UNIT 11 ENFORCEMENT ISSUES IN CYBERSPACE

Structure

11.1 INTRODUCTION

In the previous unit we have discussed the jurisdictional issues involved in computer wrongs. The next step in logical order is to discuss the issue of enforcement i.e. how the law should be applied. This area includes various matters such as prevention, investigation, computer forensics etc. This unit discusses some of these issues.

Computer crimes generally and crimes committed through the Internet in particular are extremely challenging because of their sophistication and variance from crime in the ordinary sense. Crimes on the Internet are characterised by high technological innovation, anonymity, distance from the scene of crime, extent of its reach and most important, the unusual profile of the criminal, many times a juvenile. The challenge posed to law enforcement with the advent of Internet is two fold; (a) new crimes and new kinds of delinquent behaviour using the Internet and computers, for example, hacking, spamming, logic bombs, etc.; (b) new methods of committing traditional crimes, for instance, commission of a bank fraud using the net or defamation through e-mail.

There is significant difference between crime on the Internet and a crime with another modern technology like the telephone. While crimes are rarely directed against a telephone as an instrument, computers often become the victims of attack.[1] Nature of crime on the computer is challenging and requires new definitions and understanding and a restatement of accepted norms of criminal conduct and punishment because of several reasons. Computers, apart from being costly equipment are also the repository of immense amount of data. This data can sometimes contain valuable scientific inputs, purely personal matter, study works, e-mails, and official work. Tampering with this data or stealing it is much more harmful than stealing the computer. This requires the recognition of data as a special form of property and data as a privacy right.

Clearly, with the development of new technology, and with the realisation that such technology affects human life and relations and the peace and order and proprietary rights in society, laws must be framed to regulate conduct accordingly. Let's take for instance theft of passwords. Passwords are central to the operation of computers. These are nothing but keys to gain entry into computer systems and nothing but a combination of alphabets and numbers. Stealing a password or unauthorized access using someone else's password must be recognised as the beginning of crime. Similarly, networks need to be recognised as highways for movement of information and communication and not the sites for cranks to dig holes or put up impediments. Networks, as private roads, can be entered into only by authorization. Web pages, as private property akin to display in shops, can be browsed, but not tampered with or destroyed. Law enforcement can be divided into two parts: (a) prevention and (b) detection.

Cyber-terrorism is the use of computers and information technology, particularly the Internet, to cause harm or severe disruption with the aim of advancing the attacker's own political or religious goals. As the Internet becomes more pervasive in all areas of human endeavour, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i.e. members of an ethnic group or belief), communities and entire countries.[2] It is not naïve to think that terrorist groups could cause serious damage through the use of this method of terrorism. For instance, terrorists could from a remote location hack into the systems of let's say an airlines, and manipulate it in such a way that systems collapse. This could lead to severe damages and loss of life too. Of course most systems in senistive agencies would be highly secure, but even the most secure systems have chances of being sabotaged. In terms of the damage that cyber terrorism can cause, this is a very big challege to contemporary law enforcement.

11.2 OBJECTIVES

After studying this unit you should be able to:

- analyse the sophisticated nature of the computer related crimes;
- discuss how the prevention techniques in computer related crimes are different from that of traditional crimes;
- examine to the extent to which technology can be helpful in prevention of such crimes and the role that the public awareness about such crimes can play in this direction; and
- analyse the concept of computer forensics i.e. have an idea as to how the detection of cyber crimes involves different kind of technique.

11.3 PREVENTION

As far as the law enforcement agencies are concerned, prevention of crime is more important and one of priority than the detection of one after it has occurred.

In the physical world, the police prevents crime through techniques like patrolling, rushing on emergency calls, presence at important functions, fairs, festivals, rallies, guarding of vital installations and providing security to VIP's. Collections of intelligence on suspects, surveillance, warning minor offenders are also important aspects of crime prevention. The question is, are these techniques used by police in the real world for the prevention of crime desirable or practical in the wired world. Are they sufficient or should new and innovative methods of prevention be used? Another concern facing us is that, many of the social norms and ethics, which act as a deterrent to the commission of crime in the real world, are either non-existent or undeveloped for conduct over the Net.

If Internet is accepted as a medium of communication and publication and exchange of ideas, the caution here must be that any form of preventive measures should be minimal and least obtrusive. Otherwise, preventive methods may run into difficulties of "prior-censoring", "violation of privacy," which would never be acceptable in a democratic country. Prevention of crime online definitely needs a different approach than in the real world, some of which are discussed below.

11.3.1 Deterrence as a Means of Prevention

Neal Katiyal[3] in his article argues that increasing the costs of commission of cyber crimes is an important method of prevention. He argues that cyber crime when compared to real world crimes is cost effective and less risky which makes it more attractive to commit. Such crimes are also difficult to detect because the number of parties involved in its commission are, in most cases, the criminal and his/her computer; the element of conspiracy is noticeably lacking making detection difficult and costly. These are adequate reasons to increase the risks of commission of such crimes and to make their commission more costly. If similar acts are committed online and offline, Katiyal argues that online crimes must bear more punishment and more fines. His argument for increase in costs is also based on the ground that most criminals on the Net are youngsters who are always short of cash. He also argues that sites that cater to illegal materials, for example, those which supply hacking tools, must compulsorily be made pay sites. He bases this argument on the ground that, in the past if a site like Napster that offered freely copyright protected music for download, were a pay site, the number of people downloading music from it would have been much lesser than what it was.

11.3.2 Technology as Aid to Prevention

High technology crime must be prevented using high technology. Rather than relying on social pressure or legal sanctions, Lessig explains how physical and electronic barriers can prevent harmful acts.[4] In real space, installing lights on street corners can prevent muggings and other forms of street crime, and placing concrete barricades near inner-city highway ramps can prevent suburbanites from quickly driving in and out to purchase drugs. In cyberspace, Internet browsers can be configured to prevent repeated password entry attempts for sensitive Web sites or could be coded to prevent certain forms of encryption. Larry Lessig contends that cyberspace can be regulated through law and programming code.

This form of regulation using the architecture appears to be an effective and unobtrusive form of regulation. A good example of the beneficial uses of technology is the use of filters by parents to protect their minor children from online pornography. Of course, a closer scrutiny also raises the issue of undue power in the hands of Internet service providers or governments to lay down ground rules of conduct. While technological inputs like virus detectors or filters to keep away certain kinds of pornography is helpful, this is conferring power on some agency to examine contents over the Internet, inviting dangers of censorship.

Encryption is another way by which crime can be prevented. Encryption is a system or technique that renders a message unintelligible to anyone other than the intended recipient of the message. Encryption while being a boon to prevent crime has also the demerit of being used by criminals, terrorists, narcotic smugglers, and child pornographers to conceal their crime. Encryption was a major controversy during the early days of telegraph too.[5]

11.3.3 User Awareness

Since computers which are the subjects of crime are in the possession of victims, making them aware of security measures is one of the best means of preventing crime on the Internet. The following quote attributed to James Barksdale, CEO of Netscape underlines the necessity to build awareness, "in the mind of those with large financial stakes in the development of electronic commerce and money, security is to the Internet what safety is to the airlines". The greatest security threat to computer systems is from insiders. Studies reveal that over 70% of all computer theft is committed from within organizations. Keeping a check on one's own employees is a means to prevent such offences. But the problem here is that some of the means of monitoring like keystroke monitoring, checking logs of usage, etc. may be in conflict with privacy rights.

Some of the ways in which security can be protected are – access control through use of secure passwords, cryptographic tools making communications secure, shielding of emissions, firewall technology to screen traffic.[6] Organizations stand to gain a lot by training their employees in safe practices and threats to security.

11.3.4 The IT Act and Prevention of Offences

The IT Act has also conferred power on the police to prevent the commission of offences under the Act. Section 80 (1) states, "Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act".

Explanation to the section says that for the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public". Therefore, a police officer can enter a cyber café on his/her regular rounds just to check if offences under the Act are being committed. Apart from this some state governments[7] have also initiated moves to regulate the operation of cyber cafés including their registration and maintenance of records regarding accessing of computers at such places.

Sub-section (1) of section 80 provides that any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a state government authorized by the Central Government in this behalf may enter any public place and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under the Act. For the purposes of sub-section (1), the expression 'public place' has been explained to include any conveyance, any hotel, any shop or any other place intended for use by, or accessible by the public.

Powers under sub-section (1) of section 80 have been considered as very wide powers. However, the reason for giving such wide powers might have been the concern over the convenience with which one can commit acts from a public place amounting to an offence under the Act and escape at the minimum possible time as also the possibility of wiping away of evidence. In this process, what has been overlooked is the fact of undue harassment of the owners of such places like cyber cafés and also possible misuse of such powers. The provisions of the Code of Criminal Procedure are to apply in relation to any entry, search or arrest made under section 80, subject of course to the provisions of the section itself.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

a) Discuss various means by which cyber crimes can be prevented? How far can technology be used for this purpose?

....

....

....

....

....

....

b) Discuss the provisions of the IT Act relating to the prevention of cyber crimes.

....

....

....

....

....

11.4 DETECTION OF CRIME

Investigation, for the purposes of the Code of Criminal Procedure, 1973, has been held by the Supreme Court [*State of Maharashtra* v. *Rajendra*, (1997) 3 Crimes 285] to consist generally of the following steps:

1) proceeding to the spot
2) ascertaining all the facts and circumstances of the case
3) discovery and arrest of the suspected offender
4) collection of evidence relating to the commission of the offence which may consist of,
   a) the examination of various persons (including, the accused) and the reduction of their statement into writing, if the officer thinks fit,
   b) the search of places and seizure of things considered necessary for the investigation and to be produced at the trial, and
5) formation of the opinion as to whether on the materials collected, there is a case to place the accused before a magistrate for trial and if so, taking the necessary steps for the same by filing a charge-sheet under section 173.

Investigation of crimes on the Internet is still in its infancy. Investigators are literally writing the book on investigative techniques with each new case.[8] Detection of crime on the Net can be only as good as the investigators. The specialised nature of computer crime requires a specialised response. It requires cops especially suited and trained to deal with it.[9] Often detection of cyber crime is a team effort by police along with technical assistance.

Difficulty in detection of computer crimes arises mostly because of availability of various crime-concealment techniques in cyberspace: passwords, digital compression, steganography, remote storage (at remote ISP hosts), audit disabling (disabling log of activities), etc. Concealing crimes through anonymity using anonymous re-mailer service, sending anonymous e-mails or anonymous digital cash helps in money laundering, computer penetrating and lopping (breaking into another computer and using that as a launching pad to cover tracks).[10]

Detection of computer crimes requires Internet research skills, necessary court orders including search warrants of premises and electronic surveillance. Traditional tools of investigation like questioning suspects, witnesses, collecting fingerprints, laying traps, etc. are also used. Computer logs, IP number of attackers, the route taken by him/her, monitoring of public sites, chat sites, bulletin boards, securing ISP's help in reading e-mails, analysing evidence from a hacker's computer all offer clues in investigation of computer related crimes. Investigators in such investigation face a large number of obstacles mainly because they are dealing with smart young geniuses. For instance, a hacker might hide or 'spoof' his/her Internet Protocol (IP) address, or, bounce a communication through many intermediate computers. Some victims don't keep logs or don't discover hacking until it is too late. Computer hackers may alter the logs upon gaining unauthorized access to a computer. Again some Internet service providers don't keep records. One of the most challenging aspects of investigation is the question of jurisdiction.

