ISSN 2367-5721

SOCIOBRAINS

INTERNATIONAL SCIENTIFIC ONLINE JOURNAL
WWW.SOCIOBRAINS.COM
ISSUE 12, AUGUST 2015

PUBLISHER:
"SMART IDEAS – WISE DECISIONS" Ltd., BULGARIA
SADIA RASOOL 21 - 34

CYBER SECURITY THREAT IN PAKISTAN: CAUSES CHALLENGES AND WAY FORWARD

Sadia Rasool

Student: Msc international relations (IR)
at National University of modern languages Islamabad, Pakistan

PAKISTAN
Sadia.rasool77@gmail.com

ABSTRACT: The cyber security threat in Pakistan is a rising issue, Because of incompatible cyber security parameterized; it is enhancing more challenges for Pakistan. As Pakistan is quickly expending its resilience on cyberspace, in the similar way it is not securing its digital networks. That's why the national infrastructure of Pakistan is also losing its strength. Now it has becomes a national security threat for Pakistan so here Pakistan really needs a proper cyber secure mechanism for the protection of her national security.

KEY WORDS: cyber security, cyber jihad, hacktivists aggression, cyber terrorism.

Introduction:

In 21 century the non-traditional threats have gained more importance than traditional threats. This century has been labelled as the "information age"; where in the technological advancement and the information and communication technology revolution have facilitated the emergence of cyber warfare. Therefore, a slow shift of the battlefield from land, air and sea to cyberspace can be noted. Cyber war is a serious threat to the national sovereignty and security due to its wide-ranging domestic, international and transnational implications. As, there are no cyber-borders between countries; it makes identification of an enemy a difficult task.

It's not a surprise that Pakistan is also facing cyber space dilemma. In case of Pakistan cyberspace has been spreading into the institutions of banking, education as well as, military and government sectors. However, Pakistan lags behind in securing its technical parameters. The major sectors of Pakistan are facing cyber illegal access problems. Pakistan has still not developed sophisticated system to ensure its security from cyber threats. Now it has become a national security threat for Pakistan because the personal data of government or individual is not secure. For the sake of public and private security different laws have already been passed but they are not that effective. They are not practiced in Pakistan. At present, a bill has been designed and offered but it has not been approved by the parliament yet. That, for sure is the failure of government and other stake holders are not paying attention to this issue. Pakistan needs to work efficiently in this particular area.

OBJECTIVES OF THE STUDY:

ISSN 2367-5721
SOCIOBRAINS
INTERNATIONAL SCIENTIFIC ONLINE JOURNAL
WWW.SOCIOBRAINS.COM
PUBLISHER:
"SMART IDEAS – WISE DECISIONS" Ltd., BULGARIA
ISSUE 12, AUGUST 2015
SADIA RASOOL 21 - 34

THE study intends to achieve following objectives:

- To find out the major Pakistan's cyber sectors and their security dilemmas, how government, military and banking sector is getting involved in cyberspace world and what are their possible parameterizes to protect the system.
- To see how huge expansion of cyberspace creates major problems for Pakistan and lack of cyber secure parameterize become vulnerable for her.
- To emphasize that the negligence on behalf of Pakistani government will further create security dilemma.
- To analyze the loopholes present in the cyber security apparatus.

Causes and challenges of cyber security in Pakistan:

Causes:

THE banking sector of Pakistan has expanded its reliability on digital networks and has started providing online banking facilities, but their systems are not highly advanced to encounter the illegal access to banking accounts. In banking zone ATM frauds have become very common. Hackers install skimmer devices in ATM machines to hack card details and withdraw money from other people's accounts. Pakistani bank, Allied Bank Limited's site was hacked and hackers left the massage on their site that your system not secures. Even some other banks have suffered from cyber attacks and lost large amount of money. However, they claim that they have insurance policies. That's why they are not much interested in securing their system but the public of Pakistan is highly affected by such attacks. The public seems to share a mutual distrust of online banking. The government of Pakistan has fixed a very small budget for the fields of Science and technology. The government does not view this field as its major priority that is why; they do not spend more on it. As a result Pakistan has faced severe economic decline for years. Then the secretary ministry of science and technology Kamran Ali Qureshi said to the committee of Pakistan that Japan is spending 25 percent budget on science and technology while Pakistan is spending less than one percent. Then committee gave a suggestion that now we needed to end up anti-science attitude and give more importance to this field in economy.

A cyber warfare is more tricky then the traditional threats between Pakistan and India. Pakistan is not paying attention to the field of technology; however India is investing more on its technological field thus creating further challenges for Pakistan in cyber warfare. Israel is providing help to India against Pakistan. So Pakistan comparatively is far behind India in the fields of science and technology. India has more sophisticated technology than Pakistan. This factor automatically creates a sense of insecurity for our state. Both the rivalling countries have cyber armies working on their defence. However, Indian hackers dominate Pakistani hackers in breaking the safe boundaries of cyber walls. As Pakistan is a sovereign state so it has to take a practical initiative for the protection of cyber threats. Both countries have cyber armies. Both attack or hack each other's data. Since India has the upper hand in this regard, this creates a dangerous situation for Pakistan, because it doesn't have proper system to secure its data from cyber threats. For the sake of deterrence Pakistan, like other states, requires an efficient cyber army to counter cyber-attacks. Unfortunately Pakistan's cyber army lacks the desired technology.

IN Pakistan there are some organizations working on cyber awareness. Pakistan Information Security Association (PISA) took an initiative to arrange a conference on cyber security to create awareness. While the independent bodies can create certain level of

awareness among citizens, heavy responsibility lies with the government which appears to have little interest in such initiatives.

THEN the senator Mushahid Hussain Sayed presented the first ever cyber security bill in Pakistan named as Cyber Security Council Bill in 2014, in which he tries to draw attention from traditional threat to non traditional threat. It shows a clear danger to Pakistan's national security. But still this bill has not been passed yet due to lack of government interest in it. Presently, there are number of laws on cyber security in Pakistan, but many of them are not effective and others are not practiced. That is basic cause of cyber warfare in Pakistan.

IN Pakistan there is a platform for cyber complains know as "national response centre for cyber crimes". Its basic responsibility is to take action against cyber criminals who are involved in information stealing, financial matters and even in terrorism. But practically it's not being very much effective due to the cyber unawareness among Pakistani people. People don't know how to put complains to the required department and some others think that it can create more problems for them so they avoid to do complain. Federal investigation agency (FIA) also deal with cyber crimes related to face book, twitter, Google, Skype etc. But its progress is also not that much effective due to the lawlessness.

Challenges:

THERE are several rising cyber security challenges for Pakistan. Because of the more dependency on cyberspace explores the more digital vulnerability of Pakistan. Here are some of the challenges.

THE government of Pakistan has restricted many sites owing to the available objectionable data like YouTube and Torrents, these sites can be easily accessed by using different software. So it has created dangerous situation for state, because it clearly shows that government is not that much strong to stop these sites properly.

THE Pakistan Telecommunication Authority (PTA) is government agency which is designed for the establishment or maintenance of telecommunication. It regulates the whole communication setup and bans the illegal or threatening sites for the betterment of cyber security reasons. In 2012, 2013 PTA blocked 15,380 websites/links because of some objectionable data on it, but this agency is not that much successful in banning the sites like YouTube? Still it is accessible in Pakistan so it shows the bigger failure of government. That creates an alarming situation for Pakistan national security to prevail the situation.

FURTHERMORE the American National Security Agency (NSA) is spying on Pakistan through internet and online communication systems. They took 13.5 billion pieces of email, phone and fax communications intercepted, that makes Pakistan the second highest country to be observed by the NSA after Iran. That is an alarming situation for Pakistan to take this issue seriously and make proper policies for the assurance of their personal data or system from such types of spying activities.

THE banking sector is enhancing its dependence on cyber space and providing E-banking facility to the Pakistani people, but the system is not secure that's why now mostly people they are losing their trust from online banking system. However in Pakistan different banking organizations do not provide proper insurance to their customers that's why people are more comfortable in keeping their money and reserves at home rather than banks. Money transitions through manual branch to other branches take too much time like five to ten days

ISSN 2367-5721
SOCIOBRAINS
INTERNATIONAL SCIENTIFIC ONLINE JOURNAL
WWW.SOCIOBRAINS.COM
ISSUE 12, AUGUST 2015
PUBLISHER:
"SMART IDEAS – WISE DECISIONS" Ltd., BULGARIA
SADIA RASOOL 21 - 34

because of the slow transaction of money, and because of this business sector or other sector suffers a lot. People cancel their important deals because of not getting their money on time.

THEN there are many terrorist organizations and anonymous groups throughout the globe. They have more sophisticated technology and well trained people in the field of cyber. In which individual and some group of people are involved, they are working independently. In which not any type of law can be enforced on them because to browse them is also a major challenge. That's why these organizations and anonymous groups are creating a great dangerous situation for Pakistan's national security. Pakistan's digital system is not effective to counter or stop the illegal access. Secondly many terrorist organizations are being present in Pakistan so it shows more difficult situation for the security of Pakistan.

THE lack of cyber awareness amongst people is also a major rising challenge. People don't know how to protect their personal data from hacking or illegal access because of which they are becoming victims to its misuse.

MANY hackers of Pakistan are claiming that the national database and registration authority (NADRA) Pakistani site is not secure. NADRA's data is easily accessible so they need to take some serious measures for the protection of their site. Because it's a very sensitive site of Pakistan, personal data of Pakistan individual is available on it so it shows a serious threat to NADRA. This requires making proper policies for the security of their digital data.

HACKTIVISM is unchecked in Pakistan, in present time period there are number of Pakistan's government official sites that are being defaced by hackers and the government is totally unable to counter them, because of not having advance technology to prevent these cyber attacks.

Hacktivist aggression among hackers and its impacts on Pakistan

HACKTIVISM is basically a politically, religiously, ethnically, or ideologically an inspired or motivated energy. In which a person who hacks, defaces or removes a website or data because of his association with any above mentioned categories. For that sake different states get benefits from their skills and use them for their own purposes. Hacktivist aim is to support one party or group and convey their massages through using cheap tools of network. But these hackers are remaining hidden behind the fog of policies, religious and ethnical messages.

THESE types of hacktivists activities are also present in Pakistan. Many supporter of a party are inspired enough from their party leader so they try to pull down other parties for the sake of their own leader popularity among the public. They hack the personal data of other political parties and try to expose each other's secret.

Cyber terrorists:

CYBER terrorists customarily motivated by religiously and politically beliefs, aim to build up fear. These cyber terrorists are more dangerous because of having professional skills and more goal originated hackers. The ultimately motivation of cyber terrorists is to spread fear, horror and terror.

IN Pakistan where it is already facing religious extremism, now these extremist is finding latest ways to expend their ideology and creating fear among people. They are using

digital network for the proliferation of their ideas and it create more threatening condition for Pakistan.

Create cyber Defensive mechanism:

IN present time period states need to create a cyber defensive mechanism. Because historically world faced first horrible digital weapon known as "digital missile." That was used against Iran by U.S and Israel. The Stuxnet creep attacked on Iranian nuclear facility at Natanz nearly four year ago. Stuxnet virus was powerful enough because usually viruses only hijack the targeted system or steal the information but stuxnet also physically destroyed the most controlling components of computer. It destroyed the whole Iranian digital work on nuclear.

SIMILARLY Pakistan's nuclear program material is also available on cyberspace so it needs to build up highly secured parameterize for its protection. Even there is a claim that Israelis also try to use their money, talent and advance technology to defame Pakistan's nuclear program. It create highly tense situation for Pakistan to adopt more sophisticated technology for the security of its nuclear programs. Because historically such type of attack is present as an example so Pakistan's should take the threat more seriously.

Hacktivism in Pakistan:

TODAY Pakistan is facing swear problems because of hacktivism. There are many hackers or group of hackers that are defacing, stealing or misusing government personal data. A numberof government sites are being hacked or defaced because of hacktivism. In which Lahore high court (LHC), Pakistan people's party (PPP), ministry of oversees Pakistanis and human resources development (ophrd.gov.pk), the cabinet secretariat (cabinet.gov.pk), ministry of petroleum and natural resources (mpnr.gov.pk), ministry of defence (mod.gov.pk), ministry of defence production (modp.gov.pk), ministry of water and power (mowp.gov.pk), ministry of education, trainings and standards in higher education (moptt.gov.com), ministry of railways (railways.gov.pk), the ministry of parliamentary affairs (mopa.gov.pk), ministry of national harmony (monh.gov.com), Pakistan Tareek e Insaf (PTI) have been included.

Major reason of hacktivism in Pakistan:

THERE are number of reasons of hacktivism in Pakistan. Below some of them are being mentioned.

- Political extremism.
- Unemployment.
- Extremism.
- Ethnic association
- Terrorism.

Types of cyber crimes in Pakistan:

HERE are some types of cyber crimes those are being practice in Pakistan.

