INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (online)
ISSN 2348 - 9359 (Print)

An Internationally Indexed Peer Reviewed & Refereed Journal

www.IRJMSH.com
www.isarasolutions.com

Published by iSaRa Solutions

Digital Push of Indian Economy by the Government: with special reference to Safety and Security Strategies of the Government to Control Cyber Crimes and Future of Our Digital India

Ms. Megha Ojha
LL.M., UGC JRF & NET, RPSC-SET
Research Scholar : School Of Law, Gujarat University, Ahmedabad
Email ID medhasango@gmail.com

Abstract: *Cyber crimes and cyber attacks are occurring at a greater frequency and intensity all over the world. Presently digitalization policy make people to use of information technology (IT) enabled services such as e-governance, online business and electronic transactions, this step made India favourite among cyber criminals and posing severe economic and national security challenges According to cyber security experts fast digitalization of economy may open a pandora's box of cyber crimes in India. In present scenario it is very important to adopt new strategies and enforcement mechanism, seems to be the most immediate needs for cyber security and to ensure cyber safety in India. Yet neither a concrete plan has been outlined on how to build cyber security policy nor any action has been taken to build the cyber warriors pipeline. This paper presents for investigating future of our digital India, effects of digitalization and our policies to control cyber crimes or cyber threats.*

Key Word: Effects of digitalization, cyber threats, cyber crimes and future of digital India

Digital India

To hasten India's transition from an Analog or analogue to a digital economy our Prime Minister Narendra Modi has started series of transformative initiatives including Aadhar, De-monetization and Digital India. The Digital India (DI) initiative inaugurated by Prime minister on 1 July, 2015 with aim to make all citizens digitally literate and bring the internet and e-governance to all sections of the society.[1] The vision of Digital India programme also aims at inclusive growth in areas of electronic services, products and manufacturing. Digital India mission was really jumpstart for India's economic growth but these goals would not be achievable unless India dramatically improves its cyber security infrastructure and law enforcement mechanism in case of cyber crime and cyber attacks.

Vulnerabilities of digital India in terms of Cyber Securities

Vulnerabilities of digital India in terms of cyber securities goes fast and grows at a worrying pace. News related to hacking of the social media accounts of our politicians and news reporters draws attention to another kind cyber vulnerability in India. With one more big step of demonetisation pushing Indians to adopt e-platforms at great pace, this vulnerability is also growing fast. On October, 2016 approx 3.2 million Indian debit cards were reported to had been compromised.[2] As per RBI report crimes related to ATM, Debit Card and credit card

total 16,468 crimes were reported in India in year 2015-2016.[3] An ASSOCHAM report published in October 2016 as per report number of mobile frauds in India is expected to grow by 65% in current year.[4]

Union Minister of state for home affairs of India, Kiren Rijiju said that "Total 707 websites associated with the Indian government both central and state have been hit with security breaches in the past four years". [5] As now government is collecting large no of data in terms of volume and therefore in case of government website hacking it can be misused by hackers or cyber criminals from anywhere in the world. In this case the Cyber law enforcement question arises because if law enforcement machinery will not function effectively than whole digitalization mission will be on stake. There is a question about the reliability of digital lockers also in which all citizens will have their official documentation. By this mission government intended to bring people who are semi-literate therefore there is one more question regarding the operative part of e-governance by rural and illiterate citizens. Hence, proper training is also required to make rural Indians computer literate.

Cyber Attacks

Cyber-attack is any type of offensive manoeuvre employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.[6]

Terrorists and criminals are trying to exploit any vulnerability in digital system. In present situation, any country, in any part of the world, could find itself used as a transit point and any country would become the target of an attack. Global nuclear watchdog IAEA (International Atomic Energy Agency) and the US-based non-profit group Nuclear Threat Initiative (NIT) on 12th April 2017 alerted the world community of a possible threat of cyber and terrorist attack on nuclear facilities.[7] Recently Indian security forces alerted by central intelligence agencies, central intelligence agencies warned our defence personnel including the army, paramilitary as well as police forces that their login data and bank PIN numbers would be at stake.[8] It has been warned that WhatsApp virus is threatening to hack their personal information and banking data.[9] It seems to be that this whatsApp virus developed for specifically targeting the country's defence forces. Therefore ensuring effective cyber security is important for everyone and in our nation. Now as and when we are talking about India, it emerged as a favourite among cybercriminals, mostly hackers and other malicious users are using the internet to commit crimes. The origin of these crimes widely based abroad in countries like USA, China, Pakistan, Bangladesh etc.

