

Intellectual Property Rights & Cyber Law

Final Report

**BSCS (Hons) Semester-VIII
Session 2016-2020**

Comparison of National
cyber policies of different
countries
(US, India, Pakistan)

Submitted by Taha Hussain, 121-BSCS-16

Department of Computer Science
GC University, Lahore

Table of Contents

Introduction	3
The National policy and Strategy	3
Cyber Security	3
The national cyber policy and strategy	4
The US national cyber strategy/policy	4
The India national cyber strategy/policy	5
The Pakistan national cyber strategy/policy	6
Conclusion	6
References	7

Introduction

Cyber security is one the main concern for countries these days. Cyber space is known as 5th dimension of war. Internet is now considered the basic right human. The development and prosperity of country now a day depends on its digital power and capabilities. Every country is trying to become better and better is this race of development. The Internet made our lives easy and the cloud made it possible for everyone to store their data and do processing without some kind of special hardware. Nations are using this cloud and internet to digitize themselves. But the internet also opens a new way of attacks and crimes So every nation must have some national policies to maintain the security and use of internet and cyberspace. Without these policies nothing is secure and our data government as well as private is in danger. Data is most important assets. Losing this data can cause heavy destruction. In this paper we will look at cyber policies of different countries and compare them with each other. We will also see where Pakistan stands right know.

A national policy/strategy:

Policy is a course of action that help in decision making and made to meet a specific goal. It consist of principle and guide lines .Its full course of action. National policy is the policy made by policy maker and is made for a country and implemented on nation, Policy defines vision and goal for government and all related departments. It's an alignment for nation. Whole nation and government must have to follow it. Policies are part of strategies.

Cyber Security:

Internet is the connection of networks, hardware, and computers, this network of networks is growing day by days. Banks are digitizing them self, government as well as private organizations are digitizing them self. Business are going online. And cloud is introduced without any specific hardware you can use cloud to store data and process it. Country prosperity is directly linked to its it industry and digitization. The internet is also called cyber space. It made life easier that is the cause of its popularity. Everything is just one click away we can communicate with people from all around the world. But as it made life easier. It also has become a hub for crimes. Dark web constitutes a major part of this space where from child pornography to terrorist selection and funding drugs to hacking every kind of crime is there. Hackers are hacking computer stealing data from countries. Virus and a lot of threats are there. The security is must be provided to make internet peaceful. The Security from all these crimes and punishment to the crimes must be introduced. The term cyber security means protection from the threats on internet and taking appropriate measures if something happens and make sure it does not happen again.

The national cyber policy and strategy

The security of its people and nation is the prime responsibility of nation. Cyber security as define is the security of people on internet. The policy or strategy made to protect people and nation from cyber threats made by policy makers and align different institutes and government together are national cyber polices or strategy. Data is the most important assets for any institute or nation. every country protects its data at any cost. Countries made their strategies and policy to inforce the protection of it people and its self. We will look at their differences and similarities.

US Cyber Strategy/Policy.

US as we know is one of the most powerful and advance country. The IT field is one the gigantic field in US.US is very focused on its cyber security and protection of national data, it is full digitalize nation. The office of NCC (National Cyber Security Coordinator) is the lead of cyber security in US. It has direct access to the president. The department of home land Security (DHS), the national Security Agency(NSA) and Cybercom are main agency responsible for cyber security. The DHS protects the national critical infrastructure. The electricity grid, water works, rails and air ways are controlled using digital signal by SCADA .US CERT is responsible for response to cyber emerges and is under DHA. Other two bodies NSA and Cybercom are run by military. The Central Security Service and NSA are responsible for cryptology. Cybercom conducts cyber warfare and operation. The US cyber security budget shows the importance of this security (\$17.4 billion of budget). In 2018 a new cyber policy was made in white house with several amendments. In which America said the it will not sit back and it will respond defensively and aggressively to cyber threats. And will insure the protection of its people and government data. The American cyber strategies have 4 main pillars whose brief summary is

- Promotion of American life style, people and homeland by protection and cooperation which other countries to track down criminals
- American prosperity promotion by high quality professionals and government work with tech companies for enforcement of cyber security in products and trainings of workforce in his domain
- Preserving peace through strength by using all power to get criminal meet their consequences and collaboration with countries in this regard
- Advancement in American Influence by helping allies to fight cyber threat.

Indian Cyber security strategy/policy.

The Indian definition of cyber security is the protection of system and information using appropriate techniques and procedure. India is one the country that is known for its contribution to IT industry. Indian government is very serious for its cyber security and there is an in charge of cyber security that guides prime minister in this regard. India has its own department or Computer Emergency Response Team(CERT). Indian has been forming forums with other countries in cyber security regards. Three pacts were made by CERT with japan, Malaysia and Singapore. India had dialogue on cyber security with US and they both agree on increase cybersecurity and digital eco system.

India Israel relation are also expanding in this area. The Israel president has agreed on cooperation on big data and cybersecurity. Similarly, India has many discussions with Russia on the topic of cyber security and also an agreement is also signed.

In 2015 Cybersecurity budget was 775 cores and now 3,958 crore in 2020. The prime minister Modi is very focused on digitizing India. There were found few problems with policies and the government and officers took urgent steps to solve it. The national cyber Coordination Centre was made.

India is highly focused in his goals and there are trainings and other courses also offered for training of people and get them better educated.

Summary of few Main points India Cyber security policy are;

- Creation of secure cyber ecosystem, trust building in IT and adoption of IT
- Frame for cyber security policies according to global standard
- Regulation frame work for protected cyber space
- Creation of 24/7 national, sectoral mechanism for cyber security. Scenarios using prediction for response and crisis.
- Capacity building, skill development and training for 500,000 people in 5 year
- Information protection, protection of citizen data and reduction of loss due to data theft and cyber crime
- Enabling effective prevention, investigation and enhancing law

STRATEGIES

- Create secure ecosystem
- Create assurance frame work
- Increase strength of regulation framework

Comparison of National Cyber policies of Pakistan

- Mechanism creation for early warning, vulnerability management, security threat and response to them
- E Governance service security
- Research and development
- Training of human resource
- Awareness
- Public private partnership for effectiveness
- Relationship with other countries

For cyber Crime they have information Technology Act 2000

Pakistan Cyber security strategy/policy.

Like other countries around the globe Pakistan is also facing cyber threats. Few times there were discussion of cyber security policy e.g. cyber secure Pakistan seminar. The main thing done in Pakistan is the protection for electronic Crime at 2016 which defines punishment for cybercrimes including child pornography, Unauthorized access to information etc. But It was indeed a good work by government. But there is criticism that it gives too much power to PTA and freedom of speech and freedom of expression is taken away. Pakistan is one of the countries which other countries dislike much. Pakistani banks have been hacked more 6\$ million were lost with the information of accounts credit and debit card a report by Pak CERT but the head bank of Pakistan reported this happened on in bank of Islamic. Before Chinese President visit to Pakistan the foreign office computer was hacked. UK has a large number of communication data from Pakistan. There is no central authority to coordinate and no one is there to advise prime minister. Our FIA has NR3C national cyber response center for cybercrimes but it is limited and there is lack in its act as first responder to any crime. There is an initiative for cyber security training but is very limited. The judges here are not properly trained on cyber law

Conclusion

Pakistan is at very critical point. Countries like India and US are fully focusing on their cyber securities. In Pakistan there is only focus on border protection and all those physical thing. The topic of cyber security is not taken seriously. We need to develop a proper infrastructure of this. Like all other countries there must a Cyber security officer directly under prime minister to support him and advise him in this regard. Proper policies should be made for the policy making proper person should be there with keen knowledge and experience in relevant field. Proper training and awareness should be given to youth. As well as the Proper department

Comparison of National Cyber policies of Pakistan

should be made. Professional global merit training should be given to mass to generate a workforce that can help in any kind of threats CERT responsibly should be assigned and proper budget should be allocated as it is allocated to all other defensive. If we are failed to do so in time soon we will be doomed by not any physical war but this digital war. There will be no security or privacy for our nation. The government should also add proper cyber security testing in products. Pakistan should invest more in research development . Pakistan is constantly fighting terrorist and enemy and Think what can happen if NADRA and all our records and data is destroyed or stole and miss use by terrorist?

Yes, the situation is very critical. Our Government and national defense departments need to take this issue as a national security issue. Plus, the PECA Act and its problem must be resolve and our judges need to be properly trained .Pakistan need to collaborated with other countries as India is getting powerful as it made pacts with Israel .

References:

- [1] <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis>
- [2] www.cybercom.mil/About/Mission-and-Vision
- [3] dailytimes.com.pk/352011/cybersecurity-threats-policy-gaps-challenges-and-way-forward/
- [4] <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- [5] http://www.na.gov.pk/uploads/documents/1470910659_707.pdf
- [6] <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis>
- [7] Cyber Security: Where Does Pakistan Stand? By Rubab Syed, Ahmed Awais Khaver & Muhammad Yasin
- [8] Information Technology act 2000 (wikipedia)
- [9] National security Policy 2013
- [10] Cyberspace Management in Pakistan by Dr. Tughrul Yami
- [11] Nineteen national cyber security strategies by Eric Luijff* and Kim Besseling
- [13] UK hacked routers to monitor Pakistan communications data: Snowden. (2015, 6 October 2015). The Express Tribune. Retrieved from <http://tribune.com.pk/story/968194/uk-hacked-routers-to-monitor-pakistan-communications-data-snowden>

