Frequently Asked Questions Regarding
The E-Crimes Bill 2007

1. Does the law help my business?

   No.

   It creates an insecure environment for business generally Pakistan and a particularly hostile environment for IT and IT enabled businesses to operate, invest and conduct business in Pakistan. This will not just obstruct and discourage foreign businesses but will force many Pakistani businesses to move their operations, investments and businesses out of Pakistan.

2. Does the law protect me from cyber crimes?

   No.

   For the following reasons getting a conviction under this Law will be unlikely against Cyber criminals and Pakistan will become a safe haven for Cyber criminal to operate out of:

   - The definitions of each type of cyber crimes are incorrect both from an IT technical point of view and also from a legal point of view. They are completely different from internationally recognized definitions and are simply incorrect. (e.g. Malicious code, data damage, electronic fraud, electronic forgery, spoofing, cyber stalking, cyber terrorism are all wrong and so cannot be implemented).

   - The undefined investigation powers, lack of safeguards, violation of Fundamental Human Rights and Unconstitutional provisions of the Bill will assist the Cyber criminal.

   - These incorrect definitions will help cyber criminals in disproving charges and obstruct investigation agencies from fulfilling their duties.

   Effectively and practically the law will be useless against cyber crimes but create enormous obstructions and nuisances for IT enabled (anyone using Computers or Electronic devices) businesses and individuals.

3. Will the government be able to implement the law effectively?

   No.

   Due to the reasons given above and the complete and utter failure to provide procedural provisions and safeguards in the Law (these cannot be provided in Rules since it must be legislated) will make the job of the designated investigation agency and intelligence agencies very difficult with difficulty in also cooperating with other international agencies.

4. Does it cover cyber crimes?

   No.

   The definitions are so ridiculously not related to cyber crimes that the law will leave huge lacunas and gaps in the real cyber crimes for which a law is actually required. In fact many of the offences created in the law have nothing to do with Electronic or Cyber Crime (e.g. Holy Quran, The Prophet, Cyber Terrorism). Due to the lack of technical understanding demonstrated in the law, IT and IT enabled businesses and individuals will find that the crimes they wish to prevent and seek recourse to under this law will be very difficult if not impossible.

5. Does it represent international best practice?

   No.

   The law does not represent from anywhere adherence to either the principles or definitions of the Cyber Crime Convention (Budapest Convention 2001) and is in fact in such total violation of the law that if Pakistan ever wanted to join the Convention which will be the only effective way to Counter Cyber Crime and Cyber Terrorism that it will be impossible and Pakistan would be in violation of International Law. Various parts of the law already are in violation of United Nations Treaties and Conventions. In fact the law is even contrary to the laws available in the USA, UK and generally in the EU and other developed countries successfully dealing with Cyber crimes.

6. Does it violate the International Treaty/Convention on Cyber Crimes?

   Yes. See last answer.

7. Does it violate any other international treaty to which Pakistan is a party?

   Yes. The UN Charter and the UN 1966 United Nations International Covenant on Civil and Political Rights.

8. Does it violate the Constitution of Pakistan?

   Yes. It violates Fundamental Human Rights and Freedoms protected by Chapter I of the 1973 Constitution.

9. Who will be the implementing agency and what will be their rights and powers?

   FIA is at the moment designated for the purpose.

   They can issue their own warrants.
   There is no requirement for mandatory grounds being given for obtaining a search and seizure warrant
   - The search and seizure can take place
   - At any time
   - Any where
   - Any number of locations
   - In regards any number of Computers (whether or not they also house other businesses/people's data)
   - Copies can be made without any chain of custody
   - The Computers can be seized (even if they are vital to run a business or operation of a Bank, ISP or other establishment like a Mainframe, thus, shutting down all operations for some data being searched for on the Mainframe/Server of one customer)

   The business/person being investigated has no right to:
   - Challenge such action
   - Keep a verified copy of the data (to ensure it cannot be tampered)
   - To ensure protection of Intellectual Property
   - To ensure that the data is kept secure
   - To ensure that the Data is destroyed after the investigation/end of the case

10. What are my rights?

    None. The Law does not mention any rights whatsoever.

11. Will it help in combating terrorism?

No.

It will actually encourage Cyber Terrorism. Since the definition does not cover the actual technical and legal definition of Cyber Terrorism, all offences of what is internationally recognized to be Cyber Terrorism will remain unaffected. Pakistan will become a safe haven and choice of forum for Cyber Terrorism.

12. Will it help in combating cyber terrorism?

No.

For the reasons given above such as incorrect definitions, Unconstitutionality, conflict with the technical, legal and international definitions of cyber terrorism, the Investigating Agencies and Prosecution will be unable to prove Cyber Terrorism. Cyber Terrorists will likely be acquitted and Pakistan will become a safe haven for them.

13. Will it obstruct Pakistan to effectively cooperate with international agencies?

Yes.

International Cyber Crime agencies will find that Pakistani agencies will be unable to assist in combating cyber criminals and also find that the designated agency has no effective mechanism to cooperate. The cooperation mechanism requires existing arrangements. Obviously, in the Cyber world there will be no time for Pakistani agencies to enter into approved arrangements through summaries and approvals processes. Pakistani cooperation will be so slow that cyber crimes emanating from other countries with which Pakistan has no arrangement will ensure immunity from investigation to Cyber Criminals using foreign IT systems. Similarly, offences from Pakistan into foreign territories where Pakistan does not have a pre-existing arrangement will hamper International Agencies from effectively cooperating with Pakistani authorities since response to cyber crimes requires real time and speedy tracing and forensics.

14. What impact will it have on Pakistan's perception internationally?

Pakistan is likely to be perceived as a difficult if not impossible place to do IT business, investment and operations. It will also be seen as safe haven for Cyber Criminals, Cyber Terrorists and all kinds of International Crime.

15. What impact will have on Pakistan's economy?

On promulgation of this law, in its current form, many businesses will have to move their operations and IT enabled investments outside of Pakistan. These will not only include foreign investors but also local Pakistani IT enabled companies who will have no choice but to move operations abroad due to the enormity of the Security Risk to businesses and individuals. Hundreds of Thousands of jobs will be lost and much economic investment as well as tax revenue to the government will be affected.

16. What can I do to assist the government as a stakeholder in this process?

    Write to the Ministry, the President and Prime Minister and join the efforts spearheaded by PASHA and the Computer Society and many other concerned businesses and citizens. Visit their websites, download the material available on the law and write to them.