SOVEREIGN INTERNET FRAMEWORKS IN CONTEMPORARY COUNTRIES AND WAY FORWARD FOR PAKISTAN

MCS

By

Bilal Ahmed

0000281278

Submitted to the Faculty of Department of Information Security Military College of Signals, National University of Sciences and Technology, Islamabad in partial fulfillment of the requirements for the degree of MS in Information Security

SEPTEMBER 2020

ABSTRACT

In today's world, state power is demonstrated in a number of ways in tangible domain, may it be sea, air, land or space. Domain of Internet, though intangible is no exception. Although geographical boundaries are not recognized on Internet nor the addresses for structuring, but Internet protocol(s) recognize network service providers. Snowden Revelations have jolted the world of free Internet and given; even allies of United States, a run for their data security. Majority of countries are already working on security of their data in some form. Russia and China in this regard have taken lead by controlling the flow of information by their devised methods. Latest developments on RUnet and great firewall of China are testimonies of political will by Russian and Chinese governments. Both these countries have been advocating internet sovereignty as a way to secure sensitive information from foreign tailing.

Pakistan in this regard have been lagging behind and no concrete vision or framework exists to control the Cyber Space. In order to propose a way forward for Pakistan, best practices have been identified after analyzing the Sovereign Internet Framework of Russia and China. Then a detailed study has been conducted to ascertain the current state of Cyber Space in Pakistan against these best practices and propose for Pakistan to take Cyber Space under control. The proposed way forward is mix of higher level regulatory, legislative and administrative measures to take a holistic approach best suited for Pakistan.

ACKNOWLEDGEMENTS

All praise to Allah Almighty for giving me strength to keep going on with this thesis, despite the challenges and troubles.

I am grateful to my parents and my sister for their continuous support and encouragement. Without their consistent support and prayers, this thesis would not have been possible. My brother, a professional software engineer, who has been an inspiration for me to pursue higher studies and read about emerging technologies. Last but not the least my better half who has been a source of strength for me and supporting me through hard times.

I am very grateful to my Project Supervisor Brig Dr. Imran Rashid who supervised the thesis / research in a very encouraging and helpful manner. He has always been source of guidance and a mentor.

I am also thankful to committee members who have always guided me with their profound and valuable support that has helped me in achieving my research aims, especially Maj Sohaib Ahmed who has been guiding me in detailed manner always been a helpful senior and Dr Fawad for sharing his first-hand experience at internet usage inside China.

Special thanks to Brig Waqar Haider for his encouragement and motivational talks. I would also like to thank Ahmed Raheeq Sultan, for his encouraging and thoughtful discussions on Thesis and its management. I would also thank Mehmood ul Hassan for his technical help and support.

Finally, I would like to express my appreciation to all the people who have provided valuable support to my study and whose names I couldn' t bring to memory.

Contents

ACRONYMS

APCERT ..... Asia Pacific Computer Emergency Response Team
CAC ..... Cyberspace Administration of China
CC ..... Coordination Center of China
CERT ..... Cyber Emergency Response Team
CIA ..... Central Intelligence agency
CII ..... Critical Information Infrastructure
CNIC ..... Computerized National Identity Card
CNCERT ..... National Computer Network Emergency Response Technical Team
CNTIC ..... China National Cyber Threat Intelligence Collaboration
CPC ..... Chinese Communist Party
FIA ..... Federal Investigation Agency
FSTEC ..... Federal Service for Technical and Export Control
gTLD ..... Generic Top Level Domain
HEC ..... Higher Education Commission
ICT ..... Information and Telecommunication Technology
IMCEW ..... Inter Ministerial Committee for Evaluation of Websites
ISP ..... Internet Service Provider
IXP ..... Internet Exchange Point
JPCERT ..... Japan Computer Emergency Response Team
KPCERC ..... Khyberpakhtunkhwa Cyber Emergency Response Center
KPITB ..... Khyberpakhtunkhwa Information Technology Board
LEAs ..... Law enforcement agencies
MoIT ..... Ministry of Information Technology
NCCCI ..... National Coordination Center for Computer Incidents
NCCS ..... National Center for Cyber Security
NCSAEL ..... National Cyber Security Auditing and Evaluation Lab
NR3C ..... National Response Center for Cyber Crimes
NSA ..... National Security Agency
OICCERT Organization of The Islamic Cooperation Computer Emergency Response Team
OSCCA ..... Office of State Commercial Cryptography Administration
PASHA ..... Pakistan Software Houses Association
PECA ..... Prevention of Electronic Crimes Act
PIE ..... Pakistan Internet Exchange Point
PII ..... Personally identifiable information
PISA ..... Pakistan Information Security Association
PITB ..... Punjab Information Technology Board

PSEB ..... Pakistan Software Export Board
PTA ..... Pakistan Telecommunications Authority
PTCL ..... Pakistan Telecommunication Company Limited
PUBG ..... Players Unknown Battlegrounds
SOC ..... Security Operational Center
TLD ..... Top Level Domain
VPN ..... Virtual Private Networks

List of Figures

List of Tables

Chapter 1

Introduction

Internet is a mutual asset among countries, and a ground-breaking correspondence medium with a profound social and political impact. Country states clearly have a solid stake in guaranteeing that social values are kept, and political soundness is secured. Nations are relied upon to pursue already set up worldwide standards, including respecting autonomy of other states in their geographical and in-house matters [1]. Notwithstanding worldwide ethics, nations still participate in intangible domain of conflict through focused propaganda [2]. The Internet was at first made for the free trade of data without any understanding that it would be as amazing a power as it is today, with the capacity to change social orders, trigger insurgencies, and unseat rulers by mobilizing protests [3]. The idea of no borders on internet is accepted as a fact however the capability to erect borders on internet has been present and the political will to erect these barriers has gradually matured among the nations.

In 2013, following the reports of surveillance by National Security Agency of USA, a debate started about the control of internet as "United States National Telecommunication and Information Administration intended to transition key Internet domain name functions to global multi stakeholder community" [4], countering the massive impact of surveillance by foreign governments and adopt sovereignty in technical and cyber domains [5]. In response to revelations by Snowden, technical community maintaining the internet infrastructure has already warned against internet fragmentation on national grounds and advocated the multi stakeholder management of internet globally. Stakeholders to include all governments on equal traction, private sector, civil society and academia [6]. Internet sovereignty and Data localization efforts in the wake of Snowden revelations may cost US cloud computing industry up to $ 35 billion as they lose credibility in the eyes of Asian and

European clients; warned by stakeholder [7]. European Union also considered establishing a Europe only network named as Schengen cloud [8]. The General Data Protection Regulation (GDPR) imposes heavy fines for infringement of the regulation by data processors [9], and give rights to data subjects to confirm purpose and occasion of processing of their data [10]. Other countries are also not far behind; Australia passed personally controlled electronic health record Act (PCEHR) which restricts transfer of health record outside Australia [11], Brazil passed Marco Civil da Internet law which ensures civil rights in use of internet [12], Canadian national law; Personal Information Protection and Electronic Document Act (PIPEDA) does not restrict personal data transfer outside Canada but imposes conditional exclusions [13], British Columbia Freedom of Information and Protection of Privacy Act mandates public bodies to store the personal information in its control to be stored and accessed in Canada only along with few exceptions [14], Chinese Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services information Systems prohibit personal data being transferred abroad without consent of the subject of data or approval of the legal authority [15], France have promoted local data center infrastructure also known as *le cloud souverain* and invested in cloud computing firms directly [16], Germany is working on providing Cyber security solutions dubbed as IT Security made in Germany [17], Indian National Security Council proposed a policy that mandated all email service providers to host servers in India for India operations [18], Indonesia's electronic information and transaction law mandates data centers and disaster recovery centers for public services to be placed inside Indonesia [19], Malaysian Personal Data Protection Act (PDPA) mandates data about Malaysian nationals to be stored inside Malaysia [20], South Korean Personal Information Protection Act mandates consent of data subjects before providing data overseas [21] and Vietnamese "Management Provision and use of Internet Services and Information Content Online" law impose a ban on use of internet for criticizing government [22].

1.1 Problem Statement

The control of internet is decentralized by design and special measure have to be undertaken to exert control over internet in a particular geographical region, as done by China and Russia. Nation states have been working progressively on controlling the internet in their respective countries however Pakistan has been lagging behind in this aspect. With the rapid advancement in ICT technologies and their commissioning in private and public sector, now is the time for Pakistan to take special measures in order to be able to achieve internet sovereignty.
The Thesis aims at **Critical analysis of the Sovereign Internet Frameworks in contemporary countries and propose a way forward for Pakistan**

1.2 Research Objective

Main objectives of the Thesis are:-

(a) Analyzing already implemented Sovereign Internet Frameworks in China and Russia including structure, success and their setbacks.

(b) Identify best practices in achievement of Internet Sovereignty.

(c) Analyze current state of cyber space in Pakistan n the light of identified best practices.

(d) Propose a Sovereign Internet Framework for Pakistan.

1.3 Scope

The scope of research is as under:-

(a) Taking in to account the management of Cyber space in Russia and China and their quest for Internet Sovereignty.

(b) Tracking the achievements and setback of the measures taken by Russia and China while achieving Internet Sovereignty.

(c) Analysis of current cyber space in Pakistan with exception of defence forces and installations.

1.4 Contribution

The research will contribute in following ways:-

(a) Study of Russian internet landscape and how they pursued internet sovereignty by developing RUnet.

(b) Study of Chinese internet, Great firewall of China and how they controlled and censored internet inside China.

(c) Comparison of Russian and Chinese models while accessing their successes and setbacks.

(d) Identification of best practices with regards to achievement of Internet Sovereignty.

(e) Analysis of Pakistan with respect to identified best practices.

(f) Recommending a way forward for Pakistan based on study of Russian and Chinese Models.

1.5 Thesis Outline

The Thesis is organized as under:-

Chapter 1 **Introduction** describe the basiscs of the research topic and its importance. It also describe the problem statement, research objectives, thesis scope and contributions by this research.

Chapter 2 **Existing Models** will describe in detail the internet sovereignty models of Russia and China.

Chapter 3 **Analysis of Existing Models** will analyze internet sovereignty frameworks followed by Russia and China, gauge the impact of these frameworks and also shed light on measures taken by few other countries.

Chapter 4 **International Best Practices** will describe the best practices identified after study of the Russian and Chinese models.

Chapter 5 **Best Practices and state of affairs in Pakistan** will analyze the current cyber state in Pakistan from the point of view of identified best practices. It will also highlight additional observations in Cyber Space of Pakistan.

Chapter 6 **Way forward for Pakistan** will recommend a course of action for Pakistan to secure its Cyber space and achieve Internet Sovereignty in Pakistan.

Chapter 2

Existing Models

Internet Sovereignty Models of under study countries are examined below in detail.

2.1 Russia

Russian government aimed for dividing internet in National Segments dubbed as RUnet. RUnet is the title given to Country Code Top Level Domain .RU which was previously .SU for Soviet Union however it is functional till date and around 100,000 domains names are still registered with .SU [23]. Later it was used for referring to geographically defined network space within control of the state. Russian lawmakers and government agencies have been working on various legislations in a bid to secure and stabilize internet in Russian territory independent from global internet and external defies [24]. Work on these legislations is under progress with different level of success at each level. In 2018 Russian Cyber Security Index was 0.836 [25] and internet Internet Penetration rate was 76.1 % [26].

2.1.1 Re framing Cybersecurity

Russian Doctrine on Information Security refers Cyber Security as Information Security and was approved by President of Russian in 2016 [27]. It defines Information Security as

> State of protection of individual, society and the state from internal and external information threats.

Russian doctrine re frames cybersecurity as a National security issue in information domain as by treating threat to information security as threat to National Interest

[28].

2.1.2 Recruitment of Cyber Troops

The Framework titled *Conceptual views on the activity of Armed Forces in the information space* was developed in 2011 by Ministry of Defense of the Russian Federation [29]. In 2017 it was official that Russia has Information Operation troops [30]. According to a Russian Cyber Security Firm Zecurion, in 2017 Russia was in top five countries as per spending and number of cyber troops [31]. The capabilities of Russian troops were not told officially but their supposed purpose is to repel Cyber Attacks [32].

2.1.3 Russian CERTs

At minimum five Russian CERTS are working in different sectors:

RU-CERT:

RU-CERT provides response to all users within Russian territory. It is also assisting in contacting with LEAs [33]. RU-CERT is member of Forum of Incident Response and Security Teams (FIRST) [34]. **CERT-GIB:**

CERT-GIB provides emergency response to all clients round the clock in cases of DoS / DDos, Network Intrusion, Malware, Phishing and online frauds. A leading Russian Cyber Security firm with expertise in APTs. They collaborate with all Russian toplevel domains and collaborate with anti-cybercrime agencies worldwide. CERT-GIB is member of FIRST and official partner of Interpol and Europol [35]. **GOV-CERT:**

GOV-Cert is Cyber Security and Incident Response Team for the Russian government networks. It coordinates LEAs and local & state authorities in dealing with computer incidents in state networks. It deals incidents of malware, botnets, Dos / DDos and unauthorized access [36]. **Fin CERT:**

FinCERT is part of Directorate of Security & Protection of Bank of Russia. It coordinates information exchange between LEAs and Financial Institutions, analyze attacks on Financial Institutions and issue protection guidelines for financial trasactions [37] **KASPERSKY ICS CERT:**

ICS-CERT –Industrial Control Systems Cyber Emergency Response Team is working in the field of industrial cybersecurity. Its primary objective is to help collaborate and coordinate between automation system manufacturers, operators, owners and researchers [38].

2.1.4 Russian version of Online Services

Russia have not blocked international services altogether, but they have created national alternatives of them in house which are running in addition to international services [39, 40, 41] . The popular ones are listed in Table 2.1 :-

Russian Service	Global Service	Category
Yandex	Google	Search Engine
VK	Facebook	Social Network
Mail.ru	Yahoo	Social Network
OK.ru	Facebook	Social Network
Moi Mir	Facebook	Social Network
Telegram	Whatsapp	Messenger
Avito.ru	OLX	E-Commerce
Uchi.ru	Khan Academy	Online Learning
yaklass.ru	Khan Academy	Online Learning
Rutube.ru	Youtube	Videos and streaming
Yandex maps	Google Maps	Maps

Table 2.1: Russian Services against Global Services

2.1.5 Establishment of GOSSOPKA & Coordination of Threat Intelligence

In 2013 a Presidential Decree was signed to ensure Information Security of Russian, authorizing the Federal Security Service (FSB) to take necessary steps in order to create a system for detection and prevention of consequences of Cyber Attacks known as GOSSOPKA [42]. The motive of this initiative was to raise a system capable of threat forecasting and act as point of interaction for all stake holders in information security domain. It will also monitor the state of security for Critical Information Infrastructure (CII). First centers under GOSSOPKA emerged in 2015 in some Government Organizations [24]. In 2017 Russian parliament passed Law FZ-187. It defined GOSSOPKA as; geographically distributed centers comprising a system where information about Cyberattacks is shared. These centers were mandatory to be established in all private and public entities owning CII. Law also defined CII objects and established a registry for CII objects. [43]. Criminal liabilities were also included in the law for actions against CII as amendment to Criminal Code of Russia. Unauthorized access to data at CII is liable to imprisonment upto 6 years and a fine of upto 1 million Rubles [44]. As per the concept of GOSSOPKA, its

territorial structure has a form as in Figure 2.1 [45].

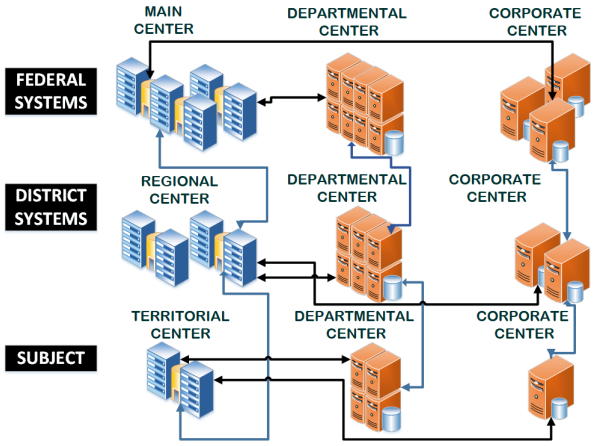

Figure 2.1: Structure of GOSSOPKA Centers

In 2018 several legislations were passed for establishment of National Coordination Center for Computer Incidents (NCCCI), listing of information required to be shared with GOSSOPKA [46] and regulating information exchange among CII [47]. NCCCI was mandated with dealing with all international interactions for incident response with the authority of even refusing the information sharing if it deemed it harmful for Russian National Security [24].

2.1.6 IT made in Russia:

In 2015 a government decree imposed a ban on foreign software for state use. In compliance a Register of Russian Softwares is maintained having more than Five Thousand Records [48]. The softwares listed in register are preferred for government procurement.

2.1.7 Internet Kill Switch:

In 2014 Russian Ministry of Communications conducted Cyber Exercise to access the security and stability of national segment of internet and the degree of its connectivity with global internet was studied [49]. The outcome of this Cyber

Exercise was communicated in a report in 2015. The report asks for more legal and technical measure. Among legal measures it asked for more state regulations, stricter control over operators and a traffic monitoring system. Technical measures include reserving root DNS servers and duplicate registry of IP addresses. These were suggested to cater for an event of external internet shutdown [50].

In 2017 another Cyber Exercise was conducted to test security and stability of Russian Internet. Russian Government is concerned with threat of an external shutdown of Internet and both exercises were conducted to test the resilience of RUnet, however the exercises yielded same result that RUnet is vulnerable to external attacks [51]. In 2019, Ministry of Communication passed a law under in which Roskomnadzor would be allowed to un-plug the Runet from Global internet under three types of threats including; threat to RUnet's integrity, resilience and network security [52].

2.1.8 Content Censorship

In 2012, as per amendments in law on Information Protection, Operators were required to restrict internet access to prohibited content. A register for prohibited content was made having domain names, network addresses and internet resources containing illegal content. Whenever a site hosting forbidden content was found, Roskomnadzor would send a notification to remove the content. If the content hosting site failed to remove it within 3 days, the site will be added to the register for prohibited content.

In 2015 a system called Revizor was introduced to check compliance by the operators regarding register for prohibited content. Violation would result in heavy fines for the operators [53]. By 2020 a system for safer internet for children will be implemented under a state program; *Digital Economy*. Under this program internet users will be able to visit the web content from only the white-list. For un-censored access the user will have to request the service provider specifically [54].

2.1.9 Localized Data Storage and Processing

In 2016 Law (FZ-242) for local storage of data and processing came into force and it required all companies to store and process their data about Russians inside Russia. It also required to shift hosting and storage services in Russia. Violators are to face fine and may face blockage [24].

2.1.10 Data Protection for Cross Border Data Transfer

Russian Data protection law allows cross border transfer of personal data only if it is authorized either under Russian law or under an international agreement, to which Russian is a party. Any agreement between data transferring entities should have mandatory terms as used in Russian Law. Consent of subject individuals should be sought before the transfer. For countries which are not part of International treaties and not considered providing adequate data protection by Russian organization Roskomandzor, written consent is mandatory [55].

2.1.11 Management of Critical Internet Resources

Russian Government is keen on protecting RUnet from an external shutdown [56]. State law on the Security of Critical Information Infrastructure went into effect on January 1st 2018. It encompassed government, defence industries, finance, energy and nuclear sectors. Law requires these critical systems to be connected to GOSSOPKA [57]. Discussions about independent national segment of internet have been going on in Russia since 2016. The 2016 Bill introduced by Ministry of Communications described elements of Critical Infrastructure. Several amendments were issued in 2016 and 2017 adding details about critical infrastructure. It included IXPs, TLD registries, IP addresses and Autonomous System numbers. In 2018 a new Bill was introduced which required operators to route traffic through traffic exchange points listed in special registry. It also established national DNS. Bill also asked operators to install special means for protection of their networks [24]. This new law was signed in May 2019 [58]. It will be implemented in Nov 2019 and another thirty by-laws are

required to fill in the gaps identified [59].

2.2 China

Chinese concept of Internet Sovereignty stem from two principles i.e No unauthorized influence in Information space of country and Shifting of management of Internet to an international body [60]. Influence in Information space is seen as a threat for the stability in Chinese community and internet is taken as a facilitator, providing multiple avenues of information exchange without control of state. Although no mass agitation has been staged with the help of social media in China but potential applications of social media platforms and internet such as civil disobedience and mass protests are seen as a deep concern [61], so much so that during Arab spring peak in 2011, China placed censorship control over terms like *Jasmine* in a bid to deal with call of *Jasmine Revolution*. Physical police force was also employed to deal with protests [62]. The issue of International management of Internet is based on the general sentiment that cyberspace is America centric and it is an issue in itself. Snowden's revelations of PRISM surveillance program are a proof for that [63]. Although there is no unified policy document for Chinese Cyber space, available open source data about chinese policies have been examined below. In 2018 Chinese Cyber Security Index was 0.828 [25] and Internet Penetration rate (2019) was 58.4 % [26]:

2.2.1 Cyber Security in State Security policy

Internet Sovereignty is considered critical for maintenance of Chinese core values. Government of China views Telecommunication resources as a matter of *high politics* which is intermingled with national security and stability [64]. Cyberspace is no exception to dominance by Chinese nationalist sentiments. The government have commissioned numerous projects to control the information and data flow on the internet including Great Firewall of China and Great Cannon.

