CYBER WARFARE AND NATIONAL SECURITY

E. DILIPRAJ

INTRODUCTION

In the wake of the 21st century, the cyber world began to spread its roots deep into the society and penetrated the lives of the people so much so that the internet became an indispensable part of the citizens' life, thus upgrading them to the status of 'netizens'. Moreover, technology in cyber space gained dynamism, increasing the population of netizens. This became possible in the cyber space not because all the citizens became technically sound but also because the cyber technology became more user friendly. Nevertheless, the height of the 'liberty to express' was readily available in the cyber space by virtue of the very low level of restrictions and legal barriers applied by the governments of the countries in the cyber space.

The cyber space began to grow in terms of information and also in the population of users with the passage of time. The users of the cyber space ranged from children looking for information for school assignments to business tycoons seeking profits; from the governments' e-governance services for the public to terrorists/non-state actors using it for their online communications and covert operations. As a result, in due course, this unregulated cyber space became a mine of information worth billions, thus, opening up a battleground for the netizens to acquire such vast information

Mr **E. Dilipraj** is a Research Associate at Centre for Air Power Studies, New Delhi.

Citizens of a country who were unable to express their hatred and fight against a rival state brazenly, found cyber space a suitable option.

and also to sabotage the same to fulfil their own motives. The important feature of this battle was that it did not require an army to fight it—an individual, capable of writing a few lines of codes and with a minimal level of expertise in cyber technology, could wage a war against a country.

This form of battle among the netizens in the cyber space is referred to by various terms like cyber crime, cyber war and cyber terrorism, depending on the nature of the perpetrators and the consequences. This also became the preferred form of the fight of the public against their perceived enemies ranging from an individual to a government due to the following reasons: the low level of restrictions and legal barriers, the anonymity and no casualties, and, most importantly, the indispensability of minimal resources and the need of infinitesimal people with little expertise. Almost all the countries of the world faced this challenge in their respective cyber space on a regular basis and it was more often experienced in the networks of rival states. In addition, citizens of a country who were unable to express their hatred and fight against a rival state brazenly, found cyber space a suitable option to vent their anger and hatred as it provided them a natural outlet and anonymity, along with the weapon of technology. In this regard, no country of the world was an exception in this cyber hate contest, including India and Pakistan.

India and Pakistan: The South Asian neighbours have fought three major conventional wars ever since their birth in 1947, until the end of the 20th century – in 1947-48, 1965 and 1971, and a smaller war in 1999. At the end of the 20th century, the tension between the two nations increased to its highest level, as both countries achieved the status of 'nuclear weapon states' after successfully conducting nuclear explosive tests for military purposes, one after the other. Although nuclear deterrence and other international pressures prevented these two countries from getting into another major war in the later scenarios, the hatred for each other in the minds of their citizens has only got aggravated. This hatred deepened when the state sponsored terrorism from Pakistan became the highest national security threat for India from the 1990s and the Indian armed forces were busy retaliating against it. The people were waiting for an opportunity to express their anger and hatred towards each other.

Actions of people in the cyber world against any network belonging to someone else are referred to as cyber attacks.

THE ICE BREAKER

As mentioned earlier, the world of cyber space advanced rapidly but with almost no regulations, resulting in vulnerability to the use of technological luxuries for immoral and anti-social purposes. As a result, this became the voluntary medium for the people to express their views and emotions to their targeted audience all over the world and they started using it for this purpose. These actions of people in the cyber world against any network belonging to someone else are referred to as cyber attacks and these started spreading all over the world with the number of incidents increasing over a period of time. They reached India on June 3, 1998, when the Indian website owned by the Bhabha Atomic Research Centre (BARC) came under a cyber attack by a group called 'milw0rm'. The attack was caused by breaching into the website of BARC and defacing the same. It was also found that the attackers had downloaded five megabytes of e-mails and data from the database.[1]The attackers claimed in their message in the defaced website that the attack was in response to the testing of nuclear weapons by India on May 11 and 13, 1998. The defaced website of BARC had a message from the hackers as follows:

> Nuclear Tests in India. This page has been hacked in protest of a nuclear race between India, Pakistan and China. It is the world's concern that such actions must be put to an end since nobody wants yet another world war. I hope you understand that our intentions were good, thus, no damage has been done to this system. No files have been copied or deleted, and

[1] http://ces.iisc.ernet.in/hpg/envis/doc98html/miscbarc69.html, as accessed on September 3, 2012, 11:30 am

> main file has been just renamed. Stop the Nuclear Race! We Don't Want a Nuclear Holocaust.[2]

At first, it was believed that these attacks were from Pakistani hackers backed by the Inter-Services Intelligence (ISI) but later, after a thorough investigation, it was revealed that hackers were individuals who only had contacts among themselves through the internet, were operating under their pseudonyms and belonged to different nations. The group consisted of teenagers who went by the aliases of JR, Keystroke, ExtreemUK, savec0re, and VeNoMouS[3]. VeNoMouS, 18, hailed from New Zealand, ExtreemUK and JR, both 15, from England, Keystroke, 16, from the US, and Savec0re, 17, from Russia.[4]

Although, the first major cyber attack faced by an important Indian website was not by Pakistani hackers, the initial blame on them which came as the immediate response from the Indian side clearly exhibits the level of suspicion due to the distrust in the minds of the people. However, the attack on the website was proved to be not an act of the Pakistani hackers. This incident was the ice-breaking one which cleared the way for future cyber attacks between these two countries' netizens. After this incident, in the year 1999, there were four attacks on Indian cyber networks that were recorded and the investigations revealed that these were carried out from Pakistan. This count increased drastically to 72 in the year 2000, and there were also reports confirming seven attacks in 1999 and 18 attacks in 2000 on the Pakistani networks conducted from India.[5] Thus, a mutual cyber hatred contest began without much fanfare in the cables between the netizens of India and Pakistan.

This saga of the cyber hatred contest continued even in the 21st century where the first half of 2001 witnessed 150 incidents of defacing of websites on the Indian side; they also took place the Pakistani side but in comparatively

[2] http://www.youtube.com/watch?v=XcL9EqUbg4Y, as accessed on 3/09/2012, 11:45 am

[3] William C. Boni & Gerald L. Kovacich, *I-way Robbery* (UK: Butterworth-Heinemann, 1999), p. 142.

[4] "India: Sahara India Mass Communication," *Rashtriya Sahara*, 1996.

[5] Iftikhar Alam, "Pakistan India Cyber War Begins", *The Nation*, December 5, 2010.

fewer numbers[6]. Such cyber hatred attacks on both sides kept increasing every year and the victims of these cyber skirmishes were the key websites of both countries. Mr. Munawwar Iqbal, President of the Pakistan Computer Association (PCA) once stated in an interview:

> As per my information, there are two groups of hackers from both countries: one is called the Indian Cyber Army and the other is known as the Pakistan Cyber Army. Both are in competition to hack each other's websites. It is totally illegal, and should be stopped in the greater regional and international interest, as well as that of both countries' people. [7]

In the meantime, many new hacking groups started emerging and displaying their skills in the networks. Of these, one of the most notorious and dangerous groups originated from Pakistan – this was the Z Company Hackers Crew (ZHC) which has a record of attacking 1,846 Indian websites, both government and civilian.[8] There are also other hackers groups like Pakistani Hackers Club (PHC) whose founder is claimed to be from Karachi, and the G-Force, which is believed to be consisting of eight members, is from Lahore.[9]

On the Indian side also, there was the emergence of many groups of which H2O or the Hindustan Hackers Organisation[10] is famous among the cyber hacking community and another group called TEAM NUTS that did a record hacking and defacement of 57 commercial sites in Pakistan in one day in 2010.[11]

THE SPILLOVER EFFECT

As the cyber contest was nurtured on hatred and anger, growing day by day among the private hackers groups of India and Pakistan, it led to an increase

[6] Alamzeb Khan, "Pakistan Cyber Warfare and Internet Hacking", January 17, 2012, URL: http://www.simple-talk.com/opinion/opinion-pieces/pakistan-cyber-warfare-and-internet-hacking/

[7] Ibid.

[8] http://www.hackread.com/read/hackread/3289

[9] Alam, n. 5.

[10] Ibid.

[11] http://thehackernews.com/2010/12/57-pakistani-websites-hacked-by-team.html

in the number of cyber attacks exchanged between them. Although this became a daily affair of the private hackers of both countries, it remained unrecognised and was not considered a threat to national security by either the Indian or Pakistani government. But the spillover effect of this cyber contest soon came into the limelight.

As the various cyber hacking groups in both countries were waiting on a standby mode for an opportunity to sabotage the other in a massive way, the D-Day finally arrived on November 26, 2010, the second anniversary of the 26/11 Mumbai terror attacks. On this day, the members of the Indian Cyber Army (ICA) launched an all out attack on 870[12] Pakistani websites out of which 34 were crucial government websites belonging to the Pakistan Navy, Maritime Security Agency, Foreign Ministry, the Chief Minister of Sind, etc. The ICA spokesperson stated, "Our objective of launching cyber attacks was to pay our homage to the martyrs of 26/11," on the website called Hacker Regiment.

This act of the ICA instigated the hacker groups in Pakistan, and their most powerful group called Pakistan Cyber Army retaliated with a similar all out attack on December 3, 2010, on the 39th anniversary of the 1971 Indo-Pak war by attacking 270 [13] Indian websites of which the worst affected was the website of the Central Bureau of Investigation (CBI) which remained offline for almost one month after the attack before being revoked with great difficulty. The entire software had to be tested and revalidated again before making it available online. It was later identified by the Department of Information Technology that the hackers who attacked the CBI website were based in Peshawar and they had used an Indian Air Force website as a back gate to enter into the CBI website which shared the same database and this became a major security lapse.[14] The hacked CBI website had a message saying:

> This attempt is in response to the Pakistani websites hacked by 'Indian Cyber Army'. We told you before too... we are sleeping but not dead..

[12] Sandeep Unnithan, " Inside the Indo Pak Cyber Wars", *India Today*, March 18, 2011.

[13] Ibid

[14] Khan, n. 6.

> Remember PCA (Pakistan Cyber Army)! back off kids or we will smoke your d00rs off like we did before.. let's see what your investigating agency, so-called CBI can do for you or for us! Haha.. one more attempt from your side.. We got your every website lying around here like its our local server! Buahahaha...so we would like to say to your 31337 hackers and your 31337 NIC team go and read some more books... you guys are seriously bunch of script_kiddies!..you know nothing rite now..got r00t access to NTC server? Wtf mass defacements...how about something like this...a planned attack! Haha...btw we got r00t to your NIC too :P.. Your filtering sucks... have fun! And DO NOT DISTURB... we got better things to do.. :D.. stop complaining about Pakistani websites security.. secure your own ass first..thats what intelligent people do!..lol..tata.:D.[15]

In retaliation, the ICA attacked and defaced the website of the Oil and Natural Gas Regulatory Agency (ONGA)[16], the Pakistani counterpart of the Oil and Natural Gas Commission (ONGC) of India on December 4, 2010. The defaced website of ONGA had the following message: "You Have Been Hacked by the INDIAN CYBER ARMY This Is a Retaliation of Hacking 'CBI."[17]

Pakistani government sources claimed that the attacks on 870 of their websites on November 26, 2010, were planned and executed by India's technical intelligence agency called the National Technical Research Organisation (NTRO) by hiring hackers for their offensive cyber operations which was never proved. Similarly, India also accused Pakistan's ISI for the attack on December 3, 2010, on 270 of its websites and, most importantly, the website of the CBI, which was the most affected. India also claimed that the ISI had recruited hackers for waging a cyber war against India.

These attacks carried out by the Indian and Pakistani hacker groups on each other's cyber networks during the months of November and December 2010, are considered to be among the major cyber attacks that have ever taken place between any two countries of the world without

[15] www.cbi.gov.in/index.php, accessed on December 3, 2010.

[16] Alam, n. 5.

[17] www.Hackerreginet.com

their governments' support. Nevertheless, these attacks are seen only as a prelude to a much bigger contest in the cyber space between India and Pakistan in the future.

However, these attacks carried out by the private hacking groups of both India and Pakistan succeeded in catching the attention of the governments. Immediately after the attacks, a multi-level meeting was called by Mr. Sachin Pilot, India's Minister of State for Communication and Information Technology, from the various agencies like CBI, NTRO and National Informatics Centre (NIC) to discuss the issue[18]. Although the hacking saga faded away after the government's intervention, the hacking groups of both countries now claim to have easier access to the other's cyber networks. "We still own many servers of Pakistan and are prepared to respond to any attack from the PCA or any other Pakistani hacker group," says 'Disfigure' a hacker from the ICA[19].

Although many small cyber skirmishes and cyber attacks took place after the major cyber clash between the hackers of India and Pakistan, they were not considered harmful until the situation became intense again on January 26, 2012, when India geared up to celebrate its 63nd Republic Day. An India-based hacker group called 'Jaguar Hacker' defaced 21 Pakistani websites and posted a message saying: "Nothing Personal But It's Just That Today Is Our Republic Day.. :)).Don't worry nothing has been deleted... Just Index page renamed (*sic*)."[20]

In retaliation to this, the famous hacking group from Pakistan, Z Company Hacking Crew hacked some 400 websites of India and posted:

> You claim to be the largest democracy in the world but when it comes to Kashmir and Kashmiri people, you tend to forget all your democratic principles. You kill our fathers, our brothers, shoot down teenagers point blank and detain them under draconian laws like PSA without even giving them a fair trial, you rape our sisters and mothers. After years of atrocities

[18] Unnithan, n. 12.

[19] http://www.civilspedia.com/2010/12/indiaica-pakistanpca-cyber-army-warfare.html, as accessed on 13/09/2012, 14:20 pm

[20] http://www.mid-day.com/news/2012/jan/280112-Indo-Pak-cyber-war-on-Jan-26.htm

> and oppression we say that we will Rise and Rise Again ... Until Lambs become Lions !!!(*sic*).[21]

WHY DOES THIS MATTER SO MUCH?

The cyber attacks between India and Pakistan (by the various hacking groups of these countries) were not a surprise for the cyber technology management groups as they encounter such activities regularly. According to a report from the Computer Emergency Response Team of India (CERT-IN), it has an account of around 3,600[22] Indian websites that were hacked in the first half of the year 2010, which amounts to approximately 20 hacking instances per day. There are also reports of 774 government websites that have been hacked in the last five years. In spite of all these reports, it is unfortunate to know from many independent cyber security observers in India that despite regular reports of hacking incidents, the government organisations have not been vigilant enough to take the necessary steps to improve any sort of security to the Indian cyber networks. It has been reported after an audit that out of about 7,000 Indian government websites, only 3,192 have been audited for Information Technology (IT) security, while 3,556 others are being audited. Yash Kadakia, head of Security Brigade, a government-empanelled security auditor says,

> According to our data, about half the government websites are vulnerable to cyber attacks. Most of the government websites do not have proper security checks in place.[23]

The same kind of lethargy prevails on the Pakistani side in securing their cyber infrastructures. When asked about the steps taken for management of security to the Pakistani cyber networks, a senior official in the Electronic Government Directorate (EGD), the agency officially responsible for monitoring the hacking saga in Pakistan said,

[21] Ibid.

[22] "India and Pakistan in Cyber Warfare", *Al Jazeera*, December 4, 2010.

[23] Piyali Mandal, "Half the Govt Websites in India are Prone to Cyber Attacks", *Business Standard*, January 6, 2013.

> The government has so far secured only 33 websites belonging to government ministries and departments, out of thousands of official government websites. And there is no system that can't be hacked. You can break any kind of lock, and the same is the case with hacking websites. The government never demonstrates seriousness in dealing with the hacking problem, which poses a constant threat to all state and privately-run websites.[24]

While aggression is the only tactic followed by the hacker groups in both countries, on the contrary, the security providers for the cyber space have always been lacking in 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,' "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 stopped with the hacking and defacing of websites. But, in reality, it moves on to the next stages. The same people who carry out hacking and website defacing jobs may get involved in cyber espionage and data mining against their enemies. These people may also volunteer their expert services to the terrorist organisations in return for money and other forms of remuneration. According to a cyber security professional working with one of India's intelligence agencies,

> We once sat down to check the Delhi [internet] Backbone. We found thousands of systems compromised. All were government systems, Research and Analysis Wing, Intelligence Bureau, Military Intelligence... we don't realise how much damage has already happened.[25]

[24] Khan, n. 6.

[25] Pierre Mario Fitter, "Stuxnet Attack Wakes India Up to Threat to Critical Infrastructure", *India Today*, September 5, 2012.

The lack of awareness and the lethargic approach in monitoring and providing security to the cyber networks by India led to thousands of compromised computers across the country. The infection ranges from small Viruses, Botnets[26] to that of Stuxnet[27] level malwares which can hamper the total operations of the network connected to the compromised computer. It has been observed that out of the 10,000 Stuxnet infected Indian computers, 15 were located at critical infrastructure facilities. These included the Gujarat and Haryana Electricity Boards and an ONGC offshore oil rig. Though Stuxnet reached the networks of these infrastructures, thankfully, it did not activate itself on them. In other words, India was only a few flawed lines of code away from having its power and oil sectors crippled.[28]

The list of new malwares goes on – Stuxnet, Flame[29], Duqu[30], etc – and many more are in the process of coding; their abilities to operate as cyber weapons are incredible and, at the same time, unbearable, if not protected against properly. Assuming that the hacker groups get access such malwares, then the situation would become extremely dangerous for the national security as it is equivalent to terrorists getting access to nuclear weapons. While talking about the same, Mr. Sachin Pilot, Minister of State for Communications and Information Technology said:

[26] 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.

[27] It is believed that Stuxnet was jointly programmed by the US and Israeli intelligence as part of a project called Olympic Games in order to sabotage Iranian nuclear facilities. It spread from computer to computer, hunting down the exact one that controlled Nantanz's centrifuges and caused big damage to it. It was reported that around 2,000 centrifuges in the Nantanz facility were damaged due to this Stuxnet attack. But a flaw in Stuxnet's code caused it to spread further than planned, infecting more than one lakh other machines worldwide.

[28] Fitter, n. 25.

[29] Flame is a modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. The programme is being used for targeted cyber espionage in the Middle Eastern countries.

[30] Duqu is a computer worm discovered on September 1, 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.

> 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.[31]

A careful study of the series of hacking on one another's websites and networks by the private hacking groups of India and Pakistan would reveal a basic fact that something which started as a small act of hate has now taken on a much different shape 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 unwanted event that disturbed the internal security of India in August 2012. The Indian government was alerted by the exodus after thousands of people from the northeast gathered at railway stations in various cities all over the country after being threatened by the rounds of SMS and violent morphed pictures that were being circulated on more than 100 websites. The SMS threatened the northeastern people living in various cities in India of a targeted attack on them, asking them to go back to their homeland, whereas the pictures circulated on the internet were images of some violent bloodshed. Out of the various SMS that were in circulation, one said:

> It is a request to everyone to call back their relatives, sons and daughters in Bangalore as soon as possible. Last night, four northeastern guys were killed by Muslims in Bangalore (two Manipuri, two Nepali). Two Nepali girls were kidnapped from Brigade Road. The reports say that from August 20, marking Ramzan, after 2 pm, they are going to attack every north-eastern person. The riot started because of the situation in Assam.[32]

Another SMS said:

> Many northeast students staying in Pune were beaten up by miscreants believed to be Muslims following the Assam riots. Heard that it is happening

[31] Ibid.
[32] "TRAI Tracking Panic-Spreading SMS"; *The New Indian Express,* August 17, 2012.

> in Muslim areas like Mumbai, Andhra Pradesh, Bangalore. At Neelasandra, two boys were killed and one near passport office.[33]

The Government of India reacted soon on this matter and a 43-page report was prepared by intelligence agencies along with the National Technical Research Organisation (NTRO) and India Computer Emergency Response Team (CERT-IN) which traced several doctored images to Pakistan. The origins of these morphed images were later traced back in specific to Lahore, Rawalpindi and other Pakistani cities by the Indian intelligence agencies. "From all available forensic evidence, we are fairly convinced that all those postings came from Pakistan," said an official of NTRO.

Another senior official who has been involved in India's Pakistan watch for several years said,

> It has been happening for several months now. This is a low cost, very effective way of destabilising us. They don't need to send terrorists and explosives to create mayhem. Internet has been a very effective platform for instigating communal divisions in India. They also have a multiplier effect, first resulting in anger and hatred, then riots and, finally, many taking to terrorism.

This act of unnecessary involvement by Pakistan-based elements is seen as cyber terrorism and cyber psychological warfare against India to cause internal security disturbance and eventually to create a huge crisis in the country. This incident which created major turmoil in the internal security of the country is the biggest example of the adverse effects of wrong use of cyber technology.

WHAT COULD BE DONE?

Any anti-social element, be it an individual or a hacking group, and whatever may be its motive, would certainly need a lot of time to study, analyse

[33] Ibid.

There is also a need to increase the number of cyber security experts and IT security auditors, in which the country is facing a crisis at present.

and make the required arrangements in order to penetrate the existing security system. If such elements can spend so much time and effort to plan and carry out an attack, why cannot a country like India, which claims to have a pool of talent in the IT sector, make an attempt to secure its networks and websites with the available talent? This would be possible only when there is political will to address the issue, which India is lacking but the consoling fact is that realisation is now slowly dawning. Also, India’s legal system needs to be upgraded towards enhanced cyber laws as its present form is still dwelling on the IT Act 2000, IT Amendment Bill 2006 and IT Amendment Bill 2008 which are unable to cover all forms of the problem in a field which is racing ahead every single day. Finally, there is also a need to increase the number of cyber security experts and IT security auditors, in which the country is facing a crisis at present. Currently, the number of IT security auditors stands at 60 in India.[34] J. Satyanarayana, the Information Technology Secretary of India stated, “We need five lakh professionals to protect our cyber space. We only have a small fraction of this”[35]

For India, it is not only Pakistan that challenges its security in the cyber front but there is always the Red Giant Cyber Dragon – China – above India, which has more a advanced and organised form of cyber army, with which it challenges even the United States through cyber espionage operations like ‘Titan Rain’[36]. It is believed that the Chinese cyber warfare policy is based on the 6th century B.C. Chinese strategist Sun Tzu regarding, “the art of fighting without fighting”. There have already been instances between India and China where officials in the Indian government have alleged that attacks on Indian government networks, such as that on the Indian National Security Council, have originated in 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

[34] Mandal, n. 23.

[35] Unnithan, n. 12.

[36] Nathan Thornburgh, “Inside the Chinese Hack Attack”, *TIME,* August 25, 2005.

Huawei, due to their ties with the Chinese military.[37] India's intelligence agencies have warned about Huawei's penetration into the Indian telecom. Their worst fear is that the Chinese firm could be a Trojan horse, meant to infiltrate India's network in peace-time and disable it through remote 'kill switches' in war-time, through hidden 'trapdoors' and malicious programmes that could then open a channel back to its designers.[38] In 2010, the cyber attacks on the computers of India's National Security Adviser's (NSA's) office, Indian Air Force and Indian Navy are suspected to have originated 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 join hands in the future for cyber offensive operations against India. In order to avoid such extreme situations, the Indian government should take quick measures to identify the real people behind these hacking sagas on the Indian side and rehabilitate those who are deserving, and recruit them into its cyber security infrastructures. As most of the hackers are teenagers, this act of converting the 'Black Hat Hackers' into 'White Hat Hackers' would be the right step for the government to get its hands on them and mould them. This will not only give a future to these youngsters but will also create a strong cyber security culture in the country. Also, India is fortunate to have pool of talent in the private IT sector which can be fruitful if used in the proper way. The experts of cyber security in the private sector can be invited to train the government cyber security professionals and can help in conducting security drills from time to time in the government and other cyber networks of the country. Extremely efficient and reliable government cyber security civilian professionals can, in turn, be used to train the defence cyber security personnel so that not only the security of the networks is updated but also it helps in a broader perspective of national interest in the years to come with regard to both national and cyber security.

[37] Indrani Bagchi, "China Mounts Cyber Attacks on Indian Sites", *The Times of India*, May 5, 2008.
[38] Unnithan, n. 12.