INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

 ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

ANALYZING LEGAL AND SECURITY ISSUES IN CYBER SECURITY CONTRACT & MEASURES TO REDUCE CYBER SECURITY RISKS

AUTHORED BY: GUNJAN,
Assistant Professor,
Law Department (Guest Faculty),
Himachal Pradesh University Regional Center, Mohli, Dharmshala, District Kangra, Himachal Pradesh 176218

ABSTRACT

Would we achieve higher standards for software and data security if contractors and subcontractors accepted stringent cyber security requirements in software development agreements, vendors signed off on similar requirements in software license agreements, and service providers included cyber security components in their offerings? One might expect that contractual provisions would improve the current situation, but we frequently see that results do not turn out as well as anticipated, usually for ignored or unrecognized reasons. In this article, we will identify cyber security risks inherent in developed and acquired software products as well as software related service issues. Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is cyber crimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

The issue of cyber crimes has received much attention of late, as individual and organizational losses from online crimes frequently reach into the hundreds of thousands or even millions of dollars per incident. Computer criminals have begun deploying advanced, distributed techniques, which are increasingly effective and devastating. This paper describes a number of these techniques and details one particularly prevalent trend: the employment of large networks of

 ISSN: 2582-6433

compromised computers, or botnets, to conduct a wide variety of online crimes. The paper also relates a number of the practical, legal, and ethical challenges experienced by practitioners, law enforcement, and researchers who must deal with these emergent threats.

Keywords— Contract Law, Cyber Law, Cyber Security, Mobile Law

INTRODUCTION

The technological development has given rise to a cyber world constituting cyber space. Cyber space is witnessing considerable advancement with the rapid increase in the information technology. It is always hard to determine or predict something in the future in an accurate manner. There is a possibility to consolidate the technological advancements in the past.[1] Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today's technical environment many latest technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are thus increasing day by day.[2]

IMPORTANCE OF CONTRACTS

The Importance of Contracts

Those who negotiate and enforce computer contracts are familiar with the all-too-common vendor statement: "We'll put this

Contract in a drawer (or file folder) and never reference it again." Of course, this is often the case. When contractual terms need to be invoked, however, that statement often indicates an adversarial situation. This is also a ploy to make customers feel more comfortable with boilerplate vendor agreements and not push as vigorously as they might otherwise for stiffer contractual terms and conditions. However, not standing up for certain contract provisions that are important to your organization is a mistake. This approach is commonly used with take-it-or-leave-it contracts, where vendors are not willing to negotiate at all. The above sentence may be

*Assistant Professor, Law Department,(Guest Faculty) Himachal Pradesh University Regional Center, Mohli , Dharmshala District Kangra 176218

[1] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[2] CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

 ISSN: 2582-6433

accompanied by this reassurance: "Well, our major customers have already agreed to this." Such assertions may not necessarily be true and should be verified if possible. Contracts serve the very important purpose of mitigating risks — not only for customers but also for suppliers — and of specifying each party's responsibilities and liabilities when a covered event occurs or when there is a breach of contract. It is up to each party to anticipate what those risks might be and to specify how to handle them. When it comes to computer software, risks have escalated rapidly over time, with massive changes happening at an accelerating pace during recent years.3

CYBER SECURITY CONTRACT -MEANING

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures. There will be new attacks on Android operating system based devices, but it will not be on massive scale.[4] The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.[5]

SOFTWARE CONTRACTS AND CYBER SECURITY

We now examine typical provisions included in software con-tracts by software category. It is important to realize that software products (or pre-packaged software) are typically licensed rather than purchased, so that the vendor retains ownership. The organization paying for the development usually owns custom-built software, whether internal staff or third parties are developing it. Open source software belongs to everybody or nobody. Yet even as it is freely available, those who use the software have contractual requirements. Embedded software can fall

[3] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.
[4] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy.
[5] CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

 ISSN: 2582-6433

into any of the above categories, but the system or service provider generally handles conditions of use and support. The latter is retained in-house, managed by a third party or situated in the cloud. Cyber security has been increasingly included in software contracts, for both products and services, over the past several decades and well into the future. The dia-gram intersperses the various technologies that have emerged over this same period. Considering that the internet did not become popular until the 1990s, the lack of awareness about cyber security for many years is quite understandable.

There are many additional areas where formal agreement is required. Here is a more comprehensive list of requirements that should be included in software and/or a service agreement:

Risk assessment- Conduct risk assessments prior to and periodically throughout the term of an agreement. If unacceptable risks are encountered, explicit remediation and mitigation processes, as should have been detailed in the agreement, need to be activated. Their successful completion should be certified in writing.

Confidentiality – Ensure that certain types of data customer, client and employee personal information, intellectual property and business plans — should be protected to the extent necessary to minimize the risk of access, manipulation, destruction, etc.

Privacy –Meet legal and regulatory requirements for protecting data and not disclosing personal data, whether accidently or intentionally or unintentionally.

Performance - Determine that the product and service can meet pre-specified performance criteria, such as transaction through-put and response time, under various load situations (number of users and transactions processed per second).

RISK ASSESEEMENT- Conduct risk assessments rior to ae

LATEST ON CYBER SECURITY ISSUES

Privacy and data theft will be the top security issues that organizations need to focus. We live in a world where all information is in digital form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. There will be new attacks on Android operating system based devices, but it will not be on a massive scale.[6] The fact tablets

[6] Majesty, H., Cyber Crime Strategy, S.o.S.f.t.H. Department, Editor. 2010, The Stationery Office Limited: UK. p. 42.

 ISSN: 2582-6433

share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android.[7]

RECENT SURVEY ISSUES ON CYBER SECURITY TRENDS

The following list was developed from cyber security research and survey.

A. Mobile Devices and Apps

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack, as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.[8]

B. Social Media Networking

Growing use of social media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.[9]

C. Cloud Computing

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are

[7] www.uncjin.org/Documents/EighthCongress.html.
[8] Williams, G.L., Glanville Williams Learning the Law, A.T.H. Smith, Editor. 2006, Sweet & Maxwell.
[9] http://www.thefreedictionary.com/Gun+Crime)

 ISSN: 2582-6433

underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.[10]

D. Protect systems rather Information

The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies - to protect the data stored therein.[11]

E. New Platforms and Devices

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows. But the proliferation of new platforms and new devices - the iPhone, the iPad, Android, for example - will likely create new threats. The Android phone saw its first Trojan this summer, and reports continue with malicious apps and spyware, and not just on Android.[12]

F. Everything Physical can be Digital

The written notes on a piece of paper, the report binder and even the pictures on the wall can be copied in digital format and gleaned for the tools to allow a activist-type of security violation, and increasingly this will be a problem.

PRACTICES AND CONCERN BY GOVERNMENTS FOR CYBER SECURITY CONTRACTS

Ensure that national cyber security policies encompass the needs of all citizens and not just central government facilities. Encourage the widespread ratification and use of the Cybercrime Convention and other potential international treaties. Support end-user education as this benefits

[10] Jones, A., Technology: illegal, immoral, or fattening?, in Proceedings of the 32nd annual ACM SIGUCCS fall conference. 2004, ACM: Baltimore, MD, USA. p. 305-309
[11] Ibid
[12] Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, in International Conference on Electro/Information Technology, 2007 IEEE. 2007: Chicago, IL. p. 610-615.

 ISSN: 2582-6433

not only the individual user and system but reduces the numbers of unprotected computers that are available for hijacking by criminals and then used to mount attacks. Use procurement power, standards-setting and licensing to influence computer industry suppliers to provide properly tested hardware and software. Extend the development of specialist police and forensic computing resources. Support the international Computer Emergency Response Team (CERT) community, including through funding, as the most likely means by which a large-scale Internet problem can be averted or mitigated. Fund research into such areas as: Strengthened Internet protocols, Risk Analysis, Contingency Planning and Disaster Propagation Analysis, Human Factors in the use of computer systems, Security Economics.[13]

TRENDS CHANGING CYBER SECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

A. Web servers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.[14]

B. Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it

[13] Peter Sommer, Ian Brown, OECO Project, "Reducing Systemic Cyber Security Risk", 2011
[14] Amichai Shulan, Application Defense Center (ADC), Amicha Regularly Lactures, Security, 2011.

 ISSN: 2582-6433

should always be noted that as the cloud evolves so as its security concerns increase.[15]

C. APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.[16]

D. Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.[17]

E. IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.[18]

F. Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is

[15] Booz Allen and Hamilton, Reports, "Top Ten Cyber Security Trends for Financial Services", 2012.
[16] ITU Cyber Security Work Program to Assist Development Countries, 2008
[17] Unisys Corporation, "Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security" USA, 2011
[18] Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India

 ISSN: 2582-6433

usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.[19]

ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data. In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses.[20]

In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report. Though social media can be used for cyber crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done.

However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in

[19] Yang, Miao, "ACM International Conference Proceeding Series", vol. 113
[20] Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005

 ISSN: 2582-6433

order to stay away from risks. One must handle social media by using certain policies and right technologies.[21]

CYBER SECURITY TECHNIQUES

A. Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

B. Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.[22]

C. Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to a malfare.[23]

D. Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important in detecting the malware.[24]

E. Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs

[21] Ibid
[22] ITU Cyber Security Work Program to Assist Development Countries, 2008
[23] Arun Prabhudesai, "Cyber Attacks In India", 2011.
[24] Audry Watters, Read Write Cloud, RWW Solution Series, 2010.

 ISSN: 2582-6433

include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.[25]

CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

A. DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world .

B. Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

C. Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.

D. Do not operate others accounts using their passwords.

E. Never try to send any kind of malware to other's systems and make them corrupt.

F. Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.

G. When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

H. Always adhere to copyrighted information and download games or videos only if they are permissible.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.[26]

CONCLUSION

Cyber conract and cyber security is a vast topic that is becoming more important because the

[25] ibid
[26] Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India.

 ISSN: 2582-6433

world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.