2.2.2 Chinese Cyber Troops

China has exclusive Cyber troops operational in Civil and Military domains. Within civil sphere there are cyber specialists employed in organizations, even in some ministries. In PLA, there are Military Network Warfare forces for offensive and defensive operations [65]. According to estimates China is second largest country as per spending on cyber troops and largest as per number of such personals [31]. A new domain in PLA was introduced in 2015 by raising of Strategic Support Force (SSF), having status equal to PLA Land forces, Air force and Naval force. SSF will look after complete war effort in information sphere encompassing space, cyber and electromagnetic domains [66].

2.2.3 Cyber Militias and Hacktivist Units

These are cyber groups active in chinese cyber space other than PLA cyber units. Cyber militias are composed of IT experts, IT firms, domain experts, hackers, foreign language speakers etc. They participate in Military exercises but aren't managed directly by PLA [67]. Most prominent group of them is *Red Hacker Alliance* once having a massive number of eighty thousand members. Such groups operate parallel to government and unlikely to be under serious government control. [68].

2.2.4 Chinese CERTs

A number of Chinese CERTS are functional in multiple domains. All of them are member of FIRST. 5 of them are looking after their coporate services, solutions and their vulnerabilities They include Huawei Product Security Incident Response Team (Huawei PSIRT), ZTE Product Security Incident Response Team (ZTE PSIRT), Dahua Product Security Incident Response Team (Dahua PSIRT), China Mobile CERT (CM-CERT) and Alibaba Security Response Center (ASRC) [69, 70, 71, 72]. Remaining are as under:

CNCERT/CC:

National Computer Network Emergency Response Technical Team / Coordination Center of China is non-profit / non-government cybersecurity technical center. It coordinates China's cybersecurity emergency response community. It acts a National CERT of china and guard Critical Information Infrastructure. It also manages Great Firewall of China [73]. **Eversec:**

Hengan Jiaxin Technology is network security provider to telecom operators, government and corporate sector [74]. **HSRC:**

Hikvision runs a private cyber security center providing support in recognized cyber security standards [75]. **Qi An Xin CERT:**

Qi An Xin Group is cyber security firm providing services to government, finance, energy and telecom sectors. They specialize in big data [76]. **Data Star Observatory:**

Data Star Observatory is providing digital asset threat management and operations services, asset threat monitoring, analysis and vulnerability lifecycle management services [77].

2.2.5 Chinese version of Online Services

Another strategy of china has been to block the global services and replicate them in-house. The popular ones are listed in Table 2.2 :-

2.2.6 Social Management Strategy

Internet in China has been employed for implementing social management in a way where involvement of state is neither invasive nor direct [78]. The trio of technical, legal and regulatory measures instill a change of conduct in internet users,

Chinese Service	Global Service	Category
Baidu	Google	Search Engine
QQ	MSN messenger	Instant messaging
Weibo	Twitter	Social Network
Zhihu	Quora	Social Network
Taobao	Amazon	Online Shopping
Youku	Youtube	Video
Pan.baidu	Dropbox	Online Storage
QQ Music	Spotify	Online Music
dian ping	Groupon	Lifestyle
Baidu Maps	Google Maps	Maps
Gaode Maps	Google Maps	Maps

Table 2.2: Chinese Services against Global Services

due to fear of litigation. Such actions preserve social stability in Chinese community insulating it from global internet effects.

2.2.7 Great Firewall of China

The Great Firewall of China (GFW) was commissioned in 1990 and is technically managed by CNCERT/CC under umbrella of Ministry of Industry and Information Technology (MIIT). Censorship policies and decisions are given by government institutions including the Central Propaganda Department, the State Council Information Office (SCIO), and the Public Information Network Security Supervision Department of Ministry of Public Security (MPS). Hardware used in GFW is domestically produced by Sugon and Huawei. There are three international gateways, located in Beijing, Shangai and Guangzhou and bulk of filtering hardware is placed at border routers however a little portion of them is placed internally indicating surveillance of domestic traffic [79]. Number of laws regulate the flow of web data. Simplified algorithm of GFW is illustrated in Figure 2.2 [80].

Blocked website and web resources fall in classifications namely Foreign social media platforms, Foreign news sites, file sharing services, foreign social media platforms, overseas chinese portal sites & discussion forums, dissident / pro democracy

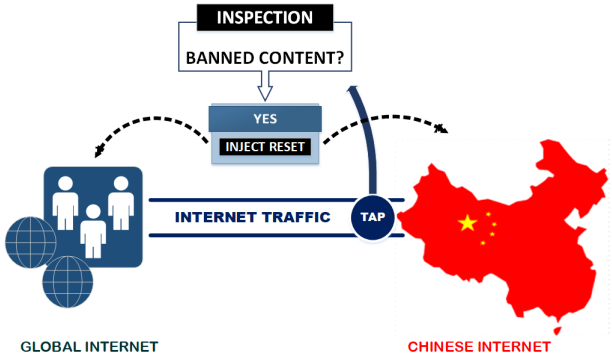

Figure 2.2: Simplified algorithm of Great Firewall

/ human right sites, circumvention & anonymity tools, sites by Falun Gong, pornography & gambling [81]. Domestic network is dealt with the help of human censors, internet police force, hired bloggers and even closing regional internet. International network traffic is dealt with IP blocking, DNS manipulation, URL filtering and filtering of keywords [79].

2.2.8 Great Cannon

The Great Cannon (GC) was commissioned in 2015 as an active tool employed for DDoS attacks. It works by redirecting intercepted web traffic to the target websites. It allows authorities to intercept traffic flowing from outside china towards chinese websites, injects malicious code and use this traffic as intended, just like a Man in the Middle attack [82]. The malicious code make a non suspecting internet user a participant in the DDoS attack. Although GC is seperate from GFW but researchers have found it collocated with the GFW. The decision flow of GC is illustrated in Figure 2.3 [80].

2.2.9 Content Localization

Cybersecurity law of China bounds companies operating in china having established network to store information inside china. Came in effect on June 1st 2017, the

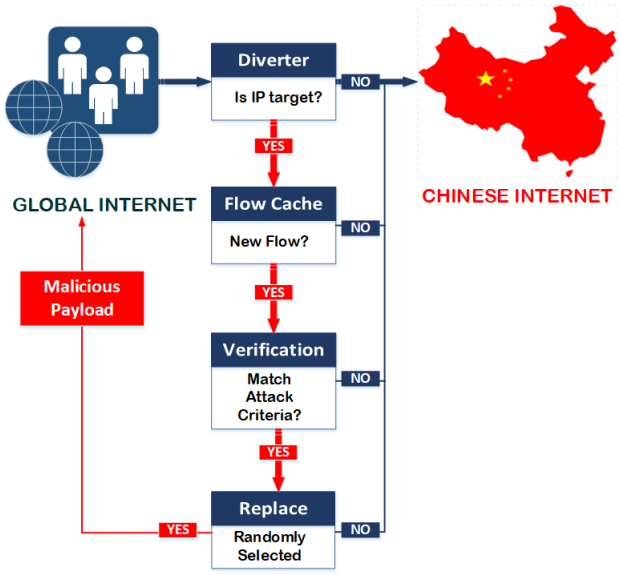

Figure 2.3: Decision flow of Great Cannon

law applies on CII operators. It includes operators in communications, information services, energy, finance and public services [83].

2.2.10 Cross Border Data Transfer Control

Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft) were issued by Cyberspace Administration of China (CAC) on June 13th 2019. The measures regulate operators and cross-border receiver of data through contract regarding protection of subject data transfer. Issued measures also deal with application and approval apparatus for cross-border data transfer [84]. Authorities may demand seizure of cross-border data transfer under following conditions [85]:-

- Data breach suffered by Operator of cross-border reciever.
- Unsustainable protection of rights and interests by data subjects.
- Operator or cross-border reciever's inability to protect data.

2.2.11 Cyber Threat Intelligence Collaboration

Chinese National Cyber Threat Intelligence Collaboration (CNTIC) was raised in 2017. Resources were contributed by government, leading Cyber Security firms and CNCERT. Aim of establishing this platform was to have a wholesome mechanism for reporting of network security risks, threat intelligence sharing and research portal [86]. With regards to International collaboration in cyber domain, China has a documented strategy on International Cooperation on cyber space under its Ministry of Foreign Affairs. Here China promotes the principles of peace, sovereignty, shared governance and shared benefits [87].

2.2.12 Future Vision

According to *Qiushi Journal* [88], a bimonthly by Central Committee of Chinese Communist Party (CPC); article by Theoretical Studies Group of Cyberspace Administration of China (CAC) provides insight about President Xi vision of Cyberspace of China i.e transforming China from a Cyber Power to Cyber Superpower. The vision calls for capacity building in domains of internet content management and creation of Possitive Energy, cyber security and critical infrastructure protection, domestic software & hardware development, assuming leading role in development and management of global internet [89]. The article asks for attention on following aspects as envisioned by President Xi:

Formulate online public opinion:

Emphasize on the importance of online public opinion formulation in ideological domain. Signify the vision of CPC in cyber domain. It also asked for innovation in publicity operations in order to grasp top places in local online media. It also named a project named *Chinese Dream* to promote positive online environment.

Safeguarding Political Security:

Article discussed measures taken for safeguarding political security of china including laws for public opinion, mechanism of online risk prevention, regulate public outrage, exclusive online sterility of rumors and traitorous audios & videos.

Strengthening of Network ecosystem:

All available technological, administrative and legislative resources to be employed for strengthening of network governance. The management of regional network by departments to be strengthened. Information on legislation to be improved.

Securing Critical Information Infrastructure:

A concrete cyber security barricade will be built aimed at protecting critical information infrastructure. Potential loopholes in communication, energy, finance and transportation sectors will be probed and prevented. *Network Product and Service Security Review Method* will be formulated.

Situational Awareness and Emergency Response:

Situational awareness and emergency response capabilities will be enhanced with a focus on network security situational awareness, event analysis, tracking & traceability, disaster recovery, network security monitoring, early response mechanisms and real time monitoring. National Cyber Security Incident Emergency Plan will be revised.

Consolidate Foundation of Network Security:

Revision and enhancement of Domain Name Management, optimization of IP addresses and website resources management.

Rights of People:

Regulation of collection and processing of personal data and its transmission across the border. Crack down against disclosure of personal information and online frauds.

Research and Innovation in ICT:

Promotion of research in high-end fields including performance oriented computing, quantum communication, artificial intelligence, cloud computing, big data, operating systems and development of hardware. item

Development of Digital Economy:

Expansion of economic development by coordinating and promoting the *Broadband China* Strategy and *Internet Plus* action plan. *Broadband China* strategy aims at driving advancement in broadband, advance its network construction and establish a Universal next generation national information infrastructure [90]. *Internet Plus* is a plan for integration of mobile internet, cloud technologies and IoT with manufacturing to stimulate development of e-commerce, industry networks and internet banking to raise internet based companies for their increased international presence [91].

Promotion of global Internet governance system:

Strengthening of international cooperation in cyber domain and promotion of Chinese idea of internet governance to achieve international concord, enhancing influence of Chinese cyber space. To promote Chinese vision for internet governance *International Cooperation Strategy for Cyberspace* was released which asked for internet cooperation within framework of United Nations. Strengthen interconnection with US internet companies and think tanks. Strengthen cooperation with Russian in cyberspace. Pursue cooperation in digital economy with Europe.

Chapter 3

Analysis of Existing Models

3.1 Analysis of Frameworks

The deep study of the countries mentioned above shed light on the state of affairs in domain of internet governance and highlight the efforts of two most advanced and developed cyber powers after US. Both Russia and China have their reasons and concerns on the un-matched dominance of US on global infrastructure of internet and its potential usage by US authorities to spy on these countries.

We will analyze the approaches taken by both these countries under Mueller framework of Internet Fragmentation; in which the effort to align the internet i.e the drive by states to establish ultimate authority over respective national segments of cyberspace is examined and methods to achieve alignment are explained as national securitization, territorialization of information flows and alignment of critical Internet resources [92]. The analysis divides the measures taken by Russia and China under the methods addressed in the framework as under:-

- National Securitization: It deals with securing national information frontier. It consist of four parts. First being naming cybersecuiy an issue of national security, second is the nationalization of threat intelligence and central threat picture, third is promotion and adoption of national ICT technologies and forth being development of a Kill switch. Details in Table 3.1

- Territorialization of information flows: It encompasses domains of content filtering, & data localization; achieved by gradual legislation and blocking of data. Details in Table 3.2

- Alignment of critical Internet resources: It deals with identification and man-

agement of critical infrastructure and its security via legislation and enforcement of law. Details in Table 3.3

Country	Cataloging of threats	Cyber Troops	Threat Intelligence	CERTs	National Technologies	Internet Kill Switch
Russia	- Potential threats were cataloged [28]. - Threats were added in Doctrinal documents [28]. - Cyber Security made part of National secuirty [28].	-5th largest spender on Cyber troops [31]. -5th largest number of Cyber troops [31].	- Creation of GOSSOPKA for wholesome picture [42]. - Establish NCCCI for dealing international incident response [46].	- 5 x Certs [33, 35, 36, 20, 38] - Dealing LEAS, general cyber threats, government networks, finance and industry [33, 35, 36, 20, 38]. - 2 x member of FIRST [34]	- Banning foreign software [48]. - Laws for transition to local software [48].	-Law passed in 2019 for unplugging Runet [53]. -Effective in Nov 2019 [53].
China	- Unauthorized influence in Information space and unrest in society are seen as threat [60].	- 2nd largest spender on cyber troops [31]. - Largest number of cyber troops [31]. - Support of Cyber Malatias [68]. - Hactivist Units [68].	- Raising CNCERT/CC. [73]. - China National Vulnerability Database(CNVD), Anti Network-Virus Alliance (ANVA) and China Cyber Threat Governance Alliance(CCTGA) [73].	- 10 x Certs [73, 72, 74, 75, 69, 76, 70, 77, 71]. - All are members of FIRST [34].	- Local development of software and hardware pursued as government vision [89].	- Speculations about China having a kill switch but never acknowledged [93].

Table 3.1: National Securitiazation

Country	Content Censorship	Data Localization
Russia	- Registry for prohibited content was made [53]. - Roskomnadzor would deal with adding names in registry [53]. - Revizor system to check compliance by operators [53]. - Digital Economy program for safer internet for children [54].	- Law for local storage of data and processing [24]. - Required to shift hosting and storage services in Russia [24].
China	- Great Firewall of China [79]. - Great Cannon [82].	- Chinese cyber law's requirement to establish local data centers [83]. - Cross border data transfer control [85].

Table 3.2: Territorialization of information flows

Country	Measures taken
Russia	- Creation of GOSSOPKA [42]. - Law on the Security of Critical Information Infrastructure [57]. - Creation of registry for Critical Information Infrastructure [24].
China	- Operations Security for Critical Information Infrastructure under Cybersecurity law [94].

Table 3.3: Alignment of Critical Internet resources

The analysis reveals that all the methods proposed by Mueller are found in the progress made by Russia and China. Now we will examine these measures for their successes and setbacks one by one.

3.2 Impact Assessment

This assessment probes overall effect of the measures taken under the umbrella of Internet Sovereignty frameworks by Russia and China. For ease of comprehension, colored symbols are used to assess the state of completeness on measures undertaken.

- Measures which have been **successfully implemented** and **achieved their intended results** are marked as ● .
- Measures which have **not been implemented completely** or **implemented with unsatisfactory results** are marked as ● .

3.2.1 Cataloging of Threats

Russia

- Range of potential threats were cataloged ●: Russia was able to draft Information Security Doctrine of the Russian Federation, enforced in December 2016; in which potential threats were identified [28]. It includes illegal cross-border flow on data, employment of ICT to influence minds of populace, foreign IT equipment (Hardware and Software), critical infrastructure exposure to threats and irregular control over critical Internet resources and its distribution. Cataloging of the threats enabled lawmakers to focus on addressing them. The developments against these cataloged threats are discussed below one by one:-
  - *Illegal cross-border flow on data:* Law FZ-242 was adopted on July 4th 2014 [95].It highlights a clear local data policy. It requires operators to ensure any data collection or processing is done in Russia, nullifying any illegal content sharing across border.

- *Employment of ICT to influence minds of populace:* Amendments in law on Information Protection, were passed in 2012 which required Operators to restrict internet access to prohibited content. This prohibited content was cataloged in a national registry [53].
- *Foreign IT equipment (Hardware and Software):* Government decree was passed in 2015 which imposed ban on foreign software for state use [48].
- *Critical infrastructure exposure to threats:* Security of Critical Information Infrastructure law went into effect in January 2018 [57].
- *Irregular control over critical Internet resources and its distribution:* Law FZ187 was passed in 2017 defined CII objects, its owners and established a registry for CII objects [43].

- Addition of Information Security to Russian Doctrinal documents ●: Russia added Information security as part of Russian National Security Strategy, published in December 2015 [96]. It enabled lawmakers to focus on Information Security and Information Security Doctrine of Russian Federation was enforced in December 2016 [97].

China

- Unauthorized influence in Information space and unrest in society ●: Unauthorized influence in information space and unrest in society is seen as an intermingled phenomena in China. China have successfully curtailed both by a blend of technical, legal and regulatory measures which isolate local internet users from global internet, prevents a possibility of influence by foreign thoughts & ideas and instill a change of conduct in internet users, due to fear of ligigations [78].

3.2.2 Cyber Troops

Russia

- 5th Largest spender on Cyber troops ● : Russia has earned a reputable stature as a cyber power in recent times. The 2015 cyber attack against Ukraine caused huge power outage and 2016 cyber attacks against Ukraine which affected critical infrastructure are attributed to Russia. [98]. The 2017 NotPetya ransomware inflicted huge financial loss to Ukrain. NotPetya is attributed to Russia by US, UK, Canada and Australia [99]. Cyber posture of Russia is also considered to be offensive rather than defensive [99]. 2016 US elections are said to be meddled by Russia however no evidence of any tempering was found [100]. A total of 11 Russian Military Intelligence officers are wanted by FBI for interference in 2016 US Elections and is posted on website of FBI [101].

China

- 2nd Largest spender on Cyber troops ● : China is housing largest number of cyber troops and is a formidable cyber power. China is attributed with many huge data breaches including 2007 Lockhead Martin breach; giving away details about F35 fighter [102], 2013 breach; which gave away designs of advanced Patriot missile, THAAD and Aegis ballistic-missile defense system [103] and 2018 breach; giving away data about advanced Naval projects of US Navy [104].

3.2.3 Threat Intelligence

Russia

- Creation of GOSSOPKA ● : Put to service in 2015 GOSSOPKA has been at the forefront of Russian Cyber defense. It has NCCCI within FSB for management of cyber defense. Our study finds that GOSSOPKA struggled with getting all requisite legislation through state duma. Incorporating CII owners, huge costs to connect with GOSSOPKA and lack of trained staff are the is-

sues, which hindered operational efficiency of GOSSOPKA at true potential. Despite these issues it has setup a base for cyber security operations incorporating state, government and corporate sectors.

Till 2016 system was in place with 10 state organizations and 2 response centers were running in Rostec and central bank of Russia. Rostec is state owned corporate holding group comprising aroud 700 enterprises, bulk comprising of defense industries and civil sector [105]. Worth analyzing events at Rostec alone are in thousands each month and *by 2020 (i.e 4 years after creation of GOSSOPKA), only 30 percent enterprises out of defense industries would be able to be connected to Rostec's cyber defense system. One of the reason of this delay is said to be lack of qualified staff* [106].

Russian Military has been accused of gaining electronic components for a research institute owned by FSB [107]. The aim of this equipment was to study cyber attack scenarios and develop responses. In addition they are also required to certify imported softwares for any bugs or back doors. *These procurements cost thousands of dollars annually, but never used by research institutes. Lack of technical staff is often fulfilled by hiring freelance hackers* [108].

However Government of Russia credit GOSSOPKA with success in dealing with 50 Million cyber attacks in 2016. WannaCry virus affected telecom and government sectors in 2017 and according to government, no critical infrastructure was damaged in these attacks [109]. 2018 saw peak of cyber attacks on the day of election of Russian President, amounting of 20,000 sources. These sources were stopped and dealt with by NCCCI who later on took work of GovCERT as part of FSB [110]. In 2019 Government announces that it tackled cyber attack against Russian power grid by US. However no further details were given [111].

China

- Establishment of CNTIC ● : China National Cyber Threat Intelligence Collaboration (CNTIC) was established in 2017. It is result of collaboration of Government and leading cyber security firms of China. The collaboration will

be addressing the issues of data fragmentation and isolation. The platform has access to over 200 Threat Intelligence sources and high value intelligence will be shared across the nation [112].

- Establishment of CNCERT ● : CNCERT is the key coordinating point for Cyber security response. Detailed inspection of CNCERT/CC website reveal details about reporting of an event, its acceptance, disposal and feedback. It also has a 24/7 helpline and it has weekly and monthly reports regarding Malicious programs, DDoS attacks and events handled by CNCERT. It has also been collaborating internationally in cyber drills mainly with Asia Pacific Emergency Organization APCERT. *From the status of its updated reports and collaboration and 24/7 helpline, one can assume that CNCERT/CC has been working optimally and fulfilled its purpose.*

  According to 2014 report by CNCERT, it *handled 56,072 incidents out of 56,180 and took down 744 large scale botnet attacks*, most of these attacks originated from 3 locations including US [113]. In 2019, CNCERT report suggests large scale cyber attacks originated from US which affected millions of Chinese computers. Moreover most of the attacks china faced are from US IPs [114]. Weekly reports of CNCERT offer detailed insight of key findings including infected computers, backdoored websites, phishing websites and new vulnerabilities cataloged by National Information Security Vulnerability Sharing Platform (CNVD).

3.2.4 CERTS

Russia

- Russian - 5 x CERTS ○ : Russian public CERTS are not engaged in 24/7 work in contrast to private sector CERTS. Only performing public CERT is FinCERT and that is a specialized structure for financial domain. Up to date data and reporting is not available on public CERT websites; RU-CERT for example is member of FIRST other than CERT-GIB but it has 8 hrs working

time and only a single publication is available on their website, regarding a phishing attack dated back to 2017. *Russia was able to raise these CERTS however efficacy of these CERTS is ambivalent.*

China

- Chinese - 10 x CERTS ● : All of Chinese CERTs are members of FIRST, CNCET/CC being the official CERT of China. Out of these; 5 x CERTS are attending their parent company's customers for product and services vulnerabilities. Eversec, Dauha, HSRC and Qi An Xin are private cyber security companies and have maintained websites having updated security advisories, best practices, publications and newsletters. CNCERT/CC was also found to have maintained website having updated reports on weekly and monthly basis. *Chinese CERTS seem to be working optimally and enhancing their portfolio and expertise.*

3.2.5 National Technologies

Russia

- Banning Foreign Software ● : Foreign software was banned for use in state and municipal requirements in 2016. National Registry of domestically produced software is maintained since then and it has 5700 plus entries. One issue which is seen in this arrangement is availability of a category titled; Russian commercial organization with foreign persons in the chain of ownership. This situation is an issue in itself. Another issue is shifting to domestic software when organization is having license for foreign software and local software is not efficient or user friendly. Moreover shifting to domestically produced alternates is not possible in short span of time [24].

  In December 2018 authorities have asked to remove software of foreign origin from national registry within 6 months and technical staff faces an uphill battle to adjust with new requirements [115]. *As of September 2019 (after span of 8*

months) software of foreign origin is still listed in National Registry. Another issue faced by Russia is lack of hardware development industries in ICT. A lot of work is yet to be done in the field of software and hardware ICT technologies. Yet no notable Russian companies are to be seen having presence except Kaspersky; a cyber security company.

China

- Local development of software and hardware pursued as government vision ● : Foreign technology is seen as a threat to China and government is sensitive about foreign technologies. Local technology companies have been able to provide potent hardware and IT services however still a portion of this technology originates from US and Europe. It is accepted almost as an unquestioned fact that foreign systems are bugged to steal Chinese secrets. For this reason, strict controls have been imposed on foreign investors.

  Chinese 15 year plan calls for not obtaining core technologies that have an impact on national economy and national security. Correspondingly, R&D spending will be increased to 2.5 percent of GDP by 2020 [68]. China has also announced a five year tax break for chip makers and software developers [116] with an aim of achieving the goals of Made in China 2025 strategy [117]. Chinese companies are among top equipment vendors in the world and china is aiming to spearhead the race for 5G. 9 out of top 20 technology firms are in China. Out of 35,744 Chinese software firms more than dozen are valued more than $ 1 Billion [118]. *These stats tell a Chinese success story in local development of ICT technologies.*

3.2.6 Internet Kill Switch

Russia

- Internet Isolation Bill - Law passed in 2019 ● : Law for unplugging Runet was signed in May 2019 by President Putin due to be enforced in Nov 2019. Russia

cites threats to stable function of national segment of internet as main reason for this law. Critiques however differ from government of Russia's stance that ICANN is an international body and cutting out, for example; Russian domains on order of government of US will result in loss of its credibility forever and may result in regional networks like 1990s.

The law also authorizes Roskomnadzor to take control of communication networks in case of threat, but there is no responsibility of network crashes on neither the operators nor the Roskomnadzor. Finally in November 2019, a complete unplug of internet was tested bu Russia. As per estimates internet shutdown in Russia would cause a loss of 3.47 Million Dollars per Hour [119]. *Unplugging internet will raise concerns for business community and service providers themselves. Some web pages and services operating in Russia might face trouble operating normally, whose data or resource come from outside Russia. Even people in other countries might also face issues whose traffic is routed through Russia.*

China

- Kill Switch - Speculations? ● : China is said to have passed security law that give government, the power to control access of internet. It exclusively require companies to use Chinese technology and help create an internet kill switch [120]. However an official acknowledgment has never been given by Chinese government. An internet shutdown in 2012 is also attributed to Chinese Internet Kill switch but never confirmed [121]. The great firewall is already working for content filtering and access to many foreigner websites is blocked. Great Cannon is also potentially able to restrict access to unwanted foreign websites but *open discussion of an internet kill switch was never found in any Chinese literature and domestic websites.* In case China shuts down internet it will have to face a loss of 179.04 Million Dollars per Hour [119].

3.2.7 Content Censorship

Russia

- Registry for prohibited content ● : After establishment of prohibited content registry a law was passed in 2018 making it mandatory to connect to this system for automatic filtering by service providers and violators were to be imposed a fine [24]. By October 2018 most of the internet companies connected their servers with the system. However Google did not do so and its was fined $ 7500. The company quietly paid the fine. By Feburary 2019 Google started removing the banned content links from its search results and have removed upto 70% of the banned content from registry. However it did not do so in the automatic way. It was done manually after analyzing each content to be banned [122]. *The case of Google indicates how a company can get away without actually complying with the law in desired way. Google have neither denied connecting to the system; giving Roskomandzor face saving and nor acknowledged connecting to the system; effectively avoiding reputation damage. This highlights the loose compliance of law.*

- Digital Economy program ● : Digital economy program will be implemented by 2020. The league of internet has its white list with more than 1 million entries. Experts have an opinion that white lists may not be that effective until the content is independently verified and prohibited content is blocked. Social Media administrators have a responsibility to remove illegal prohibited content, else adult users may turn off filtering and children will still be vulnerable [123].

China

- Great Firewall of China / Great Cannon ● : Commissioned in 1990, GFW has been world's largest censorship mechanism. *The stability in China and public acceptance of Chinese Communist Party is attributed to the effectiveness of GFW.* Among other blocked websites and services are included those websites which contain any information about civil unrest either currently or in past.

The stringent censorship polices have their effect on the business and they have to rely heavily on VPNs and proxies. Chinese internet users also rely on VPNs for accessing foreign websites [124].

GFW has understanding of popular VPN traffic patterns and will drop all packets after few minutes, thanks to Deep packet Inspection and Machine learning. Few commercial VPNs are operating however, presumably to allow foreign businesses to work with ease. Tor browser also had a hard time beating GWF algorithm and started having issues in 2012, it only started working again in 2015 after Tor released protocols using pluggable transports [125].

GC has a visible impact when it is employed. It is presumed that higher authorities are taken in loop before launching attack, as targeting a foreign website may have potential backlash. In attack by GC against Greatfire.org, Baidu international traffic was redirected. Such actions could prove costly for repute of the website / brand and may result in litigation outside China.

3.2.8 Data Localization

Russia

- Law for local storage of data and processing ● : Subject law was passed in 2016 requiring local storage of data and shifting of personal data inside Russia which is already abroad. Linkedin refused to shift its servers containing data of Russian citizens. Consequently, it was first casualty as endorsed in register of violators of rights of personal data and blocked by Roskomandzor [126]. Facebook and Twitter both did not comply with the law yet and are facing criminal proceedings [127]. Other technology giants opted to use special cloud services instead of shifting their servers physically in Russia and avoided the legal requirement for FZ-242 compliance. These include Uber, Microsoft, Lenovo, Samsung, Paypal, Ebay and Ali Express [24]. Google, Apple, Alibaba, Viber and booking.com shifted their servers in compliance [128, 129]

  As per estimates 2.4 Million businesses are affected by the law and those not

complying will face fines repeatedly and banned ultimately. Firms are likely to face capacity crunch in Data center industry and high credit charges in case of financing [130]. On the other hand shifting and development of new Data centers is a good news for Russian software engineers due to creation of lots of vacancies [131]. *Despite clear violations of law, only one firm was banned and rest are still working in Russia. Overall a weaker enforcement of law by the authorities.*

China

- Establish local data centers ● : Chinese cyber security law mandates creation of local data centers for not only the *personal data* but also *important data* which concerns critical information infrastructure. Despite the comprehensiveness, the law is still ambiguous [132]; though doing its job. Apple in compliance is establishing two data centers estimated to be completed by 2020 [133]. Amazon, Microsoft and IBM already have a footprint in China through local cloud service partners. However data centers market will suffer in developed cities due to shortage of space and infrastructure availability [134]. In contrast data centers in central, western and north-eastern part of China are only half used despite incentives by government [135]. Availability of data centers infrastructure shuns the fear of over capacity amid new Chinese law. However ambiguous definitions of terminologies will be a problem in compliance and may cause undue litigation for example definition of *important data* is not specific and will be on discretion of authorities. Moreover any new firm coming to china will have to understand the possibility of scrutiny of its data by Chinese authorities. During 1st 2 years of this law, 11,000 arrests have been made. Japanese companies have faced raids by local authorities *demonstrating will of Chinese government in its enforcement* [136].

- Cross border data transfer control ● : The law was given draft shape in June 2019 and yet to be put in force. The draft has no mention of data localization for network operators. However it is upon operator to weigh in the

pros and cons. For handling *important data* local storage is a must as per data localization law. It provides preparation time to firms categorized as operators for implementation of law as it becomes applicable [137].

3.2.9 Alignment of Critical Internet resources

Russia

- Law on the Security of Critical Information Infrastructure ●: Multiple laws have been pursued by Russian lawmakers in this aspect. First in 2016 and then in 2017. Their adoption was hindered due to objections by telecom sector and budget constraints [24]. In 2018 a new bill was introduced, which made it through the legislation process and was signed by President Putin in May 2019. Even during its debate lot of ambiguities were left un-attended. 30 by-laws will be filling in those gaps. There are doubts about the effectiveness of the proposed law as Raskomandzor failed to deal with Facebook, Twitter and Telegram in making them comply the rules [59].

  There are reports of companies who own CII objects, not complying with the requirement of FSB to inform NCCCI about cyber incidents before sharing it with international IT firms [138]. *This in turn nullifies all the effort put in creation of GOSSOPKA, defining CII and its owners and creating a registry of CII etc.*

Table 3.4: Cybersecurity measures taken by other Countries

Country	Criminal Legislation	Regulation & Compliance	CIRT	Standards	Certification	Policy	Road map for Governance	Responsible Agency	National Benchmarking	Cyber Security Index [25]
France	✓	✓	✓	✓	✓	✓	✗	✓	✓	0.918
Australia	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.890
Brazil	✓	✓	✓	✓	✓	✓	✗	✗	✓	0.577
Canada	✓	✓	✓	✓	✗	✓	✓	✓	✗	0.892
India	✓	✓	✓	✓	✗	✓	✓	✓	✓	0.719
Indonesia	✓	✓	✓	✗	✗	✗	✗	✓	✗	0.776
South Korea	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.873
Malaysia	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.893
Germany	✓	✓	✓	✓	✓	✓	✗	✓	✓	0.849
Vietnam	✓	✓	✓	✗	✗	✗	✗	✓	✗	0.693

China

- Operations Security for Critical Information Infrastructure under Cybersecurity law ● : Chinese cybersecurity law has a section dedicated for security of critical infrastructure. In May 2019 draft measures have been issued which update the exisitng law.

  The draft measures call for identification of potential security risks before procurement by CII operators and apply to Cybersecurity review office for its review. Government have incorporated all state regulators in the review process, including security, finance, industry and broadcast. It will be reviewed within 30 - 45 days keeping in view multiple aspects ranging from its procurement, supply chain, funding and operations. Service and product providers are required to abide by recently issued standards due to be enforced by December 2019. Cloud services are to be hosted within China and their operational maintenance will also be done within china, unless specifically permitted otherwise. Encryption products can only be procured after clearance by Office of State Commercial Cryptography Administration (OSCCA) [139].

  In short, government have taken a wholesome approach, incorporating all legislators on board so as to avoid issues later on. They have addressed all issues that may arise and made a sustainable and future proof mechanism of cybersecurity review system. As complex of intermeshed strategies, regulations and standards, Chinese approach is considered even more comprehensive than that of US or Europe [140].

3.3 Measures taken by other Countries

A brief comparison of Cybersecurity measures in legal, technical and organizational domains is given below concerning countries mentioned in introduction [141, 142, 143, 25]. Their measures, whether taken or not are mentioned in Table 3.4 with ✓& ✗, respectively. The analysis of these countries reveal following:-

1. All the countries have some form of criminal legislation in their country. Most elaborate one are in Canada, South Korea and Brazil.

2. All the countries have Regulation & Compliance instruments. Most elaborate one are in Vietnam

3. All countries have CIRTs, with France and Brazil having 3 of them each.

4. All countries have National standard / frameworks for cybersecurity except Indonesia and Vietnam having no national framework. While India is relying on ISMS ISO 27001.

5. Most of the countries have cybersecurity certification / accreditation framework. While Canada, India, Indonesia and Vietnam have none.

6. All countries have one or more cybersecurity policies, except Vietnam and Indonesia.

7. Five countries have defined national roadmap for cybersecurity while Germany, Indonesia, Vietnam and Brazil have none. No data was available for France.

8. All countries have a national agency looking after cybersecurity. Both Australia and Canada have four such agencies.

9. All countries have some form of national benchmarking or referential except Indonesia and Vietnam.

10. Highest internet penetration rates (above 80 %) are in France, Australia, Germany, South Korea, Malaysia and Canada.

11. Penetration rates (less than 80 %) are in Brazil, Vietnam, Indonesia and India.

12. Highest Global Cyber security Index (above 0.8) is for France, Australia, Germany, South Korea, Malaysia and Canada.

13. Lowest Global Cyber security Index (less than 0.8) is for Brazil, Vietnam, Indonesia and India.

14. The emerging pattern is:-

- Higher the internet penetration rate, more the possibility of finding cybersecurity legislation and vice versa.
- Higher the number of cybersecurity measures, higher the Global cybersecurity index rating and vice versa.
- Higher the penetration rate, higher the Global cybersecurity index rating and vice versa.
- A country with more penetration rate may have lesser internet users in number and still have better cybersecurity index than a country with more internet users.

3.4 Conclusion

Russia and China are setting cyber norms in the new age of connected world. Each having their own philosophy and world view. Our systems today are much intervened and cannot be simply disconnected in order to be sovereign. Much more is at stake and need to be settled before this unplug.

Russia has gathered all the political will & support to take on this painstaking venture of a Sovereign RUnet. The Cybersecurity is now taken a national security issue and a potent cyber force has been raised. Establishment of GOSSOPKA and NCCCI are right steps for national level coordination required to thwart the dangers of cyber threats. Latest law authorizing a Russian Internet Kill switch will be a litmus test of synergy of Russian political will, legislature, law enforcement and industry. The law had holes and are bieng filled but will it be able to achieve its purpose, only time will tell.

China on the other hand has always been canny about internet in China and significance of maintaining Chinese core values. These values have been kept preserved by strict use of censorship and data control over the internet. Ruthless implementation of Cybersecurity law of China and upcoming Cross border data transfer control

are instrumental in implementing the vision of sovereign Chinese internet. It is the Chinese political will, that has forced foreign companies like Apple to build data centers inside China. The President Xi vision for China as a Cyber Superpower is encompassing and preemptive in addressing challenges posed by the future.

Chapter 4

International Best Practices

After analyzing the Internet Sovereignty Frameworks implemented by Russia and China we will look for the best practices followed by them.

4.1 Management of ccTLD under Government control

(a) Registrations, operations and management of ccTLD is handled by a non-commercial / government entity.

(b) Websites hosted by government & private organizations, individuals and businesses to use ccTLD.

4.1.1 Russia

(a) .RU and .РФis managed by a noncommercial entity CC for TLD RU, Coordination Center for Top Level Domain RU [144].

(b) CC for TLD RU also applied for another gTLD, Generic Top Level Domain .ДЕТИin 2012; the russian equivilant of *.children*. This ccTLD was specific for use by children and younger audience inside Russia. It aimed at safe internet usage for children.

4.1.2 China

(a) .CN is managed by Ministry of Industry and Information through CNNIC, China Internet Network Information Center. Raised in [145]

(b) In 2009 .CN was only allowed to be used by registered businesses. Individuals could only apply for other TLDs for example .net or .com etc [146].

(c) .CN was later banned for non chinese individuals and entitis [145].

(d) in 2011 Chinese also applied for .公司and .网络the Chinese equivalent of .compnay and .network.

4.2 Consideration of Cyber Security as matter of National Security

(a) Cyber Security is considered essential part of National Security Doctrine and given due importance. Number of supporting laws and legislation are passed to cater for securing the Cyber Domain of the nation state.

(b) Actions aiming for Internet Sovereignty and Digital Sovereignty stem from the ideas of sovereignty as perceived by the state and the challenges it is facing.

4.2.1 Russia

(a) Russia deals Cyber Security as an issue of National security in Information Domain.

(b) Any threat to security of information and internet is taken as threat to National Interest [28].

4.2.2 China

(a) China views any influence in information space as a threat to stability in Chinese society.

(b) China takes internet as a venue of exchange of information without any control by the state. This avenue can be exploited by the anti China forces for pursuing their agenda.

(c) China sees architecture of internet under American Influence by design and supports shifting of management of internet to an international body without influence of United States. Snowden Revelations have in 2013 also support the Chinese concerns [63].

4.3 Establishment of Potent Cyber Offensive Forces

(a) Establishment of Offensive Cyber force is pursued as regular kinetic military forces.

(b) These forces are given due share in national resources and training.

(c) Cyber offensive forces have been used to gain vital information and disrupt enemy at the time of need in coordination with regular military operations [146].

4.3.1 Russia

(a) Russia is perceived to have possessed Offensive Cyber Capability.

(b) It is the 5th largest spender on Cyber Troops.

(c) Many successful Cyber attacks are accredited to Russian including DDOS attack against Georgia in 2008 along with military operation [146], Cyber attacks on Ukraine in 2015 and 2016 targeting critical infrastructure [98], and Notpetya ransom ware attack in 2017 [99].

4.3.2 China

(a) China is a formidable Cyber Offensive power.

(b) China is second largest spender on Cyber Troops.

(c) Lockhead Martin data breach about F35 fighter jet in 2007 [102], data breach about THAAD and Aegis Ballistic missile defense system in 2013 [103] and breach about Projects of US Navy in 2018 [104] are accredited to China.

4.4 Raising of Potent CERTs in different sectors

(a) Dedicated CERTs available 24/7 are raised which deal in different sectors.

(b) A National level body to coordinate the response at National Level.

(c) Designation of National CERT.

(d) Legislation and designation of authority for international cooperation in Cyber domain.

(e) An updated central portal of National Level security advisories, best practices, publications and newsletters.

(f) Maintenance of data on reported security breaches and their followups.

(g) A defined mechanism to report cyber security incidents.

4.4.1 Russia

(a) Russia have 5 x CERTS dealing in different sectors [33, 35, 36, 20, 38].

(b) Sectors include general cyber incidents, government networks, financial sector, dealing with LEAs and industrial control systems.

4.4.2 China

(a) China have 10 x CERTS dealing in different sectors [73, 72, 74, 75, 69, 76, 70, 77, 71].

(b) CNCET/CC is designated as official CERT of China.

(c) Eversec, Dauha, HSRC and Qi An Xin are private cyber security companies and have maintained websites having updated security advisories, best practices, publications and newsletters

(d) CNCERT/CC have maintained a web portal containing reports on cyber security incidents on weekly and monthly basis.

(e) CNCERT/CC also coordinates with other stake holders in cyber Security domain inside and outside China.

4.5 Definition, protections and cataloging of Critical Information Infrastructure (CII)

(a) Legislation for definition and protection of CII including actions against defaulters and inland data storage for CII assets.

(b) Cataloging of CII assets.

(c) Establishment of an interconnected system for protection of CII assets.

(d) Inclusion of all ICT assets in protection of CII assets and networks.

(e) Security review of Networks, services and hardware for CII while procurement and periodic security audit review.

4.5.1 Russia

(a) In laws passed in 2016 and 2017 IXPs, TLD registers IP addresses and Autonomous System numbers are described as elements of CII.

(b) State law for Security of CII was enforced on 1st Jan 2018. It includes sectors of government, defence industries, finance, energy and nuclear technologies. The law requires these critical systems to be connected to GOSSOPKA; an interconnected system for protection of CII assets [57].

(c) A national registry of CII assets was made [24].

4.5.2 China

(a) A dedicated section for Security of Critical Infrastructure is added in Chinese Cyber Law.

(b) Cyber Security review office will review the the procurements by CII operators for any potential security risks.

(c) All CII operations producing or utilizing PII and cloud services are bound to be hosted, operated and maintained inside China.

(d) All encryption products will sough clearance before procurement from Office of State Commercial Cryptography Administration (OSCCA)

(e) Chinese state encourages operators other than CII operators to participate in CII protection.

(f) Creation of special security management teams and emergency plans for CII assets.

(g) Periodic review of security arrangements of CII assets and networks will be arranged for security loopholes.

(h) Bans and fines will be imposed on non compliance [**?**].

4.6 Information and threat intelligence sharing among Cyber Security tentacles inside the country

(a) A central organization for cyber security threat intelligence sharing.

(b) Central system aimed at detecting and forecasting cyber security threats.

(c) CII owners are required to create information sharing centers in their setups.

(d) Legislation for sharing of information with central organization.

4.6.1 Russia

(a) A 2013 law paved the way for establishment of GOSSOPKA; a system aiming to detect and prevent the consequences of Cyber Attacks [42].

(b) System was also made capable to forecast threat and act as single point of interaction.

(c) All private and public entities owning CII were required to established these centers in their organizations which were interconnected. Legislation was done for punishing anyone acting against CII systems.

4.6.2 China

(a) In 2017, CNTIC was raised; a collaboration was Cyber Threat Intelligence in China [86].

(b) Chinese government, CNCERT and domestic cyber security firms contributed their resources.

(c) This collaboration is aimed at proactive response to cyber threats.

4.7 Dedicated responsibility for international interactions for incident response

(a) Dedicated and defined responsibility is given to an organization which steer international collaboration in response for Cyber Security incidents.

(b) The organization is final authority in allowing anyone to share details of any incident internationally.

(c) The organization can deny sharing any information if it deem it a threat to national interest.

4.7.1 Russia

(a) National Coordination Center for Computer Incidents (NCCCI) was raised in 2018 [24].

(b) NCCCI was tasked with dealing in international collaboration for incident response.

(c) NCCCI could reuse to provide information if deemed against national security of Russia.

4.7.2 China

(a) Ministry of Foreign Affairs have a documented strategy for International Cooperation in Cyber Security [87].

4.8 Promotion of National Technologies

(a) Formulation of a vision for development of local technologies.

(b) Banning of Foreign Software for use in government offices.

(c) Establishment of catalog for local software.

(d) Identification of software from local companies with foreign owners.

(e) Diverting R&D resources for local production of technologies.

(f) Incentives for local technology companies.

4.8.1 Russia

(a) Foreign software was banned for use in government offices.

(b) A National level registry was maintained for locally produced software for procurement by government [24].

4.8.2 China

(a) In 2019, all government and public offices are ordered to remove foreign hardware and software within three years [147].

(b) Strict checks imposed over foreign investors.

(c) R&D spending have been increased to 2.5 percent of GDP [68].

(d) 5 year tax break has been given to promote local production of chipsets and software [116].

(e) Made in China 2025 strategy has been announced [117].

4.9 Implementation of Internet Kill Switch

(a) Analysis of extent of dependance on internet.

(b) Legislation to enable technical means to support independent internet.

(c) Creation of independent root DNS server and registry of IP addresses etc.

4.9.1 Russia

(a) Cyber exercises conducted to guage the extent of dependance on internet [51].

(b) Results of exercises advocated more technical measures including reserving DNS servers etc [50].

(c) Legislation done 2014 to 2019 to enable the internet in Russia to be operated independently.

4.9.2 China

(a) China is supposedly said to have a law that enables government to cut internet if required [120].

(b) The law also required companies to contribute in creating an internet kill switch by using Chinese technology.

(c)

4.10 Content Censorship

(a) Establishment of a repository for banned domains, network addresses and internet resources.

(b) A dedicated authority for managing network operators regarding banned content.

(c) Operators are bound to ban the resources mentioned in Banned content repository.

(d) A system to monitor compliance by operators.

(e) Requisite legislation for defining the banned content and fines for non compliance.

(f) Internet resources not safe for children are banned under separate program.

(g) Firewall filtering of international and domestic traffic as per the criteria for banned content.

(h) Human censorship for monitoring of internet resources.

4.10.1 Russia

(a) Russia have created a register for prohibited content resources.

(b) Roskomnadzor asks hosting site to remove banned content withing 3 days. On failure the site is included in banned content register.

(c) A system called as Revizor was put in place to check compliance by operators regarding banning of the content by consulting the register. Heavy fines were imposed for defaulters [53]

(d) Digital Economy program was introduced for provision of a safe internet for children by applying concept of white list [54].

4.10.2 China

(a) Functional since 1990 Great Firewall of China implements censorship policies by the government. 12 categories of internet resources are banned [81].

(b) International gateways have filtering mechanisms for international traffic filtering.

(c) IP blocking, DNS manipulation, URL filtering and filtering of keywords is used to censor international traffic.

(d) Human censors, internet police force and hired bloggers are employed for monitoring domestic network.

(e) National traffic is also censored by placing filtering mechanisms within internal networks [79].

(f) DDos attacks by redirecting legitimate traffic to websites meant to be blocked [82].

4.11 Localized Data Storage and Processing

(a) Bounding companies for storage and processing of data about the citizens inside the country.

(b) Shifting of hosting and storage service inside the country.

(c) Legislation for binding the operators and fine for defaulters.

(d) Information and services concerning CII assets to be kept inside country.

4.11.1 Russia

(a) Law FZ242 mandated storage and processing of data about Russians inside Russia.

(b) Shifting of hosting and storage services to Russia was also made compulsory.

(c) Defaulters were heavily fined and could face banning [24].

4.11.2 China

(a) Cybersecurity Law of China mandates CII operators to keep the information inside China [83].

4.12 Data Protection for Cross border transfer

(a) Legislation for Cross Border transfer of Data.

(b) Mandatory compliance of national law by the firms involved in transfer of data.

(c) Become party to international treaties regarding data protection.

(d) Defined procedure for application and approval of cross border data transfer.

(e) Verify compliance to data protection by other countries as per national law for data transfer permissions.

4.12.1 Russia

(a) Cross border data transfer allowed only if allowed under Russian law.

(b) Firms involved in data transfer to have agreements in between them, having terms included in the Russian law.

(c) Individual consent is required for data transfer.

(d) Written individual consent is required if countries are not included in the list of countries providing adequate data protection [55].

4.12.2 China

(a) Cyberspace administration of China (CAC) regulated parties involved in cross border transfer of data.

(b) Prior approval is necessary before data transfer.

(c) Contract between sending and receiving entity is required [84].

(d) Conditions for cancellation of permission in case of data breach or inadequate security measures [85].

4.13 Local Version of International Services

(a) Local services are promoted as alternate of international services.

(b) International services are blocked to prevent movement of data outside national borders.

4.13.1 Russia

(a) Russia have created alternate of global services and they are operational along with global services [41].

4.13.2 China

(a) China have blocked global services and replicated them locally.

4.14 Social Management using Internet

(a) Internet is taken as a tool for social management.

(b) Fear of litigation is used to enforce discipline in internet usage by population.

(c) Real identities are used for using social media accounts.

(d) Activities of users are logged and kept in record for a specified period.

4.14.1 Russia

(a) Russia have gradually enacted laws to control internet usage.

(b) Bloggers have to register themselves with Roskomandzor which have an audience of 3000 readers per day [148].

(c) Internet companies are obliged to provide access to government regarding user data [148].

(d) Data about users will be kept for 6 months and that to inside the Russian territory [148].

(e) Law also states that Bloggers cannot stay anonymous.

4.14.2 China

(a) Chinese ruling party takes internet as a social management tool [149].

(b) Social Credit System is used to make every action of a citizen accountable and having consequences [150].

(c) Government have agreements for cooperation with technology firms in order to provide data about the users [149].

(d) Users of Social Media have to register themselves with real identities [151].

(e) Service Providers will keep the record of user's all activities for 60 days and have to delete any prohibited content and inform the government [151].

4.15 National Standards for Certifications and inspections

(a) National Certification body should certify the equipment procured for use in Critical Infrastructure.

(b) Private certification bodies should be recognized by the government after necessary verification.

(c) A registry for certified software and hardware components is maintained for easy reference.

(d) All components of critical systems are endorsed in the national certification system.

(e) Certification is valid for a limited time.

4.15.1 Russia

(a) All equipment for critical systems have to get certification from Federal Service for Technical and Export Control (FSTEC) [152].

(b) There are 3 assessment levels to ascertain the number of critical components of the system.

(c) All software and hardware components of critical system will be endorsed in the FSTEC systems [152].

(d) A list is maintained for the components which are already certified by FSTEC for use in the operational technologies [153].

(e) Accreditation is performed by the certification bodies owned by the state [153].

4.15.2 China

(a) Critical Network Equipment Security Testing Implementing Measures are drafted [154].

(b) Definition of critical network equipment is given in Catalog of Critical Network Equipment and Specialized Cybersecurity Products [154].

(c) Organizations are Qualified for security testing after recognition by Certification and Accreditation Administration of China [154]. Certification is valid for a 3 years and equipment is required to be certified again after validation time [154].

Chapter 5

Best Practices and State of affairs in Pakistan

After analyzing in detail the best practices followed by Russia and China in pursuit of internet sovereignty we will review the state of internet and control of state over it under the lens of these best practices.

5.1 Management of ccTLD under Government control

Operations pertaining to ccTLD **.PK** maintained by a commercial organization named PKNIC since 1992. It control the operations of Domain Name System (DNS) for .PK, registration and maintenance of .PK domains. The owner of PKNIC is an Pakistani American named Mr. Asher Nisar. Currently the Company only have one office in Pakistan located in Garden Town Lahore [155]. The issues in current arrangement are as under:-

(a) There is no control of Government of Pakistan over .PK ccTLD.

(b) No stake of government of Pakistan in its management.

(c) No control of Government for provision of ownership data of domains in case of cyber crimes and their investigation as no WHOIS service is offered by PKNIC and owner data is only available on case to case basis after a formal request [156].

(d) Risk of non availability of .PK domains if Internet access to Pakistan is disconnected.

(e) Only mirror server is placed in Pakistan and original server is still inside USA subject to US laws. Any sanctions from US in future might impact the websites hosted on .PK domain.

5.2 Consideration of Cyber Security as matter of National Security

World over cyber security is taken as a matter of grave national security concern and due attention is given to it. Despite growing cyber threats and occurrences of cyber security incidents, no special measures have been take, nor Cyber Security considered as a matter of National Security. A 2018 breach involving sensitive data of Pakistani nationals surfaced including their names, CNICs, NADRA family tree and criminal records [157]. A recent breach is under investigation by PTA involving data of 115 million telecom users [158]. The issue cannot be oversimplified by blaming government for lack of interest only. Multiple factors are contributing to this current state of affairs. They include:-

(a) Cybersecurity is taken as an optional issue as country has been dealing with numerous issues at national level including dealing with terrorism and weak economy.

(b) No dedicated organization or government body is responsible for cyber security in particular at the moment. Even Ministry of Information Technology does not have this in their core responsibilities. That is why cyber security is no one's responsibility as documented.

(c) Time and again there have been data breaches including PII of millions of citizens and data dumps of bank cards on dark web costing hundreds of millions to banks and ordinary citizens. But no financial loss has occurred to the government. That is why government has been casual to this aspect.

(d) Many government departments and segments of public entities are still having paper based records. For this reason it is deemed that not much

is required to be done for security of information and digital space.

(e) Whatever mere security protocols have been implemented in government departments for the security of information and digitized records it is thought to be enough. No dedicated effort or responsible team or setup is there to ensure the security.

(f) Cyber Laws have been promulgated via Presidential Ordinance however its fruits can not be reaped by legislature and agencies as it was a temporary arrangement as Presidential Ordinance is valid for 120 days only [159].

(g) Another contributor for not giving due attention to the Cyber Security is the fact that very less number of Cyber crimes are reported in the reporting channels. Although NR3C - National Response Center for Cyber Crimes setup under FIA is mandated to see the complaints of citizens. However due to leak of personal information and fear of police and litigation very less number of crimes are reported. These low number donot merit the otherwise due attention of the decision makers.

(h) Any effort to take under control the use of social media and banning of chat platforms which are encrypted and used extensively by terrorist organizations is potrayed in the media as an act against basic human rights. This draws the undue hue and cry from media and civil society organizations. Such actions trigger citizens for agitation and makes implementation of any such law almost impossible.

(i) Change is always difficult and adapting to new laws is even hard for the government and people alike. Changing laws lead to change in routine and a hurdle in ease of use. This has also been a reason for no concrete attention towards the Cyber security and its recognition as a matter of National Security.

(j) What ever laws or directives have been passed and bans implemented over certain platforms like Banning Telegram or Blocking Youtube over Blasphemous content, people have always found a way to bypass these by using VPNs - Virtual Private Networks or Proxy Servers etc. Mostly free

versions of these services are used which are themselves home of malware and backdoor. This practice ultimately discourage the spirit of the said bans and discourage the decision makers.

5.3 Establishment of Potent Cyber Offensive Forces

There is no acknowledged cyber offensive force or setup currently functional in Pakistan. However private hacker groups have always remained active and time to time have displayed their proficiency by defacing my websites inside Pakistan usually aiming to highlight the security lapses in their websites. They have also defaced many Indian websites multiple times whenever there are tensions between two countries who are traditional rivals. According to a 2020 report, Pakistani Hackers have been in lead along with Chinese Hackers in hacking of Indian websites whose number amounts to 1 lac 30 thousand in five years [160].

5.4 Raising of Potent CERTs in different sectors

Ideally a CERT is a national level government organization which is tasked with protecting the national assets including critical infrastructures in case of a cyber attack. Currently in Pakistan there is no government agency which is dealing with this aspect and complete digital realm of the country is without any defense. Only government agency currently functional at this moment is NR3C under FIA which is primarily tasked with dealing matters involving Digital Forensics. There are few private organizations providing some level of incident response capabilities. However none of them is neither taken on board nor have the resources to respond to a national level cyber incident. National Cyber Security Council Act 2014 proposed for establishment of an independent CERT [161]. However this act could never got approval of the law making body. Currently following incident response resources are working in Pakistan:-

5.4.1 PakCERT

PakCERT was raised in early 2000 and was the sole solution provider in information security domain as official CERT of Pakistan. Its aim was to detect , prevent and respond to cyber threats. It also issues advisories and regarding latest vulnerabilities and cyber threats to affiliated community. It contributed to the cyber security community by discovering vulnerabilities in Microsoft Dot Net passport services [162]. PakCERT remained operational till 2011 and currently is not capable to respond to National level Cyber Incidents.

5.4.2 PISA Cert

Another CERT named as PISA CERT - Pakistan Information Security Association CERT was raised in 2009 [163] however it is also not operational as a CERT now. It is limited to educate the member community about latest threats and promote exchange of information security tips and techniques.

5.4.3 Triam Information Security Services

A sub-brand of Trillium Information Security Systems Private Limited, TRIAM provides specialized services like security monitoring, assessment and response. Currently it is providing services to corporate industry in multiple sectors [164].

5.4.4 NCSAEL CERT

NCSAEL also known as National Cyber Security Auditing and Evaluation Lab is established at NUST. It is affiliated with NCCS - National Center for Cyber Security and funded by HEC [165]. NCSAEL CERT acts as an academic CERT with limited scope, however they have participated in OIC CERT Cyber Drill in 2019 and stood first among teams participating from Pakistan [166].

5.4.5 NR3C under FIA

NR3C was raised in 2007 under FIA. It is aimed at handaling crimes involving technology and prevent technology abuse. It boasts about its expertise in Digital Forensic, Information security audits, penetration testing and technical investigations. Nr3C also informs organizations under DOS attacks. However its expertise are mostly focused on digital forensics including mobile, computer, video, and network forensics [167].

5.4.6 KPCERC

Khyberpakhtunkhwa Cyber Emergency Response Center (KPCERC) was raised by Khyberpakhtunkhwa Information Technology Board (KPITB). It is looking after security and digital health of the applications and services deployed, managed and under usage by the Government of KPK. It is also working for Cyber Security Framework of the province and aims to establish Provincial Security Operational Center (SOC) and Cyber Emergency Response Team (CERT). The center also offers courses related to Cyber Security and offer its services to industry in advisory roles [168].

5.5 Definition, protection and cataloging of Critical Information Infrastructure (CII)

At the moment there is no definition of sectors which can be termed as critical infrastructure for legislation purposes. Broad definition of critical infrastructure and critical infrastructure information systems has been given in PECA law 2016 [169]. But that is subject to its contextual definition. PECA Law also slaps imprisonment and fine on unauthorized acess, copy, interference with CII or transmission of critical infrastructure data.

Defacto CII setups can be counted as Army, SPD, NESCOM, Nuclear Installations, Power Grids, Internet and Communication service providers, Financial Institutions and Public Service departments. Defence organizations of Pakistan are working with

Air Gapped systems mostly and can be said to have adequate protection mechanisms in place. However public sector organizations have no such mechanisms in place. The fall out of cyber attacks on these sectors can be catastrophic and can have compound damage at national level.

5.6 Information and threat intelligence sharing among Cyber Security tentacles inside the country

The available cyber security assets inside the country are working mostly in isolation and at national level there is lack of a coordinating body. NR3C under FIA and NTISB under Cabinet Division issues warnings and advisories regarding emerging threats time to time. HEC and planning commission of Pakistan have raised NCCS - National Center for Cyber Security in 2018. The center has established 11 affiliated labs in different universities which specialize in different domains of cyber security. NCCS aims at playing a leading role in securing Pakistan's Cyber Space by a coordinated effort in building national capacity for R&D in cyber security and fulfill domestic cyber security needs [170]. Another initiative of NCCS is Pakistan Cyber Security Cluster which comprise of organizations and companies working in cyber security. It aims at providing a platform for government, industry, academia and end users to handle advanced cyber threats by utilizing collective knowledge [171]. The activities of NCCS are coordinated by a National steering committee. These initiatives may mature with time to share threat intelligence among the cyber security tentacles of Pakistan but for now, no formal information and threat intelligence sharing mechanism is available.

5.7 Dedicated responsibility for international interactions for incident response

There is no designated organization at official level for international interaction in case of cyber security incidents. PISA - Pakistan Information Security Association, a non profit organization has been active in international interaction and represented Pakistan in international cyber security forums. It has also represented Pakistan in APCERT, JPCERT and OICCERT events.

5.8 Promotion of National Technologies

Pakistan is currently completely relying on imported technologies including computer systems, networking hardware, cybersecurity hardware, operating systems, software etc. This includes all the cyber security hardware and software too. As a result complete digital eco system is exposed to potential influence by foreign powers with dedicated agenda. Recently there have been reports where *Pegasus* malware is said to compromise mobile phones of Senior government and military officials. Advisories on the subject have been issued by NTISB regarding banning WhatsApp for government officials [172]. There is limited to no capacity for hardware manufacturing inside the country. Recently government have approved policy for local manufacturing of Mobile phones [173]. However sizable software industry exists and in 2018-19 IT exports of Pakistan stood at $ 3 Billion [171]. This prowess in software is being used to some extent by government at federal and provincial levels.

5.8.1 National Information Technology Board (NITB)

At Federal Level NITB is entrusted with provision of IT services to government and ministries. It specializes in implementing e-governance programs, consultancy in digital transformation of departments and develop ICT applications as per requirements of Ministries and Departments [174].

5.8.2 Provincial IT Boards / Departments

At Provincial level governments of Punjab, Sind, KPK and Azad Kashmir are working at their level for in house development of IT solutions for government usage and public service provision [175, 176, 177, 178] with the help of provincial IT boards / departments.

Despite having these resources at hand there is no national framework or vision for replacing foreign technologies in favor of national technologies. There is no capacity building plan for replacing foreign technologies in public sector of government offices involving hardware, operating systems or cyber security assets etc.

5.9 Implementation of Internet Kill Switch

Currently there are 2 landing points for Submarine cables in Pakistan i.e. Karachi and Gwadar. And in total 8 cable are landing in Pakistan. Out of these Orient Express operated by Wi-Tribe and PEACE cable operated by Cybernet are due to be completed in 2020 and 2021 respectively with both having landing points in Karachi and Gwadar. The existing 6 cables are operated by PTCL and Transworld Pvt Limited. Currently there is no central control or oversight by the government over these cables and they are looked after by respective companies. At National level there is no central oversight or control at the landing points of submarine cables [179]. Therefore no central kill switch for the internet is available at the hand of authorities. However internet shutdown has been practiced at regional level on various occasions due to security and law & order situations in the country [180]. This shutdown has only been practiced in the case of wireless internet (3G, 4G and WLL services) usually coupled with suspension of cellular services.

5.10 Content Censorship

According to Article 19 of the Constitution of Pakistan, reasonable restrictions can be imposed on the freedom of speech for security of the state and glory of Islam [181]. Internet censorship is being managed by PTA - Pakistan Telecommunications Authority and FIA - Federal Investigation Agency on intermittent basis. In 2006 IMCEW - Inter Ministerial Committee for Evaluation of Websites was established and tasked with surveying and blocking the web resources which are against the state, contain pornography or are blasphemous. Orders to block content are given by Higher courts or Government to MoIT- Ministry of Information Technology and PTA. Sometimes direct instructions are passed to PTA and ISPs to block certain content [182]. This arrangement worked for sometime until challenged in the court by civil society and was stopped from working by Islamabad High court in 2014 [183]. In 2015 IMCEW was de-notified by the government and PTA was given powers to manage the content [184]. However content management and censorship is always touted by the civil society against freedom of speech, basic human rights and abuse of power by the state [184]. In reality such blatant behavior by civil society is itself quiet much exercise of freedom of speech.

5.10.1 Anti Terrorism Act 1997

Anti Terrorism Act 1997 is also available to the government for litigation in matters of banned content [185]. Section 11W covers creation and distribution of hate material. However the act misses sections to specifically deal with internet as a media. Clarification of offenses related to Internet are also lacking [186].

5.10.2 PECA 2016

PECA - Prevention of Electronic Crimes Act was passed in 2016. Section 10 of of the act deals with Cyber Terrorism and Section 37 deals with unlawful content. However PECA is far from perfect and major flaw in it is the vagueness in the definitions of multiple terms. These terms are left to be interpreted by Law Enforcement

Agencies and this fact draws criticism from civil society. The same vagueness can also be misinterpreted and offenders might get away with offenses [169].
The helplessness of government is evident from the fact that even the Minister for Information Technology and Telecommunication said that PECA Law has been amended and weakened due to the NGOs working for vested interests [187]. There is also a serious lack of capacity with NR3C in handling the complaints received under PECA.

5.10.3 Citizens Protection against Online Harm Rules 2020

In January 2020, government of Pakistan passed a law named *Citizens Protection against Online Harm Rules 2020*. The law nominated a National coordinator responsible to overall coordinate the regulation of online systems. It will also be government's representative to interact with social media companies. The section of the law were very elaborate and wholesome which can be summarized as under [188]:-

- Social media companies were required to act within 24 hours of receiving the intimation from PTA regarding blocking access to any content violating the existing laws.
- This time is further reduced to 6 hours in case of emergency.
- Social media companies are also required to ensure that no online streaming of content is allowed which is in violation of any law enforced at the time.
- Social media companies will establish offices in Islamabad within 3 months, with physical address and a nominated focal person of contact who will report to the national coordinator.
- Social Media company will establish servers in Pakistan within 12 months and all data will be stored within territory of Pakistan.
- Companies will be bound to remove or block access to user generated content of Pakistanis living outside Pakistan which include fake news, defamation or

violates religious or cultural boundaries or is against the national security of Pakistan.

- Upon notification by PTA regarding a content being false, the company is bound to put a notification on that and will be obliged to provide investigation agencies any data asked in unencrypted form.

- Upon failing to abide by the rules social media company may face blockage and fine upto 500 million rupees.

Like all the previous efforts to reign in the social media and enact boundaries to the online content, this law also faced severe criticism from the National and International NGOs and Civil Society. The prime minister decided to take all stake holders on board before implementing the law [189]. Currently the law is in suspended state and under broad based consultation by a committee headed by chairman PTA [190].

5.10.4 Notable Censorship and Bans

Over the years there has been numerous incidents of internet censorship and blockage. The notables ones are listed below:-

- In 2016, PTA blocked 84000 websites which contained objectionable material [191].

- In 2016, PTA asked all ISPs to block 429343 websites containing obscene material [192].

- In 2019 between January to June, Facebook restricted access to 128 pages and groups, 5376 posts, 7 Instagram accounts and 171 Instagram posts on the request of PTA [193].

- In 2019 between July to December, Facebook restricted access to 140 pages and groups, 2009 posts, 5 Instagram accounts and 116 Instagram posts on the request of PTA [193].

- From September 2013 to January 2016 Youtube was banned in Pakistan due to release of a blasphemous movie and Youtube's denial of blocking it. The ban was only lifted when Youtube launched a local version of the website. According to officials Google has provided a portal for reporting and requesting blocking of access to content violating local laws. Same will be reviewed by Youtube as per community guidelines and then accepted or rejected [194]. According to google transparency report, from January 2020 - March 2020 151,444 videos from Pakistan have been removed [195].

- According to Citizenlab Pakistan have been using Canadian firm Netsweeper filtering products on PTCL and PIE - Pakistan Internet Exchange Point. According to the report these products have been used to filter websites containing sensitive content including religion and human rights [196].

- Wordpress also faced a brief ban in 2015 over National Security reasons [197].

- In November 2017 a 37 hours blanket ban on Twitter, Youtube and Facebook was implemented by PTA in support of operation by LEAs - Law enforcement agencies against Faizabad sit-in participants. Access to these social media network were restricted on all mobile operator network. Fixed operators including PTCL, Cybernet and Witribe are blocked the platforms [198, 199].

- In July 2020, South Korean game PUBG - Player Unknown's Battlegrounds was banned by PTA after receiving complaints regarding its negative effects on the youth and reportedly multiple suicide cases due to failure in the game tasks. The game was un banned after company formally met the PTA officials and agreed to address the concerns of PTA [200, 201].

5.10.5 Missing Elements as per best practices

Content Censorship is practiced all over the world and being extensively exercised in the contemporary countries under study. While content is censored and blocked in Pakistan too and managed by PTA. The arrangement is more of adhoc

in nature and usually lacks legal strong footing. Legislation to define the banned content in terms of cyber space and punishments for non compliance are not present. As a result government decisions to ban any content or platform is usually reversed by court rulings. The orders for blocking a particular content are given time to time and there is no dedicated list or repository which is updated periodically and operators are bound to consult the list and ban the content. Operators are not strictly forced to adhere to given instructions to block a particular content. At times few web resources are banned by one service provider and not banned by the other. Usually fixed service providers like PTCL, Nayatel etc are more compliant to the government instructions. Currently there is no dedicated system or authority to monitor compliance by these operators. The younger population including children are equally exposed to the internet and its harms and no policy or vision exist to make internet usage safe for the children. There is no internet police force or human censorship arrangement at National level to clean the web of fake news and anti state or anti Islamic material.

5.11 Localized Data Storage and Processing

At the moment no law in Pakistan bounds companies working in Pakistan to keep the data stored inside Pakistan. Pakistan have a growing base of social media users and users of mobile apps whose data, including PII is stored by the companies in their servers outside Pakistan. Citizens Protection against Online Harm Rules 2020 asked the social media companies to store their data inside Pakistan, however due to hue and cry of civil society the said law is under review at the moment [188]. To add to the worries many critical websites are hosted outside Pakistan including website of Inter Services Selection Board (www.issb.com.pk), National testing Service (www.nts.org.pk), National Highway Authority (www.nha.gov.pk), Inter Services Public Relation (www.ispr.gov.pk) and many financial institutions [202]. Some of these are even using CDN services too.

Another glaring problem is that even the websites hosted inside Pakistan when accessed from within Pakistan, there traffic is routed from outside Pakistan. This is

alarming situation as traffic generated due to access of a service inside Pakistan does not route inside Pakistan and can potentially be easily eavesdropped while it traverse the global internet network [202].

5.12 Data Protection for Cross border transfer

Currently there is no Data Protection Authority in Pakistan. Draft of Personal Data Protection Bill 2020 is under discussion. The bill formulates obligations for anyone processing the data including requirements with regards to user consent, disclosure of information, retention of information, notification about data breach incident and regarding any cross border transfer of data. The law also demands a local representative of the data processing entity should be established inside Pakistan. Law also give the right to the subject of the data to access, correct, withdraw, erase and halt the processing of their data. Law also bounds the data processors to localize the data storage.
Law specifically defines personal data as information relating to a subject, who is identifiable from that and / or other information in possession of data controller. This information is only allowed to be sent outside Pakistan when the other country offers the same level of protection for personal data at the minimum [203].

5.13 Local Version of International Services

At National level no initiative is supported to promote local versions of international services. There have been efforts from local start-ups but they have not been much successful, as they could not face the onslaught of established platforms. An interesting thing to note is that when YouTube was banned in Pakistan in 2012 a local website Tune.pk got fame and was available as a local alternative to YouTube. The site was otherwise struggling since 2007. In 2015 the website was ranked 16th in Pakistan [204]. However as YouTube was unblocked later tune.pk lost the following. As of at the time of writing these lines Tune.pk ranked 1971 in Pakistan according to Alexa Ranking [205]. Similarly a start up TelloTalk aimed to give an alternate to

WhatsApp in Pakistan. Launched in 2017 it has a modest following and in 2020 at the time of writing these lines it has downloads of more than 500,000 on Google app store [206].

5.14 Social Management using Internet

Internet has witnessed a haphazard growth in Pakistan. Uncontrolled onslaught of foreign technologies and their unchecked adoption has raised concerns about the future of internet and its impact over society over the course of time. Absence of laws and failure to punish people due to weak litigation by the authorities and undue intervention by the civil society has resulted in almost no fear of litigation in case of spreading fake news, defamation campaigns, wrongful acquisitions, un-due criticism on government and law enforcement agencies, open propaganda by hostile elements on social media and open support for anti state elements. Daily we see new organized campaigns launched against government and armed forces on social media. All government machinery is focused on clearing the air and is on the back foot in this aspect. There is no mechanism to ensure that real identities are used to create social media accounts. Anyone can create a fake identity and start publishing anything he or she wants. Currently ISPs are bound to keep the internet log of user activities for 90 days [207], which can be used for digital forensics and investigations.

5.15 National Standards for Certifications and inspections

NCSB - National Communication Security Board was renamed as NTISB in 2002 with a revised charter of duties keeping in view the evolving nature of technologies. It is functionally under the Cabinet Division and tasked with following affairs [208]:-

- Advisory role with government for security aspects in use of ICT technologies in Pakistan's Public and Private sector, dealing with laws and offenses related to breaches in ICT security etc.

- Deal in policy matters with regards to use of ICT technologies in government departments and Armed forces.
- Advise government on national security with regards to ICT technologies.
- Oversee induction of communication security equipment after approval of NTISB.
- Assign projects for development of equipment related to ICT security.
- Periodic inspection of Government organizations with regards to communication security.
- Promotion of education in information security and related fields.
- Propose mitigation and advisories on reported flaws and security compromises.

NTISB is mandated with dealing all matters related to induction of security equipment for ICT Technologies. And they have been regularly issuing security advisories related to ICT related flaws and their mitigation [209]. However there is no capacity or defined role of any organization including NTISB in certifying the equipment procured for usage in government organizations or even Critical Infrastructure. There are no defined National Standard to follow while procuring any foreign technology for official use at government level. There is no capacity at private level to certify any imported technology. While there is no standard to follow for certification, there is no central repository for approved technologies which could be referred while procurement.

5.16 Additional Observations in Pakistan

5.16.1 Digital Pakistan Policy

In 2018 government announced Pakistan' s first Digital Policy [210]. It was aimed at promoting the IT industry of Pakistan and ultimately setup an environment which can harness the benefits offered by a digital ecosystem. Whole of the policy

was focused on stimulating the economic impact of digital productivity of Pakistan. The policy did not discuss much about Cyber Security or any control over the digital domain. It even offered complete foreign ownership of the digital ventures. Which clearly shows the lack of deliberation put in by the policy makers with regards to secure the cyber frontiers of the country. As policy aimed to digitize the government departments with no oversight regarding securing it is a disaster waiting to happen.

Digital Pakistan Vision

In December 2019 Government announced *Digital Pakistan Vision*. It aims at improving the digital connectivity, infrastructure, skills and promotion of innovation across the Pakistan. The Digital Pakistan Vision covers features which are overlapping with Digital Pakistan Policy of 2018 [211]. Although no complete document is available for Digital Pakistan Vision however Digital Pakistan Five Priorities as shared by Tania Adris, former Google Executive who is heading Digital Pakistan Vision enlist them as under:-

- Access and connectivity
- Digital Infrastructure
- eGovernment
- Digital Skilling & Training
- Innovation and Entrepreneurship

These five priorities are placed on top of Policy / Legal and Cyber Security stack. So it is a welcome sight to see Cyber Security in the planning parameters of Digital Pakistan Vision.

5.16.2 Provision of Encryption Equipment by Crypto AG

Crypto AG Operations

Cyrpto AG a Swiss company has been dominating the field of encryption devices for secure communication between governments and their assets world wide including diplomats. They have been at it since the World War 2 and transformed it from mechanical parts to the microchips and software. The company is known to provide this encryption equipment to more than 120 countries including Pakistan [212].

Operation Rubicon

In February 2020, it was revealed that the company Crypto AG was owned by CIA - Central Intelligence Agency in collaboration with German Intelligence in the operation named as *Thesaurus* and later renamed as *Rubicon*. And since 1970 CIA and NSA - National Security Agency steered all aspects of the company and its technologies including algorithms and its customers. These rigged equipments were sold for good money and US and German intelligence would eavesdrop over seemingly secure communication [212].

Russian and Chinese avoidance of Crypto AG

China and Russian (former Soviet Union) have always had anti western sentiment and the same sentiment prevented them from purchasing Crypto equipment from Crypto AG. As a result they were shielded from the effects of this CIA led operation. However concerns have also been raised on Kaspersky - Russian Cyber Security Firm [213] and Huawei - Chinese Giant working in Telecom [214] too about their influence by their respective governments.

Crypto AG and Pakistan

Pakistan has been using Crypto AG equipment for securing its communication channels between government officials across the globe. After these revelations it

can safely be said that these channels have been compromised and all the secret conversations ever done on these channels were readily available to US and German intelligence. Moreover these secrets were also said to be shared with few other countries including Britain.

5.16.3 Internet Exchange Point in Pakistan

Internet Exchange Point (IXP) was established in Pakistan in 2017 by PTA as PKIXP [215]. The aim was IXP was to direct traffic between ISPs inside Pakistan via this exchange instead of switching somewhere outside Pakistan. This will be beneficial in saving the foreign exchange in terms of payments to global internet networks and also will shield the internet traffic of Pakistan from foreign influence.

Development of PKIXP

PKIXP established two traffic exchange points in Pakistan at the venues of HEC. One at Islamabad and One at Karachi. Third traffic exchange point is planned to be established at Lahore. There are 9 operators in Islamabad and 8 operators in Karachi who have joined the exchange point at respective locations [216]. Bulk of

Operators in Islamabad	**Operators at Karachi**
PTCL	Cyberbet
Telenor	Multinet
Nayatel	Wateen
Wateen	Connect
PERN	GCS
Worldcall	PERN
Cybernet	Satcom
Multinet	Telenor
Witribe	-

Table 5.1: Operators connected to PKIXP

the population access the internet via mobile phone after the launching of 3G / 4G Mobile services. However only 2 operators i.e Telenor and Ufone (via PTCL)

have connected to the PKIXP. Remaining two operators Zong and Jazz formerly Mobilink have not yet agreed to connect to the PKIXP. To put it in perspective, Jazz is currently the largest mobile operator in terms of subscriber base. Together Jazz and Zong almost cater for half of the internet users in Pakistan. Currently there is no regulation which could force the operators to connect to PKIXP inside Pakistan. Due to their own agenda and policy IXP can not harness its full potential. Similarly this arrangement could have been instrumental in applying traffic monitoring and content censorship.

5.16.4 Use of Dark Web

Dark web has been in lime from time to time over repeated cases of Child Pornography and leaked data of Pakistani banks.

Noteable Incidents

In 2018 member of a global child pornographic ring was arrested from Sargodha. He was in possession of 650,000 items of child pornographic images or videos. Same year another person was arrested for rape and murder of a child from Kasur. He was later hanged. These incidents sparked a debate over dark web and its access inside Pakistan. 2018 also saw the reports of leaked bank data of 20,000 Pakistani Citizens on Dark Web. Another incident of mobile user data of 115 million Pakistanis is also found for sale on Dark Web in 2020.

Average Pakistani Internet User and Dark Web

An average internet user in Pakistan is not concerned with the dark web. Moreover average user gets easily scammed while using surface web by means of phishing campaigns. As a result they loose credentials, face financial looses and social media profile getting hacked. They are not likely to survive the dark web at all and may be easily scammed and get their system infected with Malware etc.

Law Enforcement and Dark Web in Pakistan

In cases of child pornography most of the arrests were made after assistance from foreign law enforcement agencies. The police presence on the dark web to monitor the happenings and infiltrating dark web dedicated circles of child pornography and other groups need considerable time, financial resources in the form of bit-coins and dedicated IT experts. Currently only functional organization dealing with cyber crimes is Nr3C under FIA. However they are mostly dealing with digital forensics. How to deal with crimes involving Dark Web is a currently a Myth and no special teams or prosecution courts or law exist at the moment.

5.16.5 Use of VPN Services in Pakistan

VPN services are used in Pakistan for number of reasons. Top most is the usage for accessing corporate networks and business to business transactions specially in financial sector. Other reason include accessing websites and content which are otherwise banned in Pakistan. Usage of VPNs by average internet user saw a boom when YouTube was banned in Pakistan in 2102.

Usage of Free VPNs

An average user uses free VPN for personal usage. And these users are most of the time oblivious of the harms of free VPNs. Beside slow browsing an average user does not notice anything unusual happening however these VPNs can do much more. They might themselves be containing malware. They might be tracking user activities. Free VPNs may also be redirecting their user to other sites un called for like HotSpot Shield has been found doing with its users. VPNs may also be collecting information about the user and this user data may be shared with respective governments under their own laws.

VPN Registration by PTA

PTA have recently given deadline to register all VPNs in the country by 30 June 2020. According to PTA the move is aimed at curbing the grey traffic through illegal exchanges and gateways which are causing loss to national exchequer. PTA has also commissioned a Deep Packet Inspection system from Sandvine, a Canadian firm to monitor the web and communications. Traffic will be analyzed and any traffic which is potentially VPN like will be flagged and connection be terminated [217]. Although the law for registering VPNs existed since 2010 and it is only implemented now. It is yet to be seen how it implementation is taken along as Civil Society and software houses working on small scale have objected to this measure of blocking VPNs. Only those software houses will be allowed to register their VPNs who will be registered with PSEB - Pakistan Software Export Board and PASHA - Pakistan Software Houses Association.

5.16.6 Lack of a Regulating Authority

Another issue which is hampering overall implementation of cyber laws and controlling the cyber landscape is absence of a central authority. As we see presence of an authority in Financial Sector in the form of State Bank of Pakistan, Power Sector in the form of Wapda, Petroleum and Gas in the form of OGRA and National Defence in the form of Ministry of Defence; there is no authority or regulating body to regulate the Cyber Landscape. Many laws have been approved and measures taken in isolation by PTA, Ministry of IT, FIA, NTISB etc but there is no national oversight and long term vision.

5.16.7 Legislation and Compliance

Number of laws are passed time to time. However no comprehensive Cyber Security law was ever passed after thorough analysis and consultation of the country's cyber space. Most of the laws when presented in draft form were either shelved or went through unprecedented amendments in the name of taking all sections on board.

This happened because there has never been a consideration that Cyber Security is also a domain of National Security now.
Existing laws were hardly ever updated over technological evolution, nor were implemented with true letter and spirit. This was due to multiple reasons:-

- There is no central authority to champion this cause.
- Laws have been made as and when something is highlighted after any incident, otherwise nothing was done as per any vision.
- There is not enough Technical Resource on board to monitor and implement the cyber laws.
- Undue importance is given to objections of civil society and this has led to judicial interference in implementation of laws as most of them were were either implemented through ordinances or adhoc measures e.g. blocking of banned content through IMCEW - Inter Ministerial Committee for Evaluation of Websites, however same was barred from working due to order of Islamabad High court on plea of Civil Society.
- There is no realization that cyber security is important for national security.
- Whatever laws we have, they have not been implemented harshly and very less number of convictions are done. In 5 years only 14 convictions were done under PECA which is alarming and disappointing at the same time.

We have seen in previous chapters that purposeful legislation was done to achieve vision of the state by Russia and China and it was ruthlessly implemented by the state.

5.17 Conclusion

Number of Laws exist and many cases have also been registered and people sentenced. However the law enforcement and policy making has mostly been at the

back foot and overly influenced by the Civil Society and Judicial oversight. There is lack of technical input in the courts to defend the cases involving cyber domain and there is no overall vision upon which cyber domain is regulated. Moreover there is no regulating authority which is pivot of policy making and its implementation in cyber domain.

Chapter 6

Way Forward for Pakistan

6.1 Introduction

As the days pass by, there has been increase in reliance on the ICT systems and interdependent systems. The lack of regulating framework and absence of a monitoring organization makes the cyber space of Pakistan a low hanging fruit for hostile cyber elements. Un-regulated growth of internet, e services, applications and foreign social media services add to the troubles and a threat to the Sovereignty of Internet in Pakistan. Moreover there is a dire need to recognize the importance of cyber space and recognize its security as an element of national security. This scenario merits raising a dedicated organization with a detailed framework who will champion the cause of securing the National Cyber Space and secure the Internet Sovereignty of Pakistan. This organization will work under the legal cover of National Cyber Space Act. The Act will have Sections pertaining to specific domains and these sections will be added and amended as per the evolving technologies and situations. The onus of drafting the Act and particular sections will be on the National Cyber Space Authority (Planning and Policy Division).

6.2 Vision

To secure the National Cyber Space of Pakistan with an aim to achieve Sovereignty in cyber domain vis a vis making it profitable for the Government, Citizens, Corporate Sector and IT Industry.

6.3 Establishment of National Cyber Space Authority (NCSA)

6.3.1 Guiding Principles

Raising of a National Body to oversee the Cyber Space of Pakistan will be based on the following guiding principles.

(a) Declaration of Cyber Security as National Security issue.

(b) Legislation to regulate the cyber space and exert sovereignty on National Segment of the Internet.

(c) Secure National Cyber Space by raising a dedicated authority at National Level.

(d) National level coordination by this Authority to prevent duplication of efforts and resources.

(e) Cataloging of threats.

(f) Development of Cyber Offensive and Defensive resources.

(g) Localization of data and services.

(h) Territorialization of Information.

(i) Development and promotion of local technologies and services.

(j) Development of Internet Kill Switch

(k) Strict implementation of laws.

6.3.2 NCSA Concept

There is dire need to establish a National Level body as NCSA - National Cyber Space Authority. This authority will be overall responsible for the National Cyber Space, over see long term goals and coordinate the efforts of all stake holders in Cyber Space for achievement of these goals. The NCSA will be headed by the **Chairman**

NCSA. He will be responsible for communicating all National Cyber Space issues to the Prime Minister of Pakistan. The NCSA will comprise of five divisions; Cyber Threat Intelligence Division, Cyber Operations Division, Cyber Content Management Division, Enforcement and Audit Division, Planning and Policy Division. The detailed about the hierarchy of the NCSA is as under.

6.3.3 Advisory Body

The chairman will be assisted by the National Cyber Space Advisory Body. The Advisory Body will have the reps from Industry (ISPs, Telecom companies, Cyber Security service providers, PISA, Chief Information Security Officers of the Industry Organizations, White Hat Hackers, PASHA and Technical Experts), Academia (Research organizations, Universities, Academic CERTs, Cybersecurity labs), Government organizations (Pakistan Telecommunication Authority, Federal Investigation Agency, Intelligence Bureau, Ministry of Information and Broadcasting, Ministry of Science and Technology) and Reps from Armed Forces (Inter Services Intelligence, Military Intelligence, Technical Experts from Army).

6.3.4 Cyber Threat Intelligence Division (TI System)

This Division will enforce and coordinate information sharing among cyber space elements in Pakistan. This information will be used to Analyze the threats and forecast the cyber attacks. Cyber Threat Intelligence Division will comprise of 3 wings; Critical Information Infrastructure Wing, Threat Analysis and Forecasting Wing, Surveillance and Monitoring. This Division will run a unified Threat Intelligence System (TI System) which will be fed by CII Wing, Threat Analysis and Forecasting Wing via information received from National Cyber Security Assets and Surveillance & Monitoring Wing by extracting cyber intelligence from National and International Cyber Landscape.

1. **Critical Information Infrastructure Wing (CII Wing)**
   This wing will be responsible to Catalog all CII assets in the country. These

CII assets will be connected to the CII wing via their Cyber Security Centers. Any attack on one CII asset will be immediately communicated to all Cyber Security Centers of other CII assets. All procurements in the CII assets will be communicated to the CII wing and their catalog will be updated accordingly. The established flaws will be patched and mitigation steps be taken accordingly by all CII Cyber Security Centers. CII Wing will also make sure that no CII services and those using PII to be hosted, operated and maintained outside Pakistan. Special security management teams will conduct periodic review of the security measures taken by the CII asset owners and these teams will be authorized to impose heavy fines on the CII asset owners.

2. **Threat Analysis & Forecasting Wing**
   This wing will be point of contact for all Cyber Security assets in the country. Any threat or breach noticed by any Cyber Security asset in the country will be reported to the Threat Analysis & Forecasting Wing. The Wing will analyze and forcast emerging Cyber Threats. This will be communicated to all other Cyber Security assets in the country and alerts / advisories be generated at National Level via TI System.

3. **Surveillance & Monitoring Wing**
   This wing will be responsible for Surveillance of National and International Cyber Space to identify the threats. It will feed TI System.

6.3.5 Cyber Operations Division

Cyber Operations Division will be responsible for the active operations in cyber domain by special resource and incident management by the CERTs for the Government and different sectors. The Division will also collaborate will all available Cyber operations resources in the country. Cyber Operations Division will also be empowered to collaborate or negate sharing of data about cyber incidents internationally ensuring National Interest. It will comprise of 3 wings; Collaboration Wing, CERTs and Special Operations Wing.

1. **Collaboration Wing**

   This wing will pool up cyber resources at national level for cyber operations of the division and help coordinate and collaborate. It will have collaboration desks for Academic Certs, Corporate Certs, Private Certs, Armed Forces, International Liaison, NR3C, Intelligence Bureau etc. The Wing will also be authorized to requisition resources in case of National Emergencies on behalf of the Cyber Operations Division.

2. **CERTs Wing**

   The CERTs wing will be responsible to mange the cyber incidents in the National Cyber Space. It will have dedicated certs for specific sectors.

   (a) GOV CERT will look after all government networks and installations.

   (b) FIN CERT will look after safety and incident response for financial sector of Pakistan including State bank, commercial banks, Stock Exchanges, Investment institutions etc.

   (c) TEL CERT will be responsible for telecommunication sector and internet service providers in the Pakistan.

   (d) PAK CERT will coordinate the response of all the CERTs. Moreover it will be responsible for managing any incident in the National Cyber Space. PAK CERT will also be the official representative of Pakistan in the world. A National Portal for the cyber threats to Pakistan and reported incidents and responses will be maintained by PAKCERT. This portal will be the available for research purposes and monitoring the trends. The portal will be updated weekly.

3. **Special Operations Wing**

   Special Operations Wing will be responsible for offensive cyber operations. The wing will raise/ hire and manage pool of Hacktivists, Volunteers and Special resources at National level which can be used for special assignments in support of the Government and National Narrative. Special Pool of Cyber Experts be

raised in Army for offensive cyber operations. The resources of Army and Hacktivists will also undergo cyber exercises together.

6.3.6 Cyber Content Management Division

This Division will be responsible for management and blocking of the Banned Content. It will consist of 2 wings; Banned Content Registry Wing and Compliance Wing.

1. **Banned Content Repository Wing**
   This wing will manage and upkeep the Banned Content Repository (BCR). This repository will have banned domains, network addresses and internet resources. The repository will be updated daily at 9 AM and all service providers will be required to consult and ban the resources mentioned in the repository.

2. **Compliance Wing**
   Compliance Wing will be responsible for overseeing the compliance by the Service Providers regarding the Banned Content Registry. It will impose fines on the service providers upon failure to comply. THe wing will have a pool of Human Censors who will scan the cyber space for banned material. They will mark the objectionable content and websites will be asked to remove the content within 24 hours. Upon failure the website itself will be added in the BCR. The human censors will also identify and block / ask for modification of banned content on the websites.

6.3.7 Enforcement and Audit Division

This Division will be responsible for Auditing the Government Setups and Networks. It will also deal with all the legal issues and dealing with the litigation proceedings. The division consist of 2 Wings; Legal Wing and Technical Wing.

1. **Legal Wing**
   This wing will be looking after the legal issues, dealing with the courts, Cyber Space Legislation and litigation proceedings.

2. **Technical Wing**
   This wing will audit the government departments and ensure compliance of the Cyber Space policies by the government setups.

6.3.8 Planning and Policy Division

This Division will be responsible for long term planning and policy development accordingly. It consist of 2 Wings; Capacity Building Wing and Planning Wing.

1. **Capacity Building Wing**
   This wing will be responsible to oversee the capacity cuilding in cyber expertise as per the national requirement and emerging technologies. It will also support and steer the National Initiative for Local Web Services. It will be in collaboration with the Higher Education Commision and Ministry of Education.

2. **Planning Wing**
   This wing will responsible for the long term planning and vision for the Cyber Space of Pakistan. It will be having a Research Group at its disposal for conducting studies and give input in formulating the policies and long term plans.

The proposed hierarchy of National Cyber Space Authority is illustrated in Figure 6.1

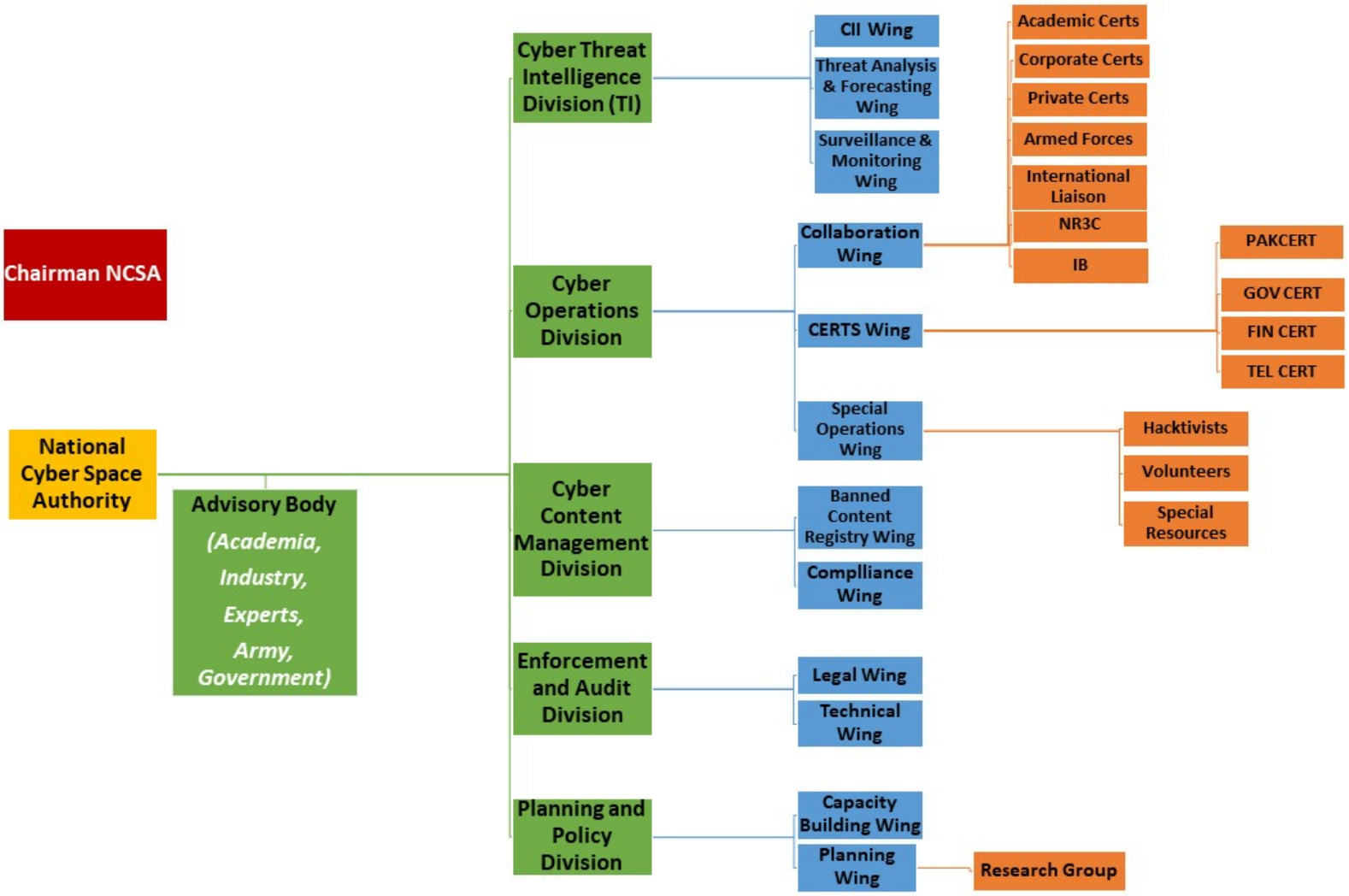

Figure 6.1: Proposed Hierarchy of Natioanl Cyber Space Authority

6.4 Management of .PK domain

Government should take all necessary measure to shift the .PK domain server and operation inside Pakistan under government control. Any .pk website will be registered only in the name of a Pakistani Citizen.

6.5 Localized Data Storage and Processing

All international web services wishing to operate inside Pakistan should launch the .PK local version of the website. Any website dealing with the PII of the Pakistani Citizens should be made to locally store all the information about Pakistani Citizens and all servers and hosting of such website will be managed inside the territory of Pakistan. Heavy Fines and even ban on the service should be implemented in case of non compliance. The routing for internet traffic generated by the local hosted services will be ensured to route within Pakistan.

6.6 Management of CII Assets

1. Sectors including Telecommunication, Internet Service Providers, Finance, Energy and Government Networks be declared CII.
2. All systems dealing with PII also to be declared CII assets.
3. It will be mandatory to have cyber security center in all CII assets.
4. All CII assets will connect to the CII Wing Cyber Security Center.
5. Defaulters will be heavily fined.
6. All procurements done in CII setups be done after approval from National Certification Body.
7. Requisite legislation be made.

6.7 Information Sharing among Cyber Security Assets

It will be mandatory for the Cyber Security assets in the country to share information with Threat Intelligence System (TI System) of the Cyber Threat Intelligence Division. Any important information will be communicated Nationwide via TI system to all concerned assets. The flow of feeding of TI System is illustrated in Figure 6.2

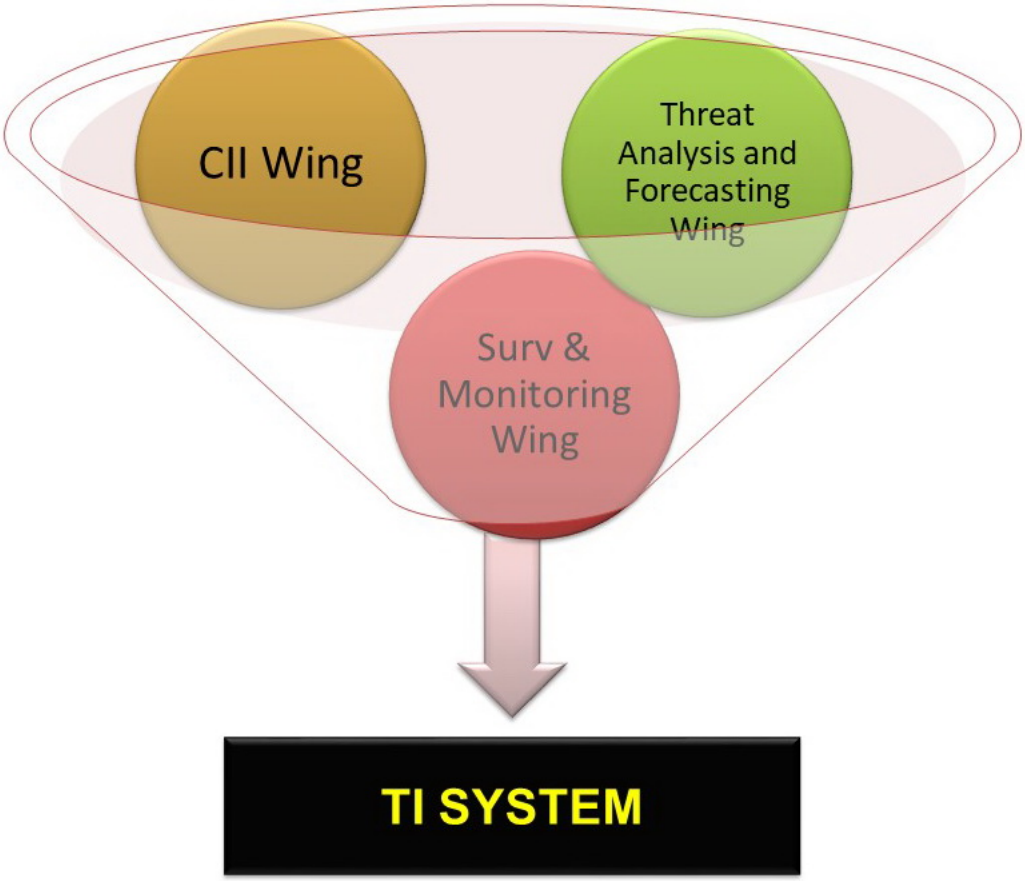

Figure 6.2: Threat Intelligence System

6.8 Content Censorship

Clear legislation will be done by Government for identifying and marking the banned content and its punishment.

6.8.1 Banned Content Repository

It will be mandatory for all ISPs to connect to the Banned Content Repository (BCR) maintained by the Cyber Content Management Division and automatically comply to ban the web resources in the repository. The repository will be updated daily at 9 AM and all service providers will be required to implement the ban within 24 hours. Service provider will be fined upon the delay to ban the content within 24 hours. On failure to comply within 3 days, the Service Provider will be liable to enhanced fine / ban or both. In case of the removable / modifiable banned content on website the website will be asked to remove the content within 24 hours window. Upon failure the website itself will end-up in BCR.

6.8.2 Human Censors

Compliance wing of the Cyber Content Management Division will also have a pool of Human Censors to survey the websites and web resources and manually ban / edit the **banned information** and **fake news** as required. ISPs and the website admins will be bound to comply with the authorities is this regard.

6.8.3 Management of International Traffic

All international traffic will be scanned and managed at IXPs at Karachi and Gawadar.

6.8.4 Fake News / Propaganda

It will be mandatory for the social media accounts and bloggers having either more than Three thousand views per day or a Follower base of Ten Thousand or

more will be required to register their accounts / social media handles with their Real Identity (Real Names and CNIC etc) at the Compliance Wing. Failing which their accounts will be banned within a month of reaching the said criteria. In addition strict punishments will be given on Fake News / Propaganda by anyone on the cyber space. The flow of information in support of Content Censorship with BCR is illustrated in Figure 6.3

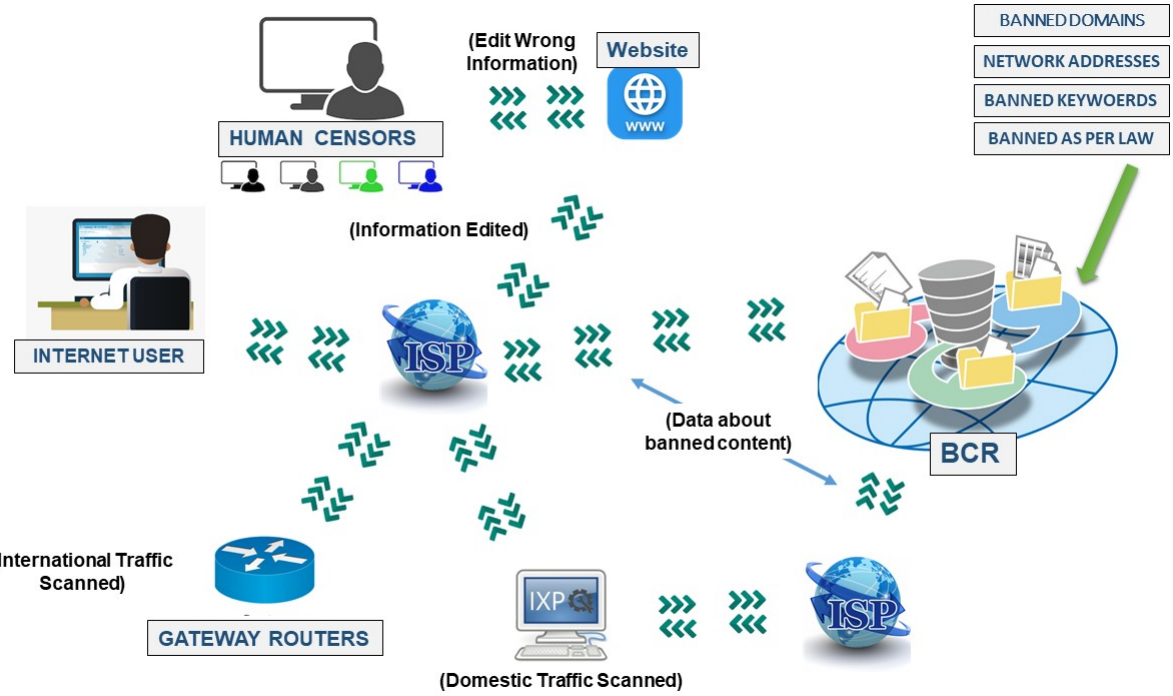

Figure 6.3: Banned Content Repository

6.9 Enactment of Citizens Protection against Online Harm Rules 2020

The Citizens Protection against Online Harm Rules 2020 law should be reviewed and enacted as soon as possible while ensuring government control over the social media companies.

6.10 Promotion of Local technologies

A long term plan for capacity building of local industry is required to be formulated to cater for the country's software and hardware needs. In that following is required to be done:-

1. Local software be gradually introduced in government offices and all public sector organizations.
2. Promotion of local social media platforms and incentives for the software company.
3. Hardware development industry to be setup inside Pakistan and gradually all Hardware to be manufactured inside Pakistan.
4. Locally developed applications and portals be used for official correspondence and communicatiuon between government ministries and organizations.

6.11 Internet Exchange Point (IXP)

To ensure optimum utilization of IXP following must be ensured:-

1. Legislation to force all operators to connect to IXP.
2. Ensure Routing of all local services within Pakistan.
3. Heavy fines for non compliance and canceling of licenses for operators.

6.12 Internet Kill Switch

Following actions must be taken for implementation of Internet Kill Switch:- Conduct Cyber Exercise to ascertain the level of dependency of National Segment of the Internet on Global Internet. Force all foreign websites wishing to operate in Pakistan to launch .pk versions. Any website dealing with PII of

the Pakistani Citizens to store their data and shift the processing inside Pakistan. Bring .pk ccTLD operations inside Pakistan under Government Control. Create Reserve DNS query Server for .pk domains inside Pakistan. Force all routing for local services to remain inside Pakistan. Force all Operators to connect to IXP.

The proposed schema for local routing and reserve DNS query operations is illustrated in Figure 6.4

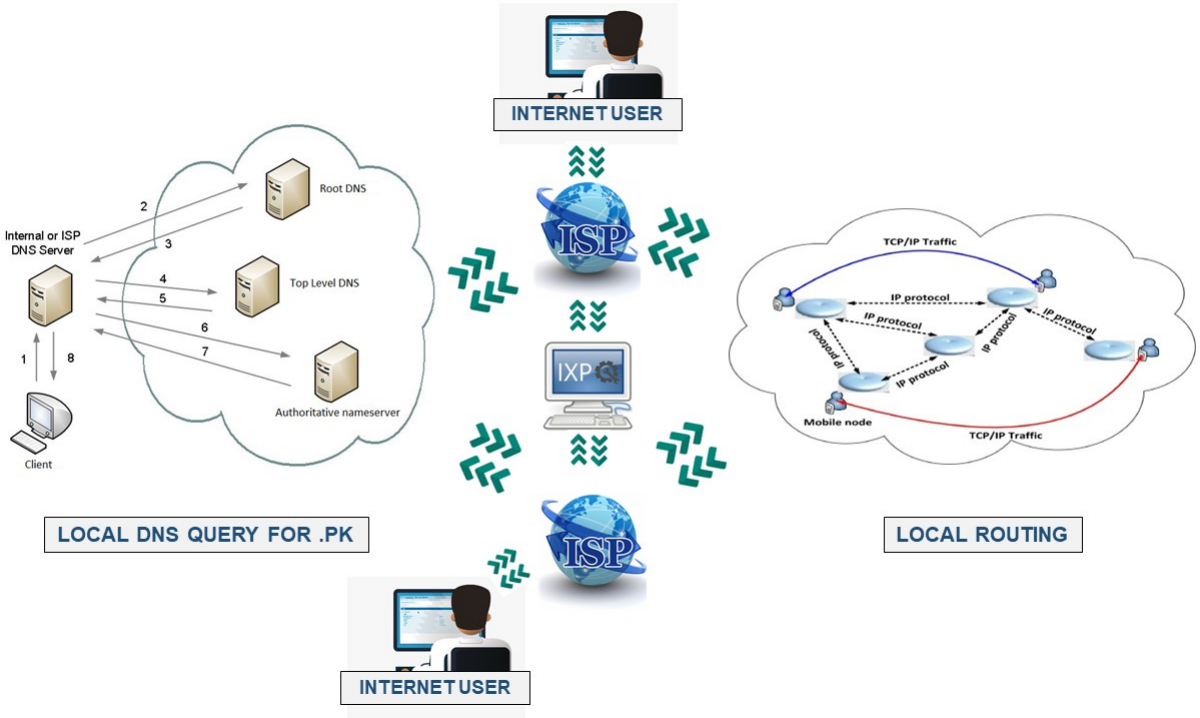

Figure 6.4: Local Routing in support of Internet Kill Switch

6.13 Data Protection for PII

Following measures be taken for protection of PII:-

4. Personal Data Protection Bill to be implemented as soon as possible.

2. Any foreign company operating in Pakistan dealing with PII of Pakistani Citizens to store data inside Pakistan.

6.14 Social Management using Cyber Space

Following measures be taken to harness the potential of Cyber Space in order to implement social control:-

1. Legislation be done to ban fake accounts and fake news.
2. Severe fines and imprisonment for defaulters.
3. Promotion of local social media platforms by government and mandatory usage of real name and identity for registration on them.

6.15 Capacity Building of NR3C

NR3C should be enhanced and its capacity building should be pursued. Following measures are recommended to be taken :-

1. Raising of Cyber Police Wing under NR3C, with its physical presence in all provinces for apprehensions, arrests and strict implementation of Cyber Laws.
2. Special Operation wing be raised in NR3C to deal with crimes involving emerging technologies like Block chain, IoT devices and Dark web etc.
3. Special Wing be given requisite resources including financail resources like bitcoins at their disposal to infiltrate dark web cartels.
4. Pakistan to sign Mutual legal assistance treaties with other countries to share data on cyber crimes and assistance in investigations.

6.16 National Standards and Certification

Following actions should be taken for National Cyber Standards and Certifications:-

1. National Certification Body to be raised.
2. It will develop standards for all technology components used inside country.
3. It will certify all technology components (software and hardware) being used inside the country.
4. Registry for approved software and hardware be maintained for government usage.
5. The registry will also contain all certified components used in CII assets.
6. Any certification done to be valid for 3 years and require re certification after validity period.

6.16.1 National Certification Body (NCB)

The NCB will inspect and certify all pieces of technology being procured or produced inside the country. They will be scanned and certified to be free of backdoor and bugs which may pose threat to National Security. NCB will have 6 Divisions; Network Division, Software Division, Mobile Division, Computer Hardware Division, Cryptography Division and Planning & Policy Division. NCB will be directly answerable to the Cabinet Division. It will scan all Network components, software & mobile applications, mobile devices, computer hardware and cryptography hardware procured in the country for bugs, backdoors, malwares and any potential threat to National Security. Upon any potential threat the said piece of technology (hardware, software, mobile application) will be banned in the country. The proposed hierarchy of National Certification Body is illustrated in Figure 6.6. The working of National Certification Body is illustrated in Figure 6.5

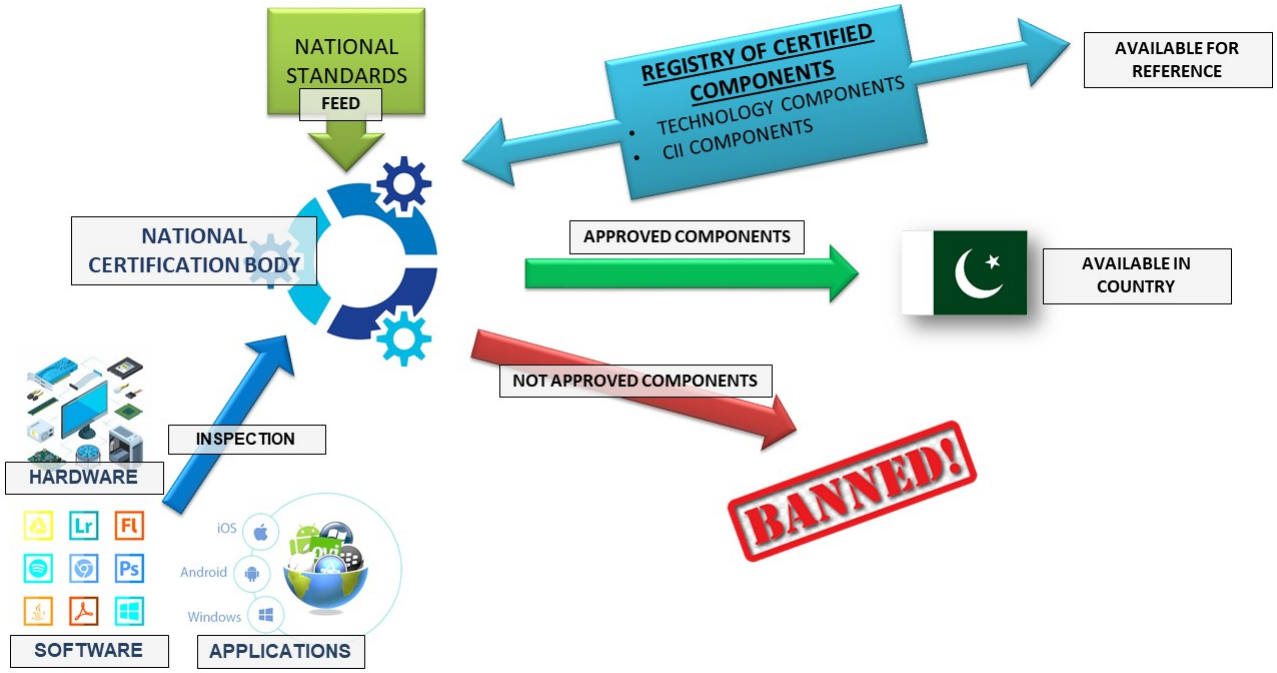

Figure 6.5: Working of National Certification Body

6.17 Conclusion

The Cyber Space is continuously evolving along with evolving technologies around the world. With such pace of evolution it is a tough job to keep up with the legislation and its implementation. A dedicated authority with dedicated agenda will be able to perform in this regard. The requirement from the government will be to provide the legal cover and justification so as to avoid un necessary litigation and reversal of the gains by this dedicated organization.

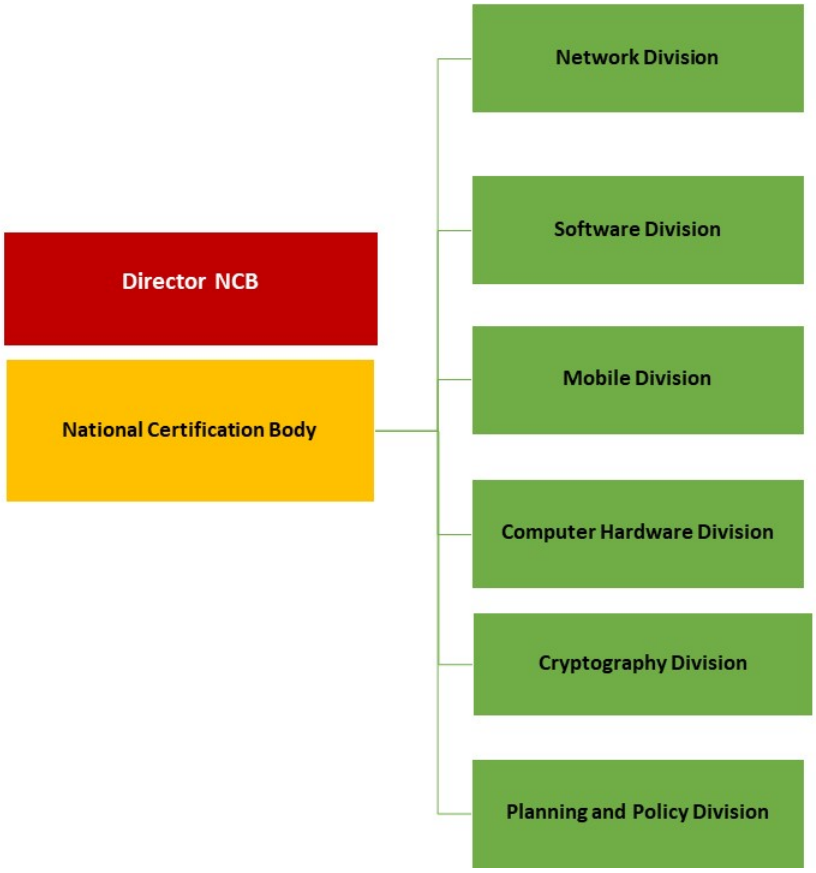

Figure 6.6: Proposed Hierarchy of National Certification Body

Chapter 7

Conclusion

The Cyber Space is a national security domain and the earlier a nation realizes it the better. China and Russian modles have been tailored according to their own needs and situation. Internet by design is decentralized and special measures will be required for control over this entity which is present in virtual cyber space. Pakistan have not done enough in this regard till date. Now is the time to take Cyber Security a component of National Security and take a systematic approach to streamline the matters including legislative, technical and administrative measures. Consideration of Cyber Security as an element of Natioanl Security will be 1st step in this direction. With the legal backing the preceding steps will be fruitful and decisive in achieving the final goal of sovereignty on the national element of internet.

Bibliography

[1] "Internet sovereignty," Mar 2017. [Online]. Available: https://digital.report/internet-sovereignty/

[2] I. Cobain, "Revealed: Us spy operation that manipulates social media," Mar 2011. [Online]. Available: https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

[3] A. Breuer, "The role of social media in mobilizing political protest: evidence from the tunisian revolution," *German Development Institute Discussion Paper*, no. 10, pp. 1860–0441, 2012.

[4] N. Telecommunications and I. Administration, "Ntia announces intent to transition key internet domain name functions," Mar 2014. [Online]. Available: https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

[5] T. Maurer, I. Skierka, R. Morgus, and M. Hohmann, "Technological sovereignty: Missing the point?" in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*. IEEE, 2015, pp. 53–68.

[6] "Montevideo statement on the future of internet cooperation," Oct 2013. [Online]. Available: https://www.icann.org/news/announcement-2013-10-07-en

[7] D. Castro, "How much will prism cost the us cloud computing industry," *The Information Technology & Innovation Foundation*, pp. 1–9, 2013.

[8] "U.s. knocks plans for european communication network," April 2014. [Online]. Available: https://tinyurl.com/y3xjaeh6

[9] "General data protection regulation," Apr 2016. [Online]. Available: https://eur-lex.europa.eu/

[10] "Gdpr key changes," Apr 2017. [Online]. Available: https://eugdpr.org/the-regulation/

[11] F. R. of Legislation, "Personally controlled electronic health records act 2012," Jun 2014. [Online]. Available: https://tinyurl.com/y2ufbpku

[12] "Marco civil," May 2014. [Online]. Available: https://www.publicknowledge.org/documents/marco-civil-english-version

[13] "Personal information protection and electronic documents act (s.c. 2000, c. 5)," Jul 2019. [Online]. Available: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html

[14] "British columbia's personal information protection act," Jan 2004. [Online]. Available: https://www.oipc.bc.ca/about/legislation/

[15] "Revisiting the data protection regime in china," May 2014. [Online]. Available: https://globaldatahub.taylorwessing.com/article/revisiting-the-data-protection-regime-in-china

[16] "A guide to the french national clouds," Nov 2013. [Online]. Available: https://gigaom.com/2013/11/18/a-guide-to-the-french-national-clouds/

[17] "It security made in germany," Aug 2019. [Online]. Available: https://www.teletrust.de/en/it-security-made-in-germany/

[18] "National security council proposes 3-pronged plan to protect internet users," Feb 2014. [Online]. Available: https://tinyurl.com/yyv82e67

[19] "Law no. 11 of 2008 on electronic information and transactions," Dec 2012. [Online]. Available: https://s3.amazonaws.com/documents.lexology.com/b1169086-e530-408f-ba00-70365b7bd2ed.pdf

[20] "Laws of malaysia, act 709, personal data protection act," 2010. [Online]. Available: https://www.kkmm.gov.my/pdf/

[21] "Personal information protection act," Mar 2011. [Online]. Available: http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf/

[22] "Management, provision and use of internet services and online information," Jul 2013. [Online]. Available: https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF/

[23] ".su domain name." [Online]. Available: https://www.netim.com/domain-name/su-domain.html/

[24] I. Stadnik, "Internet governance in russia–sovereign basics for independent runet," *Available at SSRN 3421984*, 2019.

[25] "Global cybersecurity index," 2019. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[26] I. W. Stats, "Internet world stats, usage and polulation statistics," accessed on 18 Sep 2019. [Online]. Available: https://www.internetworldstats.com/list1.htm

[27] "Approved doctrine of information security of russia," Dec 2016. [Online]. Available: http://kremlin.ru/acts/news/53418

[28] "Information security doctrine of the russian federation," Dec 2016. [Online]. Available: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

[29] "Conceptual views on the activities of the armed forces of the russian federation in the information space," 2011. [Online]. Available: https://tinyurl.com/yxdmelhe

[30] "The ministry of defense of the russian federation created the troops of information operations," Feb 2017. [Online]. Available: https://www.interfax.ru/russia/551054

[31] "Introduced cyber military," Oct 2017. [Online]. Available: https://www.kommersant.ru/doc/3187320

[32] "Cyber wars 2017: Balance of forces in the world," Jan 2017. [Online]. Available: https://tinyurl.com/y3m8x9l6

[33] "Ru cert." [Online]. Available: https://www.cert.ru/en/about.shtml

[34] "First." [Online]. Available: https://www.first.org/

[35] "Cert gib." [Online]. Available: https://www.group-ib.com/cert.html

[36] "Gov cert." [Online]. Available: http://www.gov-cert.ru/en/incident.htmll

[37] "Fincert." [Online]. Available: https://www.cbr.ru/eng/fincert/

[38] "Kaspersky industrial cybersecurity." [Online]. Available: https://ics.kaspersky.com/

[39] "Maps.net." [Online]. Available: https://www.maps.net/yandex-maps

[40] "Russia' s top 10 websites." [Online]. Available: https://venturebeat.com/2016/10/01/russias-top-10-websites-include-facebook-google-instagram-and-youtube/

[41] "Top sites ranking for all categories in russian federation." [Online]. Available: https://www.similarweb.com/top-websites/russian-federation

[42] "Decree of the president of the russian federation of january 15, 2013 n 31s moscow," Jan 2013. [Online]. Available: https://rg.ru/2013/01/18/komp-ataki-site-dok.html

[43] "Protection of critical information infrastructure, russian federation," Jul 2017. [Online]. Available: https://tinyurl.com/yydo3wm6

[44] "Russian itc security policy and cybercrime," Jul 2019. [Online]. Available: http://www.ponarseurasia.org/memo/russian-itc-security-policy-and-cybercrime

[45] "Territorial structure of gossopka," Mar 2015. [Online]. Available: https://www.securitylab.ru/blog/personal/sborisov/131813.php

[46] "List of information submitted to the state system," Sep 2018. [Online]. Available: https://tinyurl.com/y4pz73eu

[47] "Procedure for exchange of information on computer incidents," Sep 2018. [Online]. Available: https://tinyurl.com/y3544rag

[48] "Register of russian programs." [Online]. Available: https://reestr.minsvyaz.ru/reestr/

[49] "The ministry of communications, the fsb and the ministry of defense conducted exercises to protect the russian segment of the internet." [Online]. Available: https://digital.gov.ru/ru/events/31441/

[50] "Report on the sovereignty of the russian internet." [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/03/26/ministr-svyazi-predlozhit-gosudarstvu-vzyat-runet-pod-kontrol

[51] "Ministry of telecommunications and communications conducts exercises to improve information security, integrity and stability of the functioning of the unified telecommunication network of the russian federation." [Online]. Available: https://digital.gov.ru/ru/events/37727/

[52] "Procedure for centralized management of a public communication network." [Online]. Available: https://regulation.gov.ru/projects#npa=91558

[53] "Revizor: how does the system for controlling prohibited content work." [Online]. Available: https://tinyurl.com/y38tmnxg

[54] "A national internet filtering system will appear in russia for russians will prepare "white lists" of trusted sites," Aug 2017. [Online]. Available: https://iz.ru/627080/natcionalnaia-sistema-filtratcii-internet-trafika-poiavitsia-v-rossii

[55] "Russia - data protection overview," Aug. 2019. [Online]. Available: https://www.dataguidance.com/notes/russia-data-protection-overview

[56] "Russia clarifies threats that would lead it to decouple runet from world wide web," May 2019. [Online]. Available: https://tinyurl.com/yxjpdfwy

[57] "Duma toughens punishment for cyber attacks on critical infrastructure," Jul 2017. [Online]. Available: https://www.rbc.ru/rbcfreenews/5965db569a7947293d13be16

[58] "Amendments to the federal law on communications and the federal law on information, information technologies and the protection of information," May 2019. [Online]. Available: https://tinyurl.com/y6p3hr8f

[59] "A closer look at the "sovereign runet" law," May 2019. [Online]. Available: https://tinyurl.com/yyt8wz3a

[60] N. Schia and L. Gjesvik, "China's cyber sovereignty (policy brief)," 04 2017. [Online]. Available: https://tinyurl.com/y5y9fvcs

[61] L. Diamond, "Liberation technology 1," in *In Search of Democracy*. Routledge, 2015, pp. 132–146.

[62] "State stamps out small 'jasmine' protests in china," Feb 2011. [Online]. Available: http://content.time.com/time/world/article/0,8599,2052860,00.html

[63] "Nsa prism program taps in to user data of apple, google and others." [Online]. Available: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[64] D. C. Pitt, N. Levine, and X. Yan, "Touching stones to cross the river: Evolving telecommunication policy priorities in contemporary china," *Journal of Contemporary China*, vol. 5, no. 13, pp. 347–365, 1996.

[65] "China (finally) admits to hacking," Mar 2015. [Online]. Available: https://thediplomat.com/2015/03/china-finally-admits-to-hacking/

[66] E. B. Kania and J. K. Costello, "The strategic support force and the future of chinese information operations," *The Cyber Defense Review*, vol. 3, no. 1, pp. 105–122, 2018.

[67] T. Stevens, "Breaching protocol. the threat of cyber spionage," *Jane's Intelligence Review (Coulsdon)*, vol. 22, no. 3, pp. 8–13, 2016.

[68] M. Reud, "China and cyber: Attitudes, strategies, organization," *Tallinn Paper*, pp. 5–34, 2016.

[69] "Huawei product security incident response team." [Online]. Available: https://www.huawei.com/en/psirt

[70] "Zte psirt." [Online]. Available: http://wwwen.zte.com.cn

[71] "Dahua psirt." [Online]. Available: https://www.dahuasecurity.com/support/cybersecurity/

[72] "Alibaba security response center." [Online]. Available: https://security.alibaba.com/

[73] "National computer network emergency response technical team/coordination center of china." [Online]. Available: https://www.cert.org.cn/publish/english/index.html

[74] "Everec - hengan jiaxin (beijing) technology co., ltd." [Online]. Available: http://eversec.com.cn/about_eversec/

[75] "Hikvision cyber security center." [Online]. Available: https://www.hikvision.com/en/Support/Cybersecurity-Center/

[76] "Qi an xin cert." [Online]. Available: https://www.qianxin.com

[77] "Data star observatory." [Online]. Available: https://www.shuziguanxing.com/about.html

[78] F. N. Pieke, "The communist party and social management in china," in *Critical Readings on Communist Party of China*. BRILL, 2017, pp. 998–1018.

[79] F. Shen, *Great Firewall of China*, 01 2014, pp. 599–602.

[80] B. Marczak, N. Weaver, J. Dalek, R. Ensafi, D. Fifield, S. McKune, A. Rey, J. Scott-Railton, R. Deibert, and V. Paxson, "An analysis of china' s "great cannon" ," in *5th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 15)*, 2015.

[81] "Complete list of blocked websites in china." [Online]. Available: https://www.vpnmentor.com/blog/the-complete-list-of-blocked-websites-in-china-how-to-access-them/

[82] "China is said to use powerful new weapon to censor internet," April 2015. [Online]. Available: https://nyti.ms/1Nj59yc

[83] "China' s cybersecurity law - 2017," May 2018. [Online]. Available: https://www.chinalawblog.com/2018/05/china-data-protection-regulations-cdpr.html

[84] "Development of prc regulations on cross-border data transfer," Jun 2019. [Online]. Available: https://www.chinalawinsight.com/2019/06/articles/crossing-borders/development-of-prc-regulations-on-cross-border-data-transfer/

[85] "China issues draft regulation on cross-border transfer of personal information," Jun 2019. [Online]. Available: https://tinyurl.com/y65ffmmg

[86] "China' s first cyber threat intelligence sharing platform expected to further upgrade nation' s cyber defense," Jan. 2019. [Online]. Available: http://en.people.cn/n3/2019/0118/c90000-9539303.html

[87] M. of Foreign Affairs, "International strategy of cooperation on cyberspace," 2017. [Online]. Available: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml

[88] "Qiushi journal - organ of the central committee of the communist party of china."

[89] "In-depth implementation of general secretary xi jinping's strategic thinking of network power, solidly promote network security and informationization," Sep 2017. [Online]. Available: https://tinyurl.com/y38aom8q

[90] "Broadband china strategy." [Online]. Available: https://tinyurl.com/y4f46s2a

[91] "Internet plus," May 2015. [Online]. Available: https://tinyurl.com/y4mo4jgc

[92] M. Mueller, *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Wiley, 2017.

[93] "Does china have an internet kill switch?" Apr 2012. [Online]. Available: https://tinyurl.com/y45au2jv

[94] "Section 2: Operations security for critical information infrastructure - cybersecurity law of the people' s republic of china," Jun. 2018. [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[95] R. FEDERATION, "Federal law no. 242-fz," Jul. 2014. [Online]. Available: https://pd.rkn.gov.ru/authority/p146/p191/

[96] "Russian national security strategy," Dec 2015. [Online]. Available: https://tinyurl.com/y64bgcum

[97] "New kremlin information-security doctrine calls for 'managing' internet in russia," Dec 2016. [Online]. Available: https://www.rferl.org/a/russia-informaiton-security-internet-freedome-concerns/28159130.html

[98] "Cyber operations tracker." [Online]. Available: https://www.cfr.org/interactive/cyber-operations#CyberOperations

[99] N. Popescu and S. Secrieru, "Hacks, leaks and disruptions: Russian cyber strategies," *Luxembourg: Publications Office*, Oct. 2018. [Online]. Available: https://tinyurl.com/y6raocmw

[100] "New senate intelligence report shows "extensive" russia 2016 election interference," Jul. 2019. [Online]. Available: https://www.vox.com/2019/7/25/8930616/senate-intelligence-report-russia-50-states

[101] "Russian interference in 2016 u.s. elections." [Online]. Available: https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

[102] "Hackers breach defences of joint strike fighter jet programme," Apr. 2009. [Online]. Available: https://www.theguardian.com/world/2009/apr/21/hackers-us-fighter-jet-strike

[103] "U.s. weapons system designs compromised by chinese cyberspies," May 2013. [Online]. Available: https://tinyurl.com/y4pgtb88

[104] "China has stolen vast amounts of navy submarine, missile data in multiple breaches from contractor' s servers," Jun. 2018. [Online]. Available: https://tinyurl.com/y2cxgn5b

[105] "Rostec." [Online]. Available: https://rostec.ru/en/about/history/

[106] "Rostec engaged in a response to cyber threats," Nov. 2016. [Online]. Available: https://iz.ru/news/642771

[107] "microelectronics illegally purchased in the usa can be used to create wiretapping technologies and to falsify negotiations in the interests of russian special service," Oct. 2013. [Online]. Available: https://tinyurl.com/y6nondcx

[108] "Moscow's cyber-defense how the russian government plans to protect the country from the coming cyberwar," Jul. 2017. [Online]. Available: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense

[109] “ “threats to information security are becoming ever more sophisticated and widespread.” ,” May 2017. [Online]. Available: https://www.kommersant.ru/doc/3303788

[110] “Ntsci: The maximum number of computer attacks on the runet was recorded on the day of the election of the president of the russian federation,” Nov. 2018. [Online]. Available: https://www.mskagency.ru/materials/2844609

[111] “Russia thwarts u.s. cyber attacks on its infrastructure,” 2019. [Online]. Available: https://tinyurl.com/yytykeqe

[112] “China broadens cyber options,” Jan. 2020 - Retrieved on 15 August 2020. [Online]. Available: https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/

[113] “China’s cybersecurity landscape from the perspective of cncert/cc,” 2014. [Online]. Available: https://tinyurl.com/y4zg7grd

[114] “New cncert report shows most cyber attacks on china originate from united states,” 2019. [Online]. Available: https://tinyurl.com/y6rszbqh

[115] “Russian software is disconnected from abroad,” Dec 2018. [Online]. Available: https://www.kommersant.ru/doc/3827670

[116] “China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech,” May 2019. [Online]. Available: https://tinyurl.com/y4j5759o

[117] “Made in china 2025, explained,” Feb 2019. [Online]. Available: https://thediplomat.com/2019/02/made-in-china-2025-explained/

[118] “The 5 biggest chinese software companies,” Jun 2019. [Online]. Available: https://www.investopedia.com/articles/markets/032616/5-biggest-chinese-software-companies-chl-tcehy.asp

[119] "The cost of shutting down the internet," Apr. 2019. [Online]. Available: https://www.websitebuilderexpert.com/blog/cost-of-shutting-down-the-internet/

[120] "China presses for internet 'kill switch'," Jul. 2015. [Online]. Available: https://www.endtime.com/prophecy-news/china-presses-for-internet-kill-switch/

[121] "China's internet users temporarily blocked from foreign websites," Apr. 2012. [Online]. Available: https://www.theguardian.com/world/2012/apr/12/china-internet-users-foreign-websites

[122] "Google began to remove sites banned in russia from search," Feb 2019. [Online]. Available: https://www.vedomosti.ru/technology/articles/2019/02/06/793499-google

[123] "A national internet filtering system will appear in russia," Aug 2017. [Online]. Available: https://iz.ru/627080/natcionalnaia-sistema-filtratcii-internet-trafika-poiavitsia-v-rossii

[124] C. Tang, "In depth analysis - great firewall of china," Dec 2016. [Online]. Available: https://www.cs.tufts.edu/comp/116/archive/fall2016/ctang.pdf

[125] "Tor: Pluggable transports." [Online]. Available: https://2019.www.torproject.org/docs/pluggable-transports.html.en

[126] C. Tang, "Linkedin blocked by roskomandzor," Nov 2016. [Online]. Available: https://rkn.gov.ru/news/rsoc/news41615.htm

[127] "Russia opens civil proceedings against facebook and twitter," Jan 2019. [Online]. Available: https://www.cnbc.com/2019/01/21/russia-reportedly-opens-civil-proceedings-against-facebook-twitter.html

[128] "Russian data localization laws: Enriching "security" & the economy," Feb. 2018. [Online]. Available: https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/

[129] "Apple provides details on compliance with russian data-localization law," Feb. 2019. [Online]. Available: https://tinyurl.com/y5uz6hoy

[130] "Datacenterdynamics, "data moves to mother russia" ." [Online]. Available: https://tinyurl.com/y3meresp

[131] "Huawei moves into russian cloud market with third-party data centre support," Mar. 2019. [Online]. Available: https://tinyurl.com/yy89uq8j

[132] "Chinese data localization law: Comprehensive but ambiguous," Feb. 2018. [Online]. Available: https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/

[133] "Apple' s data center in guizhou develops rapidly amid trade war," 2019 - Retrieved on 16 August 2020. [Online]. Available: https://www.globaltimes.cn/content/1173163.shtml

[134] "https://data-economy.com/asia-2020-everything-is-bigger-in-china/," May 2019. [Online]. Available: https://data-economy.com/asia-2020-everything-is-bigger-in-china/

[135] "Regional data centres in china are only half-used admits government," Nov. 2018. [Online]. Available: https://tinyurl.com/y4dabf97

[136] "China's strict new cybersecurity law ensnares japanese companies," Jun. 2018. [Online]. Available: https://asia.nikkei.com/Business/Business-trends/China-s-strict-new-cybersecurity-law-ensnares-Japanese-companies

[137] "Development of prc regulations on cross-border data transfer," Jun. 2019. [Online]. Available: https://www.chinalawinsight.com/2019/06/articles/crossing-borders/development-of-prc-regulations-on-cross-border-data-transfer/

[138] "Law "about security of critical information infrastructure of the russian federation"," Jul. 2019. [Online]. Available: https://tinyurl.com/y6j4t3zm

[139] "Recent developments in chinese cybersecurity and information technology regulations," Jun. 2019. [Online]. Available: https://www.jdsupra.com/legalnews/recent-developments-in-chinese-28952/

[140] "China' s emerging cyber governance system," 2019. [Online]. Available: https://www.csis.org/chinas-emerging-cyber-governance-system

[141] "Social indicators," 2019. [Online]. Available: https://unstats.un.org/unsd/demographic/products/socind/default.htm

[142] "Itu statistics," 2019. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[143] "Global cybersecurity index & cyberwellness profiles," 2019. [Online]. Available: https://www.itu.int/pub/D-STR-SECU

[144] ICANNWiki, ".ru cctld." [Online]. Available: https://icannwiki.org/Coordination_Center_for_TLD_RU

[145] ——, ".cn cctld." [Online]. Available: https://icannwiki.org/China_Internet_Network_Information_Center

[146] M. Smeets, "The strategic promise of offensive cyber operations," 2018. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf

[147] "Beijing orders state offices to replace foreign pcs and software." [Online]. Available: https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406

[148] BBC, "Russia enacts 'draconian' law for bloggers and online media," 2014. [Online]. Available: https://www.bbc.com/news/technology-28583669

[149] T. Guardian, "Why you should worry if you have a chinese smartphone." [Online]. Available: https://www.theguardian.com/technology/2019/oct/26/china-technology-social-management-internet-social-credit-system

[150] S. Council, "Circular of the state council on printing and distributing the outline of the construction of the social credit system (2014-2020)," 2014. [Online]. Available: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

[151] "Government responses to disinformation on social media platforms: China," 2020. [Online]. Available: https://www.loc.gov/law/help/social-media-disinformation/china.php

[152] "What fstec says about industrial cyber security standards," 2019. [Online]. Available: https://h-on.it/fstec-russian-industrial-cyber-security/

[153] FSTEC, "State register of certified information security tools." [Online]. Available: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi

[154] "New draft rules for 'critical network equipment security testing' in china," 2019. [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-critical-network-equipment-testing-implementing-measures-draft-comment/

[155] "About pknic." [Online]. Available: https://www.pknic.net.pk/about.html

[156] "Middle east domain study," Oct. 2015. [Online]. Available: https://www.icann.org/en/system/files/files/eurid-middle-east-dns-study-initial-13oct15-en.pdf

[157] Pakistantoday, "Data of nadra, police and telecom companies being publicly sold: report," May 2018. [Online]. Available: https://www.pakistantoday.com.pk/2018/05/07/data-of-nadra-police-and-telecom-companies-being-publicly-sold-report/

[158] A. Sheikh, "Pakistan starts investigations into data breach of 115 million telecom users," Apr.

2020. [Online]. Available: https://pk.mashable.com/tech/2620/pakistan-starts-investigations-into-data-breach-of-115-million-telecom-users

[159] M. S. Ullah, "A caveat in pakistan' s cyber laws," Online, Apr. 2019 - Accessed 01 July 2020. [Online]. Available: https://nation.com.pk/20-Apr-2019/a-caveat-in-pakistan-s-cyber-laws

[160] zeenews, "China, pakistan lead cyber attacks against india, over 1 lakh websites hacked since 2015," Online, Mar. 2020 - Retrived on 2 July 2020. [Online]. Available: https://tinyurl.com/woopzt6

[161] "National cyber security council act 2014," 2014 - Retrived on 04 July 2020. [Online]. Available: http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf

[162] "Pakcert," Retrived on 2 July 2020. [Online]. Available: https://www.pakcert.org/aboutus.html

[163] "Pisa," Retrived on 4 July 2020. [Online]. Available: https://www.pisa.org.pk/

[164] "Trillium," Retrived on 04 July 2020. [Online]. Available: https://infosecurity.com.pk/index.php

[165] "Ncsael," Retrieved on 05 July 2020. [Online]. Available: https://ncsael.mcs.nust.edu.pk/AboutUs.html

[166] "Nust csael team makes pakistan proud at oic-cert cyber drill," Retrieved on 05 July 2020. [Online]. Available: http://www.nust.edu.pk/News/Pages/NUST-CSAEL-Team-makes-Pakistan-Proud-at-OIC-CERT-Cyber-Drill.aspx

[167] "Nr3c," Retrieved on 05 July 2020. [Online]. Available: http://www.nr3c.gov.pk/index.html

[168] "Kpcerc," 2020- Retrieved on 19 August 2020. [Online]. Available: https://www.kpcerc.com/

[169] "Peca," 2016 - Retrieved on 05v July 2020. [Online]. Available: http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

[170] "Nccs," Retrieved on 06 July 2020. [Online]. Available: http://www.nccs.pk/

[171] "Pakistan cyber security cluster," Retrieved on 06 July 2020. [Online]. Available: http://www.nccs.pk/cluster/cluster-home

[172] "Punjab govt bans use of whatsapp in government offices," Feb. 2020 - Retrieved on 06 July 2020. [Online]. Available: https://nation.com.pk/16-Feb-2020/punjab-govt-bans-use-of-whatsapp-in-government-offices

[173] "Cabinet approves policy for local manufacturing of mobile phone," Jun. 2020 - Retrieved on 06 July 2020. [Online]. Available: https://profit.pakistantoday.com.pk/2020/06/03/cabinet-approves-policy-for-local-manufacturing-of-mobile-phones/

[174] "Nitb," Retrieved on 06 July 2020. [Online]. Available: https://nitb.gov.pk/AllServices

[175] "Pitb." [Online]. Available: https://www.pitb.gov.pk/about

[176] "Information, science & technology department, goivernment of sind," Retrieved on 06 Jul 2020. [Online]. Available: https://istd.sindh.gov.pk/

[177] "Kpitb," Retrieved on 06 Jul 2020. [Online]. Available: https://www.kpitb.gov.pk/about

[178] "It board og aj&k," Retrieved on 06 Jul 2020. [Online]. Available: https://itb.ajk.gov.pk/

[179] "Submarinecablemap," Retrieved on 06 july 2020. [Online]. Available: https://www.submarinecablemap.com/

[180] "Killswitch timeline in pakistan," Retrieved on 06 July 2020. [Online]. Available: https://killswitch.pk/

[181] "The constitution of pakistan," Retrieved on 06 July 2020. [Online]. Available: http://www.pakistani.org/pakistan/constitution/part2.ch1.html

[182] R. R. J. Z. Ronald Deibert, John Palfrey, Ed., *Access contested : security, identity, and resistance in Asian cyberspace*, 2011.

[183] "Ihc stops imcew from issuing directions to pta," 2014 - Retrieved on 07 July 2020. [Online]. Available: https://nation.com.pk/16-Dec-2014/ihc-stops-imcew-from-issuing-directions-to-pta

[184] Dailytimes, "Bolo bhi submits written arguments in case against govt, pta," Nov. 2017 0 Retrieved on 078 July 2020. [Online]. Available: https://dailytimes.com.pk/145903/bolo-bhi-submits-written-arguments-case-govt-pta/

[185] G. of Pakistan, "Anti terrorism act 1997," Retrieved on 08 July 2020. [Online]. Available: https://www.ppra.org.pk/doc/anti-t-act.pdf

[186] U. S. I. O. PEACE, "An appraisal of pakistan' s anti-terrorism act," Online, 2015 - Retrieved on 8 July 2020. [Online]. Available: https://www.usip.org/sites/default/files/SR377-An-Appraisal-of-Pakistan%E2%80%99s-Anti-Terrorism-Act.pdf

[187] Propakistani, "Ngos weakened cyber crime law for vested interests: Anusha," 2017 - Retrieved on 07 July 2020. [Online]. Available: https://propakistani.pk/2017/04/05/ngos-weakened-cyber-crime-law-vested-interests-anusha/

[188] G. of Pakistan, "Citizens protection (against online harm) rules, 2020," Jan. 2020 - Retrieved on 13 July 2020. [Online]. Available: https://www.medianama.com/wp-content/uploads/CP_Against_Online_Harm_Rules_2020.pdf

[189] DAWN, "Pm wants all stakeholders on board over social media rules," Feb. 2020 - Retrieved on 13 July 2020. [Online]. Available: https://perma.cc/BSK3-8CDB

[190] T. Ahmad, "Pakistan: Federal government issues controversial rules on social media content," Mar. 2020 - Retrieved on 13 July 2020. [Online]. Available: https://www.loc.gov/law/foreign-news/article/pakistan-federal-government-issues-controversial-rules-on-social-media-content/

[191] DAWN, "Impossible to block all obscene content, pta tells sc," Feb. 2016 - Retrieved on 13 July 2020. [Online]. Available: https://www.dawn.com/news/1237500

[192] Tribune, "Pakistan to block over 400,000 porn websites," Jan. 2020 - Retrieved on 19 July 2020. [Online]. Available: https://tribune.com.pk/story/1034224/objectionable-content-isps-ordered-to-block-400000-pornographic-websites

[193] "Faebook transparency pakistan," 2019 - Retrieved on 13 July 2020. [Online]. Available: https://govtrequests.facebook.com/content-restrictions/country/PK/

[194] BBC, "Pakistan unblocks access to youtube," Jan. 2016 - Retrieved on 14 July 2020. [Online]. Available: https://www.bbc.com/news/world-asia-35345872

[195] "Google transparency report," 2020 - Retrieved on 14 July 2020. [Online]. Available: https://tinyurl.com/y7g4ta2c

[196] T. C. Lab, "O pakistan, we stand on guard for thee," Jun. 2013 - retrieved n 14 July 2020. [Online]. Available: https://citizenlab.ca/2013/06/o-pakistan/

[197] D. News, "Wordpress banned in pakistan over," Mar. 2015 - Retrieved n 14 July 202. [Online]. Available: http://dunyanews.tv/en/Technology/269156-WordPress-banned-in-Pakistan-over-security-issues

[198] Digitalrightsfoundation, "Drf and netblocks find blanket and nation-wide ban on social media in pakistan and demand it to be lifted immediately," Nov. 2017 - Retrieved on 14 July 202. [Online]. Available: https://digitalrightsfoundation.pk/press-release-drf-and-netblocks-find-blanket-and-nation-wide-ban-on-social-media-in-pakistan-a

[199] T. Nation, "Activists assail blanket ban on social media," Nov. 2017 - Retrieved on 14 July 202. [Online]. Available: https://nation.com.pk/27-Nov-2017/activists-assail-blanket-ban-on-social-media

[200] S. Jamal, "Playerunknown's battlegrounds banned in pakistan following spate of suicides," Jul. 2020 - Retrieved on 14 July 202. [Online]. Available: https://gulfnews.com/world/asia/pakistan/playerunknowns-battlegrounds-banned-in-pakistan-following-spate-of-suicides-1.72382025

[201] "Pubg unbanned," 2020 Retrieved on 20 August 2020. [Online]. Available: https://www.dawn.com/news/1571972

[202] S. K. Niazi, "A critical analysis of various web domains in pakistan –anomalies and countermeasures," Master's thesis, National University of Scuiences and Technology, 2017.

[203] natlawreview, "Pakistan's data protection bill includes localization and registration provisions," May 2020 - Retrieved on 14 July 2020. [Online]. Available: https://www.natlawreview.com/article/pakistan-s-data-protection-bill-includes-localization-and-registration-provisions

[204] "Tune.pk desrve 2nd rank in pakistan," 2015 - Retrieved on 15 July 2020. [Online]. Available: http://oraaq.blogspot.com/2015/07/top-10-earning-websites-of-pakistan-in.html

[205] "Alexa ranking tune.pk," Jul. 2020 - Retrieved on 15 July 2020. [Online]. Available: https://www.alexa.com/siteinfo/tune.pk

[206] "Tellotalk," Jul. 2020 - Retrieved on 15 July 2020. [Online]. Available: https://play.google.com/store/apps/details?id=com.udna.tellotalk

[207] N. Shafqat, "Pakistan's cyber space security. critical analysis and counter measures," Master's thesis, National University of Sciences and Technology, Jan. 2016.

[208] "National telecommunication & information security board (ntisb)," Retrieved on 15 july 2020. [Online]. Available: http://www.cabinet.gov.pk/Detail/OWYxZTYxMWQtNDZhMC00M2IyLTk1NDgtODNmNTMxNmNlNGU0

[209] "Ntisb advisories," Retrieved on 15 July 2020. [Online]. Available: http://www.cabinet.gov.pk/Detail/NjcwOTM5YTgtMDM4MC00OWQ4LWIyZGItYTc0MjBjZGVhODcw

[210] "Digital pakistan 2018," 2018 - Retrieved on 16 July 2020. [Online]. Available: http://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY(22-05-2018).pdf

[211] Digitalpakistan, "The digital pakistan policy: Vision and execution," Apr. 2020 - Retrieved on 16 July 2020. [Online]. Available: https://digitalpakistan.pk/blog/the-digital-pakistan-policy-vision-and-execution/

[212] G. Miller, "The intelligence coup of the century," Feb. 2020 - Retrieved on 18 July 2020. [Online]. Available: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

[213] llen Nakashima and J. Gillum, "U.s. moves to ban kaspersky software in federal agencies amid concerns of russian espionage," Sep. 2017 - Retrieved on 18 July 2020. [Online]. Available: https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html

[214] G. S. Ellen Nakashima and J. Hudson, "Leaked documents reveal huawei' s secret operations to build north korea' s wireless network," Jul. 2019 - Retrieved on 18 July 2020. [Online]. Available: https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html

[215] "Ixp in pakistan," Retrieved on 19 July 2020. [Online]. Available: http://www.pkix.pk/stakeholders.html

[216] R. Mitchell, "Trust, neutrality keys to sustainable internet exchange, pakistan," Jun. 2020 - Retrieved on 19 July 2020. [Online]. Available: https://blog.apnic.net/2020/06/17/trust-neutrality-keys-to-sustainable-internet-exchange-pakistan/

[217] "Pta asks internet users to register vpns to avoid ban after june 30," Jun. 2020- Retrieved on 20 July 2020. [Online]. Available: https://www.dawn.com/news/1563843