and food supplements (such as iron, or iodine) can cause a fatality when ingested even in relatively small quantities. For instance, iodine can lead to heart failure in persons who get enough through their daily diet or happen to be allergic to the substance. Both publishers and advertisers collect information about thought and behaviour patterns, and consumption habits, of the targets of such experiments through innocuous reader surveys. Supplies of the food supplements mentioned in editorial columns are placed in stores frequented by them as a part of general marketing strategy. Target individuals, known to be readers of a particular magazine and its health columns, keen on food supplements etc, may be expected to purchase the stuff voluntarily and poison themselves. In order to complete such operations logistic support as well as research, data and data analysis is necessary, along with a fair amount of patience. Depending on the objective of such dry runs, different types of data are needed.

Acquisition of correct data is a primary and key building block of information warfare. The use of computer technology has created enormous amounts of electronic data on human activity and the activities of organizations in the form of signals, including voice communications and radar signals. It is believed that at this time the United States is the only country with the technology and expertise to analyze and collate the enormous amounts of data being collected by security organizations with global outreach. Maps of different types of signal networks covering different types of activity are created: as modern computer networks process data there is a dial tone of protocols (design/system) and link-ups that determine the paths and speeds of the transmission. These protocols are identifiable. Modern information warfare depends on acquiring data gathered through monitoring of a series of such key signals through data code breaker computer programmes. One of these is called "Proforma". Since this particular programme was identified on the US Navy's ill-fated spy plane in April 2001 it has probably been replaced or redesigned.

The principle on which such programmes work is simple and the objective is clear. The objective is to gain access to key protocols thereby acquiring the ability to manipulate, deceive and disable the sophisticated computers that are now used for military, intelligence gathering and surveillance operations. Since one machine and software programme is used against another machine and its software programme this is called machine-to-machine warfare — one side analysis software and manipulates data in order to penetrate the adversary's central command and control systems. The end purpose is to gain access to strategic information and plans in order to have the capacity to alter them without being detected. The intensity of struggles for control of global power systems has thrust questions of ethics and morality in information warfare into the background. Information like everything else is being brutalized and brutally used. As we acquire knowledge of the tools of state policy that are used to control populations questions arise about the need for international standards and the regulation of Information Warfare as a tool of aggression.

(concluded)

E-mail queries and comments to: shahwar@nation.com.pk