- ***Email hacking:*** Email hacking, where hackers can easily access the mailing address of a person and then use it for negative purposes. The email hacking is creating more dangerous situation for Pakistan because NASA is getting access over the Pakistan's all

email system. They check each and every email of Pakistani people, so that is a major weakness of government to not providing security to its public from illegal access.

- ***Password hacking:*** Password hacking is a process of retaking password from the data that has already been stored in. That is the most common activity of hackers and Pakistan become its victim very easily.
- ***Online banking hacking:*** Online banking hacking where hacker gain unauthorized access to the bank accounts or passwords without the permission or account holder knowledge. Hackers steal the whole record and later they destroy the data. That is a major problem for the Pakistani banking sector to stop it and secure their date properly.
- ***Data diddling:*** In data diddling the attackers play with personal data and use that information where it is needed.
- ***Salami attacks:*** Salami attacks, those are used to crash the system. In which hackers send requests more than the capability of the system. They use different viruses and worms and ultimate cause the massive damage of a system.
- ***Cyber stalking:*** In cyber stalking, hacker may follow a person through using internet and watch his all activities and send him constant emails.
- ***System damaging:*** In system damaging the hackers use to get full control over the other person's PC or laptop and later destroy his whole system or important data.
- ***Financial crimes:*** In financial crimes the attacker target the credit cards and money laundering. Then hackers use it for online shopping.
- ***Web jacking:*** It is also practised in Pakistan, in which hacker gain control over the web site and then that site is not in the control of owner.

Cyber warfare against Islam and Pakistan:

IN present cyber warfare, most of the European countries try to do propaganda against Islam and Pakistan's nuclear program. According to a report Israel recently build up cyber task forces for wagging digital war against Islam and Pakistan's nuclear program. They are spending more the $ 1, 50, 000, 00 budgets on cyber agencies and force them to put the various cyber spies, and getting information related to the operation strategies of government of Pakistan which is being used by it. In addition Israel also has set up work forces to write on internet against Pakistan and its nuclear program. Through these types of propaganda they want to change the opinion of public that nuclear program is not in the secure hands and it will be going to fall in the hands of Al-Qaeda.

THEN Israeli lobbies in United States and U.K are spreading similar propaganda through using different channels like BBC and FOX and in print media using Washington post and New York Time. Now Israel's new tactics include using social networks and expanding their false or negative information about Pakistan nuclear program and they also claim that Pakistan's nuclear facility is also under the control of Taliban's. They also target to defame Pakistani government, security institutions and show them vulnerable to providing security to their nation from terrorism.

WESTERN countries are claiming that Muslim countries are having Islamist hacker groups those are present in different countries and regions and continually they are attacking on western websites. In most famous groups such as "Iranian cyber army," and "Osama bin laden crew," involved. Before 9/11 western activists hacked the site of pro Taliban because Taliban's announced that they were going to shut down the internet from Afghanistan.

ISSN 2367-5721
SOCIOBRAINS
INTERNATIONAL SCIENTIFIC ONLINE JOURNAL
WWW.SOCIOBRAINS.COM
ISSUE 12, AUGUST 2015
PUBLISHER:
"SMART IDEAS – WISE DECISIONS" Ltd., BULGARIA
SADIA RASOOL 21 - 34

STILL most of the western countries are claiming that in Pakistan more terrorist organizations are being working and its public is also very much aggressive religiously so they are trying to spread Islam through social networks and creating more extremism throughout the globe.

IN this situation Pakistan needs to build up dedicated professional forces to fight against all sorts of cyber warfare tactics. Because in cyberspace we cannot put the blame on any country, the attackers remain invisible. These types of reports are just a claim but it put bad impact on Pakistan as well as its nuclear program.

How to control the supremacy of hacktivism:

HACKTIVISM or activism in present conditions is becoming a rising challenge for states. It is not impossible to control but it is near impossible because there is no state in which governments and stake holders are also not involved in it. They hire state sponsored hackers for their interests and pay them enough money. The only way to control the supremacy of activism is to make proper offensive and defensive cyber mechanism.

AS far as Pakistan is concerned about how to control the supremacy of hacktivism, Pakistan needs to invest more on IT field and make actual defensive cyber secure policies to how to tackle hacktivism within Pakistan.

Means and strategies, used for the prevention and Expansion of Cyberspace

THERE are many tools, means and strategies are being used in cyberspace prevention and expansion. In 21th century cyber security became a central challenge for states at both national and international level. Strategies are basically used for political and economic purpose. In which states try to pursue their interests through their different strategies. Mostly develop or major states having their own cyberspace strategies, through them they try to protect their digital system from cyber attacks. Pakistan is also trying to make a strong strategy for the prevention of cyber attacks. But unfortunately it does remain a retrace in Pakistan because the government is less interest in its formation. Here are different strategies of major countries for the protection of cyber security.

Pakistan:

AS far as Pakistan's cyber secure strategy is concerned, still there is no proper strategy available in Pakistan. A continuous debate on cyber security is going on in the parliament but practically they are not taking serious decision about the protection of internet system. The chairman of senate committee on defence and defence production Mr. Mushid hussain said that our cyber security system must needs three basic elements.

- Pakistan's digital system should be more sophisticated to restrict the cyber attacks.
- It can prevent the emerging cyber threats.
- Able to recover quickly from cyber attacks.

STILL these elements are in process no practical implementation of them is seen in Pakistan, because the national government of Pakistan is not paying much attention to this current issue.

ISSN 2367-5721
SOCIOBRAINS
INTERNATIONAL SCIENTIFIC ONLINE JOURNAL
WWW.SOCIOBRAINS.COM
PUBLISHER:
"SMART IDEAS – WISE DECISIONS" Ltd., BULGARIA
ISSUE 12, AUGUST 2015
SADIA RASOOL 21 - 34

Cyber warfare:

We can divide cyber warfare into three basic categories. First one is computer network exploitation (CNE), second is computer network attacks (CNA), and last one is computer network defence (CND). Then latter on protection of system and network is involved in illegitimate access. In cyber warfare there are many resources and tools are being used for harming other state. In which small and big groups, an individual with information and technology (IT) skilful person are being used. They can easily launch a cyber attack against enemy state or even their own state for the sake of economic and personal interests. In such type of situation states use these hackers as a tool for their strategic, political, and economic interests. They finance them who are willing to work for them, because cyber warfare is a battle of protection among states and it's very much difficult for a state to secure their system for cyber battle field.

The major states they are setting on the top level of sophisticated information technology are able to spy or do cyber strike against any hostile state, which American famous agency NSA playing very much important role. They are having advanced technology through can spy or watch the all activities of different states through internet. In which recently Pakistan became the victim of it. NSA spying on Pakistan took 13.5 billion pieces of information through internet and telecommunication networks.

Cyber attack procedure:

The cyber attack procedure is enhancing more difficulties for Pakistan because the other global states are having much more sophisticated technology and equipment rather than Pakistan. They can easily set their target against Pakistan and make it their worst victim.

Strategies for cybercrimes prevention:

Cyber criminals are not different from traditional criminals; currently they can make money more quickly and faster than before. But through little bit technical advancement and using common sense we can avoid the cyber crimes. The following strategies help us in cybercrime prevention. But the problem with the state of Pakistan is that its public is not having that much awareness about their system prevention from cyber attacks.

- ***Keep the computer system updated:*** Cyber criminals always use different software to attack on computer system frequently and anonymously. Mostly in windows based systems in which a program downloaded and updated automatically. Here's cyber criminals exploit the situation and set the target or break into your system.
- ***Pick a strong password and preserve it:*** Username, password and identification numbers are being used in every online affair today. So the password should be based on the mixture of letters and number that make the password more strong and difficult to access. Then using same password for various sites is very much dangerous and highly risky because cyber criminals easily discover and exploit the data. Furthermore Change your password in short time it makes your data more secure and protected. But the public of Pakistan usually picks the simple password because they don't know the outcomes of it. So as a result they easily become victim of cyber attacks.
- ***Place updated antivirus software:*** Antivirus software basically designed for the prevention of cyber attacks. Hackers they send the viruses in your computer and they infect the computer without the user's knowledge. Then with the passage of time

ISSN 2367-5721
SOCIOBRAINS
INTERNATIONAL SCIENTIFIC ONLINE JOURNAL
WWW.SOCIOBRAINS.COM
PUBLISHER:
"SMART IDEAS – WISE DECISIONS" Ltd., BULGARIA
ISSUE 12, AUGUST 2015
SADIA RASOOL 21 - 34

hackers make more strong and dangerous viruses so you need to update your system that can protect your computer from harmful access.

- ***Protect personal information:*** Today using many online services require the basic personal information in which user name, home address, phone number and email address is included. In which best way to prevent the data from cybercrime is to not give response to the unknown emails which have misspelled content, grammar mistakes or web sites with strange extensions. Pakistan is not having an actual approach to prevent the digital illegal access.
- ***Turn off computer system:*** In the growing age of high speed internet connection many people selected to turn on their computer, ready for action. It provides a great opportunity to hacker to access the computer and steal his desirable data from it.
- ***Read the whole website privacy policies:*** Some time on different social network when you share your pictures or other personal material and put privacy on it to keep the information secured. But you ignore the full statement which is being mentioned that website observer can also access your information. Here hackers take benefit from this policy and easily access your information and use it for negative purpose. That is major lacking of Pakistani people that they usually do not read the whole statement or condition and accept the program. So as a result they become fool by the hands of hackers.

Impacts of cyber terrorism on states national infrastructure:

THE basic target of cyber terrorism is to destroy the critical infrastructure of the state. In which water supply, telecommunication, electricity system, universities, military operations, finance and banking institutions, schools and hospitals are included. Most of the states infrastructure is well protected but still they need to fully restrict their system from cyber advance ways of terrorism. But regrettably the state of Pakistan is facing the impacts of cyber terrorism and it is badly affecting the national infrastructure yet sadly not any system has been available to provide protection to these sensitive sites. There are three major scenarios that how cyber terrorism become cause of massive damages of nations and its national infrastructure.

Possible future scenarios of the cyberspace threats:

- ***Information warfare:*** The information warfare is relatively a new phenomenon. It can be used at strategic political and economic level for as a diplomatic talk among two or more states. In which parties try to pressurize the other party through different means. They use different social networks or web sites and build the public opinion according to their own interests then they got their desirable goals. It can also be used for tactical or operational level, or connect with military conflict.

  As Pakistan is a weak state in cyber technology so it becomes easy victim of cyber information. Pakistan is not having cyber defensive mechanism to secure itself in cyber information warfare that why other states get advantage from this situation and can easily target Pakistan through information warfare.
- ***Intellectual properties lose:*** The most important area of lose is intellectual property or business private information. It is very much difficult to estimate the losses. Cyber spying is not a zero sum game. Spies steel the information that may be related to the company future plan, list of customer, or its research results. The company may even don't know that they have no longer control over that information. A company spend

ISSN 2367-5721
SOCIOBRAINS
INTERNATIONAL SCIENTIFIC ONLINE JOURNAL
WWW.SOCIOBRAINS.COM
PUBLISHER:
"SMART IDEAS – WISE DECISIONS" Ltd., BULGARIA
ISSUE 12, AUGUST 2015
SADIA RASOOL 21 - 34

billions of dollars for the production of plan and someone steals the plan so company will get zero percent benefit even after spending billions of dollars.

Historically states sponsored criminal espionage more focus on government and such as military or advance technology. But in recent time period it seems very much common, countries use cyber spying as a part of business. In Pakistan the major problem is cyber insecurity that's why many business men avoid investing here. Because they know that Pakistani cyber system is not that much secure through they can protect their important information related to their future plans. So as a result they prefer to start their business in abroad rather than Pakistan.

- ***Cyber jihad:*** Some Islamic terrorist consider cyberspace a means of fulfilling jihad. Jihad comes from Arabic word jihadi, which principally means "to struggle" or "to strive in the path of Allah." The term has made headlines many times in recent years as terrorist activity has escalated around the world. Seemingly, whenever the United States takes a stand against terrorist Muslims, a jihad or "holy war" is declare against the United States.

  Later the cyber jihad also became a threat for Pakistan because many terrorist organizations are present in Pakistan. They are having links with Islamic state and Al-Qaeda so as a result more sectarian issues have started in Pakistan and both Shia and Sunni extremist use digital means for widening their ideology.

- **To become a cyber Jihadist:** Those organizations that are working for the cyber jihad have targeted the mostly young or extremely religious minded people. They are having believes that they will lose their lives in services to Allah and guaranteed to enter into heaven. These people are easy to mould in any direction so like Al-Qaeda they use them for their personal interests. These cyber jihadists carry out cyber jihad against those states, those they consider as enemy state. So extremists attack them, even many educated persons become part of such type of organizations. Now it has become a rapidly rising threat for states. A state like Pakistan is already facing extremism, ethnical problem or terrorism, so in this situation its being very much hard for the government of Pakistan to control the negative religious fundamentalism.

- **Motivation behind E- jihad:** The most motivating spirit for cyber jihad is having strong affiliation with religion or having a specific agenda. Those cyber jihadists are more influenced with any specific ideology they take cyberspace as a tool for spreading their ideology among other people. Some time these cyber jihadists having specific agenda so through using digital network they try to change the ideas of others and set their minds according to their desirable direction. So such type of condition create more vulnerable situation for states to find out the difference between right and wrong jihad. Pakistan is badly affected by E-jihad because they are using cyberspace and getting access on educated class of Pakistan. So subsequently many educated classes of Pakistan are becoming part of it and government is vulnerable to stop them.

How to intercept cyber jihad:

THERE are controversial thoughts about the interception of cyber jihad in Pakistan. In which two different types of opinions come, one, those are extremist and try to spread radical Islam and second the one who belong to the Islamic scholars and they try to give counter argument to those who display wrong image of religion. But it's very much difficult to find

out the difference that who is doing right jihad. So it is arising threat for states because no one can fully stop them or not even fully sport them. As westerns states are concerns they took it as a national security threat they try to suppress e- jihad. But as far as Muslims countries they capture it as a way to escalate their religious ideology. In this situation different states get advantage from it and use cyber jihad for their own interests.

Enlarged the cost of cyber security:

IN present situation the expenditure of cyber security is being increased in different countries. According to a report estimated governments and companies spend 7% information technology budget allocated for the security and per year spending of global o cyber security is $60 billion. U.S federal agencies expenditure on cyber security is more the $15 billion. In 2012 different companies spend almost $1 billion to insure their system from all sorts of cyber crimes and cyber spying. Still these companies and government are allocating more budgets for their network privacy. As globally states are spending more income on their cyber protection as per the requirement of 21th century. But in case of Pakistan, it is spending less than 1% budget on cyber security so further it will be create serious challenge for Pakistan because it is not understand the basic need of present time period. It's not possible for Pakistan to isolate itself from the emerging challenge of cyber security.

Public lack of trust:

IN Pakistan people also feel insecure to use online banking because of security issue. Many of them are trying to avoid e banking and think better to visit physically. Here's the responsibly of state, when it is expanding its dependency on digital system so it needs to make proper parameterize for the assurance of networks. Then definitely people will get facilitated from the cyber system and feel batter to use online banking or shopping rather than personal visit.

Anonymous declare war against terrorists websites:

RECENTLY an anonymous group of hackers has promised to attack online websites attach with violent jihadist Islamists retaliation for the current threat of panic attack in Paris. These hackers declared war against Al Qaeda, Islamic state and other terrorists. Their basic purpose to take down the extremists sites those are spreading terror among people. The anonymous hackers also shut down and deface the sites of those governments they are suspiciously supporting these groups. That is raising issue for Pakistan because there are many terrorist organization present and they are using cyberspace for their personal interests. These terrorists' organizations are having strong alliances and linkages with well known terrorists groups so directly or in directly Pakistan get involved in cyber war. The state of Pakistan is unable to control them.

Conclusion:

IN case of Pakistan's cyber security emerging challenges, it needs to be very much strong parameterize for assuring its security. Because system is anarchy in which different countries are trying to put down Pakistan through their sophisticated technology of cyber. Pakistan needs to strengthen its army by becoming more offensive rather than defensive. The national security needs self help approach to handle the responsibility of state governance, make proper policies for cyber security and develop a system through which she can counter

the threat. She must secure his governmental, banking sector, military sites or individual data from cyber thief.

PAKISTANIS' reliance on cyberspace is growing faster but most of them are unable to understand the critical side of digital network. Only those who become victim of cyber crimes now are taking cyber security preventing measures. Exclusively those belong to IT field and some people are familiar with the term of cyber threats or cyber warfare. So the government of Pakistan needs to do work on it and spread cyber awareness among its public.

THE most dangerous factor is the hacktivism unchecked or uncontrolled in Pakistan. That can badly affect the nuclear sites of Pakistan because in the history a state could experience similar incident. In the contemporary situation many hackers of Pakistan are claiming that different hacktivists groups are trying to deface the nuclear digital data of Pakistan. So the government of Pakistan should work seriously on the security of nuclear sites because it can affect their national security.

PAKISTANI government needs to start working on cyber security and observe the strategies of advance and first world countries that how they are dealing with cyber threats and protecting their digital system from unauthorized access. Then make a similar cyber mechanism for own system.

Recommendations:

PAKISTAN needs to join multilateral or bilateral treaties on cyber security. Because they can help Pakistan more effectively to secure its digital system and it can also got latest technology from advance states.

IN Pakistan there are many talented people in hacking or hijacking, those are involved in negative activities of cyber crimes but the government of Pakistan can use them positively in research or development sector. So they can help Pakistan to secure its cyber system.

AN important step should be taken by the government to make computer as a compulsory subject in school and college levels so the next generation can easily fight back against cyber attacks.

GOVERNMENT of Pakistan make proper legislative committees, those are powerful enough to enforce cyber laws and the one how violate the law they can take strict actions against them.

EVERY public and private institution and organization those are more relying on digital networks should have cyber professional's team, who deal with cyber attacks and make proper mechanism to secure their institution data from illegal access. In case of cyber attack these people are responsible to give answer to their organization.

THE government of Pakistan requires giving more strength to its research and development sector and build up analysis capabilities to gain more perception into risks and threats in the cyber domain.

PAKISTAN needs to develop first and second strike capability in non traditional threats like cyber security.

REFERENCES

1. **alamzeb, khan, 2012:** "pakistan: cyber warfare and internet hacking ." *dawn*, 17 jan 2012:
2. **Cavelty, Myriam Dunn, 2007:** *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* Routledge, 2007.
3. *Cybersecurity for ALL: An Overview of ITU's Cybersecurity Activities* . Yaoundé: Jean-Jacques MASSIMA-LANDJI, ITU Representative for Central Africa and Madagascar, 2013.
dawn. "'anonymous pakistan' take down government sites, leak bank records." 1 september 2014:
dawn. "cyberstalking: new challenges ." 17 april 2014:
dawn. "indian hacker's deface LHC website." 14 oct 2014:
dawn. "indian hackers deface ppp website." 14 oct 2014:
dawn. "indian hackers deface ppp website." 8 oct 2014:
dawn. "preparing pakistan for a cyber war." 17 october 2012:
editorial. "hacktivism unchecked." *dawn*, 9 september 2014:
4. Heickerö, Roland. *The Dark Sides of the Internet: On Cyber Threats and Information Warfare.* The Dark Sides of the Internet: On Cyber Threats and Information Warfare, 2012.
5. jalalzai, musa khan. "The danger of nuclear terrorism in South Asia." *daily times* , 22 july 2014:
6. **Jalil, Shamsuddin Abdul, 2003**: "Countering Cyber Terrorism Effectively: Are We Ready To Rumble?" *SANS Institute*, 2003:
7. **jamal, shahid, 2014:** "cyberstalking: new challenges." *dawn*, 17 april 2014:
8. **John Arquilla, David Ronfeldt, 2001:** "Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 50. Rand Corporation, 2001.
9. **john, herhalt, 2011:** "cyber crime_ a growing challenge for governments." *kpmg*, 2011:
10. **kakakhel, ijaz, 2015:** "Pakistan lags behind in science and technology, Senate told." *daily times*, 17 January 2015:
11. **khaleeq, kiani, 2014:** "govt to set up cyber authority, court." *dawn*, 12 jan 2014:
12. **Lewis, James A., 2002:** "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." *Center for Strategic and International Studies* , 2002:
13. McAfee. "2014 Threats Predictions: Cybercrime and Hacktivism Will Continue to Grow." 8 jan 2014:
14. McAfee. *the economic impact of cyber crime and cyber espionage* . center for strategic and international studies , 2013.
15. **Mohiuddin, Zibber, 2007:** "CYBER LAWS IN PAKISTAN; A SITUATIONAL ANALYSIS AND WAY FORWARD ." 26 june 2007:
16. **momein, fahad abdul, and m nawaz brohi, 2010:** "cyber crime and internet growth in pakistan." *asian*, 2010:
17. **murtaza, haider, 2014:** "pakathon: hacking into progress for pakistan." *dawn*, 8 oct 2014:
18. **naureen, adeela, and umar waqar, 2012:** "indo.pakistan cyber war: reality chcek." *the nation*, 28 august 2012:
19. **puran, rajeev c., 2003:** "beyond conventinal terrorism. the cyber assault." *sans*, 2003:
20. **redins, larisa, 2012:** "Understanding Cyberterrorism." 5 october 2012:
21. reporter, the newpaper's staff. "pakistan should allocate more budget for science and technology." *dawn*, 14 nov 2012:

22. reporter, the news paper's staff. "govt not prepared to handle cyber threats:experts." *dawn*, 1 october 2014:
23. **shahid, jamal, 2014:** "cyberstalking:new challenges." *dawn*, 17 april 2014: