## 5. WEAKNESS OF CYBER LAW IN BANGLADESH:

The offences of the Bangladesh Information & Communication Technology Act 2006 are non-cognigible in nature under section 76(2). The victim has to file an allegation to the law enforcing agencies to get remedy. This is the main weakness of the said act. In the time of enactment of the said act it was said in section 68 that a special tribunal named Cyber Tribunal will be established in every district of Bangladesh. But till now only a tribunal has established in Dhaka City.

Because of the dependency of technology specialist and well trained lawyer and judges the disposal of Cyber cases are rare. To remove such kind of pendency of cases judges, lawyer and specialist should be well trained.

The Bangladesh police have a special branch named "Anti-cyber Crime Department" headed by the Deputy Commissioner of Police to protect e-mail fraud, treat by e-mail, defamation or publishing of unauthorized pictures. But the department is yet to fulfill the public demand due to the scarcity of well trained man power. A case cannot be started due to the non visibility of the plaintiff. There is no scope for the state to take liabilities as being a plaintiff.

The Cyber Tribunal has not yet reward any punishment to any criminal. Due to this the criminals are insisting to occur crimes thinking that they will not be punished. This is one of the main weaknesses of the implementation of the Bangladesh Information & Communication Technology Act 2006.

There are a lot of systems to protect and trace the cyber criminals worldwide. Among them Computer Emergency Response Team (CERT7) is the most efficient method. It consists of the cyber specialists all over the world. The function of CERT is to monitor the computer network of the world. When any interruption, irregularities or any kind of unlawful activities occurred CERT can know about it. Knowing about it necessary steps are taken to protect or prevent the crime. By this no occurrence of network is unknown to CERT. Bangladesh has formed the authority of CERT by taking permission from the international CERT. But the government is yet to permit this for this it is working only for the necessity of international CERT. But not for the necessity of Bangladesh. According to the specialist of Bangladesh if the government permits the authorization of CERT of Bangladesh every occurrence will be traced by the law enforcing agencies. In these cases the crimes may be traced at the initial stage and then legal enforcement may be taken easily. On the other hand taking initiatives in accordance with the law may become easier in the case of taking contingence and filing any case. As cyber crimes can be traced technically by the specialist of Bangladesh and necessary knowledge can be ensured by the Bangladeshi for this a specialists team of CERT. can be formed for the greater benefit of the people of Bangladesh8.

7.CERT is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems and to limiting damage and ensure continuity of critical services in spite of successful attacks, accidents, or failures. For more detailed information about our work, see Meet CERT.

8. www.cert.org/faq/cert\_faq.html

6. Overview:

Professional and developers of ICT-software, -middleware and -hardware and others responsible for ICT innovations have a crucial role in providing the knowledge and means by which information protection can be enhanced. As home users and small- and medium-sized enterprises (SMEs) usually do not have the resources or professional skill sets to design ICT systems and their means of protection in face of the growing number of cyber incidents, there are double responsibilities for public and private institutions, and for countries to establish security procurement policies and standards.

It is therefore recommended to:-

- Establish means and processes of evaluating new ICT developments and products that might include establishing accreditation agencies, certification policies and procedures of information security enhancing measures.

- Continue development of national CERTS (Computer Emergency Response Teams) around the world, and their liaison with the international FIRST (Forum of Incident, Response and Security Teams) community. Their activities should include not only information sharing, analysis case studies and warning roles, but also a response capability operated by ICT security professionals. This will improve end-user awareness and responsibilities with respect to safeguarding information, security and privacy. Unwittingly, these end users in cooperation's, SME's, and at home can become a â€žlaunch point (pad)" for attacks on the basic communication and other infrastructure.

Heighten awareness of end users in developing - as well as in developed -countries, as they acquire or upgrade ICT capabilities, of major risks, and of the importance of security policies and capabilities. This recommendation pinpoints the need especially for home users and SMEs to learn more about information protection and privacy, by, inter alia, participation in education and training programs; the development of model education curricula and â€ždrivers licenses" for computer users;

Develop warning and reporting points'(WARPs, at www.niscc.gov.uk) which serve as a means Information sharing about incidents at a local community and business level. These can be developed in association with local government, the local branches of the International Chamber of Commerce, and like-minded SMEs and other civil society groups.

7. Conclusion:

As stated in the introduction to this document, the underlying central premise of the Panel's work is to help ensure that the full benefits of the information age accrue to all users of ICTs, and that they are not undercut by negative uses of these technologies, be it through cyber attacks on digital archives and the flow of messages and on information infrastructures, or be it through denials of access. In the view of the World Federation of Scientists it is important to safeguard the integrity and privacy of communications and thus full confidence in ICTs and their security, but also the choice to access freely the full range of information available through these technologies and principally through the Internet9.

The free flow of information is a basic tenet, indeed fundamental characteristics of free societies. Established under the auspices of the World Federation of Scientists, this Permanent Monitoring Panel feels a special obligation to support the appeal of the Erice Statement [[1](https://www.ukessays.com/essays/information-technology/weakness-of-cyber-law-in-bangladesh-information-technology-essay.php?utm_expid=309629-42.KXZ6CCs5RRCgVDyVYVWeng.0&utm_referrer=https%3A%2F%2Fwww.google.com%2F" \l "ftn1)] to all governments to make every effort to reduce or eliminate restrictions on the free flow of information, ideas and people. This appeal is consonant with Article 19 of the United Nations' Universal Declaration of Human Rights which explicitly guarantees the freedom to "receive and impart information and ideas through any media and regardless of frontiers". The broader authority that issues from this Declaration is independent of the exact signatory status of individual countries. It establishes the basic principle of free communication through the Internet. The Declaration of Principles adopted at the Geneva phase of the World Summit solemnly confirms Article 19 in its paragraph A 4, strengthening its language, and affirming that it is central to the Information Society.