In 2013 Pakistani hackers, calling themselves "True Cyber Army" hacked and defaced 1,059 websites of Indian election bodies.[10] As per information provided by Ministry of Electronic and Information technology total 155, 164, 199 and 39 websites of central ministries department were hacked (into) during the year 2014, 2015, 2016 and 2017(upto February) respectively.[11] On January, 2017 Pakistan-affiliated operatives had hacked the official website of the elite National Security Guard (NSG) and defaced it with an abusive message against the Prime Minister along with anti-India content.[12] The hackers of the NSG website had identified themselves as 'Alone Injector', and posted the offensive content on the site's home page.[12a]

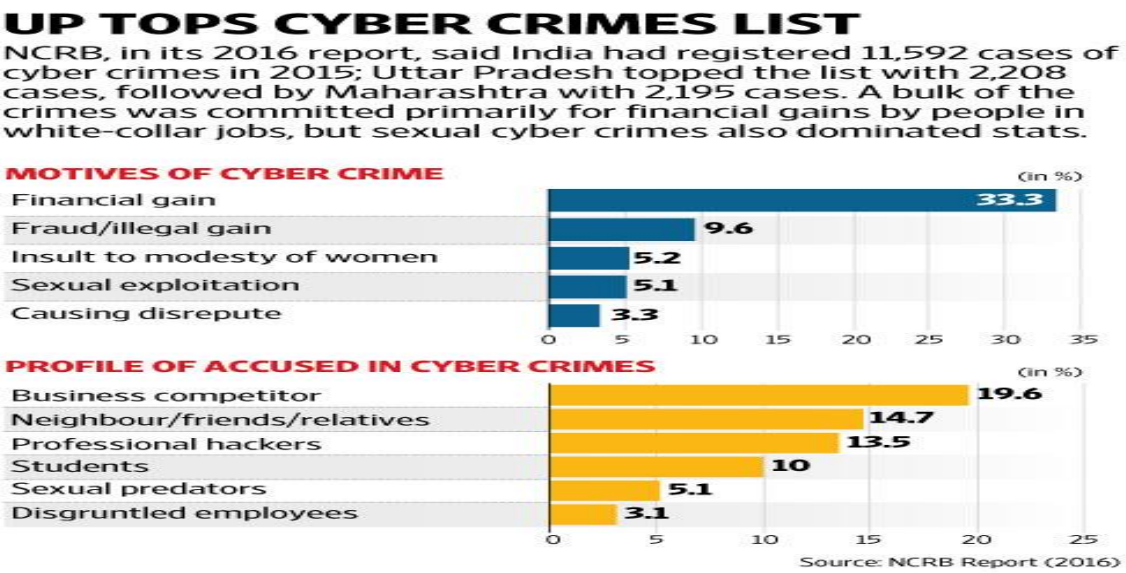
Cyber Warfare and Cyber Terrorism

In cyber warfare attacker use computers networks and other technologies of defending and attacking information and computer networks of an enemy. On the other hand Cyber terrorism is "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[13] That means the end result of both cyber warfare and cyber terrorism is the same, to damage critical infrastructures and computer systems linked together within the confines of cyberspace. Therefore to ensure long-term security of our military and our civilian infrastructure, we must implement a forward-looking strategy to deal with this cyber warfare and cyber terrorism. The government sector military and private sector must develop a framework for securing the country's critical infrastructure from cyber terrorism and cyber attacks.

Cyber Space Security and Controlling on hacking

The economic growth of any nation and its security whether internal or external and competitiveness depends on how well is its cyberspace secured and protected. Our government should rethink about application of law and delivery of justice under current circumstances. In our country special courts are needed to deal with cyber-crime and therefore, government and judiciary need to look beyond law books, case papers and settled law in case of cyber crimes because the slow process would not help the victims of cyber crime. In present scenario, it is unfortunate in our country that the rule of law is same for the nation, but application of mind varies from judge to judge and case to case therefore there is a strong possibility that villagers and poor people get suffer more compare to literate and techno-friendly people in case of cyber crimes because our enforcement system is very week.

Below image is showing what types of cyber crimes are prevailing in India in Utter Pradesh.



India was ranked third worldwide, next to US and China, as a source of malicious activity in 2015[14]. According to 2016 report by Symantec Corp, a software security firm, India was ranked second as a source of malicious code and fourth and eight as a source or origin for web attacks and network attacks, respectively, in 2015.[15] In recent times, India witnessing increasing number of cyber crimes. In fact the gullible nature of Indians puts them at very high cyber risk. In Northern Cyber Security survey report, it has been found that 34% of Indians are not hesitating to give their passwords and other details to the strangers or unauthenticated person.[16] Recently self-proclaimed group of hackers from our country 'Kerala Cyber Warriors' hacked the homepage of the Pakistan Academy for Rural Development's (PARD), Peshawar on 17 April, 2017 and were demanding justice for Kulbhushan Jadhav.[17] India is standing 8th in the list of top ten Cyber criminals and hacker's countries in the world, Indian hackers take a share of 2.3% in the global cyber crime,[18] therefore Indian tourists are most prone to cyber attacks and hacking by our (Indian) hackers. India will get success in complete digitalization and smarter e-governance only if it get smart and tough on cybercrimes, steadfast in building digital literacy and kept its databases hugely safe.

