Formulation of Pakistan's Cyber Security Policy: Comparative Approaches

Afeera Firdous

Introduction

Contemporary period has evidenced such swift advancements in computer technologies that the era is described as the Digital Age. The most astonishing change that the digital age brought, is the development and advancement of interdependent, interconnected, and globalized network of computer and communication devices. In the twenty-first century, this network of networks has transformed into a global interactive platform for joint activities, and the trading of information and ideas by people globally.[1] In recent years, cyberspace expanded practically exponentially. It offers a stage for innovation and well-being, and provides ways to further advancements. Along with the positives, there are also some negatives of this new technology. With the global scope of a light or unregulated digital infrastructure, there are great risks which affect nation-states, private organizations, and personal rights of an individual. Today, many states almost completely depend on cyberspace in regard to education, health, communications, energy, transport, infrastructure, financial services and military forces movements.

Cyber operations are increasingly being used by states to accomplish their political, economic, and military objectives. Unfortunately, non-state actors are also resorting to cyber operations for their nefarious purposes. The enhanced scope and incidence of cyber-attacks as a political tool forms an extremely dangerous trend in international relations. Vulnerable data systems are attractive targets for other states and non-state actors. As the dependence on information and communication technologies (ICT) has increased with the sophisticated methods, the tendency of cyber-attacks has also transformed from small-scale intrusions and financial breaches to highly organized state-sponsored attacks. To be able to protect from the threat posed to vulnerable data on cyberspace, states take multiple initiatives such as formulating legal frameworks to regulate cyber use, but most significant is the articulation of a policy framework to develop nation's approach against such threats.

Threat Scenario and Significance of National Policy Framework

Cyber threat has changed in its nature, scope and scale in the past few years. There are some examples of use of cyber deterrence like Stuxnet which put back Iran's nuclear program by several years, cyber compellence such as hacking of Sony Picture Entertainment (SPE), influence on political outcomes such as alleged Russian hackers' involvement in US Presidential elections and world-wide cyber ransomware attacks like Petya, NonPetya and WannaCry when billions of dollars were paid as ransom globally. The Center for Strategic and International Studies (CSIS) has maintained a list of significant global cyber incidents since 2006.[2] This list consists of three hundred and thirteen incidents, focusing on cyber-attacks on governments, defense and high-tech companies, or economic crimes and each incident resulted in the losses of more than a million dollars. There are a few recent examples of cyber incidents which pose dire consequences for national security.

Speaking at a public event in Islamabad, Chief Technical Advisor of United Nations Development Program (UNDP) Mr. Tariq Malik[3] related an example of cyber compellence that few years back Saudi Arabia started working on an agreement with AirBus to buy aircraft. When the agreement got finalized, country A (he intentionally did not name the country) hacked all the data related to agreement between Saudi Arabia and AirBus. Country A informed the Saudi officials that agreement data had been hacked. The hacked data revealed that some of the Saudi officials were involved in taking commission/bribe in the agreement. Then, country A proposed to Saudi officials that whether Saudi Arabia needed to cancel the agreement with AirBus and buy aircraft from Boeing or country A will share the data with AirBus and French government. Saudi Arabia, thus, was left with no option but to cancel the agreement with AirBus and sign an agreement with the Boeing.

An Indian journalist, Rachna Khaira, associated with The Tribune newspaper reported that, in January 2018, an anonymous agent on WhatsApp had sold Aadhar[4] data to her for only $7.84 (Rs.500).[5] The hacking of the Unique Identification Authority of India (UIAI) and its Aadhar system provided the access to the personal data of more than one billion Indian citizens. After a month, the news of Chinese cyber espionage against African Union (AU) emerged. French daily, Le Monde, published a report that China had tapped confidential data of IT networks of African Union headquarters, which was built by Chinese investor, for five years from 2012 to 2017.[6] In February 2018, another incident happened when Pyeongchang Winter Olympic Games website went offline for more than twelve hours. The US intelligence officials claimed that few hundred computers had been hacked by Russian hackers during the Olympic opening ceremony which not only effected its website but also interrupted wifi service and televisions at the Olympic stadium.[7] US officials termed this attack as false-flag operation while saying that the Russian hackers did so, trying to make it appear as though the intrusion was conducted by North Korea.

In March 2018, New York Times reported that 2017's cyber-attacks on the Saudi petrochemical companies were not aimed to destroy data or fold the operations of the plants, but were intended to disrupt the company's operational procedures and trigger an explosion to cause physical damage.[8] Cybersecurity researchers fear that the attackers could repeat it in other parts of the world, since different countries, all over the world, depend on the same American-engineered computer systems that were compromised in Saudi petrochemical plant. During the Russian Presidential elections in March 2018, Russia's Central Election Commission reported that there was a cyber-attack on commission's website on the election day, which targeted its information center.[9] In the same month, another scandal came to press about personal data leak of Facebook to Cambridge Analytica.[10] Christopher Wylie, who assisted a Cambridge University academic to obtain the data, said that Cambridge Analytica collected millions of Facebook profiles of US voters and used them to build a powerful software program to predict and influence choices at the ballot box.[11] This software program was not only used by Donald Trump's election team but also for winning Brexit campaign in UK.

The FBI assesses that only US losses from cybercrime in 2016 exceeded $1.3 billion,[12] and some industry experts predict such losses could cost the global economy $6 trillion by 2021.[13] In 2008, cyber threat was not even a part of US worldwide threat assessment report, but in 2018, Worldwide Threat Assessment report of the US intelligence community considered cyber threat as top threat to US and its allies, leaving fear of WMD and terrorism behind.[14] Director of National Intelligence (DNI) also acknowledged that the potential of surprise and risk in the cyber domain will increase in the next year and beyond.[15]

The answer to the question 'What is Cyber Security Policy and why it is important?' is a bit intricate. US Department of Homeland Security has defined cyber security policy "it includes strategy, policy, and standards with regards to the security of and operations in cyberspace. It encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure".[16]

Policy making is most important of all components of a state's security framework, for it lays the goals and over all objectives that a state desire to pursue. The strategy, on the other hand, allows the state to mobilize its resources and potential for accomplishment of those objectives. States usually have separate policy and strategy for achieving the overall objectives such as foreign policy, defense policy and economic policy etc. Cyberspace has emerged as a serious threat for national security of the state. As Ola Hjalmarsson states that within the framework of the securitization theory[17], some concepts are important: a securitizing player is a title given to the actor who evokes the sense of securitization, the referent entity is the object which is considered as it is needed to be securitized by the securitizing actor, the spectators or audience is the populace which requires to be persuaded of the weakness of the referred entity, and the requisite of outstanding steps to guard it so that the process of securitization becomes a success.[18] Modern states perceive certain activities in cyberspace as potential threat, therefore a national cyber security policy is all the more significant to preserve national interests in cyberspace.

Comparative approaches in Cybersecurity Policies

The inherent vulnerable nature and weakness of cyberspace and increasing number of cyber-attacks constantly threaten the security and economy of states, as well as the daily life of citizens. More than fifty countries have framed their cyber security policies/strategies to mitigate the serious cyber security threats faced by their nations. A national cyber security policy/strategy is not only designed to protect national cyberspace from vindictive cyber threats, but due to diverse and unpredictable threat landscape, significant variations can be rooted in the preventive, defensive, and offensive approaches implemented by different nations.[19]

International Telecommunications Union (ITU)[20] categorizes countries' efforts with regards to cybersecurity on five parameters i.e. legal, technical, organizational, capacity building and cooperation. In 2017, ITU's Global Cybersecurity Index (GCI) ranked Singapore at the first place, with regards to its efforts in cyber security, ahead of US, UK, Russia, France, Estonia, Canada and Israel.[21] Top ten ranking countries are shown in Table 1.

ITU Ranking	Country
1	Singapore
2	US
3	Malaysia
4	Oman
5	Estonia
6	Mauritius
7	Australia
8	Georgia, France
9	Canada
10	Russian Federation

Table. 1 ITU's Global Cybersecurity Index 2017

Different countries have also included action plans in their cyber security policies/strategies. The US, UK, France, Netherlands and Germany have specifically acknowledged dual aspects of cyber security like cyber offense and cyber defense.[22] All the national cyber security strategies, however, have similar objectives of protecting the cyberspace against potential threats and enhancing cyber resilience. Countries have taken into account their peculiar cyber threat landscape, socio-political conditions, security trends, traditions, level of awareness while developing their cyber security approaches.[23] The formulation of cyber security policy/strategy effort gained serious attention after 2008 when from simple breaches state-sponsored cyber-attacks such as an incident in Estonia in 2007 came to notice.[24] The US had, though, published its first cyber security strategy draft in 2003, before the cyber-attacks became so common.[25] Publication and revision of national cyber security policies/strategies of different countries are given in Table 2.

Countries	**Year Policy/Strategy Issued**
US	Strategy 2003 Strategy Review 2009 Policy 2011 Strategy for critical infrastructure 2014 Dept. of Defence's Strategy 2015
UK	Strategy 2009 Strategy Review 2011
Australia	Strategy 2009
Canada	Strategy 2010 Action Plan for Strategy 2013

Estonia	Strategy 2008 Strategy Review 2014
France	Strategy 2011
Germany	Strategy 2011
Japan	Strategy 2013
India	Strategy 2013
Saudi Arabia	Strategy 2013

Table 2. Timeline of Cyber Security Strategies

United States

Countries such as UK, US, Estonia, Netherlands, and Czech Republic have frequently published updated drafts of their cyber security strategies, but the US is the only country which has regularly reviewed and updated its cyber security strategy. The most recent document on cyber security strategy[26] was published by US Department of Defence in April 2015. In the document, US has defined its strategic goals as follows:

- Form and sustain ready forces and capabilities to conduct cyberspace operations.
- Build defence for DoD networks, protect data, and lessen vulnerabilities to DoD missions.
- Be prepared to defend the US homeland and US vital interests from disruptive or destructive cyberattacks of significant consequence.
- Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.

- Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

The document also describes the central role of DoD's Cyber Mission Force (CMF) which was approved in 2012. It stated that after being operational, CMF will consist of 6200 military/defence, civilian and contractor support personnel from all military departments. CMF comprised cyber operators organized into 133 teams and sub-teams such as Cyber Protection Force, National Mission Force, and Combat Mission Force etc. DoD cyber strategy mentioned all types of cyber offenders like China, Iran, North Korea; and non-state actors such as Islamic State (IS) etc as potential source of threat for the US.

India

India announced its first national Cyber Security Policy[27] in 2013, against the backdrop of Snowden's revelations about NSA surveillance program.[28] India's cyber security policy charted key areas of focus such as building protected cyber ecosystem, producing assurance framework, creating mechanisms for security threat early warning, vulnerability management and response to security threats, secure e-governance mechanism and resilient critical information infrastructure, promote R&D and cyber security awareness, develop human workforce, and integrate public-private partnership. Some significant cyber policy objectives of India are as follows:

- Build a strong regulatory framework for securing cyberspace ecosystem.
- Build a 24 x 7 apparatuses on national and sectoral level for tracking down strategic information about dangers to ICT infrastructure and crafting response.

- Establish a 24 x 7 National Critical Information Infrastructure Protection Center (NCIIPC).
- Build a force of 500,000 professionals trained in cyber security till 2018 through capacity building programs.
- Develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.
- Build global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Arun Sukumar, the head of the Cyber Security and Internet Governance Initiative at the Observer Research Foundation (ORF)[29] India, called it "a statement of first principles" rather than a comprehensive framework.[30] Though, India's cyber security policy is not a detailed document but it could work as a working draft to start with. In 2014, India established National Critical Information Infrastructure Protection Center.[31] On the other hand, India projected to build a force of 5,00,000 cyber professionals within five years but it could not meet the numbers as envisioned.[32] National cyber security policy also outlined necessity of a nodal agency to coordinate all the matters related to cyber security within the country. In 2017, India IT Ministry setup a National Cyber Coordination Center (NCCC) to examine the country's online traffic to identify threats.[33] Indian government has also made operational Botnet and Malware Cleaning Center to detect malicious software in devices of citizens and clean them.[34]

Pakistan's Efforts in Formulating National Cybersecurity Policy

Countries, around the world are deploying online services and Pakistan is also developing IT services and integrating it to different sectors. Microsoft's most recent Security Intelligence Report (SIR) showed Pakistan amongst the states which are most at risk of malicious software attacks.[35] National Database and Registration Authority (NADRA) maintains a centralized national ID database of Pakistan, which is shared among banks, passport offices, Election Commission of Pakistan (ECP), mobile networks and Federal Investigation Agency etc. NADRA is the only organization which registers and stores the information about the population. According to Threat Track Security 2014 report, NADRA is on the top ranking organizations in the world because of use of state of the art technologies for its services.[36]

