South Asian Studies
A Research Journal of South Asian Studies
Vol. 33, No. 1, January – June 2018, pp. 35 – 48

Cyber-Threats to Strategic Networks: Challenges for Pakistan's Security

Rizwan Naseer
COMSATS Institute of Information Technology Islamabad, Pakistan.
Musarat Amin
Fatima Jinnah Women University Rawalpindi, Pakistan.

ABSTRACT

Nuclear weapons revolutionized security affairs after Hiroshima and Nagasaki annihilation. States went nuclear eventually after the United States, Russia, UK, France and China but India and Pakistan joined that exclusive club too in 1974 and 1998 respectively. Nuclear weapons a source of security motivated Israel, Iran and North Korea too. Another development that started undermining nuclear security itself was cyber warfare. Pakistan being developing country in the list of Global Innovation Index finds it hard to catch up with other leading nations in science and technology. Leading countries including US, Russia, China, UK, Germany, France etc are not safe from cyber-threats they face then how Pakistan can be considered safe against cyber-sabotaging to its strategic weapons. Pakistan's nuclear security though has gained better levels but cyber security is the field that requires comprehensive strategy to establish cyber nuclear doctrine. China being reliable strategic partner can be a resourceful partner unlike other great powers. This strategy would add much security to Pakistan's already existing nuclear security and would open new avenues of cooperation with international organizations to gain next milestone of Nuclear Suppliers' Group membership.

Key Words: **Cyber Security, Nuclear Security, Comprehensive Strategy, Cyber Doctrine**

Introduction

Nuclear weapons are technical weapons and are judged by their capability in terms of accuracy, speed, reliability and above all the power of destruction they obtrude. Strategic weapons are political creature, the major concern is that these weapons are not be used (Basrur, 2005). Despite intense armed conflicts the possessors preferred to deescalate like in the case of Cuban Missile Crisis (1962) and India-Pakistan Kargil confrontation (1999).Though the fear of nuclear war has not averted yet. States being rationale actors have been returning back from the tipping point of brinksmanship. Nuclear Weapons are regularized by Command and Control and their efficiency, safety and security are gauged by the level of command and control. Nuclear actors make sure that these strategic weapons are not misused. To dispel any chances of their misuse, control should be more than command because in case the control of the weapons is compromised, risk is borne by possessor itself. Better control of nuclear warheads also cut down the fear of

nuclear terrorism. Nuclear terrorism is not only act that an individual can perform physically, it can also be carried out by a computer wizard sitting in the other part of the world.

Sabotaging Strategic networks

History is littered with the instances of cyber-attacks for the purpose of espionage and sabotage of nuclear systems. Notable examples are Farewell Dossier, Operation Orchard, Aurora Generator Test and Stuxnet. All these were sabotage of system to acquire sensitive information. In 1991 a group of hackers broke into US military networks and they were looking for nuclear secrets, nuclear designs, and missile data to sell those to Iraqi ruler Saddam Hussein prior to US Operation Desert Storm, similarly China tried to acquire US sensitive information about W88 thermonuclear warhead. Matthew Mckinzie termed it as an 'unprecedented act of espionage' (Futter, 2016).

Over the last two decades cyberspace has taken place into strategic matters and it is intensively employed to achieve tasks like surveillance, disruption, and destabilization of nuclear systems, networks of adversaries (Hughes, 2010). News of cyber-breach emerge almost on regular basis. Even the world's largest enterprise have been under cyber-attack including the companies like Sony, Blue Cross Blue Shield, Experian, Arby's and Saks Fifth Avenue have been victimized of these attacks. The implications of such attacks are staggering, as attack on *Yahoo* emails compromised about 3 billion accounts with the breach of classified data and information. Apart from private entities, government systems have also been hit including US office of Personnel Management (Stoutland, 2017). Such incidents reflect no state is secure from such devastating attacks.

The interesting part of such deeds is that the cyber-attacker cannot be traced easily because of the attribution problem. Because of the inherent loopholes of cyber-security it becomes achievable for states and non-state actors to sabotage a system. Such acts and counteracts generate cyber warfare and states pour massive amount of money to underrate their enemies without physically fighting into battlefield. Leading cyber powers US, Russia and China are often found locking horns to outsmart each other. U.S. government exposed Chinese computer network set-ups (named Titan Rain) in 2005, which effectively penetrated several secure strategic infrastructures including U.S. Department of Defense (DoD), Department of Homeland Security, Department of State, National Aeronautics and Space Administration, and even the Office of British Foreign Commonwealth (Jason & Karl, 2013). A number of denial-of-service assaults in Estonia (2007) and Georgia (2008) were associated with Russia's Foreign Military Intelligence Agency and Federal Security Service for designating sophisticated hackers to launch coordinated cyberattacks against these tech dependent countries (Derek S, 2012). But Cyber-attack on Iranian Nuclear program rattled the strategists in Islamabad and New Delhi. The Stuxnet attack on the Iranian nuclear facility Natanz in 2010

was designed to disrupt command and control of the facility. Computer virus Stuxnet was designed to sabotage critical computer infrastructure dealing with software; proved that shakedowns might spread to real lives as well. Stuxnet is a significant new piece of virus which totally changed the security landscape of state's military strategies (Thomas M. Chen, 2011).After Stuxnet, two other embattled computer malwares for surveillance surfaced named as Duqu in September, 2011, followed by Flame in May, 2012. Media reported that these two were also designed to target Iran's nuclear infrastructure but were not as successful as Stuxnet (Nakashima, 2012). India and Pakistan kept their nuclear weapons under foolproof security from any physical threat. Physical threat is comparatively easy to counter whereas cyber-threat is more complex and devastating. There have been rumours about the vulnerability of terrorist attacks on Pakistan's nuclear weapons based on the assumption that if General Headquarter(GHQ) came under terrorist attack then how could nuclear weapons be secured. Former Ambassador to United Nations Masood Khan while addressing United Nations General Assembly assured the UN that Pakistan's tactical weapons were secure from entire spectrum of threats including cyber attacks. He also put forth that "Pakistan's nuclear weapons' security is guided by five Ds, that is to Deter, detect, delay, defend and destroy" (APP, 2013). Despite acknowledgement of the safety of Pakistan's nuclear weapons, cyber-threats remain a larger concern because guarding weapons with trained and well equipped guards is different from guarding it against an unknown threat which might attack anytime and sabotaging network like Stuxnet did with Iran.

Massive Hacking of Crucial Websites

On the eve of Pakistan's 70th Independence Day, through a well coordinated cyber-attack, websites of Pakistan's key ministries were hacked including Ministry of Defence, Ministry of Water and Power, Ministry of Information, Ministry of Environment Change and Ministry of Food Security (Zaidi, 2017). As an act of disgrace that hackers posted Indian flag and a Happy Independence Day message for India on those websites. Pakistan Telecommunication Authority (PTA) had to shut down the websites. Losing a control over Ministry of defence website is quite embarrassing because such incidents encourage hackers to hit on bigger things like strategic assets and their control. Such attacks might sound like nonsense to those who control it but not for those who hear news of crucial websites and system hacking on frequent basis not only from Pakistan but from highly technological nations.

Nobody could ever imagine a century ago that cyber domain could be used to triumph state policies as a mixture of hard and soft power. In the contemporary times Cyber space is a sphere of unimaginable power which until 21st century was not imaginable even by several leading states yet this has now become a non-traditional threat for state security. States being sovereign actors, always try to maximise their security and autonomy by adopting various new policies and

approaches. To triumph in a cyber-warfare, states secretly build their own technological infrastructure without letting other know about its capability and potential. Kenneth Waltz' argument holds substance that because of the anarchic nature of this international system, states do not trust each other. Therefore bringing them to a single platform for cooperation against a common threat is still difficult. Such common danger requires immediate attention of all stakeholder and their concrete measures to counter such threats which may trigger war between states. Having discussed foresight, the strategic culture of South Asia can neither be neglected nor taken for granted because traditional deterrence is getting obsolete and it is clearly categorized by use of sophisticated use of technology between India and Pakistan. Conventional arms' race, hostilities, increasing uncertainty and eventually nuclearization of subcontinent is the result of this persistent hostility (Latif, 2014). Having advanced missile technology, both nuclear arch-rivals are making great strands in missile technology and beyond. In contemporary era of technology conventional security approaches are switched with cyber-strategy (Malik, 2014). Pakistan being a nuclear state shares the same threat with other nuclear states. Pakistan's nuclear doctrine of Credible Minimum Deterrence (CMD) is undoubtedly a comprehensive set of policy which encounters all decisions related to conventional threat perception but it has not been updated according to the changing nature of threats. Let alone banking sector, educational institutions and governmental websites, nuclear assets are also on a verge of one single motivated attacker. Pakistan still lags behind in this realm having less than any concrete policy related to such risk. Cyber domain is much trickier than other traditional threat. Technology is one of the most neglected field in Pakistan; however, India's massive spending on its hi-tech aims for excelling in cyber-space to outsmart other contenders in the region. India's technological cooperation with Israel in cyber space has benefitted the former. India feels superiority in technological field which in the form of their National Cyber Security Policy was established in 2013. Since the formation of their policy in 2013, India for past 5 years allocates a handsome amount of budget for research and development in cyber domain. Pertinently, according to Business Standard (2017), for the budget of year 2017-18, India dispensed 8% of its I.T. budget for development in cyber domain which is apart from 2,58,589 crores of its defense budget's allocation for cyber arena (Budget, 2017). On the other hand Pakistan has not made much progress in cyber domain in particular and technological innovation in general.According to World Intellectual Property Organization (WIPO), Global Innovation Index that provides detailed metrics of innovations of 127 countries around the world. This survey incorporates 81 indicators to explore invocation, education, political environment, infrastructure and business sophistication.

Country	Score	Rank
United States	61.93	3
China	50.57	25
India	33.61	66
Iran	30.52	78
Sri Lanka	28.92	91
Bhutan	27.88	96
Nepal	23.13	115
Bangladesh	22.86	117
Pakistan	22.63	119

Source: World Intellectual Property Organization can be retrieved http://www.wipo.int/pressroom/en/articles/2016/article_0008.html

The table reflects that South Asian countries are at the bottom of the innovation except India. Pakistan's ranking comes even after other small nations of South Asia like Nepal, Bhutan and Sri Lanka. Pakistan needs to step up revolutionary measures which can improve Pakistan's ranking in global innovation index on the one hand and also put the country on the path to technological development. With the existing resources available at hand, Pakistan may find it immensely challenging to guard against cyber-threats on strategic infrastructure.

Cyber-attack to critical infrastructure is becoming a risk factor for both South Asia's nuclear states. It is observed that both states are striving hard to get cyber supremacy on each other but Indian hackers have an edge which is a threat perceived by Pakistan (Rasool, 2015). In order to attain a sustainable deterrence in the region, Pakistan needs to strengthen itself in cyber domain too.

Non-conventional Threats

Each war ended with new challenges for peace seekers. Spread of biological warfare at the end of World War I threatened peace again, World War II ended with atomic bombing of Hiroshima and Nagasaki ,cold war ended giving rise to globalization and tech-led terrorism, but the tragic incident of 9/11 triggered another global war but against terrorism. Terrorist networks got technical know-how and made links with tech-led individuals and groups who wanted to wreak havoc. Danger of nuclear terrorism grew larger not from physical threats but cyber threats too. These enormous in size and danger threats, require global collaboration to deal with but no such cooperation is happening at least in the case of South Asia which is the most affected region in the world in the wake of War against terrorism. Article 'V' of NATO was first time invoked after 9/11 to wage war against terrorists responsible for 9/11 attacks. NATO members may enjoy a sense of security under the umbrella of Article V but in terms of cyber-security, these states even commit cyber-espionage on each other. United States National Security Agency tapped phone calls of German chancellor Angela Merkel and her advisors for years to get tip off International financial crisis, Iran issue and Euro zone crisis (Reuters, 2015).

States made relentless efforts to excel in warfare but the irony is that laws, agreements and procedures dealing with kinetic warfare cannot be applied on the

cyber related warfare activities because of the diametrically opposing nature of the both. Ultimate goal could be the same for example threatening or devastating the adversary but means are different in a great way (Oona A. Hathaway, 2012) . The Council of Europe (CoE), made some hallmark steps by reaching world's first treaty, making rules and norms related to the internet and cyber-space crimes named 2001 Council of Europe Convention on Cybercrime, commonly known as the 'Budapest Convention'. This treaty made a milestone by taking first step towards this process but unfortunately no other initiative reached this point because of lack of interest by states. World's leading power, United States is not willing to give up some of its so called state privileges whose absence will threaten its security, United States may not expect better complying by other states who always look towards United States.NPT and CTBT are still in limbo, India and Pakistan not signing it terming it as discriminatory (Jr, 2013). The threat for a state of being used by single person is a nightmare for every state but if not cooperated with one another for the savage of selfish interest than this does not work like *chicken, prisoner's dilemma* or zero-sum game but this actually is *stag hunt*, and *iterated game* (Greenwald, 2013).

Mele (2013) indifferently identified the legal and strategic aspects of cyber weapons along with series of implication, if taken for granted. He underlines security of weapons and fears that security may be compromised at some point (Monarch, 2014). As a consequence of cyber-attack states may lose precious data which undermines state security and its nuclear installations. Particularly after the Stuxnet cyber-attack on Iranian facility, many other countries started reshaping their cyber-nuclear policies to prevent such occurrences (Sanger, 2013). Fear of cyber-sabotaging increased after the United States crafted a policy of cyber warfare. It's not that a hacker needs to hack a computer, it simply works that during manufacturing of the systems, a malicious device is deliberately attached to the system through which on any later stage it can be activated. Chances of such sabotage are brighter to succeed as computer related hardware and software is not manufactured in Pakistan (Sabotage, 2008). "The Department of Defense operates and estimated 3.5 million PCs and 100,000 local-area networks at 1,500 sites in 65 countries. In one study a common piece of network equipment sold by a US company was found to have nearly 70 percent of the components produced by foreign suppliers. This equipment is critical to our security as well as our economy. If we cannot trust the computer equipment out of the box, then where are we? At this point it would be impractical to validate each and every computer before we place it into operations" (paisley, 2008).

US Department of Defense disclosed a report as *offensive military operations via the cyber-space***,** which aims serving US interests but might undermine other nations. *Hersh and Pakistan's Nukes* 2009, provides a piece of information which was later rejected by Krepon that joint meetings between Washington and Islamabad that US military unit will help Pakistan to provide extra security to the Pakistan's stockpiles, if there arises any incident of emergency (Krepon, 2009).

Krepon boldly rejected Hersh's claim by quoting the statement of Gen. Tariq Majid, the then Chairman of the Joint Chiefs of Staff Committee, that regardless of any urgency, there is undeniably no way of sharing or permitting any other entity to have access to highly sensitive strategic assets. Seeking assistance to bolster security from other states relies mainly upon 2 different terms and those are non-interference and our right to pick and choose. Pakistan acknowledged US concerns regarding the nuclear safety and will accept such proposal until assistance keeps a safe distance. Pakistan possesses the right to take all apt able decisions for its survival and security.

Historically even the closest allies at some point in future turn against each other.US and USSR fought World War II against Axis powers and after the end of the WWII, cold War which was more dangerous than WWII, triggered between both former partners of WWII, therefore states do not empower other states to the extent where they start undermining their partners' security. That scenario is quite likely that India in future may come at cross purposes with US and may become a threat for US interests in the region. US empowerment of India through Indo-US civil nuclear deal opened up new horizons for India to enter into civil nuclear pacts with other nuclear actors. Though being non-signatory of NPT and CTBT India was not entitled to acquire that. India's constant upgrading of nuclear naval and military installments tips balance of power in India's favour and also underrates stability of South Asia (Lewis, 2010). Having nuclear weapons puts more responsibility upon holders because of risks of cyber-insecurity that has the potential to compromise nuclear security either done by states or non-states actors(individual hackers).Samuel Gibbs published a story in *The Guardian* UK's leading newspaper about the influence of Indians in silicon valley. Indian talented graduates who entered into Silicon Valley in Northern California in 1970s and1980s have made incredible breakthrough (Gibbs, 2014) .Indian are now assuming the leadership positions in Microsoft Corp,Google Inc,Adobe Systems Inc,Nokia Corp most notable Indian Nadella, Pichai, Suri and Narayen, (Mizroch, 2015).

Pakistan's official stance is that it got nuclear weapons because India acquired them to threaten Pakistan's existence. Pakistan managed to maintain deterrence with India by testing nuclear weapons in 1998 but in cyber security domain Pakistan needs a lot to achieve comparable to India. Cyber-security takes priority in Pakistan's military strategy, political and criminal investigation but Pakistan has dearth of resources to match with IT giants but Pakistan's initiatives soon would be bridging that gap. Lahore Garrison University (LGU) has started first of it kind Digital Forensic Research and Services Centre (DFRSC).Lahore Garrison University's vice-chancellor Major General (Rtd) Obaid Bin Zakaria claimed that "the centre is first and one of its kind in the SAARC and it's combining the elements of cyber security, cyber warfare, digital forensics, trainings for all tiers – technical and non-technical, research and preparing field-ready experts" (Sheikh, 2016) A well known digital security company Symantec Corp, identified a sustained cyber spying campaign most likely state sponsored against Indian and

Pakistani entities involved in regional security issues. Symantec identified these malwares attack during heightened tensions between India and Pakistan. Though cyber expert in India and Pakistan work cautiously to avoid any attack of malware but attackers use decoy documents that are hard to figure out but most of them are about security issues in South Asia. These malware use names like reports from Reuters, The Hindu, Zee News, Kashmir Conflict etc. India has established a centre to respond to such threats and help companies detect and remove the malware that corrupts system. That Centre is operated by Indian Computer Emergency Response Team (CERT-In). (Reuters, 2017).

Pakistan should beef up its security using technology in cyberspace and contemporary counter strategy before the times passes and these threats become to strong to control. Even security of Nuclear weapons is maintained through cyber networks but presumably they are highly protective. Nuclear security is highly sensitive issue and countries with less secure nuclear weapons would certainly get unprecedented pressure from international community to secure them because the ultimate fear is that if these nukes go into the hands of terrorists they would terrorize world peace and may also launch one to intimidate the whole international community. Therefore even the great powers work on securing their nukes without making any large claims of reaching highest level of security.

A single cyber-attack from one state to another can accelerate confrontation leading to war and that war may escalate into nuclear clash. One can foresee by keeping in view the evolution and progression of international cyber norms that next five years are crucial for the idea. The United Nations Group of Legislature report defined the basic rules of engagement during war and peacetimes. Since then, United Nations is urging all the states to take concrete steps like the Tallinn Manual 2009, issued by a bunch of non-governmental authorities under the sponsorship of the North Atlantic Treaty Organization (NATO), Compliant Cyber Defense Centre of Excellence which had endeavored to shape the guidelines of engagement during war times. It still remains to be seen whether these initiatives will come up with comprehensive, categorized set of standards, but international community appears to reaching the conclusion that every cyber-attack is impossible to contain whereas state with insurmountable resources, manpower, infrastructure and most importantly by collaboration with other states can make it happen. It works with the same logic as once the second strike capability was seen as mere impossible but with the spread of nuclear weapons to other states and unprecedented progression in the field of missile technology, states not only achieved second strike but started reaching beyond that now cyber-attacks enable hackers to hack the system and jam or activate that. Threat of unauthorized use of nuclear weapons remains bigger challenge for states and leading actors are working on it to cope up with this challenge.

Reality of Virtual World

The security of nuclear assets was never as much significant as it is now in the age of cyber-security when malware attacks carry the ability to sabotage or misuse nuclear weapons. South Asia is termed as nuclear flashpoint because of the fragile peace between India and Pakistan. Under such uncertain situation credible deterrence between both states bodes relative stability, Pakistan having made greater strands in the field of nuclear technology needs a cyber nuclear doctrine that would provide fool-proof security to nuclear assets on one side and also let Pakistan be counted among those few responsible nuclear actors who have designed cyber-nuclear doctrines.

China took another leap by legislating about cyber security law in the month of June, 2017.It is heralded as milestone in data privacy regulations. Under this law protection of personal information to individuals from misuse of their personal details in case, by using personal details, their even bank accounts become more prone to scams and frauds via cyber-technology. This law has been formulated by the local companies, which are going global, prevent taking away data out of China and same is applicable to foreign companies. This law serves the purpose of legal protection to interests of the masses in cyberspace and also strengthens national sovereignty of China on cyberspace and security (Yan, 2017).

Andrew Futter does think that though cyber-security is necessary but it has to go a long way to become potential threat to nuclear weapons. He cites an example of highly sophisticated stuxnet worm which took years to become harmful but it still was limited in its destruction. He dispels the notion of a possible cyber Pearl Harbor and Cyber 9/11 but agrees that at least not at the moment. To him hackers might steal sensitive data, change software codes, infiltrate into networks, disrupt communication networks. Such developments and technological advancements present serious challenges to nuclear weapons management and their security (Futter, 2016).

In this fast transforming world, Pakistan needs to catch up with the cyber demands and need to comprehensively design a cyber strategy that incorporates nuclear assets as well to avoid any cyber attack as was Stuxnet. Contrary to this, Kerr (2010) in his book *Pakistan's nuclear weapons: Proliferation and security issues* clarified that U.S officials' various times expressed their confidence on the security of Pakistan's nuclear weapons (Kerr, 2010). Former U.S President Barak Obama highlighted this issue in his address on April 29, 2009:

> "I am confident that we can make sure that Pakistan's nuclear assets are secure, primarily, initially, because of the Pakistani army, I think, recognize the hazards of those weapons falling into the wrong hands. We have got strong military to military consultation and cooperation".(Kerr,2010:1)

The traditional threat to Pakistan's nuclear weapons that some terrorist networks were struggling to acquire nuclear technology by either stealing or infiltrating into arsenal, are false in case of Pakistan. Harvard Kennedy School report (2016) affirming that Pakistan has substantially strengthened its nuclear security in the past two decades at administration level of nuclear facilities including training of staff, methods to personnel checking, equipment and accounting and movement of nuclear material from one place to another, techniques of guarding nuclear sites are the factors contributing towards overall nuclear security of Pakistan (Matthew Bunn, 2016). Adopting measures for strengthening nuclear cyber domain improve confidence building measures between Pakistan and International Atomic Energy Agency (IAEA).

Why Pakistan needs Cyber Nuclear Doctrine

Pakistan's war against terrorism turned many anti-US militant groups against Pakistan. Pakistan's armed forces launched multiple operations in Federally Administrated Tribal Areas (FATA) and regained control of territories. War against terrorism increased the security risk to Pakistan armed forces and civilians alike. There have been attacks on military personnel and their convoys but terrorist attacks on military bases, naval bases, airports and even General Headquarters (GHQ) baffled the whole international community. Some of the critics raised voices how could Pakistan secure nuclear weapons from the terrorist attacks? But it's not only Pakistan that faced terrorist attacks on military bases but India and United States too have such apprehensions. Nobody could ever imagine that Pentagon might come under terrorist attack. It happened but nobody raised doubts about the fragile security of US nukes. States being responsible actors of International relations need to cooperate against a common threat. Apart from traditional threats to nuclear weapons or strategic assets, cyber-attacks are also a challenge. The ripe time to initiate countering non-traditional threats was when national Command Authority was established and Strategic Plans Division started its functioning.

Salik and Luongo (2013) assessed Pakistan's security situation in detail and pinpointed several aspects which needed more attention to bolster security (Salik, 2013). Despite many security measures and upgradations, establishment of tasks forces, a perpetual need of improvement still exists to deter any untoward situation. U.S. Department of Defense's former official Lawrence J. Korb visited Pakistan in 2009, and mentioned possibility of Armageddon for Pakistan, as a consequence of Pakistan's failure in responding to non-traditional threats.

United States dominates in cyber-security but such incidents have happened in the United States that are eye-opener for other nuclear actors. In 2010 about 50 Minuteman missiles installed in the underground silos mysteriously disappeared from their launching crews' monitors for nearly an hour. The crew could not have fired missiles even on the presidential order. Presumable some hacker was trying

to launch them from remote location. Senior officials in the strategic ranks were rattled by this situation and President Barack Obama ordered an investigation into the matter. But Air force was rapid to determine the improperly installed circuit card which caused the lockout. That terrifying problem was fixed afterwards (Blair, 2017). Beyza Unal researches on nuclear weapon and cyber security in a UK based think-tank Chatham House states that the risk is not limited to the threat that hackers may launch missiles remotely but temper the system so it detects that it's being attacked which would trigger retaliation to go off. Another possible threat that Unal presents that hackers could introduce malicious codes into weapons during their procurement which they misuse whenever they want to. Joe Burton of a faculty member at Waikato University New Zealand mentioned recent cyber attacks on Ukraine possibly carried out by Russia (Clark, 2017).

Noor refers to a term *Rubicon in the cyber sphere*, which is comparatively in the domain of security studies. Simply constant surveillance of the air gap can limit the threat of cyber-attack up to 80% (Clark, 2017). It is widely renowned software – which was specially aimed to spy, sabotage, reprogram and physically damage its target in an independent and programmed way. According to Shin & Kwon (2013) programmers of malwares like Stuxnet, Duqu, Flame etc., are state-sponsored because they performed specific Advanced Persistent Threat (APT) cyber-attacks on specific targets (Clark, 2017). Chances of being human effort also cannot be ruled out but such efficiency ridden, risky and high budget secret programs can only be carried out by huge stakeholders. Edwards Snowdens's revelations already opened up a new debate that how the NSA keeps strict check on flow of information and cyber espionage is the order of the day to obtain information that can be used for strategic purposes (Naughton, 2012).

Attackers strongly prefer to develop malicious codes rather than penetrating in the computer networks of the facilities because infecting computer systems with malicious malwares is easier rather directly penetrating in the computer setup mounted with numerous security programs such as firewalls and virus detection system. These virus starts their work on small bases which is penetrating from various exposed surfing sites such as gambling, porn, game, P2P, on which attackers can easily setup their viruses for their bigger goals. Aforementioned are the web-sites that mostly are used by organization workers on their PCs in order to download illegal software which may have been feed with harmful viruses. Then it is just a matter of time that PC is infected with malicious virus, now it can conveniently be used for Distributed Denial of Service (DDoS) attack or transmitting the data within the computer to attack without the permission and knowledge of the PC user. Ultimately the goal would be achieved when the nuclear facility's vital material is automatically available if the facility administrator's computer network is compromised. Edward Snowden's revelations came as altogether a new debate in which the involvement of states like US, UK and Israel became confirmed in state sponsored cyber-attacks and where the public good(Internet) was being used as a disguise for "spying, sabotage and war".

Involvement of non-state actors in tracing down the origin of a cyber-attack has become even more complicated (Gellman, 2013).

Donald Trump's unexpected rise to presidency in the United States was also linked to possible election rigging where Russia helped Donald Trump to get him elected as the President of the United States. New York Times reported that according to a declassified report by US intelligence agencies, Russian President Vladimir Putin ordered an effort to disrupt US elections 2016,it also included cyber attacks on email accounts and systems of Democratic Party officials (Times, 2016). The most recent cyber-attack was witnessed on United Kingdom's hospitals and government departments. British Chief of National Cyber Security Centre Ciaran Martin warned to British government that Russian cyber-attacks on Western and British government and industries are more persistent than United States and British officials acknowledged previously. They have attempted attacks on British energy, media industries and telecommunications. Britain was hit by North Korean attack in 2017 which temporarily disabled computer systems in hospitals, rescheduled the operations and diverted ambulances but a lone amateur defused it successfully (Kirkpatrick, 2017). In the above cited examples it has been argued that United States, Russia, Britain, China and leading countries in cyber-space and cyber-technology are at risk of cyber-attacks which is not limited to individuals but also to government agencies, organizations and government's classified data. It therefore, is argued that Pakistan needs to improve cyber-security particularly it needs to bolster cyber-nuclear doctrine that would provide multilayered security to Pakistan's nuclear assets. Government is already working on it and have achieved better results but given the threat, Pakistan has long way to go. It may also reach cooperation with China which has been a trustworthy strategic partner and may help Pakistan without much suspicion to empower against India. Other countries including US, UK, France being the U.S. ally may face some pressure from the U.S. but China withstood foreign pressure and continued support for Pakistan. If the cooperation between China and Pakistan steps up in cyber nuclear domain, then it certainly would add much security to Pakistan's nuclear shield. Maximizing nuclear security would also acquire benefits from European nations as they may safely engage into nuclear energy cooperation with Pakistan but that step is far to achieve but not impossible.

Reference

APP. (2013, November 7). Pakistan's nukes safe from cyber, other threats: Masood Khan. *The Express Tribune*. Retrieved from https://tribune.com.pk/story/628411/pakistans-nukes-safe-from-cyber-other-threats-masood-khan/

Basrur, R. M. (2005). Nuclear command-and-control and strategic politics in South Asia. *Contemporary South Asia*, 155-157.

Blair, B. G. (2017, March 14). Why Our Nuclear Weapons Can Be Hacked. Retrieved from https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html

BLAIR, B. G. (2017, March 14). Why Our Nuclear Weapons Can Be Hacked. Retrieved from https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html

Budget. (2017). *Business Standard*. Retrieved from http://www.business-standard.com/budget/article/budget-2017-it-telecom-players-expect-more-for-cyber-security-broadband-117012600345_1.html

Clark, L. (2017, August 9). Trump can't use cyber to stop North Korea's nuclear weapons. Retrieved from http://www.wired.co.uk/article/us-cyber-war-against-north-korea

Derek S, R. (2012). *Cyberspace and national security: threats, opportunities, and power in a virtual world.* Washington D.C: Gerorgetown University Press.

Futter, A. (2016). *Cyber threats and nuclear weapons: New questions for command and control, security and strategy.* London: Royal United Service Institute.

Gellman, B. a. (2013). US spy agencies mounted 231 offensive cyber-operations in 2011, documents show. Retrieved from https://www.washingtonpost.com/

Gibbs, S. (2014, April 11). The most powerful Indian technologists in Silicon Valley. Retrieved from https://www.theguardian.com/technology/2014/apr/11/powerful-indians-silicon-valley

Greenwald, G. E. (2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian, 9*(6), p. 2.

Hughes, R. (2010). A treaty for cyberspace. *International Affairs*, 523.

Jason, H., & Karl, G. (2013). *A Fierce Domain: Conflict in Cyberspace.* Washington D C: Cyber Conflict Studies Association.

Jr, J. S. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists, 69*(5), 8-14.

Kerr, P. K. (2010). Pakistan's nuclear weapons: proliferation and security issues. . Diane Publishing.

Kirkpatrick, D. D. (2017, November 14). British Cybersecurity Chief Warns of Russian Hacking. Retrieved from https://www.nytimes.com/2017/11/14/world/europe/britain-russia-cybersecurity-hacking.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking

Krepon, M. (2009, November 19). Sy Hersh and Pakistan's Nukes. Retrieved from Arms Control Wonk

Latif, A. (2014). A Comparative Study of Nuclear Doctrines of India and Pakistan. *Journal of Global Peace and Conflict*, 129-146.

Lewis, J. A. (2010). Cyber war and competition in the China-US relationship. *Remarks delivered at the China Institutes of Contemporary International Relations*, 13.

Malik, M. B. (2014). Pakistan and India Cyber Security Strategy. *Defence Journal*, 59.

Matthew Bunn, M. B. (2016, March). Preventing Nuclear Terrorism,Continuous Improvement or Dangerous Deccline. Retrieved from https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf

Mizroch, A. (2015, August 11). Why America's Top Technology Jobs Are Going to Indian Executives. Retrieved from https://www.wsj.com/articles/why-americas-top-technology-jobs-are-going-to-indian-executives-1439338706

Monarch, B. L. (2014). One Minute to Midnight: Amending the War Powers Resolution to Confront the Coming Cyber Wars. *Ky. LJ* , p. 457.

Nakashima, E. G. (2012). US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. *The Washington Post*. Retrieved from https://cyber-peace.org/wp-content/uploads/2013/06/U.S.pdf

Naughton, J. (2012, June 17). How Flame virus has changed everything for online security firms. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2012/jun/17/flame-virus-online-security

Oona A. Hathaway, R. C. (2012). The Law of Cyber-Attack. *California Law Review, 100*(4), 817.

paisley. (2008, February 6). Cyber Sabotage. Retrieved from https://www.military.com/defensetech/2008/02/06/cyber-sabotage

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal, 12*, 21-32.

Reuters. (2015, July 8). NSA tapped German Chancellery for decades, WikiLeaks claims. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel

Reuters. (2017, August 29). Pakistan and India hit by spy malware, says cybersecurity firm. *Dawn*. Retrieved from https://www.dawn.com/news/1354649

Sabotage, C. (2008, February 6). Paisley. Retrieved from https://www.military.com/defensetech/2008/02/06/cyber-sabotage

Salik, N. a. (2013). Challenges for Pakistan's Nuclear Security. *Arms Control Today, 43*(2), 14.

Sanger, D. E. (2013). Broad powers seen for Obama in cyberstrikes. *The New York Times*, p. 3.

Sheikh, A. (2016, November 27). Cyber security: Inside Pakistan's first digital forensic research lab. Retrieved from https://tribune.com.pk/story/1246290/cyber-security-inside-pakistans-first-digital-forensic-research-lab/

Stoutland, P. (2017, October 18). Growing threat: Cyber and nuclear weapons systems. Retrieved from https://thebulletin.org/growing-threat-cyber-and-nuclear-weapons-systems11201

Thomas M. Chen, S. A.-N. (2011). Lessons from. doi:10.1109/MC.2011.115

Times, N. Y. (2016, July 27). Following the Links from Russian Hacker to US Election. Retrieved from https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking

Yan, S. (2017, June 1). China's new cybersecurity law takes effect today, and many are confused. Retrieved from https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html

Zaidi, M. (2017, August 14). Major Pakistani government sites hacked on 70th Independence Day. *The Hindu*. Retrieved from http://www.thehindu.com/news/international/major-pakistani-government-sites-hacked-by-indian-hackers-on-70-independence-day/article19493079.ece

Biographical Note

Dr.Rizwan Naseer is Assistant Professor of International Relations at Department of Humanities COMSATS Institute of Information Technology Islamabad, Pakistan.

Dr. Musarat Amin is Assistant Professor at Department of Defence and Diplomatic Studies, Fatima Jinnah Women University Rawalpindi, Pakistan.