Often leads go through foreign countries as the hackers operate from one country, use the ISP of another country and target systems of yet another country. Securing cooperation in investigation from other countries and securing extradition are major problems in investigation.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

1) Discuss the problem of detection of cyber crimes. How far is it different from that of other crimes?

....

....

....

....

....

....

....

....

....

....

....

....

11.5 USE OF CYBER FORENSICS

Use of Cyber Forensics is a very important ingredient in the investigation of cyber crimes. Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime. Two distinct components exist in the emerging field of cyber forensics. The first, computer forensics, deals with gathering evidence from computer media seized at the crime scene. Principal concerns with computer forensics involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes. For this purpose several computer forensic tools are available to investigators. The second component, network forensics, is a more technically challenging aspect of cyber forensics. It gathers digital evidence that is distributed across large-scale, complex networks. Often this evidence is transient in nature and is not preserved within permanent storage media. Network forensics deals primarily with in-depth analysis of computer network intrusion evidence, while current commercial intrusion analysis tools are inadequate to deal with today’s networked, distributed environments.[11]

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What is computer forensics?

....

....

....

....

....

....

....

....

....

....

....

....

11.6 ON-GOING EFFORTS IN INDIA

In India, the government has conducted several awareness and training programmes on cyber crimes for law enforcement agencies including those on the use of cyber Forensics Software packages and the associated procedures with it to collect digital evidence from the scene of crime. Special training programmes have also been conducted for the judiciary to train them on the techno-legal aspects of cyber crimes and on the analysis of digital evidence presented before them.

Countering cyber crimes is a coordinated effort on the part of several agencies in the Ministry of Home Affairs and in the Ministry of Communications and Information Technology. The law enforcement agencies such as the Central Bureau of Investigation, The Intelligence Bureau, state police organizations and other specialised organizations such as the National Police Academy and the Indian Computer Emergency Response Team (CERT-In) are the prominent ones who tackle cyber crimes. CERT-In is involved in developing appropriate security guidelines and other best practices to advise the systems administrators of computer systems and networks all over the country to implement them so as to avoid the systems from being attacked by hackers and other criminals. In the event of systems being attacked, CERT-In helps the victim organizations recover their systems from the computer security incidents so as to make them operational at the earliest. Both the CBI and many state police organizations are today geared to tackle cyber crime through specialised cyber crime cells that they have set up.

Table 1 and 2 show the extent of registration of cyber crimes in India. Cases falling under the definition of cyber crimes could be registered either under the IT Act or under the IPC or by using provisions of both the statutes. The two tables below show registration of cases under both these statutes. The figures clearly show that registration is still very low. However it must not be forgotten that of the estimated number of occurrences of cyber offences only a fraction get reported. This is because many corporates do not wish to publicise offences that have taken place against their companies.

Table 1: Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2003 & 2004

Sl. No.	Crime Head	Cases Registered		% Variation in 2004 over 2003	Persons Arrested		% Variation in 2004 over 2003
		2003	2004		2003	2004	
1)	Tampering computer source department	8	2	–75.00	6	0	–100.00
2)	Hacking Computer Systems						
	i) Loss/damage to computer resource/utility	13	14	7.7	11	31	181.82
	ii) Hacking	8	12	50.0	7	1	–85.71
3)	Obscence publication/transmission in electronic form	20	34	70.00	17	21	23.53
4)	Failure						
	i) Of compliance/orders of certifying Authority	0	0	–	0	0	–
	ii) To assist to decoy or the information in interception by Govt. Agency	6	0	–100.00	12	0	–100.00
5)	Un-authorized access/attempt to access of protected Computer system	1	0	–100.00	0	0	–
6)	Obtaining Licence or Digital Signature by misrepresentation/supression of fact	0	0	–	0	0	–
7)	Publishing false digital Signature certificate	0	0	–	0	0	–
8)	Fraud Digital/Signature	1	0	–100.00	2	0	–100.00
9)	Breach of confidentiality/privacy	3	6	100.00	0	7	–
10)	Other	0	0	–	0	0	–
11)	**Total**	**60**	**68**	**13.33**	**55**	**60**	**9.09**

Table 2: Cyber Crimes/Cases Registered and Persons Arrested under IPC during 2004

Sl. No.	Crime Head	Cases Registered		% Variation in 2004 over 2003	Persons Arrested		% Variation in 2004 over 2003
		2003	2004		2003	2004	
1)	Public Servant Offences by/Against	0	0	–	0	0	–
2)	False electronic evidence	0	0	–	0	0	–
3)	Destruction of electronic evidence	0	0	–	0	0	–
4)	Forgery	89	77	–13.48	102	81	–20.59
5)	Criminal Breach of Trust/Fraud	269	173	–35.68	255	181	–29.02
6)	Counterfeiting						
	i) Property/mark	4	12	200.00	10	8	–
	ii) Tampering	8	7	–12.50	33	16	–51.52
	iii) Currency/Staps	41	10	–75.61	75	43	–42.67
	Total	**411**	**279**	**–32.11**	**475**	**329**	**–30.74**

11.7 SUMMARY

In this unit we have discussed the law enforcement issues of cyberspace. Investigation of cyber crimes involves a combination of traditional investigative techniques and the use of modern technology and cyber forensics. Constant training and technological upgrading is required on the part of the law enforcement machinery to keep the cyber criminals who are mostly deviant geniuses in check. Awareness amongst the users of cyberspace can also play an important role in this connection. Though in India not very many cases under cyber crimes have been reported, in the near future, with the immense penetration of the use of the internet, such cases are bound to increase.

11.8 TERMINAL QUESTIONS

1) Discuss the various types of cyber crimes.

2) Discuss the ways of prevention of cyber crimes. What role can technology and user awareness play in this respect?

3) Discuss the issues involved in the investigation of cyber crime.

11.9 ANSWERS AND HINTS

1a) Computer crimes generally, and crimes committed through the Internet in particular, are extremely challenging because of their sophistication and variance from crime in the ordinary sense. Prevention of crime online definitely needs a different approach than in the real world, some of which are discussed below.

1) Deterrence as a means of prevention

Neal Katiyal [Neal Kumar Katiyal, "Criminal Law in Cyberspace", 149 *U. Pa. L. Rev.* 1003, 1009 (April 2001)]. in his article argues that increasing the costs of commission of cyber crimes is an important method of prevention. He argues that cyber crime when compared to real world crimes is cost effective and less risky which makes it more attractive to commit. Such crimes are also difficult to detect because the number of parties involved in its commission are, in most cases, the criminal and his/her computer; the element of conspiracy is noticeably lacking making detection difficult and costly. These are Ade encryption. Larry Lessig contends that cyberspace can be regulated through law and programming code.

This form of regulation using the architecture appears to be an effective and unobtrusive form of regulation. A good example of the beneficial uses of technology is the use of filters by parents to protect their minor children from online pornography. Of course, a closer scrutiny also raises the issue of undue power in the hands of Internet service providers or governments to lay down ground rules of conduct.

Encryption is another way by which crime can be prevented. Encryption is a system or technique that renders a message unintelligible by anyone other than intended recipient of the message. Encryption while being a boon to prevent crime has also the demerit of being used by criminals, terrorists, narcotic smugglers, and child pornographers to conceal their crime.

Since computers which are the subjects of crime are in the possession of victims, making them aware of security measures is one of the best means of preventing crime on the Internet. The greatest security threat to computer systems is from insiders. Studies reveal that over 70% of all computer theft is committed from within organizations. Keeping a check on one's own employees is a means to prevent such offences. But the problem here is that some of the means of monitoring like keystroke monitoring checking logs of usage, etc. may be in conflict with privacy rights.

b) **The IT Act and Prevention of offences**

The IT Act has conferred power on the police to prevent the commission of offences under the Act. Section 80 (1) states, "Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act. "Explanation to the section says that for the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public". Therefore, a police officer can enter a cyber café on his/her regular rounds just to check if offences under the Act are being committed. Apart from this some state governments have also initiated moves to regulate the operation of cyber cafés including their registration and maintenance of records regarding accessing of computers at such places.

Sub-section (1) of section 80 provides that any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a state government authorized by the Central Government in this behalf may enter any public place and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under the Act. For the purposes of sub-section (1), the expression 'public place' has been explained to include any conveyance, any hotel, any shop or any other place intended for use by, or accessible by the public.

2) Problem in detection of computer crimes arises mostly because of availability of various crime-concealment techniques in cyberspace: passwords, digital compression, steganography, remote storage (at remote ISP hosts), audit disabling (disabling log of activities), etc. Concealing crimes through anonymity using anonymous re-mailer service, sending anonymous e-mails or anonymous digital cash helps in money laundering, computer penetrating and lopping (breaking into another computer and using that as a launching pad to cover tracks). Detection of computer crimes requires Internet research skills, necessary court orders including search warrants of premises and electronic surveillance. Use of Cyber Forensics is a very important ingredient in the investigation of cyber crimes. Cyber

forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve the crime.

3) Use of Cyber Forensics is a very important ingredient in the investigation of cyber crimes. Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime. Two distinct components exist in the emerging field of cyber forensics. The first, computer forensics, deals with gathering evidence from computer media seized at the crime scene. Principal concerns with computer forensics involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes. For this purpose several computer forensic tools are available to investigators. The second component, network forensics, is a more technically challenging aspect of cyber forensics. It gathers digital evidence that is distributed across large-scale, complex networks. Often this evidence is transient in nature and is not preserved within permanent storage media. Network forensics deals primarily with in-depth analysis of computer network intrusion evidence, while current commercial intrusion analysis tools are inadequate to deal with today's networked, distributed environments.

11.10 REFERENCES AND SUGGESTED READINGS

1. E.g., virus attacks, hacking, denial of service, clogging of networks etc.

2. <http://en.wikipedia.org/wiki/Cyber-terrorism>.

3. Neal Kumar Datival. “Criminal Law in Cyberspace”. U. Pa. L. Rev. 149 April. 2001:1003-1009.

4. Lawrence Lesser. “Code and Other Laws of Cyberspace”. (1999): 53-60 quoted in ibid.

5. See generally. Tom Standage. *the Victorian Internet* (1998): 100-107.

6. A hardware and/or software system that protects an internal system or network from the outside world or protects one part of the network from another.

7. See for instance the Karnataka Act dealing with the registration of cyber cafés.

8. William R. Spernow. “Cyber crooks on the Net: Why Traditional Law Enforcement will be Unable to Cope with Threats to the Electronic *Commerce System*”. Cyber crime and Security. (1998): 1.6-8

9. Skills required being a Cyber Cop: The actual data that may make or break a case can never be touched. The electrical field that is used to shift the polarity of a group of molecules that becomes one of the bits in the data on the hard drive that belongs to your suspect can never be seen. A TCP/IP packet colliding with another packet on the Internet can never be heard. In essence, the primary physical skills that make a great street cop lend little to the skills to be a Cyber Cop. The only skill that is transferable is the power of observation, and that skill, along with an insatiable curiosity about how things work, are the foundational skills required to be a Cyber Cop. William R. Spernow. "Cyber crooks on the Net". Cyber crime & Security, (1998): 1.6-7.

10. Dorothy E. Denning, Wiliam E. Baugh Jr., "Hiding Crimes in Cyberspace", Cyber crime and Security, 1.14-14, 1.14-19 (1998).

11. National Crime Record Bureau. "Crime in India 2004". Ministry of Home Affairs Publication <http://www.afrlhorizons.com/Briefs/June01/IF0016.html>.