Cyber Crime Report and Cyber Courts in India

In whole India there is only one court specially for Cyber Crime that is in Delhi. In cyber appellate tribunal chairperson seat is vacant since 2012.[19] More pathetic condition is that in IT Act , 2000 there is a provision of the adjudicating officer as per the provisions of section 47, but at present in India this post is vacant or non-functional in many states.[20] Therefore it is well understood that in digital India mission there was not concrete planning for grievance handing mechanism. Now most urgent need to establish more dedicated Courts for cyber crimes in India and proper appointment in the cyber courts.

Due to pathetic condition of the grievance handling, cyber courts and enforcement machinery, it is understood that if in any of the rare cases if someone found that cyber criminals get arrested, then there must be many computer professionals and law enforcement officers with cyber expertise were working together in the background because without extreme efficiency and approach it is impossible to fight cyber criminals.

In India only 74.04% people are literate as per senses 2011,[21] only few of our population are techno-friendly therefore in case of cyber crimes people are clueless as in where do report and how to get money back. In India government should make necessary changes in cyber laws so that victims will be encouraged to report cybercrimes. In survey report it has been found that only 20% of cyber crimes are being reported in our country.[22]

Getting bullet proof evidence against the cyber criminals is always tough task. In fact in cyber crime or cyber theft cases it is very difficult to prove that theft or crime has happened. We can understand it with a situation, suppose if there is any attack on the bank server and if someone ends up losing lakhs of his hard earned money then there is no way by which that person can prove that the attack has been planned by a particular person or some group. If a person get successful in proving that the attack has been carried out by some hackers then most of the hackers don't have any identity, many of them are from outside India, therefore it is difficult to catch the cyber crime accused. Hence strong international co-operation is also required to control cyber crime because if in case of no co- operation from other countries it will be impossible to get justice in cyber crime cases.

Cyber Security strategies and other countries co-operation

Our IT and law minister Mr. Ravi Shankar Prasad attended the G20 Digital Ministerial Meeting held in Dusseldorf, Germany on 7th April 2017.[23] Ravi Shankar called for G20 countries to actively cooperate to combat cyber crimes and cyber terrorism. G20 countries were also promised to cooperate actively to control this type of crime. This meeting was good step toward international co-operation to control cyber crime and cyber terrorism.

Developed Countries like UK, Japan, Germany and US have already developed a series of 3-5 cyber security strategies with clearly defined budgets on cyber security and cyber warriors task force in case of cyber emergency. But like other developed countries India is not working in the direction to develop cyber warriors offensive and defensive force.

In November 2016, UK's National Cyber Security Strategy 2016-21, released, the strategy commits to invest GBP 1.9 billion (Rs 16,000 crore) over the five year period.[24] The strategy focuses on three critical levels:

- To defending national IT infrastructure (Government and citizens),

- To deterring and counter-acting cybercrime and cyber-terrorism
- To developing capabilities (both people and new technology) to protect British cyberspace.[25]

Conclusion and Suggestion

We need to work on national level as well as international level to control cyberspace related crime. Our 2017 budget is a pivotal budget for cyber security and for digital economy in many ways but still it is inadequate to implement national level programme for cyber security therefore government should fix more funds for cyber space security. As Cyber security is a field that evolving continuously therefore our governments alone cannot manage for all elements of the cyber security strategy at all level in this cyber world therefore, for cyber security positive international response is also compulsory. It is also required to highlight cyber security programme. To get success in digitalization mission government should develop standards and guidelines to promote security. Improvement in grievance handing in cyber crime cases, development for law enforcement and developed national standard guidelines and governance structure to ensure security in public and private sector all these are compulsory steps for success of our digitalization mission. As developed countries have already developed a series of 3-5 cyber security strategies therefore in present scenario our government should also need to develop overall strategy involving academia, private sector and civil societies. It is also required to develop cyber warrior offensive and defensive work force for cyber emergency.

NOTES AND REFERENCES

1. Press Information Bureau Government of India, Prime Minister to Launch Digital India Week on the First July (27 June 2015) Ministry of Communications & Information Technology, Retrieved from http://pib.nic.in/newsite/printRelease.aspx?relid=122837
2. Saloni Shukla & Pratik Bhakta, 3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit, Eu Bureau, (20 Oct 2016,), Retrieved from http://economictimes.indiatimes.com/news/industry/banking/finance/banking/3-2-million- debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-an axis-worst-hit/articleshow/54945561.cms
3. Shashidhar KJ, RBI reported 16,468 instances of financial cyber crime in 2015-16, **(**7 April 2017**)** Retrieved from http://www.medianama.com/2017/04/223-rbi-cyber-crime-fraud
4. India will see 65% rise in mobile frauds by 2017, ASSOCHAMEY study report, **(12 Dec 2016)** Retrieved from http://www.assocham.org/newsdetail.php?id=6087
5. Manish Singh, More than 700 Indian government websites hacked in last four years(08 Feb 2017) Retrieved from http://mashable.com/2017/02/08/indian-government-security-attacks/#nO91bA_WQSqW
6. Lewis, James Center for Strategic and International Studies, United States, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats (2002) Washington, Retrieved from https://en.wikipedia.org/wiki/Cyber-attack
7. Press Trust Of India : Govt, IAEA flags cyber threats concerns for nuclear facilities (12 April 2017) Retrieved from http://www.dnaindia.com/world/report-zambian-opposition-leader-hichilema-charged-with-treason-police-2398216

8. SOHINI MITTER, Indian security forces alerted of possible WhatsApp virus attack (04 Jan 2017) Retrieved from HTTP://MASHABLE.COM/2017/01/04/INDIA-SECURITY-FORCES-WHATSAPP-VIRUS-ALERT/#IJAQ89R7XPQK*Id.*

9. The News International Staff "Cyber Secure Pakistan' initiative launched"(22 April 2013) Retrieved from https://en.wikipedia.org/wiki/Cyber-attack

10. 550 Govt websites hacked in 3 yrs, 39 already in 2017 (22 March2017) , Deccan Herald; New Delhi, DHNS: 1:01 IST, Available : http://www.deccanherald.com/content/602531/550-govt-websites-hacked-3.html

11. Home Ministry Website Blocked After Attempted Hack, Press Trust of India, (12 February 2017) Report Updated: 14:29 IST, Retrieved from http://www.ndtv.com/india-news/home-ministry-website-blocked-after-attempted-hack-report-1658558

12. 12a. Id.

13. Lewis & James. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats (D.C.2002). Center for Strategic and International Studies ,Washington, United States , Retrieved from https://en.wikipedia.org/wiki/Cyber-attack

14. India ranks third in the world as a source of malicious internet activities, India Spend, (02 Jun 2016) Retrieved from https://www.newslaundry.com/2016/06/02/india-ranks-third-in-the-world-as-asource-of-malicious-internet-activities

15. **Chaitanya Mallapur,** Cyber Crimes Up 19 Times Over 10 Years: Report, (06 June 2016) India Spend, As Internet Use Spreads, Available : https://www.youthkiawaaz.com/2016/06/cyber-crime-rate-in-india

16. Are Banks Failing to Ensure Security of Digital Money of Customers?, NDTV INDIA, NEWS, Available on http://youtu.be/t2qbBRBkOGw

17. Kerala Cyber Warriors Hack Pakistan Website to Protest Kulbhushan Jadhav's Death Sentence, News18.com, (17 April 2017) IST 6:41 PM, Available : http://www.news18.com/news/india/kerala-cyber-warriors-hack-pakistan-website-to-protest-jadhavs-death-sentence-1375981.html

18. TOP 10 COUNTRIES WITH MOST HACKERS IN THE WORLD, Trends Reports Analysis (7 September 2016) Available : https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94e

19. ANUJ SRIVAS, The Tragic and Comedic Functioning of India's Cyber Appellate Tribunal, (12 Dec 2016) Available : https://thewire.in/86414/tragic-comedic-functioning-indias-cyber-appellate-tribunal/

20. NDTV INDIA, NEWS , Are Banks Failing to Ensure Security of Digital Money of Customers?, Available : http://youtu.be/t2qbBRBkOGw

21. Available : www.census2011.co.in/literacy.php

22. **Chaitanya Mallapur,** Cyber Crimes Up 19 Times Over 10 Years: Report,India Spend, (6 June 2016) Internet Use Spreads, available: https://www.youthkiawaaz.com/2016/06/cyber-crime-rate-in-india

23. Shravan Nune, G20 Digital India Ministerial meeting on Digital Economy held in Germany (11 April 2017) , Retrieved from http://www.jagranjosh.com/current- affairs/g20-digital-ministerial-meeting-on-digital-economy-held-in-germany-1491915114-1

24. **Sivrama Krishnan,** Keeping safe our digital India plans Countries such as UK, Germany and US have developed a series of 3-5 cyber security strategies along with clearly defined budgets, **(**28 March 2017) IST ; 08:27, Retrieved from http://tech.economictimes.indiatimes.com/news/internet/keeping-safe-our-digital-india-plans/57865455 *Id.*

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM