INTERNATIONAL JOURNAL OF BASIC AND APPLIED RESEARCH
www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Technological challenges to Human Security in the Age of Information and Cyber Wars

Divya Dwivedi

Senior Research Fellow
Department of Defence& Strategic Studies
University of Allahabad, Allahabad, India

Abstract: This paper gives a close look to the very important aspect of human security in today's world of globalization and information cyber security. The role of social media, cyber security and cyber terrorism are dealt in the paper. We are witnessing a worldwide technological boom, wherein highly sensitive Government data to minute details of everyday life is digitally handled. Rules of warfare are changing and there is no longer a need for well-equipped brigade of foot soldiers to wage a war. Modern warriors, also known as hackers have the ability to hack into computer systems that can collapse networks and cause both human and infrastructural loss.

Social media is a great facilitator. It has not only brought people together. But since the number of internet users in world is growing, no doubt, the number of social media users is also on the increase. It was revealed that Social networking sites permit for information to spread very quickly amongst the public.

One of the biggest threat of technological warfare is that no one can really predict the time and source of the miscreant activity. It can be remotely initiated, and a lot of times the repercussion of the infringement is only realized after a considerable damage. Although, respective Government of world's nation are spending a great deal of resources and effort to protect their data and information from falling into wrong hands, the onslaught of social media porches namely Facebook, Twitter, YouTube and emergence of non-profit media organizations such as the WikiLeaks, who have a track record of exposing undisclosed Government information on public domain are making such efforts difficult. These trends are posing a threat to human security, and there is a need for greater Government security and awareness amongst citizens to safeguard their information on the World Wide Web.

Keywords: Human Security, Social media, Cyber terrorism, Information war, Privacy Issues, Cyber Crime.

I. INTRODUCTION:

"Information warfare" has been buzzword for quite some time now. The new terminology has captured the attention of security specialists, Government officials and curious onlookers. Technology has enabled us to be connected to each other all the time. The term "Information Warfare" is used in scenarios were using just a keyboard and mouse, information terrorists can hack into any computer and cause mass scale chaos and destructions. They can cause planes to crash, the television transponders can be imposed with false news to create panic in the country. The subverted networks will bring to halt the bank transactions. The jamming of telephone lines

Received: 5 January Revised: 13 January Accepted: 22 January
Index in Cosmos

can leave the civil government and the military blind, and the people gasping. None of these happened yet, could happen given the ease at which technology is available to teenagers.[1]

With the advancement of technology and availability of easy Internet access are quickly enhancing the speed and reach of critical information. This will result in a phenomenon of "Butter-fly effect". In chaos theory, the butterfly effect is the sensitive dependence on initial conditions in which a small change in one specific state of a large, complex system can cause considerable result in large differences in a later state located far away from source. A lot of times, these effects are spread across time, which is therefore hard to predict how and when these effects would occur.[2]

Last year, when Sony Pictures Entertainment (SPE), one of the world's largest media and technological enterprise fell prey to a state sponsored North Korean hacking conspiracy, the debate on the woes of new age technological warfare took center stage. We are witnessing a worldwide technological boom, wherein highly sensitive Government data to minute details of everyday life is digitally handled. Rules of warfare are changing and there is no longer a need for well-equipped brigade of foot soldiers to wage a war. Modern warriors, also known as hackers have the ability to hack into computer systems that can collapse networks and cause both human and infrastructural loss. Cyber-attacks, network security and information pose complex problems that reach into new areas for national security and public policy.

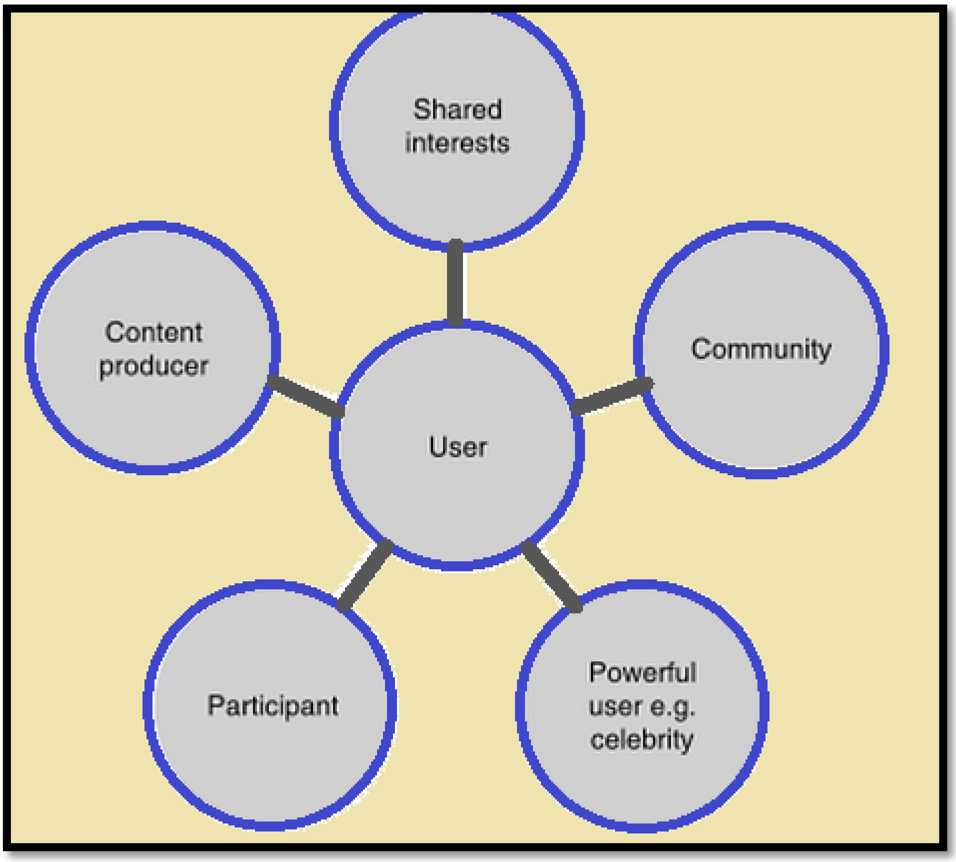
II. SOCIAL MEDIA AND SOCIAL NETWORK- A CHALLENGE

Social media is explained by a number of tools, which includes blogs, Wikis, discussion forums, micro-blogs, twitter and social networking sites Facebook. It has been observed that twitter is an effectual coordination mechanism for instigating riots and trying to initiate negative publicity. Since the number of internet users in world is growing, no doubt, the number of social media users is also on the increase. It was revealed that Social networking sites permit for information to spread very quickly amongst the public. Social networking sites enable users to exchange ideas, to post updates and comments, or to partake in activities and events, while sharing their interests. From general chit-chat to propagating breaking news, from scheduling a date to following election results or coordinating disaster response, from gentle humour to serious research, social networks are now used for a host of different reasons by various user communities. At same time, social networking sites make secret information all the more insecure.[3]

Social media platforms like Facebook, LinkedIn, Twitter has taken the world by storm. With the constant desire to interact with one another and be connected, the ability and dependence on internet to deliver this networking capability grows stronger.

Social network sites are platforms that allow people to create a public or semi-public profile online, connect with different users with whom they share a common connection on the same/different platform usually called "Friends" and converse with them through the system. The platform also enables users to view their friend's interests, conversations, their personal and social life details. Social networking sites is an online platform that attracts a community of users and enables them to create their personal and social profile. The users share their profile with people who share common interests, goals or causes. The profile or perceived impression of self will enable users to connect with different people or so called friends. They communicate in their social group through forums, emails, instant messaging or otherwise.[4]

Fig 1-Social connectivity of users (Source: Scaife, 2014)

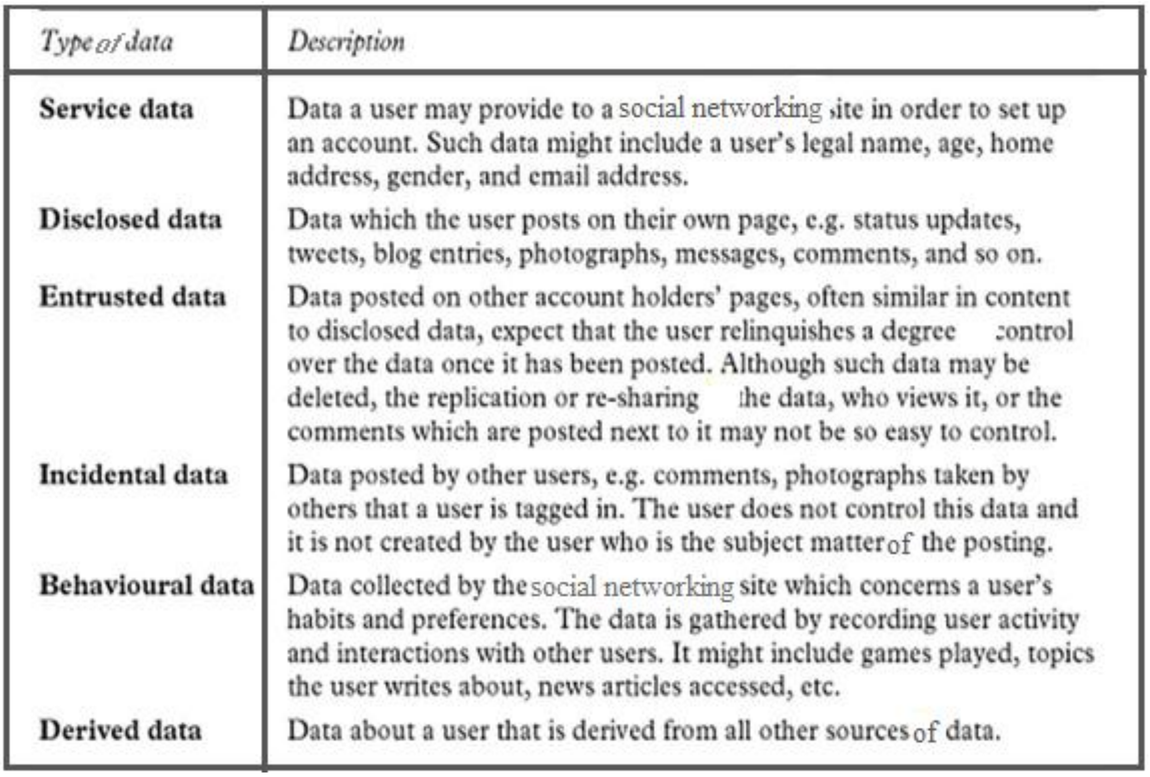


***Personal Safety**

By posting personal information on social networking services, the user create hazard to personal security. For example, revealing that you will be away from home, especially if your address is posted in your profile, increases the risk that your home will be burglarized.

There is also a growing trend towards location based service. By simple checking in you can share your location to your friends and family on social network sites. While it's a great way to inform people about your whereabouts, there are times when such information can prove harmful to your personal safety.

Table 1: Taxonomy of social networking data (Source: Scaife, 2014)



Type of data	*Description*
Service data	Data a user may provide to a social networking ,ite in order to set up an account. Such data might include a user's legal name, age, home address, gender, and email address.
Disclosed data	Data which the user posts on their own page, e.g. status updates, tweets, blog entries, photographs, messages, comments, and so on.
Entrusted data	Data posted on other account holders' pages, often similar in content to disclosed data, expect that the user relinquishes a degree :ontrol over the data once it has been posted. Although such data may be deleted, the replication or re-sharing the data, who views it, or the comments which are posted next to it may not be so easy to control.
Incidental data	Data posted by other users, e.g. comments, photographs taken by others that a user is tagged in. The user does not control this data and it is not created by the user who is the subject matter of the posting.
Behavioural data	Data collected by the social networking site which concerns a user's habits and preferences. The data is gathered by recording user activity and interactions with other users. It might include games played, topics the user writes about, news articles accessed, etc.
Derived data	Data about a user that is derived from all other sources of data.

