LIBERAL STUDIES

Vol. 1, Issue 2, July–December 2016

E. Dilipraj[*]

Hacking – Tracing the History: What can India do with its Hackers?

We keep moving forward, opening new doors, and doing new things, because we're curious and curiosity keeps leading us down new paths. – Walt Disney

In the process of evolution, the human emotion of curiosity has played a major role in advancing the evolutionary process from one phase to the next. Such curious minds have ultimately been responsible for the inventions and discoveries, which make mankind the technologically evolved race of today. Even otherwise, the daily routine of any common man is filled with an insatiable curiosity to learn, understand, study, explore, discover, and invent something new based on one's own interests, irrespective of the field. And each and every outcome of this consuming curiosity opens a new avenue for further exploration of the path – a process which then proceeds into an explosive chain reaction of newer discoveries and inventions. One of the greatest discoveries that has evolved thus and which was a direct result of the curiosity to connect with the whole world, is the technology of telecommunication which has revolutionised the world and is continuing to do so since its inception.

The telecommunication technology has undergone a massive revolution in a short span of time, a direct result of the enthusiastic minds who wanted to transform the very model of human communication. Once the telecommunication networks were established and operational, the same curiosity and thirst for further development of several techno-savvy individuals of societies all around the world stimulated an exploration of this new technology; albeit with varying intentions. Such forays into this highly

[*] **The author** is an Associate Fellow at the Centre for Air Power Studies (CAPS), New Delhi, India.

technological and complex universe of virtual networks led to the birth of ‘Hackers’ and the numerous ‘Hacking’ instances that have been occurring all around the world. Although the terms hacking and hackers have acquired a negative connotation over a period of time due to varying reasons, this was not the story when it all began.

Tracing the History

It is all purported to have started in the United States of America, the cradle of modern technology, more so, after World War II. Before the introduction of computer networks and the establishment of a global internet, there existed another network, which was globally connected and fully operational – the telephone network. This network of telephone connections was in fact the first ‘real-time’ global communication system in use for commercial purposes. The fact that modern technology was associated with this complex network had intrigued many curious ‘techno-freak’ minds in the society to try and figure out the system; an aspect which can be attributed to the basic human tendency ‘to explore’. This process of exploration then led to many methods and tricks which essentially played around with the telephone network. Though nobody knows or can be certain about when or who started it all, there was already a widespread knowledge among the enthusiasts by the late 1960s. This routine of meddling with the telephone network or bluntly speaking, exploiting the technical loopholes in the telephone network is recognised as ‘Phone Phreaking’ or just ‘Phreaking’.

Phreaking

This was a trick act which started off for fun, but gradually took shape of a hobby for those interested in telephone networks and in general – modern technology. According to a famous phone phreak *Mark Bernay*, “the kick was to find out how to beat the system; how to get at things one was not supposed to know about; how to do things with the system that one was not supposed to be able to do.”[1] As the community of the phone phreak enthusiasts expanded, different groups of phone phreaks started to discuss and share new emerging and evolving techniques with other groups across the country by making free phone calls using various methods of phreaking. Thus, over a period of time, underground syndicates of those phone phreaks also came into existence which were operating more for economic interests than fun.

The fundamental idea for any phone phreak was to find methods to make free calls (irrespective of whether it was a privately owned phone or a public pay phone) by somehow evading the system set up by the phone companies.

However, phone phreaks with higher technological capability were able to accomplish much more than making free calls. For instance, the famous phone phreak *John Draper* aka *Captain Crunch* was able to “send his voice around the world one way, going east on one phone, and going west on the other, going through cable one way, satellite the other, coming back together at the same time, ringing the phones simultaneously and picking them up and whipping his voice both ways around the world back to himself.”[2] This may not amuse many, as many of us in our childhood would have tried to call the other phone in the same room, but the manner in which *Captain Crunch* made such calls was the important aspect as he would not use the dial pad on either phones to make the calls and he was also able to route his calls, one through the cables and the other through satellite without any assistance from the phone companies.

The phone phreaks employed many methods for their act of phreaking such as whistling, using specially engineered devices/ boxes, methods like loop-arounds, etc. Among all, the first and most interesting method was whistling into the mouthpiece of a telephone to make free calls. *Joe Engressia* aka *Jollybubble* who was visually challenged, was considered by the Phone phreaking community as the prime mover in the trade, as he was the first person to discover that by whistling in the required quality, at the right frequency into

Source: http://sites.psu.edu/thedeepweb/2015/09/17/captain-crunch-and -his-toy-whistle, accessed on 11 February 2016.

Image 1: Cap’n Crunch Whistle

the phone's mouthpiece one could make free calls. Though this was becoming a popular method among the phone phreak enthusiasts, it remained hard for them to find the right frequency through manual whistling. This was when *John Draper* aka *Captain Crunch* came to the rescue of phone phreaks by discovering that a toy whistle which was given out as a freebie along with 'Captain Crunch' cereal packet had the proper pitch of 2600Hz – the frequency which was needed to phreak the telephone sets. He had not only found the right whistles, but also annexed the name of the product as his pseudonym.

Apart from whistling, another popular method was loop-around which was mainly popularised by the phone phreak Mark Bernay. In simple terms a loop-around is a test circuit which has two phones at different terminals that would be employed by the phone company to test their circuit line to remote offices without needing a person in the other terminal. The phone phreaks exploited this test facility and began to use these lines as party lines, chat rooms or for alternate phone numbers.[3]

However, the golden age of phone phreaking began after the invention of 'Blue Box' in the late 1960s. A cleverly engineered device which can be utilised to trick the phone company's long distance switching systems to allow the Blue Box user to make free long distance calls. *Al Gilbertson* (not real name) is credited to have invented this device according to Ron Rosenbaum, the author of the first article that exposed the Blue Box to the general public.[4] The Blue Box was at times also referred as M-F-ers that stands for multi-frequencies. At a time when long distance calls were rather expensive, this phone phreaking device became an immediate hit among the phone phreaking enthusiasts. Eventually, in 1970s and 80s many devices like the Blue Box were invented by various phone phreaks with different functionalities.

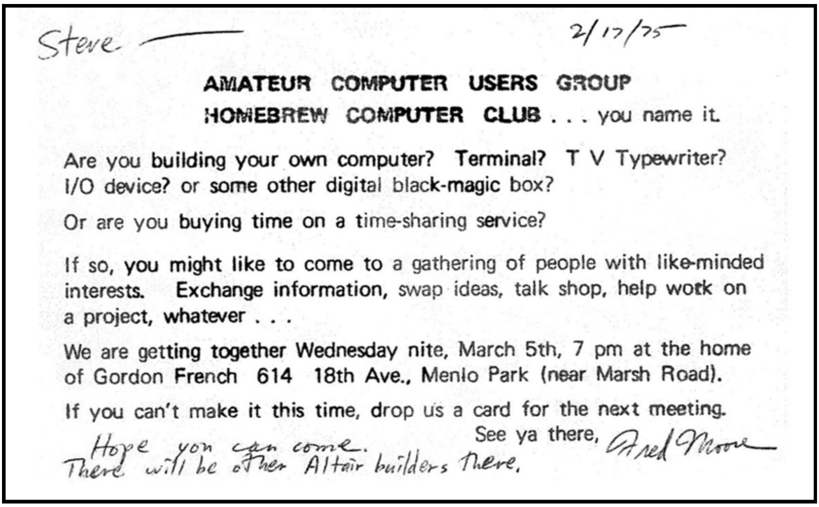
While phreaking became a widespread hobby among the technical enthusiasts, the fact that such a technology exists to evade the telephone systems attracted many underground groups towards the phone phreaks. Many phone phreaks' technological expertise was hired by underground groups and drug cartels for non-traceable illegal activities. For instance, a Las Vegas syndicate ordered thousand beeper boxes (similar device like the blue box) to keep the lines open for hours from coast to coast for them to place bets, which would be expensive if they had to pay for the calls. The phone phreaks would even get bulk orders for manufacturing Blue Boxes worth $300,000 from such underground groups.[5]

Although few phone phreaks who were attracted by the money involved in it, took the illegal primrose path along with underground groups, a few others who were aware of the legal repercussions stayed away from such illegal activities. On the flip side, the telephone companies like Ma Bell and AT&T in association with the law enforcement agencies also succeeded in their attempts to nab phone phreaks who indulged in illegal activities from time to time. In other words, a cat and mouse game was established. However, there were a few other phone phreaks who were attracted only towards the technological aspect involved in the trade and they continued to explore more new technologies as and when they were introduced. One such fascinating technological product which started to come forth in the 1970s was the technology of data processors/ computers.

Although, the initial models of computers in the 1970s were not all that user friendly as they are today, the adventure involved in their tremendous potentials in various areas of the visualised near future, attracted several of the techno-freaks towards these devices and their interests grew in a much higher quotient as they began to tamper with them. Even the famous phone phreaks like Mark Barney and *Al Gilbertson* started meddling with the computers which they found, suited their phone phreak sensibilities much more. In fact, the sense of attraction for a techno- freak was not limited to a particular device/ system like the telephone and its network but, on all Automatic Electronic equipments. Berney had once quoted about his fascination towards playing with automatic electronic equipments that "there are lots of things you can play with. Things break down in interesting ways."[6] Therefore, this sense of exploration and curiosity about the computer technology is considered to be this new age wave of the future brought about not only by the phone phreaks but also by the many others who were exploring avenues in the world of 'computer freaking'.

Computer Freaking

In the late 1970s, as Computers became the watch word among techno-freaks, everybody wanted to either explore or exploit this modern machine and its functioning. This bit of meddling with the early day computers was known as computer freaking and it started pulling in a large band of followers or enthusiasts. As computers were not a common phenomenon in the 1970s, a group of enthusiasts would gather together in a common place, mostly in a garage, to meddle with the computer device that they would have acquired somehow. As the number of enthusiasts grew, few computer freaks were able to organize a bigger gathering for fellow computer freaks; viz. on 05 March 1975 and this convention was called "Home Brew Computer Club."[7]



Steve ——— 2/17/75

AMATEUR COMPUTER USERS GROUP

HOMEBREW COMPUTER CLUB . . . you name it.

Are you building your own computer? Terminal? T V Typewriter? I/O device? or some other digital black-magic box?

Or are you buying time on a time-sharing service?

If so, you might like to come to a gathering of people with like-minded interests. Exchange information, swap ideas, talk shop, help wotk on a project, whatever . . .

We are getting together Wednesday nite, March 5th, 7 pm at the home of Gordon French 614 18th Ave., Menlo Park (near Marsh Road).

If you can't make it this time, drop us a card for the next meeting.

Hope you can come.
There will be other Altair builders there.

See ya there, Fred Moore

Source: https://en.wikipedia.org/wiki/Homebrew_Computer_Club, accessed on 23 February 2016.

Image 2: Invitation Poster for the First Homebrew Computer Club Meeting

This club throughout its existence till 1986, contributed immensely to the computer world as 23 computer companies were started by the members of this club including the famous 'Apple Computer, Inc.', jointly established by Steve Wozniac and Steve Jobs, who were also members of this club.[8]

The various methods and techniques that were invented by the computer freaks to meddle with the computer devices and to customize the machine to their interest was collectively addressed as "hack", a word or a jargon which emerged from the 'Tech Model Railroad Club' of Massachusetts Institute of Technology (MIT) in 1960s.[9] It was from this jargon, the words 'Hacking' and 'Hacker' emerged in later stages and gained popularity through media.

Hacking

All through the 1970s, the act of computer freaking, from now on addressed as hacking, spread and attracted a large number of techno-freaks, and as a result created a sort of sub-culture in the society which was popularly known as "Hackers' culture." The hackers considered their culture as a counter-culture to that of the computer engineers who were professionally more sophisticated and had better resources. Moreover, the development of personal computers by companies like IBM, Radio shack, etc in early 1980s gave a big boost to this hackers' culture as computers were available more easily for these enthusiasts in order to develop their skills and feed their inquisitive minds. The 1980s is known as the golden age of hacking not just because computers were no more a rare phenomenon but more so because of the fact that devices like modems, which enabled computers to communicate with each other over telephone lines, were also widely available and thus significantly extending the reach of a hacker.[10]

The nature of a hacker is to spend inordinate amount of time to learn how computer systems, operating system software, application programs, computer hardware, and networks function. Hackers believe that essential lessons can be learnt about the systems – about the world – from taking things apart, seeing how they work, and using this knowledge to create new and even more interesting things.[11] Hackers by large are self taught in the trade, however, there is also a strong bond of information (techniques and methods) sharing amongst their community which is evident from the various conventions starting from Home Brew Computer Club to the twenty-first century hackers conferences like the DEFCON, ShmooCon, ToorCon, etc. Therefore, it is said that hackers are the true native habitants of the cyber world.[12]

Although 1980s is known as the golden age of hacking, it was a golden age only for the hackers, not for their image or actions. To start with, in 1983, a movie named 'Wargames' was released in theatres which had a storyline about a teenage whiz kid from America who hacks into the super computer of a nuclear missile base of the country and almost starts a global nuclear war. Though articles about hackers and their activities would appear in journals and magazines now and then predating the movie, their circulation was nothing compared to the viewership of this movie. Moreover, the visual impact of the movie created a sort of phobia in the minds of non-technical general public viewers towards hackers. Post the release of the movie, more and more articles and news started addressing the hackers and hacking which all exaggerated the credentials of the hackers negatively which further contributed to the negative image that had the hackers were already portrayed in.

By definition, a hacker is a person who enjoys exploring the details of programmable systems and finds methods to stretch their capabilities.[13] Hacking can be defined as the thrill of exploration and the excitement of learning how something works in order to modify or improve it.[14] However, due to the negative publicity through popular media and journalistic exaggeration, hacker definition changed to – an inquisitive malicious meddler of computers who tries to discover information by poking around. Such perception towards hackers was unacceptable by the traditional hackers who felt that traditional hacking is completely different from the widespread existing perception in the minds of the people. Therefore, the hacking community came up with a jargon in 1985 known as 'Cracker', which became an expression after getting inducted into the 3rd edition of *The New Hacker's Dictionary* edited by Eric S. Raymond.[15]

By definition, a Cracker is one who breaks the security of a system. This term was coined in 1985 by traditional hackers in defence against journalistic misuse of the term hacker in a negative sense. While it is expected that any real hacker would have done some playful cracking and knows many of the basic techniques, anyone past the 'larval stage'[16] is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done). Thus, there is far less overlapping between hacker and cracker contrary to the perception of general public who are misled by sensationalistic journalism.[17]

In a similar fashion, cracking is the act of breaking into a computer system; what a cracker does. Contrary to widespread myth, this does not usually involve some mysterious leap of 'hacker' brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems.[18]

Therefore, having realised the growth of hacking and cracking culture and anticipating its impacts on the society in the future, the US government passed a law in the Congress which was known as the Computer Fraud and Abuse Act in 1986.[19] Moreover, in late 1980s a philosophical divide started emerging in the hacking community itself as an increasing number of hackers were no longer satisfied with benign exploration of systems merely to learn how they worked but to use their skills for individual gain. The same was expressed by Kevin Mitnik, probably one of the most popular hacker; he stated that "Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business…."[20]

Furthermore, the factor which differentiated or was instrumental in creating the difference between traditional hackers and the new group of hackers that emerged was what the hackers refer to as "the hacker ethics." The hacker ethics is a set of loosely binding ethical rules conceived by the early hackers in order to regulate their operations and to make sure their activities do not cause damage to the computer resources. These hacker ethics are:

1. The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source code and facilitating access to information and to computing resources wherever possible.

2. The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality.[21]

Both these ethical principles are widely, but not universally, accepted as a code of ethics and hence a code for modus operandi among hackers. Most hackers subscribe to the hacker ethic in sense 1, and many act on it by writing and giving away open-source software. A few go further and assert that all information should be free and any proprietary control of it is bad; a philosophy which has created disputes between hackers and business oriented information companies and defenders of intellectual property rights. Again, sense 2 is more controversial as some people consider the act of cracking itself to be unethical, like breaking and entering. However, there is also a belief that 'ethical' cracking excludes destruction and so, atleast moderates the behaviour of people who see themselves as `benign'/ harmless crackers. On this view, it may be "one of the highest forms of 'hackerly' courtesy to (a) break into a system, and then (b) explain to the concerned authorities about the vulnerability and exactly how it was done and how the hole can be plugged."[22] This is thus a widely followed practice which many hackers practice using various techniques like exploiting zero day vulnerabilities to hack into systems, networks and software and then report it back to the authorities, in most cases for monetary benefits and in the least of the cases, for nothing but enhanced security. However, this aspect is again exploited by crackers, as many crack into the vulnerabilities existing in the systems and software only for their monetary and other gains rather than raising an alarm as put down originally by the hacker ethics.

So, the end of the twentieth century has seen an increased number of a new breed of unethical hackers or hackers with their own interpretation of ethics driven by self interest and monetary gains directing their knowledge and skill towards illegal pursuits, including activities like distribution of pirated commercial software, games and malwares. Throughout the late 1980s and 1990s, as the hackers community started fragmenting more and more on the basis of their intentions, they started forming groups involving like-minded hackers which eventually led to the formation of 'electronic gangs' driven by their self motivated interests.[23] Many such gangs were mostly motivated by economic and political interests and started to use their skills to tap into the sensitive information housed within large institutions, like government departments, educational centres, banks, research facilities, etc. Eventually, as it happens with the conventional gangs in the real world, it didn't take long for the gangs to fight amongst themselves which further escalated the fear and aversion towards hackers in the minds of the public as they witnessed phone networks and other public networks getting jammed and disrupted from time to time. Thus hacking too ventured onto the murky road similar to its predecessor phone ‘phreaking’.

Added to this, in the 1990s, as computers became a household device and the internet was commercialised and spread globally, becoming accessible to most people the world over, hacking took on global proportions. Though the presence of hackers had always been universal globally even before the advent of global internet, just the fact that internet connected everything in real-time facilitated easy access for the hackers throughout the world and also to connect to their peers beyond borders. Thus, all forms of hacking started spreading rapidly like wild fire across the globe. Soon, it became a part of life through media reporting, resulting due to the disturbances the minor fire-works caused to the regular life of the public through their actions like web defacements, denial of service, spreading malwares, stealing information, breaking into sensitive networks, and by conducting other forms of cyber attacks for their self motivated gains.

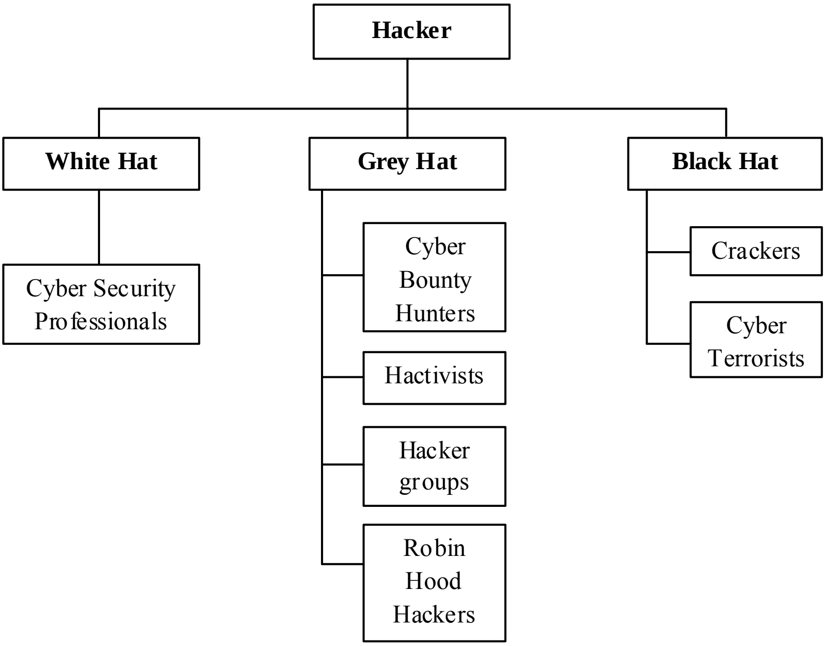


Chart 1: Intent Based Classification of Hackers

Therefore, having reviewed the history of hacking and hackers themselves, it would be prudent to classify hackers, now based on their intentions for hacking. Thus, a better classification of hackers based on their intention could be as follows.

It should also be noted here that for a hacker his/her skills is the most important aspect and all hackers do not possess similar level of skills in the trade and therefore, every hacker or a cracker cannot accomplish all tasks. Based on their level of skills, the hackers are generally classified between the two extremes of a Script Kiddie and an Elite Hacker.

A script kiddie is the lowest form of cracker/ hacker with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems. They do mischief with scripts and programs written by others, often without understanding the exploit they are using.[24] An elite hacker is a social status among hackers for those who have high skills in the trade and are capable of accomplishing highly complex hacking tasks. Normally elite hackers are highly connected among their peers and newly discovered exploits are circulated among this group of hackers/ crackers.[25]

Hacking at present has grown to become an everyday activity which the global population has to live with, in the current globalised world. Hackers across the world operate and conduct their operations for various motives like vendetta, jokes/ hoaxes/ prank, terrorism, political and military espionage, monetary benefits, hate, etc. The law enforcement agencies on the other hand are on constant pursuit of the hackers to bring them before law. However, this cat and mouse game will continue despite strong legislations being implemented or even after many new security roadblocks have been discharged, as long as computers and technology driven-communication systems is available at our disposal. On one aspect, it is helping the evolution process of the domain as hackers push for new innovations when they are in the process of exploiting and devaluing the older ones. Thus, the solution or final game here, is not to find ways of elimination of hacking; rather it should be to strive to bring the hackers into the mainstream and focus their energy and skill towards development.

The Indian Experience

According to the annual report from Computer Emergency Response Team of India (CERT-in), the agency has tracked around 25,037 Indian websites' defacements including a number of government websites and other attacks in the year 2014, which amounts to approximately 68 hacking instances on an average per day. In spite of all these reports, it is unfortunate to know from many independent cyber security observers in India that although there are regular reports of hacking incidents, the government organisations are not vigilant enough to take any necessary steps to improve any sort of security to the Indian cyber networks. It has been reported after an audit that out of 7,000 Indian government websites, only 3,192 have been audited for information technology (IT) security, while 3,556 others are yet to be audited. Yash Kadakia, head of Security Brigade, a government-empanelled security auditor says that "According to our data, about half the government websites are vulnerable to cyber attacks. Most of the government websites do not have any proper security checks in place."[26]

While aggression is the only tactic followed by the groups of hackers around the world, the security providers of the cyber space have always lacked in their vigilance to provide security to their country's cyber networks and infrastructures. Sunil Abraham, Executive Director of the Bangalore-based 'Centre for Internet and Society' said during an interview to *Al Jazeera* that "The Indian government has a very low level of cyber awareness and cyber security. We don't take cyber security as seriously as the rest of the world."

The problem of cyber attacks by the hacking groups would not be a big problem if it would stop with the hacking and defacing of websites. But in reality it moves on to the next stage. The same people who carry on with hacking and defacing websites-jobs could even involve in cyber espionage and data mining against their enemies. These people may also volunteer their expert service to the terrorist organisations in return for monetary benefits and other forms of remunerations. A cyber security professional working with one of India's intelligence agencies said "We once sat down to check the Delhi [internet] Backbone. We found thousands of systems compromised. All were government's systems," "Research and Analysis Wing, Intelligence Bureau, Military Intelligence...we don't realise how much damage has already happened."[27]

The lack of awareness and lethargic approach in monitoring and providing security to the cyber networks in India have already led to thousands of compromised computers across the country. The infection ranges from small Viruses, Botnets[28] to that of Stuxnet[29] level malwares which can hamper the total operations of the network connected to the compromised computer.

The list of new malwares such as Stuxnet, Flame[30], Duqu,[31] etc. and many more are under the process of coding and their abilities to operate as a cyber weapon are incredible and at the same time unbearable if not properly protected. Assuming that the hackers groups get access to these kinds of malwares, then the situation would be extremely dangerous to the national security as it is equivalent to terrorists getting access to nuclear weapons. While talking about the same, Mr. Sachin Pilot, the then Minister of State for Communications and Information Technology said that: “The entire economies of some countries have been paralysed by viruses from across the border. We have to make ourselves more resilient. Power, telecom, defence; these areas are on top of our agenda.”[32]

A careful study of the series of hacking on Indian websites and networks by hackers around the world would reveal a basic fact that something which started as a minor display of cyber skills has now taken the form of a large scale act in the form of personal revenge, economic profits, a race to show off technical supremacy and anti-national propaganda.

This was very much evident from one unfortunate event that disturbed the internal security of India in August 2012. Indian government was alerted after an exodus of thousands of people of North Eastern origin gathered together in railway stations of south Indian cities, especially Bengaluru after being threatened by ‘SMSes’ and violent morphed pictures that were being circulated on more than 100 websites. The ‘SMSes’ threatened the people of North Eastern origin living in various cities in India with a targeted attack on them and asking them to go back to their homeland and some of the pictures circulated on the internet were images of violent bloodshed.

The government of India reacted soon on this matter and a 43-page report was prepared by intelligence agencies in collaboration with National Technical Research Organisation (NTRO) and India Computer Emergency Response Team (CERT-IN) which traced back the origin of several of the doctored images back to Pakistan. The origins of these morphed images were later traced back specifically to Lahore, Rawalpindi and other Pakistani cities by the Indian Intelligence agencies. This involvement of Pakistan based elements in such intolerable behaviour is seen as cyber terrorism and cyber psychological warfare against India to cause internal security disturbances and eventually to create a huge crisis in the country. This incident, which created an imbalance of major proportions in the internal security of the country is one of the prime examples of the adverse effects of wrong utility or misuse of cyber technology and hacking skills.

For India, it is not only Pakistan that challenges its security in the cyber front but there is another Red Giant Cyber Dragon – China, above India, which, in fact has a more advanced and organised form of cyber army at its disposal with which it is even able to challenge United States through cyber espionage operations like ‘Titan Rain’.[33] It is believed that Chinese cyber warfare policy is based on sixth century B.C. Chinese strategist Sun Tzu: “The art of fighting without fighting.” There are instances between India and China where officials in the Indian government have alleged that attacks on Indian government networks, such as that of the Indian National Security Council, have originated from China. According to the Indian government, Chinese hackers are experts in operating Botnets. Fears of Chinese cyber espionage have resulted in the blocking of deals with Chinese telecoms, like Huawei, due to their ties with the Chinese military.[34] The Indian intelligence agencies raised many doubts and warned about Huawei’s potential ill fated penetration into Indian telecom. Their worst fear was that the Chinese firm could be a Trojan horse, meant to infiltrate Indian networks in peacetime and disable it through remote ‘kill switches’ during wartime, through hidden ‘trapdoors’ and malicious programmes that could then open a channel back to its designers.[35] In 2010, the cyber attacks on the computers of India’s National Security Adviser’s (NSA) office, Indian Air Force and Indian Navy are suspected to be from China. In each case, it opened up several small windows through which classified documents and presentations were whisked away. At this juncture, Pakistan’s affiliation towards China is an important factor and this affiliation can become deadly for India if they both join hands in the future for a two-front cyber offensive operation against India.

What can India do with its Hackers?

In order to avoid such explosive situations, the Indian government should take swift measures by identifying the talented Indian hackers and rehabilitate and encourage those who are deserving and also recruit them into the Indian cyber security infrastructures. As most of the hackers are teenagers, this act of converting the ‘Black Hat Hackers’ or ‘Grey Hat Hackers’ into ‘White Hat Hackers’ would be the right step for the government to mould them into hackers that could work for the Indian cyber safety. This will not only give the right push to the future of such youngsters but will also create an ultimate cyber security culture in the country.

India’s Information Technology sector is a significant contributor to the economy of the country, and India is one of the leaders in this sector, in the world. The country has enough young IT talents who, unfortunately, remain scattered across the Indian subcontinent. In fact, most of these talented young minds are in contact with one another through various platforms on the internet. They operate in the cyber space with strange pseudonyms and with different agendas. Although a few wander off as black hat hackers, there are many prospective young vibrant brains which, if harnessed properly, could prove to be potential assets to the country. The Government of India definitely needs to tap these young talented individuals to overcome its shortage of a highly skilled workforce of cyber security experts. While this seems to be an easy enough strategy, the question remains as to how this talent can be identified from amongst the vast Indian population. One answer could be by conducting a nation-wide talent hunt through 'Cyber competitions'.

The Path Weavers: This is not a new technique as it is being followed by many leading countries of the world, like USA and China. On 08 May 2009, the White House came up with a proposal for conducting a nation-wide cyber challenge with the aim of finding and developing 10,000 cyber security specialists to help the United States regain the lead in cyberspace.[36] In the same proposal, the following statement by *Jim Gosler*, NSA Visiting Scientist and the founding Director of the CIA's Clandestine Information Technology Office, was highlighted: "There are about 1000 security people in the US who have the specialised security skills to operate effectively in cyberspace. We need 10,000 to 30,000.*"*[37] It was also mentioned in the proposal that such competitions would act as a diversion to young talented people from going astray. This competition was conducted by the government of USA in association with SANS Institute – a leading institution in Information Security Training and Security Certification in the world.

In fact, it could be said that the Americans borrowed this idea of conducting nationwide cyber challenge from the Asian giant and Indian neighbour, China. The practice of conducting such cyber competitions in China is prevalent since early twenty-first century and they have a more structured approach to it. China's approach can be seen in two stages: one at the regional level and a progressive next step which is the national level. The People's Liberation Army (PLA) conducts these competitions on behalf of the Chinese government. As a first step, the PLA invites young talented people to participate in the regional level cyber competitions which are conducted in all the military regions of the country. In the second stage, the top few contenders of every region are formed as a team and made to represent the region in the nation-wide competition.[38]

The victorious talented lot is then tapped by the PLA to work for them either as private operatives or recruited into their cyber armies, like Unit 61398 in PLA. The most popular case of one such identified talent of China is *Tan Dailin*[39] who operated with the pseudonym 'Wicked Rose' and who, at the young age of 20, was the leader of a private hacking unit from China called

Network Crack Program Hacker (NCPH). ‘Wicked Rose’ was the champion of the national cyber challenge of China in the year 2005. After his victory, he started operating with few other cyber experts as a team known as NCPH. He was sponsored by the PLA for his missions and the group was an expert in exploiting “Zero-day vulnerabilities” in Microsoft Office software and they were also experts in building Trojans. Using this technique they were able to make a number of successful attacks on their targets, including the critical infrastructures of the US and were able to extract thousands of documents for their commanders in the PLA.[40]

The Way Ahead

Although India does not support or encourage such covert cyber operations by any individual/ groups, yet the above mentioned factors can be taken as an example to understand the ability of young minds in this highly technical and complex domain. Though few cyber related competitions are conducted by even fewer Indian educational institutions, Universities and sometimes, on the sidelines of high level cyber conferences, their reach and level of testing is far below the desired standards. However, if the same is conducted on a larger scale by the government, it might have a nation-wide reach and participation from all parts of the country that would enable the Indian government to identify the hidden talent. There are a number of pro-Indian hacker groups in the country who have been voluntarily involved in hacking wars with their counterparts from Pakistan, China and other countries. The talents of such hackers would be a potential supplement for the country if harnessed properly, or else they could end up being an embarrassment for India.

However, mere identification of talents will not be enough for the country to acquire the desired results. The government needs to take steps to form a framework which would enable the identified talented youth to be groomed and put their skills to work in preserving our national interest, which in turn would serve the purpose of defending the cyber front of the country. The proposed National Cyber security Coordination Centre (NCCC), operating under the Prime Minister’s Office could be made as the nodal agency to undertake this onerous task of enhancing India’s cyber security by identifying, grooming and producing highly skilled cyber warriors for the country. The proposed technical university by the state-run telecom service company, BSNL, can also be involved in the process to provide technical training and grooming the identified talented youth.[41]

Another strategy to hunt for talented youth for enhancing cyber security of the country is to announce rewards to experts who can help solve complex cyber problems. Again taking an instance from the US, where the federal government announced its “first cyber Bug Bounty Program in the history of the federal government,” officially inviting hackers to take up the challenge. Dubbed “Hack the Pentagon,” the bug bounty program invites the hackers and security researchers only from the United States to target its networks as well as the public websites which are registered under DoD.[42] The successful participants were awarded cash rewards as well as recognition for their work. Such ‘Capture the flag’ style programs initiated by the Indian government will not only help the government to reach out to the right talents but will also help identify loopholes in the country’s defensive systems which could be plugged to enhance the country’s cyber security.

As the saying goes in the Indian Armed forces “Catch them young”, the same approach has to be followed in the cyber domain, which will not only provide an effective offensive and defensive cyber capability in the future but would also help turn the perceived evil of hacking into a strength for the country.

Notes

1. Ron Rosenbaum, “Secrets of the Little Blue Box”, *Esquire*, October 1971, p. 222.
2. *Ibid*, p. 121.
3. “Telephone Loop Lines”, http://home.ptd.net/~n3cvj/looplines.htm (Accessed on 13 February 2016).
4. Rosenbaum, n.1.
5. *Ibid.*
6. *Ibid.*
7. Steven Levy, *Hackers: Heroes of the Computer Revolution*, Dell Publishing, 1984.
8. “The Secret History of Hacking”, *Discovery Channel*, US: Discovery Channel, 2001, DVD.
9. Robert Trigaux, “Hackers: The Underbelly of Cyberspace”, *St.Petersburg Times*, 14 June 1998, http://www.sptimes.com/Hackers/underbelly_of_cyberspace.html (Accessed on 23 February 2016).
10. Zuley Clarke, James Clawson, and Maria Cordell, *A Brief History of Hacking,* (Thesis) Georgia Tech, November 2003, p. 1.
11. Levy, n. 7.
12. Jarkko Moilanen, “Realms of Cyberwarriors – Definitions and Applications”, (Master’s Thesis) University of Tampere, August 2009, p. 15.
13. Eric S. Raymond, *The New Hacker’s Dictionary*, 3rd edition, MIT Press, 1993.
14. Clarke, n. 10.
15. Raymond, n. 13.
16. A period of monomaniacal concentration on coding apparently passed through by all fledgling hackers. Common symptoms include the perpetration of more than one

36-hour hacking run in a given week; neglect of all other activities including usual basics like food, sleep, and personal hygiene; and a chronic case of advanced bleary-eye. Can last from 6 months to 2 years, while the apparent median being around 18 months. A few so afflicted never resume a more ‘normal’ life, but the ordeal seems to be necessary to produce really wizardly programmers.

17. Raymond, n. 13.
18. *Ibid.*
19. Jose Pagliery, “The evolution of hacking”, *CNN*, 05 June 2015, http://edition.cnn.com/2015/03/11/tech/computer-hacking-history/ (Accessed on 26 February 2016).
20. Gerry Smith, “Kevin Mitnick, Former Fugitive Hacker, Laments How the Game Has Changed”, *The Huffington Post*, 16 August 2011, http://www.huffingtonpost.com/2011/08/16/kevin-mitnick-hacker-book_n_928107.html?ir=India&adsSiteOverride=in, accessed on 10 January 2015.
21. Raymond, n. 13.
22. *Ibid.*
23. Clarke, n. 10.
24. Raymond, n. 13.
25. Douglas Thomas, *Hacker Culture*, University of Minnesota Press, 2002.
26. Piyali Mandal, “Half the govt. websites in India are prone to cyber attacks”, *Business Standard*, 06 January 2013.
27. Pierre Mario Fitter, “Stuxnet attack wakes India up to threat to critical infrastructure”, *India Today,* 05 September 2012.
28. The term bot is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet.
29. Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyberweapon, although no organisation or state has officially admitted responsibility. However, anonymous US officials speaking to The Washington Post claimed the worm was developed during the Bush administration to sabotage Iran’s nuclear program with what would seem like a long series of unfortunate accidents.
30. Flame is modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. The program is being used for targeted cyber espionage in Middle Eastern countries.
31. Duqu is a computer worm discovered on 01 September 2011, thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu. Duqu got its name from the prefix “~DQ” it gives to the names of files it creates.
32. *Ibid.*
33. Nathan Thornburgh, “Inside the Chinese Hack attack”, *TIME,* 25 August 2005.

34. Indrani Bagchi, “China mounts cyber attacks on Indian sites”, *The Times of India*, 05 May 2008.
35. Sandeep Unnithan, “Inside the Indo Pak cyber wars”, *India Today*, 18 March 2011, http://indiatoday.intoday.in/story/cyberspace-china-india/1/226396.html, accessed on 18 February 2016.
36. “The United States Cyber Challenge”, *The White House Files*, 08 May 2009.
37. *Ibid.*
38. Ken Dunham, Jim Melnick, “Wicked Rose and the NCPH Hacking Group”, *An iDefence Research Report,* 2007.
39. More details about Tan Dailin and NCPH can be found in the chapter titled “Dragon’s Fire in the Virtual World.”
40. Ken Dunham, Jim Melnick, “Wicked Rose and the NCPH Hacking Group”, An iDefence Research Report, 2007.
41. “BSNL to open technical university, offer cyber security training”, *The Times of India*, 13 April 2014, http://timesofindia.indiatimes.com/tech/jobs/BSNL-to-open-technical-university-offer-cybersecurity-training/articleshow/33700956.cms, accessed on 08 March 2016.
42. Statement by Pentagon Press Secretary Peter Cook on DoD’s “Hack the Pentagon Cybersecurity Initiative”, *U.S. Department of Defence*, Press Release No. NR-070-16, 02 March 2016, http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe, accessed on 08 March 2016.