South Asia Analysis Group

Published on *South Asia Analysis Group* (http://www.southasiaanalysis.org)

PROXY WAR IN CYBER SPACE

Submitted by asiaadmin2 on Thu, 09/20/2012 - 06:35

Paper no. 150

by B.Raman

The principal threats to networked information systems (IS) arise from paralysis or destruction, clandestine data distortion or transfer and defacements.

Paralysis or destruction could be caused either by directly interfering with the IS or by indirectly disabling the source of power supply or the telecommunication system, without which networks cannot function. The war in Iraq in 1991 saw the US and the UK allegedly paralysing the networks in Baghdad by direct interference with the IS through microchip moles planted in the hardware/software supplied to Iraq during the Iran-Iraq war of the 1980s as well as by aerial strikes on the telecommunication system. During the Kosovo conflict last year, the power stations in Belgrade were paralysed by the US through the use of the graphite bombs, thereby rendering the networks non-functional.

Effective use of the graphite bombs requires precise identification of the location of the power stations. With the Nuclear-Driven Radio Frequency Warheads (NDRF), reportedly under development by the US, such identification is not necessary.

From a satellite, one can reportedly cause the explosion of the NDRF at a height of 50 to 100 KMs over a target area, creating an intense electro-magnetic field, which, it is claimed, would disrupt all command and control equipment, computer networks, power grids and telecommunication systems within a radius of about 1,000 kms, without any radiation fall-out or other collateral damage on the ground.

Data distortion is a new stealth weapon, the dangers of which have not been adequately understood by security experts, particularly in India. When data are destroyed or defaced, one immediately notices it and can manage the resulting crisis with the help of back-up systems and redundancies, consciously created at different nodal points, in the State as well as in the private sector, as in University networks for example, with the latter's co-operation.

Skilful and clandestine data distortion will often be noticed only after something has seriously gone wrong, such as a missile failing on the launch pad or going astray.

Data transfer, which involves the theft of sensitive or classified data from an IS, often remains unnoticed unless the establishment concerned has a competent computer security staff.

Data defacement is the most widely-reported, but not-so-dangerous of the possible threats to IS from internal or external elements. One notices it immediately after it has occurred and can take the necessary corrective action. In fact, defacements help one, in a way, by making one aware of the weak points in one's IS.

Governments as well as private establishments avoid admitting penetration of their IS, lest public confidence in the dependability of their systems be shaken. As such, available statistics, tabulated by groups such as "Attrition", are often incomplete. Moreover, they document mostly instances of defacements. No reliable data are available of successful instances of IS penetration, which resulted in paralysis or destruction of systems or in data transfer or distortion.

But, these statistics do give an idea of the increasing magnitude of the threats to IS security due to the activities of hackers, working either independently or at the possible instance of intelligence agencies or alienated anti-government groups, including terrorists. Hackers are the mercenaries of the new millennium and the advent of the networked IS has enabled individuals to wage a war against a State, unnoticed and often undetected till the worst has happened.

Since August 1995, there have been 7,912 reported instances of penetration for defacements, of which 5,149 or 65.08 per cent were in the US, and the remaining 2,763 or 34.92 per cent were in other countries. Amongst the US establishments whose IS was reportedly penetrated were private companies (3,303), non-governmental organisations (556), network providers (435), universities and research laboratories (376), the Navy (58), the National Aeronautic and Space Administration (50), the Army (47), the Air Force (12), the Marines (5), other military establishments (34), the Department of Energy, which controls nuclear research laboratories (8), other Government departments (231) and banks (47).

The large number of penetrations in the US could be attributed partly to the large spread of networked IS in the US, as compared to other countries, and to the better system of reporting due to the regular sensitisation of public servants and business executives about the need for prompt reporting of penetrations and about the dangers of a cover-up.

The US is believed to have the best IS security infrastructure in the world in terms of laws, trained computer security experts, protection technologies etc. The fact that, despite this, there have been so many instances of reported and often undetected (until post-event) penetration would give an idea of the seriousness of the threats which countries such as India, which are at least 10 years behind the US in developing similar computer security consciousness and protection infrastructure, face from potential cyber invaders.

In Asia, the largest number of penetrations for defacements since 1995 has been from South Korea (142), followed by Japan (63), China (59), Malaysia (46), India (37), Singapore (20) and Pakistan (17). The much smaller number in Pakistan as compared to India does not necessarily mean that IS security there is better than in India. It is more due to the fact of a much larger spread of networks in India. The more the networks, the greater the possibility of penetration.

Pakistan lags far behind India in Information Technology (IT), but Gen. Pervez Musharraf, its self-styled Chief Executive, has embarked on an ambitious programme for catching up with India. Budgetary allocations have been increased considerably to promote computer education and research and to persuade Pakistani IT experts in the West to help Pakistan in this regard.

However, there is one domain in which Pakistan seems to have taken a lead over India-- in mobilising the resources of overseas Pakistani and other Islamic IT experts and hackers in its electronic Psychological Warfare (Psywar) against India and in raising a dedicated corps of hackers, who could be used to identify weak points in the IS of Indian establishments and use them appropriately.

The potential of the World Wide Web (WWW) for Psywar purposes was realised by the Inter-Services Intelligence (ISI) long before the Indian intelligence did.

There are about 150 jehadi websites on the WWW today. They provide the following services:

* Dissemination of information regarding jehad in different countries.

* Instructions on how to become a Mujahideen, how to prepare improvised explosive devices etc.

* Database on where one could purchase arms and ammunition and their prices.

* A bibliography of 266 articles on urban guerilla warfare and low-intensity conflicts.

* Anti-State propaganda.

About one-third of these web sites relate to the so-called jehad in Kashmir and are run by organisations such as the JKLF, the Harkat-ul-Mujahideen, the Lashkar-e-Toiba etc.

Groups such as Attrition periodically publish a list of the 10 most active hacker groups of the world. Two groups of Pakistani hackers, calling themselves "GforcePakistan" and "Pakistanhc" figure in this list. The first one is estimated to have caused 110 defacements all over the world since 1995 and the second 99 defacements. Their targets include not only India, but also the US to protest against the US attitude on Kashmir.

A third group calling itself the Muslim Online Syndicate (MOS) surfaced in March last, with an unverified claim of having defaced almost 600 Web sites in India and taken control of several Indian government and private computer systems, in protest against alleged Indian atrocities in Kashmir.

Mr.D. Ian Hopper, the CNN's Interactive Technology Editor, reported as follows: "Unlike the majority of Web vandals, the MOS members say they secretly take control of a server, then deface the site only when they "have no more use" for the data or the server itself."

He quoted one of the members of the group as saying as follows: "The servers we control range from harmless mail and Web services to 'heavy-duty" government servers. The data is only being archived for later use if deemed necessary."

It was suspected that the MOS managed to have access to Indian Websites and IS through Alabanza, a Pakistani-controlled American Internet Service Provider, which had reportedly a collaboration agreement with a well-known Indian dot.com company, without the latter being aware of its Pakistani connection.

There are many other Pakistani and Islamic hacker groups which have been active, with some of them giving online tutorials on how to use malicious software and hack and even providing malicious software, which can be downloaded and sent to someone whose computer one wants to damage.

These groups describe the growing number of hackers in the Pakistani Diaspora abroad as "Pakistan's greatest natural resource". The fact that they are able to indulge in such blatantly illegal activities online despite stringent Western laws against cyber crime and vandalism should be a matter of concern to Indian national security managers.

Cyber Space Security Management has already become an important component of National Security Management, Military-related Scientific Security Management and Intelligence Management all over the world. Future intrusions threatening our national security may not necessarily come from across the land frontier, or in air space or across maritime waters only, but could also come in cyber space. Intelligence operations and covert actions will be increasingly cyber based. It is important that our intelligence agencies gear themselves up to this possibility from now onwards.

It is, therefore, advisable to put in place a National Cyber Space Security Management policy to define the tasks that need attention, specify the responsibilities of the individual agencies and provide for an integrated approach and architecture.

Category:
Papers [1]

Topics:
Technology [2]

Links
[1] http://www.southasiaanalysis.org/papers
[2] http://www.southasiaanalysis.org/technology