***Mobile Social Networks**

Nowadays most of the social networking services are providing services on mobile by way of their applications which provide their users ability to interact with their personal networks via their mobile phones. Examples are Facebook,WhatsApp, hike, viber, twitter, LinkedIn, Instagram, YouTube, skype, hangoutetc., using personal mobile numbers and personal information making it visible to public and also exposing your current location to public. This itself is a big threat to human security.[5]

Smartphone powered by fast and reliable internet connection and empowered people like never before. Information transfer has never been so easy before. A person from one end of the world can transmit data and information to another person in matter of minutes. And you can do all this through a simple tap and share button on your smartphone.

***Addictive in nature**

Number of problems stems out while using these sites, many times it is used to deliver hate speeches. There are many who in the hide of judging social development are actually synthesizing there vested interests. Many groups in the name of making fun actually weakening the democratic setup and ushering it towards its downfall. The addictive nature of social networking sites also create problem. Most of the activity that happens on a Facebook page is self-promotion, sharing of thoughts and liking content posted by friends. Many of the pages shared are meaningless and much of the conversation is not of high social value.[6]

***The Privacy Issues**

The cyber attackers or hackers may use these social networking sites as a platform to propagate their malicious ideas or they may access personal information concerning a user's identity, location, contact information, and personal or professional relationships. The user may also unintentionally reveal information to unofficial individuals by performing certain actions.

Table 2-Structure of Profile Information in some Social Networks.
*** means the field exist**

Profile Information	Facebook	Twitter	9jabook	LinkedIn	Orkut	Friendster	Tribe	MySpace
Photo	*	*	*	*	*	*	*	*
Professional Detail	*	*	*	*	*		*	
Gender	*	*	*	*	*	*	*	*
Age/Date of Birth	*	*	*	*	*	*	*	*
Sexual Orientation					*			*
Marital Status	*	*	*	*	*	*		*
Sense of Humor					*			
Hobbies/Interest	*	*	*	*	*	*	*	*
Favorite Music	*		*	*	*	*	*	*
Favorite TV	*	*			*	*	*	*
Favorite Books	*	*			*	*	*	*
Favorite Food					*			
Location	*	*	*	*	*	*	*	*
Home Town	*	*	*	*	*	*	*	*
Here for…				*	*	*	*	*
Schools	*	*	*	*		*	*	*
College/University	*	*	*	*		*		
Clubs & Organizations	*	*	*				*	
Languages	*	*	*	*			*	
Religion	*	*	*	*	*			*
Smoking					*	*		*
Drinking					*	*		*
Nationality	*	*		*	*	*	*	*

III. CYBER TERRORISM

The recent Info-technical revolutions in this new liberal and globalised world have helped in making individual identities, new methods and operating mechanisms for 'Non-State criminals'. In the internet age, these non-state users penetrate into the present legal connections by laundering money which is the principle link connecting the criminal market to the global economy. Also, it's possible for them to build independent web nodes (terrorist groups or criminal org.) and non-

state operations around the world. This way of operating gives them a robust web connectivity and network links. Individual node destruction within a big network is easy. Like, Al-Qaeda or ISIS in the present, are heavily skilled at using the networks and media to propagate their terrorist activities. Their networks are well established and perfect to operate anywhere in the world. These technological advancements have abled non-state groups to affect powerful nations through cyber-attacks and also gathering millions of follower's globally.[7]
Today every country is battling for the security of its citizens against violent/virtual threats like cyber terrorism and information warfare. These activities of 'Non-State users' break the physical borders and capture a virtual space. Since it's clear that the information and knowledge are the ultimate sources of wealth and in the near future cyberspace will be independent of military or resources.[8]

The technology giants today are "the order-and powerhouse networks preferred by terrorist". Social networking giants like Facebook, Twitter, Apple, Google, Microsoft, Yahoo and many other services like WhatsApp, YouTube, Instagram, Tumblr and Skype are accelerating the effects of global terrorism. Al-Qaida once and now the ISIS are being helped by these firm to raise funds, recruit, brainwash, train and spread their believes.[9]

ISIS used the potency of the social media in a step to release the execution video of American Reporter James Foley on 19th of August. First a video was uploaded on YouTube and tweets went viral showing pictures of James Foley's beheading shot by shot. This shook the social media to the core as millions of tweets and posts went viral.

On January 20, ISIS shared a YouTube video on twitter; the video had 'Jihadi John', ISIS' famous be-header, threatening two Japanese hostages to death against a ransom of $200 million within 72 hours from the Japanese government.[10]

The growth of a global rebellion without the Internet and social forums is impossible. A huge chunk of Muslim population is being lead to the wrong through this. Jihadi recruitments are increasing because the online flow of misleading content by these services wasn't checked.[11]

Since in the recent times terrorist groups have gained expertise in social networking skills, we have to keep a check on these 3 challenges:

1. Use of multimedia to infiltrate the Social Media- Social media has been conventionally used to attract attention through pictures and videos. And the availability of high-tech gadgets anywhere has made it significantly easy to produce high resolution images and videos. Eg. ISIS (execution etc.) videos.

2. Making topics 'Viral'(on top of the feed) - The architecture of most social networking domains like Facebook, Twitter etc. is designed in a way where individuals can connect/follow many other users. This connection results in users receiving updates on followed people or connected users. This protocol has been benefitting the extreme groups to a great extent.

3. Benefiting the shorthanded approach of others - The difference in proficiencies of the extremist groups and national governments is one of the base cause contributing to the success of these groups in exploiting online world through social media.

This implies that most governments aren't skilled and knowledgeable enough to tackle the summons of social web platforms. The extremist groups had easy access to the social media and it helped them to develop skills and platforms which is near to impossible for the governments.[12]

IV. THE MOST AFFECTED GROUP

The Javelin 2010 Fraud Survey Report stated that 'young adults' are most vulnerable to fraud victimization with these frauds attacking through social networking forums.

People of ages 18-24 not only experienced online theft the most through social networking, but also took the longest count of days (132 days) to detect it and were also affected for the longest count (149 days). They were quite attentive to changing bank frauds.

On January 21, BBC news reported in an article that the youth are more prone to theft and frauds of identity because of their dependence online as they shop and "conduct more of their lives" online. An international marketing firm viz. CPP conducted a survey confirming that the possibility of delicate personal data being posted online has exponentially increased by heir usage of social networking domains.[13]

Multiple accounts of their victims are being increasingly targeted and taken over by fraudsters. They are collectively going after inspecting accounts - mobile phone accounts, credit card information, internet personal accounts all in one bundle.

Fraudsters are able to use organised crime like combination of advanced malware, phishing attacks, keystroke logging (Key Loggers) for theft of identities. And yet another way is social networking in which consumers reveal their personal data to a very large audience, in a way helping the fraudsters to carry through with their scams.

V. SUGGESTIONS TO KEEP SAFE

In the present world of digitalization masses have welcomed the mobile solutions that speed up daily transactions, such as online shopping and banking, for the reason that it can be accessed anywhere and anytime. Such users generally fall prey to the cyber criminals who always try to device new ways to rob the innocent users by taking edge of unsecured wireless networks,third-party applications, and texting to acquire personal information. At this technologically advanced stage, to protect yourself and your information, it is important to take these steps.[14]

- Restrict access to your wireless network by only allowing access to authorized users.
- Create passwords that would be difficult for an outsider to guess.
- Keep your anti-virus software updated to protect against viruses, spyware, and malware.

- Use caution when downloading or clicking on any unknown links.
- Keep personal information secure to avoid identity theft. Only transfer personal information to trusted sites.
- The more profile information a user discloses or filled in his/her account, the more the user made public his/her private issues.
- Users should also take full advantage of the feature that allows them to select which information in their profile will be visible to others.
- The closer potential connections between communities' members can be, the more information is the member willing to give about himself, beware!
- Use caution when interacting with others online through platforms such as social networking sites, chat rooms, instant messaging, or online dating.
- Keep children safe online by monitoring their internet usage in order to reduce the likelihood they will find themselves in a dangerous situation. Also remind children of important internet safety tips to follow.

VI. CONCLUSION

In the present world of the confluence of globalization and cyber revolution, the world is witnessing the novel problem for human security. The prime challenge is to protect the human security from state to non-state actors.

The most common and popular use of internet is for social networking. Looking at its popularity it has even become a popular place for cyber-attacks by hackers/cyber criminals. It is likely that social networking site will be more prone to such attacks as its popularity grows.
It is now the duty of the government to secure the social network and to work with more endeavor to carb the present cybercriminals, also to devise ways to restrict the youth from taking this path. For cybercrime not only the national but also global efforts are required to have check over it and to ensure that none of its seed is left across the globe.
New law must encompass within its preview not only the safety from criminals but also to have provision to regularize the behavior of the ones entrusted with important information
—who will doubtless continue to leak information in ever-greater amounts, as we have observed throughout the past decade.

As the use of technology increased, chances of falling prey to cyber-crimes is also getting roots. It is pertinent for the users to be more alert and able to recognize the tactics like cyber stalking and cyber bullying posing threat to personal safety.Tactics such as hacking and phishing are used to trick people into revealing personal information. Email scams are a common form of fraud that cyber criminals use to take advantage of unsuspecting people.

One of the biggest threat of technological warfare is that no one can really predict the time and source of the miscreant activity. It can be remotely initiated, and a lot of times the repercussion of the infringement is only realized after a considerable damage. Although, respective Government of world's nation are spending a great deal of resources and effort to protect their data and information from falling into wrong hands, the onslaught of social media porches namely Facebook, Twitter, YouTube and emergence of non-profit media organizations such as the WikiLeaks, who have a track record of exposing undisclosed Government information on public domain are making such efforts difficult. These trends are posing a threat to human security, and there is a need for greater Government security and awareness amongst citizens to safeguard their information on the World Wide Web.

International legal issues of Information warfare and cyber-crimes in general and Indian perspective in particular must be understood thoroughly by Indian government to fight against Information warfare.

REFERENCES:

1. Dorothy E.Denning, Information Warfare & Security Addison Wesley Longmen, Singapore Pte. Ltd.1999.
2. Nestian Gabriela, 'The human security in the Information age', RevistaAcademieiFortelorTerestre, June 2011, Vol.16, Issue 2, p.143-155, 13p.1 graph
3. Role of media and social networking sites in internal security challenges, www.civilserviceindia.com
4. Shafi'i M. Abdulhamid[1], Sulaiman Ahmad[2], Victor O. Waziri [3] and Fatima N. Jibril[4] Privacy and National Security Issues in Social Networks: The Challenges,Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.
5. James A.Lewis, 'Assessing the risks of cyber terrorism, cyberwar and other cyber threats', Center for Strategic and Internation Studies, Dec.2002.
6. Role of media and social , No.3
7. Magdalena Defort, 'Human Security in the Digital Age: Relocation of power and control over security from State to Non state Actors', Small war journal, June 3 2015.
8. Ibid.
9. Yigal Carmon & Steven Stalinsky, Terrorists use of social media a national security threat, Triblive the opinion/the review, Feb 9 2015.
10. Yigal Carmon & Steven Stalinsky, Terrorist use of U.S. social media is a national security threat, Forbes opinion, 30 Jan 2015.
11. Yigal Carmon, No.9
12. SatyamoorthyKabilan, Social media and terrorism: three key challenges, Public Safety Canada Kanishka Project Symposium in Ottawa, ON.April 13 2015
13. Social networking websites: the next cyber war zone?, Medill National Security zone, www.nationalsecurityzone.org
14. Staying safe in the Cyber world, Mass.gov blog, 24 Oct 2013, blog.mass.gov