CYBER SECURITY CHALLENGES IN SOUTH ASIA AND ROOM FOR CYBER DIPLOMACY

Dr. Rizwan Naseer, Dr. Musarat Amin and Kinza Shaheen[*]

Abstract

With the advent of information revolution, states are tangled into an undeclared cyber war. The paper starts with some glimpses of cyberwar between India and Pakistan then it underlines the consequences that cyberwar may lead towards unimaginable circumstances. It then recommends cyber diplomacy at regional and global level to pacify the cyberwar. The Budapest Convention, Tallinn Manual, The United Nations Resolutions 64/211 and International Multilateral Partnership against Cyber Threats, have been the plausible feats that achieved niftier support from international actors. The paper also discusses that cyberwar and cyber diplomacy are simultaneously at play between great powers. The paper highlights undeclared cyberwar between great powers but it mainly focuses on India and Pakistan (South Asian region). Though India and Pakistan are nuclear actors but they still face numerous cyber threats to their strategic and financial institutions. It underlines the challenges that cyberwar incurs. This paper recommends cyber confidence building measures between India and Pakistan to pre-empt any undesirable incident perpetrated by unknown hacktivists.

Keywords: Cyber War, Cyber Diplomacy, India-Pakistan, Cyber Confidence Building Measures.

Introduction

Cyber-attacks have become frequent ranging from multinational corporations to international organizations; these attacks are launched by states and non-state actors. But if such an attack causes havoc in another country (strategic weapons, defense institutions, financial institutions etc.) it is considered an act of war. Pakistan's financial institutions and research databases have been hit by cyberattacks originating from Indian backed hackers and India has been responded to by Pakistan in a similar fashion. This new domain of cyberspace is more sophisticated as without firing a bullet, any country can inflict unprecedented loss on its rival country. Acknowledging the significance of cyberspace Dan Kuehl (National Defence University Washington D.C.) admits "We operate in five domains: air, land, sea, outer space and cyberspace.[1] India

[*]Dr. Rizwan Naseer is Assistant Professor of International Relations at the Department of Humanities, COMSATS University Islamabad, Pakistan. Dr. Musarat Amin is Assistant Professor at the Department of Defence and Diplomatic Studies (DDS), Fatima Jinnah Women University Rawalpindi, Pakistan. Kinza Shaheen is MPhil Scholar at the Department of Humanities, COMSATS University Islamabad, Pakistan.

believes that India's largest Bank (The State Bank of India) was hit by anonymous hackers from Pakistan on December 25, 2008 and Indian authorities declined any significant losses of data and money.[2] The undeclared cyberwarfare had already started between India and Pakistan after nuclear tests of 1998 but they got intensified and frequent after 2010. Notorious Indian hackers had launched cyberattacks multiple times against Pakistan. Details of the cyber-attacks between India and Pakistan can be accessed at "Hotspot analysis: Regional Rivalry between India and Pakistan, tit for tat in cyberspace".[3]

India and Pakistan have a checkered history of relations marked by nuclear tests on both sides in May 1998 which was followed by The Lahore Declaration (February 21, 1999) and then Kargil War broke out in May 1999. Because of the balance of terror, both countries disengaged but it remains a nuclear flashpoint. The new dimension of conflict between both the contenders is cyberspace. Indian hacktivists and patriotic hackers who launched multiple cyberattacks against Pakistan by targeting government websites and various organizations including banks, airports and government websites. This indicates that their political motives and intentions should be noticed by Pakistan. Indian hackers prepared Hanove malware in 2013 with an intention to cyberespionage and targeted dozens of industries in the U.S., China, U.K, Germany, Taiwan, Indonesia, Jordan, Norway, Iran and Pakistan. The Hanove malware was designed to steal important documents, to register keystrokes and screenshots by uploading secret data to a remote server. Another similar malware BADNEWS was used for a similar purpose by monitoring USB-drives and download files.[4] In response to Indian cyberattacks Pakistani hackers also developed a malware MSIL/Crimson that could record keystrokes, gather login information, and activate webcams and gaining control of emails from Microsoft outlook. India named some of the anonymous hackers as Pakistan Cyber Army (PCA) to give a false impression that the government had the backing of such cyber-attacks against India. The cybersecurity firm Threat Connect (2013) tried to trace the hackers but did not get any clue that PCA has any ties with the government.

To protect Indian websites from cyberattacks the Mallu Cyber Soldiers (a group of Indian cybersecurity experts) has been proactively working since 2014. But at the same time, this group also declares that it works without any governmental control. But this group primarily targets China and Pakistan for cyber espionage purposes. The Norman Shark and the Shadow server Foundation report (2013) enlisted several Indian cybersecurity contractors involved in cyberwar. This war in the domain of cyber space is likely to intensify because for countries it is easier to disavow any connection with hacktivists or patriotic hackers. The game changer in the history of cyberwarfare was 'The Stuxnet virus' that massively damaged Iran's nuclear program. Stuart Winer published in *the Times of Israel*, that the CIA, Mossad and Dutch intelligence agencies

recruited an Iranian engineer as a mole who implanted virus into Iran's Natanz enrichment facility. That implanted virus penetrated into Iran's nuclear program and sabotaged enrichment process by speeding up centrifuges. He also mentions that out of 5000 centrifuges, up to 1000 were damaged due to virus.[5] India's track record of malwares reflects that India may seek a similar attack on Pakistan, but it may do so in collaboration with Israel. Azriel Bermant (a research associate at the Institute for National Security Studies in Tel Aviv) published in *Haaretz* that Pakistan does not call for Israel's destruction, but it poses a threat to Israel.[6] India's current leadership has invoked hatred in India against Pakistan as well as Muslims living in India. Pakistan-India are exchanging heavy fire at line of control which seriously undermines regional security.

Pakistan is among the most targeted countries in the world. The main targets in Pakistan include nuclear installations, media houses, communication networks, government departments, transportation etc. Such threats were confirmed by the release of Snowden documents (2013-2014) stating that Pakistan was under the surveillance of NSA using malware SECONDATE. Another recent cyberattack was on Pakistan's navy 'Rattlesnake',[7] It is imperative for Pakistan to prepare cybernetwork that not only counters such threats but also leads a forum for cyber diplomacy to gather regional and global stakeholders on a single platform.

Traditional security can be managed by seeing rising tensions, but cybersecurity needs a proper response that not only addresses challenges of cybersecurity but also promotes cyber-diplomacy among regional as well as global actors. Without cooperation of great powers and international stakeholders it will be harder to control even cyber-crimes which are far less dangerous than cyberwarfare.

International Cooperation among States on Cyber-Crimes

The 'Cyberspace' has been recognized by the world's leading states as the fifth zone of the clash. The developed states have taken their eyes off from the conventional warfare and are engaged in cyber-attacking to get an asymmetric edge over the adversaries. The Russian cyber-attacks against Estonia, Georgia, manipulation of Ukrainian, U.S. and French presidential elections have opened up a new phase of cyber warfare. Furthermore, the joint venture of the U.S. and Israel to sabotage the Iranian Natanz nuclear power plant by Stuxnet was an eye opener for the nations possessing nuclear weapons. There is a gradual shift from conventional warfare to cyber warfare among states. On one side the states are mounting offensive cyber capabilities and launching cyber-attacks against the adversary states but on the other side, realizing the cataclysm embedded in cyber warfare, they have begun cooperation by reaching bilateral

and multilateral treaties and Confidence Building Measures (CBMs) in cyberspace. The 'Budapest Convention' is the most significant international regime, concluded by the states to team up in the cyber domain. The Budapest Convention was drafted by the Council of Europe in Strasbourg on 8 Nov 2001, which entered into force on July 1st, 2004. It was the first International Treaty on international group efforts in the cyberspace. The treaty comprises of 48 Articles and calls for enacting laws and permits sharing of data relevant to cybercriminals among the signatory states. The treaty aims to foster an international coalition to protect the Information and Communication Technologies data against the cybercriminals.[8] The conclusion of the 'Tallinn Manual' is another effort of states to work together in the cyberspace. In 2009, an International group of experts was invited by the Tallinn based organization of military known as "NATO Cooperative Cyber Defence Centre of Excellence" to produce clauses of International law on cyber warfare. The group is comprised of private entities and was convened to draft rules of international law applicable in jus ad bellum and jus in bellum in the cyber purview. According to the Tallinn manual, international law is applicable only if a state violates the sovereignty and jurisdiction of another state by launching cyber-attacks.[9] Old concept of sovereignty needs to be updated in the purview of latest developments in international relations.

Above and beyond the states, the Inter-governmental organizations especially the United Nations is taking measures to counter threats to cybersecurity. The United Nations Resolution such as Resolution 64/211 passed in March, 2010 linked to the cybersecurity was tabled in the UN General Assembly to address the teething troubles sprung from the cyber threats. The issue of cybersecurity is becoming the top priority of the United Nations and it did institute a special agency 'International Multilateral Partnership Against Cyber Threats' (IMPACT) at the World Cyber Security Summit held in 2008 to bring together academia, corporations and governments to sweep away the cyber threats. The task of IMPACT is to provide access to the appropriate resources to the 152 member signatory states of the International Telecommunication Union against the cyber threats.[10]

The above-mentioned regimes and organizations are some of the steps taken by the international community of the states to boost mutual cooperation in the cyber domain for common good. The leading states and the permanent members of the United Nations Security Council as the U.S, U.K, France, China and Russia, became the victims of cyber-attacks, therefore, they had to set off cooperation to combat cyber-threats. India and Pakistan are also nuclear weapons states like other UNSC permanent members but unfortunately, they have not attained any mutual cooperation against a common threat to advance towards détente in the cyberspace. With the beginning of the war against terrorism in the wake of 9/11, terrorists started using social media as a platform to

advance their ideology and recruitment campaigns. Peace is fragile in South Asia and any terrorist attack perpetrated by any terrorist groups, can trigger a war between India and Pakistan. As a consequence of *Pulwama attack* (Feb, 2019), India demonstrated bellicose behavior and led towards brinksmanship which was fortunately averted because of Pakistan's appeasement efforts to achieve de-escalation. In such circumstances if a lethal cyber-attack is triggered by anonymous non-state actors, either damages critical infrastructure of Pakistan or India may lead to a disastrous war. Both of the states are facing the menace of cyber-attacks by non-state actors but no joint initiative has been taken for countering cyber-threats. India and Pakistan being neighbours and nuclear powers should engage into cyber diplomacy similar to Tallinn Manual or International Multilateral Partnership against Cyber Threats' (IMPACT). Even the forum of the United Nations is also open for cyber diplomacy under the UNSCR-/211(2010) to address the troubles arising from cyber threats.

The Era of Cyber Threats

Historically, some major events which revolutionized the military strategies remained significant such as the invention of gunpowder, industrial revolution in Europe and the invention and usage of the atomic bomb in World War II (on Hiroshima and Nagasaki). Nonetheless, in the contemporary era, a revolution in telecommunication and computer network has shifted the conventional war towards non-conventional cyberwarfare, in which non-state actors emerged as a greater challenge to state sovereignty. Joseph S. Nye Jr. in one of his essays titled "The Future of Power" argues that in the upcoming era the concentration of power will not be confined to the states only rather will be shifted to the non-state actors, who were not significant actors in the international system earlier. Cyber domain is a vibrant example of the diffusion of power from a nation-state to the non-state actors.[11]

The states could have control over territory, air, sea, and space but in the domain of cyber, they are facing immense challenges to secure the basic infrastructure from the cyber-attacks. The physical structure of a nuclear plant could have strictly been guarded by the states but such security does not guarantee the protection of nuclear data, stored in the computers because some eccentric computer hackers may access such data if they find some loopholes in the security of the system.[12] *The Future of Power* describes the transition of power from governments to non-state actors and it is said as one of the great power shifts of this century. The great powers are unlikely to be able to dominate this domain as much as they have dominated land, sea, air, and space. Currently, states are facing four types of cyber threats. The nation states are mainly involved in cyber warfare and espionage while cybercrimes and cyber terrorism are attributed to the non-state actors.[13] Both the states, India and Pakistan came under

attack of cyber espionage and ATM theft from non-state actors. Even the United States was not safe from leakage of classified data perpetrated by the Edward Snowden. It also undermines US national security by making classified data public. It also invited much criticism from the then US president Obama. Another such example is the "Wikileaks", after the leakage of diplomatic cables and other classified reports about the opulent lifestyles of Tunisian President and his family which eventually led to sparking the Arab Spring (December,2010). Major data breaches have been reported almost in all of the sectors but most notable are technology, media and entertainment, retail, financial and insurance services, hospitality, gaming, government, healthcare, telecommunications, education, airlines, energy and several others.[14] India is a major stake holder in cyber diplomacy as there have been numerous cyber-attacks from non-state actors and according to the credible survey done by a security company 'Symantec', India is the second-most vulnerable country targeted by cyber-attacks. India's economy has shifted to IT-extensive services including commerce, banking and healthcare.[15]

Conventional to Cyber Space

The genesis of India-Pakistan conflict dates back to 1947 when the two nations of the subcontinent got independence from the British Raj. The unresolved issue of Kashmir has remained a real trouble between the two states and they were involved in fighting wars which further worsened their bilateral relations until recently. Instead of cooperation, both the states opted for the policies of aggression and engaged in a massive military buildup. India's acquisition of nuclear weapons in 1974 seriously threatened Pakistan and the latter decided to acquire a similar capability no matter what! India's nuclear tests of May 1998 invoked Pakistan to declare nuclear weapons and reach nuclear parity. Because of India-Pakistan's volatility of relations, South Asia is also termed as nuclear flashpoint but the next tug of war between both the contenders is in the domain of cyber warfare (baker 2014).[16]Modern technology especially the internet has revolutionized the communication even between the two adversary states, India and Pakistan. This technology in the hands of non-state actors posed a threat to state security as these actors started launching cyber-attacks on different states.

Defacing of Websites

The free and easy access of individuals to cyberspace makes states and their cyber infrastructure more prone to cyber-attacks, launched by anonymous hackers as well as states. Being confrontational even in cyberspace, India and Pakistan are facing cyber-attacks by non-state actors which sometimes are dubbed as state-sponsored attacks. Hackers, who deface websites of either government cheer by writing their desirous names and texts. But cyber threats are not limited to websites or cyberspace

even the critical infrastructure including strategic sites are also the ultimate target of such groups. Hackers on both sides are proactive in defacing the websites of government. Any red-letter day or a national event becomes the timeslot for hackers to hack and deface websites of the government organizations. There is another act that non-state-actors are performing i.e. espionage rivalry. While, defacing of the government website is not considered as a deadliest cyber-attack but with the passage of time, cybercriminals may dare to attack strategic system either through penetration into it or by bugging. An attack on a strategic system may trigger even war between the rival states. Moreover, it is hard to pinpoint those cyber attackers as they might operate from any part of the world.[17]

The month of May, 1998 is an important month in the calendar of Pakistan and India relations as India reincarnated India's nuclear status by threatening Pakistan's security whereas the latter retaliated by testing its nuclear weapon to bring a nuclear parity in the subcontinent. That was the time of initiation of cyber-war between both the nuclear actors. A group of hackers attacked India's Bhabha Atomic Research Centre's (BARC) website for which India blamed Pakistan for breaching cyber-security of BARC. That was the time when such sporadic cyber-attacks started happening on both sides. In November 2010, a group called 'The Indian cyber army' defaced a number of crucial governmental websites of Pakistan, including the ministry of defence, claiming cyber superiority.[18]

Some Pakistani hackers to retaliate to Indian hackers breached cyber-security of Indian Railways on September 14, 2014. Indian official website of Railways was hacked by the Pakistani cyber crew which operates under the title "XERXES" online. The hackers defaced 46 subdomains of the Indian Railways in response to the hacking of Pakistani Railways website by the Indian hackers.[19] Referring to the claims of Director General of Indian Military, Indian forces carried out surgical strikes inside Pakistan's territory on September 28, 2016, in the wake of the terrorist attack in Uri sector of Jammu and Kashmir. It was a terrorist attack on military check-post Uri which claimed the lives of 19 soldiers.[20]

Following the Uri terrorist attack, Indian hackers tried to hit Pakistan's key institutions but remained unsuccessful. In a reprisal of the false claims of Indian surgical strike against Pakistan, the Pakistan based hacker group defaced the website of India's National Green Tribunals on October 3, 2016. A hacker under the name of Faisal 1337 hacked Bihar State Electronics Development Commission website and Parbhani District Police website on 6 October 2016. From the Indian side, there was a similar response. Indian hacker "Hell Shield Hackers" group penetrated into several websites of Pakistan government such as the Ministry of textile and Central Cotton Committees.[21] Another

cyber-attack on the website of the Government of Pakistan by the Indian hackers reflected their intentions to breach the security of Pakistan's key organizations. Indian hackers disfigured the website of Pakistan "www.pakistan.gov.pk" on August 4, 2017, and posted Indian national anthem and Independence Day greetings on its wall. Indian hackers had defaced 30 websites of Pakistan government as a protest against the death sentence of captured former Indian Navy officer Kulbhushan Jadhav who was guilty of carrying out terrorist activities inside Pakistan.[22]

One of the cyber-attacks on Baluchistan government portal (balochistanculture.gov.pk) by the Indian hackers on 17 August 2017, left a message on the website stating that "We are Indian Cyber Heroes".[23] On April 26, 2017, in retribution of defacing Pakistan's Ministry of Railways' website, Pakistan hackers defaced 10 official websites of Indian universities including the website of Delhi University and Institute of Technology, leaving the words "Pakistan Zindabad" on their websites. The state-level confrontation between the two states has affected the psyche of the public, who perceive each other as arch enemies. Both the states are nuclear-armed rivals in South Asia and there is a need to promote Confidence-building Measures (CBMs) regarding cyber-security. If any non-state-actor attacks nuclear infrastructure through lethal malware then the possibility of nuclear clash cannot be ruled out.[24]

Cyber Espionage

Cyber espionage is an act of acquiring classified data or sensitive information without the knowledge and permission of the holder of information (individuals, organizations, governments). In the age of information revolution when states are engaged in cyber warfare, the cyber-espionage has reached its zenith and is mostly carried out by the technologically advanced nations. In cyber-espionage unethical means are employed to get access to the secret data, stored in the computers of a state. As with the advent of internet, states have switched to e-governance, such a breach becomes a serious threat to the security of the classified data of a state. In most of the cases, the hackers make use of 'Trojan horse' malware in the computer system of a target to exploit the data. Once the Trojan is installed in the targeted system it enables the hackers to get access to the computer network.[25]

Russia is one of the leading nations in cyber espionage and is using three types of hacking groups such as APT28, Uroboros and Energetic Bear. The APT28 is a Russian cyber espionage group, active since 2007 to steal data, create disruption and destroy the infrastructure. The group targeted various governments, armed forces and corporations via malicious code "Sofacy" across the world. The same espionage group is also accused of manipulating the presidential elections of the U.S. in 2016. Phishing emails were sent

to the members of the National Democratic Committee to change the password and then use the information to get access to the network of the committee.[26] Uroboros, originally a rootkit, invented in 2011 by Russia is also a very sophisticated computer virus which remained out of sight to the anti-virus software corporations. The virus remained undetected for 8 years.

The rootkit is able to take control of an infected machine, execute arbitrary commands and hide system activities. The virus has the ability to exploit the data and control the traffic of a computer network. The targets of Uroboros are governments and Information Technology firms. The German security agency G-Data reported that Uroburous is as deadly as the Stuxnet in its nature of attacks. The virus targets the windows of computers and software installed in the network. The U.S. government shielded against the Uroburous cyber-attack launched on the Department of Defense in 2010.[27] Cyber-attack on the power grid is more deadly than that of the military attack because electricity works like oxygen to run the system of a state. The compromised power system could have paralyzed the whole structure of a state in hours if it is not restored.

The states with cyber offensive capability like Russia are active to target the power grids of adversary states by the use of Energetic Bear. The Energetic Bear targets oil companies across the world but the major focus is on Europe and the U.S. From 2016 to 2017, the numbers of attacks on the energy companies of Turkey have exponentially increased. The Energetic Bear group is active since 2010. The group sends phishing emails, attached with documents drive in with the virus to the infected servers to get access to the classified data.[28] The Wall Street Journal reported that the Russian sponsored hacker groups specifically; Energetic Bear has acquired access to the power companies of the United States. Following a conflict with Ukraine over Crimea, the Russian hackers carried out cyber-attacks on the power grid twice in 2015 and 2016. There was speculation that the attack was a warning against nationalization of power plants owned by a Russian tycoon. The first cyber-attack has affected almost affected 225,000 people. However; the second attack was more sophisticated in its nature, which knocked out one-fifth of Kiev's power consumption.[29] Cyber-attacks on the Indian power grid are also increasing. In 2010, the Stuxnet virus affected about 10,000 computers in India. The Virus also hit the computer network of Haryana and Gujarat boards of electricity. Moreover, the Indian offshore Oil Company "ONGC" was also hit by the virus. Similarly, Jawaharlal Nehru Port Trust, the largest container port came under the cyber-attack in June 2017. Consequently, the port had to shut down its three stations following a cyber-attack.[30]

In 2017, Wanna Cryransomware affected 150 states including the U.S and France, infected 40,000 computers across the world. It also targeted the electric company of Indian state West Bengal. The company had to suspend the payment of bills for a whole day.[31] As India claims to be one of the largest economies and if such cyber-attacks continue on the power grid, eventually the economic growth will halt, leading towards unrest and riots. Besides Russia, China is also proactive in cyber espionage. The cyber espionage group Axiom is a Chinese sponsored group which is accused of attacking different agencies of the U.S. over the last 6 years, the Axiom espionage group uses malware against human rights organizations, corporations, and government. The group is accused of stealing trade data of the U.S. It is a matter of concern for India as India is a competitor of China and also has developed I.T sector. With the increased competition of China and India in economic reality, there is a grave possibility of cyber-attacks on Chinese financial institutions and vice versa.[32] Managing director of Fire Eye, a U.S based cybersecurity, reported that the Chinese sponsored cyber-espionage group "APT10" is active in the U.S, Japan, and Europe in stealing business data from the industries such as engineering, construction, aerospace, and telecommunication. For India, fear is high given the stakes. India is an emerging economy and cyber espionage in the economic sector is a setback for investors. If cyber-espionage continues in the economic sector, the investors are likely to transfer their capital to another country. Such a situation will worsen relations between India and China.[33]

"Kaspersky" a cybersecurity and antivirus firm based in Moscow estimated that India is under the attack of cyber espionage carried by a hacker group known as "Danti". The group is accused of targeting government websites to steal classified data. Referring to the findings of the firm, the group is sponsored by Chinese hackers. The group targets the vulnerability of the computer network and gets access to the data, stored in the exploited machines.[34] Like India, Pakistan has also become the prey of cyber espionage. The United States' National Security Agency (NSA) is, in the name of data monitoring, spying on Pakistan through online communication systems. The NSA bugged systems to intercept 13.5 billion emails, phone and fax communications of Pakistani citizens. Pakistan is the second most monitored nation after Iran.[35] Iran and Pakistan have become a victim of state-sponsored cyber espionage; therefore they need to team up against such kinds of attacks.

As cybersecurity agency "Symantec" reported that the security units of India and Pakistan are under the attack of state-sponsored cyber espionage since 2016. Referring to the reviewed report by Reuters, both the states are becoming the target of espionage campaigns of hacker groups. The similarities of attack and goals illustrate that the targeting groups are sponsored by a single entity in due course (a country). The espionage campaign intensified at the time of India and China face-off along the border

following a border conflict near Bhutan. The report warned that in future the militaries and security agencies in South Asia are vulnerable to serious cyber-attacks. The hackers install malware in the documents which are about the security issues of South Asia such as separatist movement, intrastate conflict, and Kashmir. Once the target opens the document, the malware embedded in the files has the potential to take a screenshot of the data, stored in the computer system and exploit it.

Commenting on the cyber espionage the official of FireEye Tim Wellsmore, director of threat intelligence for the Asia Pacific region, said that the South Asian region is a hotspot of such a conflict. Any issue between the states speeds up the cyber espionage in the region. The report of "FireEye" is an eye-opener for India and Pakistan because both of the states have become a prey to cyber espionage and it has become a challenge to protect the classified data from state-sponsored cyber espionage. Moreover, adversary states and nonstate actors such as terrorist groups could have taken advantage of the persistent Indo Pak conflict through espionage. Both states need to collaborate in cyberspace to avoid cyber-attacks.[36]

Threats to Financial Institutions

Once the banks were considered a safe place to keep the money but with the increase of cyber-scamming even banks are not safe. Hackers because of the cyber spoofing are able to steal money from banks and other financial institutions. The phenomenon of ATM theft is not a new one. In 2010, the hackers used skimming devices in European countries to withdraw cash. Likewise, the banking sector is on the hit-list of cybercriminal and every year hackers steal billions from all over the world.

The Center for Secure Information Systems (CSIS) reported in 2014, that the economic sector is more prone to cyber-attacks. As a result the annual loss of the economy to cybercriminals has reached up to $ 500 billion. The cyber-attacks on the financial institution are due to the digitalization of data and online transfer of money. As people, firms, agencies, and governments deposit money in banks to do transactions and business. The money deposited in banks is at the risk of theft because of the skimming devices. Although banks have increased their security, that is not foolproof yet. Meanwhile, cybercriminals have also acquired advance offensive technology to steal money. The CSIS suspects the involvement of hackers from three states in financial theft specifically Iran, North Korea, and Russia.[37]

In the case of India and Pakistan, the banking sector has become a lucrative target for cybercriminals. The cyber-attacks against the financial institutions will shake the confidence of foreign investors to invest money. The halt of FDI in both states will affect the growth of the economy to the largest extent. In September 2015, Indian based

hackers launched a cyber-attack on Habib Bank Limited. As a result, the bank blocked the credit cards of the customers for the time being to avoid loss of funds. In 2016, the bank came under the cyber-attack once again and blocked the debit cards of the customers.[38]

In 2017, almost 559 bank accounts of Habib Bank Limited (HBL) customers were compromised through card skimming devices and Rs10.2 million were stolen.[39] The FIA in response to the complaint of HBL investigated that the hackers used skimmer devices in Khayaban-e-Ittihad (Karachi) to steal money from the accounts of people.[40] The head of FIA Capt. Mohammad Shoaib revealed that data from all the banks of Pakistan was stolen in a recent cyber-attack. The hackers based outside of Pakistan breached the security system of the banks and stole money from the accounts. Almost 10 banks blocked the international transaction temporarily as the data of 800 accounts was sold in the black market. Another cyber-attack was reported by the Bank Islami on 27 October 2018. The bank lost about Rs2.6 million.[41] Referring to the report of cyber Security Company "IB" the data of 19,000 debit cards of 22 banks of Pakistan were compromised in cyber-attacks on the banks which took place on 26 October 2018. The stolen data of accounts was dumped on the dark web under the title of "PAKISTAN WORLD-EU-MIX-01". The hackers sold the data of at least nine Pakistani banks on dark web. There were more than 8,000 reduplicated ATM cards available for sale between $100 to $135 each. On Oct 28, a press release of Bank Islami stated that it had become a victim of cyber-attack.

According to the report of State Bank of Pakistan, the compromised ATM cards were charged in Russia and the U.S. A total of 19,864 debit card details belonging to 22 Pakistani banks are being sold in the dumps circulating on the Darknet Numbers courtesy cybersecurity firm PakCERT.[42] Like Pakistan, the banking sector of India is also one of the most vulnerable sectors to hackers. The Indian government Union minister Hansraj Gangaram Ahir affirmed that from 2016 to 2017, almost 50 cyber-attacks on the 19 financial institutions were reported. According to the minister, banks were given a guiding principle by the Reserve Bank of India (RBI) for the cybersecurity. Moreover, mock cyber drills were organized among 148 financial institutions for the alertness of cyber-attack. In order to upgrade the technology against cyber-attacks, Rs.1000 crore were allocated to conduct research on the issues related to cybersecurity.[43]

However, despite government efforts to put a curb on financial theft, the cybercriminals continue to rob money from the banks. The one of the oldest Urban cooperative banks of India "Cosmos" came under the cyber-attack on 11 August 2018. The hackers cashed out around 100 crores in 28 different countries. The Reuters reported that the hackers launched an attack on the server of the bank via malware to steal the data of

the customers. Moreover, 139 million rupees were transferred to a Hong Kong-based company by the use of "SWIFT" a secure network to transfer money among the 212 states. India is considered as a leading country in the IT sector and Pakistan has the potential of the workforce. Sharing of the data of cybercriminals and their modus operandi and a joint effort by both the states is likely to reduce the potential of cyber-attacks in the coming future. In addition, both states need to develop a proper mechanism to try cyber criminals in the courts. Otherwise, cybercriminals will keep haunting financial institutions and they may also dare to attack strategic assets of both the countries.[44]

Cyber Threat to Nuclear Actors

Pakistan and India are nuclear states and the emerging threats of cyber warfare pose a grave challenge to protect the nuclear arsenals from the reach of cybercriminals because nuclear arsenals are connected with the computer system which is vulnerable to be hacked by the states and nonstate actors. The hackers by the means of malware could penetrate into the nuclear facility, steal data, alter code or even sabotage the plant. The first ever such kind of nuclear incident happened in the U.S. in 1979 at American Air/Aerospace Defense Command (NORAD26), when an employee downloaded the war game movie on the computer. The computer began to give alert that a missile from the submarine of the west coast of the U.S. has been launched. As a consequence, nuclear weapons went on alert following a declaration of states level nuclear war. That was the time of cold war in which US-Soviet rivalry was on its peak. The misperception created by the computer could have led to a nuclear exchange between the two nuclear contenders.

Incoming era, the security, and management of nuclear weapon will be very hard-hitting for the policymakers because of the reliance on nuclear weapons on a complicated network of computers. Because some of the missiles are installed in remote areas and those are controlled through the network of computer codes. Though such programs are highly confidential they still are under the threat of cyber-attacks which may either launch those missiles accidentally or sabotage the system completely so that despite command from authorities these missiles may not work. This kind of threat was unimaginable 50 years ago but now has become a reality. The attack Stuxnet is the glaring example of cyber sabotage. The Stuxnet virus was launched by the U.S. in collaboration with Israel against the Iranian nuclear program which physically destroyed the centrifuges of Natanz nuclear power plant.

The Stuxnet has emerged as a new security challenge for the safety of nuclear arsenal from the state-sponsored cyber-attacks. There is quite a great possibility that an

adversary state may steal nuclear secrets or strategic data through cyber espionage. However, the nuclear espionage started as early as the 1940s when the spies of soviet acquired the design of American nuclear bomb "The Manhattan project". However, the cyber nuclear espionage is attributed to Markus Hess a German administrator who penetrated into the computer system of the U.S defense and military establishment in 1986 to attain data of nuclear weapons. He, being a KGB operative was assigned the task of acquiring information about the nuclear plans of the Reagan administration and the Strategic Defense Initiative. Later that year, India's Bhabha Atomic Research Centre (BARC) was hit by an American teenage hacker and he downloaded several files containing critical data. In the same way, Russia is accused by the U.S for sponsoring 'Moonlight Maze' attack in 1999 to get the classified information from the network of Pentagon and government institutions.

Day by day state-sponsored cyber nuclear espionage is snowballing which is a serious violation of state sovereignty. The web world is the most connected world in the world where citizens, friends and adversaries can interact with each other even if the other side does not want to contact. Similarly, access to the information contained by the system is valuable, which the hackers seek to obtain and stash. Israel launched "Operation Orchard in 2007" against Syria after penetrating into the government institutions by installing a Trojan to obtain information about nuclear ambitions.[45]

In a similar case, a group of teenagers, On 3 June 1998, penetrated into the security system of Indian "Bhabha Atomic Research Centre" and got access to the classified data as a retaliation of Indian nuclear test. The incident exposed the vulnerability of India in cyberspace. It raised concerns about the safety of nuclear weapons in the cyber age. The cyberspace is so vulnerable that even a group of teenagers could penetrate into the critical infrastructure of a state, whereas India quickly holds Pakistan responsible for such cyber-attacks without any concrete evidence at hand.[46]

From Nuclear to Cyber Confidence Building Measures

India and Pakistan need to develop confidence-building measures in the first phase of cooperation and the second phase should be more pragmatic to reach some agreements to avoid any accidental confrontation and mutual coordination to curb cyber-attacks on either party. There has been a history of CBMs between India and Pakistan despite conflict over the Kashmir. India and Pakistan's respective prime ministers (Rajiv Gandhi and Benazir Bhutto) concluded a landmark Agreement "India-Pakistan Non-Nuclear Aggression Agreement" On December 31, 1988. It was a landmark achievement of CBMs between both rivals. By concluding the agreement, both states reaffirmed to refrain from damaging the nuclear facilities of each other. Because there

was a fear if any state launches an attack on other's nuclear facility that might lead to a nuclear clash. After the nuclear tests of May 1998, it was anticipated that India and Pakistan will be engaged in nuclear confrontation but there started a new era of CBMs between the BJP led government and Pakistan. The Lahore Declaration of February, 1999 marked a new era in India-Pakistan bilateral ties when Atal Bihari Vajpayee visited Pakistan to sign the historic Lahore Declaration and kicked off CBMs.

Both the sides pledged to "take immediate steps for reducing the risk of accidental or unauthorized use of nuclear weapons and discuss concepts and doctrines with a view to elaborating measures for confidence building in the nuclear and conventional fields, aimed at prevention of conflict (NTI 2011). The terrorist attack on Indian parliament in December 2001 derailed the peace process between both the countries as the time passed by both the nations could not reach the same level of CBMs. With the increase of cyber-attacks on India and Pakistan both the states are still blaming each other instead of cooperating to pinpoint the state and nonstate actors that are to cause serious infliction to India-Pakistan bilateral relations. Recent shadows of war between Pakistan and India were looming in the wake of Pulwama terrorist attack. Indian air force tried to make surgical strikes in Pakistan that could certainly lead both the nations into a devastating war, but Pakistan's restraint prevented the war. According to the press release of the foreign office, India and Pakistan exchanged a list of nuclear installations on 1st January 2019. Pakistan also handed over the list of its nuclear installations to the Indian high commissioner at the Ministry of Foreign Affairs. Both the states share the list of nuclear installations on the 1st January every year in compliance with article II of the "India-Pakistan Non-Nuclear Aggression Agreement" signed on 31st December 1988. Pakistan and India need to conclude an agreement in cyberspace because both are facing a similar threat of cyber-attacks by nonstate actors or any other country. India did sign agreements with U.S, Israel and many other countries but it did not sign any agreement with Pakistan in the cyber domain. As the hackers on both sides are hyper-active in defacing of websites and cyber espionage, therefore, India and Pakistan need to take concrete measures to prevent such cyber-attacks on their strategic assets.[47]

Conclusion

Cyber war is the war of future where cyber powers will be attacking their rival states through malwares and crashing their systems whether connected to any public service or strategic weapons. Technologically advanced countries are in an undeclared state of cyber-war against each other because it is complicated to obtain evidence against cyber attackers for being sponsored by states. Therefore, individual hackers are blamed for such cyber intrusions. The United States and Israel jointly tried to disrupt the nuclear

program of Iran through Stuxnet but such a war may lead to an undesirable consequence if even individual hackers or non-state-actors manage to penetrate into nuclear program of any nuclear actor. *The New York Times* report on Russian series of cyber-attacks on the US nuclear facilities, water and electric system between 2015 to 2017, and US accusations of manipulating presidential elections (2016) are far graver than expected. In case of India and Pakistan though the cyber-attacks have not been very serious, but it is just the beginning of cyber-war which may get serious. In order to develop a mechanism to deal with cyber-attacks from non-state-actors, both the countries should engage in cyber-diplomacy and share details of such cyber-attacks on their respective institutions. Such a diplomatic engagement is likely to avoid any mistrust and direct clash between both the countries and they may know potential cyber threats coming from great powers or non-state-actors.

References

[1] Marie Baezner, "Regional Rivalry between India-Pakistan: Tit-for-Tat in Cyberspace" (Zürich Switzerland: Center for Security Studies (CSS), ETH Zürich, August 2018), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Stuart Winer, "'Dutch Mole' Planted Stuxnet Virus in Iran Nuclear Site on Behalf of CIA, Mossad," The Times of Israel, accessed November 19, 2020, https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/.

[6] Azriel Bermant, "Pakistan Is the Only Muslim Nuclear State – so Why Is Israel's Hysteria Reserved for Iran?," Haaretz, May 20, 2015, https://www.haaretz.com/opinion/.premium-why-isn-t-israel-hysterical-over-pakistan-s-nuclear-bomb-1.5364286.

[7] Basma Khalil, "Emerging Cyber Warfare Threats to Pakistan, Modern Diplomacy," Modern Diplomacy, February 14, 2020, https://moderndiplomacy.eu/2020/02/14/emerging-cyber-warfare-threats-to-pakistan/

[8] "Convention on cyber crime" Europal. 8 November, 2013.

[9] Michael N. Schmitt, ed, *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press (2013): 1-12

[10] Rita Boland, "Improving Threats Hunting with Big Data" Afcea, 2008, Retrieved January 10, 2019 from https://www.afcea.org/content/countries-collaborate-counter-cybercrime

[11] Joseph Nye S Jr, "Nuclear Lessons for Cyber Securit?," *Strategic Study Quarterly* (2011): 18-38.

[12] Elizabeth White Baker, "A Model for the Impact of Cybersecurity Infrastructure on Economic Development in Emerging Economies: Evaluating the Contrasting Cases of India and Pakistan," *Information Technology for Development* (2014): 122-139.

[13] Baker.

[14] Benedikt Kammel, Demetrios Pogkas, and Mathieu Benhamou, "These Are the Worst Corporate Hacks of All Time," *Bloomberg.Com*, accessed November 19, 2020, https://www.bloomberg.com/graphics/corporate-hacks-cyber-attacks/.

[15] Reda Baig, "Could Offensive Cyber Capabilities Tip India and Pakistan to War?," The Diplomat, March 26, 2019, https://thediplomat.com/2019/03/could-offensive-cyber-capabilities-tip-india-and-pakistan-to-war/.

[16] Baig.

[17] Baezner, "Regional Rivalry between India-Pakistan: Tit-for-Tat in Cyberspace."

[18] Aqsa Garsein, "Pakistan vs India: Who's the Better Hacker?," The Express Tribune, August 16, 2012, http://tribune.com.pk/article/13457/pakistan-vs-india-whos-the-best-hacker.

[19] Abhishek Kumar Jha, "Pakistani Hackers Defaces Official Website of Ministry of Railways of India," *TechWorm* (blog), September 14, 2014, https://www.techworm.net/2014/09/pakistani-hacks-indian-railways-website.html.

[20] Arka Biswas, "Surgical Strikes and deterrence- stability in South Asia", *Observer Research Journal.* (2017): 1-24.

[21] Aditya Purani, "How India-Pakistan hackers escalated cyber war post surgical strikes," *Daliyo*, October 12, 2012, https://www.dailyo.in/politics/India-Pakistan-war-cyber-security-national-green-tribunal-hackers/story/1/13367.html

[22] Shashank Shekhar, "India and Pakistan at war in cyber space ahead of Independence Day," *Bussiness Today*, August 4,2017. https://www.businesstoday.in/ current/economy-politics/india-and-pakistan-at-war-on-cyber-space-ahead-of-independence-day/story/257753.html

[23] "India's cyber attack on Balochistan government," *Times of Islamabad*, August 17, 2018, https://timesofislamabad.com/17-Aug-2018/india-s-cyber-attack-on-balochistan-government

[24] "10 Indian University Websites Hacked by Pakistani Hackers," *Techjuice*, April 26, 2017, https://www.techjuice.pk/10-indian-university-websites-hacked-by-pakistani-hackers/

[25] Mambodza T Walter, "Cyber Espionage a threat to Information Security", *International Journal of Computer Application* vol 5, no 3 (2015): 91-97.

[26] Pierluigi, Paganini, "APT28: Fire Eye uncovered a Russian cyber espionage campaign," *Security Affairs*, October 29,2014. https://securityaffairs.co/wordpress/29683/ intelligence/apt28-fireeye-russian-espionage.html

[27] Geraldine, Hunt, "Is the RussianGovernment behind the Snake Virus?", *Titanhq*, March 23,2014. https://www.titanhq.com/blog/the-russian-snake-uroboros-virus-stealing-your-data-for-8-years

[28] "Energetic Bear/Crouching Yeti: Attacks on Servers," Kaspersky, April 23, 2018, https://securelist.com/energetic-bear-crouching-yeti/85345/.

[29] "Russian Hackers Penetrate US Power Stations," *BBC News*, July 24, 2018.

[30] "Critical infrastructure on target: A cyber attack that could be worse than war," The Economic Times, November 4, 2017, https://economictimes.indiatimes.com/tech/internet/critical-infrastructure-on-target-a-cyber-attack-that-could-be-worse-than-war/articleshow/61508816.cms

[31] Nir Kshetri and Rely Voas Jeff, "Hacking Power Grids:A current problem", *Computer*, vol 15 (2017): 91-95.

[32] Mambodza T Walter, "Cyber Espionage a threat to Information Security", *International Journal of Computer Application* vol 5, no 3 (2015): 91-97.

[33] "FireEye Says China-Based Hacker Group Now Targeting Firms in India," *Gadgets*, April 10, 2017, https://gadgets.ndtv.com: https://gadgets.ndtv.com/internet/news/fireeye-says-china-based-hacker-group-now-targeting-firms-in-india-1679607

[34] "Kaspersky suspects cyber espionage attack on government accounts", May 25, 2016, https://www.thehindubusinessline.com/info-tech/kaspersky-suspects-cyber-espionage-attack-on-government-accounts/article8646361.ece

[35] Sadia Rasool, "Cyber security threat in Pakistan: causes Challenges and way forward", *SocioBrains* (2015): 21 - 34.

[36] Rahul Bhatia, "Exclusive: India and Pakistan hit by spy malware - cybersecurity firm", *Reuters*, August 28, 2017, https://www.reuters.com/article/us-india-cyber-threat/exclusive-india-and-pakistan-hit-by-spy-malware-cybersecurity-firm-idUSKCN1B80Y2

[37] James Lewis, "Economic Impact of Cybercrime— No Slowing Dow", *CSIS* (2018), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

[38] Jawad Ali, "HBL under cyber attack", *Technology Review*, March 7, 2017, http://www.technologyreview.pk/hbl-under-cyber-attacks/

[39] Zubair Ashraf, "In Pakistan, the banking sector most vulnerable to cyber attacks", *The News*, December 17, 2018, https://www.thenews.com.pk/print/257280-in-pakistan-banking-sector-most-vulnerable-to-cyber-attacks

[40] Salman Siddiqui, "Beware - hackers are going after ATMs in Pakistan" *Tribune*, December 3, 2017, https://tribune.com.pk/story/1574702/2-beware-hackers-going-atms-pakistan/

[41] Shakeel Qarar, "Almost all' Pakistani banks hacked in security breach, says FIA cybercrime head", *Dawn*, November 6, 2018, https://www.dawn.com/news/1443970

[42] "Over 19,000 card details from 22 Pakistani banks stolen in the cyber-security breach", *Geo News*, November 6, 2018, https://www.geo.tv/latest/217471-cyber-attack-on-Pakistani-banks-what-we-know-so-far

[43] "50 cyber attack incidents reported in the financial sector: Govt", *Livemint*, August 1, 2017, https://www.livemint.com/Industry/MBqlWLIFkpR4W34sdA6TqN/50-cyber-attack-incidents-reported-in-financial-sector-govt.html

[44] Dan Gunderman, "Incident Of The Week: Indian Bank Loses $13.5M In Costly Cyber-Attack", *Cshub*, August 17, 2018,https://www.cshub.com/attacks/news/incident-of-the-week-indian-bank-loses-135m-in-costly-cyber-attack

[45] Andrew Futter, "Cyber Threats and Nuclear Weapons New Questions for Command and Control, Security and Strategy," *RUSI* (2016): 1-39.

[46] "When India's Nuclear Secrets Were Hacked," Madras Courier, May 17, 2017.

[47] "Pakistan, India exchange lists of nuclear installations", *The News*, January 1, 2019.