Social Networking: Boon or Bane for the Armed Forces

*Suyash Sharma**

The social networking sites can be exploited by the cyber operators by infiltration and influencing the opinion where feasible. Cyber espionage has already became the cornerstone of some nations, where international cyber security agencies have reasons to believe, of state complicity in major hacking, denial of service attacks in the last couple of years. Since social networks become easy prey to such agencies, there is a need to increase awareness of defence personal about their vulnerabilities.

"No man is an island" said John Donne, i.e. human beings do not thrive when isolated from others. Donne was a Christian but this concept is shared by other religions, principally Buddhism.[1] Homo sapiens are social animals and isolation or seclusion generally sends shivers down their spines. Mandela and Syu Ki are revered as they could withstand this ordeal during their prolonged incarceration. Social networking is, thus, an emotional and psychological need. Since times immemorial men have sought ways and means of socialising, and the elaborate means of communication available today are precisely to fulfil that need. The media, of course, kept evolving from speech to voice transmission to present day live video streaming and who knows tele-transporting would cease to be in the realms of sci-fi in the days to come.

With the advent of internet, networking at organisational level was achieved, but it took Mr Sabir Bhatia to conjure up the hotmail and soon the flood gates had opened. Today there is a plethora of social networking sites available and more often than not, the geeks are hopping from one to the other in a flash, i.e. from Facebook to Twitter to LinkedIn to Orkut or YouTube, MySpace and many more, these sites are commonly referred to as Web 2.0. All of these appear in a ranking of the world's most popular networks by total monthly web visits, which also includes Orkut, a Google owned service that is heavily used in India and Brazil, and QQ, which is big in China. On top of these, there are other big national community sites such as Skyrock in France, VKontakte in Russia, and Cyworld in South Korea, as well as numerous smaller social networks that appeal to specific interests such as Muxlim, aimed at the world's Muslims, and ResearchGATE, which connects scientists and researchers; they obviously have only disdain for the snail mail types.[2]

* **Colonel Suyash Sharma** is a Directing Staff at DSSC, Wellington.

These sites are very inviting for the networking hungry generation of today. Instant gratification is the need of the minute not of the hour. The youngsters naturally took to them like ducks to water and gradually the older generations have also caught the bug. Through these sites, they are trying to look for those lost threads of friends who have gone into oblivion of adult hood, on growing up in different parts of the globe. On the flip side, these started to intrude on our closely guarded privacy and security conscious organisations are at a loss as to how to prevent breaches in security which is bound to occur through these portals.

As a democratic society one has to let these “hundred flowers bloom”, but for a security conscious organisation, this is anathema, potential threat in being.

As a democratic society one has to let these “hundred flowers bloom”, but for a security conscious organisation, this is anathema, potential threat in being. Social networking has already profoundly redefined business practises-think e-bay and Craiglist. The impact of social networking will not end with business and politics. National security is next.[3] Our armed forces are also in a state of transition from the strictly reclusive and cocooned organisation to a vibrant and lively one where, our soldiers, sailors and airmen are increasingly seeking to join the mainstream. In fact, it is no longer possible to quarantine them from outside influences unlike in the bygone era. The unfolding revolution has engulfed even our organisation and unless we find ways and means of exploiting this medium to channelize our troops, it may just slide into an abyss, a sort of anarchy which needless to say would spell doom. It is a crying need and it just cannot be wished away. So far we have adopted an ostrich like attitude of waiting for the storm to subside but any further delays will simply be too late.

We have service specific wide area networks which cater to our day to day official correspondence but there is no medium for our personal requirements. The system of field post offices was evolved primarily to cater to the soldiers’ need for communication with their families back home in the 20th century and it provided succour when they needed it most. A letter from home revived sagging morale and brought cheer on their faces, ready to take on the world again for a couple of weeks, till the next one arrived.

Now the situation has changed with this requirement of communication having become a daily need and at times even hourly one. We can debate on the issue whether this is a healthy trend, but the fact remains that it is the need of the hour. In the absence of availability of any official means, they have simply grabbed what is easily available outside. Even a layman would understand the consequences of this mindless proliferation, naturally our closely guarded citadel has been stormed and we have been simply overwhelmed. In the armed forces where we are bound by certain regulations regarding communicating in the open domain, there are gag orders, i.e. persons in uniform are not supposed to be members of any of these social networking groups. Obviously it is with noble intentions but at the same time it reflects our knee jerk reaction to this situation where we have been caught unaware and are simply reacting in the manner best known to us. Fundamental reforms will be required for conducting national security in a world driven by global listening.[4] The government of the day must first comprehend the nuances of this tool and then proceed to exploit it to gain ascendancy in the cyber domain.

The Web 2.0

Why are these social networking sites so popular and appealing? Apart from meeting the emotional and psychological need, these cater to their common attributes, tastes, interests, causes or activities. The group dynamics are naturally different from each member of the group as they evolve and acquire a unique dimension of its own. A social network is a complex system. When systems become complex, their behaviour cannot be easily predicted by traditional methods of analysis.[5]

> Apart from meeting the emotional and psychological need, these cater to their common attributes, tastes, interests, causes or activities.

While social networks are not the sole preserve of the internet, as mentioned above, they have proliferated remarkably since 2003. This was primarily due to the quantum leap in storage capacity of personal machines accompanied by reduction in cost and development of software for storage and retrieval of data. These softwares facilitated the posting and hosting of blogs, video clips, photographs and audio clips. The popularity of new web tools and services is remarkable. MySpace, for example, established in 2003, had 80 million members and hosted more than 6 million web pages within three years.[6] In precisely nine years, Wikipedia has grown to be the largest repository of knowledge thereby making the Britannica and Encarta redundant. The Wikipedia is dynamic as it is updated by the users themselves and hence remains current. Facebook and twitter have made e-mails passé and the convergence of computer with communication enabled the mobile phone makers to provide this connectivity in the palms of the users thereby helping it mushroom to such gigantic proportions. Simultaneously, other new and different social networking is likely to emerge in the future as nanotechnology and new materials are developed that could greatly reduce the weight, cost and power requirements for information sharing technologies.[7]

Threats

Is it too late already or can we take certain measures to address this issue? Let us start with the threats first, internet. Facebook, the globe's largest online social network boasts over 350 million users, which would make Facebook the world's third most populous after China and India. That is not the only striking statistic associated with the business. Its users now post over 55 million updates a day on the site and share more than 3.5 million pieces of content with one another every week.[8] Some of us may seek refuge behind the argument that our troops have not reached this level of computer awareness as yet, well then it would come as a rude shock to you that almost 20 per cent of our troops have access to the net on a daily basis and about 10 per cent are actively using it. Mind you, we are talking about a 1.1 million strong army; hence even these numbers are scary to say the least. But are our officers security conscious, far from it, in fact a casual browse on facebook or the number of school/college and other associations which have conglomerated into web-groups, would reveal that our officers share information like their designation, telephone and mail contacts as also the nature of work they are indulged in a routine manner.

A casual browse on facebook or the number of school/ college and other associations which have conglomerated into web-groups, would reveal that our officers share information like their designation, telephone and mail contacts as also the nature of work they are indulged in a routine manner.

We have also had a few instances when officers' computers have been compromised. The computer of the officer, who is stationed in the Andaman and Nicobar Islands, had been emailing critical information from the system to a Pakistani email account. The tip-off, according to the *India Times*, came from the U.S. Intelligence Agency. An Army investigation has found that the information e-mailed from a Major's computer was a case of "cyber security breach" and not espionage, said Defence Minister A K Antony.[9] Indian probe agencies are looking into the possible role of two senior army officers in a suspected espionage ring, following the hacking of the computer of a major based in the Andamans. Two senior officers of the Integrated Defence Staff (IDS) could be called for questioning soon, the sources said, but refused to give their rank or designation.[10]

The threats envisaged in the cyber space are not just innocuous eavesdropping variety but more serious espionage as also destruction or corruption of own data-bases. Once the computers are compromised the victim is at the mercy of the hacker. He may choose to simply monitor or when the time comes wreak havoc on the system as a whole and not just at the individual computer. On the net malware, spywares are common modes through which these hackers cease control of the processors and the applications being run on them. These are introduced through innocuous mails, advertisements and sometimes by merely by getting on the net itself. Malware, short for *malicious software*, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or programme code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. Software is considered to be malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, crimeware, most rootkits, and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of several U. S. states.[11] The most common route for these malware introduction are to a large degree organised and operated through the misuse of social networking and cloud computing platforms, including Google, Baidu, Yahoo, and Twitter, in addition to traditional command and control servers.[12] Malware samples from a variety of attacks were collected that determined the exploits the attackers used, the theme used to lure targets into executing the malware, as well as the command and control servers used by the attackers. Malware samples consisted primarily of the files with the PDF, DOC, PPT and EXE file extensions.[13]

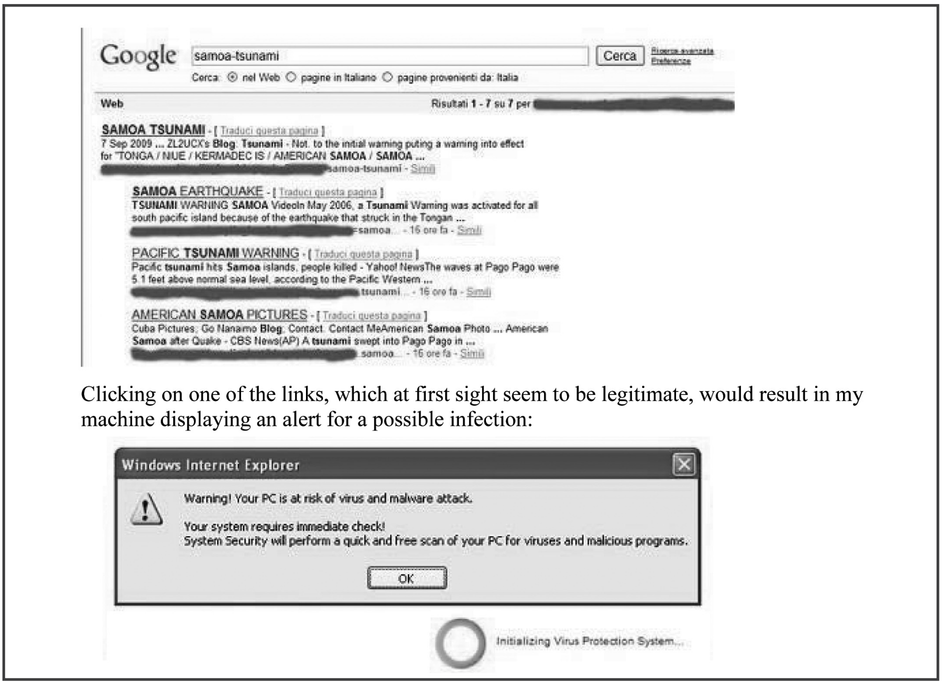
How did the individuals behind the Ghostnet espionage ring manage to entice so many people (1300 computers in 103 countries) to open an infected document which loaded a Chinese Trojan named *ghostRAT* onto their systems? They crafted an enticing e-mail and document that was tailor made for their audience-supporters and/or employees of the Office of His Holiness the Dalai Lama. It was such an effective social engineering campaign that 30 per cent of the infected computers were in sensitive government offices. Most anti-virus softwares failed to identify the Trojan.[14]

These networks are ideal hunting ground for our adversaries looking to collect actionable intelligence on our personnel, both in the defence and bureaucracy. According to a recent study conducted for one of the US Armed Services, 60 per cent of the service members posting on MySpace have posted enough information to make themselves vulnerable to adversary targeting. The details included their first and family names, their home state, their present duty location, public account and their job profile.[15] The way it works is that Facebook's partner firms install Connect buttons on their websites and devices which give Facebook users automatic access to information about their friends' activities. At Huff.Po Social News, a site run by the Huffington Post, a well known American blog, Facebook users can see what their friends have been reading and exchange stories and comments with them. At Netflix, which hires out DVDs and Blu-ray discs by post, they can see which films their friends have watched and what other people have written about them.[16]

> These networks are ideal hunting ground for our adversaries looking to collect actionable intelligence on our personnel, both in the defence and bureaucracy.

The second risk category is disinformation or rumour mongering/propaganda. It is reported that in Mumbai terrorist attack of 26/11, there was a deluge of tweets regarding the reported sighting of terrorists at a number of other places, thus, adding to the chaos and confusion prevailing in the decision making hierarchy. Then, the aspect of faking the identity or identity theft, i.e. cyber impersonation to gain the confidence of the group and then elicit information on that mistrust. Recently even Dr Amartya Sen, the Nobel laureate had fallen prey to this, where someone had pre-empted him and used his identity to create his own facebook account. Through this medium he was propagating views contrary to those of the Nobel laureate.

Fraudulent security software, also called fake AV, fake alert, and rogue anti-virus - continues to plague both enterprises and consumers. Do not be fooled by the slick GUI or frightening reports they give. These are scams designed solely to trick unsuspecting users into parting with their money. One of the most common ways of distributing fake AV is through poisoned search engine results or seizing on disasters or celebrity deaths.[17]


Google
samoa-tsunami
Cerca
Ricerca avanzata
Preferenze
Cerca: ● nel Web ○ pagine in Italiano ○ pagine provenienti da: Italia
Web

Risultati 1 - 7 su 7 per [redacted]

SAMOA TSUNAMI - [Traduci questa pagina]
7 Sep 2009 ... ZL2UCX's Blog: Tsunami - Not. to the initial warning puting a warning into effect for "TONGA / NIUE / KERMADEC IS / AMERICAN SAMOA / SAMOA ...
[redacted]samoa-tsunami - Simili

SAMOA EARTHQUAKE - [Traduci questa pagina]
TSUNAMI WARNING SAMOA VideoIn May 2006, a Tsunami Warning was activated for all south pacific island because of the earthquake that struck in the Tongan ...
[redacted]samoa... - 16 ore fa - Simili

PACIFIC TSUNAMI WARNING - [Traduci questa pagina]
Pacific tsunami hits Samoa islands, people killed - Yahoo! NewsThe waves at Pago Pago were 5.1 feet above normal sea level, according to the Pacific Western ...
[redacted]tsunami... - 16 ore fa - Simili

AMERICAN SAMOA PICTURES - [Traduci questa pagina]
Cuba Pictures; Go Nanamo Blog; Contact. Contact MeAmerican Samoa Photo ... American Samoa after Quake - CBS News(AP) A tsunami swept into Pago Pago in ...
[redacted]samoa... - 16 ore fa - Simili

Clicking on one of the links, which at first sight seem to be legitimate, would result in my machine displaying an alert for a possible infection:

Warning! Your PC is at risk of virus and malware attack.

Your system requires immediate check!
System Security will perform a quick and free scan of your PC for viruses and malicious programs.

Initializing Virus Protection System...

Figure: Disasters are prime fodder for fake AV designers. These images, based on the Samoas earthquake and tsunami, appeared in a McAfee Labs blog by researcher Patrick Comiotto.[18]

Phishing Activity

Phishing is a term associated with stealing the vital data by impersonating/ masquerading as a genuine site and leading the user to reveal important data. It continues to evolve into new forms and tactics. Late in the quarter the fake IRS notice of "Underreported Earnings," associated with Zeus, was very popular. We also saw PayPal phishaggressively distributed via SMS as well as email that claimed "Your MailBox is over the required size. You will not receive or send further email messages until you contact us here." Some of these tactics are very effective.[19]

This list of threats is by no means exhaustive, as everyday there are new methods being evolved to hone the skills of cyber warriors/criminals, both hand in glove, using similar means to achieve their own objectives.

Alternatives

Since the need for social networking is well established and high pressure professions such as armed forces being even more dependent on such activities, there is a definite need to formalise it. As of now, army personnel are prohibited from participating in such activities, but such a gag order is difficult to be monitored, nor is it desirable. Troops need to get in touch with their near and dear ones more often, as the families back home are no longer living in the protective cocoon of joint families. Today, the number of soldiers using the net for such activities may be small, but cell phones are available with all and sundry. Soon majority of them would rely on this medium to keep them connected. The need for securing our exclusive service networks is paramount, and it can be ensured by keeping the internet enabled PCs totally separate in the units. These PCs should not be in the same room/premises, as even inadvertently this slip up can prove very dangerous.

But that still cannot justify this gag order. In fact, need of the hour is to establish virtual private networks, duly firewalled, for personal use only with facility to log in from anywhere. These networks could ride on civil networks/media available or the services could use its own available bandwidth for the purpose. Naturally, the civil media would be preferable, both for ease of access, as also for security reasons. This network could then enable 3G/ 4G value added services also for ease of access through cellular phones as well.

The idea may appear to be too far-fetched right now, but a closer scrutiny would provide obvious advantages accrued. We could also establish kiosks at each level, which could be co-located with the Field Post office detachments. These kiosks should provide the connectivity free of cost, time stipulations could be laid down. Initially, these may be inadequate but slowly these could be extended down to battalions/company /platoon posts.

We in the armed forces need our very own cyber groups, it is a very important forum for our personnel in uniform. Today, our men and their families have enhanced levels of awareness, where they can voice their opinion without fear or favour. This forum will fulfill a long outstanding need. Old timers would scoff at such an act and would probably term it as sacrilege, but it is better to have them vent their feelings in house rather than in open source, where they are highly vulnerable to subterfuge by the adversaries cyber espionage means.

In the interim, and even after these networks are in place there is need to increase awareness of men in uniform about their vulnerabilities on this medium as also the rudimentary protective measures which are mandatory for first level of security.

Force Multipliers?

These networks can be exploited by the cyber warriors, who could be snooping on the adversaries round the clock for breaches in security. More importantly, they could infiltrate into these groups and influence the opinion where feasible. Cyber espionage has already become the cornerstone of some nations, China in particular, where international cyber security agencies have reasons to believe,

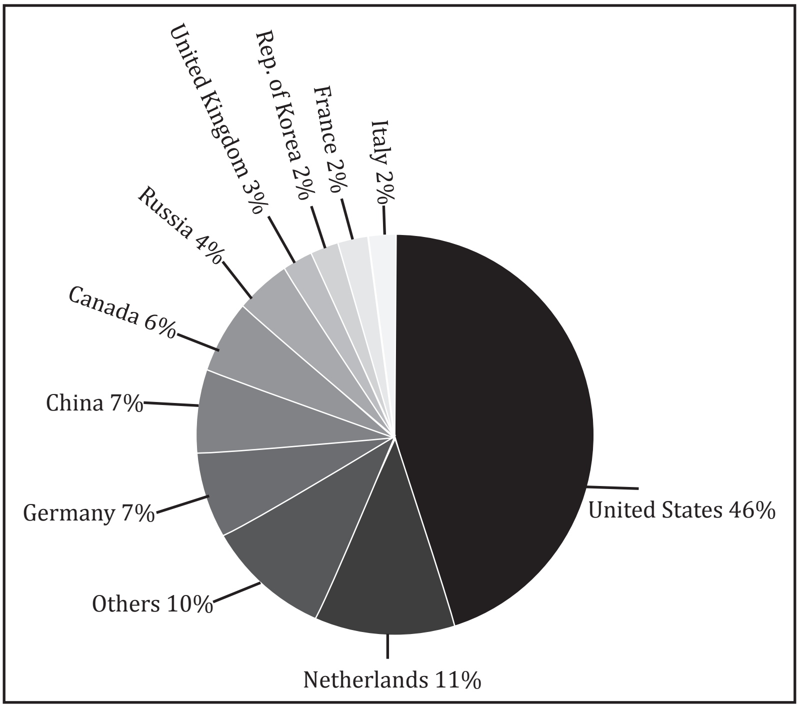


Figure: Distribution of phishing websites.[20]

of state complicity in major hacking, denial of service attacks in the last couple of years. Since these are clandestine operations, obviously any of our agencies' involvements in similar pursuits are not in public domain. But international monitoring organisations have some statistics where, Indians do not figure anywhere, whereas the Chinese and the Russians are on top of the charts. Either we have been too good to have not got noticed, or we have not ventured into this field, the way it should be exploited.

Cyber warfare is a serious enough threat to be pegged as the number 3 priority in the Federal Bureau of Investigation (FBI)'s list even way back in 2002. Indian authorities, however, just don't seem to get the seriousness of the situation, deploying far less than what is required to combat cyber-attacks, said independent cyber security consultant Ankit Fadia in Kolkata.

"According to Nasscom, India needs about 77,000 ethical hackers every year to fix the situation and we are not even producing half of them," says Fadia, addressing the media after his session with the students. Fadia claims that there are cells where the Chinese government actually trains and operates cyber mercenaries who incessantly keep attacking Indian, American and Japanese websites mostly belonging to the governments and some even to the corporates.[21]

Protective Measures

- **Audit of Personal Information Posted:** Information posted on these sites which could be misused, such as photographs, professional details, address, telephone, mail contacts or information about one's schedule or routine. It is important to ensure that one's contacts also are careful not to post this vital information at their end.

It is important to ensure that one's contacts also are careful not to post this vital information at their end.

- **The Networking Site is in Open Domain:** Information once shared cannot be retracted, hence only that information should be posted which has no security value. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines. This includes information and photos in one's profile and in blogs and other forums.

- **Strangers are not to be Trusted:** Even if a person claims to be someone, remember it is his virtual identity that one is interacting with. This identity could have been a stolen one. Hence always confirm their authenticity through other sources before confiding in them. Classified information is still an anathema though.

- **Be Aware of Rumour-mongers:** Information on the net need not be treated as gospel, as this could be planted to mislead and create confusion. These could also be ideally utilized for fifth columnist propaganda.

- **Customise Settings:** The default settings for most of these sites allow open access to one's profile. Customize the settings to restrict access to only approved contacts. However, there are risks that even this private information could be exposed, so avoid posting anything that would compromise on security. Also, while enabling applications, settings need to be verified to see what information the applications will be able to access.

- **Strong Passwords:** Passwords need to be alphanumeric with mix of special symbols as well. There is a need for changing it periodically. Avoid using easily guessed passwords such as dates of birth, names of self, spouse, kids or parents etc.

- **Check Privacy Policies:** Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam.

- **Use and Maintain Anti-Virus Software:** Anti-virus software recognizes most known viruses and protects the computer against them, so *"detection is better than cure"*. Attackers are continually writing new viruses, it is important to keep these updated.

Conclusion

The twenty fist century informationalised armed forces cannot and should not adopt the 20th century instruments to keep the nation safe, secure and prosperous. It has to evolve with the times and set the stage rather than be a laggard. Social networking is here to stay and will only proliferate further down the hierarchy. The Western armies have already taken a lead by permitting the participation of their troops on these sites officially, having realised the folly of banning it earlier. India is an IT powerhouse with a number of talented youngsters. The need is to tap this potential post haste as any delays will only be at very grim costs to the national security. These realities must be viewed as an opportunity, by identifying those elements of the fast growing, almost infinite multimedia language where information high ground can be achieved. The need of the hour is to shed the baggage of hierarchy and the need for micro management. Empowering our officers and men to respond by devolving specific

India is an IT powerhouse with a number of talented youngsters. The need is to tap this potential post haste as any delays will only be at very grim costs to the national security.

responsibility for handling real time information would pay handsome dividends both in short and long term. Our attempt at the unfortunate gag order is recipe for disaster as it is tantamount to unilateral disarmament.

Notes:

[1] *Devotions upon emergent occasions and several steps in my sickness - Meditation XVII*, 1624

[2] “A World of Connections”, *The Economist*, January 2010.

[3] Carafano, James Jay, *Social Networking and National Security: How to Harness Web 2.0 to Protect the Country*, 18 May 2009 available at http://www.heritage.org/research/reports/2009/05/social-networking-and-national-security-how-to-harness-web-2-0-to-protect-the-country.

[4] Ibid.

[5] Amaral, L.A.N. and Ottino, J.M., “Complex Networks: Augmenting the Framework for the Study of Complex Systems”, *The European Physical Journal,* 14 May 2004, available at http://amaral.northwestern.edu/Publications.

[6] Barsky, E. and Purdon, M., “Introducing Web2.0” Social Networking and Social Book marking for Health Librarians”, available at http://pubs.nrc-cnrc.gc.ca/jchla/jchla27/c06=024.pdf

[7] Carafano, James Jay and Gudgei, Andrew, “Nanotechnology and National Security: Small Changes, Big Impact”, Heritage Foundation Backgrounder No 2071, 21 September 2007, available at http://www.heritage.org/Research.

[8] “A World of Connections” *The Economist*, 30 January 2010.

[9] Available at http://ibnlive.in.com/news/army-officers-computer-hacked-govt.

[10] Computer hacking: Two senior army officers under scanner http://www.thaindian.com/newsportal/south-asia/computer-hacking-two-senior-army-officers-under-scanner_100380867.html#ixzz0vKcGUPYY

[11] Available at http://en.wikipedia.org/wiki/Malware

[12] *Shadows in the Cloud: An Investigation into Cyber Espionage 2.0*

[13] Ibid.

[14] Carr, Jeff, “The National Security Risks of Gov 2.0 and the Social Web”, 1 June 2009, available at http://radar.oreilly.com/2009/06/lokis-net-the-national-securit.html

[15] –––––––. “Non –State Hackers and the Social Web”; “Mapping the Cyber Underworld inside Cyber Warfare”, pp. 93.

[16] “Global Swap Shops: Why social networks have grown so fast.and how Facebook has become so dominant”, *The Economist,* 30 January 2010.

[17] Marcus, David,et al., “McAfee Threats Report: Third Quarter 2009“, McAfee Labs™, pp. 17, available at www.mcafee.com/us/.../reports/7315rpt_threat_1009.pdf.

[18] Ibid.

[19] Ibid., pp. 12.

[20] Ibid.

[21] “China, Pakistan pip India in cybersecurity”, *WBRi IBNS Newswire,*12 September 2010.