Governance and Management Review (GMR)
Vol.3, No. 1, January-June 2018

Cyberspace Management in Pakistan

Dr. Tughral Yamin*
Associate Dean
Centre for International Peace & Stability
National University of Sciences and Technology (NUST)

Abstract

Although security ranks high on Pakistan's national agenda but in the increasingly complex threat milieu, cyber security usually gets relegated to the bottom rung and sometimes it is literally ignored. There is no gainsaying the fact that we ignore this vital subject only at our own peril. Given the chaotic nature of the cyberspace, it is important to manage it properly. Internet has its advantage. It has made the availability of knowledge at the click of the button. Connectivity has made life simpler at different planes, ranging from the personal to official, but has also introduced a number of vulnerabilities. Access to Internet is now considered as a basic human right. At the same time cyberspace has become the fifth dimension of warfare. In the absence of international cyber treaties and agreements, states are actively carrying out pervasive surveillance against friends and foes and launching devastating cyber-attacks. Terrorists are using cyberspace for recruitment, funding and propaganda. Criminals are having a field day in siphoning off millions of dollars from online ecommerce activity; the kid in the basement and freelancers high on digital adrenaline are hacking just for the kicks of it.

Such threats need to be responded to by coordinating cyber security activities at the national level. Robust cyber governance bodies needs to be created at all levels. Cyber leaders and advisors need to craft effective policies and enact legislations to counter the ill-effects of debilitating cyber-attacks i.e. disruption of communication services and damage to command and control systems that

---

* The author is a retired brigadier. He is the author of a book on Cyberspace CBMs between Pakistan and India. He heads the Centre for International Peace and Stability (CIPS) in the National University of Sciences and Technology (NUST), Islamabad.

cause the government to malfunction and make the businesses and industry lose hours of productivity among other things. Unfortunately, Pakistan is way behind other nations in putting its cyber act together.

This paper discusses the voids at the policy planning level and suggests proposals to come up with a suitable strategy to respond to the emerging cyber challenges.

Keywords: Cyberspace Management, Cybersecurity, Cyber Policy, Cyber Budget.

Introduction

Data's importance in the digital age cannot be under estimated. There is no gainsaying the fact that it has to be protected at all costs because it is of vital importance to a country and an organization. All countries use all possible means to syphon off information populating the computer networks of their adversaries and competitors to gain a competitive edge over them. Domestically data has been used to discredit political opponents. The debacle of Mr. Nawaz Sharif because of the treasure trove of unloaded by the Consortium of Investigative Journalists provided incontrovertible about his family's business investments in dubious off shore companies. The proliferation of social media has made it easier to harvest information provided willingly by unwary users. Facebook is a case in point. The information gathered by Cambridge Analytica by posting an application on his widely used platform to help Donald Trump, the unlikely candidate, to win the American election in 2017.

Data security in Pakistan is unfortunately not the top of either the national or any organization‟s agenda. There regular reports of databases being breached. The hacking of Careem ride share services is a case in point. Cybersecurity experts darkly hint that foreign hackers are planning to hack the electoral data bases ahead of the upcoming elections. Officials of the National Database and Registration Authority (NADRA) had been at pains to explain that data has not been made available that may skewer the results of the elections.

Data loss can be extremely damaging to the nation and commercial concerns. Why this official neglect? There are a number of reasons for this. mainly people at the helm of affairs fail to grasp the importance of cyber security management. At the end, a few suggestions have been made to improve the cyber security apparatus in Pakistan. A qualitative research method has been used to put this paper together.

Officially Pakistan does not have a national policy on cyber security. From time to time cyber security makes an appearance in the national debate but there is never a sustained discussion on the subject e.g. speaking at a seminar organized by an Islamabad think tank on the subject of "Cyber Secure Pakistan – A Policy Framework," the former National Security. Advisor (NSA) Lieutenant

General Nasser Khan Janjua (retired) proposed that the country needed e-governance council to formulate cyber policy on globally accepted parameters (Jabri, 2018). So the policy or the lack of it is visibly mainly in terms of statements by policy makers at policy forums.

The most visible activity on the Pakistani cyber landscape has been the legislation on cybercrime. The Cyber Crime bill aka Prevention of Electronic Crimes Act (PECA) was approved in 2016 by both houses of the parliament (Haq, 2016). Several amendments raised by digital rights activists in the interest of the digital consumers were added in PECA (Usman, 2016). The very vocal activist lobby had waged a relentless campaign to oppose those parts of the bill that they thought infringed upon the rights of the citizens ("Bolo Bhi‟s Meeting and Our Call-To-Action on Cybercrime Bill,"). The animated discussion over the PECA actually diverted the attention of all concerned from the real issue at hand i.e. cybersecurity

I met the minister of IT in the summer of 2015 to present her my book Cyber CBMs between Pakistan and India published by NUST publishing in 2014. She graciously granted me an immediate audience. After I had thanked her and presented her my book, I broached the subject of cybersecurity. The minister was candid enough to admit that the issue had not blipped on the official radar. I quite understand her point of view because at that particular moment in our national history, the government was involved fulltime in containing the toxic fallout from the protests organized by the Pakistan Tehreek-e-Insaf (PTI) from spreading from Ground Zero in D Chowk next to the Constitution Avenue to other corners of the country. Quite interestingly, PTI was making effective use of the social media to mobilize and sustain its agitation for three long months. So, the government was actually ignored the threat emanating from the cyberspace at its own peril.

The second thing that came up in our discussion was the issue of responsibility i.e. who was supposed to look after the cyber borders, if at all there is such a thing in digital space. The minister wasn‟t sure whether it fell in her domain or that of the ministries of interior of defence or the intelligence agencies. She was again right; cyberspace is the collective responsibility of a number of ministries and departments and needs joint ownership. The correct person to deal with cyber issues in the minister‟s mind was Senator Mushahid Hussain Syed. In his capacity as the Chairman of Senate‟s Defense Committee he had been instrumental in organizing Policy Seminar on Cybersecurity, establishment of Cybersecurity Task Force and publication of a manual for journalists for awareness in cyber issues. Due to his keen interest in the subject I had invited him as chief guest for the launching ceremony of my book on cyber CBMs. Senator Syed‟s credentials as a champion of cybersecurity notwithstanding, it was rather discomfiting to note that the minister was willing to cede space on an important issue of national security to a person, who at that time was a member of the opposition and.

had limited political influence or clout to put cybersecurity in the national limelight. The political status of the Senator has experienced a change after his re-election to the Senate with the support of the ruling party in 2018. Perhaps he would be in a better position to contribute positively to the issue of cybersecurity in the country with his new political affiliation.

National Security

The subject of security figures high on any country‟s national agenda. It is after all the primary responsibility of a government to protect the state and its citizens from any kind of internal or external threat. No government can afford to shirk this responsibility. Outsourcing it to someone else can amount to bartering away the nation‟s sovereignty. The duty of the government to protect the life and limbs of its citizens is enshrined in Article 9 of the constitution. Security covers a wide spectrum of issues, such as its territorial integrity, political sovereignty, economic autarky, self-sufficiency in food and energy, environment protection and in the modern age and era cybersecurity. Even in Pakistan in informed circles cyber security is considered a matter of national security (Baloch, 2015). This notwithstanding, there is a stark realization is stark that this subject has yet to find a niche for itself in the pantheon of national security (Desk, 2015).

In dispensing its duty to ensure national security, the government is assisted by the parliament, so that no law is passed that simultaneously safeguards the interests of the state and protects it from external aggression and internal turmoil, while ensuring the civil rights and liberties of its citizen. To ensure that the writ of the state extends all over its sovereign territories, it uses all instruments of the sate such as the armed forces and law enforcement agencies and the judiciary to implement its national security mandate. A citizen owing allegiance to a state is required to support the government in this sacred duty. The ability of the government to provide security to its citizens depends upon its national power potential, which is directly proportional to its political power, diplomatic influence, economic capacity and military might. A number of governments including Pakistan arrogate the responsibility of coordinating national security matters to the National Security Council (NSC). In Pakistan this forum brings together the civilian and military leadership so that they are on one page insofar as national security is concerned. The Pakistani NSC has as its members the President, the Prime Minister, the Chief Ministers of all provinces, the Chairman Senate, the Leader of Opposition in the Parliament and all the services chiefs (Ali, 2015).

The appointment of retired Lieutenant General Nasir Khan Janjua to the office of the NSA in 2015 by the previous government was considered an enhancement in the stature of the office (Nation, 2015). Besides the NSA‟s office, there are other cabinet and parliamentary committees that look into national security matters. Some of these such as the Cabinet Committee on National Security (CCNS)

has been accused of underperforming.

All security issues need to be seen through the prism of a comprehensive security policy. Such policy should be supported by four essential pillars. First and foremost only a strong leadership with the backing of the authorities concerned can provide strategic vision and across the board coordination on security matters entrusted to them. Secondly, a policy framework needs a clear cut and precise mission statement. Thirdly, to execute the vision and mission there is a need for adequate material and human resources. Fourthly, the managers of any enterprise needing security must be equipped to operate under clear and unambiguous sets of rules and regulations that they can enforce firmly. These principles are necessary in all issues concerning security (PILDAT, 2005).

There is no comprehensive security policy in Pakistan covering all forms of internal and external threats. The Defence Policy and the National Internal Security Policy (NISP) address these threats separately. The defence matters are dealt with by the MOD and usually remains the exclusive preserve of the armed forces. Internal security is mainly the responsibility of the MOI. The first NISP was issued by the MOI in 2014(Rana, 2013). It mentioned that it focus on cybersecurity without going into the specifics (Nation, 2014). The basic thrust of the Policy remained on how to eliminate terrorism. This Policy was supplemented by the National Action Plan (NAP) of 2015 - A twenty point agenda to eliminate terrorism in the country. Again, it did take cognizance of the cybersecurity aspects but only within the framework of counter terrorists (Pakistan). In 2018, the MOI issued NISP 2018, laying out a roadmap for internal security for the next five years.

Cyber Security

The entire gamut of cybersecurity means protecting, detecting and responding to attacks directed against computers and servers storing private and official records; personal computers and cell phones; entertainment gadgets like digital cable, mp3s; intelligent systems controlling the means of travel like car engines and airplane navigation systems; online electronic shopping stores and credit cards etc (CERT, 2019). One of the primary issues of cybersecurity involves protection of personal, professional and official data. There are several definitions of cybersecurity. A popular one states: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user‟s assets. Organization and user‟s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user‟s assets against relevant security risks in the cyber environment. The general security objectives includes,

availability, Integrity; which may include authenticity and non-repudiation and Confidentiality (ITU).

Cybersecurity refers not only to the protection of official and personal computer and data processing infrastructure and operating systems (OS) from harmful interference but also protection of critical infrastructure. In fact defining what is national critical infrastructure and how to defend it on the digital fund occupies the attentions and energies of most developed countries. Large sums of monies are actually devoted for this purpose.

Cyber-attacks can result in long downtimes that can momentarily or for the long term disrupt the decision making loop. There are minor irritations like the defacement of official and private websites. Major disruptions can be caused crashing of servers or loss of huge amounts of data. Cyber-attacks can cause not only psychological trauma but also physical damage and financial losses and acute loss of faith in a system. It can cause panic among the people, collapse of a system and paralysis at the highest echelons of decision making.

Cyberspace is not the sole preserve of state actors. It is open territory for non-state actors, criminals, freelancers and the kid in the basement to operate with impunity. This makes it all the more difficult to forensically retrace the trail of a cyber-attack and attribute it to a particular person or entity. Many times the actual source of attack is an insider within the organization with the urge to settle a score or satisfy an ideological leaning(Stolfo et al., 2008). It is difficult to mount a cyber-counterattack because of problems related to attribution, absence of set rules of engagement and the proportionality of the response. International norms and rules on the subject are hazy but countries and organizations have crafted laws to persecute those interfering with their digital systems(Schaeffer, Chan, & Ogulnick).

The issue of information security has been on the UN agenda since the Russian Federation in 1998 first introduced a draft resolution in the First Committee of the UN General Assembly and was adopted without a vote (UNODA). The matter has, however, not been sent to the UN Security Council. A Security Council resolution as opposed to the General Assembly resolution is binding on member states.

The US government, as do many others, attach great importance to their national cybersecurity. In the opinion of former President Obama: America‟s economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas (Policy).

Five things uppermost in US administration's priorities on cybersecurity are:

- Protection of the critical infrastructure.
- Improving the ability to identify and report cyber incidents to carry out a timely response.
- Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.
- Securing federal networks by setting clear security targets and holding agencies accountable for meeting targets.
- Shaping a cyber-savvy workforce (Order).

In February, 2013, President Obama signed the Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity (Government, 2017)." In May 2017 President Trump issued another executive order to strengthen the cybersecurity of his country. A host of other documents clearly give out the US government‟s position on cybersecurity such as the Cybersecurity Framework, a guide developed collaboratively with the private sector for private industry to enhance their cybersecurity (NIST). The US International Strategy for Cyberspace includes plans to develop international norms of behavior in cyberspace, promote collaboration in cybercrime investigations (Mutual Legal Assistance Treaty modernization) and international cybersecurity capacity building (W. House, 2011). The Cybersecurity Cross Agency Priority (CAP) Goal represents US Administration‟s highest cybersecurity priorities for securing unclassified federal networks (Daniel). Other important documents include:

- Presidential Policy Directive 28 (PPD-28) "Signals Intelligence Activities," 2014 (Government).
- Presidential Policy Directive 21 (PPD-21) "Critical Infrastructure Security and Resilience," 2013.
- Presidential Policy Directive 8 (PPD-8) "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 2011.
- Cyberspace Policy Review, 2009.

Cybersecurity Models

Most countries of the world have designated organization or organizations to deal with national cybersecurity needs. The leadership is usually assigned to powerful and influential people with direct access to the country‟s chief executive. Adequate sums of money are allocated for cybersecurity and clear cut policy guidelines exist for cybersecurity management. A great deal of resources are invested to secure the national critical infrastructure.

The Office of the National Cybersecurity Coordinator is at the top of the US cybersecurity food chain. The cybersecurity czar has direct access to the president. Currently Michael Daniel, a Special

Assistant to the President is the Cybersecurity Coordinator. 43 Three agencies in the US are responsible for cybersecurity i.e. Department of Homeland Security (DHS), the National Security Agency (NSA) and Cyber Command or Cybercom. The DHS more or less resembles the Ministry of Interior in Pakistan and was created after the 9/11 attacks. Its mandate includes the protection of national critical infrastructure (Security). In the US most national infrastructure like the electricity grid, water works, railways and airlines are controlled through Supervisory Control and Data Acquisition (SCADA). This remotely monitors, controls and operates systems with coded signals over communication channels and are extremely vulnerable to cyber-attacks. A designated Cyber Emergency Response Team (CERT) under the DHS provides a united response to cyber emergencies (CERT). The NSA and Cybercom carry out cyber surveillance and offensive cyber operations respectively. Both these organizations are being run by the military. The NSA and the Central Security Service (CSS) leads the US Government in cryptology that includes both Signals Intelligence (SIGINT) and Information Assurance (IA) to provide it a decisive edge in Computer Network Operations (CNO). The NSA won international notoriety after the Snowden leaks (Agency). US Army Cybercom and 2nd Army "directs and conducts integrated electronic warfare, information and cyberspace operations," to "ensure freedom of action in and through cyberspace and the information environment, and to deny the same" to its adversaries(Snowden, 2014).

The size of US cybersecurity budget goes to show the importance it attaches to this national security matter. In 2016 President Obama sought $14 billion for cybersecurity efforts "to better protect federal and private networks from hacking threats budget proposal for the 2016 fiscal year." In Financial Year (FY) 2017, the US government spent about 19 billion dollars on cybersecurity spending, representing a 35 percent increase from the previous year. For FY 2018, the Homeland Security Department (HSD) alone wants 971 million dollars for its cybersecurity operations (Command; Shalal & Selyukh, 2015).

In Australia, the lead agency in cybersecurity is the Australian Cybersecurity Centre (ACSC). "This Centre brings cybersecurity capabilities from across the Australian Government together into a single location. It is the hub for private and public sector collaboration and information sharing to combat cybersecurity threats (The Statistics Portal, 2018)." CERT Australia looks after national computer emergencies in Australia(Centre; The Statisca Portal, 2018). In the UK computer emergencies are handled by Cert-UK (CERT). The Office of Cybersecurity & Information Assurance (OCSIA) in the UK supports the ministers and the NSC "in determining priorities in relation to securing cyberspace." The unit provides strategic direction and coordinates the cybersecurity program for the government, enhancing cybersecurity and information assurance in the UK.

The OCSIA works with other lead government departments and agencies such as the Home Office, Ministry of Defence (MOD), Government Communications Headquarters (GCHQ), the Communications-Electronics Security Department (CESG), the Centre for the Protection of National Infrastructure (CPNI), the Foreign & Commonwealth Office (FCO) and the Department for Culture, Media & Sport.

