Electronic Commerce and Cyber Crime

Introduction

Pakistan entered the realm of electronic commerce regulation with the promulgation of the Electronic Transactions Ordinance ("ETO"), 2002 on 11th September 2002. The primary objective of the regulation is to promote the development of e-commerce by providing a mechanism and procedure for secure on-line transactions, protect violation of privacy of information and damage to information systems and limit liability on Network Service Providers in certain situations. The Ordinance gives recognition to information in writing, to sign a document, to produce a document or to retain information or a document in electronic form subject to certain minimum criteria being satisfied. Additionally, it provides for a verification system where digital signatures can be accepted as being the equivalent to a written signature, thumbprint or identification for any means of electronic transactions.

Electronic Commerce

Now as we all know, in the real world when two parties wish to enter into a commercial relationship, there is first an intention and mutual consent of the parties, which is expressed by an offer and an acceptance and the general and agreed terms and conditions are reduced into writing in a document which is signed by the parties. A contract normally comes into existence by inscribing a signature on the agreement or by exchange of communication duly signed by two parties. With respect to handwritten signatures, Scrutton L.J. in *L'Estrange v. F. Groucob Ltd.* [1934], 2 KB 394, observed:

> ". . .When a document containing contractual terms in signed, then, in the absence of fraud, or, I will add, misrepresentation, the party signing is bound. . . ."

For technology to achieve the same level of certainty as a handwritten signature, four security risks must be ensured for the safety of electronic commerce transactions and associated data. These are:

- Privacy. E-business transactions are protected against access by attackers who seek to make copies of them or to insert fraudulent data into the process.

- Authentication. Access to e-business applications and data is restricted to those who can provide the appropriate proofs of identity.

- Integrity. E-business data and applications are protected in such a way that any effort to change them is detected and prevented.

- Non-repudiation. The flow of data through an e-business application and the flow of transactions that drive the data are logged and reported in such a way that should a dispute arise about any transaction, proof of what actually happened can be produced.[1]

[1] See http://www-106.ibm.com/developerworks/library/s-pain.html

Let's see how ETO, 2002 facilitates the development of legally recognizable cyber contracts in light of the above four security risks. Section 7 of the Ordinance provides that "affixation of signature" required under any law shall be deemed satisfied by "Electronic Signature (ES)" or "Advanced Electronic Signatures (AES)".

According to Section 2(n) an "electronic signature" means any letters, numbers, symbols, images characters or any combination thereof in electronic form, applied to, incorporated in or associated with an electronic document, with the intention of authenticating or approving the same, in order to establish the authenticity or integrity or both.

We use ES almost all the time in our daily lives. For example, typing a name under an e-mail constitutes an electronic signature. When this is done, for instance to vary or clarify terms of a written contract, such signatures can be held to be legally valid. Clicking on a box saying "Buy" or "I accept" when purchasing goods or services on an Internet web site also functions as providing an electronic signature.

Under the above definition, an ES can be any type of signature from a simple password used for authentication purpose to a PKI[2] or RSA[3] based digital signature. The definition of ES as given under ETO, 2002 falls short of addressing all the four security risks identified above. Yet, it is arguable that the definition of an "Electronic Signature" has been purposely kept loose to facilitate admissibility of electronic signatures in legal proceedings and not to restrict technological innovation.

Nevertheless, an "Advanced Electronic Signature" under Section 2(c) offers a better solution which addresses most of the issues identified above, bringing it closer to a handwritten signature in relation to paper-based data. Section 2(c) defines AES as an Electronic Signature which is either

> (i) unique to the person signing it, capable of identifying such person, created in a manner or using a means under the sole control of the person using it, and attached to the electronic document to which it relates in a manner that any subsequent change in the electronic document is detectable; or
>
> (ii) provided by an accredited certification service provider and accredited by the Certification Council as being capable of establishing authenticity and integrity of an electronic document.

Like ES, an AES is not specific to any technology and can adopt any other system provided it technically performs the desired functions.

---

[2] PKI. The term Public Key Infrastructure (PKI) refers to a global system of authentication, trust management, and privacy protection scheme where Certification Authorities act as electronic creditials issuers. Several vendors--including Check Point Software Technologies, Entrust Technologies, IBM, Netscape, Network Associates and VeriSign—offer PKI products and services for managing digital certificates across distributed enterprise networks and integrating PKI products into existing IT environments.

[3] RSA. RSA algorithm (named after its founders Ron Rivest, Adi Shamir and Leonard Adleman) has become almost synonymous with public key cryptography.

Similarly, an AES can either be provided by an accredited Certification Service Provider or any other system that is capable of unique identification and data integrity protection.

An example of an Advanced Electronic Signature which is currently in vogue is smart card technology used by a customer or an account holder for identification by banks and financial institutions.

Section 8 provides that an electronic signature may be proved in "any manner" to verify the originator and his intention. On the other hand, Section 9 of ETO, 2002 states that if an AES is affixed, unless evidence to the contrary is produced, there will be a presumption of the identity of the originator, his intention and data integrity. This means that if a dispute arises between two parties relating to the creation of a contract, it would be easier to prove the existence of a contract by way of an AES rather than an ES.

Offences under the ETO, 2002

Having distinguished ES and AES, one may then proceed to analyze the repercussions of playing foul with this technology. Sections 34 to 37 of the Ordinance cover offences connected with the administration of the Electronic Signature System.

Section 34 (a) states that providing false information to the Certificate Service Provider (CSP) is an offence punishable with seven years imprisonment and a fine of Rupees Ten Million or with both.

Section 34 (b) is significant because not informing the CSP of any changes in the information contained in an already published certificate also carries a similar penalty. While the intention behind 34 (b) is good, it severely restricts issue of Digital Certificates with value added parameters such as a physical address, Credit Standing, etc.

Section 34 (c) provides for similar punishment if a person causes or allows a certificate or his electronic signature to be used in any fraudulent or unlawful manner. This is also a dangerous provision since it can be extended to a person who compromises his password to the file containing the private key. In a country where there are shared computers and people are yet to learn how to set good passwords, such provisions may put off users from trying out electronic signatures.

Section 35 refers to the issue of a certificate containing false information and failure to revoke/suspend a certificate when required and renders the employees of the CSP liable for seven years imprisonment and payment of compensation. It places a huge burden on the Certifying Authorities to establish the identification of the applicant to an Electronic Signature Certificate. This again could be a very onerous clause for an inadvertent administrative lapse. International Certifying authorities intending to set up office in Pakistan need to properly assess the risks to their directors and employees arising out of this provision.

Electronic Certification Accreditation Council

Now the next question that arises is who will regulate e-commerce? The Pakistan legislation creates a multi member "Electronic Certification Accreditation Council," which is yet to be

established. This would be an independent body comprising of a Council of five members, with four members being drawn from the private sector. One of the members would be designated as the Chairman with a term of appointment of three years.

There are strict qualification parameters fixed for the members of the council. For example, of the five members, one shall be a telecommunication engineer with at least 7 years of experience of which one year is in the field of Cryptographic services. Two of the members shall be professionals or academics with at least 7 years of work experience in the field of Information Technology, and one shall have an administrative background with at least seven years of experience in a private or public organization. Another member shall be an advocate with at least seven years experience and adequate knowledge of laws relating to information technology and telecommunications.

Thus the constitution of the Council ensures availability of techno-legal as well as administrative experience bringing different functional experts directly in the working of the Council with a term of three years and may prove to be quite successful as and when it comes into existence.

A revenue stream for funding the Council has been provided in the form of fees of upto Rs.10/- for every certification, besides the accreditation fees or fines collected from the Certificate Service Providers. This is a good revenue source directly related to the growth in the business of Electronic Signature Certification in the Country which also gives the Council some what financial independence.

Yet another point to be observed is that the functions assigned to the Certification Council of Pakistan includes carrying out research and studies in relation to cryptography services and to obtain public opinion in connection therewith and also give advice to any person in relation to any matter covered under the Ordinance. Consequently, the Certification Council would not only regulate the electronic signature system but also could develop into an apex research and consultancy institute of cryptography and related Industry. This forethought and developmental vision in the constitution of the apex regulatory agency is one of the significant factors of the legislation which must be appreciated.

Violation of Privacy of Information and Damage to information Systems, etc.

Besides adverting to the consequence of breach of provisions of law relating to ES and EAS and its regulation, the ETO goes a little further -- it also attempts to protect computer users from certain cyber crimes such as hacking, spyware, virus and DoS attacks.

Section 36 of the ESO-2002 is interesting. It is headlined "Violation of Privacy of Information" and states

"Any person

who gains or attempts to gain access to any information system

with or without intent to acquire the information contained therein or to gain knowledge of such information,

whether or not he is aware of the nature or contents of such information,

when he is not authorised to gain access, as aforesaid,

shall be guilty of an offence under this ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees or with both."

A close observation of this section indicates that it can cover hacking, spyware activities as well as virus introduction in some cases.

Section 37 follows with the statement

Damage to Information System etc:

(1) Any person who does or attempts to do any act with intent to alter, modify, delete, move, generate, transmit, or store any information through or in any information system knowingly that he is not authorised to do any of the foregoing shall be guilty of an offence under this ordinance.

(2) Any person who does or attempts to do any act with intent to impair the operation of or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this ordinance.

(3) The offences under sub sections (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees or with both.

This section covers the classical defacement of websites, certain virus activities, DoS, etc.

All offences under ESO have been made cognizable, non-bailable and compoundable imposing the punishment of imprisonment of either description of a term not exceeding seven years or fine with may extend to one million rupees or with both.

Extra Territorial Jurisdiction

What is interesting in this respect is that the legislation for Cyber crimes follows the UNCITRAL convention and includes the concept of "Extra territorial Jurisdiction." In layman terms, this means that just as a Pakistani can be punished for a cyber crime in the United States even though he has never set foot in the U.S., a Frenchman residing in Indonesia can also be punished for a cyber crime committed in Pakistan under ETO 2002 (pun intended and with the greatest respect to those who may fall within this category and are present here). This makes it essential for all those would be hackers resident outside Pakistan (because clearly there are none present here, not in Karachi) to be conversant with the laws of Cyber Crimes in Pakistan (but in case there are any then please do take note).

Non-Accredited Certificate Service Providers

The ETO, 2002, also facilitates international e-business, as it does not restrict the right of any certificate service provider to engage in the business of providing certification services without being accredited. Section 17 of the Ordinance specifically states that "Nothing in this ordinance shall impede or in any way restrict the rights of any certificate service provider to engage in the business of providing Certification Services without being accredited." It is only expected that no person shall hold himself out as an Accredited Certification Service Provider unless he has been so licensed.

Thus, parties are free to enter into electronic/online contracts across borders where the foreign party to the contract would like to use a digital certificate issued to him by his country's certifying authority who might not be licensed in Pakistan.

The recognition of digital signatures issued by unlicensed signatures avoids the serious problems where a person is entering into cyber contracts across the borders where the foreign party to a contract would like to use a digital certificate issued to him by his country's certifying authority who might not have been licensed in his country.

Liability of Network Service Providers for Actions of Subscribers.

Another interesting element of the ETO, 2002 is the Liability of Network Service Providers for Actions of Subscribers. This is particularly interesting because whoever commits a breach of the law, will presumably do so on the backbone of an ISP or a third-party. In this respect Section 40 of ETO, 2002 states that:

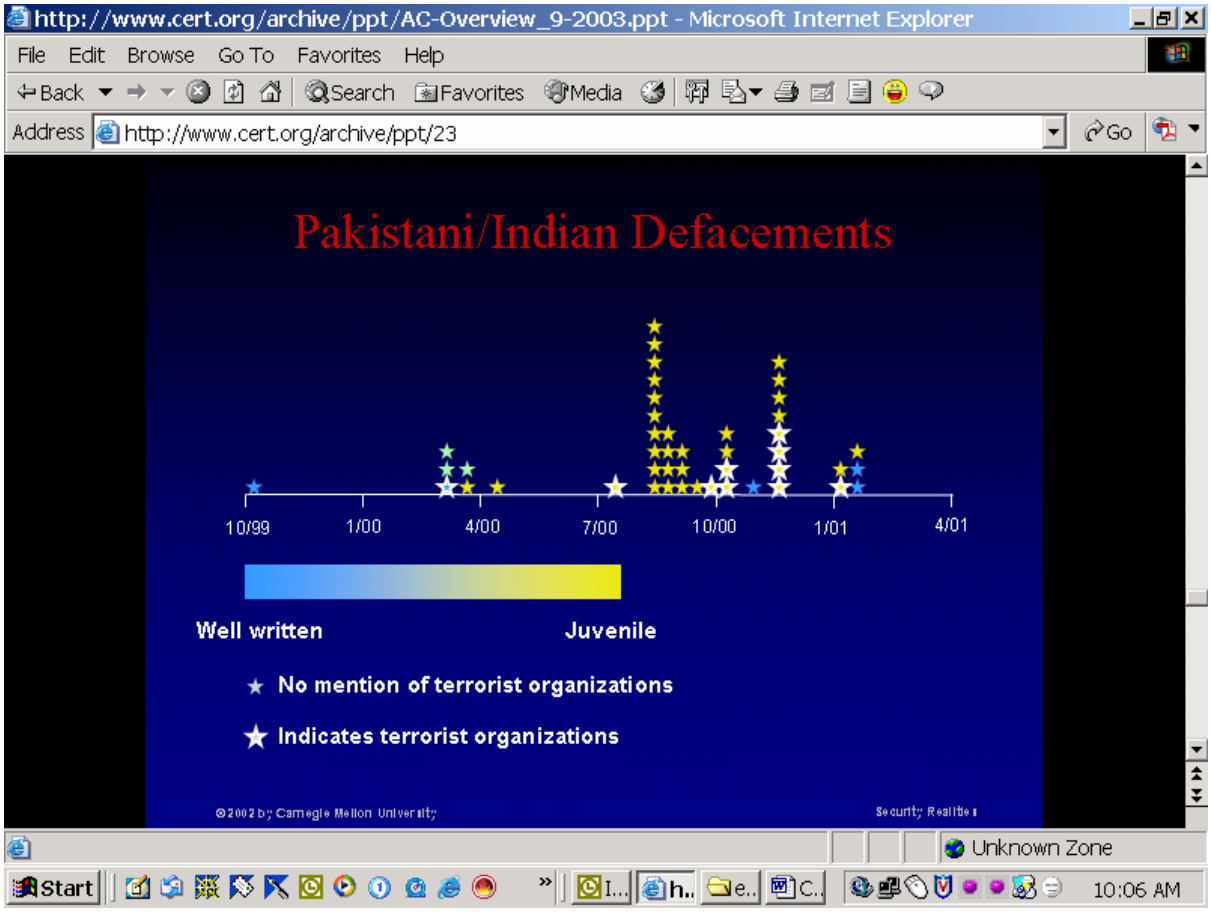
In the absence of intent to facilitate, aid or abet, a network service provider shall not be subject to any civil or criminal liability solely for the reason of use of his telecommunication system in connection with the contravention of this Ordinance by a person not subject to the direction or control of the network service provider.

Of course, Network Service Providers also normally obtain indemnification from users covering all liabilities in connection with the provision of services provided by the On-Line service provider, where such liability is alleged to have been caused by an act or omission of the user or his agent.

While the ETO 2002 is simple and covers all major cyber offences, there could be some areas such as traditional offence with cyber documents or special cyber offences such as cyber squatting, cyberjacking, where the legislation may prove inadequate. To cover this area an Electronic Crimes Bill 2004 is currently pending in Parliament.

In conclusion, the ETO 2002 is a landmark legislation and will hopefully go a long way towards facilitating the use of electronic transactions in Pakistan.

Thank you.


http://www.cert.org/archive/ppt/AC-Overview_9-2003.ppt - Microsoft Internet Explorer
File Edit Browse Go To Favorites Help
Back Search Favorites Media
Address http://www.cert.org/archive/ppt/23
Go
Pakistani/Indian Defacements
10/99
1/00
4/00
7/00
10/00
1/01
4/01
Well written
Juvenile
No mention of terrorist organizations
Indicates terrorist organizations
©2002 by Carnegie Mellon University
Unknown Zone
Start
10:06 AM

Abraham & Sarwana
Advocates, Solicitors
Tel. 568 7360, 568 7370

Jawad A. Sarwana

Daily Times - Site Edition Wednesday, December 15, 2004

Many becoming victims of Internet fraud

By Imran Akbar

ISLAMABAD: Although the Internet provides many facilities, it also carries many risks. Most common is the risk of Internet fraud. This crime affects the entire world and victims include individuals, companies and even countries.

In Pakistan, leading international and local banks have suffered huge losses from credit card fraud, despite the expensive and extensive security measures they have in place. Victims include Citibank, American Bank, Union Bank, Askari Bank, the Muslim Commercial Bank.

Cyber criminals often attack official government websites, hack into security systems, send obnoxious e-mails, damage information systems and send viruses. These days, even terrorists use the Internet to collect information on targets and build worldwide contacts and sympathisers.

It is widely accepted that there is a need to establish a policy to curb cyber crime. The government of Pakistan has established a Cyber Crime Wing, a joint venture of the Ministry of Interior, Ministry of Information Technology and Telecommunications to combat the hazard of cyber crime. The hackers manage to hack information systems, official websites and get access to unauthorised official data which is a hidden threat to the government. "Cyber Crime wing will coordinate efforts to stop increasing cyber crimes in Pakistan, the threats and the measures to counter them. It will focus on criminals communications, make fair online business, protect official websites from hackers and make solid security policy for networks and Online Official Documents," an official of Cyber Crime Wing told Daily Times.

The new wing will also regulate Internet cafés in the country as the terrorist use these café's for communication. However, very few people and officials know about the existence of this wing. Even the Islamabad police official deputed at the police exchange inquiry (9203333) expressed ignorance about the existence of this wing. "I do not know if there is a cyber crime wing working in Pakistan," said Muhammad Farooq, sub-inspector, when contacted to get the cyber crime wing's number. Given this limited police awareness, members of the public should know about common Internet scams in order to protect themselves, their money and their personal information.

The IT Ministry has also finalised a draft bill for the 'Electronic Crime Act 2004' which is an important legislation to give legal cover to the anti-cyber crime efforts.

One of the most common frauds involves distance selling. If you are going to buy something from the Internet, you should make sure that the seller provides the price of the item, arrangements for delivery, contact information so questions can be asked and the terms of cancellation. Anyone who fails to provide this basic information is probably trying to run a scam.

Another common fraud is the Nigerian Advance Fee Scam, also known internationally as the 4-1-9 fraud. The sender claims to be a government official who needs to move a large sum of money. For some reason, they need you to pay a fee and claim the money on their behalf. They say they will pay you a percentage of the total sum for your help.

They request personal and banking details from you and a 'goodwill' or 'advance fee' payment. Your information is used for illegal activities and the money you submit is never seen again.

Online auction frauds are also becoming common. These include the advance lottery fee scams, business opportunities, work from home scams and international modem dialling schemes. Another common scam invites people to claim prizes by calling a hotline number. Usually, the hotlines charge a high fee per minute and the calls last many minutes.

Some competitions invite you to claim your allocated prize by telephoning a hotline number and this could be charged at a premium rate and last many minutes. Also be cautious when offered free holidays or cheap property. You may be being invited to attend a presentation and conned into signing an agreement that forces you to pay exorbitantly high prices for 'deals'. Many of these scams do not allow you to cancel once you have signed on.

Despite general knowledge that these schemes exist, people continue to become victims. According to one website on Internet fraud, there were at least 124,509 people complained about being scammed in 2003. Many more people are often too embarrassed to report that they were scammed.

Of the reports on the website, Internet auction frauds accounted for 61 percent of the complaints, undelivered merchandise despite fee payment accounted for about 21 percent of complaints, and credit card fraud accounted for 7 percent of complaints. Check fraud, identity theft, business fraud and investment fraud were other top complaint categories.

Abraham & Sarwana
Advocates, Solicitors
Tel. 568 7360, 568 7370

Jawad A. Sarwana

Cyber Crime Wing meets today to co-ordinate efforts

By Imran Ayub (The News International, 4 October 2003)

KARACHI: Cyber Crime Wing meets in Islamabad today (Saturday) to discuss the single item agenda "co-ordinated efforts to combat cyber crime in Pakistan", sources close to the matter said.

Project Director, Federal Investigation Agency would chair the wing's meeting which would be attended by high officials of the Pakistan Telecommunications Authority and representatives of Internet service providers (ISPs) and software houses. The wing was jointly formed by the ministries of interior and telecommunications after some hackers managed to break into official websites a few months back. "We will meet to discuss one-point agenda - co-ordinated efforts to combat cyber crime in Pakistan, the threats and the measures to counter them," said an official in the ministry of IT and telecom.

He said telecom ministry had invited all the stakeholders and experts who could assist in making a campaign a success. The government a few months back formed National Response Centre (NRC) for Cyber Crime controlled by the FIA, which it said, would focus on emerging criminal threats in the wake of technology advancement.

"The centre aims to cap criminals' communications and make online business dealing a fair play," said one of the NRC members.

He said the co-ordination between the two ministries would definitely help in achieving the target. However, representatives of ISPs and software houses invited to attend the meeting said a campaign requires commitment and consistent efforts on part of government to get desired goals.

"This is not the first time that we are invited to attend such a meeting. The government did many much exercises in past also but all in vain," said an invitee to the meeting.

Meanwhile, authorities made it clear the NRC meeting had nothing to do with the Ministry of Information's Cyber Wing as it performed totally different task.

"The Cyber Wing was formed by the information ministry comprising IT professionals and experts tasked with countering virus attacks by a neighbouring country's hackers on government websites," said a telecom ministry official explaining difference between the two wings.

Indian hackers launched virus attacks on government websites earlier this year. They called themselves "Indian Snacks" and sent viruses in emails littered with anti Pakistan messages.

Members NRC said though the centre was finally formed a few months back it had remained in gestation for over a year. "The issue became a serious concern after reports that the killers of Daniel Pearl, the US journalist used cyber cafes to communicate," said a source.

He said the centre's first step is most likely to be regulating Internet cafÈs mushrooming in the country.

Abraham & Sarwana
Advocates, Solicitors
Tel. 568 7360, 568 7370

Jawad A. Sarwana

Daily Times - Site Edition Friday, July 11, 2003

FBI training FIA officers on cyber crime

KARACHI: Interior Minister Faisal Saleh Hayat said on Thursday that the US Federal Bureau of Investigation was training FIA officials in combating cyber crimes, including financial frauds.

Speaking to journalists at a seminar on Cyber Security: Challenges and Solutions, held under the auspices of the Federal Investigation Agency (FIA) and Sindh's IT department, he said besides hacking for fun and various kinds of crime, a major threat to Pakistan was cyber attacks on its official websites. He said Pakistan occupies an important position in the global security scenario and that many groups and nations opposing the country's growing image were initiating such attacks.

Referring to the Quetta massacre, the minister said a high-level inquiry was underway to investigate the incident and the involvement of a foreign hand could not be ruled out. Earlier, in his inaugural speech, Mr Hayat said the government was committed to transforming Pakistan into a modern, liberal, progressive and forward-looking state.

He said all citizens must be free to exercise their legitimate rights, as envisaged by our founding fathers.

He said Pakistan is at a crossroads of economic development and measures to combat cyber crimes must be improved. He praised the FIA and the Sindh IT department for taking up the issue before this threat became a real danger. He said while the use of the Internet was rapidly increasing in the country, people had to be made aware of its ill effects.

He said another major problem was that criminals had larger space and freedom to operate with latest technology, whereas public-sector departments lagged behind in countermeasures due to their limitations and bureaucratic channels. He stressed the need to link up with global efforts in this regard.

The director general of the FIA, Syed Mohib Asad, highlighted the importance of cyber security and asked the government and the private sector to take this issue seriously.

He said the FIA was organising such seminars in various cities of the country. He said in the next ten years only economically viable countries would survive and most trade and commerce would be managed electronically.

He stressed the highlighted for the computerisation of the security systems and said the FIA was developing an infrastructure for combating Internet crimes. The unit will be named NR3C, he said.

The Head of the national response centre for cyber crimes, NR3C, Amar Hussain Jaferi, said Internet security was needed for all users, from individual operating at home to large multinational firms and sensitive organisations.

He said a cyber threat was a serious issue since it originated from unknown places and its impact could not be assessed in the initial stage.

He said in the recent past nearly all the government sites had been under DOS attack. He informed the audience about the web site www.nr3c.gov.pk, that contains relevant information about cyber crimes and offer online training programs too.

He said efforts were being made by the FIA to create a cyber security net in the country and urged the private sector to allocate resources in this regard.

The IGP of Sindh, Syed Kamal Shah, informed the audience about the need for developing a cyber crime unit for Sindh Police and highlighted the problems faced by the department after the kidnapping of Daniel Pearl when the department was flooded with e-mails making it very difficult for the department to screen true picture of the situation.

Aftab Alam, deputy director of the Sindh IT department, Dr Asad Sheikh of Sindh University and Abid Aziz of UNISYS spoke on the occasion and discussed various solutions to problems faced in the advanced countries at the hands of hackers and Internet-based criminals.—PPI

Home | **National**

Pakistan Creates Cyber Crime Wing

Associated Press

Story location: http://www.wired.com/news/conflict/0,2100,58033,00.html

08:49 AM Mar. 13, 2003 PT

ISLAMABAD, Pakistan --A Pakistani security agency has launched a special wing to combat cyber crimes in part because the country had to rely on U.S. investigators to trace e-mails sent by the kidnappers of American journalist Daniel Pearl a year ago.

"The purpose of establishing the National Response Center for Cyber Crimes is to stop misuse of the Internet and trace those involved in cyber-related crimes," Iftikhar Ahmad, spokesman for Pakistan's Interior Ministry, told the Associated Press on Wednesday.

"The importance of this special wing was felt when Daniel Pearl was kidnapped, and his captors started sending e-mails to newspapers," he said.

The Wall Street Journal correspondent disappeared on Jan. 23, 2002, from Pakistan's southern city of Karachi.

On Jan. 27, 2002, the *Journal* and other media received an e-mail from a group calling itself the National Movement for the Restoration of Pakistani Sovereignty. The e-mail contained a photo of Pearl, 38, with a gun to his head.

The FBI traced the e-mails, and police captured those who allegedly sent them to the newspapers, but, on Feb. 21, 2002, the U.S. Embassy received a videotape showing Pearl was dead.

"The National Response Center for Cyber Crimes will play a key role in the days to come in tracing those terrorists who often use the Internet or prepaid telephone cards to communicate messages to their associates for carrying out acts of terrorism and other purposes," Ahmad said.

The special wing has been established at the headquarters of an intelligence agency in Islamabad, Pakistan's capital