

CYBER GOVERNANCE: **WHO WILL TAME THE SHREW!**

by: *J.R.Mahboobi*

(published in NETMAG, July-August Issue of 2001)

Since the launching of first node of Arpanet in 1969 and its transformation into Internet in 1980, this 20th-Century miracle never looked behind. Leaping forward beyond imagination, 10,000 nodes of 1989, turned into 1,000,000 hosts in 1992, and in 93,047,785 in 2000. Who knows where it'll land finally! The system built up initially to provide faster communication between multi-national researchers, has changed its facet from governmental research organisation to socio-cultural global village, and now taking off to transform into global virtual market. Though a good part of Internet or the Web is still devoted and used by scientists and educationists, the big chunk has been taken away by E-Commerce, Internet telephony, Emails etc. Then, like every other technology introduced in Past, Internet also has brought a host of problems haunting all those concerned with national security, privacy, IP rights, social decency, child protection, fighting, detecting and prosecuting crime. Innocent Netizens are falling prey to cheats, threats, money and identity losses, sexual abuses etc., and most of the victims around the World are still ignorant of their rights on the Web and the methodology to bring a culprit to book. It is said that Web belongs to none. Hundreds of millions of computers connected through Internet Protocols using common language understandable by all the PCs, no global administration was needed until recent past. As in the physical World, all the criminal laws, police, intelligence, security, investigation, prosecution and adjudication set-ups are aimed at that small percentage of anti-social outlaws who do not respect the rights of other fellows; the rights to person, property and prestige. Entering the Virtual World, position has worsened further. In the physical World unidentified criminals are only a small portion of the bulk. Very few criminals mask to hide their identities, but in the Virtual World, using masks and hiding identities is not a crime, and usually practised by Netizens while communicating on the Net. It becomes a crime when they do so with an intent to cause injury to the addressee, and proceed in their designs. There's another problem! Most of the pre-cyberian criminals possessed average or below average IQ, but cybercriminals are people of 'good to excellent' IQ. The problem is deteriorated by the fact that cyber crime is not committed locally, but most of the time it involves a lot of countries, and victims relate to different states, having different sets of laws and procedures. An act considered crime in one state, would be tolerated in the neighboring state. Credit card and social security numbers as well identities in different colors are stolen every day, causing losses worth millions of dollars. Scams of different styles emerge daily, enticing the innocent to part with their money to get a 'big deal'. Fake auctioneers fetch

lot of money from the bidders and provide nothing. Hackers are damaging hardware and software worth hundreds of thousands of dollars in one go. Mailing worms and Trojans to bona fide netters cause them innumerable loss by damaging valuable files and documents. Unauthorised access to your PC and stealing, replacing or damaging strategic or personal information by hackers for fun sake, for money or for espionage, can hardly be tolerated. Fake traders sell goods through E-Commerce and either do not provide goods to the buyers after receiving the money, or provide substandard goods. Even, numbers of credit cards provided by the buyers to purchase some article of a few dollars, are debited by the cheats at higher rates or even these numbers are sold out to aspiring criminals. Pornsites collect money from lustful netizens from the countries where sexually explicit material is forbidden to sell or purchase, and grab their money without remorse, as they know that such users would never lodge a complaint to Police against them, apprehending their own prosecution. Then, if a victim of any such crime dares to bring the matter to Police, then either particulars of culprits are not known, or the Police is not trained or equipped to trace the culprit, or the criminal is living beyond territorial jurisdiction of that country. So, the question arises as to whether we should wait and see how much more are ruined and victimised, or should we awake from the slumber and to take the culprit to task?

The scenario is not that gloomy! During the last decade, with the acceleration of popularity of Internet, responsible governments and voluntary organisations in many countries of the World have already commenced the task of appropriate legislation, forming websites to educate Netizens on how to use the Web, to warn about Net hazards like new viruses and scams, as well to build and strengthen Web Policing, prosecution and adjudication of cyber crime. Statutory law getting developed during the last five years is witnessing with keen interest the terminology never used before in the codified laws. A new breed of jurists, legislators, police officers, prosecutors and judges is to be sown and harvested at binary speed to cope with foreseeable workload in the days ahead. ***A long honeymoon between law and technology is needed to make the cyberspace a place to live. While yielding to rights and advantages of cyberspace, one should learn to be prepared to accept his obligations as well.***

Cyber legislation in the West has triggered a fierce debate as well. Freedom-of-speech groups are perturbed over governmental attempts to sneak into their PCs, or to intercept their mails. Equipping the Police to monitor citizens' mail on the pretext of detecting cyber terrorists or child porn traders, is considered by citizen groups as permitting the Police to enter any one's house without permission. Disclosure of 'carnivore' mobile computer detection system used by the FBI last year, caused much uproar in US. Right of privacy is also under global debate. What ought to be a fair expectancy of privacy? Courts have taken cognizance and began giving verdicts. Encryption softwares are under attack by the governmental agencies. Restrictions on export of encryption softwares were introduced to restrict spread of encrypted communications, restricting potential of law enforcing agencies to check the text in transit.

Before proceeding further to examine the need for cyber governance, I'd like to reproduce a passage from remarks of Attorney General of USA, John Ashcroft, delivered at first annual computer privacy, policy & security institute on May 22, 2001:

“Although there are no exact figures on the costs of cybercrime in America, estimates run into the billions of dollars each year. And unlike more traditional crimes, cybercrime is especially difficult to investigate.

First, the Internet can provide anonymity. On the Internet, it is easy for a criminal to create a fictitious identity to perpetrate frauds, extortions, and other crimes. Since many computer crimes – such as trading pirated software or child pornography – can be committed entirely on-line, this anonymity can significantly complicate an investigation.

Second, compounding these difficulties is the Internet's borderless nature. A criminal anywhere in the world armed with nothing more than a personal computer connected to a modem can victimize individuals and businesses worldwide.

Third, the tremendous power of today's computers makes it possible for a single cybercriminal to do a staggering amount of damage – damage far beyond what a single person could typically do in the traditional criminal world. For example, a sophisticated cybercriminal can release a virus or launch a denial of service attack affecting hundreds of thousands of computer users or critical infrastructures like power grids.”

These few lines typically depict the gravity of understanding of the problem in the West. Unfortunately, Asian countries are inviting IT revolution without compatible homework. Most of the Asian economies are not strong enough to tolerate any big loss at E-Commerce imbroglio. Even the Netizens in these countries are not provided the least care and caution while dealing with E-Commerce websites, or communicating them their credit card numbers and other personal information. In this context it is predictable that IT mania in Third World countries might cause more damage to unprepared lot, than the benefit the governments, the providers of hardware and software to these countries are acclaiming. The hard fact is, that no Netizen is prepared to live in a World without Internet. Obviously, no good government would like to deprive its citizens of an economical, useful media, causing loss even to State-run monopolies like telecommunications. Then, the only way left with us is to streamline the rules of the game, and since players are enormous, wearing different sportswear, talking different languages, expecting different levels of morality, sociology, economy and freedom, and actions are performed trans-borders at the click of a finger, it becomes inevitable to devise mutually acceptable rules for the virtual world to protect innocent surfer and to prevent and punish the cyber-criminal.

Solution looks simple, but highly difficult to implement. Even all the component states of US are not having consensus on many ethical and social issues and run different sets of laws and regulations for their respective

citizens. Then, how other independent countries would allow universal rules to adopted in their domains? Religious restrictions in many countries

would also come in the way to accept one thing, considered legitimate in the other. So far, even the institution of awarding domain names could not be globalized and many independent groups are granting domain names without any universal authorisation, or without any Treaty authorising them to collect subscriptions on such grants of domain names. Conflicts of award of domain names, while dealing with the different countries, also can not be resolved at present.

Case of ISPs is also of significant importance, as almost all the cyber traffic passes through one or the other ISP. It is obvious that an ISP has the least control over the material placed on its servers by its users. Apart from material placed on websites hosted by an ISP, a lot more material travels fast through E-mail communications, chats and internet telephony. Then, a single communication sometime uses a lot of ISPs while sending material from one continent to the other. It looks unfair to a judicial mind to deal different ISPs handling the same transaction, under different sets of laws and procedures, and expecting them to behave differently. There is consensus amongst US and Indo-Pak judiciaries that the persons similarly situated in similar circumstances, should be treated in the same manner.¹The matter of registering domain names is also a great headache. It is possible to get the same name registered with different attending agencies. It is also possible that someone get a domain name with your personal name, or with the name of your company or institution, in a hope that tomorrow you would need such a domain name, and then would be compelled to 'purchase' your own name from a stranger at a bargain price. Even, common names like loans and banks were monopolised by some people and sold out lately at handsome price. The domain name business.com was sold out for \$7.5 million, whereas Bank of America bought the domain name Loans.com for \$3 million. This field of 'business' called cybersquatting, is also calling attention of global jurists. ICANN's (Internet Corporation for Assigned Names and Numbers) Uniform Dispute Resolution Policy (UDRP) introduces a unified legal framework bringing all concerned subject to the same substantial law for dispute resolution. But if a parallel body revolts and sets up its own system, who will restrain? Also think of the case of cyberstalking, the new weapon with criminals to threat or harass the addressee by use of E-communications on internet. Question of jurisdiction will come into contact in most of the situations. Lack of extradition treaties amongst most of the nations, make it a real game for the criminals to launch their operations from 'safe havens' on the globe.

Early this year, EU Committee on Crime Problems drafted the Convention on Cyber Crime, and endeavored to cover so many aspects of the new challenge. The issue is so diverse that dozens of pages may be devoted on its various facets. It haunts the most sophisticated States and Institutions. Different States are also drafting laws to match their indigenous problems. So long the accused and the victim are residents of the same country, there is no problem, may be the ISP is located somewhere else. But if one of the

¹ Article 25 of Constitution of Pakistan. Article 14 of Indian Constitution. PLD 1957 SC(pak)9; PLD 1975 SC 506; PLD 1989 LAHORE 554; AIR 1961 SC 160.

twos is abroad, beyond the jurisdiction of the charging country, its only luck if the victim's grievance is redressed. A website offering gambling and betting while located in a Pacific Island is doing just legally, and if a resident of a Country where gambling or betting is prohibited, accesses such site and

enters into the game, who will be guilty. The host for extending access to a country where it was forbidden, or the citizen who violated the law, or both, and how they will be prosecuted. When money earned from drugs and arms trafficking, is transferred through IT channels across the continents, when such transmission was otherwise illegitimate, whether an offshore banking or financial institution receiving such money legally can be held liable and asked to return the money, and how?

The problem appears to be solved in a 3-pronged manner. Firstly, every State should immediately launch extensive education programs for the Netizens to understand security risks involved on the Net, and the ways to cope with any scam, spam or stalking, as well to understand use of encryption in personal and trade mails, cautions about security of personal information like credit card and social security numbers, and methodology to report an incident immediately to the concerned quarters. Secondly, every State should devote finance and human resources for introducing suitable IT laws for meeting domestic concerns, training for cyber-policing and prosecution, introduction of cyberlaw education at law colleges and IT institutions; and thirdly, under the auspices of UNESCO at UN, all Nations should enter into dialogue to adopt a reasonable IT Code, minimizing the threat to global community to the most, while protecting the interests of developing and under-developed Nations.

First two steps can be undertaken forthwith, whereas a global treaty may take years, for lack of mutual trust amongst World leaders and different nations, especially in the context of Infowar threats in future. Addressing before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information, in March 2000, Louis J. Freeh, Director Federal Bureau of Investigation, USA, was worried on use of IT in future wars. Let's have a piece of his fears for the future Information Warfare:

The prospect of "information warfare" by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that several foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional or "kinetic" weapons, nations see cyber attacks on our critical infrastructures or military operations as a way to hit what they perceive as America's Achilles heel – our growing dependence on information technology in government and commercial operations. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. And a Russian official has also commented that an attack on a national infrastructure could, "by virtue of

its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction."

It would also be interesting to note that US Army has already undertaken the task to thwart cyber attacks-launching massive denial-of-service assaults, feeding computer viruses or Trojans, and jamming the enemy's computer systems through electronic radio-frequency interference. Former President Clinton and Secretary of Defense William Cohen already had instructed the military to gear up to wage cyberwar. The information-warfare strategy will be detailed in a defense plan called "OPLAN 3600", that Lt. Gen. Edward Anderson, deputy commander in chief at U.S. Space Command, which was recently assigned the task of creating a cyberattack strategy, said will require "unprecedented cooperation with commercial enterprises and other organizations." There's no set deadline for completing OPLAN 3600, Anderson told Network World. But he noted that other countries, including Russia, Israel and China, are further along in building their information-warfare capabilities.

So, as I wrote earlier, the solution is simple but formidable. World has to resort to Web Governance sooner or later, but an International IT Treaty, satisfying security risks of the big and the small, might not embrace success in near future; but it would also not be a small achievement if domestic laws and education is geared up meanwhile.