Use of IT is the most effective means for improving governments delivery systems in the contemporary era. E-governance helps to improve by increasing efficiency of the services provision and enables government organizations to offer timely services to the citizens. Some of Pakistan's e-government components are Federal Board of Revenue (FBR); Excise, Taxation and Norcotics departments; Karachi Metropolitan Corporation, Punjab and Khyber Pakhtunkhwa Police Service; Punjab Metrobus Authority; Civil Aviation System; and Federal Public Service Commission (FPSC). Pakistan also has some online business and financial services such as online banking transaction facilities, mobile banking, mobile and postal money transfer services, Pakistan Stock Exchange etc. NADRA could be an attractive target for cyber-attackers to block or sabotage its essential services, hack personal confidential information and use them for their illegal purposes. In December 2012, Turkish hackers had claimed to have accessed the NADRA system and the Federal Investigation Agency's (FIA) servers, potentially acquiring personal data of millions of Pakistanis.[37] Later in 2015, NADRA officials admitted that its critical database has gone through serious hack attempts originating from US, India and Israel.[38] In 2013, several cyber-attacks on the Election Commission of Pakistan website were foiled but the website itself was shut down to avoid further attacks.[39] Apart from these examples, cyber-attacks by Indian and Pakistani hackers, on one another, have become common practice such as ahead of each other's independence days[40] and after the announcement of Kulbhushan Jadhav's death penalty.[41]

Pakistan has not, yet, devised a cybersecurity policy/strategy. There are, however, some significant measures taken by Senate of Pakistan in this direction. In July 2013, Senate Committee of Defence, in collaboration with Pakistan Information Security Association (PISA), organized a policy seminar on the topic of "Defending Pakistan through Cyber Security Strategy".[42] Chairman Senate Committee on Defence and Defence Production, Mushahid Hussain Syed announced 7-point Action Plan for Cyber Secure Pakistan, as follows:

- Cyber security threat should be accepted and recognized as new, emerging national security threat by the Government of Pakistan, similar to the threats like terrorism and military aggression.
- Relevant legislation should be done to preserve, protect and promote Pakistan's cyber security, drafting for which has already begun. The bills will be presented in Parliament for Cyber Security.
- Establishment of a National Computer Emergency Response Team (CERT).
- Establishing a Cyber-Security Task Force with affiliation with Ministry of Defence, Ministry of IT, Ministry of Interior, Ministry of Foreign Affairs, Ministry of Information and security organizations plus relevant and leading IT professionals to formulate Cyber Security Strategy for Pakistan.
- Under the office of the Chairman Joint Chiefs of Staff Committee, an Inter-Services Cyber Command should be established to coordinate cyber security and cyber defence for the Pakistan Armed Forces.

- Within the framework of SAARC, Pakistan should take the initiative to initiate talks among the member states particularly with India to establish acceptable norms of behavior in cyber security domain among the SAARC countries so that these countries are not engaged in cyber warfare against each other.
- Soon, the Senate Defence Committee, in cooperation with the Pakistan Information Security Association (PISA), will have a special media workshop to promote awareness among the public and educate opinion leaders on the issue of cyber security.

Mr. Amar Jaffri, former Additional Secretery FIA and Head of Pakistan Information Security Association, informed in an interview with the author that Chairman Senate Committee of Defence and Defence Production, Mushahid Hussain Syed, had formulated a group of experts Cyber Security Task Force in 2014. Mr. Jaffri, himself headed the task force which was tasked to formulate cyber security policy/strategy and legal framework. A forty-member team comprising experts from the government, armed force, FIA, police, intelligence community, business, academia, IT and cyber security specialists etc, met for eighteen months and drafted four policy documents. The documents included cyber security laws, cyber security policy, cyber security strategy, and draft of national cyber emergency response team. Senator Mushahid had presented all the draft documents to Senate for approval.

In March 2014, the Minister of State for Interior Balighur Rehman also acknowledged that a cyber-security strategy was being devised to counter cyber-attacks.[43] Later in April, Mr. Mushahid Hussain Syed presented a private member bill, on National Cyber Security Council Act.[44] The purpose of the bill was to launch a high level policy research institution to conduct research and analysis on policy matters related to cyber security. Proposed council would support individuals, private companies and government branches in capacity building; formulate policy and strategies; assist the government, academia and IT professionals; help in taking collaborative measures with other countries and international organizations; and help in developing and maturing legal frameworks in cyber domain.

The bill had clearly specified functions and powers of the National Cyber Security Council. Some of the functions are as follow:

- Formulate national cyber security policy[45] and strategy.[46]
- Monitor cyber security legislative framework and recommend improvements in legislations.[47]
- Recommend policies and regulatory means of standardization, harmonization and accreditation with regards to critical information infrastructure.[48]
- Coordinate with other states and international entities on implementation of policies, legislations and initiatives.[49]
- Facilitate communications between government and private sector, academia and cyber security experts on issues relevant to cyber security.[50]
- Establish an advisory group to provide operational, technical, policy and industry advisory inputs on strategic plans.[51]
- Develop ten or twenty year vision with regards to cyber security[52]
- Conduct research on upcoming cyber threats and promote general awareness.[53]

While chairing a meeting of national-level cyber security response committee, Minister of State for Information Technology, Anusha Rahman stressed the need to devise a comprehensive cyber security policy, using a multi-stakeholder model.[54] She also underlined the need for a holistic approach and a coordinated effort to ensure the security of the data right from the cell phone of an individual to the government ICT data/information.

In April 2017, Ministry of Information Technology and Telecom (MoITT) released the first draft of Digital Pakistan Policy.[55] Digital Policy/IT Policy lays emphasis on four sectors for the application of policy requirements to address and improve country's position in governance, entrepreneurship, knowledge capital, accessibility, demand stimulation, and ICT skills. These areas are:

- Sectoral digitalization.
- Cross-sector cooperative measures.
- IT sector sustainability.
- Entrepreneurship and innovation.

According to MoITT, this policy will serve as the foundation for the establishment of a holistic Digital Ecosystem in the country with advance concepts and components for rapid delivery of next generation IT services, applications and content.[56]

Way Ahead

With the cyber perpetrators gaining strength day by day, cyber-attacks methods are continuously evolving at a faster pace. No nation can, therefore, stay completely secure from cyber-attacks. Pakistan needs to focus on developing a comprehensive cyber security policy at a rapid pace. There are some features which must be part of Pakistan's cyber security policy:

- Maintain and support a secure and resilient cyberspace.
- Safeguarded critical national cyber assets and infrastructures.
- Development of a robust cybersecurity regulatory, legislative, and assurance framework.

- Establishment of National Computer Emergency Response Team (CERT) / Cyber Security Incidental Response Team (CSIRT).
- Cyber security awareness campaigns for common users.
- Development and improvement of indigenous cyber security technologies and services.
- Protection of the online rights of netizens.
- Support of public-private collaboration.
- Encouragement of international cooperation in cyber security domain mainly with the neighboring and regional countries.

Cyber security is quite a vast domain. Since there are no commonly understood definitions of cyber security key terms, Pakistan needs to define term such as cyber security and cyberspace explicitly. In the last few years, besides terrorism, and natural hazards etc., cyber-attacks, cyber espionage and cyber terrorism have also become a global menace. A comparative analysis reveals that countries have now realized the importance of cyber security and, therefore, regard it as one of the top-tier national security issues.[57] Different countries have allocated specific budgets for cyber security measures. According to publically available data, UK spends £1.9bn,[58] India Rs. 110 crore,[59] and US with highest annual cyber security spending up to $19 billion.[60] Pakistan also needs to prioritize to allocate sufficient funds, in the annual, budget for cyber security projects. In the cyber domain, the criticality of an infrastructure is defined by the services and core values that it provides and the digital information it processes, stores and transmits. The choice of critical sectors or infrastructure by any country is highly impacted by the country-specific peculiar conditions and traditions, cyber threat perception, sociopolitical factors, and geographical conditions. Pakistan also needs to clearly define its critical assets or infrastructure in its national cyber security policy in different areas such as telecommunication and

ICT, banking and finance, government and particular e-services, like electricity and water supply, health services, transportation, emergency and rescue services, and national security services like the police and armed forces etc.

Some countries have established inter-departmental cyber security response capabilities i.e. they have distributed the task of cyber security amongst multiple existing organizations working under various governmental departments.[61] The establishment of these organizations within the government is greatly influenced by cyber threat perception, resource allocation, defense etc. Pakistan also needs to decide whether it is going to follow the example of France and Estonia to create a new coordinating body to deal with cyber threats or it is going to adopt inter-departmental cyber security response capabilities. For a country to effectively deter targeted cyber threats and incidents, it is essential to have technical teams that efficiently disseminate threat information to the concerned authorities and provide cyber protection and resilience capabilities. Various forms of such teams include Computer Emergency Response Teams (CERTs), Computer Security Incident Response Team (CSIRT) and Information Sharing and Analysis Centers (ISAC). The government needs to establish a national CERT on the priority basis. Table 3. shows some countries who have established their CERTs earlier.

Country	**CERT Established**
Australia	2010
Canada	2003
Estonia	2006
France	2008
Germany	2012

India	2004
Israel	2014
Japan	1996
Malaysia	1997
Saudi Arabia	2006
Turkey	2007
UK	2014
US	2003

Table 3. CERTs establishing year of various countries

Pakistan needs to emphasize on cyber security capacity building initiatives e.g. training, awareness, R&D programs etc mentioned in the draft cyber security document. Whether on national or international levels, cyber security requires multi-stakeholder approach for effectively tackling cyber issues and increasing cyber resilience. Because of the global nature of cyberspace, apart from intra-nation cooperation (public, private sectors, ISP's etc), intra-state and international collaboration are also required. Pakistan is now part of Shanghai Cooperation Organization (SCO) which provides good opportunities to collaborate with other countries or international organizations. Shanghai Cooperation Organization has special focus on cyber security issues. It holds annual cyber drills. Pakistan needs to initiate collaborative measures to get assistance of friendly countries to develop cyber security policy, strategy and national CERT. India has recently approved an Armed Forces Cyber Division,[62] Pakistan also needs to focus on building its tri-services cyber capabilities.

Conclusion

In the contemporary international world, internet has played vibrant role in bringing global connectivity. But, on the other hand, exploitative cyberspace operations have increased the arena of security threats for nation states, both in civilian and military domains. Cyber intrusions have drastically increased in the recent years, which causes economic loss of billions of dollars annually, as the cybersecurity experts predict that offensive cyber operations could cause loss of trillions of dollars to the global economy in the next decade. Cybersecurity experts also acknowledge that the potential of risk in cyberspace will escalate in coming years rather that deceasing.

The increased number of offensive cyber operations, by states and non-state actors, have made the policy makers around the world conscious of the need to think about solutions for changing threat environment in cyber domain. Countries across the world have recognized the potential threats in cyberspace.

Keeping in mind the dire consequences of any such attack on Pakistan, government must take timely steps to counter cyber risks. Apart from government, private companies and organizations also need to prioritize and focus on protecting their systems and data, and make regular risk assessments. It is needed to make well-judged investments in cyber defense capabilities to secure the systems and accomplish national objectives. It is high time to understand that countering and diminishing the cyber threat needs a comprehensive strategy and implementation plan. Few baby-steps have already been taken by the government, but a lot more is needed to be done to secure country’s cyberspace.

Afeera Firdous is a
Research Assistant at CISS

Endnotes

[1] US policy documents characterize the Internet as a "network of networks." See Department of Homeland Security, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: Executive Office of the President of the United States, 2009, 8) https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

[2] Center for Strategic and International Studies, "Significant Cyber Incidents," https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity, accessed on March 13, 2018.

[3] Mr. Tariq Malik is former Chief Technology Officer at GHQ and he also has been former Chairman of NADRA.

[4] Aadhar Data is compilation of data-set of Indian citizens, containing their personal information such as name, DoB (age), contact details (address, mob no, e-mail), fingerprints, and facial photograph.

[5] Rachna Khaira, "Rs 500, 10 minutes, and you have access to billion Aadhaar details," *The Tribune,* January 3, 2018, http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

[6] Shannon Tiezzi, "If China Bugged the AU Headquarters, What African Countries Should Be Worried?," *The Diplomat,* January 31, 2018, https://thediplomat.com/2018/01/if-china-bugged-the-au-headquarters-what-african-countries-should-be-worried/.

(Original Report) Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," Le Monde, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

[7] Ellen Nakashima, "Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say," *The Washington Post,* February 24, 2018, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.30076f78c8fb.

[8] Nichole Perlroth and Clifford Krauss, "A cyber-attack in Saudi Arabia had a deadly goal. Experts fear another try.," *New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

[9] "Russian Central Election Commission comes under cyberattack," *RT*, March 18, 2018, https://www.rt.com/news/421622-russian-election-under-cyber-attack/.

[10] Cambridge Analytica is London-based data analysis and political consulting firm which worked with Donald Trump's election campaign team for 2016 US Presidential Elections.

[11] Carole Candwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The Guardian*, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[12] Greg Masters, "Loss from cybercrime exceeded $1.3B in 2016, FBI report," *SC Magazine*, June 26, 2017, https://www.scmagazine.com/loss-from-cybercrime-exceeded-13b-in-2016-fbi-report/article/671047/.

[13] Steve Morgan, "Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021," *Cybersecurity Ventures*, October 16, 2017, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[14] Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," *DNI*, February 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[15] Jim Garamone, "Cyber Tops List of Threats to U.S., Director of National Intelligence Says," *US department of Defence*, February 13, 2018, https://www.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/.

[16] Department of Homeland Security, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: Executive Office of the President of the United States, 2009, 5) https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

[17] In 1998, Loe Waever formally presented the theory of Securitization for the very first time in his article titled as "Security the Speech Act: Analyzing the Politics of a Word", later Rita Taureck has defined the term Securitization as: The security actor, confirming that a particular reference object is at risk in its existence, claims the right to emergency actions to ensure the preservation of the reference object.

[18] Ola Hjalmarsson, *Securitization of Cyberspace* (Sweden: Lund University Press, 2013), http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990&fileOId=3357996.

[19] Narmeen Shafqat and Ashraf Masood, "Comparative Analysis of Various National Cyber Security Strategies," *International Journal of Computer Science and Information Science* 14, no. 1 (January 2016): 129-136, https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies.

[20] International Telecommunications Union is United Nations' specialized agency for information and communication technologies.

[21] International Telecommunication Union, "Global Cybersecurity Index," 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[22] Myriam Dunn, "A Comparative Analysis of Cyber Security Initiatives Worldwide," *International Telecommunication Union*, June 2005, https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.

[23] Martti Lehto, "The Way, Mean, and Ends in Cyber Security Strategy," in *Proceedings of 12th European Conference on Information Warfare and Security*, ed. Rauno Kuusisto and Erkki Kurkinen (UK: Academic Conferences and Publishing International ltd., 2013), 182-190.

[24] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 17, 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[25] US CERT, "The National Strategy to Secure Cyberspace," February 2013, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, accessed on March 15, 2018.

[26] US Department of Defence, "Department of Defence Cyber Strategy," April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, accessed on March 15, 2018.

[27] Ministry of Communications and Information Technology, "National Cyber Security Policy-2013," http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf, accessed on March 15, 2018.

[28] "Amid spying saga, India unveils cyber security policy," *Gadget Now*, July 13, 2018, https://www.gadgetsnow.com/enterprise-it/security/Amid-spying-saga-India-unveils-cyber-security-policy/articleshow/20885499.cms?referral=PM.

[29] Observer Research Foundation is Mumbai based think tank, focuses on international security issues.

[30] Arun Mohan Sukumar, "Upgrading India's cyber security architecture," *The Hindu*, March 9, 2017, http://www.thehindu.com/todays-paper/tp-opinion/upgrading-indias-cyber-security-architecture/article8328770.ece.

[31] Saikat Datta, "Defending India's critical information infrastructure: The Development and role of NCIIPC," *Internet Democracy Project*, https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf, accessed on March 15, 2018.

[32] Kaushik Deka, "The new battlefield is online: Is India Prepared?," *India Today*, September 3, 2017, http://indiatoday.intoday.in/story/cyber-crime-cyber-attack-malware-cyber-security/1/1037598.html.

[33] "Cyber Coordination Center made operation: IT Ministry," *The Indian Express*, August 9, 2017, http://indianexpress.com/article/india/cyber-coordination-centre-made-operational-it-mininstry-4789272/.

[34] Ibed.

[35] "Pakistan, Bangladesh at high risk of cyber-attacks," *Pakistan Today*, October 26, 2017, https://www.pakistantoday.com.pk/2017/10/26/pakistan-bangladesh-at-high-risk-of-cyber-attacks/.

[36] Jawad Awan and Shahzad Memon, "Threats of Cyber Security and Challenges for Pakistan," *in Proceedings of the 11th International Conference on Cyber Warfare and Security*, ed. Tanya Zlateva and Virginia A. Greiman (Boston: Academia Conferences and Publishing International Limited, 2016), 425-30.

[37] Farooq Baloch, "Cyber Vandalism: Turkish Hackers claims gaining access to NADRA and FIA servers," *The Express Tribune*, December 15, 2012, https://tribune.com.pk/story/480044/cyber-vandalism-turkish-hacker-claims-gaining-access-to-nadra-fia-servers/.

[38] Aamir Ataa, "NADRA faces serious hacking attacksfrom United States and India," *ProPakistani*, 2015, https://propakistani.pk/2014/11/13/nadra-faces-serious-hacking-attacks-united-states-india/ or https://www.express.com.pk/epaper/PoPupwindow.aspx?newsID=1102523545&Issue=NP_LHE&Date=20141113.

[39] "Cyber-attack on Election Commission of Pakistan (ECP) website," *Teleco Alert*, March 31, 2013, https://www.telecoalert.com/cyber-attacks-on-the-election-commission-of-pakistan-ecp-website/.

[40] Shashank Shekhar, "India, Pakistan at war on cyberspace ahead of Independence Day," *Business 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.

[41] "Surgical cyber-STRIKE! Hackers take down 30 Pakistan sites to avenge Kulbhushan Jadhav's death penalty," *Daily Mail*, April 24, 2017, http://www.dailymail.co.uk/indiahome/indianews/article-4441462/Surgical-cyber-STRIKE-Hackers-attack-30-Pakistan-sites.html.

[42] APP, "Senate Committee proposes 7-point action plan for Cyber Secure Pakistan," *Dawn*, July 8, 2013, https://www.dawn.com/news/1023706; or

Senate of Pakistan, "Senate Report on Pakistan's first-ever Cyber Security Strategy Work Plan," August-September 2013, http://www.senate.gov.pk/uploads/documents/1378101374_113.pdf.

[43] Mateen Haider, "Pakistan formulating cyber security strategy," *Dawn*, March 7, 2014, https://www.dawn.com/news/1091640.

[44] Senate of Pakistan, "National Cyber Security Council Act, 2014," April 14, 2014, http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf.

[45] Section 5. (2)(a) of National Cyber Security Council Act, 2014.

[46] Section 5. (2)(b) and (c) of National Cyber Security Council Act, 2014.

[47] Section 5. (2)(g) of National Cyber Security Council Act, 2014.

[48] Section 5. (2)(i) of National Cyber Security Council Act, 2014.

[49] Section 5. (2)(j) and (n) of National Cyber Security Council Act, 2014.

[50] Section 5. (2)(k) of National Cyber Security Council Act, 2014.

[51] Section 5. (2)(l) of National Cyber Security Council Act, 2014.

[52] Section 5. (2)(q) of National Cyber Security Council Act, 2014.

[53] Section 5. (2)(o) and (p) of National Cyber Security Council Act, 2014.

[54] "Anusha urges a comprehensive cyber security policy," *Pakistan Press Foundation*, July 9, 2014, https://www.pakistanpressfoundation.org/anusha-urges-comprehensive-cyber-security-policy/.

[55] "Digital Pakistan Policy," *MoITT*, April 2017, http://digitalrightsmonitor.pk/wp-content/uploads/2017/10/Digital-Pakistan-Policy-2017.pdf, accessed on April 6, 2018.

[56] Aamir Aata, "MoIT Releases Digital Pakistan Policy 2017," *ProPakistani*, April 2017, https://propakistani.pk/2017/04/08/moit-releases-digital-pakistan-policy-2017/.

[57] Narmeen Shafqat and Ashraf Masood, "Comparative Analysis of Various National Cyber Security Strategies," International Journal of Computer Science and Information Science 14, no. 1 (January 2016): 129-136, https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies.

[58] Tracey Caldwell, "The UK's £1.9bn cyber-security spend – getting the priorities right," *Science Direct*, March 2017, https://www.sciencedirect.com/science/article/pii/S1361372317300246.

[59] "Budget 2018: Government to focus more on improving cybersecurity," *Money Control*, February 1, 2018, https://www.moneycontrol.com/news/business/economy/budget-2018-government-to-focus-more-on-improving-cybersecurity-2495175.html.

[60] "Proposed budget of the U.S. government for cyber security in FY 2016-2017 (in billion U.S. dollars)," *Statista*, https://www.statista.com/statistics/675399/us-government-spending-cyber-security/, accessed on March 16, 2018.

[61] Narmeen Shafqat and Ashraf Masood, "Comparative Analysis of Various National Cyber Security Strategies," International Journal of Computer Science and Information Science 14, no. 1 (January 2016): 129-136, https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies.

[62] "Joint Doctrine: Indian Armed Forces," *Headquarters Integrated Defence Staff Ministry of Defence*, April 2017, http://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf.