INTERNET - A WEAPON OF WAR ?

The rapid expansion of Information Technology has created an environment where information is readily available and anyone interested can access sit. Today anyone with a computer and modem with the help of a telephone connection can acquire, process and transmit vast amount of information to nearly everywhere. Local Area Networks linking two or more computers at one time are rapidly expanding into Wide Area Networks connecting remote areas of one country to the rest of the world. With the Internet, the globalization of information flow and exchange is a reality. Internet is now playing an increasingly important role in almost all types of activities. It has played a key role in Desert Storm, the Tiananmen Square episode, the attempted coup in Russia, the conflict in Bosnia and now is Kosovo.

What is the Internet?

Internet is an enormous global network of computers. The genesis is the US Department of Defense sponsored Advanced Research Project Agency Network (ARPANET) in 1970, an effort to connect researches from a distance via computers. Its main aim at that time during cold war was to develop a networked communication system, which would survive even a nuclear strike. This has now grown into a "network of networks"; it integrates thousands of dissimilar computer networks world wide through the use of technical standards that enable all types of systems to inter-operate. Individuals connected to the Internet using their desktop computer can perform the following: -

- Exchange electronic mail, or e-mail, with any other user at any location.
- Participate in offline (i.e., not current simultaneous) discussions via e-mail with large groups of individuals interested in particular topics, using "mailing lists" and "News Groups".
- Participate in online (i.e., real-time, or current) discussions with large groups of individuals using the "Internet Relay Chat" function.
- Log on to remote computer sites worldwide using the Telnet function.
- Download files from remote sites and users and upload files to remote sites and users via the FTP, or File Transfer Protocol function (the files can be text, graphics, sound or video).
- Read complex documents composed using "Hypertext" (clicking on a highlighted phrase on the screen takes the user into another domain, e.g., clicking on the word "Anthropology" creates a new screen or menu devoted to that subject), allowing hierarchical or "non-linear" structuring of documents.

The components of a single hypertext document can be multiple files residing in host computers anywhere on the worldwide net; a standard protocol fetches the desired component from its home location and presents it transparently to the user, who is unaware of the underlying processes.

- Read "multimedia" documents, resident at "World Wide Web" sites, consisting of text, graphics, sound and video using an intelligent front-end program such as Mosaic.

There is no central authority managing the internet. Participation is on a voluntary and cooperation basis requiring only the technical standards be followed to establish a presence in the net. Though it is difficult to get accurate figures it is estimated that a minimum of 30 million personal computers in over 100 countries are connected to Internet. Growth rate of personal computers connected to Internet in approximately one million per month and the rate of growth is more in third world countries that the West. The following actions are responsible for increase in Internet users: -

- **User friendly**. Improvements in technology, replacing arcane operating system commands understandable only by computer experts with user-friendly, icon-based, "point - and - click" interfaces, allowing non-technical individuals to become highly sophisticated users.

- **Universal access**. Proliferation of commercial Internet access providers offering online connections from virtually any location over telephone lines.

- **Lower cost**. Substantial reductions in the cost of access, making it affordable by a large segment of the population.

- **Increased benefits**. Large increases in the volume of information available over the Internet that is useful or entertaining.

- **Convenience**. The ability for any individuals to easily and inexpensively exchange e -mail with any other individual.

- **Cost-effectiveness**. Use of the Internet to realize low-cost improvements in business operations.

- **Momentum**. Increases in the size of the net-wide audience attracting additional information providers and businesses seeking markets, causing a spiraling effect.

- **Prestige**.

Current Trends

E-mail Address. One important trend is the growth in the proportion of professionals having personal e-mail addresses on the Internet. Increasingly, business cards include

not just voice and fax phone numbers, but Internet addresses. This trend is so strong that many professionals now assume that their counterparts have an Internet address to which they can send e-mail. Rather than considering an Internet address to be a luxury, not having one is coming to be viewed as a handicap, comparable to not having a fax.

Internal Use of E -Mail. The internal use of e-mail within organizations, by putting all personnel in direct contact with each other regardless of organizational rank, has tended to "flatten the pyramid," i.e., functionally change the organization to a certain extent from a hierarchical one to a horizontal one. There have been reports of this occurring even within a military organization.

Commercial online databases containing every form of information imaginable are now accessible (mostly for a fee) via the Internet.

Increasingly, authors of magazine and newspaper articles include their Internet addresses in their biodata, allowing readers to contact them directly to provide their reactions or ask for additional information.

State and local governments are establishing a presence on the Internet. Our very own Andhra Pradesh State government has already started this. State governments like MP and Tamil Nadu are not far behind.

Internet conference provides a unique medium for interpersonal communication on a massive scale.

Vulnerabilities. The threat from "hackers" and computer viruses is always present. Internet security is one of the greatest concerns of organizations using it. Malicious tampering with government computers could seriously disrupt various operations if sufficient countermeasures are not built in. A strategy called "firewalls" has been developed, whereby a second computer (a firewall) is placed between an organization's own computer and the Internet communication lines, to help control access and prevent "break-ins". It has recently been found that even triple firewall architecture has been successfully penetrated by hackers.

With respect to viruses, there is a kind of arms race spiral, whereby anti-virus software writers improve their software to protect against a newly discovered type of virus. The virus writers respond by creating a new virus that can circumvent that new protection, and so on.

Internet, International politics and conflicts

The Internet will play an increasingly significant role in international conflict. Political discussions among the members of the online public at large, and real world activities of national leaders, representatives of electronic political parties and interest groups world bodies such as the UN, commercial enterprises, and individual political activists, will be energized by the Internet. Current information about conflicts placed on

the Internet in real time by on-the-scene observers and alternative news sources will be voraciously devoured by the world audience and will have an immediate and tangible impact on the course of events. Video footage of military operations will be captured by inexpensive, hand-held digital video cameras operated by local individuals; transformed and edited into data files and then uploaded into the global information flow, reaching millions of people in a matter of minutes. Public opinion and calls for action (or calls to terminate actions) may be formed before national leaders have a chance to develop positions or to react to developments. These factors will greatly add to the burden on military commanders, whose actions will be subjected to an unprecedented degree of scrutiny.

Internet has already played important roles in recent and ongoing conflicts. Some of the examples are: -

During the siege of Sarajevo, the war-torn citizens of that city were prisoners in their own homes. They risked their lives just to buy food or find fuel to heat their apartments. They also were isolated; phone calls didn't go through; letters went undelivered. But a lucky few found another way to send messages to their families and friends. With one computer and a single phone line, more than 150 people were able to send electronic mail out of Sarajevo in one three-month period.

- During the coup in Moscow, the information posted to the Internet was used by Voice of America and CNN and indirectly by some other Western broadcasters and newspapers.

- IRC (Internet Relay Chat) stepped into the limelight in early 1991, due to the Persian Gulf war. During the bombing of Iraq, hundreds of users from all over the world gathered on a single channel for live reports from users logged in form the Middle East.

- Kat's bulletins, which he calls 'Zagreb diary,' don't appear in Yugoslav papers or on television. They exist in cyberspace. Kat types them on his own computer in Zagreb and send them by modem to an electronic bulletin board in Germany. From there, his stories are relayed to computers around the world via the global mega-information stream called the Internet. "Electronic mail is the only link between me and the outside world' `says Kat, writing by e-mail. The Croatian government owns all the major media in the country and is prosecuting a group of journalists for treason.

- In Latin America, the Internet has actually been used by national governments as a tool of statecraft. In the battle over the Ecuadorian border, both Ecuador and Peru have been launching verbal missiles at each other via the World Wide Web.

KOSOVO : FIRST INTERNET OR CYBER WAR?

Most major 20th century wars had their own media for that particular time.... Film in World War II, television in Vietnam, live TV in Gulf war. But the war over Kosovo is the first armed conflict in which all sides have an active presence on the Internet. Kosovo conflict is being labeled as the first Internet or Web War 1 or First Cyber war.

Web surfers who want to know more about the conflict can access information that is available on the net, from daily human rights updates from Macedonian to official Yugoslav proclamations. The Internet offers access to an uncensored Serbia point of view, whether official or individual. The Serbian case is very well represented on the Internet, so is the alliances view. Every day NATO is releasing spy satellite imaging that shows what they hit and the humanitarian situation in Kosovo. The Internet is the primary distribution channel for this. Both sides are locked in a fierce information war. On TV, radio and across the Internet the information battle goes on. Clinton compared Milosevic's crusade to rid Kosovo of ethnic Albanians to the holocaust and focussed on the plight of 7,50,000 Kosovo Albanians forced from the Serb province. Milosevic's supporters posted photos on their heavily used Belgrade based Internet sites showing sorrowful children and a severed head.

So far, Slobodan Milosevic seems to be winning. Vast majority of war coverage that is getting into Serbia is not believed. Col C Kenneth Allard, an information warfare expert says that NATO's indoctrination effort is "the most remarkably bad performance that I have ever witnessed".

Both sides claim that the other is distorting the truth with lies and propaganda. But NATO has gone further by treating Yugoslav radio and television as a military target for inciting ethnic cleansing. Radio- TV studio of Serbia was destroyed by NATO cruise missiles. Belgrade's Mayor stated ," For the first time in world history, the media war is fought with bombs." NATO and Pentagon responded by saying that Radio - TV Serbia had blood on its hands. However, what haven't weakened yet are the Internet voices of Yugoslavia, including the Yugoslav army.

US side relies on programming by Voice of America and Radio Free Europe/Radio Liberty, augmented by broadcasts from EC-130 "Commando Solo" planes. These flying radio stations transmit one- hour program four times daily of Wire - service news and NATO messages, interspersed with European pop music. But a pentagon official admits that their 10,000-watt signal is so weak " they are blanketing an area the size of my desk." NATO aircraft also have dropped 19 Million leaflets And because the plane stay outside Yugoslav air space, crews must calculate, altitude, wind direction and target distance, then hope the leaflets float to their destination.

Though hacking is theoretically forbidden, unclassified computer systems at NATO headquarters, the US Information Agency and US Navy facilities have been disrupted by barrage of e-mails (spanning) or computer generated pulses (pinging). However, John Hamre, Deputy Secretary of Defense, the number two civilian of US Department of Defense described that the conflict with Yugoslavia as "The first cyber war we are fighting" and described the cyber attacks on NATO as "Very incoherent and

amateurish". He said that the attacks were most likely Yugoslav sponsored but probably not conducted by the Serb controlled government but "messed up the NATO home page. It is all directly tied to the War."

The Internet's strongest effect on Kosovo may be as a sort of "net" that surrounds the conflict, informing it and keeping other media in check. It may not shape the war but the web has personalized Kosovo, documented it and prevented outright censorship.

Internet and Psy Ops

Internet can be used effectively in an offensive manner as an additional media in psychological operation campaign and help achieve unconventional warfare objectives. In Haiti pentagon has already used Internet as a part of sophisticated psychological operations campaign against Haitis military regime to restore deposed President Jean-Bertradant Aristide. Before US intervention CIA had sent ominous e-mail messages to some members of Haitis small exclusive ruling elite who had personal computers. However, sceptics say that psy ops succeeded in Haiti because of presence of 20,000 US soldiers to back up the message.

Indian Context

The terrorists and their sympathizes have been active on the web for a long time. PC Dogra ,Director General of Police, Punjab states, "Khalistan Terrorist organisations are making extensive use of Web sites: Our guess is that over 300 such sites are working to propagate the Khalistan ideology."

Virulent anti Indian propaganda has been unleashed in large number of J&K related websites by our adversaries. Though typically reactive and late, Indian Army launched its Internet site in August 98 WWW. ArmyinKashmir.Com to give the latest to the world on the happenings in Kashmir and on a daily basis brings in transparency to the operations by the security forces. Within two months hackers broke in and took over the Army's web site on J&K and filled it up with virulent anti-Indian propaganda. The hackers managed to change the parameters of the site and visitors were diverted to a different site. However, it was rectified and necessary locking systems were incorporated to eliminate the chances of recurrence of such mischief.

It is believed sympathisers of ULFA have also launched web sites to augment their cause. It is reported that they have started putting the orbat of the field formation of the Corps zone as per their knowledge.

Whether we like it or not the threat is upon us. We have to take suitable actions to turn the availability of Internet to our advantage and be proactive rather than reactive.

Launching of Army website on Kashmir was a welcome step in the right direction. Putting up other websites may be on the anvil. However, certain security measures have to be undertaken so that we don't go overboard on this issue and learn from mistakes committed by others. Some of the aspects are: -

- Hacking and Cyber attacks would definitely take place. The case of a group of teenaged hackers "Save Core" gaining total control over six of the eight servers of the computer system at the Bhaba Atomic Research Centre (BARC) on the barc - ernet in. domain is a case worth taken note of.

- Critical information is made available to the adversaries unwittingly. Real time satellite picture of different spots on the globe, real time weather data being shown on the weather channel are some the examples. US Deputy Secretary of Defense John Hamre said,"You have an order of battle available on the Internet". No wonder hundreds of military websites of US armed forces went off line beginning 28 Sep 98 so that military webmasters could remove sensitive information including plan for military operation, movements of units and personal data such as social security numbers, phone numbers, names and address of service members and their families. In our over exuberance information put on the web should not compromise security.

- Have firewalls.

- Arrange to have real time information on intrusion and detection. Have some sort of Computer Emergency Response Team.

- Information security should be enhanced greatly as well as enforcement of policies. Policies need to be developed immediately for the use of Internet, establishing Home pages and creating firewalls.

CONCLUSION

Internet has arrived. Sooner than later it would start affecting all aspects of our lives. We should make use of the wonderful opportunities presented by Internet and make maximum out of it. We must train our manpower, develop expertise on security measures, finalize the security policies and then implement it ruthlessly so that there are less chances of getting caught napping in future.

BIBLIOGRAPHY

1. Stategic Assessment : The Internet prepared by Mr Charles Swett, Office of the Assistant secretary of Defense for Special Operation and Low Intensity conflict (policy planning), Pentagon, 17 Jul 1995.

2. C Kennth Allard, Information Operation in Bosnia: A Preliminary assessment, Institute of National Strategic Studies, National Defese University, strategic Forum91, November 1996.

3. April Lyren, Kosovo Being Called first Internet War, Sun Fransisco Chronicle, Page A12, 15 Apr 99.

4. Michael Satchell, Captain Dragan's Serbian Cyber Corps, US News and World Report, 10 May 99.

5. Hamre, Balkans Fighting Called "First Cyber War" Army Times 23 Apr 99.

6. Gopal Ratnam, Army Web Sites First To Shut Off, Army Times 10 Dec 98.

7. Vijaya Pushkarna, War of Words, The New Khalisthanis. The Week, 02 Aug 98.

8. Hackers Hijack Army Websites on Kashmir, Newspaper Report on The Hindu, 16 Oct 98.

9. Hackers on the Prowl, Editorial in The Hindu, 09 Jun 98.

Published in Trishul March 1999.