



ICT approach to defuse the cybercriminal sedition dimension of Telangana movement

K. Madan Mohan^{1*}, Dr. P. Premchand², Dr. K. Chandra Sekharaiah³, N. Santhoshi⁴

¹ Asst. Professor, 1 Doctoral Scholar with second & third author and working Asst. Professor in Marrilaxman Reddy Institute of Tech & Mang, HYD, Telangana State, India

² Professor Dean in CSE Dept., Osmania University, Hyderabad, Telangana, India

³ Professor in SIT, JNTUH, Kukatpally, Hyderabad, Telangana State, India

⁴ Asst. Professor, Doctoral Scholar with third author and working as Asst. Professor Aditya College of Engineering Madanapalle, Chittoor, Andhra Pradesh State, India

*Corresponding author E-mail: madan.keturu@gmail.com

Abstract

Cybercrime refers to Internet usage involving any illegal activity. Cybercrimes are becoming galore throughout the length and breadth of the world owing to the increased Internet usage and the human capital involved in the usage. In India also, the same phenomenon is found as the nation has vast population. Undesirably, cybercrimes are percolating into some university academic environments. In our earlier work, we presented many facets of multiple cybercrimes in the JNTUH academic environment. The cybercrimes perpetrated, in the context of the Telangana Movement, w.r.t. the violations of State Emblem of India (Prevention of Improper Usage) Act 2005, u/s 66C-ITA2000-2008 were registered with FIRs. The cybercrime of sedition is not registered yet. Our research work explored in this regard. Under the cybercriminal Government of Telangana (CGoT) has been purportedly prevalent the JNTUHJAC, during 2011–2014 approx., as indicated in the website, <http://jntuhjac.com>, traceable through the cyber forensic web crawler tool wayback machine. Note worthily, the crime got registered against identity theft under Sec. 66-C under IT Act 2000–2008 whereas the complaint was against Sedition crime. The culprit website of JNTUHJAC organization under CGoT was operational in the JNTUH University before the enactment of Andhra Pradesh Reorganization Act 2014 and through that approx. 2000 registrations were obtained for the organizations. We present, in the case study, the many facets of the moot cybercrime issues related to the JNTUH University academic environment and how they are handled by means of the RTI Act 2005 for an empirical approach for impact on the law enforcement agencies to get alert and register the crime under sedition law violation in order to ensure that recurrence of such situations is prevented.

Keywords: ICT Information and Communication Technologies; CGoT Criminal Government of Telangana; JNTUHJAC Jawaharlal Nehru Technological University Joint Action Committee.

1. Introduction

In our paper culprit website is created i.e. www.jntuhjac.com. Which is culprit website at background cybercrime is happened. From 2011-2015 they ran fake govt of Telangana. The present Government formed in 2014 is in the aftermath of the Cybercriminal Government of Telangana that had existence since 2011 with its subsidiary outfit. The JNTUH-JAC as evidenced in the latter's website since the last quarter of 2011. We gather snapshots through a Web Crawler Tool. This cyber crime is one that violates a law i.e. cyber law code: Cr.P.C/Act/Constitution using web as a media. Cheating crime and Sedition crime are presented as the cyber crimes of interest towards handling unlawful organized activity in JNTUH. Sedition crime and cheating crime are highlighted. Over the years 2011-2014, these two crimes were ignored in the sense that no FIR is registered despite complaint. Towards the remedy, as mentioned Figure 3, the informant submitted RTI application to the ACP, Kukatpally Division, and Cyberabad Commissionerate. As the issue was pursued, finally an FIR was registered against the unregistered organized group JNTUH-JAC. Thus, cybercriminal activity became checked by our endeavors.

2. Computing the cybercrimes in the case study

The case study involves [4] cybercrimes. Nearly 2500 online registrations were made into the cybercriminal website <http://jntuhjac.com>. This means that for each of these registrations, [4] cybercrimes are applicable. Thus, there is a sense to say that 2500*4 cybercrimes are relevant in the context. This value of 10,000 crimes involved is interesting to study further. This is for [2] cybercriminal organizations involved in the case study. Thus, 10,000 *2=20,000 units of crime is involved in the case study. This is what we refer to as "degree of cybercriminal case". The term "degree of cybercrime" is rather a neologism. It refers to the computation of the cybercriminal intensity in the case study. When the cybercrimes of this kind are left unchecked, the degree of cybercrimes increases by arithmetic progression by a value of eight additively for each registration. The high value of the degree of crime indicates that the case study involves BIG DATA. This may seem misnomer as a first note. However, it is to be understood that what is BIG DATA volume in one context may not be so in another context. For instance, the value of 20,000 units of degree of cybercrime in our case study is considered as BIG DATA owing to it that the data is relevant to 'crime'.

Small statistical values as measure of degree of cybercrime should rather be considered as BIG DATA owing to it that the data is relevant to 'crime'. This data volume may not be treated as BIG DATA w.r.t. some other application which is noncriminal. The table below indicates the computational details w.r.t. degree of cybercrime in our case study.

Table 1: Computing the Degree of Crime

No of Cybercriminal Organizations	No of Registrations	No. of Crimes	Degree of Crime
2 viz. JNTUH JAC and CSGlobal	2500 approx.	4 (Cheating, Identity theft, Sedition, State Emblem of India (Prevention of Improper Use) Act2005 Violation	2500 registrations * 4 crimes * 2 cybercriminal organizations=20,000 units

3. Related work

[1-3] As per our survey we knew that the cyber crimes police station deals in various issues, complaints and frauds like email and non email related crimes.[4] Here we identified the sedition crime (i) by words, either spoken or written, or (ii) by signs, (iii) by visible representation.[5] We created peoples governance forum webpage because of the Government, University, Court and Police Stations are failed to control cyber crime in JNTUH University.[6] Research adviser website consist valuable information like research publications stastics,special lectures, articles and projects which are helpful for our developing of paper.[7] It's important reference <https://sites.google.com/site/sekharaiiahk>, we included the details of FIR report as under about a cyber crime a fake govt of Telangana [8] RTI Act 2005 is a priceless, effective instrument for an employee to remedy the lack of probity in the organizational administration by engaging the employer to ensure positive organizational behavior [11] The paper presents relevance of knowledge, Intelligence and attitude as only some of the multitudinal subject areas where research in ICT and psychology is convergent.[12] The functioning of some of the University Level Institutions in the country turns maladaptive occasionally owing to mismanagement of academics. By such an approach, they tend to turn the organizations maladaptive. [13] In this paper,we present the judgment in the aftermath of the chargesheet.We present that the Cyberabad police failed to make use of the cyber forensic evidence in handling the case.[14] In this paper, we present a case study of a cybercrime w.r.t. the Culprit organization Government of Telangana (CGoT) that has been purportedly prevalent during 2011–2015 approx. as indicated in the website home page image of <http://jntuhjac.com>. Interestingly, the crime is registered against identity theft under Sec. 66-C under IT Act 2000-2008 whereas the complaint was against Sedition crime.

4. Motivation

We highlighted the context where in the complaint was for registration of Sedition crime in the case study. But, the Cyberabad police registered the complaint under Sec. 66-C under IT Act 2000-2008. It interests us to evaluate the grounds for the non registration of the complaint against the Sedition crime. It is felt that online sedition crime, in particular, was not considered in the formulation of the IT Act 2000-2008. Perhaps, it was because of it that the Cyber-crime PS police@Cyberabad did not register the complaint against the sedition crime. In this background, the complaint was, later, made in the KPHB PS near the JNTUH University. Under the purview of any general police station, general sedition crime or online sedition crime.

5. Delineation of the case study

The author requested for Information under RTI Act 2005 regarding the higher authorities The Registrar and PIO(Public Information Officer) on October 2014.According to the attested Information to the VC,JNTUH and then CI, KPHB PS.the following Information asked the RTI Act 2005.a)Did the JNTUH authorities ever communicate with the FGoT(or)the allied JNTUH JAC members in any manner?(or)context?and asked list of JNTUH officers who considered FGoT(or)the allied JNTUHJAC ever as legal or constitutional or as to have existed as known from its website till recently as in references?b)asked about Martyrs' Relief Fund collected from staff salaries after Telangana formation in June 2014.c)why JNTUH neglected to identify the cses of students who were involved in FGoT or The allied JNTUHJAC activities for award of degrees since 2011 to till date.d)Information as to how the JNTUH authorities checked the FGoT or the allied JNTUH JAC activities in the campus year wise since 2011 till date.e).

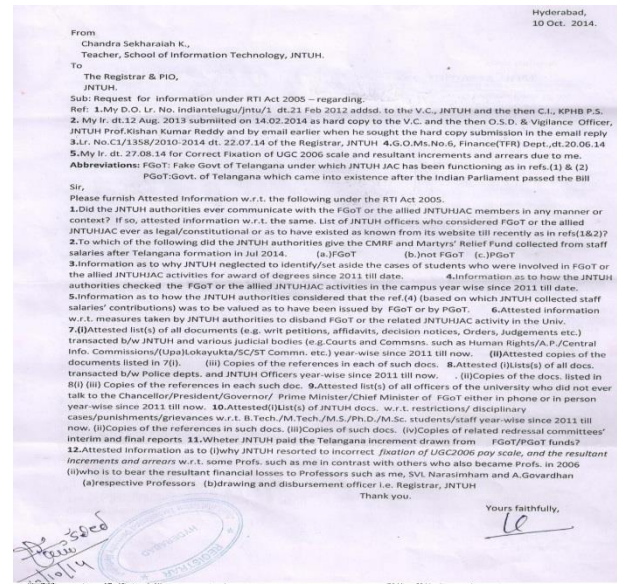


Fig. 1: An RTI Application of the Author to Elicit Attested Information W.R.T. JNTUH's Relationships with the Fake Government of Telangana vs. with the Parliament-Enacted Govt. of Telangana.

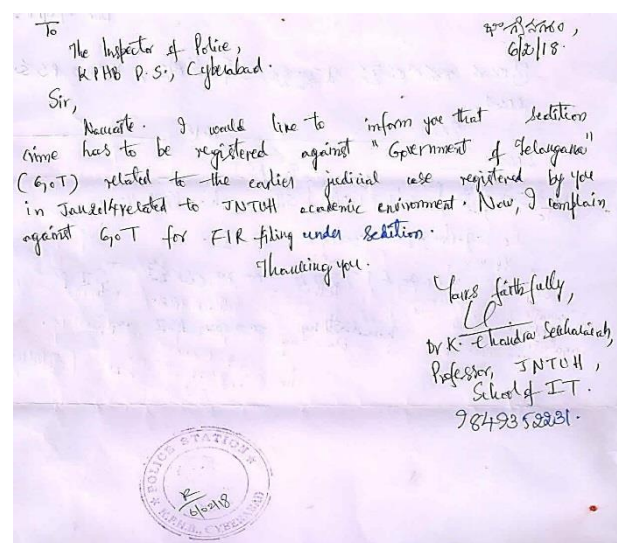


Fig. 2: Given the Complaint to the Inspector of Police, KPHB P.S., and Cyberabad. Sedition Crime has to be registered Against "Government of Telangana" (GoT).



Fig. 3: File FIR Against Sedition Informed to the DCP And ADCP, Cyberabad. It is Informed That FIR Be Filed for Immediate Action against the Culprit Government of Telangana in the Issue.

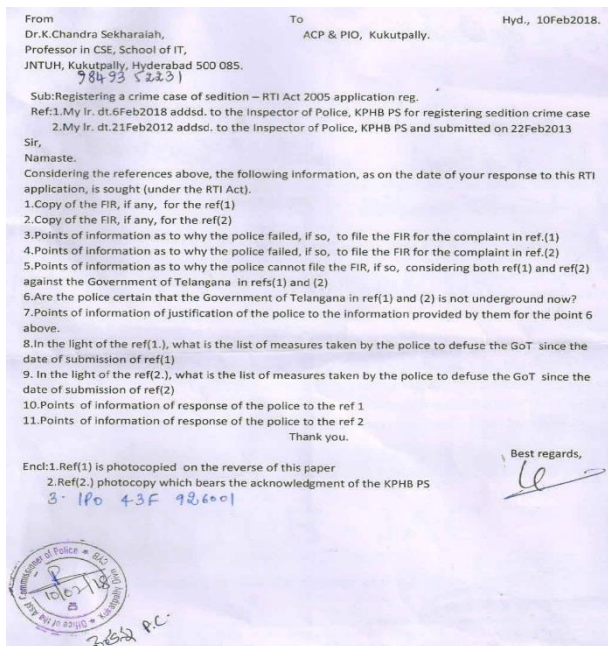


Fig. 4: Registering a Crime Case of Sedition with RTI Act 2005 Application to ACP & PIO, Kukatpally.

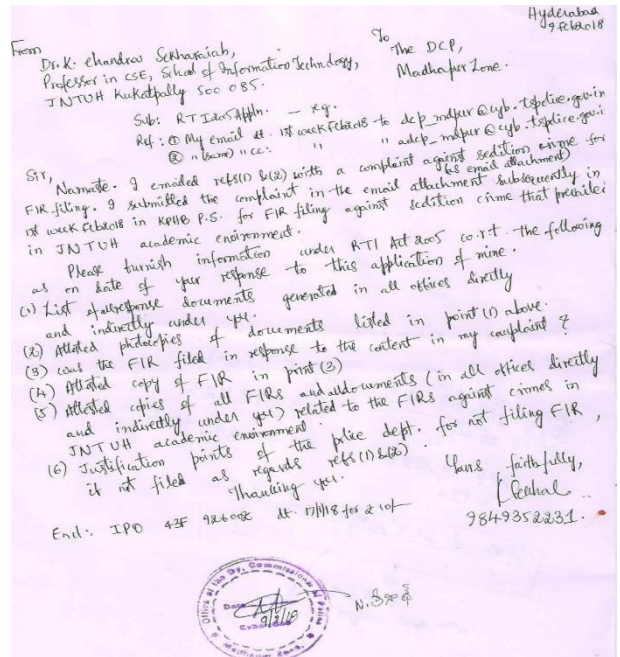


Fig. 5: RTI Act 2005 Application to the DCP, Madhapoor Zone from Research Adviser.

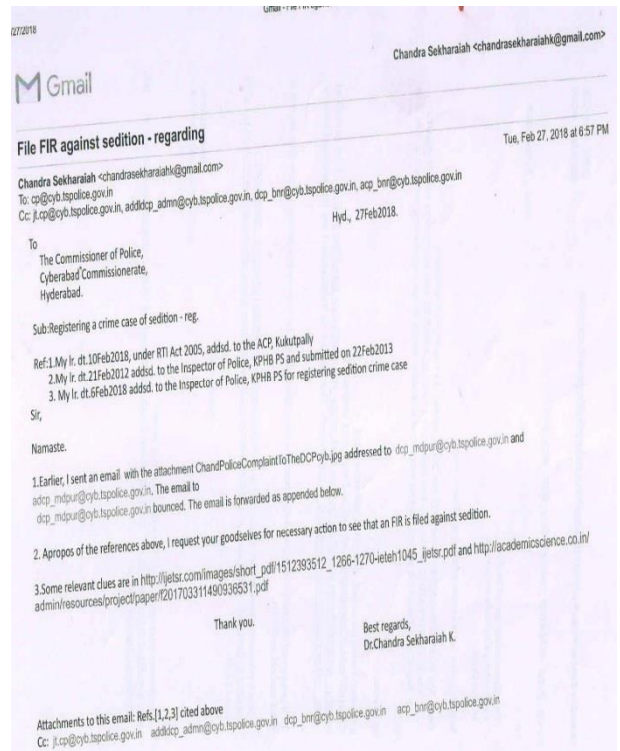


Fig. 6: Register A Crime Case of Sedition File FIR Against Sedition to the Commissioner of Police Cyberabad Commissioner Ate, Hyderabad.

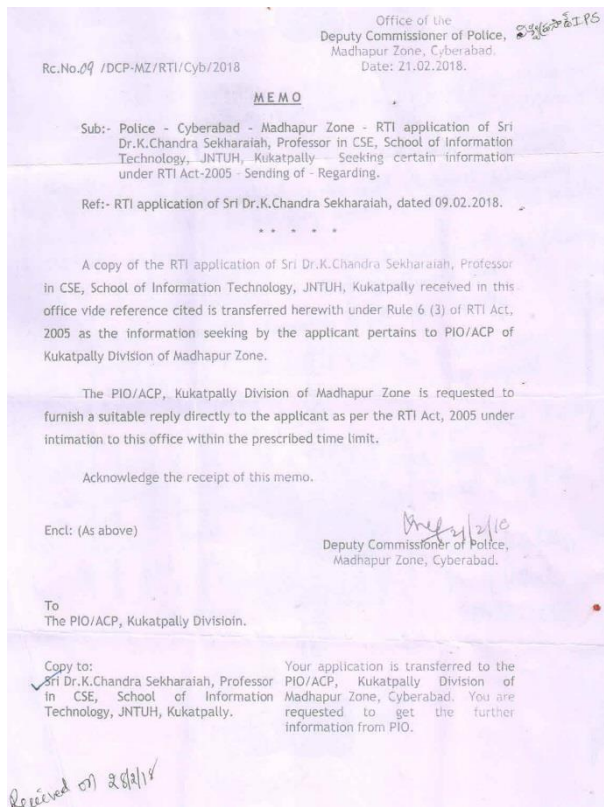


Fig. 7: Memo Send by From Office of the Deputy Commissioner of Police, IPS, Madhapur Zone, Cyberabad to the PIO/ACP, Kukatpally.

6. Conclusions

Our work has conceptualized the notion of “Degree of Cyber-crime”. The case study of multiple cybercrimes interests the research community because of it that it is a Big Data Cybercrime. What is of ‘big data’ value in the case of cybercrimes may not be so in normal applications/cases. This is because cybercrimes tend to abuse the IT application scenario. The negative impact/applications of IT should not outnumber or tend to be enormous as compared to the positive impact/applications. The significance and impact of ‘Degree of Cybercrimes’ is under study. The notion serves towards metrics of cybercrimes.

In our earlier empirical study, the police only when questioned, under the RTI Act, as to why the complaint was not registered, registered a cybercrime complaint. Now, the case study presented is a similar issue. The remedies to the common man who is patriotic and complains against a cybercrime which abuses the national assets such as the national emblem and the Government of India are bleak in the sense that the role play of the law enforcement agencies is very dissatisfactory. In sequel, we conclude that the present governments such as the State Government of Telangana (GoT2014) as well as the one at the union level should feel responsible and release white papers w.r.t. the actions taken by them to defuse the fakeGoT, CGoT, SGoT and to ensure nonrecurrence of prevalence of cyber-criminal governments. The possibility of social networking web-sites gives a hope for us to disseminate about the fake, cybercriminal GoT. Our work in this regard is on the anvil for further research.

References

- [1] <http://www.hyderabadpolice.gov.in/Cybercrimes.html>.
- [2] <https://archives.org/web>.
- [3] <https://sites.google.com/site/chandraksekharaiiah/indiaagainst-corruption-jntu>.
- [4] <http://www.rmlnlu.ac.in/webj/sedition.pdf>.
- [5] <https://sites.google.com/site/sekharaiiah/peoplesgovernanceforum>.
- [6] <https://sites.google.com/site/chandraksekharaiiah/miscellaneous333>.
- [7] <https://sites.google.com/site/sekharaiiah/folder222/cybcfir0006by2018pagesandexaminationreportobtainedfromdrkconjan2018>.
- [8] S Ravikumar Y.K.Sudnara Krishna K Madan Mohan K Chandra Sekharaiah, “IMPACT OF THE RTI ACT WITH IN A PUBLIC AUTHORITY ORGANIZATION TOWARDS EMPLOYEE-EMPLOYER ENGAGEMENT - A CASE STUDY” Presented in MRITCISTCSE-2018 in Computer Science & Engineering 19th & 20th January,2018.
- [9] K.Madan Mohan, K.Chandra Sekharaiah, P.Premchand, "A Case Study of ICT Solutions against ICT Abuse: An RTI Act 2005 Success Story", Presented in @Institution of Engineers(I), Khairatabad, Hyderabad & published in International Journal of Engineering Technology Science and Research(IJESR) ISSN 2394 – 3386, Vol. 4, Issue 11, Nov. 2017.
- [10] Ramesh Babu J., A.Radha Krishna, K.Madan Mohan, K.Chandra Sekharaiah, "Adaptive Management of Cybercriminal, Maladaptive Organizations, in the Offing, that Imperil the Nation", in Procds. 27th Annual Conference of National Academy of Psychology (NAoP)@IIT, Kharagpur, Theme:Psychology of Millennials, 22-24Dec2017.
- [11] M. Gouri Shankar, P. Usha Gayatri, S. Niraja, K. Chandra Sekharaiah, “Dealing with Indian Jurisprudence by Analyzing the Web Mining Results of a Case of Cybercrimes”, in Springer Procds. of International Conference on Communication and Networks (Com-Net 2016), Ahmedabad, India, 20-21 Feb. 2016, pp 655-665.