In India the special secretary in charge of Cybersecurity in the Prime Minister‟s Office (PMO) is the cybersecurity chief. Dr. Gulshan Rai of the Department of Electronics and Information Technology (DeitY) became the first person to occupy this position in 2015. Before that he was heading Indian Computer Emergency Response Team (CERT-In) (Agarwal, 2015). India has a number of cybersecurity cooperation forums with other countries of the world e.g. CERT-In has three pacts for cybersecurity cooperation with counterparts in Malaysia, Singapore and Japan (Aggarwal, 2015). India has a regular cybersecurity dialogue with the US that was resumed in 2015. In a joint declaration released after a cyber-dialogue, it was announced that "to increase global cybersecurity and promote the digital economy, the United States and India have committed to robust cooperation on cyber issues (Bjorkman)." India is also expanding relations with Israel in the area of cyber cooperation. In January 2018, the Israeli Prime Minister Benjamin Netanyahu made a six day long visit to India. During this high profile visit, cybersecurity and big data were identified as the new area of cooperation (T. W. House, 2015). In February 2018, the second round of "India-Russia Consultation on Security regarding use of Information and Communication Technologies (ICT)" was held in New Delhi. This was a follow up by the India-Russia Bilateral Agreement on Cooperation in ensuring security in the use of ICT signed on the sidelines of 8 th BRIC Summit held in October 2016 ("Cybersecurity, big data new areas of India-Israel cooperation: Foreign Secretary Vijay Gokhale," 2018).

Government of India allocated Rs. 775 crores for cybersecurity in 2015(Rafiq, 2018). It is quite another matter that some of their cybersecurity specialists find this amount to be "woefully inadequate(India, 2015)." Paucity of funds notwithstanding, the Indian Government is concentrating on digitizing India. Provision of Internet to all the citizens of their country figure prominently on the political parties‟ election manifestos. Modi government's "Digital India" campaign is central part of its development policy. This obviously raises questions about the need to revamp the national Cybersecurity Policy (ca. 2013). One area of weakness in cybersecurity has been identified within the framework of civil-military relations. A group of eighty leading defense, strategic and intelligence officials, ranging from former Director of the Intelligence Bureau to retired senior military officers and diplomats have urged Prime Minister Modi to "take urgent steps" to improve India‟s cybersecurity standards and formalize interaction between civil and military branches of government. It has been

suggested that the National Cyber Coordination Centre operationalized in August 2017 could serve as good forum for such collaboration (PK & Alawadhi, 2015).

Cyber Security in Pakistan

Pakistan is one of the most cyber spied upon country in the world. It is not India alone that wages a strong cyber offensive against Pakistan, many other countries are using cyber means to syphon off critical data. US is one of those countries that actively and regularly spies upon Pakistan (Thakker, 2017). Before Chinese President's landmark visit to Pakistan, the computers at the Pakistan Foreign Office (FO)‟s China desk were hacked. Although a FO spokesperson was quick to deny that such an attack had taken place, it was enough to erode the confidence of the public in the safety and security of our official data ("US authorised NSA to spy on Pakistan among 193 countries," 2014). Actually more troubling are Edward Snowden‟s allegations that UK alone has acquired vast amounts of communications data from inside Pakistan by secretly hacking into routers manufactured by the US based company Cisco ("Pakistan is facing issue of cyber attack," 2015). It is unfortunate that the issue of cyber-spying has not been raised with either the US or the British governments; notwithstanding the fact that London and Washington remain the favorite ports of call for our politicians.

There are clearly identifiable hurdles in establishing a meaningful cybersecurity architecture in Pakistan e.g. there is no central authority to coordinate on cybersecurity matters and advise the prime minister about emerging cyber threats. There is a palpable lack of awareness within the policymaking circles. Apart from the cybercrime bill there is no clear cut policy on the subject of cybersecurity. The cybersecurity stakeholders are not clearly defined and their turfs not properly marked out. There is no PK- CERT and no funds allocated for cybersecurity purposes. The Federal Investigation Agency (FIA) has a National Cyber Response Centre for Cyber Crime (NR3C) but its mandate is limited and it lacks the wherewithal to act as first responder in case of a computer emergency ("UK hacked routers to monitor Pakistan communications data: Snowden," 2015). Pakistan is represented at the UN Group of Governmental Experts on Information Security (Crime), but the national point of view expressed on these forums are not shared with the public.

There is no mechanism of interstate understanding or sharing of best practices on regional basis. The Bangladesh central bank lost 81 million dollars in a cyber-heist in 2016. The State Bank of Pakistan did not issue any instructions to avoid a similar occurrence in our country. It is not known, if any advice was sought from Bangladeshi counterparts on the subject or from SWIFT, the international banking forum through whose portals the request on Bangladesh‟s foreign exchange reserves was made(Quadir & Lema, 2016). In fact there is no coordination or collaboration in the South Asian region or the member countries of the South Asian Association for Regional Cooperation (SAARC).

This is in stark contrast to the active collaboration among the countries of the Association of East Asian Nations (ASEAN) on cybersecurity collaboration ("Here‟s how Hackers stole $80 million from Bangladesh Bank," 2016).

Conclusion

Pakistan has a very huge and talented human resource. Two Pakistani brothers from Lahore have the dubious honor of creating the first computer virus known as Brain. It was their revenge from customers selling pirated copies of the software developed by them. The „friendly virus‟ that they wrote was stamped with their names, phone numbers and the address of their shop to let victims know that they were doing so only to protect their copyrights(Kersten, 2013). Some of the best IT graduates are being produced in universities like National University of Sciences & Technology (NUST) and National University of Computers & Emerging Sciences (FAST-NU). The only thing that we lack is direction and policy and that is not possible without good cyber managers and planners. Most people at the top echelons of the security establishment lack the knowledge and vision to properly organize cybersecurity. Crash courses in cyber awareness to senior government officials and parliamentarians can go a long way in improving the cybersecurity milieu in Pakistan. Courses can be taught in cybersecurity management in the universities and it can be made part of the curriculum of the much vaunted National Defence University (NDU) security workshop.

First and foremost, there is an urgent need for a well-defined national cybersecurity architecture. The powers of coordinating all issues related to cybersecurity may be vested in the office of a cyber-security coordinator working directly under the prime minister. He may be provided secretarial services by the NSC. The NSC could be one forum, where all cybersecurity measures may be discussed. Second, a cyber-taskforce (CTF) as suggested by Senator Syed may be placed under the NSC. The mandate of the CTF should include issuing policy guidelines on cybersecurity. Third, the creation of PK-CERT is a long outstanding issue. The national CERT should be established and asked to practice cyber emergency on regular basis. Fourth, cyber funds should be allocated in the national budget and their proper utilization ensured by the national cybersecurity coordinator. Fifth, cybersecurity cooperation with other countries, particularly those belonging to South Asian Association for Regional Cooperation (SAARC) would have been ideal but unfortunately this association has become moribund due to Indian intransigence. Pakistani FO may consider raising the issue of regional cooperation in cyber security at the forum of Shanghai Cooperation Organization (SCO). This cooperation should be meaningful and expand beyond the brief reference made in the joint statement issued after the visit of the former Prime Minister Nawaz Sharif‟s visit to the White House in 2015.61 Last but not the least, a cybersecurity debate in the parliament may help set up a long term plan. It

would be a good idea for political parties to have cyber security issues included in their election manifestos.

References

[1]. Agarwal, V. (2015). Office of Cybersecurity and Information Assurance, *The Economic Times*. Retrieved from https://www.gov.uk/government/groups/office-of-cyber- security-and-information-assurance

[2]. Agency, N. S. National Security Agency Retrieved 25 April, 2016, from https://www.nsa.gov/

[3]. Aggarwal, V. (2015). Gulshan Rai becomes the first chief of cybersecurity: post created to tackle growing e-threat, *Economic Times*. Retrieved from https://economictimes.indiatimes.com/news/politics-and- nation/gulshan-rai-becomes-first-chief-of-cyber-security-post- created-to-tackle-growing-e-threats/articleshow/46449780.cms

[4]. Ali, Y. A. (2015, 10 August 2015). Pakistan‟s National Security Council?, *Pakistan Today*. Retrieved from http://www.pakistantoday.com.pk/2015/08/10/comment/ pakistans-national-security-council/

[5]. Baloch, S. (2015). Cybersecurity is a matter of national security, *Dawn*. Retrieved from http://www.dawn.com/news/1229738/cyber -security-is-a- matter-of-national-security

[6]. Bjorkman, N. U.S.-India Business Council Applauds Resumption of Cybersecurity Dialogue Retrieved 25 April, 2016, from http://www.usibc.com/press-release/us-india-business-council-applauds-resumption-cybersecurity-dialogue

[7]. Bolo Bhi‟s Meeting and Our Call-To-Action on Cybercrime Bill. Bolo Bhi Retrieved 25 April 2016 http://bolobhi.org/bolo- bhis-meeting-and-our-call-to-action-on-cybercrime-bill/

[8]. Centre, A. C. S. Australian Cyber Security Centre Retrieved 25 April, 2016, from https://www.acsc.gov.au/ CERT, U. US CERT Retrieved 25 April, 2016, from https://www.us-cert.gov/ CERT, U. (2019). *Why is Cyber Security a Problem?* : US CERT Retrieved from https://www.us-cert.gov/ncas/tips/ST04-001.

[9]. Command, A. C. Army Cyber Command Retrieved 25 April, 2016, from http://www.arcyber.army.mil/

[10]. Crime, N. R. C. f. C. National Response Centre for Cyber Crime Retrieved 25 April, 2016, from http://www.nr3c.gov.pk/

[11]. Cybersecurity, big data new areas of India-Israel cooperation: Foreign Secretary Vijay Gokhale. (15 January 2018). *The Hindu*. Retrieved from http://www.thehindu.com/news/national/isreali-pm-benjamin- netanyahu-gets-ceremonial-welcome/article22441745.ece

[12]. Daniel, J. M. Cross Agency Priority Goal: Cybersecurity FY2014 Q2 Status Update. Retrieved 25 April 2016 file:///C:/Users/Administrator/Downloads/Cyber%20Security%20FY14_Q2.pdf

[13]. Desk, N. (2015, 19 December 2015). Cybersecurity: Country lags in preparedness: experts, *Express Tribune*. Retrieved from http://tribune.com.pk/story/1012480/cyber-security-country-lags-in-preparedness-experts/

[14]. Government, U. *Presidential Policy Directive 28 Policies and Procedures*. Retrieved from https://www.fbi.gov/about- us/nsb/fbis-policies-and-procedures-presidential-policy-directive-28-1

[15]. Government, U. (2017). *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Retrieved from https://www.whitehouse.gov/presidential-actions/presidential- executive-order-strengthening-cybersecurity-federal-networks- critical-infrastructure/

[16]. Haq, R. (2016, 14 April 2016). National Assembly of Pakistan passed Cyber Crime bill, *The Express Tribune*. Retrieved from http://tribune.com.pk/story/1083974/national-assembly-approves-cybercrime-bill/

[17]. Here's how Hackers stole $80 million from Bangladesh Bank. (2016, 14 March 2016). *The Hacker News*. Retrieved from http://thehackernews.com/2016/03/bank-hacking-malware.html

[18]. House, T. W. (2015). Joint Statement: 2015 United States--India Cyber Dialogue Retrieved 25 April, 2016, from https://www.whitehouse.gov/the-press- office/2015/08/14/joint-statement-2015-united-states-india- cyber-dialogue

[19]. House, W. (2011). *International Strategy for Cyberspace: Prosperity, Security, and*

Openness in a Networked World,. Retrieved from https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[20]. India, P. T. o. (2015). Govt allocates Rs. 775 crore to combat cybersecurity threats, *Business Recorder*. Retrieved from www.business-standard.com/article/pti-stories/govt-allocates- rs-775-crore-to-combat-cyber-security-threats- 115042200785_1.html

[21]. ITU. Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity Retrieved 22 April 2016, from http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[22]. Jabri, P. (2018). Pakistan to develop e-governance council for policy formulation. *Business Recorder*. Retrieved from Business Recorder website: https://www.brecorder.com/2018/02/13/398914/pakistan-to- develop-e-governance-council-for-policy-formulation/

[23]. Kersten, J. (2013). Going Viral: How two Pakistani Brothers created the First PC Virus. Retrieved from http://mentalfloss.com/article/12462/going-viral-how- two-pakistani-brothers-created-first-pc-virus

[24]. Nation, T. (2014, 27 February 2014). Text of National Security Policy 2014-18, *The Nation*. Retrieved from http://nation.com.pk/islamabad/27-Feb-2014/text-of-national- security-policy-2014-18

[25]. Nation, T. (2015, 23 October 2015). Lt Gen (Retd) Nasir Janjua appointed National Security Adviser, *The Nation*. Retrieved from http://nation.com.pk/national/23-Oct-2015/lt-gen-retd-nasir-janjua-appointed-national-security-adviser

[26]. NIST. Cybersecurity Framework. Retrieved 25 April 2016 http://www.nist.gov/cyberframework/cybersecurity- framework-faqs.cfm

[27]. Order, C. E. *Foreign Policy*. US Government Retrieved from https://www.whitehouse.gov/issues/foreign-policy.

[28]. Pakistan, G. o. *National Action Plan*. Government of Pakistan.*Custom Today*. Retrieved from http://www.customstoday.com.pk/pakistan-is-facing-issue- of-cyber-attack/

[29]. PILDAT. (2005). *National Security Council: A Comparative Study of Pakistan and Other Selected Countries*. PILDAT Retrieved fromhttp://www.pildat.org/Publications/publication/CMR/natio nalsecuritycouncil-comparativestudy.pdf.

[30]. PK, J., & Alawadhi, N. (2015, 28 January 2018). India‟s cyber- security budget „woefully inadequate: Experts, *The Economic Times*. Retrieved from http://articles.economictimes.indiatimes.com/2015-01- 28/news/58546771_1_cyber-security-cert-in-national- cyber-coordination-centre

[31]. Policy, U. F. *Cyber Security*. US Retrieved from https://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

[32]. Portal, T. S. (2018). Proposed budget of the U.S. government for cyber security in FY 2017 to 2019 (in billion U.S. dollars) Retrieved 6 March, 2018, from https://www.statista.com/statistics/675399/us-government- spending-cyber-security/

[33]. Portal, T. S. (2018). Proposed federal IT spending by the U.S. government on cybersecurity for selected government agencies during FY 2018 (in million U.S. dollars) Retrieved 6 March, 2018, from https://www.statista.com/statistics/737504/us-fed-gov-it- cyber-security-fy-budget/

[34]. Quadir, S., & Lema, K. (2016, 14 March 2016). Man in Manila gets

[35]. $30 million cash from cyber heist; Bangladesh central bank governor quits, *Reuters*. Retrieved from http://www.reuters.com/article/us-usa-fed-bangladesh- governor-idUSKCN0WH0JF

[36]. Rafiq, A. (2018). Information Space: An Emerging India-Russia Strategic Partnership. *ISSI*. Rana, M. A. (2013). A review of National Internal Security Policy Retrieved from PIPS website: Schaeffer, B. S., Chan, H. C. H., & Ogulnick, S. Cyber Crime and Cybersecurity: A White Paper for Franchisors, Licensors, and Others Security, H. Homeland Security department USA Retrieved 25 April, 2016, from https://www.dhs.gov/

[37]. Shalal, A., & Selyukh, A. (2015). Obama seeks $14 billion to boost U.S. cybersecurity defenses. Retrieved 25 April 2016, from Reuters http://www.reuters.com/article/us-usa-budget- cybersecurity-idUSKBN0L61WQ20150202

[38]. Snowden, E. (2014). Leaks that exposed US spy programme, BBC. Retrieved from http://www.bbc.com/news/world-us-canada- 23123964

[39]. Stolfo, S., Bellovin, S. M., Keromytis, A. D., Sinclair, S., Smith, S. W., & Hershkop, S. (Eds.). (2008). Insider Attack and Cybersecurity:Beyond the Hacker (2008 ed.): Springer.

[40]. Thakker, A. (2017, 10 October 2017). It‟s Time for India to Update Its Cybersecurity Policy, The Diplomat. Retrieved from https://thediplomat.com/2017/10/its-time-for-india-to-update-its-cybersecurity-policy/

[41]. UK hacked routers to monitor Pakistan communications data: Snowden. (2015, 6 October 2015). The Express Tribune. Retrieved from from http://tribune.com.pk/story/968194/uk-hacked-routers-to-monitor-pakistan-communications-data- snowden/

[42]. UNODA. GGE Information Security: Developments in the Field Of Information and Telecommunications in the Context of International Security. Retrieved from http://www.un.org/disarmament/topics /informationsecurity/

[43]. US authorised NSA to spy on Pakistan among 193 countries. (2014, 1 July 2014). The Express Tribune. Retrieved from from http://tribune.com.pk/story/729521/us-authorised-nsa-to-spy- on-pakistan-among-193-countries/

[44]. Usman, M. (2016, 29 July 2018). Senate unanimously approves cybercrime bill with amendments, The Express Tribune. Retrieved from https://tribune.com.pk/story/1151861/senate- unanimously-approves-cybercrime-bill-amendments/