The New Stealth Weapon

B Raman

The plight of Iraq during and after the Gulf War has highlighted dramatically the vulnerabilities of nations that are dependent on imported telecommunication and information systems (IS), if they do not have adequate knowledge of how such systems and technologies could be disrupted by the suppliers and other external elements and if they do not protect themselves against such disruptions.

Writing in his book "Protection and Security on the Information Superhighway", Dr. Frederick B Cohen, a leading US expert on computer security, says: "Operation Desert Storm was an object lesson in the critical importance of information in warfare, in that it demonstrated the ability of the US to obtain and use information effectively while preventing Iraq from obtaining and using comparable information. But it was also a lesson in what happens to a country that only moderately depends on information when that information is taken away. The vast majority of the destruction in Iraq was to systems that provided the communications required for command and control of forces. The effect was the utter destruction of the Iraqi economy.... The world has seen the effect of removing the information infrastructure from a country that was only marginally dependent on it, and the effect was devastating. But what about the effect on a nation that is highly dependent on its information infrastructure?"

The power or the ability to remove vital information away from an adversary through disruption or destruction of his information infrastructure has placed in the hands of nations and individuals a new stealth weapon of mass destruction (SWMD), a weapon which destroys not individuals and property, but accumulated knowledge without which one cannot function in this information age and fight and win a war or deal with terrorists, drug smugglers and other criminals gifted in the techniques of disruption.

In an article titled "High Level of Anxiety over Security Measures" (April 3, 1996), the *Financial Times* of London has pointed out that the possible use of the computer virus as a military weapon has left the pages of science fiction and entered the pages of military tactics.

Mr. B Raman is the Director, Institute of Topical Studies, Madras, and a former Additional Secretary, Government of India.

Journal of the United Service Institution of India, Vol CXXVI, No. 524, April-June 1996.

Industrialists and businessmen as well as national security agencies of Governments have been increasingly concerned over the threats posed to their information systems by hackers and viruses. According to a Pentagon study, there are 2,000 known computer viruses. Industrialists and businessmen are concerned over the increasing losses in the US due to viruses which went up from US $ 1.4 billion in 1993 to US $ 2.7 billion in 1994, according to a study of the US National Computer Security Association.

And, national security agencies of Governments are worried over threats to national security not only from the ability of adversary nations to steal, distort and destroy stored information, but also from that of individual hackers to do so.

An oft-quoted example is that of a 16-year-old British hacker who managed to break into the IS of the Air Development Centre at Griffith Air Force Base in Rome, New York, through the Internet, collect stored data regarding North Korea's nuclear and missile capabilities and widely disseminate it over the Net. It was reported that his success led to the compromising of over one million passwords used by the US Government, which had to be changed creating temporary disruptions in US networks in East Asia. If an intelligent and determined amateur can do this, what damage can be caused by a trained and well-equipped governmental agency to the IS of adversary nations?

Unfortunately, while information technology has made tremendous strides in the Asia-Pacific region, with India in the forefront in the field of software, knowledge of IS security measures and the creation of the necessary protective expertise and infrastructure are still in the primitive stage. In India, we do not even have a deterrent law to deal with computer crimes. Such laws are essential ingredients of any protective infrastructure and have been in the statute books of western nations for nearly two decades now.

After the Gulf War, a number of countries have taken seriously the need to protect their information infrastructures from externally-induced disruptions. Important amongst them are Russia and China which have set up special research and development centres for the development of new hardware architectures that can provide enhanced protection. Countires such as Australia and Germany have also been encouraging non-governmental R & D in protective architecture. The Queensland University of Technology has special projects for the design of high-integrity networks capable of withstanding malicious distruption and for developing cryptography integrity techniques. The University of Hamburg in Germany has been concentrating on perfecting techniques to counter computer viruses.

A concern that the presently-available software and techniques are not totally effective against viruses was the underlying theme of a report titled "A False Sense of Security" prepared by two officers of the US Air Force Institute of Technology to which the *Financial Times* of April 3, 1996, has drawn attention.

They say: "It is difficult for anti-virus products to keep up with the proliferation of new virus programmes. Some accepted methods for assessing the effectiveness of virus blocking systems are seriously flawed. In some cases, products labelled as 95 per cent effective are only 60 per cent effective, leading to a misplaced sense of security by making blanket effectiveness claims in the absence of scientific data to support the claim."

Malicious software are not the only means of causing disruptions of IS. Other techniques are also increasingly available ranging from the classic disruption of power supply to networks on the one side to the use of electromagnetic pulses to destroy information processing equipment on the other.

Computer-Related Cryptography

Breaches of IS security are generally difficult without the complicity of an insider, either for stealing information or for destorting or destroying it through the infiltration of malicious software. Of course, many hackers have succeeded in breaking into systems on their own without any inside help, but such instances are less in number as compared to those involving insiders.

According to a recent study in the UK (*The Times* of March 24, 1996), 60 per cent of reported IS breaches were facilitated by insiders, through negligence or complicity. The annual industrial and business losses world-wide due to computer crime, now estimated at Pound Sterling 9 billion, is expected to rise exponentially by the year 2000, if security measures are not tightened up.

The concept of IS security and the definition of an insider have undergone a tremendous change in recent years. Till the late 1970s, computer security meant protection of a mainframe computer and of the premises within which it was kept and control of access to it. An insider was either someone in the office who had access to it or an employee of the firm responsible for its servicing and maintenance.

With the emergence of Large Area Networks (LANs) with a wide geographic spread, breaches could occur at any of the connected points and an insider posing a threat could be located at any of those points. The concept was, therefore, expanded to cover not only the physical protection of the network and access control at various points, but also techniques for safeguarding the data itself so that if someone, despite the physical security measures, manages to have access to the network, he may still not be able to read, distort or erase the data or to carry out other operations.

Thus, an important objective of IS security now is to ensure the confidentiality and integrity of the information itself. Confidentiality means enabling only authorised persons to read the data for any purpose and integrity means protection of the data against wilful distortion or erasure. Integrity also covers techniques (e.g. digital signature) by which a recipient of data or other communication can satisfy himself that it has really originated from where it claims to be coming and that it has not undergone any wilful distortion during transmission.

This new objective led to the birth of computer-related cryptography—the art of coding and decoding--whether hardware or software based. Till the 1960s, cryptography was treated as a highly sensitive and restricted field of study and application, the knowledge of which was to be kept confined to sensitive Government departments in the interest of national security. With the integration of encryption technologies into IS and the growing dependence of the business world on computer networks; cryptography has now entered the market-place.

Encryption technologies now have increasing commercial applications such as for electronic banking transactions, E-Mail, for sensitive communications between US multinationals' headquarters and their branches in other countries etc. With the priority now being given by intelligence agencies to commercial and industrial espionage, there is likely to be a growing demand for commercial cryptography.

How to facilitate the availability of encryption technologies for such commercial purposes while restricting the export of more sophisticated versions suitable for defence and national security related purposes is a question which has been under examination in the US for some time now.

As Dr. Frederick Cohen observes: "The dilemma of cryptography has haunted Governments throughout history. The people in Governments want their cryptography to be very strong in order to keep their secrets secret, but they also want everyone else's cryptography to be very weak so that they can read everyone else's secrets."

Thus, despite the easing of export controls on super computers by the US, India would still face difficulty in procuring high-grade encryption technologies for sensitive departments like its nuclear and space establishments, the armed forces, the intelligence agencies etc. Any technology which the US might eventually be prepared to share is bound to be medium or low grade which its intelligence agencies are confident of breaking into for reading, distorting or erasing vital data.

In a sensitive field like computer-related cryptography, any dependence on foreign technologies would be risky for national security and we would be exposing ourselves to risks of externally-induced distortions or loss of data. In times of war, we would find ourselves reduced to the plight of Iraq.

Role of Intelligence

What has been discussed so far is the defensive aspect of information warfare. Equally important is the offensive aspect, that is, developing a capability to penetrate and disrupt the IS of our adversaries, whether nations or extremist groups or individuals. Our ability to develop such a capability would depend upon a flow of concrete information from our intelligence agencies regarding the IS of our adversaries, their weak and strong points. In fact, our intelligence agencies have an important role to play in collecting intelligence having a bearing on the defensive as well as offensive aspects.

Unfortunately, this is a field to which the required attention has not been given by our intelligence agencies, whose thinking and operational concepts remain frozen in the 1970s, if not the 1960s. At the senior levels, there are very few with a technical bent of mind and with a clear understanding and appreciation of how the entire concept of national security and the role of intelligence has changed dramatically in this age of information networks.

To the late Shri Rajiv Gandhi should go the credit for realising the importance of our intelligence agencies keeping pace with the galloping strides in IT. Under his constant prodding, a beginning was made with the induction of equipment and IT experts from other departments, frequent interactions with IT professionals, training courses to make officers at various levels IT-literate etc, but there has subsequently been a loss of interest, with the generalist officers easing out technical professionals and downgrading their importance and reducing computers to word processors for typing out reports and as instruments for visual displays during presentations at conferences etc. The role of the computer as a weapon of information warfare has been totally lost sight of.

This state of affairs needs to be corrected. A comprehensive inter-departmental approach to IS security and information warfare, with the Ministry of Defence or the Army Headquarters acting as the nodal agency, is called for.